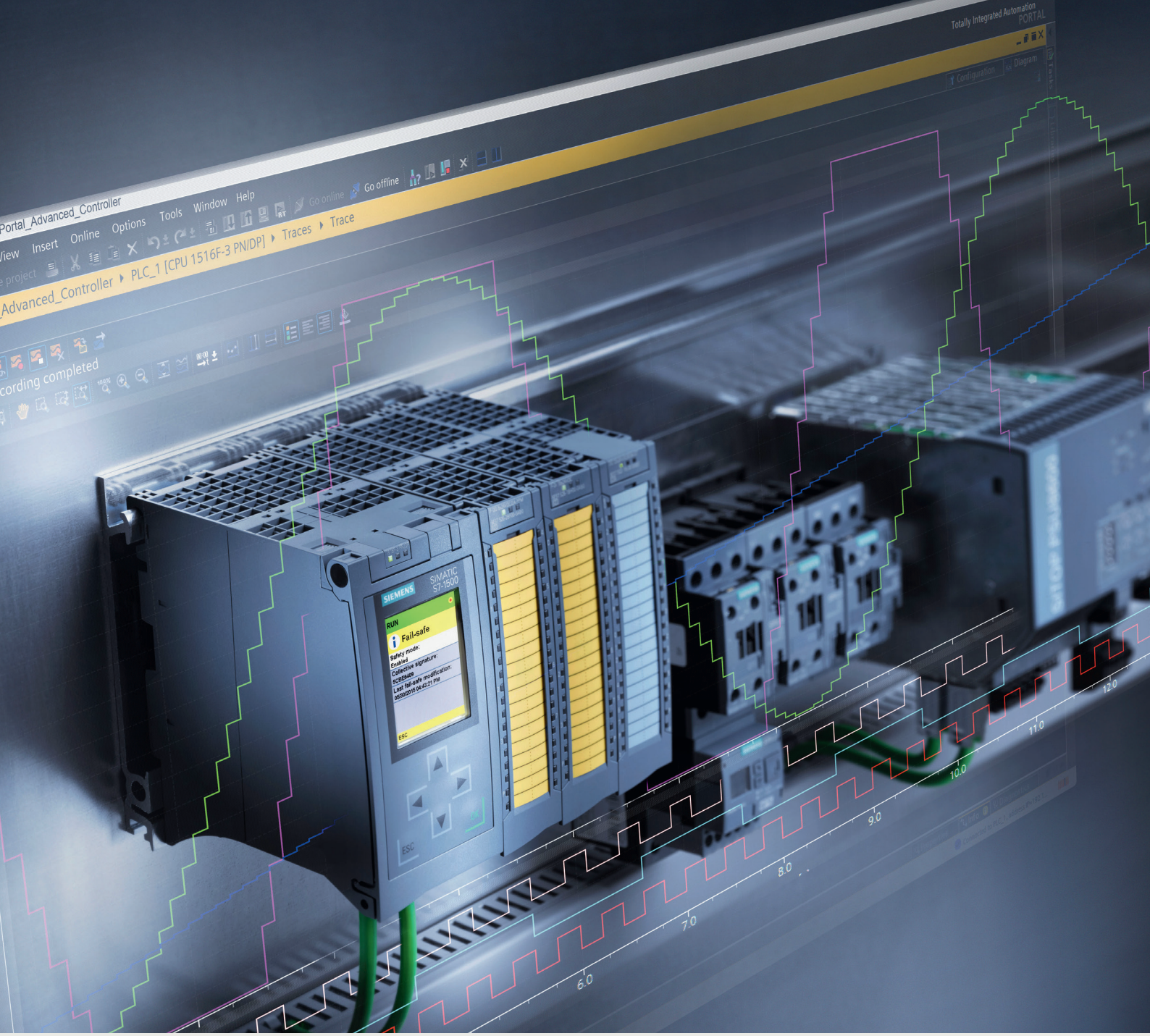


PODRĘCZNIK PROGRAMOWANIA I OBSŁUGI WYDANIE 1.

SIMATIC SAFETY

Konfiguracja i programowanie

siemens.pl/simatic

SIEMENS

SIEMENS

SIMATIC

Oprogramowanie przemysłowe SIMATIC Safety - Konfiguracja i programowanie

Instrukcja obsługi i programowania

Ważne uwagi

Opis produktu 1

Konfiguracja 2

Safety Administration Editor 3

Ochrona dostępu 4

Programowanie 5

Dostęp F-I/O 6

Wdrożenie zatwierdzenia użytkownika 7

Wymiana danych pomiędzy programem użytkownika a programem bezpieczeństwa 8

Komunikacja safety 9

Kompilowanie i finalizowanie programu bezpieczeństwa 10

Zatwierdzenie systemu 11

Obsługa i konserwacja 12

Instrukcje do STEP 7 Safety V16 13

Czasy monitorowania i odpowiedzi A

Lista kontrolna B

10/2019

A5E02714440-AK

Informacje prawne

System uwag ostrzegawczych

W niniejszej instrukcji zamieszczono uwagi, do których należy się stosować, by zapewnić bezpieczeństwo sobie, a także uchronić sprzęt przed uszkodzeniem. Uwagi dotyczące bezpieczeństwa osobistego są zaznaczone w instrukcji za pomocą symbolu ostrzegawczego, uwagi odnoszące się jedynie do możliwości uszkodzenia mienia nie są oznaczone. Ostrzeżenia przedstawione poniżej sklasyfikowano zgodnie ze stopniem zagrożenia.

⚠ NIEBEZPIECZEŃSTWO
wskazuje **wystąpienie** śmierci lub poważnego urazu ciała w przypadku niedostosowania się do środków ostrożności.
OSTRZEŻENIE
wskazuje **możliwość** wystąpienia śmierci lub poważnego urazu ciała w przypadku niedostosowania się do środków ostrożności.
⚠ **OSTROŻNIE**
wskazuje możliwość niewielkich urazów ciała w przypadku niedostosowania się do środków ostrożności.
UWAGA
wskazuje możliwość uszkodzenia mienia w przypadku niedostosowania się do środków ostrożności.

W przypadku występowania więcej niż jednego stopnia zagrożenia, zastosowane zostało ostrzeżenie przedstawiające najwyższy stopień. Ostrzeżenie przed urazem ciała z symbolem ostrzegawczym może również dotyczyć ryzyka uszkodzenia mienia.

Wykwalifikowany personel

Produkt/system opisany w niniejszej dokumentacji może być obsługiwany wyłącznie przez **wykwalifikowany personel** w celu wykonania określonego zadania zgodnie z odnośną dokumentacją, zwłaszcza z ostrzeżeniami i instrukcjami bezpieczeństwa.
Wykwalifikowany personel to osoba, w oparciu o szkolenie i doświadczenie, zdolna do identyfikowania ryzyka oraz unikania potencjalnego niebezpieczeństwa podczas pracy z produktami/systemami.

Prawidłowe użytkowanie produktów Siemens

Należy mieć na uwadze następujące zagadnienia:

⚠ OSTRZEŻENIE
Produkty firmy Siemens mogą być wykorzystywane jedynie w aplikacjach opisanych w katalogu oraz w odnośnej dokumentacji technicznej. W przypadku stosowania produktów i podzespołów innych producentów, muszą być one zalecane lub zatwierdzone przez firmę Siemens. Do zapewnienia bezpiecznej i bezproblemowej obsługi produktów konieczne jest zapewnienie odpowiedniego transportu, przechowywania, instalacji, montażu, odbioru technicznego, pracy oraz konserwacji. Należy przestrzegać dopuszczalnych warunków otoczenia. Należy stosować się do informacji zawartych w odnośnej dokumentacji.

Znaki

Wszystkie nazwy oznaczone znakiem ® są zarejestrowanymi znakami handlowymi firmy Siemens AG. Pozostałe znaki handlowe w tej dokumentacji mogą być znakami handlowymi, których wykorzystanie przez strony trzecie do własnych celów może stanowić naruszenie praw właściciela.

Ograniczenie odpowiedzialności

Treść niniejszego dokumentu została sprawdzona pod kątem spójności z opisanym sprzętem i oprogramowaniem. Jako że nie jest możliwe całkowite wykluczenie rozbieżności, nie można zagwarantować pełnej zgodności. Jednakże, informacje zawarte w tej publikacji są regularnie kontrolowane, a wszelkie niezbędne poprawki są wprowadzane w następnych edycjach.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E02714440-AK
Ⓟ 10/2019 Podlega zmianie

Copyright © Siemens AG 2011 - 2019.
Wszystkie prawa zastrzeżone

Ważne uwagi

Cel niniejszej dokumentacji

Informacje zawarte w niniejszej dokumentacji pozwalają na konfigurację (strona 41) oraz programowanie (strona 114) systemów typu fail-safe SIMATIC Safety. Ponadto zawarto informacje dotyczące odbioru (strona 376) systemu bezpieczeństwa SIMATIC Safety.

Uwaga

Instrukcja obsługi i programowania „SIMATIC Safety - Konfiguracja i programowanie" w najnowszej wersji (możliwie obejmująca informacje o produkcie) stanowi rzetelne źródło informacji dotyczących bezpieczeństwa funkcjonalnego podczas konfiguracji i programowania. Dotyczy to również przypadków rozbieżności pomiędzy instrukcją a inną dokumentacją dotyczącą bezpieczeństwa funkcjonalnego podczas konfigurowania i programowania urządzenia SIMATIC Safety.

Należy przestrzegać wszystkich ostrzeżeń zawartych w instrukcja obsługi i programowania „SIMATIC Safety - Konfiguracja i programowanie".

Podstawowe wymogi dotyczące wiedzy

Do zrozumienia tej dokumentacji wymagana jest podstawowa wiedza z zakresu automatyki. Niezbędna jest również podstawowa znajomość następujących zagadnień:

- Systemy automatyki typu fail-safe
- Systemy automatyki S7-300/400/1200/1500/1500 sterownik programowy/WinAC RTX F
- Systemy rozproszonych I/O na PROFIBUS DP/PROFINET IO
- Totally Integrated Automation Portal, w tym:
  - Konfiguracja sprzętowa za pomocą *edytora sprzętu i sieci*
  - Programowanie w językach the LAD oraz FBD przy użyciu *edytora programów*
  - Komunikacja pomiędzy CPU

Zakres niniejszej dokumentacji

Niniejsza dokumentacja dotyczy *STEP 7 Safety Advanced V16* oraz *STEP 7 Safety Basic V16*.

STEP 7 Safety Advanced V16 oraz *STEP 7 Safety Basic V16* służą do konfigurowania i programowania systemów typu fail-safe SIMATIC Safety.

W tym kontekście, integracja I/O typu fail-safe wyszczególnionych w SIMATIC

- modułów typu fail-safe S7-1500/ET 200MP
- modułów typu fail-safe ET 200SP
- modułów typu fail-safe ET 200S
- modułów I/O typu fail-safe ET 200eco
- modułów I/O typu fail-safe ET 200eco PN
- modułów O typu fail-safe ET 200pro
- modułów typu fail-safe ET 200iSP
- modułów sygnałowych typu fail-safe S7-300
- modułów typu fail-safe S7-1200
- urządzeń polowych DP opartych na GSD typu fail-safe
- urządzeń I/O opartych na GSD typu fail-safe

Aprobaty

System bezpieczeństwa SIMATIC Safety jest certyfikowany do użytku w trybie bezpieczeństwa do:

- Poziomu nienaruszalności bezpieczeństwa SIL3 zgodnie z normą IEC 61508:2010
- Poziomu niezawodności (PL) e oraz kategorii 4 zgodnie z normą ISO 13849-1:2015

Zastosowanie w architekturze informacyjnej

Zależnie od wykonywanej aplikacji, podczas pracy ze *STEP 7 Safety* konieczna będzie dokumentacja uzupełniająca.

W niniejszej dokumentacji znajdują się odniesienia do dokumentacji uzupełniającej.

Dokumentacja	Krótki opis treści
Do systemu bezpieczeństwa SIMATIC Safety	Zależnie od używanego CPU, konieczna będzie następująca dokumentacja: • W przypadku F-CPU S7-1200/1500, informacja produktowa (http://support.automation.siemens.com/WW/view/en/109478599) opisuje wszystkie rozbieżności względem odnośnych standardowych CPU. • Każdy F-CPU S7-300/400, który można zastosować, ma własną informację produktową. Informacja produktowa opisuje rozbieżności względem odnośnych standardowych CPU. • Instrukcje urządzeń (http://support.automation.siemens.com/WW/view/en/67295862/133300) opisują CPU S7-1500. • „S7-300, CPU 31xC oraz CPU 31x: instalacja" (http://support.automation.siemens.com/WW/view/en/13008499) instrukcja obsługi opisuje instalację oraz podłączenie systemów S7-300. • „CPU 31xC oraz CPU 31x, dane techniczne" (http://support.automation.siemens.com/WW/view/en/12996906) instrukcja urządzenia opisuje CPU typu 315-2 DP oraz PN/DP, CPU 317-2 DP oraz PN/DP, a także CPU 319-3 PN/DP. • Instrukcja instalacji „System automatyki S7-400, instalacja" (http://support.automation.siemens.com/WW/view/en/1117849) opisuje instalację i podłączenie systemów S7-400. • Podręcznik „System automatyki S7-400, dane CPU" (http://support.automation.siemens.com/WW/view/en/23904550) opisuje CPU 414-3 PN/DP, CPU 416-2 oraz CPU 416-3 PN/DP. • Podręcznik „Moduł interfejsu ET 200S IM 151-7 CPU" (http://support.automation.siemens.com/WW/view/en/12714722) opisuje jednostkę IM 151-7 CPU. • Podręcznik „ET 200S, moduł interfejsu IM 151-8 PN/DP CPU" (http://support.automation.siemens.com/WW/view/en/47409312) opisuje IM 151-8 PN/DP CPU. • Podręcznik „Moduł interfejsu ET 200S IM 154-8 CPU" (http://support.automation.siemens.com/WW/view/de/24363739/0/en) opisuje jednostkę IM 154-8 CPU. • Podręcznik „Windows Automation Center RTX WinAC RTX (F) 2010 (http://support.automation.siemens.com/WW/view/en/43715176)" opisuje oprogramowanie WinAC RTX 2010 oraz WinAC RTX F 2010. • Podręcznik „Sterownik programowalny S7-1500 CPU 1505SP, CPU 1507S (http://support.automation.siemens.com/WW/view/en/109249299)" opisuje sterownik programowalny SIMATIC S7-1500 1505SP oraz CPU 1507S.
Podręcznik systemowy „Bezpieczeństwo funkcjonalne S7-1200" (http://support.automation.siemens.com/WW/view/en/104547552)	Opisuje F-CPU S7-1200 oraz moduły typu fail-safe S7-1200 (w tym instalację, podłączenie oraz specyfikację techniczną)

Dokumentacja	Krótki opis treści
„Podręcznik systemowy S7-1500/ET200MP (http://support.automation.siemens.com/WW/view/en/59191792)" podręcznik systemowy oraz podręczniki produktowe (https://support.industry.siemens.com/cs/ww/en/ps/14141/man) do odnośnych modułów typu fail-safe S7-1500/ET 200MP	Opisuje warstwę sprzętową systemów S7-1500 oraz modułów typu fail-safe S7-1500/ET 200MP (w tym instalację, podłączenie oraz specyfikację techniczną)
„Rozproszone systemy I/O ET 200SP (http://support.automation.siemens.com/WW/view/en/58649293)" podręcznik systemowy oraz podręczniki produktowe (https://support.industry.siemens.com/cs/ww/en/ps/14059/man) do odnośnych modułów typu fail-safe ET 200SP	Opisuje warstwę sprzętową modułów typu fail-safe ET 200SP (w tym instalację, podłączenie oraz specyfikację techniczną)
Instrukcja „Bloki I/O typu fail-safe stacji rozproszonych I/O ET 200eco (http://support.automation.siemens.com/WW/view/en/19033850)"	Opisuje warstwę sprzętową modułu typu fail-safe ET 200eco (w tym instalację, podłączenie oraz specyfikację techniczną)
Podręcznik „ET 200eco PN F-DI 8 x 24 VDC, 4xM12 / F-DQ 3 x 24 VDC/2.0A PM, 3xM12 (https://support.industry.siemens.com/cs/ww/en/)"	Opisuje warstwę sprzętową modułu typu fail-safe ET 200eco PN (w tym instalację, podłączenie oraz specyfikację techniczną)
Instrukcja obsługi „System rozproszonych I/O ET 200S, moduły typu fail-safe (http://support.automation.siemens.com/WW/view/en/27235629)"	Opisuje warstwę sprzętową modułów typu fail-safe ET 200S (w tym instalację, podłączenie oraz specyfikację techniczną)
Podręcznik „System automatyzacji S7-300, rozproszony system I/O ET 200M, moduły sygnałowy fail-safe (http://support.automation.siemens.com/WW/view/en/19026151)"	Opisuje warstwę sprzętową modułów sygnałowych typu fail-safe S7-300 (w tym instalację, podłączenie oraz specyfikację techniczną)
Instrukcja obsługi „System rozproszonych I/O ET 200pro, moduły I/O typu fail-safe (http://support.automation.siemens.com/WW/view/en/22098524)"	Opisuje warstwę sprzętową modułów typu fail-safe ET 200pro (w tym instalację, podłączenie oraz specyfikację techniczną)
Instrukcja obsługi „Moduły fail-safe - rozproszone urządzenia I/O ET 200iSP (http://support.automation.siemens.com/WW/view/en/47357221)"	Opisuje warstwę sprzętową modułów typu fail-safe ET 200iSP (w tym instalację, podłączenie oraz specyfikację techniczną)
Pomoc do *STEP 7*	• Opisuje obsługę standardowych narzędzi w *STEP 7* • Zawiera informacje dotyczące konfiguracji i przypisania parametrów sprzętu • Zawiera opis języków programowania FBD oraz LAD

Kompletna dokumentacja *SIMATIC S7* jest dostępna na płycie DVD. Więcej informacji można znaleźć na stronie internetowej (http://www.automation.siemens.com/mcms/industrial- automation-systems-simatic/en/manual-overview/manual-collection/Pages/Default.aspx).

Przewodnik

Niniejsza dokumentacja opisuje sposób pracy z *STEP 7 Safety*. Obejmuje instrukcje oraz działy z odniesieniami (opis instrukcji do programu bezpieczeństwa).

Uwzględniono następujące zagadnienia:

- Konfiguracja SIMATIC Safety
- Ochrona dostępu do STEP 7 Safety
- Programowanie programu bezpieczeństwa (program użytkownika związany z układem bezpieczeństwa)
- Komunikacja związana z układem bezpieczeństwa
- Instrukcje do programu bezpieczeństwa
- Wsparcie dot. zatwierdzenia systemu
- Obsługa i konserwacja SIMATIC Safety

Przyjęte założenia

W niniejszej dokumentacji pojęcia „inżyniera bezpieczeństwa" oraz „inżynieria fail-safe" są stosowane zamiennie. To samo tyczy się pojęć „F-" i „fail-safe".

„STEP 7 Safety V16" oznacza *„STEP 7 Safety Advanced V16"* oraz *„STEP 7 Safety Basic V16"*.

„(S7-300)" wskazuje, że dział dotyczy **jedynie** F-CPU S7-300. F-CPU S7-300 obejmuje również F-CPU ET 200S oraz ET 200pro (F-CPU IM).

„(S7-400)" wskazuje, że dział dotyczy **jedynie** F-CPU S7-400, a także WinAC RTX F.

„(S7-1200)" wskazuje, że dział dotyczy **jedynie** F-CPU S7-1200.

„(S7-1500)" wskazuje, że dział dotyczy **jedynie** F-CPU S7-1500. F-CPU S7-1500 obejmuje także F-CPU ET 200SP, CPU 1516pro F-2 PN oraz sterownik programowy S7-1500 F.

Możliwe jest łączenie tych zakresów.

Pojęcie „program bezpieczeństwa" dotyczy fragmentu fail-safe programu użytkownika i jest stosowane zamiast sformułowania „program użytkownika typu fail-safe", „program F" itp. Aby odpowiednio je rozróżnić, część programu użytkownika niesafety jest określana jako "standardowy program użytkownika".

Konfiguracja sprzętowa obejmuje konfigurację standardowych parametrów dla CPU i standardowych I/O, a także konfigurację parametrów związanych z bezpieczeństwem dla F-CPU i F-I/O.

Konfiguracja sprzętowa safety obejmuje konfigurację parametrów związanych z bezpieczeństwem dla F-CPU, a także konfigurację urządzeń F-I/O.

Dane projektu safety obejmują konfigurację sprzętową, a także program bezpieczeństwa.

Każde ostrzeżenie jest oznaczone unikalnym numerem na końcu treści. Pozwala to na łatwe odniesienie się do innych dokumentów, na przykład, by uzyskać omówienie wymogów bezpieczeństwa dla systemu.

Dodatkowe wsparcie

W razie dalszych pytań dotyczących użycia produktów przedstawionych z niniejszym podręczniku, należy skontaktować się z lokalnym przedstawicielem firmy Siemens.

Dane kontaktowe można znaleźć na stronie (http://www.siemens.com/automation/partner).

Dostępny jest przewodnik po dokumentacji technicznej do różnych produktów i systemów SIMATIC (http://www.siemens.com/simatic-tech-doku-portal).

Na poniższej stronie znajduje się katalog online i system zamawiania produktów (www.siemens.com/industrymall).

Centrum szkoleniowe

Zapewniamy kursy pomagające rozpocząć pracę z systemem automatyki S7. Należy skontaktować się z regionalnym centrum szkoleniowym lub centralnym centrum szkoleniowym w Norymberdze (90327) w Niemczech.

Więcej informacji dostępnych jest na stronie (http://www.sitrain.com).

Wsparcie techniczne

Aby skontaktować się ze wsparciem technicznym w kwestii wszystkich produktów automatyzacji przemysłowej, należy skorzystać z formularza zapytania na stronie (http://www.siemens.com/automation/support-request).

Dodatkowe informacje o naszym wsparciu technicznym można znaleźć na stronie (http://www.siemens.com/automation/service).

Ważne uwagi dotyczące utrzymania bezpieczeństwa pracy

Uwaga

Operatorzy systemów o charakterze związanym z bezpieczeństwem muszą przestrzegać wymogów bezpiecznej obsługi. Dostawca jest również zobowiązany do spełnienia specjalnych środków monitorowania produktu. Siemens informuje operatorów systemów w formie powiadomień osobistych o rozwoju produktów oraz właściwościach, które mogą stać się lub staną się ważną kwestią w zakresie bezpieczeństwa.

Aby otrzymywać najnowsze powiadomienia o odnośnych informacjach, należy zapisać się do newslettera, co pozwoli na wprowadzenie niezbędnych modyfikacji w systemie.

Należy zalogować się do Industry Online Support. Po kliknięciu na poniższe linki należy wybrać opcję „E-mail on update" po prawej stronie ekranu:

- SIMATIC S7-300/S7-300F
  (https://support.industry.siemens.com/cs/products?pnid=13751&lc=en-WW)
- SIMATIC S7-400/S7-400H/S7-400F/FH
  (https://support.industry.siemens.com/cs/products?pnid=13828&lc=en-WW)
- SIMATIC S7-1500/SIMATIC S7-1500F
  (https://support.industry.siemens.com/cs/products?pnid=13716&lc=en-WW)
- SIMATIC S7-1200/SIMATIC S7-1200F
  (https://support.industry.siemens.com/cs/products?pnid=13683&lc=en-WW)
- Sterownik programowy
  (https://support.industry.siemens.com/cs/products?pnid=13911&lc=en-WW)
- Rozproszone I/O
  (https://support.industry.siemens.com/cs/products?pnid=14029&lc=en- WW)
- STEP 7 (TIA Portal)
  (https://support.industry.siemens.com/cs/products?pnid=14340&lc=en-WW)

Siemens zapewnia produkty i rozwiązania o funkcjach bezpieczeństwa przemysłowego wspierające bezpieczną pracę instalacji, systemów, maszyn i sieci.

Aby chronić urządzenia systemy, maszyny i sieci przed cyberzagrożeniami, konieczne jest wdrożenie - i ciągłe utrzymywanie - kompleksowej, najnowocześniejszej koncepcji bezpieczeństwa przemysłowego. Produkty i rozwiązania Siemens stanowią tylko część takiej koncepcji.

W gestii klienta leży zabezpieczenie ich instalacji, systemów, maszyn i sieci przed nieupoważnionym dostępem. Systemy, maszyny i podzespoły powinny być podłączone do sieci zakładowej lub internetu jedynie w niezbędnym zakresie i przy zachowaniu odpowiednich środków ochronnych (np. zastosowaniu zapory sieciowej i segmentacji sieci).

Więcej informacji odnośnie środków bezpieczeństwa przemysłowego, jakie można zastosować, dostępnych jest na stronie (https://www.siemens.com/industrialsecurity).

Produkty i rozwiązania Siemens są stale rozwijane, by zwiększać ich bezpieczeństwo. Siemens zaleca, by wykonywać aktualizacje produktów, gdy tylko są one dostępne, i zawsze korzystać z najnowszych wersji produktów. Korzystanie z wersji produktów, które nie są już wspierane, oraz niezastosowanie najnowszych aktualizacji może zwiększyć ryzyko zostania ofiarą cyberataku.

Aby pozostać na bieżąco z aktualizacjami produktów, zapisz się do kanału RSS Siemens Industrial Security na stronie (https://www.siemens.com/industrialsecurity).

Pomoc online Siemens Industry

Można w tym miejscu szybko i łatwo znaleźć aktualne informacje na następujące tematy:

- **Wsparcie produktowe**

  Wszystkie niezbędne informacje oraz rozległa wiedza praktyczna dotycząca danego produkt, specyfikacje techniczne, FAQ, certyfikaty, materiały do pobrania oraz instrukcje obsługi.
- **Przykłady aplikacji**

  Narzędzia i przykłady rozwiązań automatyzacji – a także bloki funkcyjne, informacje dotyczące wydajności oraz materiały wideo.
- **Usługi**

  Informacje dotyczące usług przemysłowych, usług serwisowych, wsparcia technicznego, części zamiennych oraz ofert szkoleniowych.
- **Forum**

  Odpowiedzi i rozwiązania dotyczące techniki automatyzacji.
- **mySupport**

  Twój osobisty obszar roboczy w Industry Online Support do wiadomości, zapytań dotyczących wsparcia oraz konfigurowalnych dokumentów.

Informacja ta jest dostępna w internetowej pomocy online Siemens Industry (http://www.siemens.com/automation/service&support).

Industry Mall

Industry Mall to katalog i system do zamawiania firmy Siemens AG z zakresu rozwiązań automatyki i techniki napędowej na podstawie Totally Integrated Automation (TIA) oraz Totally Integrated Power (TIP).

Katalogi do wszystkich produktów z zakresu automatyki i techniki napędowej są dostępne w internecie (https://mall.industry.siemens.com).

Spis treści

Ważne uwagi ... **3**

1 Opis produktu ... **21**

1.1 Przegląd ... 21

1.2 Elementy sprzętowe i programowe ... 23

1.3 Instalacja/deinstalacja licencji STEP 7 Safety Basic V16 ... 28

1.4 Instalacja/deinstalacja licencji STEP 7 Safety Advanced V16 ... 29

1.5 Instalacja/deinstalacja STEP 7 Safety PowerPack ... 29

1.6 Migracja projektów z S7 Distributed Safety V5.4 SP5 do STEP 7 Safety Advanced ... 30

1.7 Migracja programów PLC do F-CPU S7-1500 ... 34

1.8 Aktualizacja projektów do STEP 7 Safety V16 ... 36

1.8.1 Aktualizacja projektów ze STEP 7 Safety wersji V14 SP1 do V16 ... 36

1.8.2 Aktualizacja projektów ze STEP 7 Safety wersji V13 SP1/SP2 do V16 ... 36

1.8.3 Aktualizacja projektów ze STEP 7 Safety wersji sprzed V13 SP1 ... 38

1.9 Pierwsze kroki ... 40

2 Konfiguracja ... **41**

2.1 Omówienie konfiguracji ... 41

2.2 Szczegóły konfiguracji systemu bezpieczeństwa ... 45

2.3 Konfiguracja F-CPU ... 46

2.4 Konfiguracja F-I/O ... 51

2.5 Kontrola konfiguracji (zarządzanie opcjami) do F-I/O ... 56

2.5.1 Przykład ... 57

2.6 Konfiguracja współdzielonego urządzenia ... 61

2.7 Konfiguracja trybu izochronicznego (S7-1500) ... 62

2.8 Zalecenia dotyczące przypisywania adresu PROFIsafe ... 63

2.9 Konfiguracje obsługiwane przez system bezpieczeństwa SIMATIC Safety ... 64

2.10 Adresy PROFIsafe do F-I/O typu 1 adresowania PROFIsafe ... 66

2.11 Adresy PROFIsafe do F-I/O typu 2 adresowania PROFIsafe ... 68

2.12 Ustawianie adresów docelowych bezpieczeństwa dla F-I/O za pomocą przełączników DIP . 70

Przypisywanie adresu PROFIsafe F-I/O za pomocą SIMATIC Safety ... 70
Identyfikacja modułów bezpieczeństwa ... 72
2.13 Przypisywanie adresów PROFIsafe ... 74
2.13.1 Przypisywanie adresów PROFIsafe do modułu bezpieczeństwa ... 74
2.13.2 Zmiana adresu PROFIsafe ... 75
2.13.3 Specjalne przypadki konfiguracji urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O
2.13.4

3 Safety Administration Editor ... 79

3.1 Otwieranie Safety Administration Editor ... 81
3.2 Obszar „ogólny" ... 82
3.3 Obszar „grupa F-runtime" ... 85
3.3.1 Obszar „grupa F-runtime" ... 85
3.3.2 Przetwarzanie wstępne/końcowe (S7-1200, S7-1500) ... 86
3.4 Obszar „bloki bezpieczeństwa" ... 88
3.5 Obszar „Rodzaje danych PLC zgodnych z bezpieczeństwem" (S7-1200, S7-1500) ... 89
3.6 Obszar „Administratorzy bezpieczeństwa serwera sieciowego (S7-1200, S7-1500) ... 90
3.7 Obszar „Ustawienia" ... 91
3.8 Obszar „Flexible F-Link" (S7-1200, S7-1500) ... 98

4 Ochrona dostępu ... 103

4.1 Przegląd ochrony dostępu ... 104
4.2 Ochrona dostępu dla danych projektu związanych z bezpieczeństwem ... 106
4.3 Ochrona dostępu dla F-CPU ... 109
4.4 Ochrona dostępu przez środki organizacyjne ... 112

5 Programowanie ... 114

5.1 Omówienie programowania ... 114
5.1.1 Struktura programu bezpieczeństwa (S7-300, S7-400) ... 115
5.1.2 Struktura programu bezpieczeństwa (S7-1200, S7-1500) ... 117
5.1.3 Bloki typu fail-safe ... 119
5.1.4 Ograniczenia w językach programowania FBD/LAD ... 121
5.1.5 Rodzaje danych PLC zgodnych z bezpieczeństwem (UDT) (S7-1200, S7-1500) ... 128
5.1.5.1 Grupowanie tagów PLC dla wejść i wyjść F-I/O w strukturach (S7-1200, S7-1500) ... 129
5.1.5.2 Przykład pogrupowanych tagów PLC dla wejść i wyjść F-I/O (S7-1200, S7-1500) ... 130
5.1.6 Edycja tagów PLC za pomocą edytorów zewnętrznych ... 133
5.1.7 Korzystanie z inżynierii wieloużytkowej ... 134
5.1.8 Openess ... 134
5.1.8.1 Openess safety ... 134
5.1.8.2 Możliwe modyfikacje bezpieczeństwa ... 135
5.1.8.3 Nazwa użytkownika do historii zmian bezpieczeństwa ... 136
5.1.9 Usuwanie programu bezpieczeństwa ... 137

5.2 Definiowanie grup F-runtime ... 139
5.2.1 Zasady grup F-runtime programu bezpieczeństwa ... 139
5.2.2 Procedura definiowania grupy F-runtime (S7-300, S7-400) ... 141
5.2.3 Procedura definiowania grupy F-runtime (S7-1200, S7-1500) ... 145
5.2.4 Komunikacja grupy F-runtime (S7-300, S7-400) ... 150
5.2.5 Komunikacja grupy F-runtime (S7-1200, S7-1500) ... 154
5.2.6 DB współdzielone bezpieczeństwa (S7-300, S7-400) ... 157
5.2.7 DB informacji grupy F-runtime (S7-1200, S7-1500) ... 158
5.2.8 Usuwanie grup F-runtime ... 159
5.2.9 Zmiana grupy F-runtime (S7-300, S7-400) ... 159
5.2.10 Zmiana grupy F-runtime (S7-1200, S7-1500) ... 160
5.3 Tworzenie bloków bezpieczeństwa w FBD / LAD ... 160
5.3.1 Tworzenie bloków bezpieczeństwa ... 160
5.3.2 Ochrona wiedzy technologicznej ... 162
5.3.3 Ponowne użycie bloków bezpieczeństwa ... 163
5.4 Programowanie zabezpieczenia rozruchu ... 165

6 Dostęp F-I/O ... 166

6.1 Adresowanie F-I/O ... 166
6.2 Stan wartości (S7-1200, S7-1500) ... 168
6.3 Dane procesowe lub wartości fail-safe ... 172
6.4 F-I/O DB ... 174
6.4.1 Nazwa i numer DB F-I/O ... 174
6.4.2 Tagi DB F-I/O ... 175
6.4.2.1 PASS_ON ... 177
6.4.2.2 ACK_NEC ... 177
6.4.2.3 ACK_REI ... 178
6.4.2.4 IPAR_EN ... 179
6.4.2.5 DISABLE ... 181
6.4.2.6 QBAD/PASS_OUT/DISABLED/QBAD_I_xx/QBAD_O_xx oraz stan wartości ... 181
6.4.2.7 ACK_REQ ... 182
6.4.2.8 IPAR_OK ... 182
6.4.2.9 DIAG ... 183
6.4.3 Dostęp do tagów DB F-I/O ... 184
6.5 Pasywacja i ponowna integracja F-I/O ... 185
6.5.1 Po uruchomieniu systemu bezpieczeństwa ... 186
6.5.2 Po błędach komunikacji ... 188
6.5.3 Po usterce F-I/O lub kanału ... 190
6.5.4 Pasywacja grupy ... 194

7 Wdrożenie zatwierdzenia użytkownika ... 196

7.1 Wdrażanie zatwierdzenia użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia nadrzędnego DP lub sterownika IO ... 196
7.2 Wdrażanie zatwierdzenia użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia I-slave lub I-device ... 201

8 Wymiana danych pomiędzy standardowym programem użytkownika a programem bezpieczeństwa ...204

8.1 Transfer danych z programu bezpieczeństwa do standardowego programu użytkownika . 205

8.2 Transfer danych ze standardowego programu do programu bezpieczeństwa ... 207

9 Komunikacja safety ... 209

9.1 Konfiguracja i programowanie komunikacji (S7-300, S7-400) ... 209
9.1.1 Przegląd komunikacji ... 209
9.1.2 Komunikacja sterownik IO bezpieczeństwa – sterownik IO ... 212
9.1.2.1 Konfiguracja komunikacji sterownik IO bezpieczeństwa – sterownik IO ... 212
9.1.2.2 Komunikacja sterownik IO bezpieczeństwa – sterownik IO poprzez SENDDP i RCVDP ... 216
9.1.2.3 Komunikacja program bezpieczeństwa – sterownik IO bezpieczeństwa – sterownik IO ... 217
9.1.2.4 Komunikacja sterownik IO bezpieczeństwa –sterownik IO–ogr. transferu danych ... 221
9.1.3 Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie nadrzędne ... 222
9.1.3.1 Konfiguracja komunikacji urządzenie nadrzędne bezpieczeństwa–urządzenie nadrzędne 222
9.1.3.2 Komunik. urządzenie nadrzędne bezp.–urządzenie nadrzędne przez SENDDP i RCVDP 227
9.1.3.3 Programowanie komunikacji urządzenie nadrzędne bezp.–urządzenie nadrzędne ... 228
9.1.3.4 Komunikacja urządzenie nadrzędne bezp.–urządzenie nadrzędne: ogr. transferu danych 232
9.1.4 Komunikacja sterownik IO bezpieczeństwa – I-device ... 232
9.1.4.1 Konfiguracja komunikacji bezpieczeństwa pomiędzy sterownikiem IO a I-device ... 232
9.1.4.2 Komunikacja sterownik IO bezpieczeństwa – I-device przez SENDDP i RCVDP ... 235
9.1.4.3 Programowanie komunikacji sterownik IO bezpieczeństwa – I-device ... 236
9.1.4.4 Komunikacja sterownik IO bezpieczeństwa – urządzenie IO – ogr. transferu danych ... 238
9.1.5 Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie I-slave ... 239
9.1.5.1 Konfiguracja komunikacji urządzenie nadrzędne bezp.–urządzenie I-slave ... 239
9.1.5.2 Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave przez SENDDP i RCVDP ... 241
9.1.5.3 Programowanie kom. urządzenie nadrzędne bezp.–urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave ... 242
9.1.5.4 Ogr. transferu danych komunikacji urządzenie nadrzędne bezpieczeństwa – urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave ... 245
9.1.6 Komunikacja urządzenie I-slave bezpieczeństwa – urządzenie I-slave ... 246
9.1.6.1 Konfiguracja komunikacji urządzenie I-slave bezp.–urządzenie I-slave ... 246
9.1.6.2 Komunikacja urządzenie I-slave bezp. – urządzenie I przez SENDDP i RCVDP ... 250
9.1.6.3 Programowanie komunikacji urządzenie I-slave bezp. – urządzenie I-slave ... 250
9.1.6.4 Ogr. transferu danych kom. urządzenie I-slave bezp.–urządzenie I-slave ... 250
9.1.7 Komunikacja urządzenie I-slave bezpieczeństwa – urządzenie podrzędne ... 251
9.1.7.1 Konfiguracja komunikacji urządzenie I-slave bezp.–urządzenie I-slave ... 251
9.1.7.2 Komunikacja urządzenie I-slave bezp. – urządzenie podrzędne – dostęp F-I/O ... 256
9.1.7.3 Ogr. transferu danych kom. urządzenie I-slave bezp.– urządzenie I-slave ... 256
9.1.8 Komunikacja sterownik IO safety – urządzenie I-slave ... 257
9.1.9 Komunikacja safety poprzez połączenia S7 ... 258
9.1.9.1 Konfiguracja komunikacji związanej z bezpieczeństwem poprzez połączenia S7 ... 258
9.1.9.2 Komunikacja poprzez SENDS7, RCVS7, oraz DB komunikacji bezpieczeństwa ... 260
9.1.9.3 Programowanie komunikacji związanej z bezpieczeństwem poprzez połączenia S7 ... 261
9.1.9.4 Komunikacja bezpieczeństwa poprzez połączenia S7 — ograniczenia transferu danych ... 265

9.1.10 Komunikacja safety z innymi systemami bezpieczeństwa S7 265
9.1.10.1 Wstęp 265
9.1.10.2 Komunikacja z S7 Distributed Safety poprzez połączenie PN/PN (komunikacja sterownik IO-sterownik IO) 266
9.1.10.3 Komunikacja z S7 Distributed Safety poprzez połączenie DP/DP (komunikacja jednostka nadrzędna – jednostka nadrzędna) 267
9.1.10.4 Komunikacja z S7 Distributed Safety za pomocą połączeń S7 268
9.1.10.5 Komunikacja z systemami F/FH S7 za pomocą połączeń S7 270
9.2 Konfiguracja i programowanie komunikacji (S7-1200, S7-1500) 273
9.2.1 Przegląd komunikacji 273
9.2.2 Komunikacja sterownik IO safety – sterownik IO 276
9.2.2.1 Konfiguracja komunikacji sterownik IO safety – sterownik IO 276
9.2.2.2 Komunikacja sterownik IO bezpieczeństwa – sterownik IO poprzez SENDDP i RCVDP 280
9.2.2.3 Program komunikacji bezpieczeństwa – sterownik IO bezpieczeństwa – sterownik IO 281
9.2.2.4 Komunikacja sterownik IO bezpieczeństwa–sterownik IO–ograniczenia transferu danych .285
9.2.3 Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie nadrzędne 285
9.2.3.1 Konfiguracja komunikacji urządzenie nadrzędne bezpieczeństwa–urządzenie nadrzędne.285
9.2.3.2 Kom, urządzenie nadrzędne bezp.–urządzenie nadrzędne przez SENDDP i RCVDP 289
9.2.3.3 Programowanie kom. urządzenie nadrzędne bezpieczeństwa – urządzenie nadrzędne 290
9.2.3.4 Kom. urządzenie nadrzędne bezp.–urządzenie nadrzędne:ograniczenia transferu danych294
9.2.4 Komunikacja sterownik IO safety – I-device 294
9.2.4.1 Konfiguracja komunikacji bezpieczeństwa pomiędzy sterownikiem IO a I-device 294
9.2.4.2 Komunikacja sterownik IO bezpieczeństwa – urządzenie I poprzez SENDDP i RCVDP 297
9.2.4.3 Programowanie komunikacji sterownik IO bezpieczeństwa – I-device 298
9.2.4.4 Komunikacja sterownik IO bezpieczeństwa – urządzenie IO – ogr. transferu danych 301
9.2.5 Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie I-slave 302
9.2.5.1 Konfiguracja kom. urządzenie nadrzędne bezpieczeństwa – urządzenie I-slave 302
9.2.5.2 Komunikacja urządzenie nadrzędne I bezp. – urządzenie I przez SENDDP i RCVDP 305
9.2.5.3 Programowanie kom. urządzenie nadrzędne bezpieczeństwa – urządzenie I-slave 306
9.2.5.4 Ogr. transferu danych kom. urządzenie nadrzędne I bezpieczeństwa–urz. I-slave 308
9.2.6 Komunikacja sterownik IO bezpieczeństwa – urządzenie I-slave 309
9.2.6.1 Komunikacja sterownik IO bezpieczeństwa – urządzenie I-slave 309
9.2.7 Komunikacja bezpieczeństwa do systemu bezpieczeństwa S7 Distributed Safety 310
9.2.7.1 Wstęp 310
9.2.7.2 Komunikacja z S7 Distributed Safety za pomocą połączenia PN/PN (komunikacja sterownik IO-sterownik IO) 31
9.2.7.3 Komunikacja z S7 Distributed Safety za pomocą połączenia DP/DP (komunikacja jednostka nadrzędna – jednostka nadrzędna) 311
9.3 Konfiguracja i programowanie komunikacji z użyciem Flexible F-Link (S7-1200, S7-1500) 312
9.3.1 Flexible F-Link 312
9.3.2 Interfejsy DB komunikacji bezpieczeństwa (S7-1200, S7-1500) 316
9.4 Konfiguracja i programowanie komunikacji pomiędzy S7-300/400 a S7-1200/1500 F-CPU 319
9.4.1 Przegląd komunikacji 319
9.5 Konfigurowanie i programowanie komunikacji w kilku projektach 320
Komunikacja sterownik IO safety–I-device w kilku projektach.320 Konfiguracja komunikacji bezpieczeństwa pomiędzy sterownikiem IO a I-device 320
9.5.1 Programowanie komunikacji sterownik IO bezpieczeństwa – I-device 322

10 Kompilowanie i finalizowanie programu bezpieczeństwa 323

10.1 Kompilowanie programu bezpieczeństwa 323
10.2 Wymogi pamięci roboczej programu bezpieczeństwa (S7-300, S7-400) 324
10.3 Pobieranie danych projektu 325
10.3.1 Pobieranie danych projektu do F-CPU 325
10.3.1.1 Pobieranie danych projektu do F-CPU S7-300/400 z włożoną kartą pamięci (karta pamięci micro SIMATIC lub karta flash) 329
10.3.1.2 Pobieranie danych projektu do F-CPU S7-400 bez włożonej karty flash 329
10.3.1.3 Pobieranie danych projektu do WinAC RTX F 330
10.3.1.4 Pobieranie poszczególnych bloków bezpieczeństwa do F-CPU S7-300/400 331
10.3.1.5 Pobieranie danych projektu do F-CPU S7-1200 bez włożonej karty programu 332
10.3.1.6 Pobieranie danych projektu do F-CPU S7-1200 z włożoną kartą programu 333
10.3.1.7 Pobieranie danych projektu do F-CPU S7-1500 335
10.3.1.8 Pobieranie danych projektu do sterownika programowego S7-1500 F 335
10.3.2 Pobieranie danych projektu do karty pamięci i wkładanie karty 337
10.3.2.1 Wkładanie karty pamięci micro SIMATIC lub karty flash do F-CPU S7-300/400 338
10.3.2.2 Wkładanie karty transferowej do F-CPU S7-1200 339
10.3.3 Pobieranie danych projektu F-CPU S7-1200 z wewnętrznej pamięci roboczej na pustą kartę pamięci SIMATIC 341
10.3.4 Aktualizacja danych projektu na F-CPU S7-1200 przy użyciu karty transferowej 342
10.3.5 Przywracania kopii zapasowej programu bezpieczeństwa do F-CPU S7-300/1200/1500 342
10.3.6 Funkcje specjalne podczas tworzenia i importowania obrazów sterownika programowego S7-1500 F 343
10.3.7 Wczytywanie danych projektu z F-CPU do urządzenia programującego / PC 345
10.3.8 Wczytywanie stacji PC za poprzez plik konfiguracyjny 346
10.3.8.1 Tworzenie pliku konfiguracyjnego 347
10.3.8.2 Importowanie pliku konfiguracyjnego 348
10.4 Identyfikacja programu 352
10.5 Porównywanie programów bezpieczeństwa 354
10.6 Drukowanie danych projektu 357
10.7 Testowanie programu bezpieczeństwa 359
10.7.1 Przegląd testowania programu bezpieczeństwa 359
10.7.2 Wyłączanie trybu bezpieczeństwa 360
10.7.3 Testowanie programu bezpieczeństwa 363
10.7.4 Testowanie programu bezpieczeństwa z S7-PLCSIM 366
10.7.5 Zmiana programu bezpieczeństwa w trybie RUN (S7-300, S7-400) 371
10.7.6 Zmiana standardowego programu użytkownika w trybie RUN (S7-1200, S7-1500) 374
10.8 Historia zmian bezpieczeństwa 375

11 Zatwierdzenie systemu 376

11.1 Przegląd zatwierdzenia systemu 376
11.2 Poprawność programu bezpieczeństwa, w tym konfiguracja sprzętowa (testowanie) 378
11.3 Kompletność podsumowania bezpieczeństwa 379
11.4 Zgodność elementów biblioteki systemowej użytej w programie bezpieczeństwa z Załącznikiem 1 raportu do certyfikatu TÜV 380
11.5 Zgodność bloków bezpieczeństwa chronionej wiedzy technologicznej stosowanych w programie bezpieczeństwa z ich dokumentacją bezpieczeństwa. 38
11.6 Kompletność i poprawność konfiguracji sprzętowej 383
11.7 Kompletność i poprawność konfiguracji komunikacji 391
11.8 Identyfikacja programu online i offline 393
11.9 Pozostałe charakterystyki 394
11.10 Zatwierdzenie zmian 396

12 Obsługa i konserwacja 401

12.1 Uwagi dotyczące trybu bezpieczeństwa programu bezpieczeństwa 401
12.2 Wymiana elementów programowych i sprzętowych 404
12.3 Przewodnik po diagnostyce (S7-300, S7-400) 407
12.4 Przewodnik po diagnostyce (S7-1500) 408
12.5 Przewodnik po diagnostyce (S7-1200) 409

13 Instrukcje do STEP 7 Safety V16 410

13.1 Ogólne 411
13.1.1 LAD 411
13.1.1.1 Nowa sieć (STEP 7 Safety V16) 411
13.1.1.2 Puste pole (STEP 7 Safety V16) 412
13.1.1.3 Otwieranie rozgałęzienia (STEP 7 Safety V16) 413
13.1.1.4 Zamykanie rozgałęzienia (STEP 7 Safety V16) 414
13.1.2 FBD 415
13.1.2.1 Nowa sieć (STEP 7 Safety V16) 415
13.1.2.2 Puste pole (STEP 7 Safety V16) 416
13.1.2.3 Otwieranie rozgałęzienia (STEP 7 Safety V16) 417
13.1.2.4 Wstawianie wejścia binarnego (STEP 7 Safety V16) 418
13.1.2.5 Odwrócenie RLO (STEP 7 Safety V16) 419

13.2 Operacje na bitach logicznych ... 420
13.2.1 LAD ... 420
13.2.1.1 ---| |---: Styk NO (STEP 7 Safety V16) ... 420
13.2.1.2 ---| / |---: Styk NC (STEP 7 Safety V16) ... 421
13.2.1.3 --|NOT|--: Odwrócenie RLO (STEP 7 Safety V16) ... 422
13.2.1.4 ---( )---: Przypisanie (STEP 7 Safety V16) ... 423
13.2.1.5 ---(R)---: Wyjście reset (STEP 7 Safety V16) ... 424
13.2.1.6 ---(S)---: Wyjście set (STEP 7 Safety V16) ... 425
13.2.1.7 SR: Przerzutnik set/reset (STEP 7 Safety V16) ... 427
13.2.1.8 RS: Przerzutnik reset/set (STEP 7 Safety V16) ... 429
13.2.1.9 --|P|--: Skanowanie argumentu dla narastającego zbocza sygnału (STEP 7 Safety V16) ... 431
13.2.1.10 --|N|--: Skanowanie argumentu dla opadającego zbocza sygnału (STEP 7 Safety V16) ... 433
13.2.1.11 P_TRIG: Skanowanie PLO dla narastającego zbocza sygnału (STEP 7 Safety V16) ... 435
13.2.1.12 N_TRIG: Skanowanie PLO dla opadającego zbocza sygnału (STEP 7 Safety V16) ... 437
13.2.2 FBD ... 439
13.2.2.1 Operacja logiczna AND (STEP 7 Safety V16) ... 439
13.2.2.2 Operacja logiczna OR (STEP 7 Safety V16) ... 441
13.2.2.3 X: Operacja logiczna EXCLUSIVE OR (STEP 7 Safety V16) ... 442
13.2.2.4 =: Przypisanie (STEP 7 Safety V16) ... 444
13.2.2.5 R: Wyjście reset (STEP 7 Safety V16) ... 445
13.2.2.6 S: Wyjście set (STEP 7 Safety V16) ... 446
13.2.2.7 SR: Przerzutnik set/reset (STEP 7 Safety V16) ... 448
13.2.2.8 RS: Przerzutnik reset/set (STEP 7 Safety V16) ... 450
13.2.2.9 P: Skanowanie argumentu pod kątem narastającego zbocza sygnału (STEP 7 Safety V16) 452
13.2.2.10 N: Skanowanie argumentu pod kątem opadającego zbocza sygnału (STEP 7 Safety V16) 454
13.2.2.11 P_TRIG: Skanowanie PLO pod kątem narastającego zbocza sygnału (STEP 7 Safety V16) .
13.2.2.12 456 N_TRIG: Skanowanie PLO pod kątem opadającego zbocza sygnału (STEP 7 Safety
13.3 V16) ... 457
13.3.1 Funkcje bezpieczeństwa ... 459
13.3.2 ESTOP1: Zatrzymanie awaryjne do kategorii zatrzymania 1 (STEP 7 Safety V16) ... 459
13.3.3 TWO_HAND: Monitorowanie oburęczne (STEP 7 Safety Advanced V16)(S7-300/400) ... 465
13.3.4 TWO_H_EN: Monitorowanie oburęczne z aktywacją (STEP 7 Safety V16) ... 468
13.3.5 MUTING: Muting (STEP 7 Safety Advanced V16) (S7-300, S7-400) ... 474
13.3.6 MUT_P: Mutingrównoległy (STEP 7 Safety V16) ... 485
13.3.7 EV1oo2DI: Ocena 1oo2 z analizą rozbieżności (STEP 7 Safety V16) ... 496
13.3.8 FDBACK: Monitorowanie sygnału zwrotnego (STEP 7 Safety V16) ... 504
13.3.9 SFDOOR: Monitorowanie drzwi bezpieczeństwa (STEP 7 Safety V16) ... 511
ACK_GL: Zatwierdzenie globalne wszystkich F-I/O w grupie F-runtime (STEP 7 Safety
13.4 V16) ... 518
13.4.1 Operacje czasowe ... 520
13.4.2 TP: Generowanie impulsu (STEP 7 Safety V16) ... 520
13.4.3 TON: Generowanie opóźnienia załączenia (STEP 7 Safety V16) ... 525
13.5 TOF: Generowanie opóźnienia wyłączenia (STEP 7 Safety V16) ... 530
13.5.1 Operacje licznika ... 535
13.5.2 CTU: Zliczanie w górę (STEP 7 Safety V16) ... 535
13.5.3 CTD: Zliczanie w dół (STEP 7 Safety V16) ... 537
CTUD: Zliczanie w górę i w dół (STEP 7 Safety V16) ... 539

13.6 Operacje komparatora ... 542
13.6.1 CMP ==: Równe (STEP 7 Safety V16) ... 542
13.6.2 CMP <>: Nierówne (STEP 7 Safety V16) ... 544
13.6.3 CMP >=: Większe lub równe (STEP 7 Safety V16) ... 546
13.6.4 CMP <=: Mniejsze lub równe (STEP 7 Safety V16) ... 548
13.6.5 CMP >: Większe niż (STEP 7 Safety V16) ... 550
13.6.6 CMP <: Mniejsze niż (STEP 7 Safety V16) ... 552
13.7 Funkcje matematyczne ... 554
13.7.1 ADD: Dodawanie (STEP 7 Safety V16) ... 554
13.7.2 SUB: Odejmowanie (STEP 7 Safety V16) ... 557
13.7.3 MUL: Mnożenie (STEP 7 Safety V16) ... 560
13.7.4 DIV: Dzielenie (STEP 7 Safety V16) ... 563
13.7.5 NEG: Tworzenie uzupełnienia dwójkowego(STEP 7 Safety V16) ... 567
13.7.6 ABS: Tworzenie wartości bezwzględnej (STEP 7 Safety V16)(S7-1200, S7-1500) ... 570
13.8 Operacje przenoszenia ... 572
13.8.1 MOVE: Przenoszenie wartości (STEP 7 Safety V16) ... 572
13.8.2 RD_ARRAY_I: Odczytaj z INT F-array (STEP 7 Safety V16) (S7-1500) ... 574
13.8.3 RD_ARRAY_DI: Odczytaj z DINT F-array (STEP 7 Safety V16) (S7-1500) ... 577
13.8.4 WR_FDB: Zapis wartości pośrednio do F-DB (STEP 7 Safety V16)(S7-300, S7-400) ... 579
13.8.5 RD_FDB: Odczyt wartości pośrednio z F-DB (STEP 7 Safety V16) (S7-300, S7-400) ... 582
13.9 Operacje konwertowania ... 584
13.9.1 CONVERT: Konwertowanie wartości (STEP 7 Safety V16) ... 584
13.9.2 BO_W: Przekształcenie 16 elementów danych rodzaju BOOL na element danych rodzaju WORD (STEP 7 Safety V16) ... 586
13.9.3 W_BO: Przekształcenie elementu danych rodzaju WORD na 16 elementów danych rodzaju BOOL (STEP 7 Safety V16) ... 589
13.9.4 SCALE: Skalowanie wartości(STEP 7 Safety V16) ... 592
13.9.5 SCALE_D: Skalowanie wartoścido danych typu DINT (STEP 7 Safety V16) (S7-1200, S7-1500)595 Operacje sterowania programem ... 598
13.10 JMP: Skok, jeśli RLO = 1 (STEP 7 Safety V16) ... 598
13.10.1 JMPN: Skok, jeśli RLO = 0 (STEP 7 Safety V16) ... 600
13.10.2 LABEL: Etykieta skoku (STEP 7 Safety V16) ... 602
13.10.3 RET: Powrót (STEP 7 Safety V16) ... 604
13.10.4 OPN: Otwarty globalny blok danych (STEP 7 Safety Advanced V16) (S7-300, S7-400) ... 605
13.10.5 Operacje na słowach logicznych ... 607
13.11 AND: Operacja logiczna AND (STEP 7 Safety V16) ... 607
13.11.1 OR: Operacja logiczna OR (STEP 7 Safety V16) ... 609
13.11.2 XOR: Operacja logiczna EXCLUSIVE OR (STEP 7 Safety V16) ... 611
13.11.3 Przesunięcie i obrócenie ... 613
13.12 SHR: Przesunięcie w prawo (STEP 7 Safety V16) ... 613
13.12.1 SHL: Przesunięcie w lewo (STEP 7 Safety V16) ... 616
13.12.2

13.13 Instrukcje operatorskie 619
13.13.1 ACK_OP: Zatwierdzenie typu fail-safe (STEP 7 Safety V16) 619
13.14 Dodatkowe instrukcje 627
13.14.1 LAD 627
13.14.1.1 ---| |--- OV: Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16)(S7-300, S7-400) 627
13.14.1.2 ---| / | --OV: Pozyskiwanie zanegowanego bitu stanu OV (STEP 7 Safety Advanced V16) S7-300, S7-400) 629
13.14.2 FBD 630
13.14.2.1 OV: Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) 630
13,15 Komunikacja 631
13.15.1 PROFIBUS/PROFINET 631
13.15.1.1 SENDDP i RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) 631
13.15.2 Komunikacja S7 642
13.15.2.1 SENDS7 i RCVS7: Komunikacja poprzez połączenia S7 (STEP 7 Safety Advanced V16) (S7-300, S7-400) 642

A Czasy monitorowania i odpowiedzi 649
A.1 Konfigurowanie czasów monitorowania 650
A.1.1 Minimalny czas monitorowania dla czasu cyklu grupy F-runtime 652
A.1.2 Minimalny czas monitorowania dla kom. Bezpieczeństwa pomiędzy F-CPU a F-I/O 652
A.1.3 Minimalny czas monitorowania kom. CPU safety – CPU 654
A.1.4 Czas monitorowania dla kom. bepzieczeństwa pomiędzy grupami F-runtime 654
A.2 Czasy odpowiedzi funkcji bezpieczeństwa 655

B Lista kontrolna 658
Glosariusz 664
Indeks 677

Opis produktu

1

1.1 Omówienie

System typu fail-safe SIMATIC Safety

System typu fail-safe SIMATIC Safety pozwala na wdrożenie koncepcji bezpieczeństwa obszarze maszyny oraz ochronę personelu (przykładowo, w postacie urządzeń zatrzymania awaryjnego do wyposażenia do obróbki i przetwarzania), a także w przemyśle przetwórczym (przykładowo, do wdrożenia funkcji ochronnych dla urządzeń zabezpieczających oprzyrządowanie i elementy sterownicze palników).

⚠OSTRZEŻENIE

System bezpieczeństwa SIMATIC Safety służy do kontroli procesów, w których występuje bezpieczny stan, który można osiągnąć poprzez natychmiastowe wyłączenie.

SIMATIC Safety można wykorzystać jedynie do kontroli procesów, w których natychmiastowe wyłączenie nie stwarza zagrożenia dla personelu lub środowiska.

Podczas wykonywania aplikacji bezpieczeństwa obejmujących utworzenie danych projektu związanego z bezpieczeństwem należy uwzględnić normy, dyrektywy oraz wytyczne związane z daną aplikacją. W szczególności należy ująć normy, w których opisany jest proces tworzenia oprogramowania (przykładowo, IEC 61508-3 lub ISO 13849-1). *(S062)*

Osiągalne wymogi bezpieczeństwa

Systemy bezpieczeństwa SIMATIC Safety pozwalają na spełnienia następujących wymogów bezpieczeństwa:

- Poziomu nienaruszalności bezpieczeństwa SIL3 zgodnie z normą IEC 61508:2010
- Poziomu niezawodności (PL) e oraz kategorii 4 zgodnie z normą ISO 13849-1:2015 lub EN ISO 13849-1:2015

Zasady funkcji bezpieczeństwa w SIMATIC Safety

Bezpieczeństwo funkcjonalne jest wdrażane odgórnie poprzez funkcje bezpieczeństwa w oprogramowaniu. Funkcje bezpieczeństwa są wykonywane przez system SIMATIC Safety w celu sprowadzenia układu do bezpiecznego stanu lub utrzymania go w razie niebezpiecznego zdarzenia. Funkcje bezpieczeństwa są głównie utrzymywane w następujących elementach:

- W programie związanym z bezpieczeństwem (programie bezpieczeństwa) w F-CPU
- W wejściach i wyjściach typu fail-safe (F-I/O)

F-I/O zapewnia bezpieczne przetwarzanie informacji polowych (czujniki: np. przycisk zatrzymania awaryjnego, kurtyny świetlne; elementy wykonawcze, np: do sterowania silnikiem). Są one wyposażone we wszystkie wymagane elementy sprzętowe i programowe potrzebne do bezpiecznego przetwarzania, zgodnie z wymaganym poziomem nienaruszalności bezpieczeństwa (SIL). Użytkownik musi jedynie zaprogramować własne funkcje bezpieczeństwa. Funkcje bezpieczeństwa do procesu mogą mieć postać funkcji użytkownika lub funkcji reakcji na usterkę. W przypadku wystąpienia błędu, jeśli system bezpieczeństwa nie może dłużej wykonywać swojej faktycznej funkcji, wykonuje funkcję reakcji na usterkę; przykładowo, powiązane wyjścia są wyłączane, a F-CPU, jeśli to konieczne, przełącza się w tryb STOP.

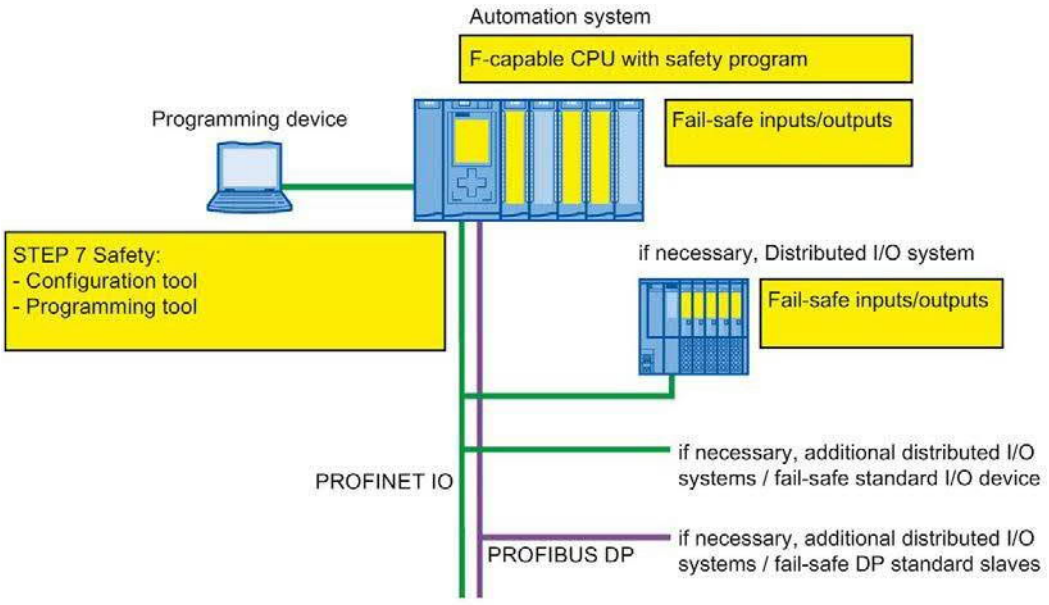
Przykład funkcji bezpieczeństwa użytkownika oraz funkcji reakcji na usterkę

W przypadku przekroczenia ciśnienia, system bezpieczeństwa otwiera zawór (funkcja bezpieczeństwa użytkownika). W razie niebezpiecznej usterki w F-CPU, wszystkie wyjścia są wyłączane (funkcja reakcji na usterkę), zawór jest otwierany, a pozostałe elementy wykonawcze przechodzą do stanu bezpiecznego. W systemie bezpieczeństwa bez usterki doszłoby jedynie do otwarcia zaworu.

1.2 Elementy sprzętowe i programowe

Elementy sprzętowe i programowe w SIMATIC Safety

Na poniższej ilustracji przedstawiono przegląd elementów sprzętowych i programowych wymaganych do konfiguracji i obsługi systemu bezpieczeństwa SIMATIC Safety.



Elementy sprzętowe do PROFIBUS DP

W systemach bezpieczeństwa SIMATIC Safety na PROFIBUS DP można zastosować następujące elementy typu fail-safe:

- F-CPU z interfejsem DP, na przykład CPU 1516F-3
- PN/DP
  - moduły sygnałowe typu fail-safe S7-300 w ET 200M
  - moduły typu fail-safe S7-1500/ET 200MP
  - moduły typu fail-safe ET 200SP
  - moduły typu fail-safe ET 200S
  - moduły sygnałowe typu fail-safe ET 200pro
  - moduły typu fail-safe ET 200iSP
  - moduły I/O typu fail-safe ET 200eco (S7-300, S7-400)
  - urządzenia podrzędne DP oparte na GSD typu fail-safe (kurtyna świetlna, skaner laserowy itp.)

Możliwe jest rozszerzenie konfiguracji za pomocą standardowych I/O.

Poniższe CP/CM można zastosować w systemie bezpieczeństwa SIMATIC Safety na PROFIBUS DP do podłączenia do rozproszonych F-I/O:

- CP 443-5 Extended
- CM 1243-5
- CM 1542-5
- CP 1542-5
- SP CM DP

Elementy sprzętowe- PROFINET I/O

W systemach bezpieczeństwa SIMATIC Safety PROFINET I/O można zastosować następujące elementy typu fail-safe:

- F-CPU z interfejsem PN, na przykład CPU 1214FC DC/DC/DC
- Wejścia i wyjścia typu fail-safe (F-I/O), takie jak:
  - moduły sygnałowe typu fail-safe S7-300 w ET 200M
  - moduły typu fail-safe S7-1500/ET 200MP
  - moduły typu fail-safe ET 200SP
  - moduły typu fail-safe ET 200S moduły typu fail-safe ET
  - 200pro
  - moduły I/O typu fail-safe ET 200eco PN
  - urządzenia I/O oparte na GSD typu fail-safe (kurtyna świetlna, skaner laserowy itp.)

Możliwe jest rozszerzenie konfiguracji za pomocą standardowych I/O.

Poniższe CP/CM można zastosować w systemie bezpieczeństwa SIMATIC Safety na PROFINET IO do podłączenia do rozproszonych F-I/O:

- CP 443-1
- CP 443-1 Advanced-IT
- CM 1542-1
- CP 1545-1

Elementy sprzętowe do konfiguracji centralnej

W systemach bezpieczeństwa SIMATIC Safety na F-CPU można zastosować centralnie następujące elementy typu fail-safe:

- moduły sygnałowe typu fail-safe S7-300
- moduły typu fail-safe S7-1200
- moduły typu fail-safe S7-1500
- moduły typu fail-safe ET 200SP
- moduły typu fail-safe ET 200S
- moduły typu fail-safe ET 200pro (możliwość stosowania również z CPU 1516proF-2)

Możliwe jest rozszerzenie konfiguracji za pomocą standardowych I/O.

STEP 7 Safety

Niniejsza dokumentacja opisuje *STEP 7 Safety Advanced V16* oraz *STEP 7 Safety Basic V16*. *STEP 7 Safety* to oprogramowanie do konfigurowania i programowania systemów bezpieczeństwa SIMATIC Safety. Wraz ze *STEP 7 Safety* otrzymuje się również:

- Wsparcie przy konfiguracji F-I/O w *edytorze sprzętu i sieci* w TIA Portal
- Wsparcie przy tworzeniu programu bezpieczeństwa przy użyciu języków LAD i FBD oraz wprowadzanie funkcji detekcji błędów do programu bezpieczeństwa
- Instrukcje programowania w LAD i FBD, które znane są ze standardowych programów użytkownika
- Instrukcje programowania w LAD i FBD przy użyciu specjalnych funkcji bezpieczeństwa

Co więcej, *STEP 7 Safety* zapewnia funkcje porównywania programów bezpieczeństwa wspierające przy zatwierdzeniu systemu.

⚠ OSTRZEŻENIE

Konfiguracja F-CPU oraz F-I/O, a także programowanie bloków bezpieczeństwa musi odbywać się z TIA Portal w sposób opisany w niniejszej dokumentacji. Należy przestrzegać wszystkich kwestii opisanych w dziale „Zatwierdzenie systemu" (strona 376), aby zagwarantować bezpieczne działanie systemu SIMATIC Safety. Inne procedury nie są dozwolone. *(S056)*

Pakiety opcjonalne

Oprócz *STEP 7 Safety*, możliwe jest zastosowanie pakietów opcjonalnych z F-I/O oraz F-CPU, a także wykorzystanie instrukcji do programowania programu bezpieczeństwa ze specjalnymi funkcjami w obrębie systemu bezpieczeństwa SIMATIC Safety. Są to przykładowo SINUMERIK lub panele mobilne HMI typu fail-safe.

Instalacja, przypisanie parametrów oraz programowanie, a także istotne kwestie do odnotowania podczas zatwierdzenia systemu, zostały opisane w dokumentacji konkretnych pakietów opcjonalnych.

Należy również zapoznać się z uwagami w „Konfiguracje obsługiwane przez system bezpieczeństwa SIMATIC Safety" (strona 64).

TIA Portal Cloud Connector

OSTRZEŻENIE

Użycie TIA Portal Cloud Connector jest przeznaczone jedynie do prac inżynierskich z TIA Portal. Oznacza to, że dostęp online podczas operacji produkcyjnej (np. SCADA) nie jest dozwolony. Ma to szczególne zastosowanie przy programach bezpieczeństwa. *(S068)*

Openess

Openess jako część *STEP 7 Safety* jest wspierany przez funkcje wymienione powyżej. Użycie Openess w operacji produkcyjnej nie jest dozwolone.

Jako część *STEP 7 Safety*, obsługiwane są następujące funkcje:

- Wstawianie / usuwanie F-CPU i F-I/O
- Kopiowanie / usuwanie F-CPU i F-I/O z szablonów
- Kompilowanie programu (w tym programu bezpieczeństwa)
- Odczyt / konfiguracja parametrów fail-safe z F-CPU
- Odczyt / konfiguracja parametrów fail-safe z urządzeń F-I/O
- Odczyt / konfiguracja modułów typu fail-safe ET 200SP
- Odczyt, deklarowanie lub usuwanie zmiennych typu fail-safe w tabeli zmiennych PLC
- Aktualizacja projektów do najnowszej wersji bloków bezpieczeństwa
- Spójny upload stanowiska
- Eksport i import bloków bezpieczeństwa oraz typów danych PLC (UDT), zgodnych z programem bezpieczeństwa
- Porównanie sprzętu i oprogramowania
- Interfejs kontroli wersji (VCI)
- Odczyt skrótu danych online PLC do programu bezpieczeństwa

Poniższe funkcje nie są obsługiwane.

- Wgranie programu do urządzenia
- Kompilowanie sprzętu

Uwaga

Jeśli ochrona dostępu jest ustawiona dla danych projektu związanych z bezpieczeństwem, czynności wymagające autoryzacji dostępu mogą być wykonane jedynie po zalogowaniu do programu. Logowanie jest możliwe jedynie poprzez interfejs użytkownika TIA Portal.

OSTRZEŻENIE

Wykorzystując Openess podczas obsługi danych projektu związanych z bezpieczeństwem, należy zagwarantować ich spójność (przykładowo, w kontekście zapisywania lub przenoszenia przez aplikacje do „Zarządzania kodem źródłowym"). W przypadku podłączenia zewnętrznych narzędzie, należy przestrzegać wymogów narzędzie obsługi offline zgodnie z IEC 61508-3. Naruszenie integralności danych projektu związanych z bezpieczeństwem nie może być określone podczas importowania przez STEP 7 Safety. Końcowa weryfikacja poprawności danych projektu związanych z bezpieczeństwem musi odbyć się zgodnie z opisem w dziale „Zatwierdzenie systemu" (strona 376). *(S070)*

Środowiska wirtualne

OSTRZEŻENIE

Użycie środowisk wirtualnych w systemie inżynierskim

Należy pamiętać, że HYPERVISOR lub klient HYPERVISOR nie może wykonywać żadnych funkcji, które powielają zarejestrowane sekwencje ramek komunikatów z właściwym zachowaniem czasowym w sieci o dostępnych systemach.

Należy upewnić się, że warunek ten jest spełniony, przykładowo, podczas korzystania z następujących funkcji:

- Reset zarejestrowanych stanów (zrzutów ekranu) maszyn wirtualnych (VM)
- Wstrzymywanie i wznawianie VM
- Odtwarzanie zarejestrowanych sekwencji w VM
- Przenoszenie VM pomiędzy komputerami głównymi podczas operacji produkcyjnej (np. Odporność na błędy (FT))
- Cyfrowe bliźniaki dla VM w środowisku wirtualnym

W razie wątpliwości należy wyłączyć te funkcje w ustawieniach (konsola administracyjna HYPERVISOR).

(S067)

Program bezpieczeństwa

Program bezpieczeństwa można utworzyć za pomocą *edytora programów*. FB i FC typu fail-safe można programować w językach FBD lub LAD, korzystając z instrukcji ze *STEP 7 Safety*, a także tworzyć DB typu fail-safe.

Kontrole bezpieczeństwa są wykonywane automatycznie, a dodatkowe bloki typu fail-safe do detekcji błędów oraz reakcji na usterki są wstawiane po skompilowaniu programu bezpieczeństwa. Gwarantuje to, że usterki i błędy zostaną wykryte oraz zostaną wyzwolone odpowiednie reakcje, by utrzymać system w bezpiecznym stanie lub sprowadzić go do niego.

Oprócz programu bezpieczeństw, na F-CPU można uruchomić standardowy program użytkownika. Standardowy program użytkownika może współistnieć wraz z programem bezpieczeństwa w F-CPU, ponieważ niezamierzona zmiana danych związanych z bezpieczeństwem jest odkrywana przez standardowy program użytkownika.

Możliwa jest wymiana danych pomiędzy programami w F-CPU

przy pomocy pamięci bitowej standardowego DB lub poprzez uzyskanie dostępu do obrazu procesuwejść i wyjść.

Zobacz także

Transfer danych z programu bezpieczeństwa do standardowego programu użytkownika (strona 205)

1.3 Instalacja/deinstalacja licencji STEP 7 Safety Basic V16

Po zainstalowaniu licencji *STEP 7 Safety Basic V16* , dostępny jest zakres funkcjonalny *STEP 7 Safety Basic V16*.

Wymagania programowe dla *STEP 7 Safety Basic V16*

Następujący pakiet programowy musi być zainstalowany na urządzeniu programistycznym lub PC:

- *SIMATIC STEP 7 Basic V16*

Instalacja licencji *STEP 7 Safety Basic V16*

1. Należy uruchomić *Automation License Manager* na urządzeniu programistycznym/PC, na którym zainstalowano pakiet oprogramowania *„SIMATIC STEP 7 Basic V16"* lub *„SIMATIC STEP 7 Advanced V16"*.
2. Należy zainstalować licencję *STEP 7 Safety Basic V16* zgodnie z opisem w *pomocy Automation License Manager*.

Deinstalacja licencji *STEP 7 Safety Basic V16*

Aby odinstalować licencję *STEP 7 Safety Basic V16,* należy postępować zgodnie z opisem w *pomocy Automation License Manager*.

1.4 Instalacja/deinstalacja licencji STEP 7 Safety Advanced V16

Po zainstalowaniu licencji *STEP 7 Safety Advanced V16*, dostępny jest zakres funkcjonalny *STEP 7 Safety Advanced V16* .

Wymagania programowe dla *STEP 7 Safety Advanced V16*

Następujący pakiet programowy musi być zainstalowany na urządzeniu programistycznym lub PC:

- *SIMATIC STEP 7 Professional V16*

Instalacja licencji *STEP 7 Safety Advanced V16*

1. Należy zacząć od instalacji *Automation License Manager* na urządzeniu programistycznym/PC, na którym zainstalowany jest pakiet programowy *„SIMATIC STEP 7 Professional V16"*.
2. Należy zainstalować licencję *STEP 7 Safety Advanced V16* zgodnie z opisem w *pomocy Automation License Manager*.

Deinstalacja licencji *STEP 7 Safety Advanced V16*

Aby odinstalować licencję *STEP 7 Safety Advanced V16,* należy postępować zgodnie z opisem w *pomocy Automation License Manager*.

1.5 Instalacja/deinstalacja STEP 7 Safety PowerPack

Po zainstalowaniu *STEP 7 Safety PowerPack*, dostępny jest zakres funkcjonalny *STEP 7 Safety Advanced V16*.

Wymagania programowe dla *STEP 7 Safety PowerPack*

Następujący pakiet programowy musi być zainstalowany na urządzeniu programistycznym lub PC:

- *SIMATIC STEP 7 Professional V16*

Instalacja *STEP 7 Safety PowerPack*

1. Należy zacząć od instalacji *Automation License Manager* na urządzeniu programistycznym/PC, na którym zainstalowany jest pakiet programowy *„SIMATIC STEP 7 Professional V16"*.
2. Należy zainstalować licencję dostępną z *STEP 7 Safety PowerPack* zgodnie z opisem w *pomocy Automation License Manager*.

Deinstalacja *STEP 7 Safety PowerPack*

Aby odinstalować licencję *STEP 7 Safety PowerPack,* należy postępować zgodnie z opisem w *pomocy Automation License Manager*.

1.6 Migracja projektów z S7 Distributed Safety V5.4 SP5 do STEP 7 Safety Advanced

Wstęp

W *STEP 7 Safety Advanced* możliwe jest dalsze korzystanie z programów utworzonych za pomocą *S7 Distributed Safety V5.4 SP5*.

Wymogi

STEP 7 Safety Advanced, *S7 Distributed Safety V5.4 SP5* oraz *F-Configuration Pack* wykorzystane do utworzenia projektu muszą być zainstalowane na komputerze używanym do migracji. Obsługiwane są *F-Configuration Pack V5.4 SP5* w wersji do *V5.5 SP13*.

W tym celu projekty muszą być skompilowane w *S7 Distributed Safety V5.4 SP5* **oraz za pomocą** *F-Configuration Pack*.

Przed migracją

Należy usunąć wszystkie bloki bezpieczeństwa, które nie są wymagane przez program bezpieczeństwa w projekcie *S7 Distributed Safety V5.4 SP5* przed wykonaniem migracji.

Procedura zgodnie ze *STEP 7 Professional*

Należy postępować tak jak w przypadku standardowych projektów, by wykonać migrację projektów z *S7 Distributed Safety V5.4 SP5* do *STEP 7 Safety Advanced*. Po zakończeniu migracji należy upewnić się, korzystając ze zbiorczego podpisu bezpieczeństwa, czy w projekcie nie wystąpiły zmiany.

Uwaga

Jeśli program bezpieczeństwa jest wykorzystywany do migrowania bloków bezpieczeństwa z ochroną wiedzy technologicznej, należy usunąć zabezpieczenie przed wykonaniem migracji.

Zabezpieczenie można ponownie przypisać po zakończeniu migracji.

Takie podejście do migracji zostało opisane w dziale „Migracja" w pomocy *STEP 7 Professional*. Specjalne uwagi dotyczące *STEP 7 Safety Advanced* zostały ujęte poniżej.

Uwaga

Zaleca się włączenie opcji „Include hardware configuration" (Uwzględnij konfigurację sprzętową) w oknie „Migrowanie projektu".

Starsze wersje sprzętowe

Starsze wersje sprzętu bezpieczeństwa mogą nie być obsługiwane przez *STEP 7 Safety Advanced* .

Jeśli zastosowano i skonfigurowano wersje F-CPU oraz F-I/O w projektach S7 Distributed Safety, które nie zostały zatwierdzone dla *STEP 7 Safety Advanced*, konieczne będzie zaktualizowanie ich do nowej wersji w *S7 Distributed Safety V5.4 SP5* oraz powiązanym *F- Configuration Pack*. Po zakończeniu aktualizacji możliwe jest dokonanie migracji do *STEP 7 Safety Advanced*. Informacja o produktach z listą zatwierdzonego sprzętu jest dostępna na stronie internetowej (https://support.industry.siemens.com/cs/ww/de/view/109481784):

Szczegóły komunikacji CPU safety – CPU poprzez połączenia S7

Informacje dotyczące specjalnych kwestii dotyczących migrowanych projektów w komunikacji CPU safety – CPU poprzez połączenia S7 w dziale „Komunikacja safety poprzez połączenia S7" (strona 258). Należy zwrócić uwagę również na dział „Komunikacja z S7 Distributed Safety za pomocą połączeń S7" (strona 268).

Szczegóły dotyczące instrukcji ESTOP1 lub FDBACK

Informacje dotyczące specjalnych względów podczas korzystania z instrukcji ESTOP1 i FDBACK można znaleźć w dziale „Wersje instrukcji" w ESTOP1: Zatrzymanie/wyłączenie awaryjne do kategorii zatrzymania 1 (STEP 7 Safety V16) (strona 459) oraz FDBACK: Monitorowanie sygnału zwrotnego (STEP 7 Safety V16) (strona 504).

Procedury pomigracyjne

Po wykonaniu migracji dostępny jest kompletny projekt z programem bezpieczeństwa, który utrzymał strukturę programu *S7 Distributed Safety* oraz zbiorczy podpis bezpieczeństwa. Bloki bezpieczeństwa z biblioteki bezpieczeństwa S7 Distributed Safety (V1)

są przekształcane na instrukcje zapewniane przez *STEP 7 Safety Advanced*.

Migrowany projekt nie wymaga wobec tego ponownej akceptacji; można go wczytać bez zmian do F-CPU, o ile nie został zmodyfikowany lub skompilowany po wykonaniu migracji.

Uwaga

Podsumowanie bezpieczeństwa

Nie jest możliwe utworzenie podsumowania bezpieczeństwa w *STEP 7 Safety Advanced* dla migrowanego projektu. Wydruk projektu utworzonego w *S7 Distributed Safety V5.4 SP5* oraz odnośne dokumenty akceptacji pozostają wciąż ważne, ponieważ został utrzymany zbiorczy podpis bezpieczeństwa.

Kompilowanie migrowanej konfiguracji sprzętowej

W przypadku odebrania komunikatu o błędzie po migracji oraz dalszej kompilacji konfiguracji sprzętowej, stwierdzający, iż adres źródłowy bezpieczeństwa nie jest zgodny z parametrem „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) F-CPU, należy zmienić parametr „Central F-source address" (Centralny adres źródłowy bezpieczeństwa).

Adres źródłowe bezpieczeństwa dla wszystkich F-I/O przypisanych do F-CPU są ponownie przypisywanie w procesie.

Jeśli po migracji SM 326; DI 24 x DC 24V (6ES7 326-1BK01-0AB0 oraz 6ES7 326- 1BK02-0AB0) i dalszej kompilacji konfiguracji sprzętowej pojawi się komunikat o błędzie „F_IParam_ID_1: Value outside the permitted range" (Wartość poza dopuszczalnym zakresem), należy usunąć F-SM i ponownie go wstawić.

W obu przypadkach wymagana jest dalsza kompilacja programu bezpieczeństwa.

Kompilowanie migrowanych programów bezpieczeństwa

W wyniku kompilacji migrowanego projektu w *STEP 7 Safety Advanced*, struktura istniejącego programu (z F-CALL) jest przekształcana na nową strukturę *STEP 7 Safety Advanced* (z głównym blokiem bezpieczeństwa). Zmienia to zbiorczy podpis bezpieczeństwa, przez co może być wymagane ponowne zatwierdzenie programu bezpieczeństwa.

(S7-300, S7-400) Należy wywołać główny blok bezpieczeństwa zgodnie z F-CALL z dowolnego bloku standardowego programu użytkownika. Zaleca się wywołanie z OB 3x.

Uwaga

Podczas pierwszej kompilacji migrowanego programu bezpieczeństwa, wywołanie F-CALL jest zastępowane automatycznie przez wywołanie głównego bloku bezpieczeństwa, jeśli blok wywołania F-CALL został utworzony przy użyciu języka LAD< FBD lub STL.

Uwaga

Zmiana wersji systemu Safety

Przed skompilowaniem po raz pierwszy z użyciem *STEP 7 Safety Advanced*, należy zmienić wersję programu bezpieczeństwa na inną niż 1.0 w obszarze „Settings" (Ustawienia) w *Safety Administration Editor*. Zaleca się korzystanie z najwyższej dostępnej wersji.

Uwaga

Korzystanie z najnowszej wersji instrukcji

Aby rozszerzyć migrowany program bezpieczeństwa, zaleca się zaktualizowanie do najnowszej wersji stosowanych instrukcji, nim wykona się pierwszą kompilację przy użyciu *STEP 7 Safety Advanced*. Należy zapoznać się z informacjami dotyczącymi wersji instrukcji.

Uwaga

Należy pamiętać, że migrowany program bezpieczeństwa wydłuża czas pracy grup(y) F-runtime i zwiększa zapotrzebowanie na pamięć dla programu bezpieczeństwa (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).

Zobacz także

Przykład aplikacji „Migracja programu bezpieczeństwa do TIA Portal"
(https://support.industry.siemens.com/cs/ww/en/view/109475826)

1.7 Migracja programów PLC do F-CPU S7-1500

Aby przenieść F-CPU S7-300/400 do F-CPU S7-1500, należy postępować tak jak w przypadku migracji standardowego CPU S7-300/400 do CPU S7-1500.

Istotne punkty po migracji:

- Czynności niepodlegające automatyzacji
  - Tworzenie grupy F-runtime oraz przypisanie jej do głównego bloku bezpieczeństwa.
  - Konfiguracja sprzętowa obejmująca I/O początkowego F-CPU nie jest automatycznie przenoszona do F-CPU S7-1500. Konfigurację sprzętową nowego CPU należy wdrożyć ręcznie po wykonaniu migracji.

    Należy również zapoznać się z działami „Określanie adresu PROFIsafe do F-I/O typu adresowania PROFIsafe 1" oraz „Określanie adresu PROFIsafe do F-I/O typu adresowania PROFIsafe 2" w rozdziale „Konfiguracja F-CPU" (strona 46). W przeciwnym razie może prowadzić to do ponownego przypisania adresu docelowego bezpieczeństwa w konfiguracji.
  - Korzystając z F-I/O w wersji protokołu PROFIsafe = Expanded Protocol (XP) (przykładowo moduły bezpieczeństwa S7-1500/ET 200MP), należy pamiętać, że wymagany jest jeden bajt więcej w obszarze adresowym F-CPU S7-1200/1500 niż w przypadku F-CPU S7-300/400.
  - Zastąpienie instrukcji OV przez połączenie wyjścia ENO do funkcji matematycznych (strona 554).
  - Zastąpienie instrukcji DB_FDB przez instrukcje RD_ARRAY_I (strona 574) oraz RD_ARRAY_DI (strona 577).
  - Zastąpienie komunikacji grupy F-runtime przez komunikację poprzez Flexible F-Link (strona 154).
- Instrukcje nieobsługiwane:
  - MUTING
  - TWO_HAND
  - WR_FDB
  - OPN
  - SENDS7
  - RCVS7
- Nieobsługiwane rodzaje danych
  - DWORD

- Zmiany w programowaniu program bezpieczeństwa
  - F_GLOBDB.VKE0/1 zastąpione przez FALSE/TRUE (strona 121).
  - Wartości możliwe do odczytania z F_GLOBDB zastąpione przez DB informacji o grupie F-runtime. Dodatkowe informacje dostępne są w dziale „DB współdzielone typu F (S7-300, S7-400)"
  - (strona 157) oraz „DB informacji o grupie F-runtime (S7-1200, S7-1500)" (strona 158). Zastąpienie taga QBAD_I_xx lub QBAD_O_xx przez status wartości. Dodatkowe informacje dostępne są w dziale „Stan wartości (S7-1200, S7-1500)" (strona 168) oraz „F-I/O DB" (strona 174).
- Nowa konwencja nazewnicza podczas nazywania DB dla F-I/O
- Zmodyfikowane zachowanie tagów QBAD oraz PASS_OUT (strona 181) dla F-I/O z profilem „RIOforFA safety".

Należy skompilować program bezpieczeństwa i usunąć wyświetlone błędy kompilacji.

Uwaga

Po migracji F-CPU należy wykonać nowe zatwierdzenie.

Zobacz także

Programowanie (strona 114)

1.8 Aktualizacja projektów do STEP 7 Safety V16

1.8.1 Aktualizacja projektów ze STEP 7 Safety wersji V14 SP1 do V16

Aby móc kontynuować pracę z projektem z *STEP 7 Safety* w wersji *V14 SP1*, należy najpierw zaktualizować projekt do *STEP 7 Safety V16*.

Aktualizację należy wykonać zgodnie ze zwykłą procedurą dla *STEP 7*. Po zaktualizowaniu do V16 należy skompilować program bezpieczeństwa.

Należy pamiętać, że istniejące historie zmian nie są aktualizowane. Wszystkie poprzednie wpisy są usuwane po aktualizacji. W razie potrzeby należy wydrukować rejestr zmian przed dokonaniem aktualizacji.

1.8.2 Aktualizacja projektów ze STEP 7 Safety wersji V13 SP1/SP2 do V16

Aby móc kontynuować pracę z projektem z *STEP 7 Safety w wersji V13 SP1*, należy najpierw zaktualizować projekt do *STEP 7 Safety V16*.

Aktualizację należy wykonać zgodnie ze zwykłą procedurą dla *STEP 7*. Po zaktualizowaniu do V16 należy skompilować program bezpieczeństwa.

(S7-300/400): Po skompilowaniu program bezpieczeństwa jest spójny, a zbiorczy podpis bezpieczeństwa zaktualizowanego programu odpowiada zbiorczemu podpisowi programu z V13 SP1. Akceptacja zmian nie jest wymagana.

(S7-1200/1500): Po skompilowaniu program bezpieczeństwa jest spójny, a zbiorczy podpis bezpieczeństwa zaktualizowanego programu uległ zmianie ze ze względów systemowych. Nowy zbiorczy podpis bezpieczeństwa programu w *STEP 7 Safety V16* zastępuje poprzedni podpis programu bezpieczeństwa w *STEP 7 Safety V13 SP1*.

Omówienie wszystkich zmian związanych z bezpieczeństwem można znaleźć w „Common data/Protocols/F- Convert Log+CPU name+time stamp". Jedną ze zmian związanych z bezpieczeństwem jest to, że *STEP 7 Safety V16* automatycznie zastępuje wersje instrukcji, które nie są już obsługiwane, nowymi, funkcjonalnie identycznymi wersjami. Omówienie zawiera porównanie poprzednich podpisów w *STEP 7 Safety V13 SP1* względem nowych podpisów w *STEP 7 Safety V16* i pokazuje automatycznie zmienione wersje instrukcji. Należy wydrukować to omówienie i przechowywać je wraz z dokumentacją akceptacji lub dokumentacją maszyny. Zatwierdzenie zmian nie jest wymagane, ponieważ „Zbiorczy podpis bezpieczeństwa w *STEP 7 Safety V13 SP1"* ujęty w omówieniu jest zgodny ze zbiorczym podpisem w bieżącej dokumentacji akceptacji.

Należy pamiętać, że istniejące historie zmian nie są aktualizowane. Wszystkie poprzednie wpisy są usuwane po aktualizacji. W razie potrzeby należy wydrukować rejestr zmian przed dokonaniem aktualizacji.

Specjalne funkcje do zatwierdzenia użytkownika i reintegracji F-I/O po usterce F-I/O lub kanału oraz PASS_ON = 1 (S7-1200, S7-1500)

Dotyczy to następujących F-I/O:

- moduły sygnałowe typu fail-safe S7-300
- moduły typu fail-safe ET 200SP
- moduły sygnałowe typu fail-safe ET 200S
- moduły typu fail-safe ET 200pro
- moduły typu fail-safe ET 200iSP

Należy pamiętać o zmienionym zachowaniu zatwierdzenia użytkownika i reintegracji podczas konfigurowania „Zachowanie po usterce kanału" = „Pasywacja kanału" oraz tag ACK_NEC (F-I/O DB) = 1. Zachowanie dostosowano do zachowania podczas konfigurowania „Zachowanie po usterce kanału" = „Pasywacja całego modułu".

W przypadku *STEP 7 Safety V14* lub wyższego, zatwierdzenie użytkownika dla skorygowanego F-I/O lub usterki kanału jest **możliwe** nawet gdy tag PASS_ON (F- I/O DB) = 1. Reintegracja (zapewnienie wartości procesowych) odbywa się **natychmiast, gdy tag PASS_ON = 0**.

Aż do *STEP 7 Safety V13 SP1*, zatwierdzenie użytkownika dla skorygowanego F-I/O lub usterki kanału **nie było możliwe**, dopóki tag PASS_ON (F-I/O DB) = 1. Zatwierdzenie użytkownika było możliwe jedynie, gdy tag PASS_ON = 0. Reintegracja (zapewnienie wartości procesowych) odbyło się niezwłocznie po zatwierdzeniu użytkownika.

Specjalne funkcje podczas korzystania z profili instrukcji

Aby użyć profilu instrukcji w projekcie z *STEP 7 Safety V13 SP1*, należy usunąć profil przed aktualizacją do *STEP 7 Safety V16*. Przed usunięciem należy zanotować swoje ustawienia. Po zaktualizowaniu można utworzyć nowy profil instrukcji, po czym wprowadzić zapisane ustawienia. Należy mieć na uwadze, że niektóre wersje instrukcji nie są obsługiwane w *STEP 7 Safety V16*. Dodatkowe informacje o obsługiwanych wersjach instrukcji są zawarte w opisach odnośnych instrukcji.

1.8.3 Aktualizacja projektów ze STEP 7 Safety wersji sprzed V13 SP1

W przypadku aktualizacji z projektu **sprzed wersji** *STEP 7 Safety V13 SP1* do *STEP 7 Safety V16*, konieczna jest aktualizacja projektu jako standardowy w *STEP 7 Safety V13 SP1* poprzez krok pośredni.

Podpis programu bezpieczeństwa nie zmienia się po aktualizacji programu do *STEP 7 Safety V13 SP1*. Dlatego też akceptacja zmian nie jest wymagana.

Aktualizację należy wykonać zgodnie ze zwykłą procedurą dla *STEP 7 Professional*.

Podczas aktualizacji projektu utworzonego w *STEP 7 Safety Advanced V11* , należy mieć na uwadze następuje zagadnienia:

Uwaga

Przed kontynuowaniem pracy z projektem zaktualizowanym ze *STEP 7 Safety Advanced V11* należy wprowadzić odpowiednie regulacje:

W informacji produktowej dla *STEP 7 Safety Advanced V11*, dotyczące ustawień parametrów „Discrepancy behavior" (Zachowanie rozbieżności) oraz „Reintegration after discrepancy error" (Reintegracja po błędzie rozbieżności) dla wejścia cyfrowego fail-safe oraz modułów wyjściowych 4F-DI/3F-DO DC24V/2A (6ES7138-4FC01-0AB0, 6ES7138-4FC00-0AB0). Parametry te mogą być nieprawidłowo wyświetlane w pewnych kombinacjach.

W oparciu o instrukcje postępowania w tej informacji produktowej, należy użyć tabeli konwersji do ustawienia parametrów, tak aby były wyświetlane niepoprawnie w podsumowaniu bezpieczeństwa i konfiguracji sprzętowej, tym samym by działały poprawnie w module bezpieczeństwa. Należy również ręcznie skorygować podsumowanie bezpieczeństwa, by zapisać rzeczywiste zachowanie modułów bezpieczeństwa.

1. Skompilować zaktualizowany projekt za pomocą *STEP 7 Safety Advanced V13 SP1*. Dla każdego modułu bezpieczeństwa w *STEP 7 Safety Advanced V11,* który został skorygowany, zostanie wyświetlony komunikat błędu: „The CRC (F_Par_CRC) of the module (xxx) does not match the calculated value (yyy)." (CRC (F_Par_CRC) modułu (xxx) nie jest zgodny z obliczoną wartością (yyy).)
2. Należy dostosować przypisanie parametrów do każdego modułu bezpieczeństwa, dla którego został wyświetlony komunikat o błędzie, by uzyskać zgodność z zapisanymi korekcjami w podsumowaniu bezpieczeństwa.
3. Należy wykonać to dla każdego F-CPU, a następnie skompilować program bezpieczeństw
4. Jeśli zbiorczy podpis bezpieczeństwa po skompilowaniu odpowiada zbiorczemu podpisowi podsumowania bezpieczeństwa, oznacza to, że wykonano wszystkie niezbędne zmiany.

Użycie CP

Do F-I/O obsługiwanych w instalacji z CP443-5 Extended, CP443-1 lub CP 443-1 Advanced-IT nie zostały automatycznie przypisane unikalne adresy docelowe bezpieczeństwa.

Po skompilowaniu sprzętu w projekcie z takimi F-I/O w *STEP 7 Safety V13 SP1*, zostaną wyszczególnione F-I/O, dla których zaszła zmiana. Konieczne jest przypisanie nowych, unikalnych adresów docelowych bezpieczeństwa dla zgłoszonych F-I/O. Dodatkowe informacje dostępne są pod adresami PROFIsafe dla typu adresu PROFIsafe 1 (strona 66), adresami PROFIsafe dla F-I/O typu adresu PROFIsafe 2 (strona 68) oraz we właściwościach podczas konfiguracji urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe (strona 76).

Zmienia to zbiorczy podpis bezpieczeństwa programu. Dzięki temu, że zbiorczy podpis F-SW pozostał niezmieniony, dokumentowane jest, że program bezpieczeństwa nie uległ zmianie. Zmieniony zbiorczy podpis F-HW wskazuje, że konfiguracja sprzętowa safety uległa zmianie. Możliwe jest teraz skontrolowanie, czy wyłącznie zmienione adresy docelowe bezpieczeństwa spowodowały tę zmianę:

- Podpis parametru bezpieczeństwa (bez adresu) dla każdego zmienionego F-I/O pozostaje bez zmian.
- Jedynie zmienione bloki danych dla F-I/O są wyszczególnione w edytorze porównania programu bezpieczeństwa, przy filtrze ustawionym na „Compare only F-blocks relevant for certification" (Porównaj jedynie bloki bezpieczeństwa istotne dla certyfikacji).

Zmienione nazwy DB dla F-I/O

Przed *STEP 7 Safety V13 SP1* możliwa było zmiana nazwy bloków danych dla F-I/O. Zmiana ta skutkowała w zmianie zbiorczego podpisu bezpieczeństwa podczas aktualizacji.

Jeśli zmiana zbiorczego podpisu bezpieczeństwa jest niepożądana, należy wykonać następujące kroki:

1. W *STEP 7 Safety V13* należy przywrócić oryginalne nazwy DB dla F-I/O.
2. Skompilować program bezpieczeństwa.

   Zbiorczy podpis bezpieczeństwa nie zmieni się.
3. Należy wykonać porównanie offline – offline pomiędzy zaktualizowanym programem a programem skompilowanym w kroku 2.
4. Wydrukować wynik porównania (strona 354).

   Przy pomocy wydruku należy upewnić się, że zmianie uległy jedynie nazwy bloków danych dla F-I/O.
5. Aktualizacja programu bezpieczeństwa do *STEP 7 Safety V13 SP1*. Po zaktualizowaniu program bezpieczeństwa ma zbiorczy podpis z kroku 2.

1.9 Pierwsze kroki

Początki pracy w SIMATIC Safety

Dostępne są trzy dokumenty „Pierwsze kroki", pomagające w rozpoczęciu pracy

z SIMATIC Safety.

Dokumentacja „Pierwsze kroki" to instrukcja obsługi zapewniająca opis krok po kroku tworzenia projektu za pomocą SIMATIC Safety. Pozwala na szybkie zaznajomienie się z zakresem funkcji SIMATIC Safety.

Treść

Dokumentacja „Pierwsze kroki" opisuje tworzenie pojedynczego, ciągłego projektu, który jest rozbudowywany z każdym działem. W oparciu o konfigurację możliwe jest zaprogramowanie wyłączenia typu fail-safe, wprowadzenie zmian w programie oraz zatwierdzenie systemu.

Oprócz szczegółowych instrukcji, dokumentacja „Pierwsze kroki" zapewnia także informacje obejmujące nowe zagadnienia, szczegółowo objaśniające stosowane funkcje oraz jak ze sobą korelują.

Odbiorca

Dokumentacja „Pierwsze kroki" jest przeznaczona dla początkujących, lecz mogą z niej korzystać również użytkownicy przechodzący z *S7 Distributed Safety*.

Do pobrania

Trzy dokumenty „Pierwsze kroki" są dostępne w formie plików PDF do darmowego pobrania z Industry Online Support:

- STEP 7 Safety Advanced V11 z F-CPU S7-300/400 (http://support.automation.siemens.com/WW/view/en/49972838)
- STEP 7 Safety Basic V13 SP1 z F-CPU S7-1200 (http://support.automation.siemens.com/WW/view/en/34612486/133300) (część instrukcji „Instrukcja obsługi S7-1200 Functional Safety")
- STEP 7 Safety Advanced V13 z F-CPU S7-1500 (http://support.automation.siemens.com/WW/view/en/101177693)

Konfiguracja 2

2.1 Omówienie konfiguracji

Wstęp

System bezpieczeństwa SIMATIC Safety konfiguruje się identycznie jak standardowe systemy automatyki S7-300, S7-400, S7-1200, S7-1500 lub ET 200MP, ET 200SP, ET 200S, ET 200iSP, ET 200eco, ET 200eco PN bądź ET 200pro w *STEP 7*.

W tym dziale przedstawiono podstawowe różnice w porównaniu do standardowej konfiguracji, jakie występują podczas konfigurowania systemu bezpieczeństwa SIMATIC Safety.

Niniejsza dokumentacja rozróżnia dwie grupy F-I/O:

F-I/O adresu PROFIsafe typu 1

F-I/O zapewniające unikalność adresu PROFIsafe wyłącznie na podstawie adresu docelowego bezpieczeństwa, przykładowo, moduły bezpieczeństwa ET 200S. Adres PROFIsafe jest zazwyczaj przypisywany za pomocą przełączników DIP.

F-I/O adresu PROFIsafe typu 2

F-I/O mogące zapewnić unikalność adresu PROFIsafe na podstawie kombinacji adresu źródłowego bezpieczeństwa oraz adresu docelowego bezpieczeństwa, przykładowo, moduły bezpieczeństwa S7-1500/ET 200MP. Adres PROFIsafe jest zazwyczaj przypisywany za pomocą *STEP 7 Safety*.

Które elementy bezpieczeństwa można skonfigurować za pomocą *STEP 7 Safety* ?

Poniższa tabela przedstawia F-CPU, które można skonfigurować w *STEP 7 Safety Basic*, a które za pomocą *STEP 7 Safety Advanced*:

F-CPU	*STEP 7 Safety Basic*	*STEP 7 Safety Advanced*
S7-300	—	x
S7-400	—	x
S7-1200	x	x
S7-1500	—	x
WinAC RTX F	—	x
Sterownik programowy S7-1500	—	x

Poniższa tabela przedstawia F-I/O, które można skonfigurować w *STEP 7 Safety Basic*, a które za pomocą *STEP 7 Safety Advanced*, a także jakie adresy PROFIsafe obsługują:

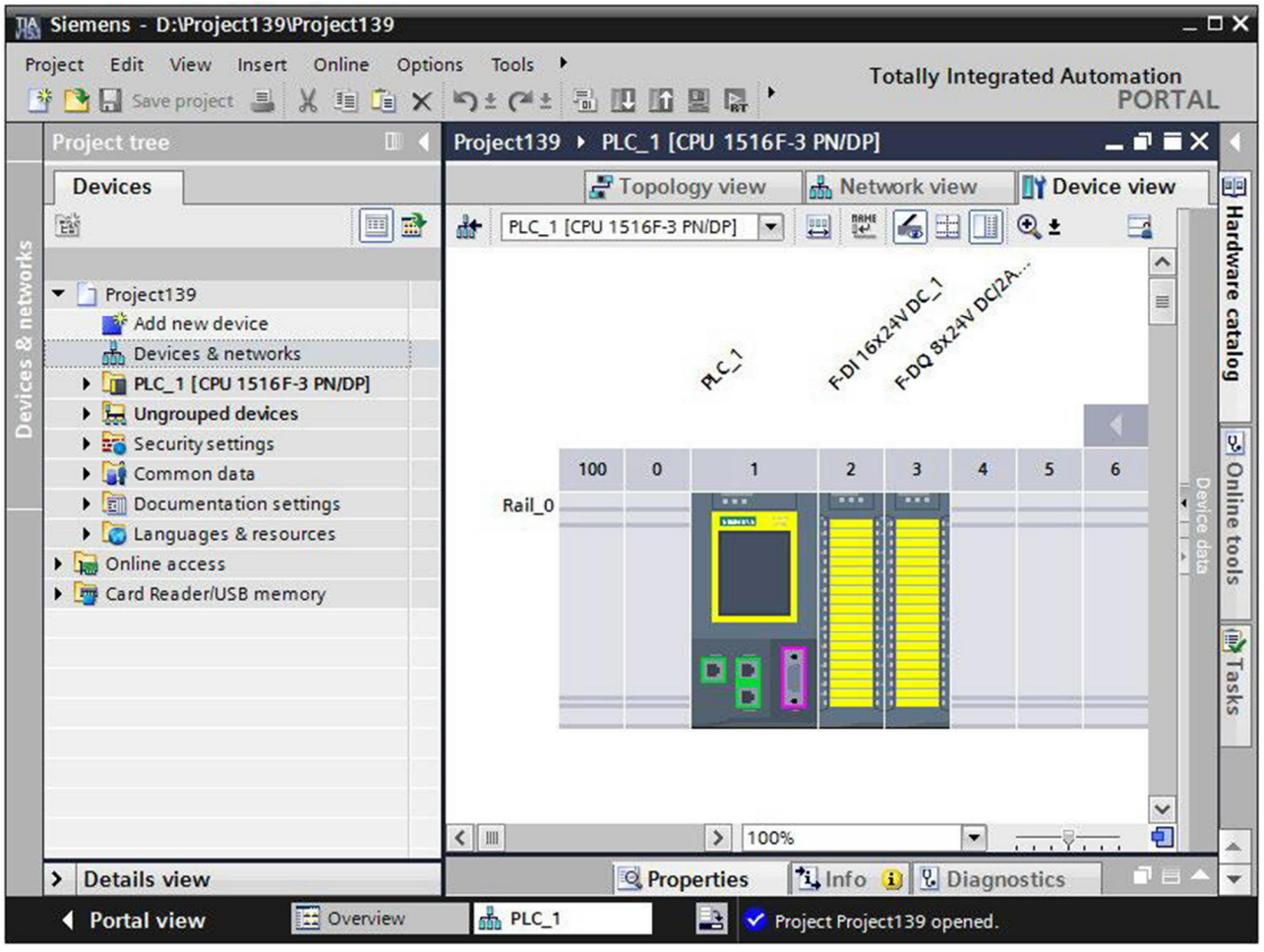
F-I/O	*STEP 7 Safety Basic*	*STEP 7 Safety Advanced*	*Typ adresu PROFIsafe*
S7-300 F-SMs	x**	x**	1
Moduły bezpieczeństwa ET 200S	x	x	1
Moduły bezpieczeństwa ET 200pro	x	x	1
Moduły bezpieczeństwa ET 200iSP	x	x	1
F-I/O do ET 200eco DP	—	Z F-CPU S7-300/400 (tylko tryb PROFIsafe V1)	1
F-I/O do ET 200eco PN	x	x	2
Moduły bezpieczeństwa S7-1200 (centralnie na F-CPU S7-1200)	x	x	2
Moduły bezpieczeństwa ET 200SP	x	x	2
Moduły bezpieczeństwa S7-1500/ET	x	x	2
Slave DP oparte na GSD fail-safe	x	x	*
I/O oparte na GSD fail-safe	x	x	*

* Należy odnieść się do dokumentacji, by określić typ adresu PROFIsafe urządzenia podrzędnego DP opartego na GSD/urządzenia I/O opartego na GSD. W razie wątpliwości należy przyjąć, iż adres PROFIsafe jest typu 1.

*** F-SM, które obsługują jedynie tryb PROFIsafe V1, mogą być wykorzystane z F-CPU S7-300/400.

Przykład: System bezpieczeństwa skonfigurowany w *STEP 7 Professional*

Poniższa ilustracja przedstawia skonfigurowany system bezpieczeństwa. Elementy typu fail-safe wybiera się na karcie zadania „Katalog sprzętowy" identycznie jak w przypadku standardowych elementów, umieszczając je w obszarze roboczym sieci(network view) lub widoku urządzenia(device view) . Komponenty bezpieczeństwa są oznaczone na żółto.



Informacje dodatkowe

Szczegółowe informacje na temat F-I/O dostępne są w *instrukcjach obsługi odnośnych F-I/O*.

Które opcje komunikacji związanej z bezpieczeństwem można skonfigurować?

Do konfiguracji opcji komunikacji związanej z bezpieczeństwem należy użyć *edytora sprzętu i sieci* (patrz „Konfiguracja i programowanie komunikacji (S7-300, S7-400)" (strona 209) lub „Konfiguracja i programowanie komunikacji (S7-1200, S7-1500)" (strona 273)):

- Przy użyciu Flexible F-Link (strona 312)
- master-master
- master-master do S7 Distributed Safety
- master-I-slave
- I-slave-I-slave
- I-slave-slave
- kontroler IO - kontroler IO
- kontroler IO - kontroler IO w S7 Distributed Safety
- kontroler IO - I-device
- kontroler IO - I-slave
- Komunikacja S7
- Komunikacja S7 do S7 Distributed Safety lub S7 F Systems

2.2 Szczegóły konfiguracji systemu bezpieczeństwa

Konfiguracja przebiega identycznie jak przy standardowych elementach

System bezpieczeństwa SIMATIC Safety konfiguruje się tak samo jak standardowy system S7. Oznacza to, że konfiguracja i przypisanie parametrów sprzętowych odbywa się w *edytorze sprzętu i sieci* jako scentralizowanym systemie (F-CPU, i, jeśli wymagane, F-IO, przykładowo CPU 1516F- 3 PN/DP oraz moduły bezpieczeństwaS7-1500/ET 200MP) i/lub jako system rozproszony (F-CPU, F-SM w ET 200M, moduły bezpieczeństwa ET 200MP, moduły bezpieczeństwa ET 200SP, ET 200S, ET 200pro, ET 200iSP, ET 200eco, ET 200eco PN, urządzenia podrzędne DP oparte na GSD typu fail-safe i/lub urządzenia I/O oparte na GSD typu fail-safe).

Specjalne parametry bezpieczeństwa

Do funkcjonalności bezpieczeństwa dostępne są specjalne parametry bezpieczeństwa, które można przeglądać i ustawiać w zakładce „Properties" (Właściwości) elementów typu fail-safe (F-CPU i F-I/O). Parametry bezpieczeństwa są oznaczone na żółto.

Parametry bezpieczeństwa zostały opisane w „Konfigurowanie F-CPU (strona 46)" oraz „Konfigurowanie F-I/O (strona 51)".

Kompilowanie konfiguracji sprzętowej

Konieczne jest skompilowanie konfiguracji sprzętowej systemu bezpieczeństwa SIMATIC Safety (menu „Compile > Hardware configuration" (Kompiluj -> Konfiguracja sprzętowa)). Skonfigurowany F-CPU z włączoną funkcjonalnością bezpieczeństwa jest jedynym wymogiem wstępnym do programowania programu bezpieczeństwa.

Uwaga

Podczas konfiguracji sprzętu mogą występować niespójności, co nie uniemożliwia zapisu. Pełna kontrola spójności konfiguracji sprzętowej oraz możliwe dane połączenia są wykonywane dopiero podczas kompilacji. Dlatego też należy regularnie wykonywać „Edit > Compile" (Edytuj > Kompiluj).

Zmiana parametrów związanych z bezpieczeństwem

Uwaga

W przypadku zmiany parametru związanego z bezpieczeństwem (oznaczonego na żółto) w F-I/O lub F-CPU, konieczne jest skompilowanie zmodyfikowanej konfiguracji oraz skompilowanie samego programu bezpieczeństwa (strona 323) (menu „Compile > Hardware and software (only changes)" (Kompiluj > Sprzęt i program (tylko zmiany)) i pobranie go. Dotyczy to również zmian w F-I/O, które nie są wykorzystywane w programie bezpieczeństwa. Nie ma to wpływu na F-I/O standardowej pracy.

2.3 Konfiguracja F-CPU

Wstęp

F-CPU konfiguruje się tak samo jak standardowy system automatyki.

F-CPU zawsze konfiguruje się w *STEP 7*, niezależnie od tego, czy zainstalowano licencję *STEP 7 Safety*. Bez zainstalowanej licencji *STEP 7 Safety*, F-CPU może działać tylko jako standardowe CPU.

Po zainstalowaniu licencji *STEP 7 Safety*, możliwe jest włączenie lub wyłączenie funkcjonalności bezpieczeństwa w F-CPU.

Aby użyć F-I/O w trybie bezpieczeństwa lub w komunikacji związanej z bezpieczeństwem, należy aktywować funkcjonalność bezpieczeństwa w F-CPU.

Funkcjonalność bezpieczeństwa jest aktywowana domyślnie po zainstalowaniu licencji *STEP 7 Safety*.

Aktywacja/wyłączenie funkcjonalności bezpieczeństwa

Aby zmodyfikować ustawienia funkcjonalności bezpieczeństwa,

1. Należy wybrać F-CPU w widoku urządzeń lub sieci, po czym przejść do zakładki „Properties" (Właściwości) w widoku nadzoru.
2. Wybrać „Fail-safe" w nawigacji obszaru.
3. Za pomocą odpowiedniego przycisku włączyć/wyłączyć funkcjonalność bezpieczeństwa.
4. Aby wyłączyć tę funkcjonalność, należy potwierdzić okno „Disable F-activation" (Wyłącz funkcjonalność bezpieczeństwa) przyciskiem „Yes" (Tak).

Wyłączanie funkcjonalności bezpieczeństwa dla istniejącego programu bezpieczeństwa

Aby wyłączyć funkcjonalność bezpieczeństwa dla F-CPU ze względu na używanie go jako standardowego CPU mimo zainstalowanego programu bezpieczeństwa, należy mieć na uwadze:

- Konieczne będzie hasło do programu bezpieczeństwa, jeśli je ustalono.
- Safety Administration Editor (strona 79) zostanie usunięty z drzewa projektu.
- Usuwane są F-OB. (S7-1200, S7-1500)
- Usuwane są wszystkie bloki bezpieczeństwa.
- Od tej chwili nie można używać F-I/O w trybie bezpieczeństwa wraz z tym F-CPU.

Konfigurowanie parametrów bezpieczeństwa dla F-CPU

W zakładce „Properties" (Właściwośc) dla F-CPU można zmienić lub zastosować domyślne ustawienia następujących parametrów:

- Zakres adresu docelowego bezpieczeństwa
  - Dolny limit adresów docelowych bezpieczeństwa
  - Górny limit adresów docelowych bezpieczeństwa
- Domyślny czas monitorowania bezpieczeństwa dla centralnego lub rozproszonego I/O w F-CPU

Uwaga

Zmiana czasu monitorowania bezpieczeństwa dla centralnego lub rozproszonego F-I/O w CPU skutkuje zmianą programu bezpieczeństwa przy ponownej kompilacji. Może być konieczna nowa akceptacja.

Określanie adresu bezpieczeństwa do F-I/O typu adresowania PROFIsafe 1

Za pomocą parametrów „Dolny limit adresów docelowych bezpieczeństwa" oraz „Górny limit adresów docelowych bezpieczeństwa" można określić zakres dla danego F-CPU, w którym adres docelowy bezpieczeństwa nowo wstawionych F-I/O adresu PROFIsafe typu 1 (strona 66) jest przypisywany automatycznie. Adres docelowy bezpieczeństwa, który nie mieści się jeszcze w zakresie adresu docelowego bezpieczeństwa, jest również przypisywany, gdy zmienia się przypisanie urządzenia I/O podrzędnego DP w F-CPU lub włącza aktywację bezpieczeństwa w F-CPU bądź zmianie adresu logicznego modułu F.

Adres docelowy bezpieczeństwa jest przypisywany w kolejności rosnącej od „dolnego limitu adresów docelowych bezpieczeństwa". Gdy brak jest dostępnych adresów w zakresie, przypisywany jest następny dostępny adres docelowy bezpieczeństwa spoza zakresu, a podczas kompilowania wyświetla się ostrzeżenie.

Maksymalny możliwy adres docelowy bezpieczeństwa dla modułów bezpieczeństwa ET 200S, ET 200eco, ET 200pro, ET 200iSP oraz F-SM S7-300 to 1022.

Adres docelowy bezpieczeństwa dla F-I/O F-I/O typu adresowania PROFIsafe 1 musi być unikalny dla całej sieci oraz CPU.

Wybierając różne zakresy adresów docelowych bezpieczeństwa dla różnych F-CPU, można zdefiniować różne zakresy do automatycznego przypisywania adresów docelowych. Przydaje się to podczas korzystania z wielu F-CPU w jednej sieci. Możliwe są dalsze ręczne zmiany adresów. (zobacz także Zalecenia dotyczące przypisywania adresu PROFIsafe (strona 63))

Przykład:

Skonfigurowano zakres adresu docelowego bezpieczeństwa w następujący sposób:

- Dolny limit adresów docelowych bezpieczeństwa = 100
- Górny limit adresów docelowych bezpieczeństwa = 199

Po wstawieniu pierwszego F-I/O typu adresowania PROFIsafe 1, przypisywany jest adres docelowy 100. Po wstawieniu dodatkowego F-I/O typu adresowania PROFIsafe 1, przypisywany jest adres docelowy 101.

Uwaga

Parametry "dolny limit adresów docelowych bezpieczeństwa" oraz „górny limit adresów docelowych bezpieczeństwa" nie mają wpływu na następujące F-I/O:

- SM 326; DI 8 x NAMUR (pod numerem zamówieniowym 6ES7326-1RF00-0AB0)
- SM 326; DO 10 x DC 24V/2A (numer zamówieniowy 6ES7326-2BF01-0AB0)
- SM 336; AI 6 x 13 bit (numer zamówieniowy 6ES7336-1HE00-0AB0)

Określanie adresu PROFIsafe do F-I/O typu adresowania PROFIsafe 2

Adres docelowy bezpieczeństwa w F-I/O typu adresowania PROFIsafe 2 (strona 68) jest przypisywany automatycznie dla każdego F-CPU w kolejności malejącej, począwszy od 65534. Dolny limit to wartość skonfigurowana za pomocą parametru „dolny limit adresów docelowych bezpieczeństwa" (dla F-I/O typu adresowania PROFIsafe 1) + 1.

Po osiągnięciu wartości skonfigurowanej jako „górny limit adresów docelowych bezpieczeństwa", podczas kompilacji wydawane jest ostrzeżenie. (zobacz także Zalecenia dotyczące przypisywania adresu PROFIsafe (strona 63))

Określanie adresu źródłowego bezpieczeństwa do F-I/O typu adresowania PROFIsafe 2

Adres źródłowy bezpieczeństwa do F-I/O typu adresowania PROFIsafe 2 (strona 68) przypisuje się do tego F-CPU za pomocą parametru „centralny adres źródłowy bezpieczeństwa". Ades źródłowy musi być unikalny dla całej sieci. (zobacz także Zalecenia dotyczące przypisywania adresu PROFIsafe (strona 63))

Uwaga

Zmiana parametru „centralny adres źródłowy bezpieczeństwa" skutkuje zmianą programu bezpieczeństwa przy ponownej kompilacji. Dlatego też może być konieczna nowa akceptacja, ponieważ w tym kroku adresy źródłowe wszystkich F-I/O typu adresowania 2 są zmieniane centralnie.

Parametr „domyślny czas monitorowania bezpieczeństwa"

Do monitorowania komunikacji pomiędzy F-CPU a F-I/O służy parametr „domyślny czas monitorowania bezpieczeństwa".

Czas monitorowania można dostosować za pomocą następujących parametrów:

- „Domyślny czas monitorowania bezpieczeństwa dla centralnego F-I/O"
- „Domyślny czas monitorowania bezpieczeństwa dla F-I/O tego interfejsu"

Domyślny czas monitorowania bezpieczeństwa dla centralnego F-I/O działa na F-I/O ustawionym centralnie, tj. w pobliżu F-CPU. Parametr ten ustawia się we właściwościach F-CPU (należy wybrać F-CPU, następnie „Properties (Właściwości) > Fail-safe > F-parameters (Parametry bezpieczeństwa)").

Domyślny czas monitorowania bezpieczeństwa dla F-I/O tego interfejsu działa na F-I/O przypisany do danego interfejsu F-CPU (PROFIBUS lub PROFINET). Parametr ten zmienia się we właściwościach odnośnego interfejsu (należy wybrać interfejs w zakładce „Device view" (Widok urządzenia), a następnie „F-parameters" (Parametry bezpieczeństwa).

Różnorodne parametry pozwalają na elastyczne dopasowanie czasu monitorowania bezpieczeństwa do warunków danego systemu bezpieczeństwa, na przykład uwzględniając różne cykle magistrali.

Możliwa jest również zmiana czasu monitorowania dla poszczególnych F-I/O w ich właściwościach (patrz Konfigurowanie F-I/O (strona 51) lub Specjalne przypadki konfiguracji urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O (strona 76)).

Uwaga

Zmiana czasu monitorowania bezpieczeństwa dla centralnego lub rozproszonego F-I/O w CPU skutkuje zmianą programu bezpieczeństwa przy ponownej kompilacji. Może być konieczna nowa akceptacja.

⚠ OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcy i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania.
(S018)

Dodatkowe informacje można znaleźć w „Czasy monitorowania i odpowiedzi"
(strona 649).

Automatyczne generowanie programu bezpieczeństwa

Program bezpieczeństwa do F-CPU składa się z jednej lub dwóch grup F-runtime zawierających bloki bezpieczeństwa (zobacz także „Definiowanie grup F-runtime" (strona 139)). Gdy F-CPU (z aktywną funkcjonalnością bezpieczeństwa) zostanie wstawiony do obszaru roboczego widoku urządzenia lub widoku sieci, program bezpieczeństwa z grupą F-runtime jest generowany automatycznie.

Możliwe jest zdefiniowanie w *STEP 7 Safety,* by wstawienie F-CPU nie powodowało generowania grupy F-runtime (z aktywną funkcjonalnością bezpieczeństwa).

Należy wykonać co następuje:

1. Wybrać polecenie menu „Options (Opcje) > Settings (Ustawienia)".
2. Wybrać obszar „STEP 7 Safety".
3. Jeśli nie jest wyłączone, należy dezaktywować automatyczne generowanie grupy F-runtime poprzez odznaczenie opcji „Generate default fail-safe program" (Generuj domyślny program fail-safe).

Zmiana ta nie ma wpływu na istniejące programy bezpieczeństwa; definiuje jedynie, czy grupa F-runtime jest automatycznie generowana dla kolejnych wstawionych F-CPU.

Konfigurowanie poziomu zabezpieczenia dla F-CPU

OSTRZEŻENIE

(S7-300, S7-400) W trybie bezpieczeństwa, dostęp za pomocą hasła CPU nie może być autoryzowany podczas wprowadzania zmian w standardowym programie użytkownika, ponieważ pozwoliłoby to na zmiany w programie bezpieczeństwa. Aby wykluczyć taką możliwość, należy ustawić poziom zabezpieczenia „Write protection for fail-safe blocks" (Ochrona zapisu dla bloków fail-safe) i skonfigurować hasło dla F-CPU. Jeśli tylko jedna osoba jest upoważniona do zmiany standardowego programu użytkownika oraz programu bezpieczeństwa, należy ustawić poziom zabezpieczenia „Write protection" (Ochrona zapisu) lub „Read/write protection" (Ochrona odczytu/zapisu), by inne osoby miały jedynie ograniczony dostęp lub brak dostępu do całego programu użytkownika (programów standardowego i bezpieczeństwa). *(S001)*

OSTRZEŻENIE

(S7-1200, S7-1500) W trybie bezpieczeństwa, program bezpieczeństwa musi być zabezpieczony hasłem. W tym celu należy ustawić poziom zabezpieczenia co najmniej „Full access (no protection)" (Pełny dostęp (brak ochrony)) i przypisać hasło do „Full access incl. fail-safe (no protection)" (Pełny dostęp wraz z fail-safe (brak ochrony)). Ten poziom zabezpieczenia pozwala jedynie na pełny dostęp do standardowego programu użytkownika, nie do bloków bezpieczeństwa.

W przypadku wybrania wyższego poziomu, na przykład w celu zabezpieczenia standardowego programu użytkownika, należy przypisać dodatkowe hasło do opcji „Full access (no protection)" (Pełny dostęp (brak ochrony)).

Poziom zabezpieczenia ustawia się identycznie jak w przypadku standardowych CPU.

Informacje dotyczące hasła do F-CPU można znaleźć w „Ochrona dostępu" (strona 103). Należy zwrócić szczególną uwagę na ostrzeżenia w „Ochrona dostępu do F-CPU" (strona 109).

2.4 Konfiguracja F-I/O

Wstęp

Konfiguracja modułów bezpieczeństwa S7-1500/ET 200MP, ET 200SP, ET 200S, ET 200eco (S7-300, S7-400),
ET 200eco PN, ET 200pro oraz ET 200iSP, a także S7-300 F-SM i S7-1200 odbywa się jak zwykle w *STEP 7*:

Po wstawieniu F-I/O do obszaru roboczego *widoku urządzenia lub sieci*, uzyskuje się dostęp do okien konfiguracyjnych poprzez wybranie odpowiedniego F-I/O i zakładki „Properties" (Właściwości).

Uwaga

Zmiany w przypisaniu parametru skutkują zmianą programu bezpieczeństwa przy ponownej kompilacji. Może być konieczna nowa akceptacja.

Użycie modułu bezpieczeństwa ET 200SP jest możliwe z:

- IM 155-6 PN ST z oprogramowaniem V1.1
- IM 155-6 PN HF
- IM 155-6 PN/2 HF z oprogramowaniem V4.2
- IM 155-6 PN/3 HF z oprogramowaniem V4.2
- IM 155-6 PN HS
- IM 155-6 DP HF

Użycie modułu bezpieczeństwa S7-1500/ET 200MP jest możliwe z:

- IM 155-5 PN BA z oprogramowaniem V4.3
- IM 155-5 PN ST z oprogramowaniem V3.0
- IM 155-5 PN HF z oprogramowaniem V2.0
- IM 155-5 DP ST z oprogramowaniem V3.0

Centralne zastosowanie modułów bezpieczeństwa S7-1500/ET 200MP jest możliwe przy użyciu F-CPU S7-1500 z oprogramowaniem V1.7, zastosowanie rozproszone z oprogramowaniem V1.5.

(S7-1200) Zaleca się, by całkowita liczba F-I/O wykorzystywanych centralnie lub w sposób rozproszony w F-CPU S7-1200 nie przekraczała 12 sztuk. Zależnie od objętości danych projektu, maksymalna liczba F-I/O może być mniejsza.

OSTRZEŻENIE

Wykonując zmiany, w których przypisanie adresów wejść/wyjść i okablowanie może się zmienić, należy wykonać test podłączenia (strona 363).

Przykładami takich zmian są:

- Dodanie F-I/O
- Zmiana adresu początkowego F-I/O
- Zmiana pozycji gniazda F-I/O
- Zmiana
  - rack'a
  - adresu urządzenia podrzędnego
  - podsieci PROFIBUS DP/PROFINET IO
  - adresu IP
  - nazwy urządzenia

(S071)

Pasywacja szczegółowa kanału po awarii kanału

Możliwe jest skonfigurowanie sposobu, w jaki F-I/O odpowie na usterki kanału, takie jak zwarcie, przeciążenie, błąd rozbieżności lub przerwa w obwodzie, o ile F-I/O obsługuje ten parametr (np. dla modułów bezpieczeństwa ET 200S lub ET 200pro). Odpowiedź tą ustawia się we właściwościach odnośnego F-I/O (parametr „Behavior after channel fault" (Zachowanie po usterce kanału)). Parametr ten służy do określania, czy w razie usterki kanału pasywacji ulega całe F-I/O czy też tylko dotknięte usterką kanały.

Uwaga

(S7-300, S7-400) Należy pamiętać, że pasywacja szczegółowa kanału zwiększa czas pracy grup(y) F-runtime w porównaniu do pasywacji całego F-I/O (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).

Parametr „Zatwierdzenie awarii kanału" (S7-1200, S7-1500)

W przypadku F-I/O obsługujących parametr kanału „Channel failure acknowledge" (Zatwierdzenie awarii kanału) (przykładowo moduły bezpieczeństwa S7-1500/ET 200MP oraz moduły bezpieczeństwa S7-1200), zastępuje to tag ACK_NEC w bloku danych F-IO.

W przypadku wykrycia awarii F-I/O, występuje pasywacja wszystkich kanałów odnośnego F-I/O. W razie wykrycia awarii kanałów, są one pasywowane, jeśli ustawiono parametr „Passivate channel" (Pasywuj kanał). Jeśli ustawiono „Passivate the entire module" (Pasywuj cały moduł), pasywacji ulega cały odnośny F-I/O. Po usunięciu awarii kanału lub całego F-I/O następuje reintegracja odnośnego F-I/O zgodnie z parametrem „Channel failure acknowledge" (Zatwierdzenie awarii kanału).

- Automatycznie
- Ręcznie
- Nastawnie (po skonfigurowaniu pasywacji poszczególnych kanałów).

OSTRZEŻENIE

Przypisanie parametru „Channel failure acknowledge = Automatic" (Zatwierdzenie awarii kanału = automatyczne) jest dozwolone jedynie, jeśli automatyczna reintegracja jest dopuszczalna dla odnośnego procesu pod względem bezpieczeństwa. *(S045)*

Uwaga

Domyślne przypisanie parametru dla „Zatwierdzenia awarii kanału" po utworzeniu modułu bezpieczeństwa to „Manually" (Ręcznie).

Blok organizacyjny/obraz procesu (S7-1200, S7-1500)

W przypadku korzystania z F-I/O w trybie standardowym, można wybrać blok organizacyjny/obraz procesu identycznie jak w przypadku standardowego I/O.

W przypadku F-I/O w trybie bezpieczeństwa, wybór nie jest możliwy. Obraz procesu jest aktualizowany na początku lub końcu F-OB (patrz dział „Struktura programu bezpieczeństwa (S7-1200, S7-1500) (strona 117)).

W przeciwieństwie do F-I/O obsługiwanego w trybie nieizochronicznym, konieczne będzie wybranie podzielenia obrazu procesowego, na przykład PIP 1 dla F-I/O, który jest obsługiwany w trybie izochronicznym (patrz „Konfiguracja trybu izochronicznego (S7-1500) (strona 62)").

Zmiana nazwy i numeru DB F-I/O

Więcej informacji można znaleźć w dziale „Blok danych I/O typu fail-safe

(strona 174)".

Dostosowywanie czasu monitorowania bezpieczeństwa dla F-I/O

Dostosowanie czasu monitorowania bezpieczeństwa jest możliwe we właściwościach F-I/O w zakładce „F-parameters" (Parametry bezpieczeństwa). Może być to konieczne, by nie doszło do wyzwolenia przekroczenia czasu, gdy nie wystąpił błąd, a F-I/O wymaga dłuższego czasu monitorowania lub gdy przypisanie z domyślnym czasem nie jest możliwe. W tym celu należy zaznaczyć odpowiednie pole i przypisać czas monitorowania bezpieczeństwa.

Uwaga

Zmiana czasu monitorowania bezpieczeństwa dla centralnego lub rozproszonego F-I/O w CPU skutkuje zmianą programu bezpieczeństwa przy ponownej kompilacji. Może być konieczna nowa akceptacja.

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcy i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Dodatkowe informacje można znaleźć w „Czasy monitorowania i odpowiedzi" (strona 649).

Diagnostyka grupowa dla modułów sygnałowych S7-300 typu fail-safe

Wyłączając kanał modułu sygnałowego typu fail-safe we właściwościach modułu, możliwe jest również wyłączenie diagnostyki grupowej dla tego kanału.

Wyjątek dla F-CPU S7-300/400:

Dla następujących modułów sygnałowych typu fail-safe S7-300

- SM 326; DI 8 x NAMUR (pod numerem zamówieniowym 6ES7326-1RF00-0AB0)
- SM 326; DO 10 x DC 24V/2A (numer zamówieniowy 6ES7326-2BF01-0AB0

parametr „Group diagnostics" (Diagnostyka grupowa) pozwala na włączenie/wyłączenie monitorowania komunikatów diagnostycznych konkretnych kanałów F-SM (na przykład przerwa w obwodzie i zwarcie) do F-CPU. Należy wyłączyć diagnostykę grupową dla **nieużywanych** kanałów wejściowych lub wyjściowych.

OSTRZEŻENIE

(S7-300, S7-400) Dla następujących modułów sygnałowych typu fail-safe S7-300 (F-SM) z aktywnym trybem bezpieczeństwa, parametr „Group diagnostics" (Diagnostyka grupowa) musi być włączony dla wszystkich podłączonych kanałów:

- SM 326; DI 8 x NAMUR (numery zamówieniowe 6ES7326-1RF00-0AB0 i 6ES7326-1RF01- 0AB0)
- SM 326; DO 10 x DC 24V/2A (numer zamówieniowy 6ES7326-2BF01-0AB0)
- SM 336; AI 6 x 13 bit (numer zamówieniowy 6ES7336-1HE00-0AB0)

Należy sprawdzić, czy wyłączono diagnostykę grupową jedynie dla tych F-SM dla kanałów wejściowych i wyjściowych, które faktycznie nie są używane. *(S003)*

Opcjonalnie można włączyć przerwania diagnostyczne.

Informacje dodatkowe

Szczegółowy opis **parametrów** dostępny jest w pomocy do właściwości odnośnego F-I/O oraz w odpowiedniej *instrukcji obsługi F-I/O*.

2.5 Kontrola konfiguracji (zarządzanie opcjami) do F-I/O

Podczas kontroli konfiguracji (zarządzania opcjami) z F-I/O należy postępować tak jak przy standardowych urządzeniach I/O. Szczegółowe informacje dostępne są po wyszukaniu hasła „Configuration control (option handling)" (Kontrola konfiguracji (zarządzanie opcjami)) w pomocy *STEP 7*.

W poniższym dziale opisano, na co należy dodatkowo zwrócić uwagę przy F-I/O.

Wymogi

- Spełnienie wymogów określonych w „Kontrola konfiguracji (zarządzanie opcjami)" w pomocy *STEP 7*.
- Spełnienie wymogów określonych w „Kontrola konfiguracji (zarządzanie opcjami)" w pomocy *STEP 7*. Należy traktować F-I/O jak standardowy I/O.
- Wersja systemu bezpieczeństwa to V2.1 lub wyższa.
- F-I/O, dla których wykonywana jest kontrola konfiguracji (zarządzanie opcjami), są umieszczone
  - w sposób rozproszony w F-CPU S7-300/400/1200/1500
  - centralnie w F-CPU S7-1500
- Adres PROFIsafe dla F-I/O został ustawiony lub przypisany.

Uwaga

Przypisanie adresów PROFIsafe (strona 70) jest możliwe jedynie, jeśli maksymalna konfiguracja jest faktycznie obecna.

Procedura

(F-CPU S7-1200/1500) Należy wyłączyć F-I/O nieistniejące w danym wariancie (opcji), ustawiając zmienną DISABLE (WYŁĄCZ) (strona 181) w powiązanym DB F-I/O (strona 174) na „1". Zapobiega to miganiu diody błędy na F-CPU i wpisom diagnostycznym programu bezpieczeństwa, które odnoszą się do tych F-I/O. Za pomocą zmiennej DISABLED (WYŁĄCZONE) (strona 181) odnośnego bloku danych F-IO można ocenić, czy moduł bezpieczeństwa jest wyłączony.

(F-CPU S7-300/400) Aby nie dopuścić do migania diody błędu na F-CPU, należy zastosować się do dalszych wskazań. Zabronione jest tłumienie wejść diagnostycznych.

OSTRZEŻENIE

Podczas korzystania z kontroli konfiguracji, rzeczywista konfiguracja odbiega od ustawionej maksymalnej konfiguracji. Identyfikacja F-I/O, które nie istnieją w bieżącej opcji (opcji stanowiska) odbywa się z użyciem rejestru kontroli jako „not available" (niedostępne).

Jeśli F-I/O oznaczony jako „niedostępny" jest mimo to możliwy w rzeczywistym systemie, należy upewnić się, że dla tych F-I/O zastosowano wartości zastępcze (0) w programie bezpieczeństwa lub na wyjściach. Osiąga się to poprzez ustawienie znacznika DISABLE (WYŁĄCZ) (S7-1200/1500) lub taga PASS_ON (S7-300/400) w powiązanym DB F-I/O na „1". *(S077)*

2.5.1 Przykład

Wstęp

Poniższy przykład pokazuje, jak

- Zaznaczyć/odznaczyć opcję stanowiska
- Wyłączyć F-I/O, które nie są obecne w opcji stanowiska (S7-1200/1500)
- Zapewnić program bezpieczeństwa do różnych opcji stanowiska

Bezpieczne zaznaczanie/odznaczanie opcji stanowiska

Bezpieczne zaznaczanie/odznaczanie opcji stanowiska jest możliwe przy pomocy wejść F-I/O podłączonego do M/L+.

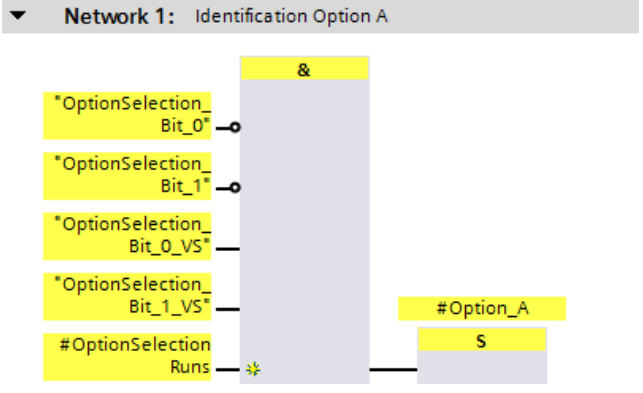
Przykładowo, można znaznaczyć do 4 opcji stanowiska za pomocą 2 wejść w F-I/O.

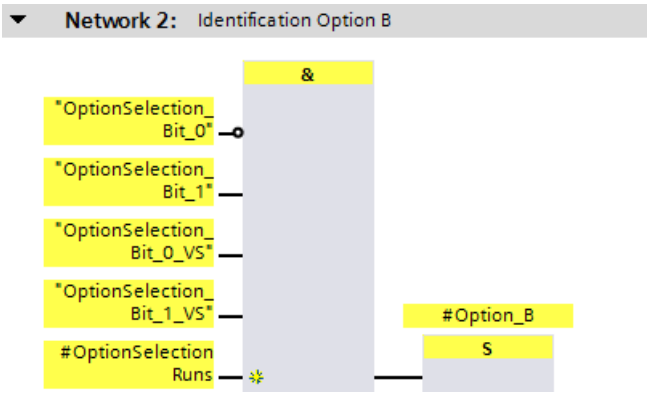
Opcje	OptionSelection_Bit_0	OptionSelection_Bit_1
Q	0	0
B	0	1
C	1	0
D	1	1

Należy pamiętać podczas detekcji opcji stanowiska, że w pewnych sytuacjach dla wejść F-I/O stosowane są wartości zastępcze (0), np. podczas rozruchu systemu bezpieczeństwa lub w przypadku wystąpienia błędu kanału F-I/O.

W takich sytuacjach nie jest możliwe wykrycie bieżącej opcji stanowiska. Należy zatem ocenić również stan wartości wejść i zastosować opcję stanowiska jednokrotnie po uruchomieniu systemu bezpieczeństwa.

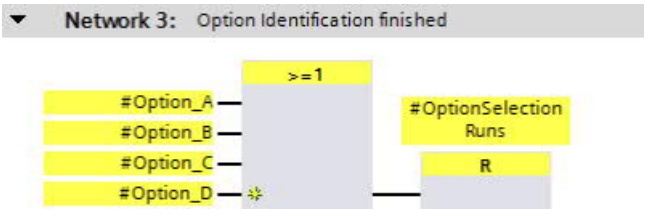
Aby wykonać jednokrotne rozpoznanie opcji stanowiska, należy zdefiniować statyczną daną lokalną, przykładowo, OptionSelectionRuns, wartością domyślną „TRUE" (PRAWDA).





Analogicznie dla opcji C i D.

Niezwłocznie po wykryciu opcji stanowiska należy zresetować statyczną daną lokalną dla jednokrotnej detekcji opcji:



Uwaga

Wykonując zaznaczenie/odznaczenie opcji stanowiska tylko w standardowym programie użytkownika, dostępna jest jedynie „opcja stanowiska" jako standardowa dana, która nie jest zabezpieczona.

Należy upewnić się, że nie spowoduje to powstanie niebezpiecznego stanu.

Należy zapoznać się z działem „Wymiana danych pomiędzy standardowym programem użytkownika a programem bezpieczeństwa" (strona 204).

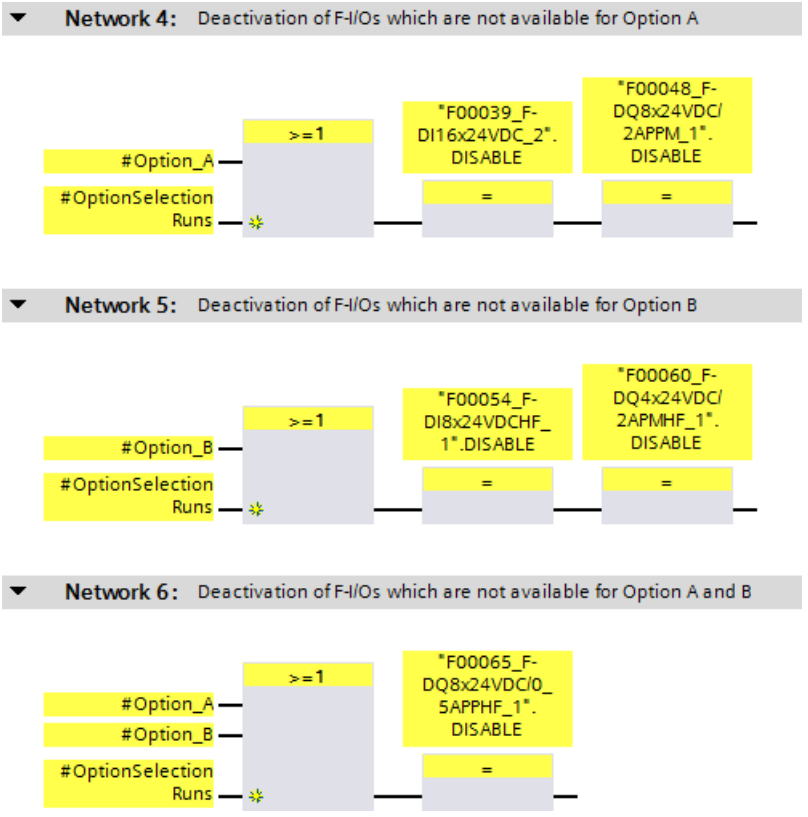
Wyłączanie F-I/O, które nie są obecne w opcji stanowiska

Jeśli jeden lub kilka F-I/O nie jest obecnych w opcji stanowiska, można zapobiec miganiu diody błędu na F-CPU, wyłączając je.

Oprócz tego tłumione są komunikaty diagnostyczne programu bezpieczeństwa, które odnoszą się do tych F-I/O.

Uwaga

Dopóki detekcja opcji stanowiska (podczas rozruchu systemu bezpieczeństwa) nie zostanie ukończona (OptionSelectionRuns = TRUE), należy wyłączyć wszystkie „opcjonalne" urządzenia F-I/O.



Zapewnienie programu bezpieczeństwa do różnych opcji stanowiska

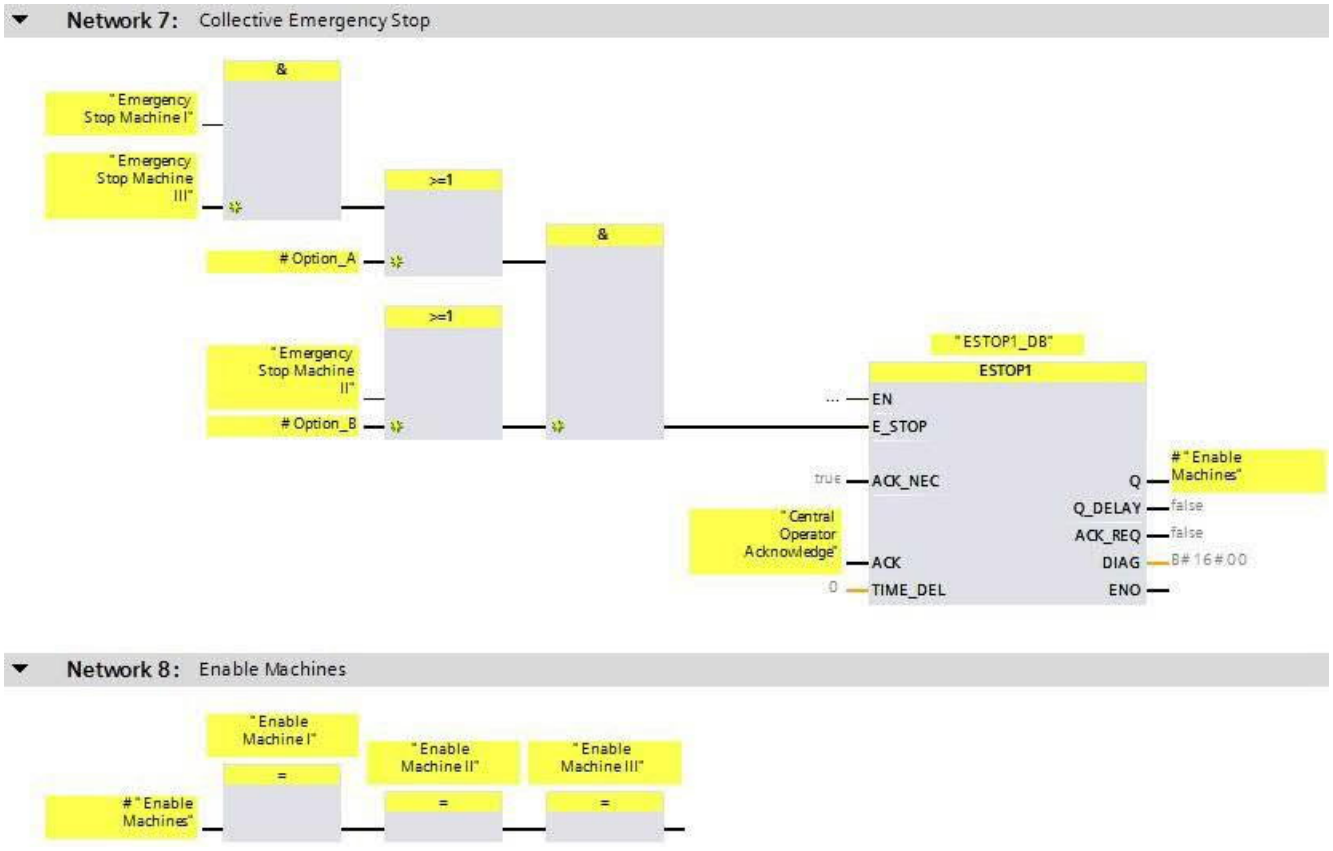
W poniższym przykładzie sygnały ZATRZYMANIE AWARYJNE z różnych jednostek w instalacji lub maszyn są łączone w zbiorczy sygnał ZATRZYMANIE AWARYJNE.

Maszyny I i III oraz odnośne F-I/O z sygnałem ZATRZYMANIE AWARYJNE dla maszyn I i III nie są obecne w opcji stanowiska A.

Maszyna II oraz odnośne F-I/O z sygnałem ZATRZYMANIE AWARYJNE dla maszyny II nie jest obecne w opcji stanowiska B.

W programie bezpieczeństwa zastosowano wobec tego wartości zastępcze (0) dla sygnałów ZATRZYMANIE AWARYJNE z odnośnych nieużywanych maszyn.

Aby nie dopuścić do wyzwolenia zbiorczego sygnału ZATRZYMANIE AWARYJNE z powodu braku obecności sygnałów maszyn / ZATRZYMANIA AWARYJNEGO w pewnych opcjach stanowisk, można stłumić ocenę sygnału awaryjnego dla niedostępnych maszyn poprzez uwzględnienie obecnej opcji stanowiska.



2.6 Konfiguracja współdzielonego urządzenia

Aby skonfigurować współdzielone urządzenia, należy wykonać procedurę identyczną jak w przypadku standardowej wersji. Konfiguracja została opisana w pomocy *STEP 7* pod hasłem „Konfiguracja współdzielonego urządzenia".

Adresy docelowe bezpieczeństwa

Należy również zapoznać się z rozdziałem „Zalecenia dotyczące przypisywania adresu (strona 63)" w celu przypisania adresu docelowego bezpieczeństwa.

Zobacz także

Przypisywanie adresów PROFIsafe do modułu bezpieczeństwa (strona 74)

2.7 Konfiguracja trybu izochronicznego (S7-1500)

Aby skonfigurować tryb izochroniczny dla F-I/O, które obsługują ten tryb, np. submoduł „Profisafe Telgr 902" sterownika SINAMICS S120 CU310-2 PN V5.1, należy postępować identycznie jak w przypadku standardowej wersji. Konfiguracja została opisana w pomocy *STEP 7* pod hasłem „Konfiguracja trybu izochronicznego".

Należy mieć na uwadze następuje zagadnienia:

- W przeciwieństwie do F-I/O obsługiwanego w trybie nieizochronicznym, konieczne będzie wybranie podzielenia obrazu procesowego, na przykład PIP 1 dla F-I/O, który jest obsługiwany w trybie izochronicznym.
  Podział obrazu procesumusi zawierać jedynie F-I/O obsługiwane w trybie izochronicznym oraz nie zawierać standardowych I/O.
- Wyznaczone OB przerwania trybu izochronicznego muszą być najpierw wygenerowane jako F-OB poprzez określenie grupy F-runtime (patrz „Procedura definiowania grupy F-runtime (S7-1200, S7-1500)" (strona 145)). Nie jest możliwe dodanie F-OB z klasą zdarzenia „Synchronous Cycle" (Cykl synchroniczny) bezpośrednio podczas konfiguracji trybu izochronicznego.

Wymogi

F-CPU S7-1500 od wersji oprogramowania 2.0, z obsługą IRT.

Połączenie F-I/O obsługiwanego w trybie izochronicznym z OB przerwania trybu izochronicznego

Dostęp do F-I/O obsługiwanego w trybie izochronicznym odbywa się identycznie jak przy standardowym I/O obsługiwanym w takim trybie, poprzez wybranie podzielenia obrazu procesowego.

W przeciwieństwie do standardowego I/O, obsługiwanego w trybie izochronicznym, podział obrazu procesujest aktualizowany przez system bezpieczeństwa na początku lub na końcu F-OB (patrz Struktura programu bezpieczeństwa (S7-1200, S7-1500) (strona 117)).

Nie jest wymagane wywołanie instrukcji SYNC_PI oraz SYNC_PO w F-OB.

Uwaga

Przy F-I/O obsługiwanych izochronicznie, nie jest zagwarantowane (fail-safe), że wszystkie dane wejściowe F-I/O przypisane do podziału obrazu procesusą spójnie dostępne na początku głównego bloku bezpieczeństwa ani też że dane wyjściowe są przesyłane spójnie do F-I/O; innymi słowy, że są logicznie i czasowo zgodne. Spójność jest gwarantowana jedynie w obrębie F-I/O.

Spójność wszystkich izochronicznych F-I/O podziału obrazu procesuzazwyczaj zależy od liczby izochronicznych F-I/O oraz zakresu programu bezpieczeństwa w OB przerwania trybu izochronicznego.

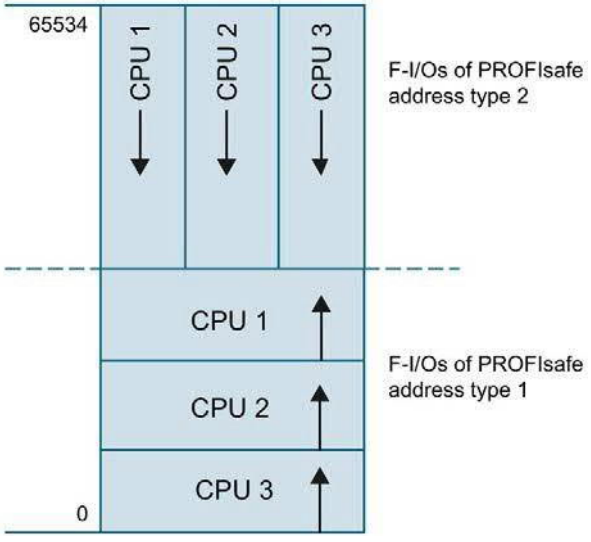
Jeśli występują odnośne wymogi dotyczące spójności, należy samodzielnie sprawdzić spójność danych wejściowych i wyjściowych. Można wykonać to, przykładowo, poprzez dodatkowe przeniesienie i wykonanie oceny tagów czasowych danych wejściowych i wyjściowych izochronicznych F-I/O.

2.8 Zalecenia dotyczące przypisywania adresu PROFIsafe

Przed wstawieniem F-I/O należy określić zakres adresowy dla każdego F-CPU dla adresów docelowych bezpieczeństwa do F-I/O typu adresowania PROFIsafe 1 (strona 66), by nie nakładał się na zakres adresowy innych F-CPU w sieci lub w CPU (w systemie). Zakres F-I/O typu adresowania PROFIsafe 1 definiuje się za pomocą parametrów „Dolny limit adresów docelowych bezpieczeństwa" oraz „Górny limit adresów docelowych bezpieczeństwa" (zobacz również dział Konfiguracja F-CPU (strona 46)).

Adresy docelowe bezpieczeństwa do F-I/O typu adresowania PROFIsafe 2 (strona 68) nie mogą nakładać się na inne zakresy adresowe do F-I/O typu adresowania PROFIsafe 1. Zakresy adresów docelowych bezpieczeństwa F-I/O typu adresowania PROFIsafe 2 mogą nakładać się, jeśli adresy źródłowe bezpieczeństwa różnią się. Ma to miejsce przy obsługiwanych konfiguracjach (strona 64), jeśli parametr „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) został ustawiony w różny sposób dla każdego F-CPU.

Należy przypisać względnie niski adres docelowy bezpieczeństwa dla F-I/O typu adresowania PROFIsafe 1 oraz względnie wysoki adres docelowy bezpieczeństwa dla F-I/O typu adresowania PROFIsafe 2.



Ilustracja 2-1 Przypisanie adresów do F-I/O typu adresowania PROFIsafe 1 i 2

Podsumowanie bezpieczeństwa (strona 379) wyszczególnia następujące informacje dla poszczególnych F-CPU:

- Parametr „Centralny adres źródłowy bezpieczeństwa" (adres źródłowy bezpieczeństwa do F-I/O typu adresowania PROFIsafe 2)
- Faktycznie używany zakres adresów docelowych bezpieczeństwa przypisanego F-I/O typu adresowania PROFIsafe 1
- Faktycznie używany zakres adresów docelowych bezpieczeństwa przypisanego F-I/O typu adresowania PROFIsafe 2

Wszelkie F-I/O skonfigurowane przy użyciu komunikacji urządzenie I-slave – urządzenie podrzędne są uwzględniane w podsumowaniu bezpieczeństwa jako część zakresu adresu docelowego bezpieczeństwa urządzenia I-slave.

Wszelkie F-I/O skonfigurowane we współdzielonym urządzeniu są określane w podsumowaniu bezpieczeństwa jako część zakresu adresu docelowego bezpieczeństwa dla F-CPU, do którego przypisany jest F-I/O.

2.9 Konfiguracje obsługiwane przez system bezpieczeństwa SIMATIC Safety

Obsługiwane konfiguracje

F-I/O (patrz „Omówienie konfiguracji" (strona 41)) są obsługiwane w następujących konfiguracjach:

konfiguracja centralna (również urządzenie I-slave):

- F-I/O znajduje się na tym samym regale co powiązany F-CPU
- F-I/O znajduje się na podregale regału powiązanego F-CPU.

konfiguracja rozproszona (przy zintegrowanym interfejsie DP-/PN CPU lub przy CP/CM):

- PROFIBUS (również po połączeniu IE/PB)
  - F-I/O znajduje się na urządzeniu podrzędnym DP.
  - F-I/O znajduje się na urządzeniu podrzędnym DP i jest adresowane poprzez komunikację urządzenie I-slave – urządzenie podrzędne.
    Przypisane urządzenie nadrzędne DP (przypisanego sterownika IO połączenia IE/PB) może być standardowym CPU lub F-CPU.
- PROFINET IO
  - F-I/O znajduje się na urządzeniu IO.
  - F-I/O znajduje się na urządzeniu współdzielonym.

Dla F-I/O nie wyszczególnionych w „Omówieniu konfiguracji" (strona 41), należy zapoznać się z odnośną dokumentacją, by sprawdzić, czy są obsługiwane one przez system bezpieczeństwa SIMATIC Safety. W razie wątpliwości należy potraktować takie F-I/O jako część konfiguracji, która nie jest obsługiwana.

Kontrole wykonywane przez system bezpieczeństwa SIMATIC Safety

- Czy parametr trybu obsługi PROFIsafe (F_Par_Version) jest ustawiony na tryb V2 w środowisku PROFINET IO**.
- Czy adresy docelowe bezpieczeństwa zostały przypisane unikalnie w obrębie CPU. Należy samodzielnie zapewnić unikalność adresów PROFIsafe w obrębie sieci.
- Czy adres źródłowy bezpieczeństwa dla F-I/O typu adresowania PROFIsafe 2 odpowiada parametrowi „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) dla F-CPU.

OSTRZEŻENIE

Korzystając z konfiguracji, które nie są uwzględnione w obsługiwanych, należy mieć na uwadze następuje zagadnienia:

- Należy upewnić się, że F-I/O tej konfiguracji występuje w podsumowaniu bezpieczeństwa oraz że DB dla F-I/O został utworzony. W przeciwnym razie nie można wykorzystać F-I/O w tej konfiguracji. (Należy skontaktować się z działem obsługi klienta.)
- Dla F-I/O w środowisku PROFINET IO**, należy sprawdzić parametr trybu pracy PROFIsafe (F_Par_Version) z podsumowaniem bezpieczeństwa, by upewnić się, że jest on poprawny. W środowisku PROFINET IO musi być ustawiony tryb V2. F-I/O obsługujące jedynie tryb V1 nie mogą być zastosowane w środowisku PROFINET IO.
- Należy upewnić się, że przypisanie adresów PROFIsafe jest unikalne w obrębie CPU* oraz w całej sieci***:
  - Należy sprawdzić poprawność adresów PROFIsafe, korzystając z podsumowania bezpieczeństwa.
  - Za pomocą podsumowania bezpieczeństwa można sprawdzić, czy adres źródłowy bezpieczeństwa odpowiada parametrowi „Centralny adres źródłowy bezpieczeństwa" F-CPU dla F-I/O typu adresowania PROFIsafe 2.
  - Dla F-I/O typu adresowania PROFIsafe 1, lub jeśli nie można ustawić adresu źródłowego bezpieczeństwa zgodnie z parametrem F-CPU „Centralny adres źródłowy bezpieczeństwa", konieczne jest zagwarantowanie unikalności adresu PROFIsafe wyłącznie poprzez przypisanie unikalnego adresu docelowego bezpieczeństwa.

  Należy sprawdzić unikalność adresu docelowego bezpieczeństwa indywidualnie dla każdego F-I/O, który znajduje się w konfiguracji, która nie jest obsługiwana, korzystając z podsumowania bezpieczeństwa. (patrz „Kompletność i poprawność konfiguracji sprzętowej" (strona 383)) *(S050)*

* „W obrębie CPU" oznacza wszystkie F-I/O przypisane do F-CPU: Centralny F-I/O tego F-CPU, a także F-I/O, dla których F-CPU to urządzenie nadrzędne DP/sterownik IO oraz przypisane F-I/O we współdzielonym urządzeniu. F-I/O adresowany przy pomocy komunikacji urządzenie I-slave – urządzenie podrzędne jest przypisywany do F-CPU urządzenia I-slave, a nie do F-CPU urządzenia nadrzędnego DP / sterownika IO.

** F-I/O znajduje się w „środowisku PROFINET IO", jeśli co najmniej część komunikacji związanej z bezpieczeństwem z F-CPU odbywa się poprzez PROFINET IO. Jeśli F-I/O jest podłączony poprzez komunikację urządzenie I-slave – urządzenie podrzędne, należy uwzględnić linię komunikacyjną do urządzenia nadrzędnego DP / sterownika IO.

*** Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

Uwaga

Więcej informacji dotyczących przypisywania adresów PROFIsafe unikalnych dla CPU oraz sieci, sprawdź FAQ (https://support.industry.siemens.com/cs/ww/en/view/109740240).

2.10 Adresy PROFIsafe do F-I/O typu adresowania PROFIsafe 1

Adres docelowy bezpieczeństwa

Unikalność adresu PROFIsafe jest zapewniana wyłącznie za sprawą adresu docelowego bezpieczeństwa. Adres źródłowy bezpieczeństwa nie jest wyświetlany i nie ma wpływu na to, czy adres PROFIsafe jest unikalny.

Dlatego też, adres docelowy bezpieczeństwa musi być unikalny w całej sieci oraz w obrębie CPU (patrz poniższe zasady przypisywania adresu).

Aby nie dopuścić do nieprawidłowego przypisania parametru, adres docelowy bezpieczeństwa, unikalny w obrębie CPU, jest automatycznie przypisywany podczas umieszczania F-I/O w obszarze roboczym urządzenia lub widoku sieci, o ile konfiguruje się jedynie obsługiwane konfiguracje (strona 64).

Aby zapewnić unikalność przypisania adresu docelowego bezpieczeństwa w całej sieci w przypadku, gdy działają w niej systemy nadrzędne DP oraz systemy PROFINET IO, należy odpowiednio ustawić „Dolny limit adresów docelowych bezpieczeństwa" oraz „Górny limit adresów docelowych bezpieczeństwa" we właściwościach F-CPU w systemach bezpieczeństwa SIMATIC Safety, nim umieści się F-I/O (patrz dział „Zalecenia dotyczące przypisywania adresu"), aby nie doszło do nałożenia zakresów adresów.

Zmieniając adres docelowy bezpieczeństwa dla F-I/O, unikalność tego adresu w obrębie CPU jest sprawdzana automatycznie dla obsługiwanych konfiguracji. Należy samodzielnie zapewnić unikalność adresów docelowych bezpieczeństwa.

Dla modułów bezpieczeństwa ET 200S, ET 200eco (PROFIBUS), ET 200pro, ET 200iSP oraz F-SM S7-300:
Przed zainstalowaniem F-I/O należy ustawić adres docelowy bezpieczeństwa, korzystając z przełącznika DIP. Możliwe jest przypisanie do 1022 różnych adresów docelowych bezpieczeństwa.

Uwaga

(S7-300, S7-400) Dla następujących modułów sygnałowych typu fail-safe S7-300, adres docelowy bezpieczeństwa to adres początkowy F-SM podzielony przez 8:

- SM 326; DI 8 x NAMUR (pod numerem zamówieniowym 6ES7326-1RF00-0AB0)
- SM 326; DO 10 x DC 24V/2A (numer zamówieniowy 6ES7326-2BF01-0AB0)
- SM 336; AI 6 x 13 bit (numer zamówieniowy 6ES7336-1HE00-0AB0)

W widoku urządzenia przeglądu można wyświetlić kolumny „F-source address" (Adres źródłowy bezpieczeństwa) oraz „F-destination address" (Adres docelowy bezpieczeństwa). Adresy wyświetlane w tych kolumnach mają charakter jedynie informacyjny. Podczas akceptacji systemu należy sprawdzić adresy docelowe bezpieczeństwa w podsumowaniu bezpieczeństwa.

Zasady przypisywania adresu

OSTRZEŻENIE

F-I/O do typu adresowania PROFIsafe 1 są unikalnie adresowane przez ich adresy docelowe bezpieczeństwa (np. za pomocą ustawienia przełącznika adresowego).

Adres docelowy bezpieczeństwa (a zatem również ustawienie przełącznika adresowego) dla F-I/O musi być unikalny w całej sieci* oraz w obrębie CPU (w obrębie systemu) **dla całego** F-I/O. Należy również uwzględnić F-I/O typu adresowania PROFIsafe 2. *(S051)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** „W obrębie CPU" oznacza wszystkie F-I/O przypisane do F-CPU: Centralny F-I/O tego F-CPU, a także F-I/O, dla których F-CPU to urządzenie nadrzędne DP/sterownik IO oraz przypisane F-I/O we współdzielonym urządzeniu. F-I/O adresowany przy pomocy komunikacji urządzenie I-slave – urządzenie podrzędne jest przypisywany do F-CPU urządzenia I-slave, a nie do F-CPU urządzenia nadrzędnego DP / sterownika IO.

Zwróć również uwagę na zalecenia dotyczące przypisywania adresu PROFIsafe (strona 63).

Uwaga

Więcej informacji dotyczących przypisywania adresów PROFIsafe unikalnych dla CPU oraz sieci, sprawdź FAQ (https://support.industry.siemens.com/cs/ww/en/view/109740240).

Zobacz także

Kompletność podsumowania bezpieczeństwa (strona 379)

2.11 Adresy PROFIsafe do F-I/O typu adresowania PROFIsafe 2

Adres źródłowy bezpieczeństwa oraz adres docelowy bezpieczeństwa

Unikalność adresu PROFIsafe jest zapewniana poprzez połączenie adresu źródłowego bezpieczeństwa oraz adresu docelowego bezpieczeństwa.

Adres PROFIsafe musi być unikalny dla całej sieci i w obrębie CPU. Osiąga się to po spełnieniu poniższych dwóch warunków:

- Adres źródłowy bezpieczeństwa (parametr „Centralny adres źródłowy bezpieczeństwa") dla F-CPU jest unikalny dla całej sieci. Należy pamiętać o tym w przypadku zmian.
- Adres docelowy bezpieczeństwa modułu bezpieczeństwa jest unikalny w obrębie CPU.

Adres źródłowy bezpieczeństwa definiuje się za pomocą parametru „Centralny adres źródłowy bezpieczeństwa" w F-CPU. Zakładając skonfigurowanie obsługiwanej konfiguracji (strona 64), parametr ten jest automatycznie stosowany jako adres źródłowy bezpieczeństwa, po czym przypisywany jest adres docelowy bezpieczeństwa unikalny w obrębie CPU (zazwyczaj w kolejności malejącej, począwszy od 65534).

Zmieniając adres docelowy bezpieczeństwa dla, unikalność tego adresu w obrębie CPU jest sprawdzana automatycznie dla obsługiwanych konfiguracji.

Konieczne jest przypisanie adresu źródłowego bezpieczeństwa oraz adresu docelowego bezpieczeństwa do F-I/O przed wykonaniem jego odbioru technicznego. Dodatkowe informacje można znaleźć w dziale „Przypisywanie adresu PROFIsafe F-I/O za pomocą SIMATIC Safety" (strona 70).

W widoku urządzenia przeglądu można wyświetlić kolumny „F-source address" (Adres źródłowy bezpieczeństwa) oraz „F-destination address" (Adres docelowy bezpieczeństwa). Adresy wyświetlane w tych kolumnach mają charakter jedynie informacyjny. Podczas akceptacji systemu należy sprawdzić adresy źródłowy i docelowy bezpieczeństwa w podsumowaniu bezpieczeństwa.

Zasady przypisywania adresu

⚠ OSTRZEŻENIE

F-I/O typu adresowania PROFIsafe 2 jest adresowany unikalnie przy pomocy połączenia adresu źródłowego bezpieczeństwa (parametr „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) przypisanego F-CPU) oraz adresu docelowego bezpieczeństwa.

Połączenie adresu źródłowego bezpieczeństwa oraz adresu docelowego bezpieczeństwa dla każdego F-I/O musi być unikalne w całej sieci* oraz w obrębie CPU** (w obrębie systemu). Ponadto, adres docelowy bezpieczeństwa nie może być zajmowany przez F-I/O typu adresowania PROFIsafe 1.

Aby zapewnić, że adresy są unikalne dla F-CPU dla obsługiwanych konfiguracji (strona 64), należy upewnić się, iż parametr „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) dla wszystkich F-CPU jest unikalny w całej sieci*. Osiąga się to poprzez różne ustawienia parametru „Centralny adres źródłowy bezpieczeństwa" dla F-CPU. *(S052)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** „W obrębie CPU" oznacza wszystkie F-I/O przypisane do F-CPU: Centralny F-I/O tego F-CPU, a także F-I/O, dla których F-CPU to urządzenie nadrzędne DP/sterownik IO oraz przypisane F-I/O we współdzielonym urządzeniu. F-I/O adresowany przy pomocy komunikacji urządzenie I-slave – urządzenie podrzędne jest przypisywany do F-CPU urządzenia I-slave, a nie do F-CPU urządzenia nadrzędnego DP / sterownika IO.

Zwróć również uwagę na Zalecenia dotyczące przypisywania adresu PROFIsafe (strona 63).

Uwaga

Więcej informacji dotyczących przypisywania adresów PROFIsafe unikalnych dla CPU oraz sieci, sprawdź FAQ (https://support.industry.siemens.com/cs/ww/en/view/109740240).

Zobacz także

Kompletność podsumowania bezpieczeństwa (strona 379)

2.12 Ustawianie adresów docelowych bezpieczeństwa dla F-I/O za pomocą przełączników DIP

Informacje dotyczące ustawiania adresu docelowego bezpieczeństwa dla F-I/O z przełącznikami DIP są dostępne w dokumentacji odnośnego F-I/O.

2.13 Przypisywanie adresu PROFIsafe F-I/O za pomocą SIMATIC Safety

Wstęp

Moduły fail-safe ET 200SP, moduły fail-safe S7-1500/ET 200MP, moduły I/O fail-safe ET 200eco PN oraz moduły fail-safe S7-1200 nie są wyposażone w przełącznik DIP, za pomocą którego ustawia się unikalny adres docelowy bezpieczeństwa dla danego modułu. Zamiast tego przypisuje się adres PROFIsafe (strona 64), zawierający adres źródłowy bezpieczeństwa oraz adres docelowy bezpieczeństwa bezpośrednio z *STEP 7 Safety* dla modułów fail-safe ET 200SP, modułów I/O fail-safe ET 200eco PN oraz modułów fail-safe S7- 1500/ET 200MP. Adresy PROFIsafe do modułów bezpieczeństwa S7-1200 są przypisywane automatycznie podczas pobierania konfiguracji sprzętowej.

W poniższych przypadkach konieczne przypisanie adresów modułów I/O fail-safe ET 200SP, fail-safe ET 200eco PN oraz modułów fail-safe S7-1500/ET 200MP:

- Późniejsze umieszczenie modułu fail-safe podczas początkowego odbioru technicznego (nie do ET 200eco PN)
- Celowa modyfikacja adresu docelowego bezpieczeństwa
- Modyfikacja parametru „Centralny adres źródłowy bezpieczeństwa" do powiązanego F-CPU (zmiana adresu źródłowego bezpieczeństwa).
- Wymiana elementu kodującego
- Odbiór techniczny maszyny z produkcji seryjnej

W poniższych przypadkach konieczne przypisanie adresów modułów fail-safe ET 200SP oraz modułów fail-safe S7-1500/ET 200MP:

- Włączenie/wyłączenie zasilania
- Wymiana modułu bezpieczeństwa (naprawa) bez PG/PC
- Wymiana BaseUnit (przeniesienie elementu kodującego z przypisanym adresem źródłowym bezpieczeństwa oraz adresem docelowym bezpieczeństwa do nowej jednostki BaseUnit)
- Wymiana BaseUnit bez elementu kodującego
- Zmiany w wykonaniu w przypadku wstawienia nowego BaseUnit przed modułem fail-safe
- Naprawa/wymiana modułu interfejsu

Ponowne przypisanie nie jest wymagane dla modułów I/O fail-safe ET 200eco PN w następujących przypadkach:

- Włączenie/wyłączenie zasilania
- Wymiana urządzenia kompaktowego (przeniesienie elementu kodującego z przypisanym adresem źródłowym bezpieczeństwa oraz adresem docelowym bezpieczeństwa do nowego urządzenia kompaktowego)

Procedura

Uwaga

Przypisanie adresu PROFIsafe do modułów fail-safe S7-1200

Procedura opisana poniżej, dotycząca identyfikacji i przypisania adresów PROFIsafe nie jest wymagana przy modułach fail-safe S7-1200.

Należy pamiętać, że F-CPU S7-1200 nie może zawierać dodatkowego,

nieskonfigurowanego modułu bezpieczeństwa.

1. Skonfigurować adres docelowy bezpieczeństwa (strona 68) oraz adres źródłowy bezpieczeństwa (strona 68) w konfiguracji sprzętowej w *STEP 7 Safety*.
2. Zidentyfikować moduły ET 200SP, S7-1500/ET 200MP lub moduły I/O typu fail-safe ET 200eco PN, do których mają zostać przypisane skonfigurowane adresy PROFIsafe.
3. Przypisać adres PROFIsafe do modułów bezpieczeństwa.

2.13.1 Identyfikacja modułów bezpieczeństwa

Wymogi

Należy spełnić następujące wymogi:

- F-CPU i moduły fail-safe zostały skonfigurowane.
- Konfiguracja sprzętowa została pobrana.
- Korzystając ze sterownika Open Controller ET 200SP Open, należy pobrać konfigurację sprzętową sterownika Open Controller ET 200SP **oraz** sterownik programowy fail-safe.
- Dostęp do F-CPU i modułów fail-safe jest możliwy online.

⚠ OSTRZEŻENIE

Należy upewnić się, że do F-CPU przed identyfikacją pobrano najnowszą konfigurację sprzętową.

Kliknięcie na „Identification" (Identyfikacja) potwierdzi poprawność fail-safe adresów PROFIsafe dla modułów fail-safe.

Dlatego też należy zachować uwagę podczas potwierdzenia modułów bezpieczeństwa za pomocą migających diod LED lub numeru seryjnego F-CPU z centralnymi modułami fail-safe lub numeru seryjnego modułu interfejsu z modułami fail-safe.

Przypisanie adresów PROFIsafe z numerem seryjnym modułu interfejsu lub F-CPU jest dozwolone jedynie, gdy przypisanie dotyczy wszystkich F-I/O stacji. Wybierając poszczególne F-I/O, należy sprawdzić i potwierdzić miganie diod poszczególnych F-I/O. *(S046)*

Procedura

Aby zidentyfikować moduły bezpieczeństwa,

1. Ustanowić połączenie online z F-CPU, z którym obsługiwane są moduły fail-safe.
2. W widoku sieci należy wybrać F-CPU z modułami fail-safe lub moduł interfejsu z modułami fail-safe, do którego ma zostać przypisany adres PROFIsafe.
3. Wybrać „Assign PROFIsafe address" (Przypisz adres PROFIsafe) w menu skrótów.
4. Pod opcją „Assign PROFIsafe address by" (Przypisz adres PROFIsafe poprzez) należy wybrać metodę identyfikacji modułów bezpieczeństwa.

   - "Identification by LED flashing" (Identyfikacja po migającej diodzie LED)

     Jest to domyślne ustawienie. Diody LED „DIAG" i „STATUS" modułów bezpieczeństwa migają podczas identyfikacji.

   - "Identification by serial number" (Identyfikacja po numerze seryjnym)

     Jeśli moduły fail-safe nie są bezpośrednio widoczne, można zidentyfikować je po numerze seryjnym F-CPU lub modułu interfejsu.

     Uwaga

     Wyświetlany numer seryjny można zastąpić rokiem produkcji porównanym do numeru seryjnego nadrukowanego na module interfejsu. Numery seryjne są jednakże identyczne.

     Uwaga

     Określanie numeru seryjnego sterownika Open Controller ET 200SP

     W przypadku stosowania modułów bezpieczeństwa ET 200SP centralnie na sterowniku Open Controller ET 200SP i identyfikacji ich po numerze seryjnym, należy odczytać numer z wyświetlacza sterownika programowego S7-1500 typu fail-safe w menu „Overview > CPU" (Przegląd > CPU).

5. W kolumnie „Assign" (Przypisz) należy wybrać wszystkie moduły bezpieczeństwa, do których ma zostać przypisany adres PROFIsafe.

   W przypadku wybrania F-CPU lub modułu interfejsu w kolumnie "Assign" (Przypisz), wszystkie moduły bezpieczeństwa stacji są zaznaczone.

6. Kliknąć na przycisk „Identification" (Identyfikacja). Należy sprawdzić, czy diody LED „DIAG" oraz „STATUS" dla modułów bezpieczeństwa, których adresy PROFIsafe mają zostać przypisane, migają na zielono. W przypadku identyfikacji po numerze seryjnym, należy porównać wyświetlany numer seryjny z numerem na F-CPU z centralnymi modułami fail-safe lub z modułem interfejsu z modułami fail-safe.

7. W przypadku skonfigurowania większej liczby modułów typu fail-safe S7-1500/ET 200MP niż istniejące online, wyświetli się okno dialogowe. Należy wprowadzić liczbę modułów typu fail-safe S7-1500/ET 200MP faktycznie obecnych i zatwierdzić okno.

   W przypadku skonfigurowania mniejszej liczby modułów typu fail-safe S7-1500/ET 200MP niż istniejące online, zostanie wyświetlona różnica online-offline, a przypisanie adresu PROFIsafe nie będzie możliwe.

2.13.2 Przypisywanie adresów PROFIsafe

Wymogi

Moduły bezpieczeństwa zostały pomyślnie zidentyfikowane.

Procedura

Aby przypisać adres PROFIsafe, należy wykonać co następuje:

1. W kolumnie „Confirm" (Zatwierdź) należy wybrać wszystkie moduły typu fail-safe, do których mają zostać przypisane adres źródłowy bezpieczeństwa oraz adres docelowy bezpieczeństwa.
2. Przy pomocy przycisku „Assign PROFIsafe address" (Przypisz adres PROFIsafe) należy przypisać adresy do modułów typu fail-safe. Może być konieczne wprowadzenie hasła do F-CPU.

   Należy zatwierdzić okno „Acknowledge assignment" (Zatwierdź przypisanie) w ciągu 60 sekund, by wprowadzić adres PROFIsafe.

2.13.3 Przypisywanie adresów PROFIsafe do modułu bezpieczeństwa

Wstęp

W oknie „Assign PROFIsafe address" (Przypisywanie adresów PROFIsafe) widoczne są jedynie te moduły bezpieczeństwa, które zostały przypisane do F-CPU tego projektu, ponieważ adres PROFIsafe modułu bezpieczeństwa we współdzielonym urządzeniu może być przypisany z projektu, w którym znajduje się F-CPU, do którego są przypisane moduły bezpieczeństwa.

Wymogi

Wymogiem do przypisania adresu PROFIsafe jest kompletne wgranie konfiguracji sprzętowej do F-CPU. Po przypisaniu modułów bezpieczeństwa w urządzeniu współdzielonym do kilku F-CPU, należy najpierw pobrać konfigurację sprzętową wszystkich odnośnych F-CPU, nim przypisze się adresy PROFIsafe.

Podczas przypisywania należy mieć na uwadze następuje zagadnienia:

Jeśli odnośny moduł interfejsu nie jest przypisany do odpowiedniego CPU, urządzenie programistyczne oraz urządzenie współdzielone muszą znajdować się w tej samej podsieci. W przeciwnym razie należy wykonać procedurę opisaną w działach Identyfikacja modułów bezpieczeństwa (strona 72) oraz Przypisywanie adresów PROFIsafe (strona 74).

Zobacz także

Konfiguracja współdzielonego urządzenia (strona 61)

2.13.4 Zmiana adresu PROFIsafe

Zmiana adresu PROFIsafe

Uwaga

Należy pamiętać, że po zmianie adresu PROFIsafe dla F-I/O należy również wykonać akceptację (strona 383), obejmującą kontrolę zmiany (strona 396) dla podsumowania bezpieczeństwa (strona 357).

1. Zmienić adres PROFIsafe (adres docelowy bezpieczeństwa, adres źródłowy bezpieczeństwa) w konfiguracji sprzętowej.
2. Skompilować konfigurację sprzętową.
3. Pobrać konfigurację sprzętową do F-CPU.
4. Wybrać „Assign PROFIsafe address" (Przypisz adres PROFIsafe) w menu skrótów.
5. Postępować zgodnie opisem w dziale Identyfikacja modułów bezpieczeństwa (strona 72) oraz Przypisywanie adresów PROFIsafe (strona 74).

2.14 Specjalne przypadki konfiguracji urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O

Wymogi

Aby użyć urządzenia podrzędnego DP opartego na GSD typu fail-safe w SIMATIC Safety, urządzenia podrzędne oparte na GSD muszą być obsługiwane na PROFIBUS DP i obsługiwać profil magistrali PROFIsafe. W przypadku wykorzystania wraz z F-CPU S7-1200/1500, muszą obsługiwać profil magistrali PROFIsafe w trybie V2.

Urządzenia podrzędne DP oparte na GSD typu fail-safe stosowane w konfiguracjach hybrydowych na PROFIBUS DP oraz PROFINET IO poniżej połączenia IE/PB muszą obsługiwać profil magistrali PROFIsafe w trybie V2.

Aby użyć urządzenia I/O opartego na GSD typu fail-safe w SIMATIC Safety, urządzenia oparte na GSD muszą być obsługiwane na PROFINET IO i obsługiwać profil magistrali PROFIsafe w trybie V2.

Konfiguracja z plikami GSD

Tak jak w przypadku standardowego systemu, podstawę konfiguracji urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O stanowi specyfikacja urządzenia w pliku GSD (plik główny urządzenia).

Plik GSD zawiera wszystkie właściwości urządzenia podrzędnego DP opartego na GSD lub urządzenia I/O opartego na GSD. W przypadku urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD typu fail-safe, niektóre części są chronione przez CRC.

Pliki GSD są dostarczane przez producentów urządzeń.

Ochrona struktury danych urządzenia w plikach GSD

Jedynie obsługiwane pliki GSD to te, które spełniają wymogi ochrony zdefiniowane w *Specyfikacji PROFIsafe* V2.0 przy użyciu CRC zapisanego w tym pliku („setpoint" dla F_IO_StructureDescCRC).

Struktura danych opisana w pliku GSD jest sprawdzana podczas dodawania F-I/O do konfiguracji sprzętowej oraz podczas jej kompilowania. W przypadku wykrycia błędu należy określić, czy plik GSD dostarczony przez producenta urządzenia zawiera nastawę dla F_IO_StructureDescCRC.

Przypisanie i ustawienie adresów PROFIsafe

OSTRZEŻENIE

Należy sprawdzić dokumentację urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD typu fail-safe, aby określić ważny typ adresu PROFIsafe. W przypadku braku niezbędnych informacji, należy przyjąć typ adresu PROFIsafe 1. Należy postępować zgodnie z opisem w dziale Adresy PROFIsafe do F-I/O typu adresowania PROFIsafe 1 (strona 66) lub Adresy PROFIsafe do F- I/O typu adresowania PROFIsafe 2 (strona 68).

Należy ustawić adres źródłowy bezpieczeństwa dla urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD typu fail-safe zgodnie ze specyfikacją producenta. Jeśli adres źródłowy bezpieczeństwa musi odpowiadać parametrowi „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) dla F-CPU (typ adresu PROFIsafe 2), można znaleźć go w zakładce „Properties" (Właściwości) F-CPU. W takim przypadku należy również sprawdzić w podsumowaniu bezpieczeństwa, czy wartość F-CPU dla parametru „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) jest zgodny z wartością adresu źródłowego bezpieczeństwa dla urządzenia podrzędnego DP opartego na GSD typu fail-safe/urządzenia I/O opartego na GSD typu fail-safe. *(S053)*

Procedura konfiguracji z plikami GSD

Pliki GSD importuje się do projektu (patrz *Pomoc do STEP 7 „Pliki GSD"*).

1. Należy wybrać urządzenie podrzędne DP oparte na GSD typu fail-safe/urządzenie I/O oparte na GSD typu fail-safe w karcie zadania „Hardware catalog" (Katalog sprzętowy) i podłączyć je do odnośnej podsieci w widoku sieci.
2. Należy wybrać urządzenie podrzędne DP oparte na GSD typu fail-safe/urządzenie I/O oparte na GSD typu fail-safe, po czym wstawić wymagane moduły bezpieczeństwa, jeśli nie nastąpiło to automatycznie.
3. Należy wybrać odnośny moduł bezpieczeństwa i otworzyć zakładkę „Properties" (Właściwości) w oknie nadzoru.

W przypadku urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD (w przeciwieństwie do innych F-I/O), parametr „Manual assignment of F-monitoring time" (Ręczne przypisanie czasu monitorowania bezpieczeństwa) jest włączony. Skutkuje to tym, że wartość określona w pliku GSD dla czasu monitorowania bezpieczeństwa jest stosowana jako wartość domyślna w przypadku podłączenia urządzeń/urządzeń podrzędnych. Obie wartości (czas oraz rodzaj przypisania) można później zmienić ręcznie.

Parametr bezpieczeństwa „F_CRC_Seed" oraz „F_Passivation" do urządzeń I/O opartych na GSD typu fail-safe

Parametry bezpieczeństwa „F_CRC_Seed" oraz „F_Passivation" wpływają na zachowanie urządzenia I/O opartego na GSD typu fail-safe. Nie jest możliwe ustawienie połączenia parametrów bezpieczeństw lecz określa się je poprzez wybranie odpowiedniego modułu bezpieczeństwa. Możliwe jest użycie do trzech wariantów modułu, zależnie od zastosowanego F-CPU S7-300/400 lub S7-1200/1500.

Wariant modułu bezpieczeństwa	F_CRC_Seed	F_Passivation	Zachowanie urządzenia I/O opartego na GSD typu fail-safe	Możliwość stosowania z F-CPU
1	Parametr nie istnieje	Parametr nie istnieje	Urządzenie I/O oparte na GSD działa z protokołem Basic Protocol (BP) z PROFIsafe. Profil „RIOforFA-Safety" nie jest obsługiwany.	S7-300/400/1200/1500* 0*
2	CRC-Seed24/32	Urządzenie/moduł	Urządzenie I/O oparte na GSD działa z protokołem Expanded Protocol (XP) z PROFIsafe. Profil „RIOforFA-Safety" nie jest obsługiwany.	S7-1200/1500
3	CRC-Seed24/32	Grupa	Urządzenie I/O oparte na GSD działa z protokołem Expanded Protocol (XP) z PROFIsafe. Profil „RIOforFA-Safety" jest obsługiwany.	S7-1200/1500

* Jeśli moduły bezpieczeństwa wariancie 2 lub 3 nie są dostępne, należy użyć modułu w wariancie 1 z F-CPU S7-1200/1500.

Informacje dodatkowe

Opis parametrów można znaleźć w pomocy urządzenia podrzędne DP oparte na GSD typu fail-safe oraz urządzeń I/O opartych na GSD.

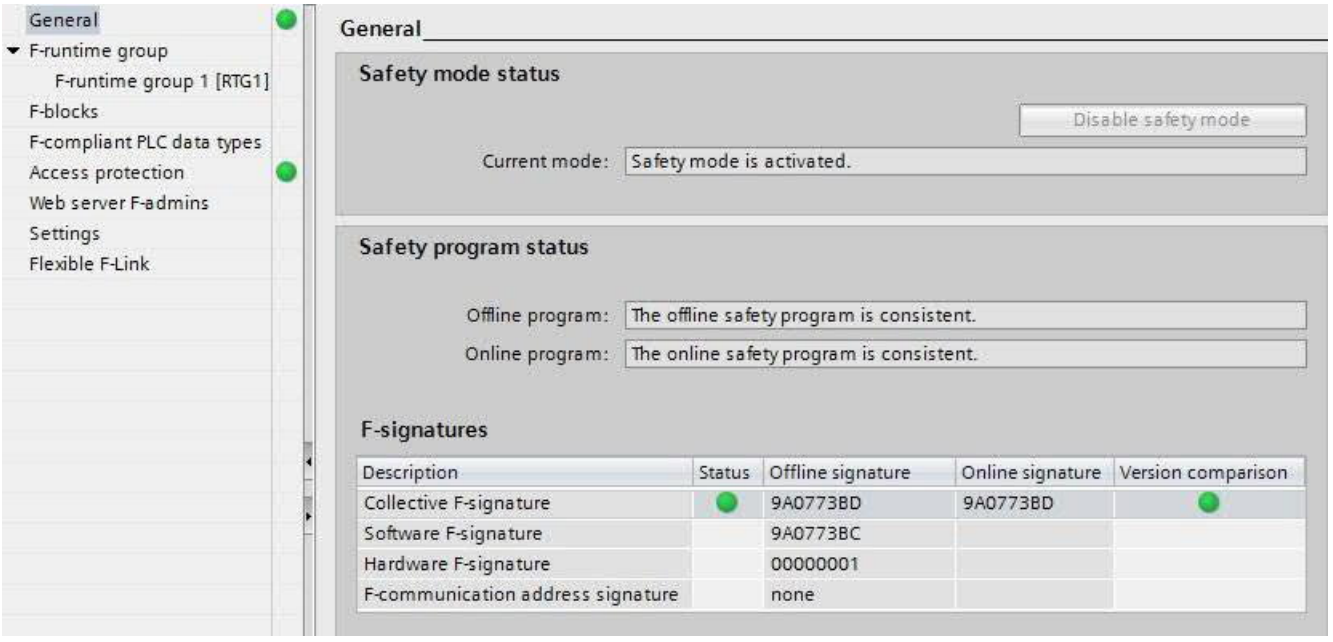
Safety Administration Editor

3

Przegląd

Safety Administration Editor ułatwia pracę w następujący sposób:

- Wyświetlanie statusu programu bezpieczeństwa
- Wyświetlanie zbiorczego podpisu bezpieczeństwa
- (S7-1200, S7-1500) Zbiorczy podpis F-SW
- (S7-1200, S7-1500) Zbiorczy podpis F-HW
- Wyświetlanie statusu trybu bezpieczeństwa
- Tworzenie i zarządzanie grupami F-runtime
- Wyświetlanie informacji o blokach bezpieczeństwa
- Wyświetlanie informacji o rodzajach danych PLC zgodnych z bezpieczeństwem (UDT)
- Informacje dla użytkowników z zezwoleniem administratora bezpieczeństwa
- Określanie/zmiana ochrony dostępu
- Ustawianie/modyfikacja ustawień programu bezpieczeństwa, np. włączanie historii zmian bezpieczeństwa
- (S7-1200, S7-1500) Tworzenie/wyświetlanie/usuwanie komunikacji bezpieczeństwa poprzez Flexible F-Link



Safety Administration Editor dzieli się na następujące obszary:

- Ogólny

  W obszarze „General" (Ogólny), wyświetlane są status trybu bezpieczeństwa, program bezpieczeństwa, zbiorczy podpis bezpieczeństwa, a także, dla F-CPU S7-1200/1500, zbiorczy podpis F-SW oraz zbiorczy podpis F-HW. Dodatkowe informacje dotyczące obszaru „Ogólny" można znaleźć w dziale Obszar „Ogólny" (strona 82).

- Grupa F-runtime

  W obszarze „F-runtime group" (Grupa F-runtime) definiuje się bloki oraz właściwości F-runtime.

  Więcej informacji o grupach F-runtime można znaleźć w dziale Obszar „Grupa F-runtime" (strona 85).

- Bloki bezpieczeństwa

  W obszarze „F-blocks" (Bloki bezpieczeństwa) znajdują się informacje dotyczące bloków bezpieczeństwa zastosowanych w programie oraz ich właściwości. Dodatkowe informacje dotyczące obszaru „Bloki bezpieczeństwa" można znaleźć w dziale Obszar „Bloki bezpieczeństwa" (strona 88).

- Rodzaje danych PLC zgodne z bezpieczeństwem

  W obszarze „F-compliant PLC data types" (Rodzaje danych PLC zgodne z bezpieczeństwem) znajdują się informacje o utworzonych danych PLC zgodnych z bezpieczeństwem (UDT). Wskazuje również, czy rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) jest używany w programie bezpieczeństwa. Dodatkowe informacje dotyczące „Rodzajów danych PLC zgodnych z bezpieczeństwem" można znaleźć w dziale Obszar „Rodzaje danych PLC zgodne z bezpieczeństwem" (S7-1200, S7-1500) (strona 89).

- Ochrona dostępu

  W obszarze „Access protection" (Ochrona dostępu) można ustawić, zmienić lub usunąć hasło do programu bezpieczeństwa. Ochrona dostępu jest obowiązkowa w działaniu produkcyjnym. Dodatkowe informacje dotyczące ochrony dostępu można znaleźć w dziale „Ochrona dostępu do danych projektowych związanych z bezpieczeństwem" (strona 106).

- Administratorzy bezpieczeństwa serwera sieciowego

  W obszarze „Web server F-admins" (Administratorzy bezpieczeństwa serwera sieciowego) można uzyskać informacje o użytkownikach z atrybutem administratora bezpieczeństwa dla serwera sieciowego F-CPU. Dodatkowe informacje dotyczące obszaru „Administratorzy bezpieczeństwa serwera sieciowego" można znaleźć w dziale Obszar „Administratorzy bezpieczeństwa serwera sieciowego" (S7-1200, S7-1500) (strona 90).

- Ustawienia

  W obszarze „Settings" (Ustawienia) można wprowadzić parametry programu bezpieczeństwa. Informacje dotyczące ustawień programu bezpieczeństwa można znaleźć w dziale Obszar „Ustawienia" (strona 91).

- Flexible F-Link

  W obszarze „Flexible F-Link" dostępne są informacje dotyczące skonfigurowanej komunikacji bezpieczeństwa poprzez Flexible F-Links, przedstawione w formie tabelarycznej. Informacje dotyczące tego tematu można znaleźć w dziale Obszar „Flexible F-Link" (S7-1200, S7-1500) (strona 98).

Zobacz także

Struktura programu bezpieczeństwa (S7-1200, S7-1500) (strona 117)

Struktura programu bezpieczeństwa (S7-300, S7-400) (strona 115)

Definiowanie grup F-runtime (strona 139)

3.1 Otwieranie Safety Administration Editor

Wymogi

Safety Administration Editor jest widoczny jako element w drzewku projektu, jeśli skonfigurowano w projekcie CPU jako F-CPU, co oznacza zaznaczenie opcji „F-capability activated" (Funkcjonalność bezpieczeństwa włączona) (we właściwościach F-CPU).

Procedura

Aby otworzyć *Safety Administration Editor*, należy wykonać poniższe kroki:

1. Otworzyć folder F-CPU w drzewku projektu.
2. Kliknąć dwukrotnie na „Safety administration" (Administrator bezpieczeństwa) lub kliknąć prawym przyciskiem i wybrać odnośne menu dla *Safety Administration Editor*.

Wynik

Safety Administration Editor dla F-CPU otworzy się w obszarze roboczym.

3.2 Obszar „Ogólny"

„Status trybu bezpieczeństwa"

„Safety mode status" (Status trybu bezpieczeństwa) przedstawia bieżący stan trybu bezpieczeństwa. Wymogiem jest istniejące połączenie online z wybranym F-CPU.

Możliwe są następujące stany:

- „Safety mode is activated" (Tryb bezpieczeństwa aktywny)
- „The safety mode is not activated"(Tryb bezpieczeństwa nie jest aktywny)
- „F-CPU is in STOP" (F-CPU jest w trybie STOP)
- „No active F-CPU available" (Brak dostępnego F-CPU)

„Wyłącz tryb bezpieczeństwa"

Przy istniejącym połączeniu online i aktywnej obłudze trybu bezpieczeństwa, istnieje możliwość użycia przycisku „Disable safety mode" (Wyłącz tryb bezpieczeństwa) w celu wyłączenia trybu bezpieczeństwa dla wybranego F-CPU. Tryb bezpieczeństwa można wyłączyć jedynie dla całego programu bezpieczeństwa, a nie dla poszczególnych grup F-runtime.

Więcej informacji można znaleźć w dziale „Wyłączanie trybu bezpieczeństwa" (strona 360).

„Status programu bezpieczeństwa"

„Safety program status" (Status programu bezpieczeństwa) wyświetla bieżący stan programu online i offline.

- Consistent (Spójny) (wraz z informacjami, jeśli nie ustawiono hasła.)
- Inconsistent (Niespójny)
- Modified (Zmodyfikowany)

Jeśli nie można nawiązać połączenia z programem online, pojawi się komunikat „No online connection)" (Brak połączenia online).

„Podpisy bezpieczeństwa”

Dla nieistniejącego połączenia online

Pod opcją „F-signatures” (Podpisy bezpieczeństwa) wyświetlanych jest wiele podpisów. Każdy podpis jest utworzony z innych części danych projektu typu fail-safe.

- Zbiorczy podpis bezpieczeństwa: Ten podpis zmienia się z każdą zmianą danych projektu typu fail-safe. Zawiera podpisy opisane poniżej:
- Podpis zbiorczy F-SW (S7-1200/1500): Ten podpis zmienia się z każdą zmianą programu bezpieczeństwa.
- Podpis zbiorczy F-HW (S7-1200/1500): Ten podpis zmienia się z każdą zmianą konfiguracji sprzętowej typu fail-safe.
- Podpis adresowy komunikacji bezpieczeństwa (S7-1200/1500): Ten podpis zmienia się z każdą zmianą nazwy komunikacji bezpieczeństwa UUID dla połączeń komunikacyjnych z flexible F-Link.

Czas ostatniego procesu kompilacji jest wyświetlany dla zbiorczego podpisu bezpieczeństwa w kolumnie „Time stamp” (Tag czasowy).

Dla istniejącego połączenia online

Dla istniejącego połączenia online, w dziale „Program signature” (Podpis programu)

- Status programu

Status	Znaczenie
	Zbiorcze podpisy bezpieczeństwa online i offline są zgodne, a do programów bezpieczeństwa online i offline przypisano hasło.
	Zbiorcze podpisy bezpieczeństwa online i offline *nie* są zgodne lub nie przypisano hasła do jednego z programów bezpieczeństwa.
—	Nie można określić statusu programu bezpieczeństwa.

- Zbiorcze podpisy bezpieczeństwa online i offline
- Gdy zbiorcze podpisy bezpieczeństwa są zgodne: Informacja o tym, czy wersje bloków bezpieczeństwa są spójne online i offline.

Status	Porównanie wersji	Komunikat
	Nieistotne	Zbiorcze podpisy bezpieczeństwa online i offline *nie* są ze sobą zgodne.
		Zbiorcze podpisy bezpieczeństwa online i offline są zgodne, lecz wersje online bloków bezpieczeństwa różnią się od wersji offline.
		Zbiorcze podpisy bezpieczeństwa online i offline są zgodne, online i offline są wykorzystywane identyczne wersje bloków bezpieczeństwa.
Nieistotne	—	Nie można określić wersji systemu bezpieczeństwa.

Dodatkowe informacje dotyczące spójności programu bezpieczeństwa online można znaleźć w dziale „Identyfikacja programu online i offline” (strona 393).

Zobacz także

Identyfikacja programu (strona 352)

3.3 Obszar „grupa F-runtime"

3.3.1 Obszar „grupa F-runtime"

Program bezpieczeństwa składa się z jednej lub dwóch grup F-runtime.

Ogólne informacje dotyczące grup F-runtime można znaleźć w dziale „Struktura programu bezpieczeństwa (S7-300, S7-400) (strona 115)" oraz w „Struktura programu bezpieczeństwa (S7-1200, S7-1500) (strona 117)".

Więcej informacji o tworzeniu grup F-runtime można znaleźć w dziale „Definiowanie grup F-runtime (strona 139)

(S7-1200, S7-1500) „Tworzenie globalnego bloku stanu F-I/O"

Możliwe jest utworzenie standardowego bloku (FB) o nazwie „RTGx_GLOB_FIO_STATUS", który ocenia, czy zamiast wartości procesowych podawane są wartości zastępcze dla co najmniej jednego F- I/O lub co najmniej jednego kanału F-I/O z grupy F-runtime x. Wynik oceny jest dostępny na wyjściu „QSTATUS". F-I/O wyłączony za pomocą zmiennej „DISABLE" w bloku danych F-I/O jest wtedy ignorowany.

Wyjście „RIOforFA_VALUE_STATUS" odpowiada wyjściu „QSTATUS", lecz uwzględnia jedynie F-I/O z profilem „RIOforFA-Safety".

Aby wygenerować taki standardowy FB, należy nacisnąć przycisk „Create global F-I/O status block" (Utwórz globalny blok stanu F-I/O). Standardowy FB można utworzyć jedynie, gdy program bezpieczeństwa został skompilowany. Standardowy FB można wywołać w dowolnym miejscu standardowego programu użytkownika.

Uwaga

Dodając lub usuwając F-I/O, należy ponownie wygenerować „RTGx_GLOB_FIO_STATUS".

Zobacz także

Dane procesowe lub wartości fail-safe (strona 172)

3.3.2 Przetwarzanie wstępne/końcowe (S7-1200, S7-1500)

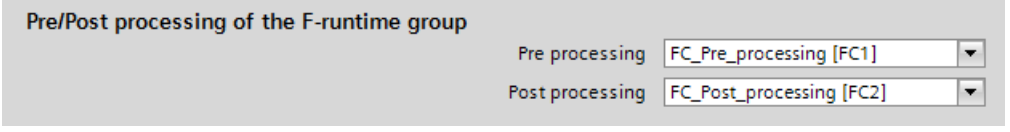
Podczas przetwarzania wstępnego i końcowego dostępna jest opcja wywołania standardowych bloków (FC) bezpośrednio przed lub za grupą F-runtime, na przykład do transferu danych komunikacji typu fail-safe poprzez Flexible F-Link (strona 312).

Wymogi

- Używane jedynie standardowe FC.
- W interfejsie bloku standardowego FC dozwolone są jedynie tymczasowe dane lokalne i stałe.

Procedura

1. Utworzyć standardowe FC do przetwarzania wstępnego i końcowego.
2. Przypisać standardowe FC w Safety Administration Editor w opcji „Pre-/postprocessing of the F-runtime group" (Przetwarzanie wstępne/końcowe grupy F-runtime).



Uwaga

W przypadku usunięcia przypisanego FC lub nadpisania go poprzez skopiowanie, jego wybór jako bloku przetwarzania wstępnego/końcowego jest automatycznie resetowany.

Wpływ na program

- Czas pracy grupy F-runtime jest wydłużany przez czas pracy standardowych FC do przetwarzania wstępnego/końcowego (wpływ na TRTG_CURR oraz TRTG_LONG w DB informacji o grupie F-runtime).
- Ze względu na to, że przetwarzanie wstępne/końcowe nie zmienia funkcjonalności programu bezpieczeństwa, zbiorczy podpis bezpieczeństwa pozostaje niezmieniony po kompilacji.

Przebieg wczytywania

Wywołania wybranych standardowych FC są umieszczane podczas kompilowania lub po wywołaniu głównego bloku bezpieczeństwa w F-OB.

Oznacza to, podczas kolejnego pobrania wymagany jest stan operacyjny STOP.

Zmiany treści wybranych standardowych FC mogą odbywać się w trybie RUN.

Wyjątek stanowią zmiany nazwy bloku oraz jego numeru, co również obejmuje kompilację programu bezpieczeństwa.

Gdy blok przetwarzania wstępnego/końcowego zostanie wgrany indywidualnie przez F-CPU, nie jest automatycznie łączony z grupą F-runtime w Safety Administration Editor.

Jeśli zamiast tego wykona się spójne wczytanie F-CPU do PG/PC, ustawienia przetwarzania wstępnego i końcowego są wgrywane zgodnie z CPU online.

3.4 Obszar „bloki bezpieczeństwa"

Przegląd

Obszar "bloki bezpieczeństwa" pomaga w następujących zadaniach:

- Wyświetlanie bloków bezpieczeństwa użytych w programie bezpieczeństwa.
- Wyświetlanie bloków bezpieczeństwa użytych w grupach F-runtime.
- Wyświetlanie dodatkowych informacji o blokach bezpieczeństwa.

Opis bloków bezpieczeństwa znajduje się w dziale „Tworzenie bloków bezpieczeństwa w FBD / LAD" (strona 160).

Wyświetlane informacje

W trybie offline bloków bezpieczeństwa wyświetlane są następujące informacje:

- Czy blok bezpieczeństwa został skompilowany i użyty?
- Funkcja bloku bezpieczeństwa w programie bezpieczeństwa
- Podpis bloku
- Znacznik czasowy ostatniej zmiany

W trybie online bloków bezpieczeństwa wyświetlane są następujące informacje:

- Status (czy blok ma taki sam znacznik czasowy w trybie online i offline)
- Funkcja bloku bezpieczeństwa w programie bezpieczeństwa
- Podpis bloku dla bloku offline
- Podpis bloku dla bloku online

Bloki bezpieczeństwa są wyświetlanie hierarchicznie, jak w folderze „Program blocks".

Opis symboli w kolumnie „Status" można znaleźć w dziale „Porównywanie programów bezpieczeństwa" (strona 354).

Uwaga

Podczas porównania offline-online, stany porównania mogą czasem różnić się pomiędzy *edytorem porównania* a stanem wyświetlanym w *Safety Administration Editor*. Decydujący status to wynik porównania w *edytorze porównania*, ponieważ jest to jedyne porównanie uwzględniające zawartość bloków bezpieczeństwa.

Funkcja filtra

Przy pomocy funkcji filtra można wybrać, czy mają być przeglądane wszystkie bloki bezpieczeństwa, określone grupy F-runtime czy też cały program bezpieczeństwa.

- Należy wybrać z rozwijanej listy „All F-blocks" (Wszystkie bloki bezpieczeństwa), by przeglądać wszystkie bloki.
- Należy wybrać z rozwijanej listy „F-runtime group" (Grupa F-runtime), by przeglądać wszystkie bloki tej grupy F-runtime.

3.5 Obszar „Rodzaje danych PLC zgodnych z bezpieczeństwem" (S7-1200, S7-1500)

Przegląd

W obszarze „F-compliant PLC data types" (Rodzaje danych PLC zgodne z bezpieczeństwem) znajdują się informacje o zdefiniowanych danych PLC zgodnych z bezpieczeństwem (UDT).

Istnieje możliwość usunięcia rodzaju danych PLC zgodne z bezpieczeństwem (UDT) z menu skrótowego.

Wyświetlane informacje

Dla rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) w trybie offline wyświetlane są następujące informacje:

- Czy rodzaj danych PLC zgodnych z bezpieczeństwem jest używany w programie bezpieczeństwa?
- Znacznik czasowy ostatniej zmiany.

Dla rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) w trybie online wyświetlane są następujące informacje:

- Status (czy rodzaje danych PLC zgodnych z bezpieczeństwem (UDT) mają ten sam znacznik czasowy w trybie offline i online)

Rodzaje danych PLC zgodne z bezpieczeństwem (IDT) są wyświetlanie hierarchicznie, tak jak w folderze „PLC Data Types".

Uwaga

Podczas porównania offline-online, statusy w *edytorze porównania* oraz w *Safety Administration Editor* mogą się różnić pod kilkoma względami. Wynik porównania w *edytorze porównania* jest decyzyjny, ponieważ jest to jedyne porównanie, które uwzględnia zawartość rodzaju danych PLC zgodnych z bezpieczeństwem (UDT).

3.6 Obszar „Administratorzy bezpieczeństwa serwera sieciowego (S7-1200, S7-1500)

Do przywrócenia kopii zapasowej (strona 342) poprzez serwer sieciowy F-CPU wymagane są prawa "administratora bezpieczeństwa". Prawa "administratora bezpieczeństwa" przypisuje się w konfiguracji sprzętowej F-CPU w opcjach zarządzania użytkownikami serwera sieciowego.

W tym dziale można uzyskać informacje dotyczące tego, którzy użytkownicy mają prawa "administrator bezpieczeństwa" online lub offline do F-CPU, które obsługują tego typu prawa. Pozwala on na sprawdzenie, czy zmiana w prawach „F-admin" (administrator bezpieczeństwa) są aktywne w F-CPU. Aby zastosować zmiany w prawach „administratora bezpieczeństwa", konieczne jest wczytanie konfiguracji do F-CPU.

Zobacz także

Kompletność i poprawność konfiguracji sprzętowej (strona 383)

3.7 Obszar „Ustawienia"

„Zakresy liczbowe generowanych bloków systemu bezpieczeństwa"

Wyznaczone tutaj zakresy liczbowe są wykorzystywane przez system bezpieczeństwa do nowych, automatycznie generowanych bloków bezpieczeństwa.

W tym miejscu można wybrać, czy zakresy numeryczne są zarządzane przez system bezpieczeństwa lub wykorzystywane są określone zakresy.

- „F-system managed" (Zarządzane przez system bezpieczeństwa)

  Zakresy numeryczne są zarządzane automatycznie przez system bezpieczeństwa, zależnie od stosowanego F-CPU. System bezpieczeństwa wybiera dostępny zakres numeryczny. Wyświetlane są wartości początkowe i końcowe zakresów.

- „Fixed range" (Stały zakres)

  Możliwy jest wybór wartości początkowej i końcowej zakresów z dostępnej puli. Dostępny zakres zależy od stosowanego F-CPU.

  Niepoprawny wybór jest wskazywany komunikatem błędu.

  Jedyna kontrola wykonywana podczas konfiguracji obejmuje sprawdzenie, czy dolny limit jest mniejszy bądź równy górnemu limitowi oraz czy znajduje się w dostępnym zakresie F-CPU. Kontrola mająca na celu określenie, czy skonfigurowany zakres jest wystarczający, jest wykonywana podczas kompilacji. Należy zapewnić wystarczająco duży zakres. Gdy dostępny zakres jest niewystarczający, wystąpi błąd kompilacji. Nie zostaną wygenerowane wszystkie bloki, a program bezpieczeństwa nie będzie wykonywalny.

Zmiany zyskają ważność dopiero podczas następnej kompilacji. Podczas kompilacji można przenieść automatycznie utworzone bloki bezpieczeństwa do nowego obszaru. Wyjątek stanowią DB do F-I/O. Zawsze utrzymują swój oryginalny numer, który można zmienić we właściwościach F-I/O.

„Wersja systemu bezpieczeństwa"

Ten parametr służy do określania wersji systemu bezpieczeństwa (w tym wersji systemowych bloków bezpieczeństwa oraz automatycznie generowanych bloków bezpieczeństwa; patrz „Omówienie programowania" (strona 114)).

Dostępnych jest kilka wersji:

Wersja [3]	S7-300/400	S7-1200	S7-1500	Funkcja
1,6	—	x	x	Wersje te mają identyczne funkcje.
2,0	x	x[1]	x[2]	Zależnie od ustawionej wersji, wynikiem mogą być różne czasy działania grup(y) F-runtime (patrz arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
2.1	—	x[1]	x[2]	Dodatkowo obsługuje zmienne „DISABLE" oraz „DISABLED" w DB F-I/O
2.2	—	x[1]	x[2]	Obsługuje komunikację CPU safety – CPU oraz komunikację grupy F-runtime poprzez Flexible F-Link.
2.3	—	x[1]	x[2]	Ta wersja ma identyczne funkcje jak wersja 2.2.

1 obsługiwane dla wersji oprogramowania V4.2

2 i wyższej obsługiwane dla wersji

3 oprogramowania V2.0 i wyższej

Po wykonaniu migracji projektów utworzonych w *S7 Distributed Safety V5.4 SP5*, automatycznie ustawiana jest wersja 1.0, by zidentyfikować migrowane projekty, który nie zostały jeszcze skompilowane przy pomocy *STEP 7 Safety Advanced*.

Zazwyczaj nie trzeba wprowadzać żadnych ustawień dla tych parametrów.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępnawersja.

„Dane lokalne wykorzystywane w programie bezpieczeństwa" (S7-300, S7-400)

Ten parametr pozwala na określenie wielkości tymczasowych danych lokalnych (w bajtach), jaka dostępna jest do hierarchii wywołania poniżej głównego bloku bezpieczeństwa.

Ustawienia dotyczą wszystkich grup F-runtime programu bezpieczeństwa. Dodatkowe informacje dotyczące grup F-runtime można znaleźć w dziale „Struktura programu bezpieczeństwa (S7-1200, S7-1500) (strona 117)" oraz w „Struktura programu bezpieczeństwa (S7-300, S7-400) (strona 115)":

Minimalna możliwa wielkość jest określona przez wymogi danych lokalnych bloków bezpieczeństwa wygenerowanych automatycznie podczas kompilacji programu bezpieczeństwa.

Z tego względu należy zapewnić co najmniej 440 bajtów. Jednakże, wymogi dla danych lokalnych do automatycznie dodanych bloków bezpieczeństwa mogą być wyższe, zależnie od wymogów danych lokalnych bloków bezpieczeństwa utworzonych w FBD lub LAD.

Dlatego też należy zapewnić możliwie jak najwięcej przestrzeni na dane lokalne. Jeśli brak jest wystarczającej ilości danych lokalnych dla automatycznie dodanych bloków bezpieczeństwa (440 bajtów lub więcej), program bezpieczeństwa zostanie skompilowany mimo to.

Dane w automatycznie dodanych F-DB są następnie wykorzystywane zamiast danych lokalnych. Zwiększa to jednakże czas pracy grup(y) F-runtime. Jeśli wymagane jest więcej danych lokalnych niż skonfigurowano, pojawi się powiadomienie.

OSTRZEŻENIE

Maksymalny czas pracy grupy F-runtime obliczony przy pomocy arkusza kalkulacyjnego do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100) nie jest w tym przypadku dłużej poprawny, ponieważ obliczenie przyjmuje wystarczającą dostępność lokalnych danych bezpieczeństwa.

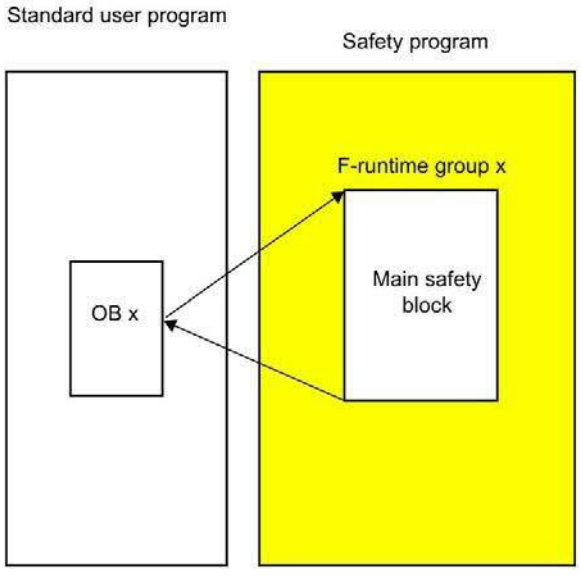
W takim przypadku należy użyć wartości skonfigurowanej dla maksymalnego czasu cyklu grupy F-runtime (czas monitorowania bezpieczeństwa) jako maksymalnego czasu pracy grupy F-runtime podczas obliczania maksymalnych czasów odpowiedzi w razie błędu oraz dla czasów pracy standardowego systemu przy pomocy wspomnianego arkusza kalkulacyjnego. *(S004)*

Maksymalna możliwa wielkość zależy od:

- Wymogi dla danych lokalnych głównego bloku bezpieczeństwa oraz standardowego programu użytkownika wyższego poziomu. Z tego względu należy wywołać główny blok bezpośrednio w OB (OB przerwania cyklicznego, tam, gdzie to możliwe), a dodatkowe dane lokalny nie powinny być deklarowane w tych OB przerwań cyklicznych.
- Maksymalna objętość danych lokalnych używanego F-CPU (patrz „Specyfikacja techniczna" w informacji o produkcie stosowanego F-CPU). W przypadku F-CPU S7-400, można skonfigurować dane lokalne dla każdej klasy pierwszeństwa. Dlatego też należy przypisać największą możliwą objętość danych lokalnych dla klas pierwszeństwa, w których wywoływany jest program bezpieczeństwa (główne bloki bezpieczeństwa) (np. OB 35).

Maksymalna możliwa objętość danych lokalnych jako funkcja wymogów danych lokalnych głównego bloku bezpieczeństwa oraz standardowego programu użytkownika wyższego poziomu (S7-300, S7-400):

Przypadek 1: Główny blok bezpieczeństwa wywoływany bezpośrednio z OB

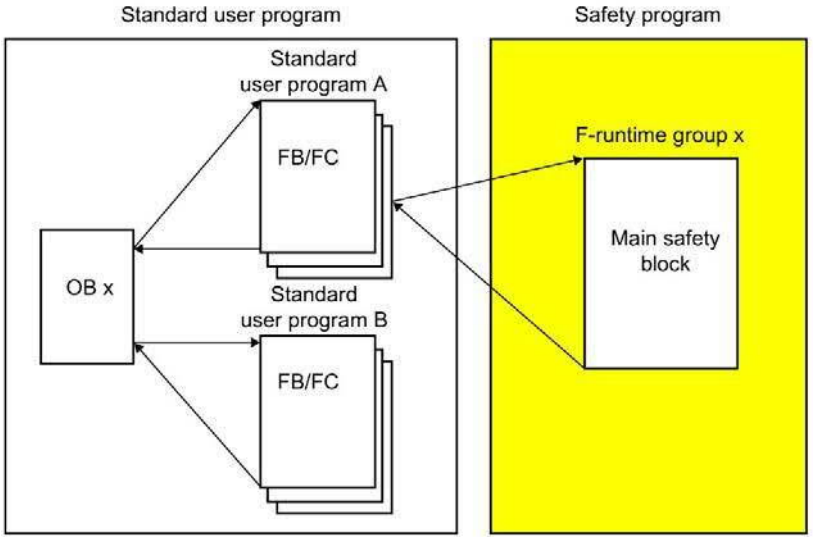


Należy ustawić parametr „Local data used in safety program" (Dane lokalne wykorzystywane w programie bezpieczeństwa) na maksymalną objętość danych zastosowanego F-CPU minus wymóg danych lokalnych głównego bloku bezpieczeństwa (jeśli główny blok bezpieczeństwa obsługuje 2 grupy F-runtime, należy użyć największego wymogu danych) oraz minus wymóg danych lokalnych OBx wywołania (jeśli występują 2 grupy F-runtime, należy użyć OB z największym wymogiem).

Uwaga: Jeśli nie zadeklarowano żadnych tymczasowych danych lokalnych w głównych blokach bezpieczeństwa oraz OBx wywołania, wymóg danych lokalnych głównego bloku bezpieczeństwa to 6 bajtów, zaś wymóg danych dla OBx wywołania to 26 bajtów. Możliwe jest wyprowadzenie wymogów danych lokalnych głównych bloków bezpieczeństwa oraz OBx wywołania ze struktury programu.

Należy wybrać używany F-CPU w drzewku projektu, a następnie „Tools > Call structure" (Narzędzia > Struktura narzędzi). Poniższa tabela zawiera wymogi danych lokalnych w ścieżce lub dla indywidualnych bloków (zobacz również pomoc do *STEP 7*).

Przypadek 2: Główny blok bezpieczeństwa nie jest wywoływany bezpośrednio z OB



Należy ustawić parametr „Local data settings" (Ustawienia danych lokalnych) na wartość obliczoną w przypadku 1, minus wymóg danych lokalnych standardowego programu użytkownika A (jeśli standardowy program użytkownika A ma 2 grupy F-runtime, należy użyć największego wymogu).

Uwaga: Możliwe jest wyprowadzenie wymogów danych lokalnych standardowego programu użytkownika A ze struktury programu.

Należy wybrać używany F-CPU w drzewku projektu, a następnie „Tools > Call structure" (Narzędzia > Struktura narzędzi). Poniższa tabela zawiera wymogi danych lokalnych w ścieżce lub dla indywidualnych bloków (zobacz również pomoc do *STEP 7*).

„Ustawienia zaawansowane"

„Safety mode can be disabled" (Możliwe wyłączenie trybu bezpieczeństwa)

Za pomocą tej opcji można uniemożliwić wyłączenie trybu bezpieczeństwa dla programu bezpieczeństwa.

Po zmianie ustawienia tej opcji konieczna jest ponowna kompilacja programu bezpieczeństwa i pobranie go do F-CPU, by zmiana weszła w życie. Zmienia to zbiorczy podpis bezpieczeństwa: oraz zbiorczy podpis F-SW programu bezpieczeństwa.

Zaleca się, by wyłączyć tę opcję przed rozpoczęciem produkcji oraz przed odbiorem programu bezpieczeństwa, by uniemożliwić niezamierzone wyłączenie trybu bezpieczeństwa.

„Enable F-change history" (Włącz historię zmiany bezpieczeństwa)

Rejestrowanie zmian w programie bezpieczeństwa włącza się za pomocą opcji „Enable F-change history" (Włącz historię zmiany bezpieczeństwa). Więcej informacji można znaleźć w dziale „Historia zmian bezpieczeństwa" (strona 375).

„Enable consistent upload from the F-CPU" (Włącz spójne wczytywanie z F-CPU) (S7-1500)

Opcja ta pozwala na spójne wczytywanie załadowanych danych projektu (w tym dane projektu safety) z F-CPU do PG/PC.

Opcję tę można włączyć jedynie, jeśli F-CPU i jego oprogramowanie obsługują wczytywanie danych projektu (w tym dane projektu safety).

Obsługiwane są F-CPU S7-1500 od wersji oprogramowania V2.1. Sterowniki programowe S7-1500 F nie są obsługiwane.

Przy każdej zmianie tej opcji należy wyczytać dane projektu do F-CPU.

Należy pamiętać, że aktywacja tej opcji wydłuża wczytywanie danych projektu związanych z bezpieczeństwem do F-CPU.

„Activate variable F-communication" (Aktywuj zmienne identyfikatory komunikacji) (S7- 1200, S7-1500)

Po aktywowaniu tej opcji możliwe jest doprowadzenie do wejścia DP_DP_ID instrukcji SENDDP lub RCVDP zmiennych wartości z globalnego F-DB.

⚠ OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie**; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości*** do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** S7-1200/1500: Od wersji V3.0 instrukcji SENDDP i RCVDP, nie jest nawiązywane połączenie na wejściu DP_DP_ID do identyfikatora komunikacji bezpieczeństwa „0".

*** S7-1200/1500: Od wersji V3.0 instrukcji the SENDDP i RCVDP, na wejście DP_DP_ID można również doprowadzać wartości zmienne z globalnego F-DB. W takim przypadku również należy skontrolować podczas odbioru programu bezpieczeństwa, czy zapewniona jest unikalność *przez cały czas*, sprawdzając algorytm do tworzenia wartości zmiennych. Jeśli nie można zagwarantować unikalnego identyfikatora komunikacji bezpieczeństwa podczas uruchomienia programu bezpieczeństwa, ponieważ jest on określany dopiero po uruchomieniu programu, należy upewnić się, że podczas tej fazy wartość na wejściu DP_DP_ID wynosi „0".

„System-generated objects" (Obiekty generowane przez system) (S7-1200, S7-1500)

„Creates F-I/O DBs without prefix" (Tworzy DB F-I/O bez prefiksu)

Po wybraniu tej opcji nazwy DB dla F-I/O (strona 174) są tworzone bez prefiksu.

„Clean up" (Czyszczenie)

Przycisk „Clean up" (Czyszczenie) jest przeznaczony do celów serwisowych i wsparcia, służąc do usuwania wyniku kompilacji fail-safe.

3.8 Obszar „Flexible F-Link" (S7-1200, S7-1500)

W obszarze „Flexible F-Link" tworzy się nowe komunikacje bezpieczeństwa, uzyskuje informacje dotyczące istniejących komunikacji oraz usuwa się je.

Wymogi

- F-CPU S7-1500 z oprogramowaniem V2.0
- F-CPU S7-1200 z oprogramowaniem V4.2
- Wersja systemu bezpieczeństwa od V2.2

Informacje o utworzonej komunikacji bezpieczeństwa

W obszarze „Flexible F-Link" dostępne są informacje dotyczące skonfigurowanej komunikacji bezpieczeństwa, przedstawione w formie tabelarycznej.

- Unikalna nazwa w obrębie CPU dla komunikacji bezpieczeństwa
- Rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) do wysyłania/odbioru danych
- Kierunek komunikacji bezpieczeństwa: Transmitowanie/odbieranie
- Czas monitorowania bezpieczeństwa komunikacji bezpieczeństwa
- Komunikacja bezpieczeństwa UUID
- Tag do danych wysyłanych
- Tag do danych odebranych

Tworzenie komunikacji bezpieczeństwa

1. W pustym wierszu tabeli należy kliknąć na „<Add new>" (Dodaj nowy)
2. Przypisać nazwę do połączenia komunikacji.
3. Wybrać rodzaj danych PLC zgodnych z bezp. (UUID) dla połączenia komunikacji.

   Jeśli jeszcze nie utworzono rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) dla połączenia komunikacji lub wymagane jest utworzenie nowych, należy utworzyć rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) (strona 128) z dowolną strukturą. Należy pamiętać, że rozmiar może wynosić do 100 bajtów.
4. Wybrać kierunek połączenia komunikacji („Send" (Wysyłanie) lub „Receive" (Odbiór)).
5. Wybrać czas monitorowania bezpieczeństwa dla połączenia komunikacji (strona 650).

UUID do komunikacji bezpieczeństwa jest wyświetlany poprzez Flexible F-Link w kolumnie „F communication UUID" (UUID komunikacji bezpieczeństwa). UUID komunikacji bezpieczeństwa zapewnia należytą unikalność ID komunikacji związanej z bezpieczeństwem nawet w poza limitami sieci.

Kolumna „Tag for send data" (Tag do danych wysyłanych) wskazuje nowo utworzony tag do wysyłanych danych DB komunikacji bezpieczeństwa.

Kolumna „Tag for receive data" (Tag do danych odebranych) wskazuje nowo utworzony tag do odebranych danych DB komunikacji bezpieczeństwa.

Nowo utworzony DB komunikacji bezpieczeństwa dla tej komunikacji znajduje się pod ścieżką „Program blocks¥System blocks¥STEP 7 Safety¥F-communication DBs".

Usuwanie komunikacji bezpieczeństwa

1. Należy zaznaczyć cały wiersz i potwierdzić „Delete" (Usuń) w menu skrótów. Jednocześnie można usunąć kilka komunikacji bezpieczeństwa.

Kopiowanie komunikacji bezpieczeństwa

1. Należy zaznaczyć cały wiersz i potwierdzić „Copy" (Kopiuj) w menu skrótów. Jednocześnie można skopiować kilka komunikacji bezpieczeństwa.
2. Za pomocą polecenia „Paste" (Wklej) można wkleić skopiowaną komunikację bezpieczeństwa do tabeli w dowolnej wymaganej ilości. UUID do odnośnej komunikacji bezpieczeństwa jest utrzymywany podczas kopiowania. W razie potrzeby można ponownie wygenerować UUID.

Generowanie nowej komunikacji bezpieczeństwa – UUID

1. Należy zaznaczyć cały wiersz i potwierdzić „Generate UUID" (Wygeneruj UUID) w menu skrótów. Jednocześnie można wygenerować kilka UUID.

Interfejs DB komunikacji bezpieczeństwa do wysyłania

Poniższa tabela przedstawia interfejs bloku danych komunikacji bezpieczeństwa służącego do połączenia komunikacji z kierunkiem „wysyłanie":

Dział	Nazwa	Rodzaj danych	Wartość początkowa	Opis
Wejście	SEND_DATA	Rodzaj danych PLC zgodnych z bezp. (UDT)	Jak dla danych PLC zgodnych z bezp. (UDT).	Dane użytkownika do wysłania:
	ACK_RCV_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	tablica z otrzymanymi nieprzetworzonymi danymi.
Wyjście	ERROR	BOOL	FALSE	Sygnalizuje aktywne błędy komunikacji lub błędy niezatwierdzone po stronie odbiorcy (nie w stanie początkowym). 1=Błąd komunikacji
	ACTIVATE_FV	BOOL	TRUE	Komunikacja pasywowana, w stanie początkowym (przykładowo, odbiornik nie jest aktywny), lub HOST wysyła ACTIVATE_FV. DEVICE wysyła bit stanu: FV_ACTVATED, lecz bez wartości zerowych. 1=Komunikacja wykorzystuje wartości fail-safe
	DIAG	Bajt	16#0	Bity błędu (przekroczenie czasu lub błąd CRC aktywne, bądź błąd komunikacji nie został depasywowany) Bit 3: Polecenie zatwierdzenia aktywne po stronie odbiorcy Bit 4: Wykryto przekroczenie czasu Bit 6: Wykryto błąd CRC
	SEND_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	tablica z otrzymanymi nieprzetworzonymi danymi
	ACK_RCV_LENGTH	UInt	0	Informacja o długości dla ACK_RCV_ARRAY w bajtach
	SEND_LENGTH	UInt	0	Informacja o długości dla SEND_ARRAY w bajtach
InOut	—	—	—	—
Statyczny	—	—	—	—

Interfejs DB komunikacji bezpieczeństwa do odbierania

Poniższa tabela przedstawia interfejs bloku danych komunikacji bezpieczeństwa służącego do połączenia komunikacji z kierunkiem „odbieranie":

Dział	Nazwa	Rodzaj danych	Wartość początkowa	Opis
Wejście	PASS_ON	BOOL	FALSE	Pozwalana pasywację danych wyjściowych (wyjście wartości pasywowania) 1=Aktywuj pasywację
	ACK_REI	BOOL	FALSE	Reintegracja (w przypadku żądania reintegracji) za pomocą zbocza dodatniego 1=Zatwierdzenie reintegracji
	RCV_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	tablica z otrzymanymi nieprzetworzonymi danymi
Wyjście	RCV_DATA	Rodzaj danych PLC zgodnych z bezp. (UDT)	Jak w danych PLC zgodnych z bezp. (UDT).	Dane wyjściowe (PASS_VALUES lub otrzymane dane).
	ERROR	BOOL	FALSE	Sygnalizuje aktywne błędy komunikacji lub błędy niezatwierdzone (nie w stanie początkowym). 1=Błąd komunikacji
	PASS_OUT	BOOL	TRUE	Przy PASS_OUT=1, PASS_VALUES stanowią wyjście. Może przyjąć: ERROR, PASS_ON, przy początkowym uruchomieniu (np. nadawca nie jest uruchomiony) lub ACK_REQ oczekuje (błąd nie został zatwierdzony)
	ACK_REQ	BOOL	FALSE	Wymóg reintegracji (komunikacja stabilna po błędzie, wciąż wyprowadzane są wartości zastępcze) 1=Wymóg zatwierdzenia do reintegracji
	SENDMODE	BOOL	FALSE	MOD_MODE jest aktywny lub komunikacja z PLCSIM Advanced na nadawczym F-CPU 1=F-CPU z nadawcą w wyłączonej bezpiecznej pracy lub przy symulowanym CPU

Dział	Nazwa	Rodzaj danych	Wartość początkowa	Opis
	DIAG	Bajt	16#0	Bity błędów (przekroczenie czasu lub błąd CRC) Bit 0: Wykryto przekroczenie czasu po stronie nadawcy Bit 1: Błąd komunikacji aktywny po stronie nadawcy Bit 2: Wykryto błąd CRC po stronie nadawcy Bit 4: Wykryto przekroczenie czasu po stronie odbiorcy Bit 6: Wykryto błąd CRC po stronie odbiorcy
	ACK_SEND_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	tablica danych nieprzetworzonych do wysłania.
	RCV_LENGTH	UInt	0	Informacja o długości dla RCV_ARRAY w bajtach
	ACK_SEND_LENGTH	UInt	0	Informacja o długości dla ACK_SEND_ARRAY w bajtach
InOut	—	—	—	—
Statyczny	PASS_VALUES	Rodzaj danych PLC zgodnych z bezpieczeństwem (UDT)	Tak jako jak w rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) lub w DB I/O	Pasywacja lub wartości zastępcze

Zobacz także

Flexible F-Link (strona 312)

Komunikacja grupy F-runtime (S7-1200, S7-1500) (strona 154)

Ochrona dostępu

4

Ochrona dostępu jest niezbędna w działaniu produkcyjnym

Ochrona dostępu do systemu bezpieczeństwa SIMATIC Safety jest obowiązkowa w działaniu produkcyjnym.

Brak ochrony dostępu jest wstępnie konieczny do celów testowych, odbioru technicznego itp. Oznacza to, że można wykonywać wszelkie czynności offline i online bez ochrony, tj. bez wpisywania hasła.

⚠OSTRZEŻENIE

Dostęp do systemu bezpieczeństwa SIMATIC Safety bez ochrony jest przeznaczony do celów testowych, odbioru technicznego itp., gdy system nie wykonuje jeszcze operacji produkcyjnej. Należy zagwarantować bezpieczeństwo systemu poprzez inne środki organizacyjne, na przykład, ograniczając dostęp do określonych obszarów.

Przed przejściem do produkcji należy skonfigurować i aktywować ochronę dostępu.

(S005)

4.1 Przegląd ochrony dostępu

Wstęp

Możliwe jest zabezpieczenie dostępu do systemu bezpieczeństwa SIMATIC Safety za pomocą dwóch haseł: jednego do programu bezpieczeństwa oraz drugiego do F-CPU.

Hasło do programu bezpieczeństwa

Hasło do programu bezpieczeństwa jest dostępne w dwóch formach:

- Hasło offline stanowi część programu bezpieczeństwa w projekcie offline na urządzeniu programistycznym lub PC.
- Hasło online stanowi części programu bezpieczeństwa w F-CPU.

Hasło do F-CPU

Ochronę dostępu ustawia się na poziomie F-CPU. To hasło służy również do identyfikacji F-CPU i dlatego musi być unikalne w całej sieci.

Przegląd przypisania hasła i jego podawania

Poniższa tabela stanowi przegląd zezwoleń na dostęp dla F-CPU oraz programu bezpieczeństwa.

W poniższych działach przedstawiono sposób przypisywania haseł oraz ustawiania, zmiany i anulowania zezwolenia na dostęp dla F-CPU oraz programu bezpieczeństwa.

	Hasło do F-CPU	**Hasło do programu bezpieczeństwa**
Przypisanie	W *edytorze sprzętu i sieci*, podczas konfigurowania F-CPU, okno inspekcji w zakładce „Settings" (Ustawienia), pod hasłem „Protection" (Ochrona), odpowiada poziomowi bezpieczeństwa, np. „Write protection for fail-safe blocks" (Ochrona zapisu dla bloków typu fail-safe) (S7-300, S7-400). Należy wybrać poziom co najmniej „Full access (no protection)" (Pełny dostęp (brak ochrony)) dla F-CPU S7-1200/1500 i przypisać hasło dla „Full access incl. fail-safe (no protection)" (Pełen dostęp wraz z fail-safe (brak ochrony)). W przypadku wybrania wyższego poziomu, na przykład w celu zabezpieczenia standardowego programu użytkownika, należy przypisać dodatkowe hasło do opcji „Full access (no protection)" (Pełny dostęp (brak ochrony)).	W *Safety Administration Editor* , po pozycją „Access Protection" (Ochrona dostępu).
Monit	W przypadku braku zezwolenia na dostęp do programu bezpieczeństwa (strona 106): Przykładowo: • Podczas wczytywania kompletnego programu bezpieczeństwa do F-CPU • (S7-300, S7-400) podczas wgrywania konfiguracji sprzętowej do F-CPU • (S7-1200, S7-1500) podczas wgrywania konfiguracji sprzętowej do F-CPU, zawierającej zmiany safety • W przypadku przypisywania adresu PROFIsafe • W przypadku pobrania i usunięcia bloków bezpieczeństwa, które są używane w programie bezpieczeństwa • Wyłączając tryb bezpieczeństwa • Przywracając kopię zapasową dla F-CPU. Wyjątek dla F-CPU S7-1200/1500: Jeśli podczas procesu przywracania nie ulega zmianie program bezpieczeństwa ani hasło F-CPU, nie jest konieczne wpisywanie hasła do F-CPU.	W przypadku przypisania hasła, które nie zostało jeszcze wprowadzone od chwili otwarcia projektu lub w przypadku braku zezwolenia na dostęp do programu bezpieczeństwa (strona 106): **Hasło offline,** np.: • Gdy hasło zostało zmienione • W przypadku modyfikacji programu bezpieczeństwa • W przypadku zmiany i usunięcia grup F-runtime • W przypadku zmiany parametrów związanych z bezpieczeństwem w F-I/O **Hasło online,** np. w przypadku wyłączenia trybu bezpieczeństwa (hasło musi zostać wprowadzone, nawet jeśli zezwolenie na dostęp do programu wciąż obowiązuje)

Ponowna kompilacja programu bezpieczeństwa jest konieczna po zmianie na standardowe DB, do których program ma dostęp odczytu lub zapisu (strona 204). Te standardowe DB nie są zarządzane przez ochronę dostępu do programu bezpieczeństwa.

(S7-300, S7-400) Należy pamiętać, że potrzebne jest również hasło F-CPU, by pobrać zmiany dotyczące bezpieczeństwa do konfiguracji sprzętowej. Dotyczy to również zmian w F-I/O, który nie jest wykorzystywany w programie bezpieczeństwa.

Aby pobrany plik był spójny, należy ponownie skompilować program bezpieczeństwa.

4.2 Ochrona dostępu dla danych projektu związanych z bezpieczeństwem

Ustawianie ochrony dostępu dla danych projektu związanych z bezpieczeństwem

Aby ustawić ochronę dostępu do danych projektu związanych z bezpieczeństwem, należy przypisać hasło do programu bezpieczeństwa. Należy wykonać co następuje:

1. Otworzyć folder F-CPU w drzewku projektu.
2. Wybrać „Safety Administration" (Zarządzanie bezpieczeństwem) i wybrać „Go to access protection" (Przejdź do ochrony dostępu) w menu skrótowym. Można również kliknąć dwukrotnie na „Safety Administration". Otworzy się *Safety Administration Editor* dla F-CPU. Wybrać „Access protection" (Ochrona dostępu) w nawigacji obszaru.
3. W „Offline safety program protection" (Ochrona programu bezpieczeństwa offline) należy kliknąć na „Setup" (Konfiguracja) i wprowadzić hasło (maks. 30 znaków) do programu bezpieczeństwa w odpowiednich polach „New password" (Nowe hasło) oraz „Confirm password" (Potwierdź hasło).
4. Wpisane hasło należy zatwierdzić przyciskiem „OK".

Ustawiono ochronę dostępu do danych projektu związanego z bezpieczeństwem i uzyskano zezwolenie na dostęp do danych projektu.

Uwaga

Nie można oddzielnie zdefiniować hasła online; stosowane jest hasło offline przypisane podczas następnego pobierania. Po zamianie hasła offline, hasła mogą różnić się do czasu następnego pobrania programu bezpieczeństwa do F-CPU.

Podczas wczytywania z urządzenia, hasło offline jest zastępowane hasłem online lub jest usuwane.

Uwaga

Należy korzystać z różnych haseł do F-CPU i programu bezpieczeństwa, by zwiększyć ochronę dostępu.

OSTRZEŻENIE

Jeśli ograniczony dostęp do określonych obszarów nie służy do przyznania dostępu do urządzenia programistycznego lub PC jedynie tym osobom, które są upoważnione do modyfikacji programu bezpieczeństwa, należy zastosować poniższe środki organizacyjne, by zapewnić skuteczność ochrony dostępu dla F-CPU w urządzeniu programistycznym lub PC:

- Jedynie upoważniony personel może mieć dostęp do hasła.
- Upoważniony personel musi jednoznacznie anulować pozwolenie na dostęp do F-CPU przed opuszczenie urządzenia programistycznego lub PC, zamykając *STEP 7* lub poprzez menu „Online > Delete access rights" (Online > Usuń prawa dostępu). Jeśli nie zostało to wdrożone, należy zastosować również wygaszacz ekranu zabezpieczony hasłem dostępnym jedynie dla upoważnionego personelu. *(S006)*

Zmiana hasła dla danych projektu związanych z bezpieczeństwem

Możliwa jest zmiana hasła do danych projektu związanych z bezpieczeństwem, dopóki dostępne są wszystkie niezbędne zezwolenia. Odbywa się to podobnie jak w obszarze „Access protection" (Ochrona dostępu) (poprzez przycisk „Change" (Zmień)) i jest wykonywane jak w systemie Windows, poprzez wprowadzenie starego hasła i dwukrotne wpisanie nowego.

Usuwanie ochrony dostępu dla danych projektu związanych z bezpieczeństwem

Aby usunąć ochronę dostępu do danych projektu związanych z bezpieczeństwem, należy usunąć hasło do programu bezpieczeństwa. Należy wykonać co następuje:

1. Otworzyć folder F-CPU w drzewku projektu.
2. Wybrać „Safety Administration" (Zarządzanie bezpieczeństwem) i wybrać „Go to access protection" (Przejdź do ochrony dostępu) w menu skrótowym. Można również kliknąć dwukrotnie na „Safety Administration". Otworzy się *Safety Administration Editor* dla F-CPU.
3. Wybrać „Access protection" (Ochrona dostępu) w nawigacji obszaru.
4. Kliknąć na przycisk „Change" (Zmień).
5. W polu „Old password" (Stare hasło) należy wprowadzić hasło do programu bezpieczeństwa.
6. Kliknąć „Revoke" (Cofnij), a następnie „OK".

Uzyskiwanie zezwolenia na dostęp poprzez logowanie do programu bezpieczeństwa

Logowanie do programu bezpieczeństwa wykonuje się następująco:

1. Otworzyć folder F-CPU w drzewku projektu.
2. Wybrać „Safety Administration" (Zarządzanie bezpieczeństwem) i wybrać „Go to access protection" (Przejdź do ochrony dostępu) w menu skrótowym.
   Można również kliknąć dwukrotnie na „Safety Administration". Otworzy się *Safety Administration Editor* dla F-CPU.
3. Wybrać „Access protection" (Ochrona dostępu) w nawigacji obszaru.
4. Wprowadzić hasło do programu bezpieczeństwa w polu „Password" (Hasło).
5. Nacisnąć przycisk „Login" (Zaloguj).

Ważność zezwolenia na dostęp dla danych projektu związanych z bezpieczeństwem

Jeśli zezwolenie na dostęp dla danych projektu związanych z bezpieczeństwem uzyskano poprzez wprowadzenie hasła, pozostaje ono aktywne do chwili zamknięcia projektu. W przypadku zamknięcia *STEP 7*, wszelkie wciąż otwarte projekty są automatycznie zamykane, a przyznane zezwolenie na dostęp jest cofane.

Wycofywanie zezwolenia na dostęp poprzez wylogowanie

Zezwolenie na dostęp do danych projektu związanych z bezpieczeństwem można wycofać w następujący sposób:

- Poprzez kliknięcie na przycisk „Log off" (Wyloguj) w obszarze „Access protection" (Ochrona dostępu) w „*Safety Administration Editor*".
- W menu skrótowym do *Safety Administration Editor* (dostęp po kliknięciu prawym przyciskiem myszy).
- Korzystając z symbolu kłódki w linii *Safety Administration Editor*.

Użytkownik zostanie następnie poproszony o wprowadzenie hasła do programu bezpieczeństwa przy wykonywaniu następnej czynności wymagającej hasła. Przejście Stop-Run jest wymagany do „cofnięcia" pozwolenia na dostęp do sterowania.

Pozwolenie na dostęp do danych projektu związanych z bezpieczeństwem jest anulowane automatycznie, jeśli projekt lub *STEP 7* zostały zamknięte.

Wyświetlanie ważności zezwolenia na dostęp

Ważność zezwolenia na dostęp jest wyświetlana w drzewku projektu w następujący sposób:

- Zezwolenie na dostęp jest ważne, jeśli symbol kłódki w linii *Safety Administration Editor* jest otwarty.
- Zezwolenie nie jest dostępne, jeśli symbol przedstawia zamkniętą kłódkę.
- Jeśli nie jest widoczny symbol kłódki, nie zostało przypisane żadne hasło.

4.3 Ochrona dostępu dla F-CPU

Ustawianie ochrony dostępu dla F-CPU

Aby ustawić ochronę dostępu dla F-CPU, należy przypisać hasło do F-CPU w konfiguracji F-CPU.

Bezpośredni dostęp do niej jest możliwy po kliknięciu na link „Go to the "Protection" area of the F-CPU" (Przejdź do obszaru „Ochrona" dla F-CPU) w obszarze „Access protection" (Ochrona dostępu) w *Safety Administration Editor*. Należy postępować zgodnie z opisem w pomocy *STEP 7* pod hasłem „Konfiguracja poziomów dostępu".

⚠ OSTRZEŻENIE

(S7-300, S7-400) W trybie bezpieczeństwa, dostęp za pomocą hasła CPU nie może być autoryzowany podczas wprowadzania zmian w standardowym programie użytkownika, ponieważ pozwoliłoby to na zmiany w programie bezpieczeństwa. Aby wykluczyć taką możliwość, należy ustawić poziom zabezpieczenia „Write protection for fail-safe blocks" (Ochrona zapisu dla bloków fail-safe) i skonfigurować hasło dla F-CPU. Jeśli tylko jedna osoba jest upoważniona do zmiany standardowego programu użytkownika oraz programu bezpieczeństwa, należy ustawić poziom zabezpieczenia „Write protection" (Ochrona zapisu) lub „Read/write protection" (Ochrona odczytu/zapisu), by inne osoby miały jedynie ograniczony dostęp lub brak dostępu do całego programu użytkownika (programów standardowego i bezpieczeństwa). *(S001)*

⚠ OSTRZEŻENIE

(S7-1200, S7-1500) W trybie bezpieczeństwa, program bezpieczeństwa musi być zabezpieczony hasłem. W tym celu należy ustawić poziom zabezpieczenia co najmniej „Full access (no protection)" (Pełny dostęp (brak ochrony)) i przypisać hasło do „Full access incl. fail-safe (no protection)" (Pełny dostęp wraz z fail-safe (brak ochrony)). Ten poziom zabezpieczenia pozwala jedynie na pełny dostęp do standardowego programu użytkownika, nie do bloków bezpieczeństwa.

W przypadku wybrania wyższego poziomu, na przykład w celu zabezpieczenia standardowego programu użytkownika, należy przypisać dodatkowe hasło do opcji „Full access (no protection)" (Pełny dostęp (brak ochrony)).

Ochronę dostępu aktywuje się poprzez pobranie (strona 325) konfiguracji sprzętowej do F-CPU.

OSTRZEŻENIE

Jeśli w sieci dostępnych jest **kilka F-CPU** (np. poprzez przemysłowy Ethernet) przy pomocy **tego samego urządzenia programistycznego lub PC**, należy podjąć następujące działania, by zagwarantować, iż dane projektu są pobierane do właściwego F-CPU:

Hasła użytkownika określone dla danego F-CPU, takie jak jednolite hasło do F-CPU z przypisanym do niego adresem ethernetowym.

Należy mieć na uwadze następuje zagadnienia:

- Aby aktywować ochronę dostępu do F-CPU podczas wczytywania konfiguracji sprzętowej po raz pierwszy, należy użyć połączenia dwupunktowego (podobnie jak w przypadku przypisywania adresu MPI do F-CPU po raz pierwszy).
- Przed pobraniem programu bezpieczeństwa do F-CPU, najpierw należy cofnąć istniejące zezwolenie na dostęp dla innych F-CPU.
- Ostatnie pobranie programu bezpieczeństwa przed przełączeniem na operację produkcyjną należy wykonać z aktywną ochroną dostępu. *(S021)*

OSTRZEŻENIE

Podczas korzystania z narzędzi do automatyzacji lub obsługi (w TIA Portal lub na serwerze sieciowym), pozwalających na ominięcie ochrony dostępu do F-CPU (np. zapisywanie lub automatyczne wprowadzanie hasła CPU dla poziomu ochrony „Full access incl. fail-safe (no protection) (Pełny dostęp wraz z fail-safe (brak ochrony)) lub hasła do serwera sieciowego), dane projektu safety mogą nie być chronione przed niezamierzonymi zmianami. *(S078)*

Zmiana hasła dla F-CPU

Aby nowe hasło zyskało ważność po zmianie dla F-CPU, należy pobrać zmienioną konfigurację do F-CPU. Jeśli to konieczne, należy wprowadzić "stare" hasło do F-CPU w celu wykonania operacji wczytania. F-CPU musi być w trybie STOP.

Usuwanie ochrony dostępu dla F-CPU

Aby usunąć ochronę dostępu dla F-CPU, należy usunąć hasło do F-CPU. W tym celu należy wykonać standardową procedurę.

Uzyskiwanie zezwolenia na dostęp dla F-CPU

Zezwolenie na dostęp dla F-CPU osiąga się – zależnie od skonfigurowanego poziomu ochrony – poprzez wprowadzenie hasła do F-CPU przed wykonaniem czynności wymagającej hasła.

Uzyskiwanie zezwolenia na dostęp dla F-CPU

Zezwolenie na dostęp dla F-CPU pozostaje ważne aż do zamknięcia projektu w *STEP 7* lub anulowaniu zezwolenia.

Anulowanie zezwolenia na dostęp dla F-CPU

Zezwolenie na dostęp anuluje się poprzez polecenie menu „Online > Delete access rights" (Online > Usuń prawa dostępu).

OSTRZEŻENIE

Jeśli ograniczony dostęp do określonych obszarów nie służy do przyznania dostępu do urządzenia programistycznego lub PC jedynie tym osobom, które są upoważnione do modyfikacji programu bezpieczeństwa, należy zastosować poniższe środki organizacyjne, by zapewnić skuteczność ochrony dostępu dla F-CPU w urządzeniu programistycznym lub PC:

- Jedynie upoważniony personel może mieć dostęp do hasła.
- Upoważniony personel musi jednoznacznie anulować pozwolenie na dostęp do F-CPU przed opuszczenie urządzenia programistycznego lub PC, zamykając *STEP 7* lub poprzez menu „Online > Delete access rights" (Online > Usuń prawa dostępu). Jeśli nie zostało to wdrożone, należy zastosować również wygaszacz ekranu zabezpieczony hasłem dostępnym jedynie dla upoważnionego personelu. *(S006)*

4.4 Ochrona dostępu przez środki organizacyjne

Aby nie dopuścić do podmienienia programu bezpieczeństwa bez upoważnienia poprzez wymianę nośnika (np. karty flash, karty pamięci SIMATIC lub dysku twardego z WinAC RTX F), należy przestrzegać następujących ostrzeżeń:

OSTRZEŻENIE

Należy ograniczyć dostęp do F-CPU osób, które są upoważnione do podłączania nośników przenośnych poprzez ograniczenie dostępu do obszaru. *(S079)*

Aby nie dopuścić do przypadkowego odinstalowania lub zainstalowania WinAC RTX F lub sterownika programowego S7-1500 F, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Należy ograniczyć dostęp do WinAC RTX F lub sterownika programowego S7-1500 F poprzez ochronę dostępu dla osób, które są upoważnione instalowania, odinstalowania lub naprawy WinAC RTX F bądź sterownika programowego S7-1500 F (np. poprzez wykorzystanie praw administratora systemu Windows (ADMIN)). *(S075)*

Funkcja „Delete Configuration" (Usuń konfigurację) jest dostępna jedynie w panelu stanowiska PC ze sterownikiem programowym S7-1500 F, gdy na F-CPU nie ustawiono ochrony dostępu. Dlatego też zaleca się, by nie ustawiać ochrona dostępu bezpieczeństwa przed wykonaniem odbioru technicznego.

Aby uniemożliwić nieupoważniony dostęp do programu bezpieczeństwa, formatowania F-CPU lub usuwania folderów programu przy użyciu wyświetlacza F-CPU S7-1500, należy zastosować się do poniższego ostrzeżenia:

OSTRZEŻENIE

Hasło wyświetlacza należy przekazywać jedynie osobom, które są upoważnione do przywracania programów bezpieczeństwa, formatowania F-CPU oraz usuwania folderów programu. Jeśli dla wyświetlacza nie zostało ustawione hasło, należy zabezpieczyć go przed nieupoważnioną obsługą poprzez środki organizacyjne. Można przykładowo ustawić ochronę dostępu do określonych pomieszczeń. *(S063)*

Aby uniemożliwić nieupoważnione przywrócenie programu bezpieczeństwa za pomocą serwera sieciowego w F-CPU S7-1200/1500, należy zastosować się do poniższego ostrzeżenia:

OSTRZEŻENIE

Upoważnienie „F-Admin" (Administrator bezpieczeństwa) dla serwera sieciowego bez zabezpieczenia hasłem (użytkownik „Everybody" (Wszyscy)) jest przeznaczone jedynie do testów, odbioru technicznego itp. Dotyczy to zatem systemu, który nie wykonuje operacji produkcyjnej. W takim przypadku należy zagwarantować bezpieczeństwo systemu poprzez inne środki organizacyjne, na przykład, zabezpieczając dostęp do określonych obszarów.

Przed przejściem do operacji produkcyjnej należy usunąć prawa „F-Admin" (administratora bezpieczeństwa) dla użytkownika „Everybody" (Wszyscy).

Jedynie upoważniony personel może mieć dostęp do hasła użytkownika serwera sieciowego z prawami „F-Admin" (Administrator bezpieczeństwa). Po pobraniu konfiguracji sprzętowej należy sprawdzić, czy jedynie upoważnieni użytkownicy serwera sieciowego mają prawo „F-Admin" na F-CPU. W tym celu należy użyć widoku online w *Safety Administration Editor*.

Zapisanie loginu i hasła serwera sieciowego w przeglądarce jest dozwolone jedynie, gdy dostęp nieupoważnionych osób jest ograniczony poprzez inne środki organizacyjne (np. ochronę dostępu do PG/PC). *(S064)*

Programowanie

5

5.1 Omówienie

Wstęp

Program bezpieczeństwa składa się z bloków bezpieczeństwa, które tworzy się przy pomocy języka programowania FBD lub LAD, oraz automatycznie dodanych bloków. Środki detekcji błędów i reakcji są dodawane automatycznie do tworzonego programu, a także wykonywane są dodatkowe testy safety. Ponadto dostępne są opcje zastosowania specjalnych, gotowych funkcji bezpieczeństwa w postaci instrukcji do programu bezpieczeństwa.

Poniżej zamieszczono przegląd elementów:

- Struktura programu bezpieczeństwa
- Bloki typu fail-safe
- Różnice w programowaniu programu bezpieczeństwa przy użyciu FBD/LAD w porównaniu do programowania standardowych programów użytkownika

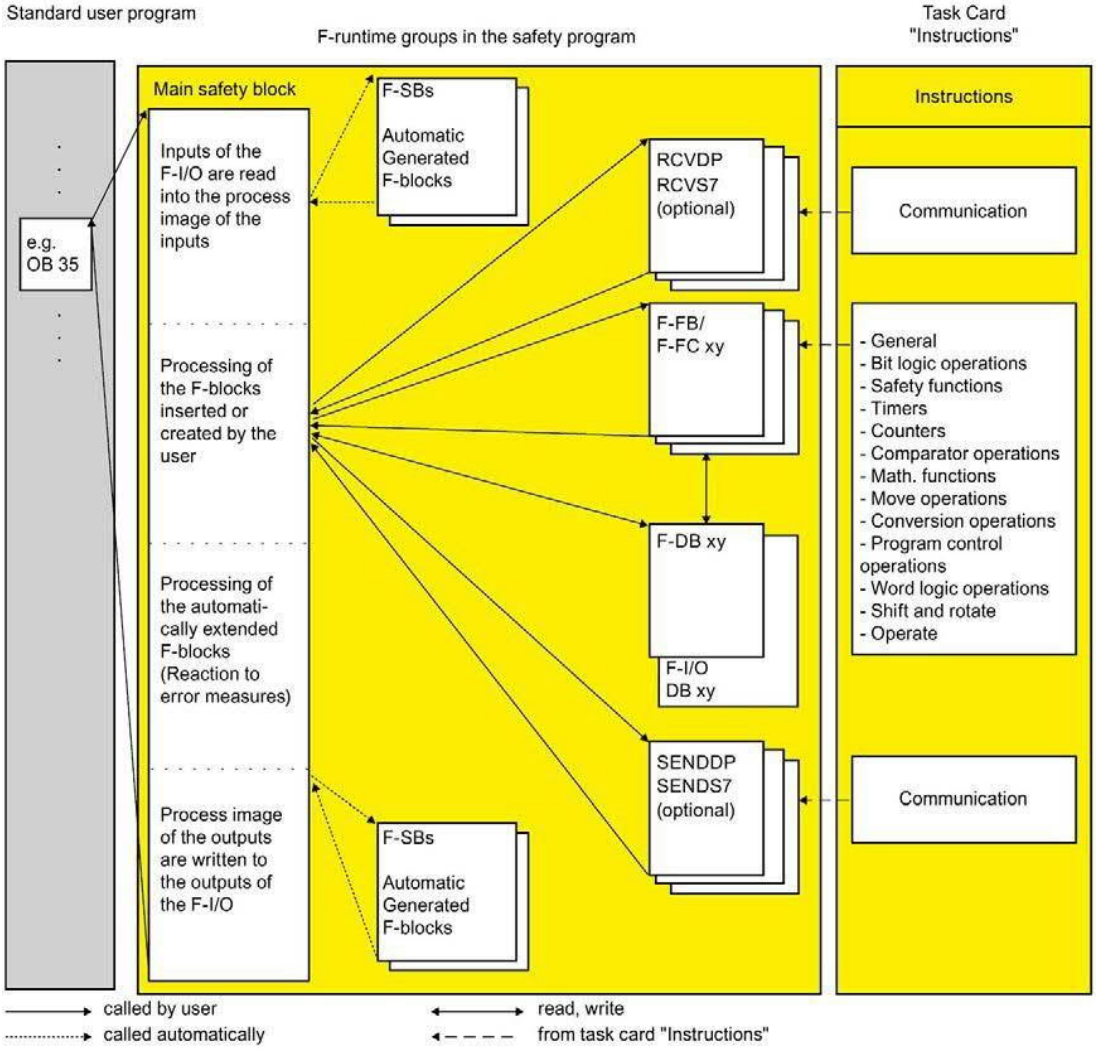
5.1.1 Struktura programu bezpieczeństwa (S7-300, S7-400)

Przedstawienie struktury programu

Ze względów strukturalnych, program bezpieczeństwa składa się z jednej lub dwóch grup F-runtime. Każda grupa F-runtime zawiera:

- Bloki bezpieczeństwa utworzone przy pomocy FBD lub LAD bądź wstawione z biblioteki projektu lub bibliotek globalnych
- Bloki bezpieczeństwa dodane automatycznie (bloki systemowe bezpieczeństwa, automatycznie generowane bloki bezpieczeństwa oraz DB F-I/O)

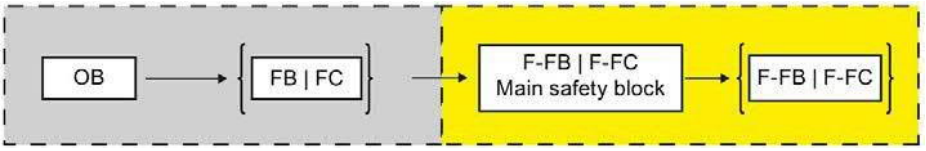
Poniżej zamieszczono schemat programu bezpieczeństwa lub grupy F-runtime dla F-CPU S7-300/400.



Główny blok bezpieczeństwa

Główny blok bezpieczeństwa to pierwszy blok programu bezpieczeństwa, który programuje się samodzielnie. Podczas kompilacji jest on uzupełniany o dodatkowe niewidoczne wywołania bloków systemowych bezpieczeństwa.

Konieczne jest przypisanie głównego bloku bezpieczeństwa do grupy F-runtime (strona 139).



Grupy F-runtime

Aby usprawnić obsługę, program bezpieczeństwa składa się z jednej lub dwóch „grup F-runtime". Grupa F-runtime to konstrukcja logiczna kilku powiązanych bloków bezpieczeństwa, które zostały utworzony wewnętrznie przez system bezpieczeństwa.

Grupa F-runtime składa się z następujących elementów:

- Głównego bloku bezpieczeństwa (F-FB/F-FC, który przypisuje się do wywołania OB (FB/FC) zgodnie z potrzebami)
- Wszelkich dodatkowych F-FB lub F-FC, które programuje się przy użyciu FBD bądź LAD oraz wywołuje z głównego bloku bezpieczeństwa
- Jednego lub kilku F-DB, zgodnie z potrzebami
- DB F-I/O
- Bloków bezpieczeństwa z biblioteki projektu lub bibliotek globalnych
- F-DB bloków systemowych bezpieczeństwa
- Automatycznie generowane bloki bezpieczeństwa

Struktura programu bezpieczeństwa w dwóch grupach F-runtime

Program bezpieczeństwa można podzielić na dwie grupy F-runtime. Poprzez uruchomienie części programu bez (jednej grupy F-runtime) w szybszej klasie pierwszeństwa, osiąga się szybsze obwody bezpieczeństwa o krótszych czasach odpowiedzi.

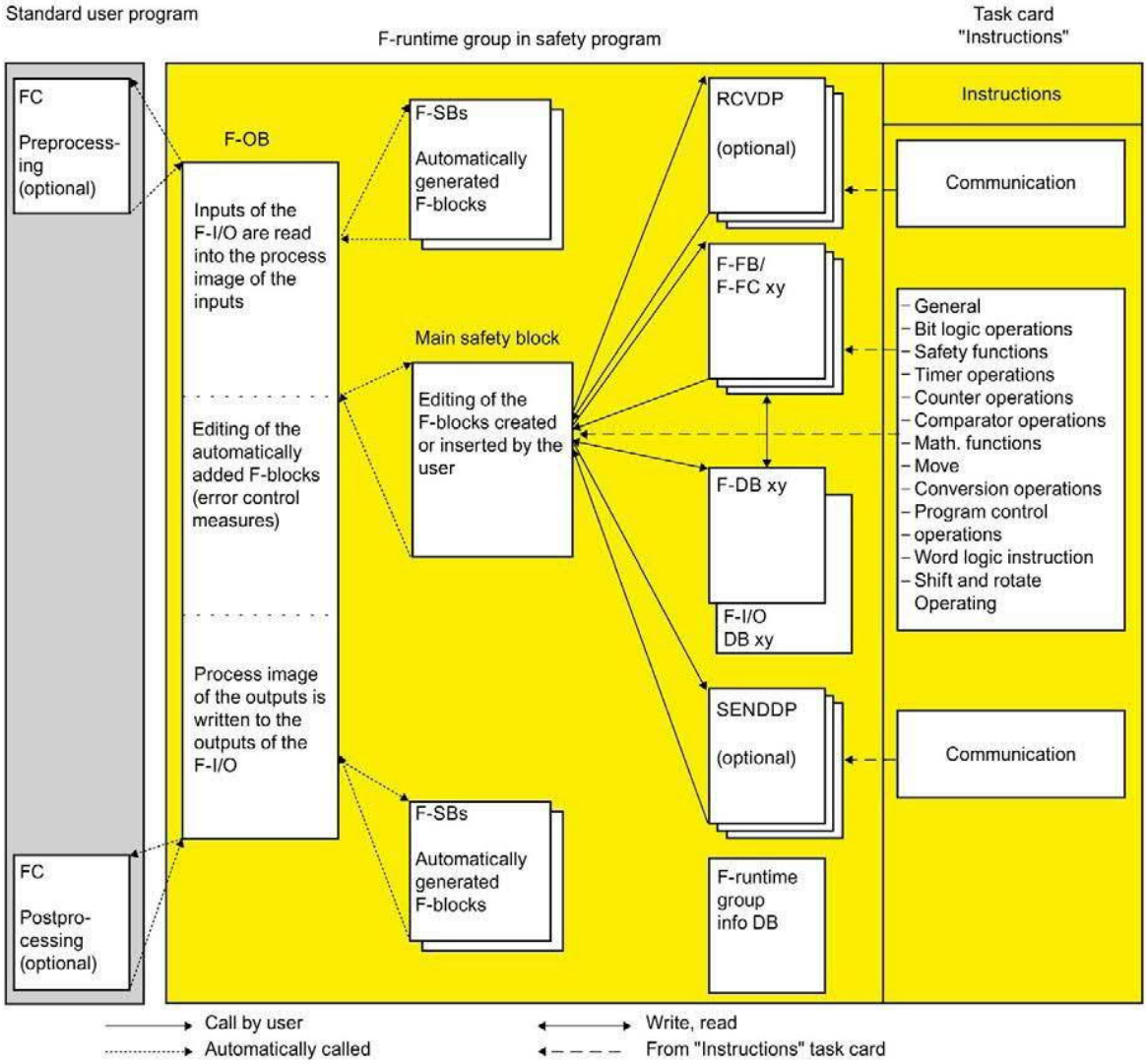
5.1.2 Struktura programu bezpieczeństwa (S7-1200, S7-1500)

Przedstawienie struktury programu

Ze względów strukturalnych, program bezpieczeństwa składa się z jednej lub dwóch grup F-runtime. Każda grupa F-runtime zawiera:

- Bloki bezpieczeństwa utworzone przy pomocy FBD lub LAD bądź wstawione z biblioteki projektu lub bibliotek globalnych
- Bloki bezpieczeństwa dodane automatycznie (bloki systemowe F-DB bezpieczeństwa, automatycznie generowane bloki bezpieczeństwa, DB F-runtime oraz DB F-I/O)

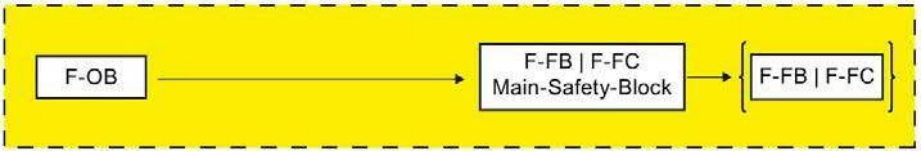
Poniżej zamieszczono schemat programu bezpieczeństwa lub grupy F-runtime dla F-CPU S7-1200/1500.



Główny blok bezpieczeństwa

Główny blok bezpieczeństwa to pierwszy blok programu bezpieczeństwa, który programuje się samodzielnie. Konieczne jest przypisanie głównego bloku bezpieczeństwa do grupy F-runtime (strona 139).

Główny blok bezpieczeństwa w F-CPU S7-1200/1500 jest wywoływany przez F-OB przypisane do grupy F-runtime.



Grupy F-runtime

Aby usprawnić obsługę, program bezpieczeństwa składa się z jednej lub dwóch „grup F-runtime". Grupa F-runtime to konstrukcja logiczna kilku powiązanych bloków bezpieczeństwa, które zostały utworzony wewnętrznie przez system bezpieczeństwa.

Grupa F-runtime składa się z następujących elementów:

- F-OB wywołującego główny blok bezpieczeństwa
- Głównego bloku bezpieczeństwa (F-FB/F-FC, który przypisuje się do F-OB)
- Wszelkich dodatkowych F-FB lub F-FC, które programuje się przy użyciu FBD bądź LAD oraz wywołuje z głównego bloku bezpieczeństwa
- Jednego lub kilku F-DB, zgodnie z potrzebami
- DB F-I/O
- DB informacji o grupie F-runtime
- Bloków bezpieczeństwa z biblioteki projektu lub bibliotek globalnych
- F-DB bloków systemowych bezpieczeństwa
- Automatycznie generowane bloki bezpieczeństwa
- Blok przetwarzania wstępnego i/lub końcowego, w razie potrzeby (patrz Przetwarzanie wstępne/końcowe (S7-1200, S7-1500) (strona 86))

Przetwarzanie wstępne/końcowe grupy F-runtime

Dostępna jest opcja wywołania bloków standardowych grup aplikacji (FC) bezpośrednio przed lub za grupą F-runtime, na przykład do transferu danych komunikacji typu fail-safe poprzez Flexible F-Link. (patrz „Przetwarzanie wstępne/końcowe (S7-1200, S7-1500)" (strona 86))

Struktura programu bezpieczeństwa w dwóch grupach F-runtime

Program bezpieczeństwa można podzielić na dwie grupy F-runtime. Poprzez uruchomienie części programu bez (jednej grupy F-runtime) w szybszej klasie pierwszeństwa, osiąga się szybsze obwody bezpieczeństwa o krótszych czasach odpowiedzi.

Zobacz także

DB informacji grupy F-runtime (S7-1200, S7-1500) (strona 158)

5.1.3 Bloki typu fail-safe

Bloki bezpieczeństwa grupy F-runtime

Poniższa tabela przedstawia bloki bezpieczeństwa wykorzystywane w

Blok bezpieczeństwa	Funkcja	F-CPU S7-300/400	F-CPU S7-1200/1500
Główny blok bezpieczeństwa	Pierwszy krok programowania programu bezpieczeństwa to główny blok bezpieczeństwa. Główny blok bezpieczeństwa w F-CPU S7-300/400 to F-FC lub F-FB (z instancją DB), który wywoływany jest przez standardowy blok (zalecenie: OB 35) ze standardowego programu użytkownika. Główny blok bezpieczeństwa w F-CPU S7-1200/1500 to F-FC lub F-FB (z instancją DB), który wywoływany jest przez F-OB.	X	X
F-FB/F-FC	Zarówno w głównym bloku bezpieczeństwa, jak i w dodatkowych F-FB i F-FC można wykonać następujące elementy: • Zaprogramować program bezpieczeństwa przy użyciu instrukcji dostępnych dla bloków bezpieczeństwa w FDB lub LAD • Wywołać inne utworzone F-FB/F-FC w celu utworzenia programu bezpieczeństwa • Wstawić bloki bezpieczeństwa z biblioteki projektowej lub bibliotek globalnych	X	X
F-DB	Opcjonalne bloki danych typu fail-safe, które można zabezpieczyć przed odczytem i zapisem w obrębie całego programu bezpieczeństwa.	X	X
DB F-I/O	DB F-I/O jest generowany automatycznie dla każdego F-I/O podczas jego konfiguracji. Istnieje możliwość lub konieczność uzyskania dostępu do taga DB F-I/O w połączeniu z dostępem F-I/O.	X	X
DB współdzielone typu F	DB współdzielone typu F to blok danych fail-safe, zawierający wszystkie współdzielone dane programu oraz dodatkowe informacje wymagane przez system bezpieczeństwa.	X	—
DB informacji o grupie F-runtime	DB informacji o grupie F-runtime jest tworzony podczas generowania grupy F-runtime. DB informacji o grupie F-runtime zapewnia informacje o grupie F-runtime oraz całym programie bezpieczeństwa.	—	X

Uwaga

Zabronione jest wstawianie bloków bezpieczeństwa z folderu „System blocks" do głównego bloku bezpieczeństwa/F-FB/F-FC.

Instrukcje do programu bezpieczeństwa

W zakładce „Instuctions" (Instrukcje) można znaleźć instrukcje do używanego F-CPU, które można wykorzystać do programowania programu bezpieczeństwa.

Dostępne są tam instrukcje znane ze standardowego programu użytkownika, takie jak operacje na bitach logicznych, funkcje matematyczne, funkcje do sterowania programem oraz operacja na słowach logicznych.

Ponadto dostępne są instrukcje dla funkcji bezpieczeństwa, np. monitorowanie oburęczne, analiza rozbieżności, muting, zatrzymanie/wyłączenie awaryjne, monitorowanie drzwi bezpieczeństwa, monitorowanie sygnału zwrotnego oraz instrukcji komunikacji związanej z bezpieczeństwem pomiędzy F-CPU.

Informacje dodatkowe

Szczegółowy opis instrukcji do programu bezpieczeństwa dostępny jest w dziale „Przegląd instrukcji" (strona 410).

Korzystanie z wersji instrukcji

Podobnie jak w przypadku instrukcji do standardowego programu użytkownika, istnieje możliwość występowania różnych wersji instrukcji do programu bezpieczeństwa.

Dodatkowe informacje dotyczące wersji instrukcji można znaleźć w pomocy do STEP 7 w „Podstawy wersji instrukcji".

Dalsze informacje na temat różnic pomiędzy wersjami instrukcji do programu bezpieczeństwa można znaleźć w odnośnym rozdziale instrukcji obsługi.

Uwaga

Należy mieć na uwadze następuje zagadnienia:

- W przypadku zmiany wersji instrukcji zastosowanej w programie bezpieczeństwa w zakładce „Instructions" (Instrukcje) na wersję, która nie ma identycznych funkcji, działanie programu bezpieczeństwa może ulec zmianie po jego ponownym skompilowaniu. Oprócz podpisu bloku bezpieczeństwa, który wykorzystuje instrukcję, zbiorczy podpis bezpieczeństwa oraz zbiorczy podpis F-SW programu bezpieczeństwa również ulegnie zmianie. Może być konieczne wykonanie testu akceptacji (strona 396).
- (S7-300/400) W przypadku wykorzystywania bloku bezpieczeństwa z chronioną wiedzę specjalistyczną w programie bezpieczeństwa, który korzysta z instrukcji o wersji innej niż ustawiona w karcie zadań „Instructions" (Instrukcje), gdy program jest kompilowany bez wprowadzenia hasła do bloku bezpieczeństwa chronionej wiedzy specjalistycznej, jest on dopasowywany do wersji ustawionej w karcie zadań „Instrukcje", o ile interfejsu wersji instrukcji są identyczne. Jeśli wersje instrukcji nie mają identycznych funkcji, działanie bloku bezpieczeństwa chronionej wiedzy technologicznej może ulec zmianie, a zawsze zmienia się jego podpis.

5.1.4 Ograniczenia w językach programowania FBD/LAD

Języki programowania LAD i FDB

Program użytkownika w F-CPU zazwyczaj składa się ze standardowego programu użytkownika oraz programu bezpieczeństwa.

Standardowy program użytkownika tworzy się przy pomocy języków programowania, takich jak SCL, STL, LAD, FDB.

W przypadku programu bezpieczeństwa, LAD iFDB można stosować z pewnymi ograniczeniami w instrukcjach i odnośnych rodzajach danych oraz obszarach argumentu. Należy zwracać uwagę na ograniczenia poszczególnych instrukcji.

Obsługiwane instrukcje

Dostępne instrukcje zależą od stosowanego F-CPU. Obsługiwane instrukcje można sprawdzić w opisie instrukcji (począwszy od instrukcji do STEP 7 Safety V16 (strona 410)).

Uwaga

Nie można połączyć włączonego wejścia EN oraz włączonego wyjścia ENO.

Wyjątek:

(S7-1200, S7-1500) Przy użyciu poniższych instrukcji można zaprogramować wykrywanie nadmiernego przepływu poprzez podłączenie włączonego wyjścia ENO:

- ADD: Dodawanie (STEP 7 Safety V16) (strona 554)
- SUB: Odejmowanie (STEP 7 Safety V16) (strona 557)
- MUL: Mnożenie (STEP 7 Safety V16) (strona 560)
- DIV: Dzielenie (STEP 7 Safety V16) (strona 563)
- NEG: Tworzenie uzupełnienia dwójkowe (STEP 7 Safety V16) (strona 567)
- ABS: Tworzenie wartości bezwzględnej (STEP 7 Safety V16) (S7-1200, S7-1500) (strona 570)

Obsługiwane rodzaje danych i parametrów

Obsługwiwane są **jedynie** poniższe rodzaje danych:

- BOOL
- INT
- WORD
- DINT
- DWORD (S7-300, S7-400)
- TIME
- ARRAY, ARRAY[*] podczas korzystania z instrukcji RD_ARRAY_I: Odczytaj z INT F-array (STEP 7 Safety V16) (S7-1500) (strona 574) oraz RD_ARRAY_DI: Odczytaj z DINT F-array (STEP 7 Safety V16) (S7-1500) (strona 577).

  Ograniczenia:

  - ARRAY jedynie w DB globalnych dla bezpieczeństwa
  - Ograniczenia dla ARRAY: 0 do maks. 10000
  - ARRAY[*] jedynie jako parametr we-wy (InOut) w F-FC oraz F-FB
  - ARRAY z UDT nie jest dozwolony
  - ARRAY typu Bool nie jest dozwolony
  - ARRAY typu Word nie jest dozwolony
  - ARRAY typu Time nie jest dozwolony
- Rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) (S7-1200, S7-1500)

Uwaga

Jeśli wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, F-CPU może przełączyć się w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.
Dlatego też należy przestrzegać dopuszczalnego zakresu dla rodzaju danych podczas tworzenia programu, wybrać pasujący rodzaj bądź użyć wyjścia ENO.

Należy zwracać uwagę na opis poszczególnych instrukcji.

Niedozwolone rodzaje danych i parametrów

Poniższe rodzaje **nie** są dozwolone:

- Wszystkie rodzaje niewyszczególnione w dziale „Obsługiwane rodzaje danych i parametrów" (np. BYTE, REAL)
- Złożone rodzaje danych (przykładowo, STRING, ARRAY (S7-300, S7-400, S7-1200), STRUCT, rodzaj danych PLC (UDT) (S7-300, S7-400))
- Rodzaje parametrów (np. BLOCK_FB, BLOCK_DB, ANY)

Obsługiwane obszary argumentów

Pamięć systemu F-CPU jest podzielona na takie same obszary argumentów jak pamięć systemu standardowego CPU. Z poziomu programu bezpieczeństwa możliwy jest dostęp do obszarów wyszczególnionych w poniższej tabeli.

Tabela 5-1 Obsługiwane obszary argumentów

Obszar argumentów	Opis
Obraz procesu wejść	
• Dla F-I/O	Możliwy dostęp „tylko do odczytu" do kanałów wejściowych F-I/O. Z tego względu nie jest możliwy transfer do parametrów IN_OUT w F-FB lub F-FC. Obraz procesu wejść F-I/O jest aktualizowany przed uruchomieniem głównego bloku bezpieczeństwa.
• Dla standardowych I/O	Kanały wejściowe standardowego I/O są dostępne jedynie do odczytu. Z tego względu nie jest możliwy transfer do parametrów IN_OUT w F-FB lub F-FC. Ponadto wymagana jest kontrola ważności związana z procesem. Patrz *pomoc STEP 7* odnośnie czasów aktualizacji obrazu procesuwejść dla standardowego I/O.
Obraz procesu wyjść	
• Dla F-I/O	Możliwy dostęp „tylko do zapisu" do kanałów wyjściowych F-I/O. Z tego względu nie jest możliwy transfer do parametrów IN_OUT w F-FB lub F-FC. W programie bezpieczeństwa, wartości dla wyjść F-I/O są obliczane i przechowywane w obrazie procesowym wyjść. Obraz procesu wyjść do F-I/O jest aktualizowany po zakończeniu głównego bloku bezpieczeństwa.
• Dla standardowych I/O	Kanały wyjściowe standardowych I/O to kanały tylko do odczytu. Z tego względu nie jest możliwy transfer do parametrów IN_OUT w F-FB lub F-FC. W programie bezpieczeństwa, wartości dla wyjść standardowych I/O również są obliczane i przechowywane w obrazie procesowym wyjść, jeśli to konieczne. Patrz *pomoc STEP 7* odnośnie czasów aktualizacji obrazu procesuwyjść dla standardowego I/O.
Pamięć bitowa	Ten obszar służy do wymiany danych ze standardowym programem użytkownika. Ponadto ochrona odczytu wymaga kontroli ważności związanej z procesem. Szczególny element pamięci bitowej może mieć ochronę odczytu lub zapisu w programie bezpieczeństwa. Z tego względu nie jest możliwy transfer do parametrów IN_OUT w F-FB lub F-FC. Należy pamiętać, że pamięci bitowej można używać jedynie do łączenia standardowego programu użytkownika i programu bezpieczeństwa; nie można stosować jej jako bufora do danych bezpieczeństwa.
Bloki danych	

Obszar argumentów	Opis
• F-DB	Bloki danych przechowują informacje do programu. Można je zdefiniować jako globalne bloki danych, takie jak F-FB, F-FC, może mieć do nich dostęp główny blok bezpieczeństwa lub można przypisać je do konkretnego F-FB lub głównego bloku bezpieczeństwa (DB instancji). Dostęp do taga współdzielonego DB może mieć tylko jedna grupa F-runtime, przy czym wywoływany jest DB instancji tylko z grupy F- runtime, w której wywoływana jest odnośna instrukcja/F-FB.
• DB	Ten obszar służy do wymiany danych ze standardowym programem użytkownika. Ponadto ochrona odczytu wymaga kontroli ważności związanej z procesem. Dla taga DB możliwy jest dostęp do odczytu lub dostęp do zapisu w programie bezpieczeństwa. Z tego względu nie jest możliwy transfer do parametrów IN_OUT w F-FB lub F-FC. Należy pamiętać, że tagów DB można używać jedynie do przenoszenia danych pomiędzy standardowym programem użytkownika i programem bezpieczeństwa; nie można stosować ich jako bufora do danych bezpieczeństwa.
Tymczasowe dane lokalne	Ten obszar pamięci zawiera tagi tymczasowe bloku (lub bloku bezpieczeństwa) gdy wykonywany jest blok (bezpieczeństwa). Stos danych lokalnych zapewnia również pamięć do przenoszenia parametrów bloku oraz zapisywania wyników pośrednich.

Konwersja rodzaju pliku

Tak samo jak w standardowym programie użytkownika, dostępne są dwie możliwości konwersji rodzaju pliku w programie bezpieczeństwa.

- Konwersja niejawna

  Konwersja niejawna jest wykonywana identycznie jak w standardowym programie użytkownika, z następującymi ograniczeniami: Długość bitu rodzaju danych źródłowych musi być zgodna z długością bitu rodzaju danych docelowych.

- Konwersja jawna

  W przypadku korzystania z instrukcji konwersji jawnej (strona 584) jest wykonywana przed faktyczną instrukcją.

Dostęp segmentowany

Dostęp segmentowany nie jest możliwy w programie bezpieczeństwa.

Niedozwolone obszary argumentów

Dostęp poprzez jednostki inne niż wyszczególnione w poniższej tabeli **nie** jest dozwolony. To samo tyczy się dostępu do obszarów argumentów, które nie zostały wymienione, w szczególności:

- Bloki danych dodane automatycznie

  Wyjątek: Określone tagi w DB F-I/O (strona 174) oraz w DB współdzielonych typu F(S7-300, S7-
- 400) (strona 157) lub DB informacji o grupie F-runtime (S7-1200, S7-1500) (strona 158)
- Obszar I/O: Wejścia

Stałe logiczne „0" bądź „FALSE" oraz „1" bądź „TRUE" (S7-300, S7-400)

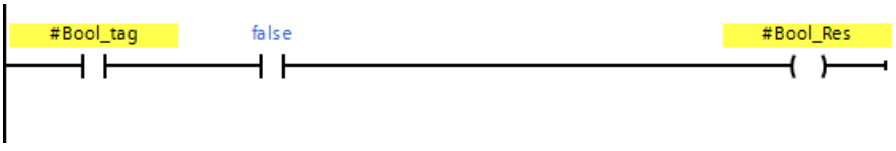
Stałe logiczne „0" bądź „FALSE" (FAŁSZ)" oraz „1" bądź „TRUE" (PRAWDA)" są dostępne dla F-CPU S7-300/400 jako „tagi" „RLO0" oraz „RLO1" w DB globalnym bezpieczeństwa. Dostęp do nich jest możliwy poprzez w pełni kwalifikowany dostęp DB („F_GLOBDB".RLO0 lub "F_GLOBDB".RLO1).

Stałe logiczne „0" bądź „FALSE" oraz „1" bądź „TRUE" (S7-1200, S7-1500)

Stałe logiczne „0" bądź „FALSE" (FAŁSZ)" oraz „1" bądź „TRUE" (PRAWDA)" są dostępne dla F-CPU S7-1200/1500 w celu przypisania parametrów podczas wywołania bloków.
Dostęp do nich jest możliwy bezpośrednio w FBD lub LAD na odnośnych wejściach bloków.

Przykład FBD:

Przykład LAD:

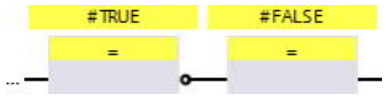


Alternatywnie, dostępna jest jak wcześniej opcja do ustawienia „1" lub „PRAWDA" w tagu korzystającym z instrukcji „Assignment" (Przypisanie) (strona 423).

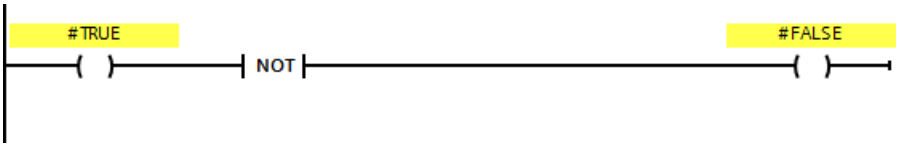
W tym celu nie należy łączyć wzajemnie wejścia pola instrukcji „Assignment" w FBD. W LAD wejście łączy się bezpośrednio z szyną zasilającą.

Tag z wartością „0" lub „FAŁSZ" otrzymuje się poprzez dalsze odwrócenie przy pomocy instrukcji „Invert RLO" (Odwróć RLO) (strona 419).

Przykład FBD:



Przykład LAD:



Obszar argumentów tymczasowych

danych

Uwaga

Podczas korzystania z obszaru argumentów tymczasowych danych lokalnych należy pamiętać, że pierwszym dostępem elementu danych lokalnych w głównym bloku bezpieczeństwa/F-FB/F-FC musi zawsze być dostęp do zapisu. Inicjalizuje to lokalny element danych.

Należy upewnić się, że element tymczasowych danych lokalnych został zainicjowany przed pierwszą instrukcją JMP, JMPN lub RET.

„Bit danych lokalnych" powinien zostać zainicjowany wraz z przypisaniem instrukcji ("=") (FBD) lub ("--( )") (LAD). Do bitu danych lokalnych należy przypisać stan sygnału „0" lub „1" jako stałą boolowską.

Bity danych lokalnych nie mogą być inicjalizowane za pomocą instrukcji przerzutnika (SR, RS), wyjścia Set (S) ani wyjścia Reset (R).

F-CPU może przejść w stan STOP, jeśli nie zostanie to wykonane. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

„W pełni kwalifikowany dostęp DB"

Dostęp do tagów bloków danych w F-FB/F-FC to "w pełni kwalifikowany dostęp DB". Dotyczy to również dostępu początkowego do tagów bloków danych po etykiecie skoku.

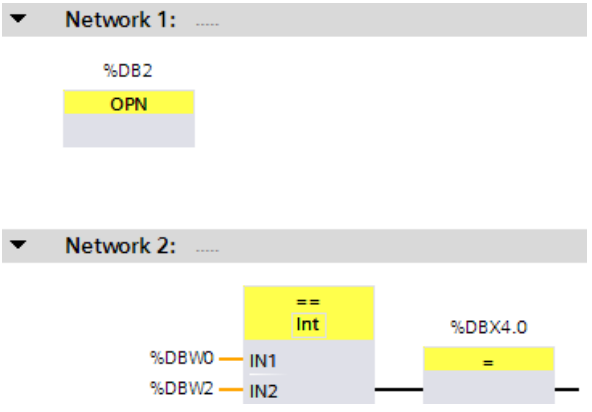
W przypadku F-CPU S7-300/400, jedynie dostęp początkowy musi mieć postać „w pełni kwalifikowany dostęp DB". Można również użyć instrukcji „OPN".

Przykład „w pełni kwalifikowanego dostępu DB":

Należy przypisać nazwę do F-DB, np. „F_Data_1". Należy korzystać z nazw przypisanych w deklaracji F-DB zamias adresów bezwzględnych.

Ilustracja Przykład z w pełni kwalifikowanym

Przykład „nie w pełni kwalifikowanego dostępu DB" (S7-300, S7-400):



Ilustracja Przykład bez w pełni kwalifikowanego

Dostęp do DB instancji

Możliwy jest również dostęp do instancji DB z F-FB z w pełni kwalifikowanym dostępem, np. do przenoszenia parametrów bloków. Nie jest możliwe uzyskanie dostępu do statycznych danych lokalnych w pojedynczej/wielu instancjach innych F-FB.

Należy pamiętać, że dostęp do instancji DB z F-FB, które nie zostały wywołane w programie bezpieczeństwa może spowodować przejście F-CPU do trybu STOP.

5.1.5 Rodzaje danych PLC zgodnych z bezpieczeństwem (UDT) (S7-1200, S7-1500)

Wstęp

Użycie rodzaju danych PLC zgodnych z bezpieczeństwem (UDT)
deklaruje się identycznie jak standardowe rodzaje danych PLC (UDT). W programie bezpieczeństwa, a także w standardowym programie użytkownika można wykorzystywać rodzaje danych PLC zgodne z bezpieczeństwem (UDT).
Różnice względem standardowego rodzaju danych PLC (UDT) zostały opisane w niniejszym rozdziale.
Informacje dotyczące użycia i deklaracji standardowego rodzaju danych PLC (UDT) są dostępne w *pomocy STEP 7* pod hasłem „Deklarowanie rodzaju danych PLC".

Deklarowanie rodzaju danych PLC zgodnych z bezpieczeństwem (UDT)

Deklarowanie rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) odbywa się identycznie jak w przypadku rodzaju danych PLC (UDT).

W rodzajach danych PLC zgodnych z bezpieczeństwem (UDT) możliwe jest użycie wszystkich rodzajów danych (strona 121), które można również wykorzystać w programach bezpieczeństwa. Wyjątek: ARRAY.

Osadzanie rodzajów danych PLC zgodnych z bezpieczeństwem (UDT) w rodzajach danych PLC zgodne z bezpieczeństwem (UDT) nie jest obsługiwane.

Aby dokonać deklaracji, należy wykonać co następuje:

1. Kliknąć na „Add new PLC data type" (Dodaj nowy rodzaj danych PLC) w folderze „PLC Data Types" (Rodzaje danych PLC) w drzewku projektu.
2. Aby utworzyć rodzaj danych PLC zgodnych z bezpieczeństwem (UDT), należy włączyć opcję „Create F-compliant PLC data type" (Utwórz rodzaj danych PLC zgodnych z bezpieczeństwem) w oknie „Add new PLC data type" (Dodaj nowy rodzaj danych PLC).

Użycie rodzaju danych PLC zgodnych z bezpieczeństwem (UDT)

Użycie rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) odbywa się identycznie jak w przypadku standardowego rodzaju danych PLC (UDT).

Zmiany w rodzaju danych PLC zgodnych z bezpieczeństwem (UDT)

Aby zmienić rodzaje danych PLC zgodne z bezpieczeństwem (UDT) wymagane jest hasło do programu bezpieczeństwa. Niezależnie od tego, czy rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) jest wykorzystywany w bloku bezpieczeństwa, w standardowym bloku czy w ogóle nie jest używany.

Zobacz także

Obszar „Rodzaje danych PLC zgodnych z bezpieczeństwem" (S7-1200, S7-1500) (strona 89)

5.1.5.1 Grupowanie zmiennych PLC dla wejść i wyjść F-I/O w strukturach (S7-1200, S7-1500)

Tagi PLC dla wejść i wyjść F-I/O w grupuje się struktury (stukturyzowany tag PLC), tak jak w przypadku wejść i wyjść standardowych I/O.

Zasady

Podczas tworzenia strukturyzowanych tagów PLC dla wejść i wyjść F-I/O należy przestrzegać poniższych zasad oprócz zasad na przypadków standardowych:

- Nie należy jednocześnie grupować wejść/wyjść standardowego I/O oraz F-I/O w strukturyzowanym tagu PLC.
- W strukturyzowanych tagach PLC możliwe jest grupowanie jedynie wejść/wyjść istniejących kanałów (wartość kanału oraz stan wartości).

  Zobacz również "Adresowanie F-I/O" (strona 166)
- W strukturyzowanych tagach PLC możliwe jest grupowanie jedynie wejść/wyjść kanałów (wartość kanału oraz stan wartości), które zostały włączone w konfiguracji sprzętowej.

  Zobacz również "Adresowanie F-I/O" (strona 166)
- Możliwe jest jedynie grupowanie wejść kanałów (wartość kanału oraz stan wartości), które zapewniają „ocenę czujnika 1oo2" z ustawionym parametrem „1oo2 sensor evaluation".

- Zobacz również "Adresowanie F-I/O" (strona 166)

  W strukturyzowanym tagu PLC dla F-I/O z wyjściami należy pogrupować wszystkie wyjścia tego F-I/O lub zakres wyjściowy z wielokrotnościami 16 bitów.
- F-CPU może przejść w stan STOP, jeśli ten wymóg zostanie pominięty. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU. Strukturyzowany tag PLC, który grupuje wyjścia F-I/O nie może nakładać się na inne tagi PLC.

  F-CPU może przejść w stan STOP, jeśli ten wymóg zostanie pominięty. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Uwaga

Aby dostosować się do tej zasady, należy odpowiednio zadeklarować rodzaj danych PLC zgodnych z bezpieczeństwem, które są używane w strukturyzowanym tagu PLC.

Adresy przyporządkowane do strukturyzowanego taga PLC znajdują się w zakładce „IO tags" (tagi IO) konfiguracji F-I/O.

5.1.5.2 Przykład pogrupowanych tagów PLC dla wejść i wyjść F-I/O (S7-1200, S7-1500)

Wstęp

Niniejszy przykład wykorzystuje moduł bezpieczeństwa 4 F-DI/3 F-DO DC24V/2A z oceną 1oo2 w celu przedstawienia, jak należy korzystać ze strukturyzowanych tagów PLC do uzyskania dostępu do F-I/O.

Struktura kanału dla modułu bezpieczeństwa 4 F-DI/3 F-DO DC24V/2A

Poniższa tabela przedstawia strukturę kanału i przypisanie adresów modułu bezpieczeństwa 4 F-DI/3 F-DO DC24V/2A z oceną 1oo2. Uzyskanie dostępu jest możliwe jedynie dla istniejących i aktywnych kanałów (adresy I15.0 do I15.3 oraz I16.0 do I16.3). Kanały te dostarczają wynik oceny 1oo2 wygenerowany wewnętrznie w module bezpieczeństwa.

Tabela 5-2 Struktura kanału oraz adresy wartości kanałów wejściowych z oceną1oo2.

Grupa	Adres
Kanał DI, wartość kanału 0	I15.0
Kanał DI, wartość kanału 1	I15.1
Kanał DI, wartość kanału 2	I15.2
Kanał DI, wartość kanału 3	I15.3
—	I15.4
—	I15.5
—	I15.6
—	I15.7

Tabela 5-3 Struktura kanału oraz adresy stanu wartości wejść z oceną1oo2.

Grupa	Adres
Kanał DI, stan wartości 0	I16.0
Kanał DI, stan wartości 1	I16.1
Kanał DI, stan wartości 2	I16.2
Kanał DI, stan wartości 3	I16.3
—	I16.4
—	I16.5
—	I16.6
—	I16.7

Tabela 5-4 Struktura kanału oraz adresy stanu wartości wyjść

Grupa	Adres
Kanał DO, stan wartości 0	I17.0
Kanał DO, stan wartości 1	I17.1
Kanał DO, stan wartości 2	I17.2
Kanał DO, stan wartości 3	I17.3

Tabela 5-5 Struktura kanału oraz adresy stanu wartości kanałów wyjściowych

Grupa	Adres
Kanał DO, wartość kanału 0	Q15.0
Kanał DO, wartość kanału 1	Q15.1
Kanał DO, wartość kanału 2	Q15.2
Kanał DO, wartość kanału 3	Q15.3

Tworzenie rodzaju danych PLC zgodnych z bezpieczeństwem (UDT)

Aby uzyskać, przykładowo, dostęp do wszystkich kanałów, należy utworzyć dwa rodzaj danych PLC zgodnych z bezpieczeństwem (UDT).

Ilustracja poniżej przedstawia rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) pozwalający na dostęp do wartości kanału oraz stanu wartości wejść z oceną 1oo2:

4 F-DI/3 F-DO DC24V/2A_DI

	Name	Data type	Comment
1	CH_DI_0	Bool	Channel 0 (DI)
2	CH_DI_1	Bool	Channel 1 (DI)
3	CH_DI_2	Bool	Channel 2 (DI)
4	CH_DI_3	Bool	Channel 3 (DI)

Ilustracja poniżej przedstawia rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) pozwalający na dostęp do wartości kanału oraz stanu wartości wyjść:

4 F-DI/3 F-DO DC24V/2A_DO

	Name	Data type	Comment
1	CH_DO_0	Bool	Channel 0 (DO)
2	CH_DO_1	Bool	Channel 1 (DO)
3	CH_DO_2	Bool	Channel 2 (DO)

Użycie rodzaju danych PLC zgodnych z bezpieczeństwem (UDT)

Jak przedstawiono na ilustracji poniżej, możliwe jest użycie dwóch rodzajów danych PLC zgodnych z bezpieczeństwem (UDT), które utworzono w F-FC (np. „Motor"):

Motor

	Name	Data type	Comment
1	Input		
2	Motor SS DI	"4 F-DI/3 F-DO DC24V/2A_DI"	Motor interface channel values DI
3	CH_DI_0	Bool	Kanal 0 (DI)
4	CH_DI_1	Bool	Kanal 1 (DI)
5	CH_DI_2	Bool	Kanal 2 (DI)
6	CH_DI_3	Bool	Kanal 3 (DI)
7	Motor SS DI VS	"4 F-DI/3 F-DO DC24V/2A_DI"	Motor interface value status DI
8	CH_DI_0	Bool	Kanal 0 (DI)
9	CH_DI_1	Bool	Kanal 1 (DI)
10	CH_DI_2	Bool	Kanal 2 (DI)
11	CH_DI_3	Bool	Kanal 3 (DI)
12	Motor SS DO VS	"4 F-DI/3 F-DO DC24V/2A_DO"	Motor interface value status DI
13	CH_DO_0	Bool	Kanal 0 (DO)
14	CH_DO_1	Bool	Kanal 1 (DO)
15	CH_DO_2	Bool	Kanal 2 (DO)
16	Output		
17	Motor SS DO	"4 F-DI/3 F-DO DC24V/2A_DO"	Motor interface channel values DO
18	CH_DO_0	Bool	Kanal 0 (DO)
19	CH_DO_1	Bool	Kanal 1 (DO)
20	CH_DO_2	Bool	Kanal 2 (DO)

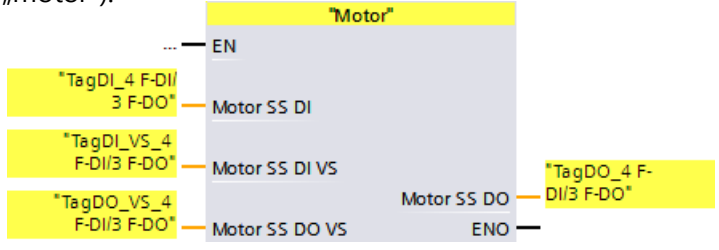
Tworzenie strukturyzowanych tagów PLC do modułu bezpieczeństwa 4 F-DI/3 F-DO DC24V/2A

Tag table_1

	Name	Data type	Address	Comment
1	TagDI_4 F-DI/3 F-DO	"4 F-DI/3 F-DO DC24V/2A_DI"	%I15.0	Motor 1 DI
2	TagDI_VS_4 F-DI/3 F-DO	"4 F-DI/3 F-DO DC24V/2A_DI"	%I16.0	Motor 1 DI VS
3	TagDO_VS_4 F-DI/3 F-DO	"4 F-DI/3 F-DO DC24V/2A_DO"	%I17.0	Motor 1 DO VS
4	TagDO_4 F-DI/3 F-DO	"4 F-DI/3 F-DO DC24V/2A_DO"	%Q15.0	Motor 1 DO

Uzyskiwanie dostępu do F-FC

Należy przenieść strukturyzowane tagi PLC utworzone podczas wywoływania F-FC (np. „motor"):



Zobacz także

Adresowanie F-I/O (strona 166)

Stan wartości (S7-1200, S7-1500) (strona 168)

5.1.6 Edycja tagów PLC za pomocą edytorów zewnętrznych

Aby edytować tagi PLC za pomocą edytorów zewnętrznych należy wykonać procedurę dla wersji standardowej. Dodatkowe informacje można znaleźć w *pomocy STEP 7* pod hasłem „Edycja tagów PLC za pomocą edytorów zewnętrznych".

Należy mieć na uwadze następuje zagadnienia:

Uwaga

Po zaimportowaniu tabeli tagów, zawierającej tagi stosowane w programie bezpieczeństwa, zbiorczy podpis bezpieczeństwa programu jest resetowany.

Aby utworzyć zbiorczy podpis bezpieczeństwa, należy ponownie skompilować dane projektu. W tym celu, wraz ochroną dostępu ustawioną dla programu bezpieczeństwa, wymagana jest ważna autoryzacja dostępu do programu bezpieczeństwa.

Aby edytować tagi PLC za pomocą edytorów zewnętrznych, zaleca się zapisanie tagów, które mają być użyte w programie bezpieczeństwa, w odrębnej tabeli tagów.

5.1.7 Korzystanie z inżynierii wieloużytkowej

Aby użyć inżynierii wieloużytkowej, należy postępować zgodnie z opisem w pomocy STEP 7 pod hasłem „Korzystanie z inżynierii wieloużytkowej".

5.1.8 Openess

5.1.8.1 Openess safety

Wymogi

Aplikacja „Openess" TIA Portal jest połączona z TIA Portal.

Patrz „Łączenie z TIA Portal" (dział „Openess: Automating creation of project"

(Openess: Automatyzacja tworzenia projektu))

Usługa Openess

Interfejs Openess (Siemens.Engineering.dll) został rozszerzony o usługę `GlobalSettings` (patrz obszar nazwy Siemens.Engineering.Safety), która zapewnia dwa działania:

- `SafetyModificationsPossible(bool safetyModificationsPossible)`
- `UsernameForFChangeHistory(string userName)`

Zasada

Należy uzyskać usługę Safety.GlobalSettings z instancji `TiaPortal`:

```
Engineering.Safety.GlobalSettings globalSettings =
TiaPortal.GetService<Engineering.Safety.GlobalSettings>();
```

5.1.8.2 SafetyModificationsPossible

Aplikacja

Działanie `SafetyModificationsPossible(bool safetyModificationsPossible)` z usługi `GlobalSettings` służy do zapobiegania zmianom w programie bezpieczeństwa w TIA Portal.

Gdy parametr `safetyModificationsPossible` jest ustawiony na `true`, TIA Portal zachowuje się zgodnie z bieżącymi ustawieniami bezpieczeństwa dla programu.

Jeśli parametr `safetyModificationsPossible` jest ustawiony na `false`, wszystkie zmiany w programie bezpieczeństwa są zablokowane, niezależnie od tego, czy użytkownik wprowadził hasło do zmiany programu. System wykorzystuje komunikaty zwrotne do przekazywania informacji, czy bieżący użytkownik jest upoważniony do wprowadzania zmian w programie bezpieczeństwa.

Jeśli nie skonfigurowano hasła lub nie przypisano go do programu bezpieczeństwa, parametr `safetyModificationsPossible` z ustawieniem false nie ma wpływu. Oznacza to, że możliwe jest wprowadzenie zmian w programie. Zablokowana jest jednakże możliwość ustawienia nowego hasła.

Nazwa	Typ	Opis
`safetyModificationsPossible`	`bool`	Autoryzacja zmian w programie bezpieczeństwa

Kod programu

Zapobiega wprowadzeniu zmian w programie bezpieczeństwa:

```
globalSettings.SafetyModificationsPossible(false);
```

5.1.8.3 UsernameForFChangeHistory

Aplikacja

Działanie `UsernameForFChangeHistory(string userName)` określa nazwę użytkownika wykorzystywaną przez TIA Portal do kolejnych operacji logowania w historii zmian bezpieczeństwa.

Maksymalna długość ciągu jest ograniczona do 256 znaków. Ciągi przekraczające tę wartość są obcinane.

Pusta nazwa użytkownika (zero lub ciąg pusty) resetuje nazwę użytkownika do wartości domyślnej. Poniższa tabela przedstawia parametry wymagane przez metodę:

Nazwa	Typ	Opis
`userName`	ciąg	Preferowana nazwa użytkownika

Kod programu

Ustawia preferowaną nazwę użytkownika:

```
globalSettings.UsernameForFChangeHistory("username");
```

5.1.9 Usuwanie programu

Usuwanie poszczególnych bloków bezpieczeństwa

Aby usunąć blok bezpieczeństwa, należy wykonać procedurę identyczną jak w *STEP 7*.

Usuwanie grup F-runtime

Zobacz Usuwanie grup F-runtime (strona 159)

(S7-300, S7-400) Należy usunąć wszystkie wywołania, które zostały użyte do wywołania programu bezpieczeństwa (Main_Safety).

Usuwanie całego programu bezpieczeństwa z F-CPU S7-300/400 *z* włożoną kartą pamięci (karta pamięci SIMATIC Micro lub karta flash)

Aby usunąć cały program bezpieczeństwa, należy wykonać co następuje:

1. Usunąć wszystkie bloki bezpieczeństwa (wskazane żółtym symbolem) z drzewka projektu.
2. Usunąć wszystkie wywołania, które zostały użyte do wywołania programu bezpieczeństwa (Main_Safety).
3. Wybrać F-CPU w *edytorze sprzętu i sieci*, po czym odznaczyć opcję „F-capability activated" (Kompatybilność bezpieczeństwa włączona) we właściwościach F-CPU.
4. Skompilować dane projektu dla F-CPU

   Projekt offline nie zawiera już programu bezpieczeństwa.

   Aby usunąć program bezpieczeństwa z karty pamięci (karta pamięci SIMATIC Micro lub karta flash), należy włożyć kartę do urządzenia programistycznego, PC lub czytnika USB SIMATIC.
5. Wybrać polecenie menu „Project > Card Reader/USB memory > Show Card Reader/USB memory" (Projekt > Czytnik kart/pamięć USB > Pokaż czytnik kart/pamięć USB) w pasku menu.

Następnie można pobrać standardowy program użytkownika offline do F-CPU.

Usuwanie całego programu bezpieczeństwa z F-CPU S7-400 *bez* włożonej karty pamięci

Aby usunąć cały program bezpieczeństwa, należy wykonać co następuje:

1. Usunąć wszystkie bloki bezpieczeństwa (wskazane żółtym symbolem) z drzewka projektu.
2. Usunąć wszystkie wywołania, które zostały użyte do wywołania programu bezpieczeństwa (Main_Safety).
3. Wybrać F-CPU w *edytorze sprzętu i sieci*, po czym odznaczyć opcję „F-capability activated" (Kompatybilność bezpieczeństwa włączona) we właściwościach F-CPU.
4. Skompilować dane projektu dla F-CPU
5. Projekt offline nie zawiera już programu bezpieczeństwa.

Następnie można pobrać standardowy program użytkownika offline do F-CPU.

Usuwanie całego programu bezpieczeństwa z F-CPU SIMATIC S7-1200/1500

Aby usunąć cały program bezpieczeństwa, należy wykonać co następuje:

1. Usunąć wszystkie bloki bezpieczeństwa (wskazane żółtym symbolem) z drzewka projektu.
2. Wybrać F-CPU w *edytorze sprzętu i sieci*, po czym odznaczyć opcję „F-capability activated" (Kompatybilność bezpieczeństwa włączona) we właściwościach F-CPU.
3. Skompilować dane projektu dla F-CPU

   Projekt offline nie zawiera już programu bezpieczeństwa.

Następnie można pobrać standardowy program użytkownika offline do F-CPU.

5.2 Definiowanie grup F-runtime

5.2.1 Zasady grup F-runtime programu bezpieczeństwa

Zasa

Należy mieć na uwadze następujące zagadnienia:

- Dostęp do kanałów (wartości kanałów oraz stan wartości) F-I/O jest możliwy jedynie z pojedynczej grupy F-runtime.
- Dostęp do tagów DB F-I/O jest możliwy tylko z jednej grupy F-runtime i to takiej, z której możliwy jest dostęp do kanałów lub stanu wartości tego F-I/O (jeśli wprowadzono dostęp).
- Możliwe jest użycie F-FB w więcej niż jednej grupie F-runtime, lecz należy wywoływać je z innymi DB instancji.
  Dostęp do DB instancji dla F-FB jest możliwy tylko z grupy F-runtime, w której wywoływany jest powiązany F-FB.
- Tag globalnego F-DB (za wyjątkiem globalnego DB bezpieczeństwa) pozwala na dostęp jedynie z jednej grupy F-runtime (choć można go zastosować w więcej niż jednej grupie F-runtime).
- (S7-300, S7-400) DB do komunikacji grupy F-runtime może być ochroniony przed odczytem i zapisem przez grupę F-runtime, do której został przypisany jako „DB do komunikacji grupy F-runtime", lecz może być jedynie zabezpieczony przed odczytem przez „odbiorczą" grupę F-runtime.
- (S7-300, S7-400) Dostęp do DB komunikacji bezpieczeństwa jest możliwy tylko z jednej grupy F-runtime.
- (S7-1200, S7-1500) Nie należy samodzielnie wywoływać głównego bloku bezpieczeństwa. Jest on automatycznie wywoływany przez przypisany F-OB.

Uwaga

F-OB są chronione przez wiedzę specjalistyczną systemu bezpieczeństwa. Informacja o uruchomieniu OB dla F-OB nie może być poddana ocenie.

- (S7-1200, S7-1500). F-OB należy utworzyć z najwyższym pierwszeństwem ze wszystkich OB.

Uwaga

Czas cyklu F-OB może zostać wydłużony, między innymi, przez obciążenie komunikacyjne, przetwarzanie przerwań o wyższym priorytecie, a także przez funkcje testowania i odbioru technicznego.

- (S7-300, S7-400) Główny blok bezpieczeństwa może zostać wywołany raz ze standardowego bloku. Wiele wywołań może spowodować przejście F-CPU do trybu STOP.
- (S7-300, S7-400) Dla optymalnego wykorzystania tymczasowych danych lokalnych, należy wywołać grupę F-runtime (główny blok bezpieczeństwa) bezpośrednio w OB (OB przerwania cyklicznego, jeśli to możliwe); nie należy deklarować żadnych dodatkowych tymczasowych danych lokalnych w tym OB przerwania cyklicznego.

- (S7-300, S7-400) W OB przerwania cyklicznego, grupa F-runtime powinna być wykonywana **przed** standardowym programem użytkownika, tj. powinna być wywołana na samym początku OB, aby grupa F-runtime zawsze była wywoływana ze stałym odstępem czasowym, niezależnie od tego, jak długo trwa przetwarzanie standardowego programu.

  Z tego względu OB przerwania cyklicznego również nie powinien być zakłócany przez przerwania o wyższym pierwszeństwie.
- Obraz procesu wejść i wyjść standardowych I/O, pamięć bitowa oraz tagi DB w standardowym programie użytkownika mogą być dostępne jako tylko do odczytu lub do odczytu/zapisu z więcej niż jednej grupy F-runtime. (zobacz również „Wymiana danych pomiędzy standardowym programem użytkownika a programem bezpieczeństwa" (strona 204)).
- F-FC mogą być wywoływane w więcej niż jednej grupie F-runtime.

Uwaga

Możliwe jest poprawienie wydajności poprzez zapisywanie sekcji programu, które nie są wymagane przez funkcję bezpieczeństwa, w standardowym programie użytkownika.

Podczas określania, które elementy można zawrzeć w standardowym programie użytkownika, a które w programie bezpieczeństwa, należy pamiętać, że standardowy program użytkownika można łatwiej modyfikować i pobierać do F-CPU. Na ogół zmiany w standardowym programie użytkownika nie wymagają zatwierdzenia.

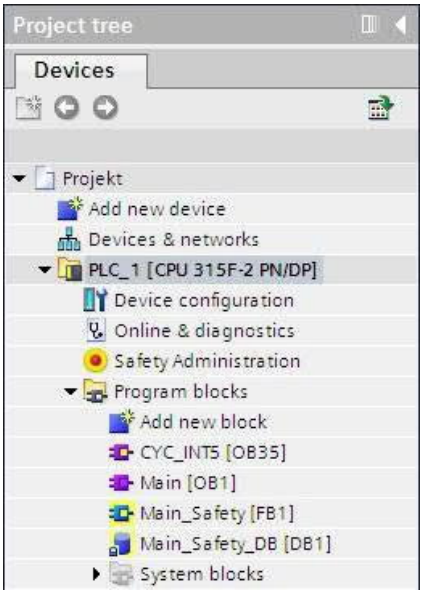
5.2.2 Procedura definiowania grupy F-runtime (S7-300, S7-400)

Wymogi

- Wstawiono F-CPU S7-300/400 F-CPU do projektu.
- W zakładce „Properties" (Właściwości) F-CPU zaznaczone jest pole „F-capability activated" (Kompatybilność bezpieczeństwa włączona) (ustawienie domyślne).

Grupa F-runtime utworzona domyślnie

STEP 7 Safety wstawia bloki bezpieczeństwa dla grupy F-runtime w drzewku projektu domyślnie po dodaniu F-CPU. Po otworzeniu „Program blocks" (Bloki programu), widoczne są bloki (bezpieczeństwa) grupy F-runtime (CYC_INT5 [OB 35], Main_Safety [FB 1] oraz Main_Safety_DB [DB1]) w drzewku projektu.



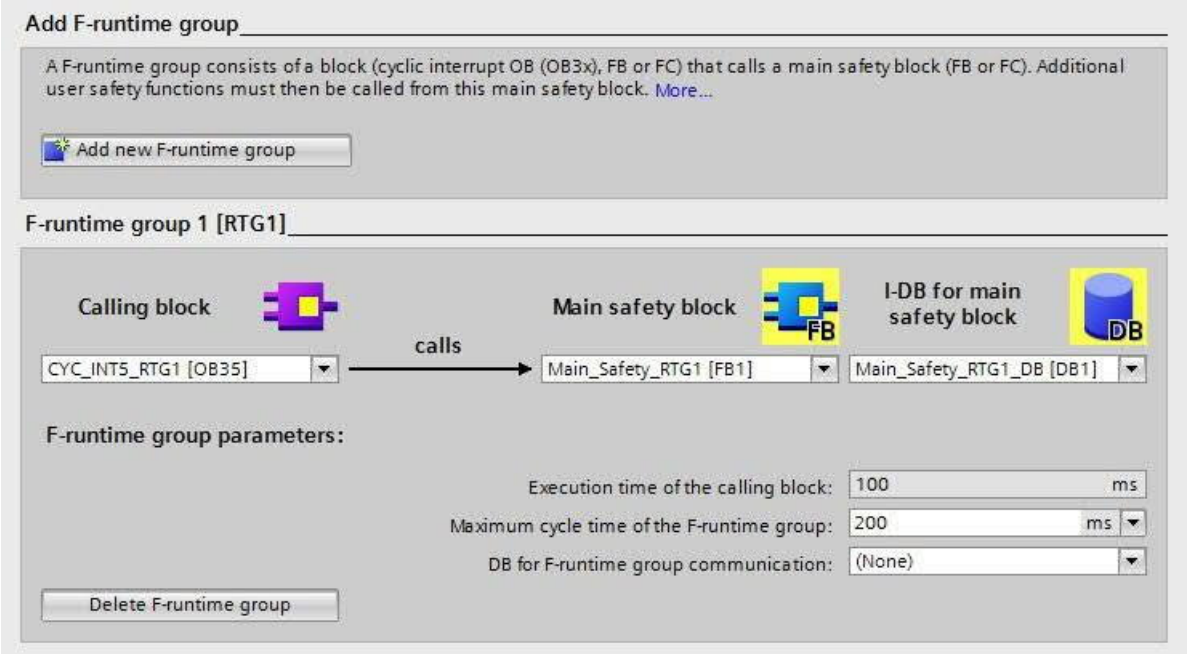
Poniższy dział opisuje sposób modyfikacji ustawień/parametrów grupy F-runtime utworzonej domyślnie lub dodania dodatkowej grupy F-runtime.

Procedura definiowania grupy F-runtime

Aby zdefiniować grupę F-runtime, należy wykonać co następuje:

1. Otworzyć *Safety Administration Editor,* klikając dwukrotnie na drzewku projektu.
2. Wybrać „F-runtime group" (Grupa F-runtime) w nawigacji obszaru.

   Wynik: Otworzy się obszar roboczy do definiowania grupy F-runtime z (domyślnymi) ustawieniami dla grupy F-runtime 1.



3. Określić blok, w którym główny blok bezpieczeństwa ma być wywoływany.

   Domyślnie sugerowany jest tutaj OB przerwania cyklicznego 35. Zaletą zastosowania OB przerwania cyklicznego jest to, że przerywają one wykonywanie programu cyklicznego w OB 1 standardowego programu użytkownika w stałych odstępach czasu; oznacza to, że program bezpieczeństwa jest wywoływany i wykonywany w stałych odstępach czasu w OB przerwania cyklicznego.

   W tym polu wejściowym można wybrać jedynie te bloki, które zostały utworzone w języku LAD, FBD lub STL. Po wybraniu bloku wywołanie jest wstawiane automatycznie do wybranego bloku, a także, jeśli to konieczne, usuwane z poprzednio wybranego bloku.

   Aby wywołać główny blok bezpieczeństwa w bloku, który został utworzony w innym języku programowania, należy samodzielnie zaprogramować to wywołanie. Pole wejściowe nie pozwala na edycję (jest wyszarzone) i możliwa jest jedynie zmiana w bloku wywołania, nie w *Safety Administration Editor*.
4. Przypisać żądany główny blok bezpieczeństwa do grupy F-runtime. Jeśli główny blok bezpieczeństwa to FB, należy również zapewnić instancję DB.

   Main_Safety [FB1] oraz Main_Safety_DB [DB1] są sugerowane domyślnie.

5. F-CPU monitoruje czasu cyklu dla grupy F-runtime. W przypadku „Maximum cycle time of F-runtime group" (Maksymalny czas cyklu grupy F-runtime), należy wprowadzić maksymalny dopuszczalny czas pomiędzy dwoma wywołaniami grupy F-runtime.

OSTRZEŻENIE

Interwał wywołania grupy F-runtime jest monitorowany dla wartości maksymalnej, tj. monitorowanie jest wykonywane w celu określenia, czy wywoływanie jest wykonywane wystarczająco często, lecz nie czy jest wykonywane zbyt często, lub, na przykład, izochronicznie. Dlatego też należy zastosować zegary fail-safe przy użyciu instrukcji TP, TON lub TOF (strona 520) z karty zadań „Instructions" (Instrukcje), bez stosowania liczników (wywołań OB). *(S007)*

OSTRZEŻENIE

Czas odpowiedzi funkcji bezpieczeństwa zależy, między innymi, od czasu cyklu F-OB, czasu pracy grupy F-runtime, oraz, w przypadku stosowania rozproszonego F-I/O, przypisania parametrów PROFINET/PROFIBUS.

Dlatego też przypisanie parametrów/konfiguracja standardowego systemu wpływa na czas odpowiedzi funkcji bezpieczeństwa.

Przykłady:

- Zwiększenie pierwszeństwa standardowego OB w porównaniu do F-OB może wydłużyć czas cyklu dla F-BO lub czas pracy grupy F-runtime ze względu na przetwarzanie priorytetowe standardowego OB. Należy pamiętać, że podczas tworzenia obiektów technologicznych, mogą zostać automatycznie utworzone OB o bardzo wysokim priorytecie.
- Zmiana w cyklu zegara wysyłania PROFINET zmienia czas cyklu F-OB z klasą zdarzenia „Cykl synchroniczny".

Należy pamiętać, że konfiguracja / przypisanie parametrów standardowego systemu nie podlega ochronie dostępu do programu bezpieczeństwa i nie prowadzi do modyfikacji zbiorczego podpisu bezpieczeństwa.

Jeśli nie zastosowano środków organizacyjnych mających na celu uniemożliwienie zmian w konfiguracji / przypisaniu parametrów standardowego systemu z wpływem na czas odpowiedzi, należy zawsze korzystać z czasów monitorowania do obliczania maksymalnego czasu odpowiedzi funkcji bezpieczeństwa (patrz „Konfigurowanie czasów monitorowania" (strona 650)).

Czasy monitorowania są chronione przed zmianą za pomocą ochrony dostępu programu bezpieczeństwa i są rejestrowane przez zbiorczy podpis bezpieczeństwa, a także przez zbiorczy podpis F-SW,

W przypadku korzystania z arkusza kalkulacyjnego do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100), należy uwzględnić wartość, która została określona dla „Any standard system runtimes" (Dowolne czasy pracy standardowego systemu) jako wartość maksymalnego czasu odpowiedzi. *(S085)*

6. Jeśli jedna grupa F-runtime ma zapewniać tagi do oceny do drugiej grupy w programie bezpieczeństwa, należy przypisać DB do komunikacji grupy F-runtime. Należy wybrać F-DB dla „DB for F-runtime group communication" (DB do komunikacji grupy F-runtime). (Zobacz także Komunikacja grupy F-runtime (S7-300, S7-400) (strona 150))
7. Aby utworzyć **drugą grupę F-runtime**, należy kliknąć na przycisk „Add new F-runtime group" (Dodaj nową grupę F-runtime).

8. Przypisać F-FB lub F-FC jako główny blok bezpieczeństwa do bloku wywołania. Ten F-FB lub F-FC jest automatycznie generowany w drzewku projektu, jeśli nie jest jeszcze obecny.
9. Jeśli główny blok bezpieczeństwa to F-FB, należy przypisać do niego instancję DB. Instancja DB jest generowana automatycznie w drzewku projektu.
10. Należy wykonać kroki 3 – 5 powyżej, aby ukończyć tworzenie drugiej grupy F-runtime.

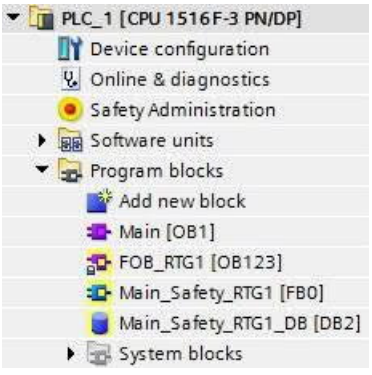
5.2.3 Procedura definiowania grupy F-runtime (S7-1200, S7-1500)

Wymogi

- Wstawiono F-CPU S7-1200/1500 F-CPU do projektu.
- W zakładce „Properties" (Właściwości) F-CPU zaznaczone jest pole „F-capability activated" (Kompatybilność bezpieczeństwa włączona) (ustawienie domyślne).

Grupa F-runtime utworzona domyślnie

STEP 7 Safety wstawia bloki bezpieczeństwa dla grupy F-runtime w drzewku projektu domyślnie po dodaniu F-CPU. Po otworzeniu „Program blocks" (Bloki programu), widoczne są bloki (bezpieczeństwa) grupy F-runtime (FOB_RTG1 [OB123], Main_Safety_RTG1 [FB1] oraz Main_Safety_RTG1_DB [DB1]) w drzewku projektu.



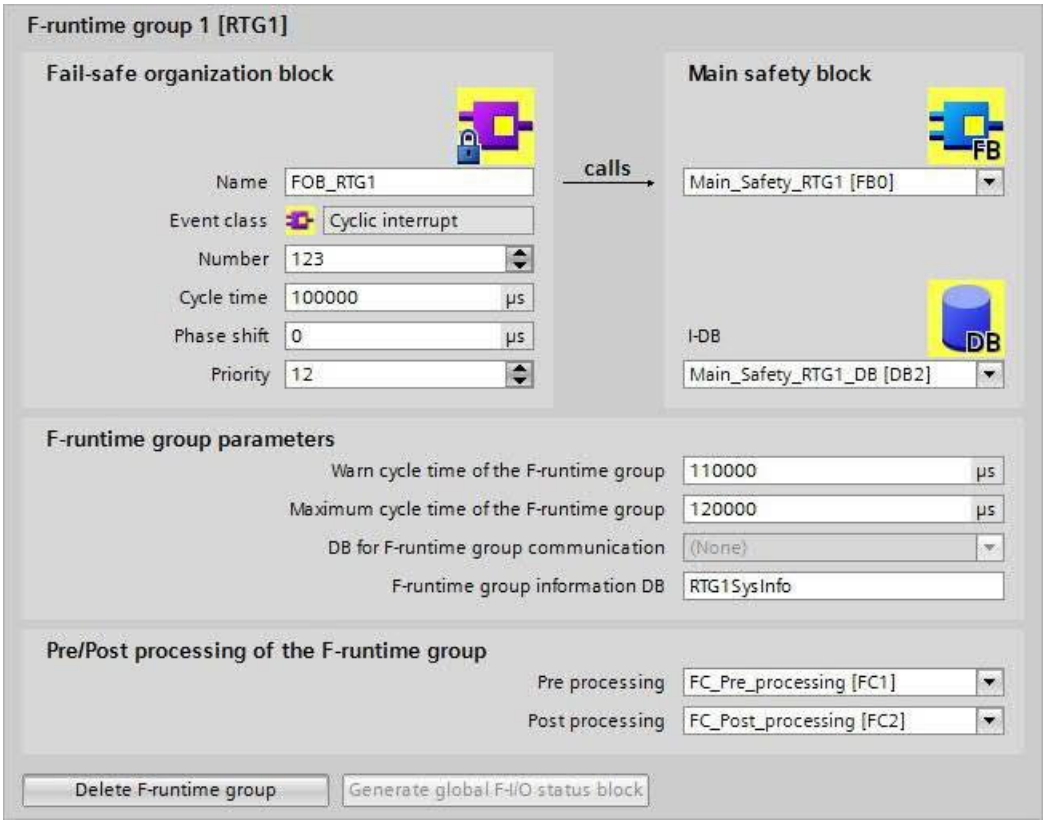
Poniższy dział opisuje sposób modyfikacji ustawień/parametrów grupy F-runtime utworzonej domyślnie lub dodania dodatkowej grupy F-runtime.

Procedura definiowania grupy F-runtime

Aby zdefiniować grupę F-runtime, należy wykonać co następuje:

1. Otworzyć *Safety Administration Editor,* klikając dwukrotnie na drzewku projektu.
2. Wybrać „F-runtime group" (Grupa F-runtime) w nawigacji obszaru.

   Wynik: Otworzy się obszar roboczy do definiowania grupy F-runtime z (domyślnymi) ustawieniami dla grupy F-runtime 1.



3. Należy przypisać nazwę do F-OB, pod „F-OB".

4. Określić klasę zdarzenia dla F-OB podczas tworzenia nowej grupy F-runtime.
   W przypadku F-OB można wybrać pomiędzy klasami zdarzenia „Program cycle" (Cykl programu), „Cyclic interrupt" (Przerwanie cykliczne) lub „Synchronous cycle" (Cykl synchroniczny).

   W przypadku grupy F-runtime utworzonej domyślnie, F-OB ma klasę zdarzenia „Cyclic interrupt" (Przerwanie cykliczne). Aby zmienić klasę zdarzenia F-OB już utworzonej grupy F-runtime, należy usunąć grupę i utworzyć nową.

   Uwaga

   Zaleca się tworzenie F-OB z klasą zdarzenia „Cyclic interrupt" (Przerwanie cykliczne) jako „cyclic interrupt OB" (OB przerwania cyklicznego). Program bezpieczeństwa będzie wtedy wywoływany i uruchamiany w stałych odstępach czasu.

   F-OB z klasą zdarzenia „Synchronous cycle" (Cykl synchroniczny) są zalecane jedynie w połączeniu z urządzeniami F-I/O, które obsługują tryb izochroniczny, na przykład submoduł „Profisafe Telgr 902" do sterownika SINAMICS S120 CU310-2 PN V5.1.

   Uwaga

   Należy zwrócić uwagę na maksymalną dopuszczalną liczbę OB (w tym F-OB) z klasą zdarzenia „Synchronous cycle" (Cykl synchroniczny) (patrz specyfikacja techniczna w instrukcji produktu CPU S7-1500).

5. Jeśli to wymagane, można ręcznie zmienić liczbę F-OB proponowaną przez system. W tym celu należy uwzględnić zakresy obowiązujące dla danej klasy zdarzenia.
6. Przypisać czas cyklu, przesunięcie fazowe oraz parametry pierwszeństwa dla F-OB z klasą zdarzenia „Cyclic interrupt" (Przerwanie cykliczne).

   Przypisać parametr pierwszeństwa do F-OB z klasą zdarzenia „Synchronous cycle"

   - Należy wybrać czas cyklu mniejszy niż „Maximum cycle time of F-runtime group" (Maksymalny czas cyklu grupy F-runtime) oraz mniejszy niż „Cycle time warning limit of F-runtime group" (Limit ostrzeżenia czasu cyklu grupy F-runtime).
   - Ustawić przesunięcie fazowe mniejsze niż czas cyklu.
   - Jeśli to możliwe, ustawić pierwszeństwo wyższe niż pierwszeństwo pozostałych OB.

   Uwaga

   Poprzez wysokie pierwszeństwo F-OB gwarantuje się, że czas pracy programu bezpieczeństwa oraz czas odpowiedzi funkcji bezpieczeństwa (strona 650) są możliwie minimalnie zakłócane przez standardowy program użytkownika.

   Uwaga

   W przypadku F-OB z klasą zdarzenia „Synchronous cycle" (Cykl synchroniczny) należy również przypisać parametry co cyklu aplikacji (ms) oraz możliwy czas opóźnienia (ms) po zdefiniowaniu grupy F-runtime oraz połączeniu izochronicznego F-I/O do OB przerwania trybu izochronicznego. Parametry te znajdują się w oknie „Properties" (Właściwości) OB przerwania trybu izochronicznego w grupie „Isochronous mode" (Tryb izochroniczny). Należy postępować zgodnie z opisem w pomocy STEP 7 pod hasłem „Konfiguracja OB przerwania trybu izochronicznego".

7. Przypisać wywołanie głównego bloku bezpieczeństwa do F-OB. Jeśli główny blok bezpieczeństwa to FB, należy również zapewnić instancję DB.

   Main_Safety_RTG1 [FB1] oraz Main_Safety_RTG1_DB [DB1] są sugerowane domyślnie.

8. F-CPU monitoruje czasu cyklu dla grupy F-runtime. Dostępne są dwa parametry:

   – Jeśli „Cycle time warning limit of F-runtime group" (Limit ostrzegawczy czasu cyklu grupy F-runtime) zostanie przekroczony, wykonywany jest wpis do bufora diagnostycznego F-CPU. Parametr ten pozwala, przykładowo, na określenie, czy czas cyklu przekracza wymaganą wartość bez przełączenia F-CPU do trybu STOP.

   – Jeśli „Maximum cycle time of F-runtime group" (Maksymalny czas cyklu grupy F-runtime) zostanie przekroczony, F-CPU przechodzi w tryb STOP. W przypadku „Maximum cycle time of F-runtime group" (Maksymalny czas cyklu grupy F-runtime), należy wybrać maksymalny dopuszczalny czas pomiędzy dwoma wywołaniami grupy F-runtime (maksymalnie 20000000 µs).

OSTRZEŻENIE

Interwał wywołania grupy F-runtime jest monitorowany dla wartości maksymalnej, tj. monitorowanie jest wykonywane w celu określenia, czy wywoływanie jest wykonywane wystarczająco często, lecz nie czy jest wykonywane zbyt często, lub, na przykład, izochronicznie. Dlatego też należy zastosować zegary fail-safe przy użyciu instrukcji TP, TON lub TOF (strona 520) z karty zadań „Instructions" (Instrukcje), bez stosowania liczników (wywołań OB). *(S007)*

OSTRZEŻENIE

Czas odpowiedzi funkcji bezpieczeństwa zależy, między innymi, od czasu cyklu F-OB, czasu pracy grupy F-runtime, oraz, w przypadku stosowania rozproszonego F-I/O, przypisania parametrów PROFINET/PROFIBUS.

Dlatego też przypisanie parametrów/konfiguracja standardowego systemu wpływa na czas odpowiedzi funkcji bezpieczeństwa.

Przykłady:

- Zwiększenie pierwszeństwa standardowego OB w porównaniu do F-OB może wydłużyć czas cyklu dla F-OB lub czas pracy grupy F-runtime ze względu na przetwarzanie priorytetowe standardowego OB. Należy pamiętać, że podczas tworzenia obiektów technologicznych, mogą zostać automatycznie utworzone OB o bardzo wysokim priorytecie.
- Zmiana w cyklu zegara wysyłania PROFINET zmienia czas cyklu F-OB z klasą zdarzenia „Cykl synchroniczny".

Należy pamiętać, że konfiguracja / przypisanie parametrów standardowego systemu nie podlega ochronie dostępu do programu bezpieczeństwa i nie prowadzi do modyfikacji zbiorczego podpisu bezpieczeństwa.

Jeśli nie zastosowano środków organizacyjnych mających na celu uniemożliwienie zmian w konfiguracji / przypisaniu parametrów standardowego systemu z wpływem na czas odpowiedzi, należy zawsze korzystać z czasów monitorowania do obliczania maksymalnego czasu odpowiedzi funkcji bezpieczeństwa (patrz „Konfigurowanie czasów monitorowania" (strona 650)).

Czasy monitorowania są chronione przed zmianą za pomocą ochrony dostępu programu bezpieczeństwa i są rejestrowane przez zbiorczy podpis bezpieczeństwa, a także przez zbiorczy podpis F-SW,

W przypadku korzystania z arkusza kalkulacyjnego do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100), należy uwzględnić wartość, która została określona dla „Any standard system runtimes" (Dowolne czasy pracy standardowego systemu) jako wartość maksymalnego czasu odpowiedzi. *(S085)*

„Cycle time warning limit of F-runtime group" Limit ostrzeżenia czasu cyklu grupy F-runtime) należy skonfigurować jako mniejszy bądź równy „Maximum cycle time of F-runtime group" (Maksymalny czas cyklu grupy F-runtime).

9. Przypisać nazwę do DB informacji o grupie F-runtime (strona 158) pod „F-runtime group DB" (DB grupy F-runtime).

10. Jeśli to konieczne, można wybrać bloki standardowego programu (FC) w przypadku przetwarzania wstępnego lub końcowego grupy F-runtime (patrz „Przetwarzanie wstępne/końcowe (S7- 1200, S7-1500)" (strona 86))
11. Aby utworzyć **drugą grupę F-runtime**, należy kliknąć na przycisk „Add new F-runtime group" (Dodaj nową grupę F-runtime). Należy wykonać kroki 3 – 10 powyżej.

5.2.4 Komunikacja grupy F-runtime (S7-300, S7-400)

Komunikacja safety pomiędzy grupami F-runtime

Komunikacja safety może odbywać się pomiędzy dwoma grupami F-runtime programu bezpieczeństwa. Oznacza to, że tagi fail-safe mogą być zapewnione przez jedną grupę F-runtime w F-DB i odczytane w innej grupie.

Uwaga

DB do komunikacji grupy F-runtime może być ochroniony przed odczytem i zapisem przez grupę F-runtime, do której został przypisany jako „DB do komunikacji grupy F-runtime", podczas gdy może być jedynie zabezpieczony przed odczytem przez „odbiorczą" grupę F-runtime.

Wskazówka: Poprawa wydajności jest możliwa poprzez ukształtowanie programu bezpieczeństwa w taki sposób, by pomiędzy grupami F-runtime było wymieniane jak najmniej tagów.

Procedura definiowania DB do komunikacji grupy F-runtime

DB do komunikacji grupy F-runtime definiuje się w obszarze roboczym „F-runtime groups" (Grupy F-runtime). Należy wykonać co następuje:

1. Kliknąć na „F-runtime groups" (Grupy F-runtime) w „*Safety Administration Editor*".
2. Wybrać istniejący F-DB w polu „DB for F-runtime group communication" (DB do komunikacji grupy F-runtime) lub przypisać nowy.
3. Przypisać nazwę do F-DB.

Aktualność odczytu tagów z innej grupy F-runtime

Uwaga

Odczyt tagów jest aktualizowany w czasie ostatniego ukończonego cyklu przetwarzania grupy F-runtime, o ile tagi są dostępne przed rozpoczęciem ich odczytu przez grupę F-runtime.

Jeśli zapewnione tagi przejdą wiele zmian podczas czasu pracy grupy F-runtime zapewniające je, grupa F-runtime odczytująca tagi otrzyma jedynie ostatnią zmianę (patrz ilustracja poniżej).

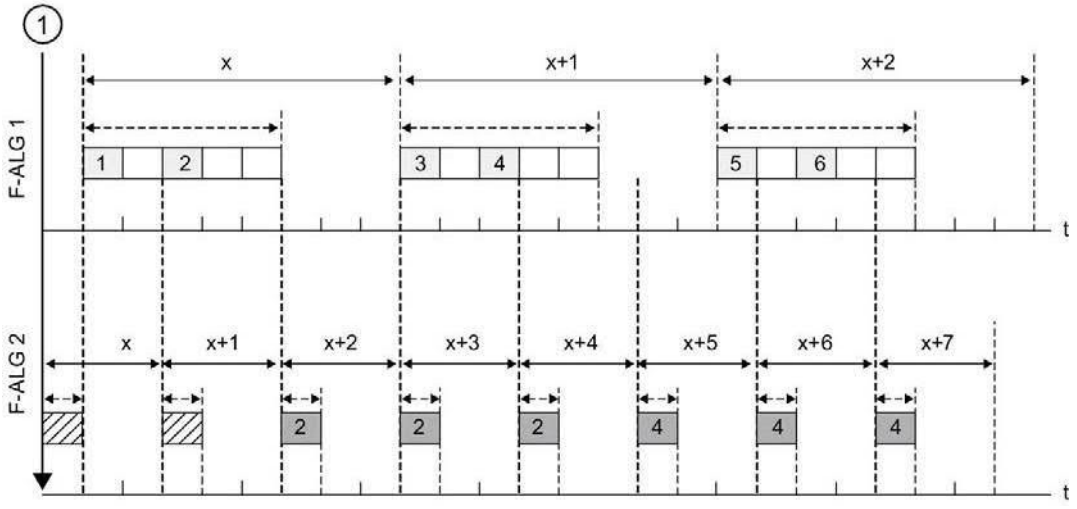
Przypisanie wartości fail-safe

Po uruchomieniu systemu bezpieczeństwa wartości fail-safe są dostarczane do grupy F-runtime mające dostęp do odczytu tagów w DB do komunikacji grupy F-runtime innej grupy (przykładowo, grupy F-runtime 2). Są to wartości określone jako wartości początkowe w DB do komunikacji grupy F-runtime 1.

Grupa F-runtime 2 odczytuje wartości fail-safe przy jej pierwszym wywołaniu. Przy drugim wywołaniu grupy F-runtime 2 odczytuje ona najnowsze tagi, jeśli grupa F-runtime 1 została przetworzona w pełni pomiędzy dwoma wywołaniami grupy F-runtime 2. Jeśli grupa F-runtime 1 nie została przetworzona w pełni, grupa F-runtime 2 kontynuuje odczyt wartości fail-safe, aż grupa F-runtime 1 zostanie w pełni przetworzona.

Ich zachowanie zostało przedstawione na poniższych dwóch ilustracjach.

Odczyt tagów z grupy F-runtime 1, która ma dłuższy cykl OB i niższy priorytet niż grupa F-runtime 2



① Rozruch systemu bezpieczeństwa

Czas cyklu (F-)OB, w którym wywoływana jest grupa F-runtime.

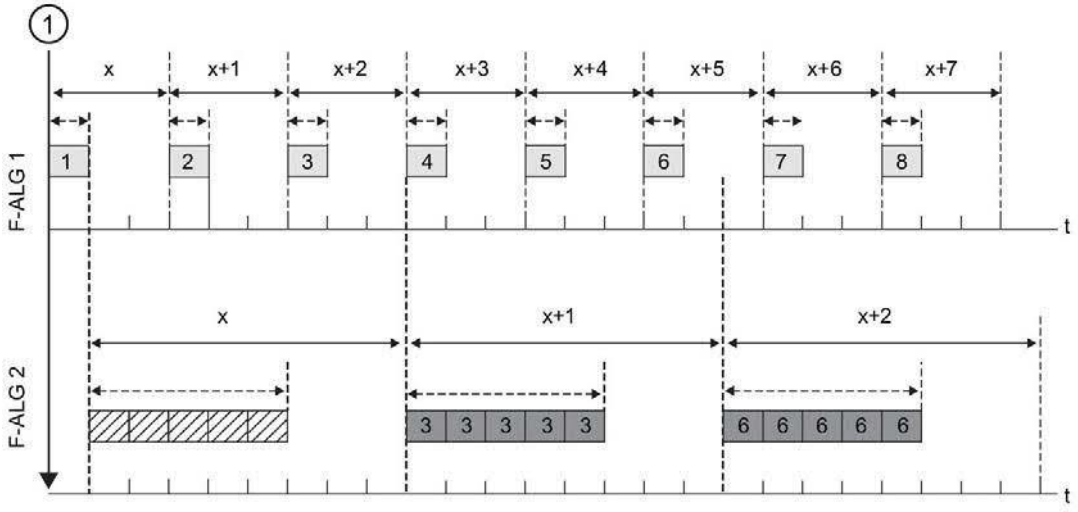
Czas pracy grupy F-runtime

1 ... Tag grupy F-runtime 1, zapisany do DB dla komunikacji grupy F-runtime w grupie F-runtime 1

2 ...Tag grupy F-runtime 2, odczytany w DB dla komunikacji grupy F-runtime w grupie F-runtime 1

Wartość początkowa w DB do komunikacji grupy F-runtime

Odczyt tagów z grupy F-runtime 1, która ma krótszy cykl OB i wyższy priorytet niż grupa F-runtime 2



① Rozruch systemu bezpieczeństwa

Czas cyklu (F-)OB, w którym wywoływana jest grupa F-runtime.

Czas pracy grupy F-runtime

1 ... Tag grupy F-runtime 1, zapisany do DB dla komunikacji grupy F-runtime w grupie F-runtime 1

2 ... Tag grupy F-runtime 2, odczytany w DB dla komunikacji grupy F-runtime w grupie F-runtime 1

Wartość początkowa w DB do komunikacji grupy F-runtime

Grupa F-runtime- brak przetwarzania zapewnionych tagów

Uwaga

Jeśli grupa F-runtime, której DB do komunikacji grupy F-runtime służy do zapewniania tagów, nie jest przetwarzana (główny blok bezpieczeństwa grupy F-runtime nie jest wywoływany), F-CPU przechodzi w tryb STOP. Jedno z poniższych zdarzeń diagnostycznych jest wprowadzane do bufora diagnostycznego F-CPU:

- Błąd w programie bezpieczeństwa: przekroczono czas cyklu
- Liczba istotnych głównych bloków bezpieczeństwa (grupy F-runtime, która nie jest przetwarzana)

5.2.5 Komunikacja grupy F-runtime (S7-1200, S7-1500)

Wstęp

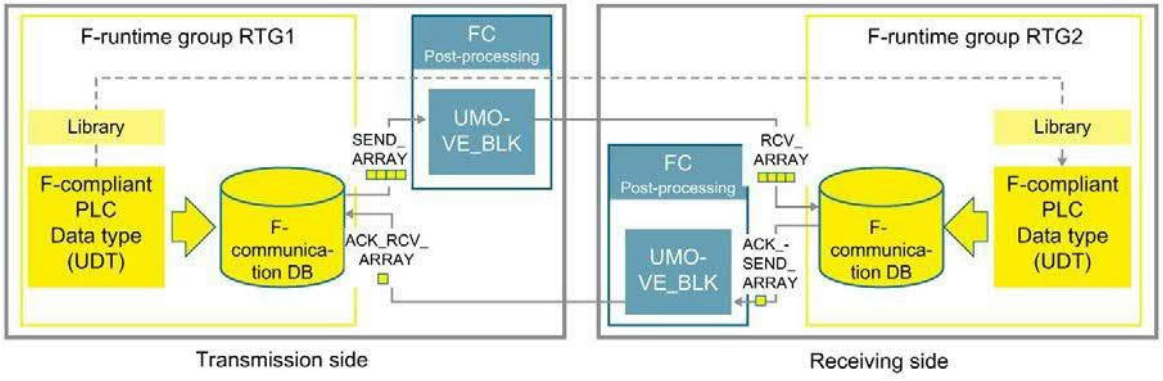
Przy pomocy Flexible F-Link wykonuje się komunikację grupy F-runtime.

Przy pomocy Flexible F-Link możliwe jest wykonanie kodowanej tablicy bezpieczeństwa do danych wysyłanych z grupy F-runtime. Kodowana tablica bezpieczeństwa jest przenoszona do innej grupy F-runtime przy pomocy standardowych instrukcji, takich jak UNMOVE_BLK.

Wymogi

- F-CPU S7-1500 z oprogramowaniem V2.0
- F-CPU S7-1200 z oprogramowaniem V4.2
- Wersja systemu bezpieczeństwa od V2.2

Komunikacja grupy F-runtime



Aby wysłać dane fail-safe z jednej grupy F-runtime do drugiej, należy wykonać następujące kroki:

1. Utworzyć rodzaj danych PLC zgodnych z bezpieczeństwem (UUID) dla komunikacji grupy F-runtime. Rozmiar może wynosić do 100 bajtów.
2. Utworzyć dwie komunikacje bezpieczeństwa dla komunikacji grupy F-runtime w Safety Administration Editor w obszarze „Flexible F-Link". Po jednej komunikacji bezpieczeństwa po stronie wysyłania oraz odbierania.
3. Należy skonfigurować ten sam czas monitorowania bezpieczeństwa oraz komunikację bezpieczeństwa UUID dla obu komunikacji grup F-runtime.

   Informacje dotyczące obliczania czasów monitorowania bezpieczeństwa można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

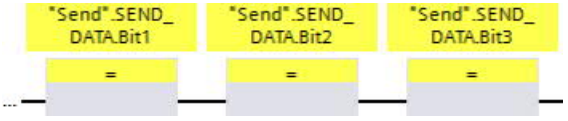
   Przykładowo:

Flexible F-Link settings

	Name	PLC Data Type	Direction	F-monitoring time: (ms)	F-communication UUID
1	Send	Data	Send	500	5d61f443-ede6-4e4e-9db6-e79af634f9ad
2	Receive	Data	Receive	500	2c85b9e5-da34-422d-98eb-f7136309a3a2

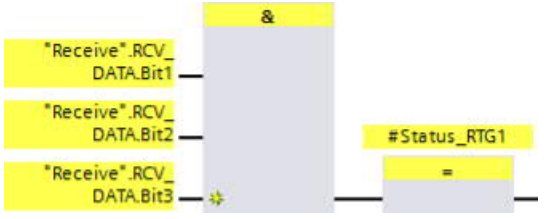
4. Po stronie wysyłania (np. RTG1) należy zapewnić dane do DB transmisji z danymi do wysłania.

   Przykładowo:

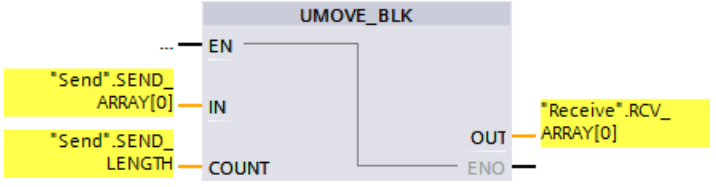


5. Odczytać dane odebrane z DB odbierającego po stronie odbioru (np. RTG2).

   Przykładowo:

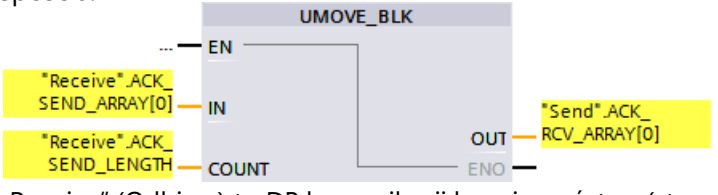


6. Należy wywołać instrukcję „UMOVE_BLK" w grupie F-runtime do danych wysyłanych (np. RTG1) w FC do przetwarzania końcowego (strona 86).
7. Należy połączyć instrukcję „UMOVE_BLK" do danych do wysłania w następujący sposób:



   „Send" (Wyślij) to DB komunikacji bezpieczeństwa (strona 98) grupy F-runtime, który wysyła dane.

   „Receive" (Odbierz) to DB komunikacji bezpieczeństwa (strona 98) grupy F-runtime, który odbiera dane.
   Należy wywołać instrukcję „UMOVE_BLK" w grupie F-runtime do zatwierdzenia (np. RTG2) w FC do przetwarzania końcowego (strona 98).
8. Należy połączyć instrukcję „UMOVE_BLK" do połączenia zatwierdzenia w następujący sposób:



   „Receive" (Odbierz) to DB komunikacji bezpieczeństwa (strona 98) grupy F-runtime, który wysyła telegram zatwierdzenia.

   „Send" (Wyślij) to DB komunikacji bezpieczeństwa (strona 98) grupy F-runtime, który odbiera telegram zatwierdzenia.

9. Skompilować program użytkownika.
10. Należy pobrać program użytkownika do F-CPU.

OSTRZEŻENIE

Podczas akceptacji należy skorzystać z podsumowania bezpieczeństwa, by sprawdzić, czy przesunięcia wszystkich elementów rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) są zgodne z wysyłanymi i odbieranymi danymi w ramce wiadomości bezpieczeństwa. Z tego względu wszystkie elementy i adresy są wyszczególnione w podsumowaniu bezpieczeństwa dla UDT. *(S088)*

OSTRZEŻENIE

Gdy w Safety Administration Editor tworzona jest nowa komunikacja Flexible F-Link, unikalny UUID komunikacji bezpieczeństwa jest zapewniany przez system. Poprzez skopiowanie komunikacji w Safety Administration Editor w obrębie tabeli parametryzacji lub podczas kopiowania do innego F-CPU, UUID komunikacji bezpieczeństwa nie są ponownie generowane, przez co tracą swoją unikalność. Jeśli do konfigurowania nowego związku komunikacji wykorzystywana jest kopia, należy samodzielnie zapewnić unikalność. W tym celu należy wybrać dane UUID i wygenerować je ponownie poprzez menu kontekstowe „Generate UUID" (Wygeneruj UUID). Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas zatwierdzenia. *(S087)*

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawce i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Aktualność odczytu tagów z innej grupy F-runtime

Mają zastosowanie te same stwierdzenia co w dziale „Komunikacja grupy F-runtime (S7-300, S7-400) (strona 150)" (za wyjątkiem lokacji rejestrowania do zapisu lub odczytu oraz wartości początkowych).

5.2.6 F- Shared DB (S7-300, S7-400)

Funkcja

F- Shared DB to blok danych typu fail-safe, zawierający wszystkie współdzielone dane programu bezpieczeństwa oraz dodatkowe informacje wymagane przez system bezpieczeństwa. DB współdzielone typu F jest automatycznie wstawiane podczas kompilowania konfiguracji sprzętowej.

Przy pomocy nazwy F_GLOBDB można ocenić określone elementy danych programu bezpieczeństwa w standardowym programie użytkownika.

Odczyt F-Shared DBw standardowym programie użytkownika

W DB współdzielonym typu F w standardowym programie użytkownika lub w systemie kontroli operatorskiej i monitorowania można odczytać następujące informacje:

- Tryb roboczy: tryb bezpieczeństwa lub wyłączony trybie bezpieczeństwa (tag „MODE")
- Informacja o błędzie „Error occurred when executing safety program" (Wystąpił błąd podczas wykonywania programu bezpieczeństwa) (tag „ERROR")
- Zbiorczy podpis bezpieczeństwa (tag „F_PROG_SIG")
- Dane kompilacji programu bezpieczeństwa (tag „F_PROG_DAT", rodzaj danych DATE_AND_TIME)

Dostęp do tagów jest możliwy poprzez w pełni kwalifikowany dostęp (np. „"F_GLOBDB".MODE").

5.2.7 DB informacji grupy F-runtime (S7-1200, S7-1500)

Wstęp

DB informacji o grupie F-runtime zapewnia kluczowe informacje o odnośnej grupie F-runtime oraz całym programie bezpieczeństwa.

DB informacji o grupie F-runtime jest tworzony automatycznie podczas tworzenia grupy F-runtime. Symbol, na przykład „RTG1SysInfo", jest przypisywany do DB informacji o grupie F-runtime. Nazwę można zmienić w *Safety Administration Editor*.

Informacje w DB informacji o grupie F-runtime

DB informacji o grupie F-runtime zapewnia następujące informacje:

Nazwa		Rodzaj danych	Do przetwarzania w programie	Do przetwarzania w standardowym programie	Opis
MODE		BOOL	x	x	1 = Wyłączony tryb bezpieczeństwa
F_SYSINFO					
	MODE	BOOL	—	x	1 = Wyłączony tryb bezpieczeństwa
	TCYC_CURR	DINT	—	x	Bieżący czas cyklu grupy F-runtime, w ms
	TCYC_LONG	DINT	—	x	Najdłuższy czas cyklu grupy F-runtime, w ms
	TRTG_CURR	DINT	—	x	Bieżący czas pracy grupy F-runtime, w ms
	TRTG_LONG	DINT	—	x	Najdłuższy czas pracy grupy F-runtime, w ms
	T1RTG_CURR	DINT	—	x	Nie obsługiwane przez *STEP 7 Safety*
	T1RTG_LONG	DINT	—	x	Nie obsługiwane przez *STEP 7 Safety*
	F_PROG_SIG	DWORD	—	x	Zbiorczy podpis bezpieczeństwa programu bezpieczeństwa
	F_PROG_DAT	DTL	—	x	Dane kompilacji programu
	F_RTG_SIG	DWORD	—	x	Podpis grup F-runtime
	F_RTG_DAT	DTL	—	x	Dane kompilacji grupy F-runtime
	VERS_S7SAF	DWORD	—	x	Identyfikator wersji dla *STEP 7 Safety*

Dostęp do treści DB informacji o grupie F-runtime jest możliwy poprzez w pełni kwalifikowane adresowanie. Zarówno zbiorczo przy rodzaju danych PLC F_SYSINFO PLC (UDT), przykładowo, „RTG1SysInfo.F_SYSINFO", zapewnionym przez system bezpieczeństwa, lub indywidualne informacje, na przykład, „RTG1SysInfo.F_SYSINFO.MODE".

Zobacz także

Identyfikacja programu (strona 352)

5.2.8 Usuwanie grup F-runtime

Usuwanie grup F-runtime

Aby usunąć grupę F-runtime, należy wykonać:

1. W nawigacji obszaru *Safety Administration Editor* kliknąć na grupę F-runtime do usunięcia.
2. Wybrać przycisk „Delete F-runtime group" (Usuń grupę F-runtime) w obszarze roboczym.
3. Zatwierdzić okno przyciskiem „Yes" (Tak).
4. Skompilować program bezpieczeństwa (strona 323) (polecenie menu „Edit > Compile" (Edytuj > Kompiluj)), by zastosować zmiany.

Przypisanie bloków bezpieczeństwa do grupy F-runtime (do bloku wywołania głównego bloku bezpieczeństwa) jest usuwane. Jednakże, blok bezpieczeństwa dalej istnieje.

5.2.9 Zmiana grupy F-runtime (S7-300, S7-400)

Zmiana grup F-runtime

Dla każdej grupy F-runtime w programie bezpieczeństwa w odnośnym obszarze roboczym „F-runtime group" (Grupa F-runtime) można wprowadzić następujące zmiany:

- Określić kolejny blok jako blok wywołania głównego bloku bezpieczeństwa.
- Określić kolejny F-FB lub F-FC jako główny blok bezpieczeństwa.
- Wprowadzić inny lub nowy I-DB do głównego bloku bezpieczeństwa.
- Zmienić wartość dla maksymalnego czasu cyklu dla grupy F-runtime.
- Określić kolejny DB jako blok danych do komunikacji grupy F-runtime.

5.2.10 Zmiana grupy F-runtime (S7-1200, S7-1500)

Zmiana grup F-runtime

Dla każdej grupy F-runtime w programie bezpieczeństwa w odnośnym obszarze roboczym „F-runtime group" (Grupa F-runtime) można wprowadzić następujące zmiany:

- Zmienić nazwę, numer, czas cyklu, przesunięcie fazowe oraz priorytet F-OB.
- Określić kolejny F-FB lub F-FC jako główny blok bezpieczeństwa.
- Wprowadzić inny lub nowy I-DB do głównego bloku bezpieczeństwa.
- Zmienić wartość dla maksymalnego czasu cyklu oraz limit ostrzeżenia czasu cyklu dla grupy F-runtime.
- Przypisać inną nazwę do DB informacji o grupie F-runtime.
- Określić FC dla przetwarzania wstępnego i końcowego.

5.3 Tworzenie bloków bezpieczeństwa w FBD / LAD

5.3.1 Tworzenie bloków bezpieczeństwa

Wstęp

Aby utworzyć F-FB, F-FC i F-DB dla programu bezpieczeństwa. należy wykonać tę samą podstawową procedurę co przy standardowych blokach. Poniżej przedstawiono jedynie elementy odbiegające od standardowej procedury.

Tworzenie F-FB, F-FC, oraz F-DB

Bloki bezpieczeństwa tworzy się identycznie jak standardowe bloki. Należy wykonać co następuje:

1. Kliknąć dwukrotnie na „Add new block" (Dodaj nowyblok) w polu „Program blocks"
2. (Bloki programu) w drzewku projektu.
   W oknie, które się otworzy, należy wpisać rodzaj, nazwę i język, po czym zaznaczyć
3. pole „Create F-block" (Utwórz blok bezpieczeństwa). (Nie zaznaczenie tego pola spowoduje utworzenie standardowego bloku.)

   Po zatwierdzeniu okna otworzy się blok bezpieczeństwa w *edytorze programu*.

Należy mieć na uwadze następujące zagadnienia

Należy mieć na uwadze następujące ważne instrukcje:

Uwaga

- Nie można zadeklarować parametrów bloku w interfejsie głównego bloku bezpieczeństwa, ponieważ nie można ich doprowadzić.
- Możliwa jest edycja wartości początkowych w instancji DB. Funkcja „Apply actual values" (Zastosuj wartości bieżące) nie jest obsługiwana.
- Nie jest możliwe uzyskanie dostępu do statycznych danych lokalnych w pojedynczej instancji lub wielu instancjach innych F-FB. Zawsze należy inicjalizować wyjścia F-FC. F-CPU może przejść w stan STOP, jeśli powyższa informacja nie zostanie uwzględniona.
- Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU
- Aby przypisać adres z obszaru danych (bloku danych) do formalnego parametru F-FC jako bieżący parametr, należy użyć w pełni kwalifikowanego dostępu DB. (S7-300, S7- 400)
- Dostęp do jego wejść jest możliwy poprzez blok w trybie odczytu, a do wyjść tylko w trybie zapisu.

  Aby uzyskać dostęp do odczytu i zapisu, należy użyć we/wy.
- Dla większej przejrzystości należy przypisać znaczące nazwy do tworzonych bloków bezpieczeństwa.

Kopiowanie/wklejanie bloków bezpieczeństwa

Możliwe jest kopiowanie F-FB, F-FC i F-DB identycznie jak w przypadku bloków standardowego programu użytkownika.

(S7-1200, S7-1500) Nie jest możliwe

kopiowanie F-OB.

Wyjątek:

Nie można kopiować bloków z folderu „Program blocks > System blocks" (Bloki programu > Bloki systemowe).

Zobacz także

Zmiana grupy F-runtime (S7-1200, S7-1500) (strona 160)

5.3.2 Ochrona wiedzy technologicznej

W przypadku bloków bezpieczeństwa ochrony wiedzy technologicznej, należy postępować zgodnie z *pomocą do STEP 7*, pod hasłem „Ochrona bloków".

Wymogi

W przypadku ochrony wiedzy technologicznej bloków bezpieczeństwa należy mieć na uwadze następujące zagadnienia:

- Blok bezpieczeństwa, do którego ma zostać przypisana ochrona wiedzy technologicznej, musi być wywołany w programie bezpieczeństwa.
- Nim możliwe będzie ustawienie ochrony wiedzy technologicznej dla bloku bezpieczeństwa, program bezpieczeństwa musi być spójny. W tym celu należy skompilować (strona 323) program bezpieczeństwa.

Uwaga

W podsumowaniu bezpieczeństwa nie jest podawany kod źródłowy bloków bezpieczeństwa chronionej wiedzy technologicznej Dlatego też należy utworzyć podsumowanie bezpieczeństwa (na przykład by wykonać przegląd kodu lub akceptację bloku bezpieczeństwa) przed ustawieniem ochrony wiedzy technologicznej.

Uwaga

Aby edytować kod programu i/lub interfejs bloku chronionej wiedzy technologicznej, zaleca się, by nie otwierać bloku bezpieczeństwa poprzez wprowadzenie hasła, lecz raczej usunąć całkowicie ochronę i ustawić ją ponownie po skompilowaniu.

Uwaga

(S7-1200, S7-1500) Gdy nazwa bloku bezpieczeństwa chronionej wiedzy technologicznej lub bloków bezpieczeństwa wywoływane przezeń ulegnie zmianie, podpis bloku bezpieczeństwa chronionej wiedzy technologicznej nie ulega zmianie do czasu wprowadzenia hasła podczas otwierania lub usuwania ochrony wiedzy technologicznej.

Uwaga

Gdy stosowane są bloki bezpieczeństwa chronionej wiedzy technologicznej, ostrzeżenia i komunikaty błędów, które mogą powodować zafałszowanie w blokach, mogą być wyświetlane podczas kompilacji programu bezpieczeństwa. Komunikaty błędów i ostrzeżenia zawierają odnośne informacje. Przykład: W bloku bezpieczeństwa chronionej wiedzy technologicznej należy wykonać dostęp do odczytu do taga standardowego programu użytkownika, do którego odbywa się dostęp do zapisu w innym bloku bezpieczeństwa (chronionej wiedzy technologicznej).

W przypadku F-CPU S7-1200/1500, można uzyskać dodatkowe informacje z podsumowania bezpieczeństwa w dziale „Bloki bezpieczeństwa chronionej wiedzy technologicznej w programie bezpieczeństwa".

Zobacz także

Ponowne użycie bloków bezpieczeństwa (strona 163)

5.3.3 Ponowne użycie bloków bezpieczeństwa

Wstęp

Możliwe jest ponowne użycie bloków bezpieczeństwa, które zostały już przetestowane, oraz, jeśli to potrzebne, zatwierdzone w innych programach bezpieczeństwa – bez konieczności kolejnego testowania i zatwierdzania.

Treść bloku bezpieczeństwa można zabezpieczyć, ustawiając ochronę wiedzy

technologicznej.

Podobnie jak w standardowych blokach, możliwe jest zapisanie bloków bezpieczeństwa jako kopii głównych lub rodzajów w bibliotekach globalnych bądź w bibliotece projektu.

Tworzenie dokumentacji bezpieczeństwa dla ponownie używanego bloku bezpieczeństwa

Dla bloku, który ma zostać ponownie wykorzystany, należy utworzyć dokumentację bezpieczeństwa z następującymi informacjami.

F-CPU S7-300/400

- Podpis i podpis wartości początkowej bloku bezp. chronionej wiedzy technologicznej
- Wersje wszystkich zastosowanych instrukcji LAD/FDB.
- Podpisy i podpisy wartości początkowych wszystkich wywołanych bloków bezp.

F-CPU S7-1200/1500

- Podpis bloku bezpieczeństwa chronionej wiedzy technologicznej
- Wersja systemu bezpieczeństwa podczas ustawiania ochrony wiedzy technologicznej
- Wersje wszystkich zastosowanych instrukcji LAD/FDB.
- Podpisy wszystkich wywołanych bloków bezpieczeństwa

Dokumentacja bezpieczeństwa powinna zawierać również opis funkcjonalności bloku bezpieczeństwa, zwłaszcza jeśli jest to chroniona wiedza technologiczna.

Wymagane informacje pozyskuje się poprzez utworzenie podsumowania bezpieczeństwa programu, w którym pierwotnie utworzono, przetestowano i zatwierdzono blok bezpieczeństwa do ponownego użycia.

To podsumowanie może również stanowić dokumentację dla ponownie używanego bloku.

Kontrole podczas korzystania z ponownie używanego bloku bezpieczeństwa

Wykorzystując ponownie blok bezpieczeństwa, należy upewnić się, że:

- Podpis i podpis wartości początkowej (S7-300/400) bloku bezp. pozostały niezmienione.
- (SIMATIC S7-1200, S7-1500) Ustawiono udokumentowaną wersję systemu bezp.
- Ustawiono udokumentowane (lub funkcjonalnie identyczne) wersje instrukcji LAD/FBD. Informacje o wersjach instrukcji są zawarte w opisach instrukcji.
- Stosowane są wywoływane bloki bezpieczeństwa z udokumentowanymi podpisami oraz podpisami wartości początkowych (S7-300/400).

Jeśli nie można wyeliminować konfliktów wersji ze względu na różne zależności, należy skontaktować się z autorem bloku chronionej wiedzy technologicznej w celu uzyskania kompatybilnej, zatwierdzonej wersji.

Zobacz także

Zgodność bloków bezpieczeństwa chronionej wiedzy technologicznej stosowanych w programie bezpieczeństwa z ich dokumentacją bezpieczeństwa. (strona 381)

5.4 Programowanie zabezpieczenia rozruchu

Wstęp

⚠OSTRZEŻENIE

STOP- przykładowo, poprzez urządzenie programistyczne/PC, przełącznik trybu, funkcję komunikacyjną lub instrukcję „STP"

Uruchomienie trybu STOP, przykładowo, za pomocą urządzenia programistycznego/PC, przełącznika trybu, funkcji komunikacyjnej lub instrukcji „STP", a także utrzymanie tego trybu nie jest powiązane z bezpieczeństwem. Taki stan STOP można łatwo (i nieumyślnie) cofnąć, przykładowo, korzystając z urządzenia programistycznego/PC.

Po przełączeniu F-CPU z trybu STOP na RUN, standardowy program użytkownika uruchamia się w normalny sposób. Po uruchomieniu programu bezpieczeństwa wszystkie F-DB są inicjalizowane z wartościami z pamięci 'load'– jak w przypadku zimnego restartu. Oznacza to, że zapisane informacje o błędach są kasowane. System bezpieczeństwa automatycznie reintegruje F-I/O.

Jeśli proces nie pozwala na taki rozruch, należy zaprogramować ochronę restartu/rozruchu w programie bezpieczeństwa: Wyjście danych procesowych musi być zablokowane do czasu ręcznego aktywowania. Aktywacja ta nie może wystąpić do chwili, gdy można bezpiecznie wyprowadzić dane procesowe, a usterki zostały skorygowane. *(S031)*

Przykład zabezpieczenia restartu/rozruchu

Aby wdrożyć zabezpieczenie restartu/rozruchu, musi być możliwe wykrycie rozruchu. Aby wykryć rozruch, należy zadeklarować tag danych rodzaju BOOL z wartością początkową „PRAWDA" w F-DB.

Należy zablokować wyjście danych procesowych, gdy tag ten ma wartość „1", przykładowo, pasywując F-I/O przy pomocy taga PASS_ON w DB F-I/O.

Aby ręcznie aktywować wyjście danych procesowych, należy zresetować tag za pomocą zatwierdzenia użytkownika.

Zobacz także

Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia nadrzędnego DP lub sterownika IO (strona 196)

Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia I-slave lub I-device (strona 201)

F-I/O DB (strona 174)

Dostęp F-I/O

6

6.1 Adresowanie F-I/O

Przegląd

Poniżej znajduje się opis sposobu adresowania F-I/O w programie bezpieczeństwa oraz to, jakich zasad należy przestrzegać w procesie.

Adresowanie poprzez obraz procesu

Tak ja w przypadku standardowych I/O, dostęp do F-I/O (np. moduły fail-safe S7-1500/ET 200MP) możliwy jest poprzez **obraz procesu** (PII i PIQ).

Bezpośredni odczyt (z identyfikacją I/O „:P") wejść lub zapis wyjść nie jest możliwy w programie bezpieczeństwa.

Aktualizacja obrazu procesu

Obraz procesu wejść F-I/O jest aktualizowany przed uruchomieniem grupy F-runtime. Obraz procesu wyjść F-I/O jest aktualizowany na końcu grupy F-runtime (patrz „Struktura programu bezpieczeństwa (S7-300, S7-400)" (strona 115) lub „Struktura programu bezpieczeństwa (S7-1200, S7-1500)" (strona 117)). Dodatkowe informacje dotyczące aktualizacji obrazu procesu dostępne są w uwadze w „Transfer danych z programu bezpieczeństwa do standardowego programu użytkownika" (strona 205).

Komunikacja wymagana pomiędzy F-CPU (obrazu procesu) a F-I/O do aktualizacji obrazu procesu wykorzystuje specjalny protokół bezpieczeństwa zgodnie z PROFIsafe.

Zasady

- Możliwe jest adresowanie kanału (wartość kanału oraz stan wartości) F-I/O w **jednej** grupie F-runtime. Pierwszy zaprogramowany adres definiuje przypisanie do grupy F-runtime.
- Możliwe jest adresowanie kanału (wartość kanału oraz stan wartości) F-I/O z jednostką, która jest zgodna z rodzajem danych kanału.
  Przykład: Aby uzyskać dostęp do kanałów wejściowych danych rodzaju BOOL, należy użyć jednostki „input (bit)" (I x.y). Dostęp do 16 kolejnych kanałów wejściowych danych rodzaju BOOL poprzez jednostkę „input word" (IW x) nie jest możliwy.
- Należy adresować jedynie te wejścia i wyjścia, które odnoszą się do faktycznie istniejących kanałów (wartość kanału i stan wartości) (np. F-DO 10xDC24V z adresem początkowym 10 wyprowadza jedynie od Q10.0 do Q11.1 dla wartości kanału oraz wejścia od I10.0 do I11.1 dla stanu wartości). Należy pamiętać, że ze względu na specjalny protokół bezpieczeństwa, F-I/O zajmuje większy obszar obrazu procesu niż wymagany dla istniejących i aktywnych kanałów na F-I/O (wartości kanałów oraz stan wartości). Aby odszukać obszar obrazu procesu, gdzie zapisane są kanały (wartości kanałów oraz stan wartości) (struktura kanału), należy odnieść się do stosownych instrukcji obsługi F-I/O.
- Możliwe jest wyłączenie kanałów dla określonego F-I/O (na przykład moduły typu fail-safe ET 200SP lub moduły typu fail-safe S7-1500/ET 200MP). Należy adresować jedynie te kanały (wartości kanałów i stan wartości), które są aktywne w konfiguracji sprzętowej. Adresowanie kanałów wyłączonych w konfiguracji sprzętowej może skutkować ostrzeżeniem podczas kompilowania programu bezpieczeństwa.
- Dla niektórych F-I/O (takich jak moduły fail-safe ET 200SP lub modułów typu fail-safe S7-1500/ET 200MP), możliwe jest określenie oceny typu „ocena czujników 1oo2 (2v2)". Dwa kanały są grupowane w jedną parę, a wynik „oceny czujników 1oo2" zazwyczaj jest dostępny pod adresem kanału z niższym numerem (patrz odnośna instrukcja do F-I/O). Należy adresować wyłącznie ten kanał (wartość kanału oraz stan wartości) z pary kanałów. Adresowanie różnych kanałów może skutkować ostrzeżeniem podczas kompilowania programu bezpieczeństwa.

OSTRZEŻENIE

W przypadku wykorzystywania dodatkowego elementu pomiędzy F-CPU (S7-300/400) a F-I/O, który kopiuje ramki komunikatów bezpieczeństwa zgodnie z PROFIsafe pomiędzy F-CPU (S7-300/400) a F-I/O na program użytkownika, należy przetestować wszystkie funkcje bezpieczeństwa, na które wpływa funkcja kopiowania za każdym razem, gdy zmieni się funkcja kopiowania programowana przez użytkownika. *(S049)*

Zobacz także

Komunikacja urządzenie I-slave safety – urządzenie podrzędne – dostęp F-I/O

(strona 256)

6.2 Stan wartości (S7-1200, S7-1500)

Właściwości

Stan wartości do dodatkowe informacje binarne dla wartości kanału F-I/O. Stan wartości jest wprowadzany do wejścia obrazu procesu(PII).

Stan wartości jest obsługiwany przez S7-1500/ET 200MP, ET 200SP, ET 200eco PN, ET 200S, ET 200iSP, ET 200pro, moduły fail-safe S7-1200 lub F-SM S7-300, standardowe urządzenia I/O typu fail-safe, a także przez standardowe urządzenia podrzędne DP obsługujące profil „RIOforFA-Safety". Informacje dotyczące stanu wartości można znaleźć w dokumentacji odnośnego F-I/O.

Zaleca się uzupełnienie nazwy wartości kanału o „_VS" w przypadku stanu wartości, np. „TagIn_1_VS".

Stan wartości zapewnia informacje dotyczące ważności odnośnych wartości kanału:

- 1: Ważna wartość procesowa jest wyprowadzana na kanał.
- 0: Wartość fail-safe jest wyprowadzana na kanał.

Dostęp do wartości kanałów oraz stanu wartości F-I/O jest możliwy jedynie z tej samej grupy F-runtime.

Położenie bitów stanu wartości w PII dla F-I/O z wejściami cyfrowymi

Bity stanu wartości występują w PII zaraz po wartościach kanału.

Tabela 6- Przykład: Przypisanie adresu w PII dla F-I/O z 16 kanałamiwejść

Bajt w F-CPU	**Przypisane bity w F-CPU na F-**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	DI_7	DI_6	DI_5	DI_4	DI_3	DI_2	DI_1	DI_0
x + 1	DI_{15}	DI_{14}	DI_{13}	DI_{12}	DI_{11}	DI_{10}	DI_9	DI_8
x + 2	Stan wartości DI_7	Stan wartości DI_6	Stan wartości DI_5	Stan wartości DI_4	Stan wartości DI_3	Stan wartości DI_2	Stan wartości DI_1	Stan wartości DI_0
x + 3	Stan wartości DI_{15}	Stan wartości DI_{14}	Stan wartości DI_{13}	Stan wartości DI_{12}	Stan wartości DI_{11}	Stan wartości DI_{10}	Stan wartości DI_9	Stan wartości DI_8

x = Adres początkowy modułu

Lokacja wartości kanału w PII jest dostępna w instrukcji urządzenia do F-I/O.

Położenie bitów stanu wartości w PII dla F-I/O z wyjściami cyfrowymi

Bity stanu wartości w PII są mapowane z taką samą strukturą jak wartości kanału w PIQ.

Tabela 6-2 Przykład: Przypisanie adresu w PIQ dla F-I/O z 4 kanałami wyjść cyfrowych

Bajt w F-CPU	**Przypisane bity w F-CPU na F-I/O:**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	—	—	—	—	DQ_3	DQ_2	DQ_1	DQ_0

x = Adres początkowy

Tabela 6-3 Przykład: Przypisanie adresu w PII dla F-I/O z 4 kanałami wyjść cyfrowych

Bajt w F-CPU	**Przypisane bity w F-CPU na F-I/O:**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	—	—	—	—	Stan wartości DQ_3	Stan wartości DQ_2	Stan wartości DQ_1	Stan wartości DQ_0

x = Adres początkowy modułu

Lokacja wartości kanału w PIQ jest dostępna w instrukcji urządzenia do F-I/O.

Położenie bitów stanu wartości w PII dla F-I/O z wejściami i wyjściami cyfrowymi

Bity stanu wartości występują w zaraz po wartościach kanału w PII w następującej kolejności:

- Bity stanu wartości dla wejść cyfrowych

Tabela 6-4 Przykład: Przypisanie adresu w PIQ dla F-I/O z 2 kanałami wyjść cyfrowych i 1 kanałem wyjścia cyfrowego

Bajt w F-CPU	**Przypisane bity w F-CPU na F-I/O:**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	—	—	—	—	—	—	—	DQ_0

x = Adres początkowy

Tabela 6-5 Przykład: Przypisanie adresu w PII dla F-I/O z 2 kanałami wyjść cyfrowych i 1 kanałem wyjścia

Bajt w F-CPU	**Przypisane bity w F-CPU na F-I/O:**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	—	—	—	—	—	—	DI_1	DI_0
x + 1	—	—	—	—	—	—	Stan wartości DI_1	Stan wartości DI_0
x + 2	—	—	—	—	—	—	—	Stan wartości DQ_0

x = Adres początkowy modułu

Lokacja wartości kanału w PII oraz PIQ jest dostępna w instrukcji urządzenia do F-I/O.

Położenie bitów stanu wartości w PII dla F-I/O z wejściami analogowymi

Bity stanu wartości występują w PII bepośrednio po wartościach

Tabela 6-6 Przykład: Przypisanie adresu w PII dla F-I/O z 6 kanałami wejść analogowych (rodzaj danych INT)

Bajt w F-CPU	**Przypisane bajty/bity w F-CPU na F-I/O:**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	Wartość kanału AI_0							
...	...							
x + 10	Wartość kanału AI_5							
x + 12	—	—	Stan wartości AI_5	Stan wartości AI_4	Stan wartości AI_3	Stan wartości AI_2	Stan wartości AI_1	Stan wartości AI_0

x = Adres początkowy modułu

Lokacja wartości kanału w PII jest dostępna w instrukcji urządzenia do F-I/O.

Położenie bitów stanu wartości w PII dla F-I/O z wyjściami analogowymi

Bity stanu wartości są mapowane w PII.

Tabela 6-7 Przykład: Przypisanie adresu w PIQ dla F-I/O z 6 kanałami wyjść analogowych (rodzaj danych INT)

Bajt w F-CPU	**Przypisane bajty w F-CPU na F-I/O:**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	Wartość kanału AO_0							
...	...							
x + 10	Wartość kanału AO_5							

x = Adres początkowy

Tabela 6-8 Przykład: Przypisanie adresu w PII dla F-I/O z 6 kanałami wyjść analogowych (rodzaj danych INT)

Bajt w F-CPU	**Przypisane bity w F-CPU na F-I/O:**							
	7	**6**	**5**	**4**	**3**	**2**	**1**	**0**
x + 0	—	—	Stan wartości AO_5	Stan wartości AO_4	Stan wartości AO_3	Stan wartości AO_2	Stan wartości AO_1	Stan wartości AO_0

x = Adres początkowy modułu

Lokacja wartości kanału w PIQ jest dostępna w instrukcji urządzenia do F-I/O.

6.3 Dane procesowe lub wartości

Kiedy stosowane są wartości fail-safe?

Funkcja bezpieczeństwa wymagana, by wartości fail-safe (0) były stosowane zamiast danych procesowych do pasywacji całego F-I/O lub poszczególnych kanałów w F-I/O w poniższych przypadkach. Dotyczy do zarówno kanałów cyfrowych (rodzaj danych BOOL), jak i kanałów analogowych (rodzaj danych INT lub DINT):

- Podczas rozruchu systemu bezpieczeństwa
- Gdy występują błędy komunikacji związanej z bezpieczeństwem (błędy komunikacji) pomiędzy F-CPU a F-I/O korzystających z protokołu bezpieczeństwa zgodnie z PROFIsafe.
- Gdy występują usterki F-I/O oraz usterki kanałów (takie jak przerwanie przewodu, zwarcie czy błędy rozbieżności)
- Dopóki pasywacja F-I/O jest aktywowana w DB F-I/O za pomocą PASS_ON = 1 (patrz poniżej)
- Dopóki pasywacja F-I/O jest wyłączona w DB F-I/O za pomocą DISABLE = 1 (patrz poniżej)

Wyjście wartości fail-safe dla F-I/O / kanałów F-I/O

Gdy występuje **pasywacja** dla **F-I/O z wejściami**, system bezpieczeństwa zapewnia program bezpieczeństwa z wartościami fail-safe (0) w PII zamiast danych procesowych obecnych na wejściach fail-safe F-I/O.

Przekroczenie wartości na kanale **SM 336; AI 6 x 13Bit** lub

SM 336; F-AI 6 x 0/4 ... 20 mA HART jest rejestrowane przez system bezpieczeństwa jako awaria F-I/O / kanału. Wartość fail-safe 0 jest podawana zamiast $7FFF_H$ (przy nadmiernej wartości) lub 8000_H (przy niedostatecznej wartości) w PII do programu bezpieczeństwa.

Aby przetwarzać wartości fail-safe inne niż „0" w programie bezpieczeństwa dla F-I/O z wejściami **do kanałów analogowych danych rodzaju INT lub DINT**, można przypisać poszczególne wartości fail-safe inne dla QBAD = 1 oraz stan wartości = 0 bądź QBAD_I_xx/QBAD_O_xx = 1 (instrukcje JMP/JMPN, LABEL i MOVE). Szczegóły charakterystyk, patrz „QBAD/PASS_OUT/DISABLED/QBAD_I_xx/QBAD_O_xx oraz stan wartości" (strona 181).

⚠ OSTRZEŻENIE

W przypadku F-I/O z kanałami wejść cyfrowych (rodzaj danych BOOL), wartość zapewniania przez PII zawsze musi być przetwarzana w programie bezpieczeństwa, niezależnie od stanu wartości lub QBAD/QBAD_I_xx. *(S009)*

Gdy **pasywacja** występuje w **F-I/O z wyjściami**, system bezpieczeństwa wyprowadza wartości fail-safe (0) na wyjściach fail-safe zamiast wartości wyjściowych zapewnianych przez program w PIQ.

<table>
<tr><th>Stan powiązanego PAA/PIQ dla ...</th><th>F-I/O z profilem „RIOforFA-Safety" z F-CPU S7-1200/1500</th><th>F-I/O bez profilu „RIOforFA-Safety" z F-CPU S7-1200/1500</th><th>F-I/O Z F-CPU S7-300/400</th></tr>
<tr><td>Rozruch systemu</td><td colspan="3" rowspan="2">System bezpieczeństwa nadpisuje PII/PIQ wartościami fail-safe (0).</td></tr>
<tr><td>Błędy komunikacji</td></tr>
<tr><td>Usterki F-I/O</td><td rowspan="2">System bezpieczeństwa nadpisuje PII wartościami fail-safe (0). W PII, wartości utworzone w programie bezpieczeństwa są utrzymywane.</td><td colspan="2" rowspan="2">System bezpieczeństwa nadpisuje PII/PIQ wartościami fail-safe (0).</td></tr>
<tr><td>Awarie kanałów w konfiguracji pasywacji kompletnego F-I/O</td></tr>
<tr><td>Awarie kanałów podczas konfiguracji pasywacji szczegółowej kanałów</td><td colspan="2">Dla objętych kanałów: System bezpieczeństwa nadpisuje PII/PIQ wartościami fail-safe (0).</td></tr>
<tr><td>Dopóki pasywacja F-I/O jest aktywowana w DB F-I/O za pomocą PASS_ON = 1</td><td colspan="3">System bezpieczeństwa nadpisuje PII/PIQ wartościami fail-safe (0).</td></tr>
<tr><td>Dopóki F-I/O jest dezaktywowane w DB F-I/O za pomocą DISABLE = 1</td><td colspan="2">System bezpieczeństwa nadpisuje PII/PIQ wartościami fail-safe (0).</td><td>-</td></tr>
</table>

Reintegracja F-I/O / kanałów F-I/O

Przełączenie z wartości fail-safe (0) na dane procesowe (**reintegracja F-I/O**) odbywa się **automatycznie** lub po **zatwierdzeniu użytkownika** w DB F-I/O. Metoda reintegracji zależy od następujących czynników:

- Powód pasywacji F-I/O lub kanałów F-I/O
- Na F-I/O bez parametru kanału „Zatwierdzenie awarii kanału" na wartości zmiennej ACK_NEC powiązanych bloków danych F-IO (strona 174).
- Na F-I/O z parametrem kanału „Zatwierdzenie awarii kanału" (na przykład moduły bezpieczeństwa S7-1500 / ET 200 MP / moduły bezpieczeństwa SIMATIC S7-1200) na wartości parametru kanału.

W przypadku urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD z profilem „RIOforFA-Safety", należy odnieść się do stosownej dokumentacji.

Uwaga

Należy pamiętać, że przy awarii kanałów w F-I/O, odbywa się szczegółowa pasywacja kanałów, jeśli została ona skonfigurowana w *edytorze sprzętu i sieci*. Na dotkniętych kanałach wyprowadzana są wartości fail-safe (0).

Reintegracja po awarii kanału obejmuje wszystkie kanały, których usterki zostały usunięte; uszkodzone kanały pozostają pasywowane.

Zobacz także

Konfiguracja F-I/O (strona 51)

6.4 DB F-I/O

Wstęp

DB F-I/O jest automatycznie generowany dla każdego F-I/O (w trybie bezpieczeństwa), gdy F-I/O jest konfigurowany w *edytorze sprzętu i sieci*. DB F-I/O zawiera tagi, dla których można przeprowadzić ocenę lub można/trzeba zapisać w programie bezpieczeństwa. Nie jest dozwolone wprowadzanie zmian w wartościach początkowych tagów bezpośrednio w DB F-I/O. Po usunięciu F-I/O powiązany DB również jest kasowany.

Dostęp do DB F-I/O

Dostęp do tagów DB F-I/O uzyskuje się z następujących powodów:

- Do reintegracji F-I/O po błędach komunikacji, usterkach F-I/O lub awarii kanałów
- Aby pasywować F-I/O zależnie od szczególnego stanu programu bezpieczeństwa (przykładowo, pasywacja grupy)
- Aby wyłączyć F-I/O (przykładowo, kontrola konfiguracji)
- Do zmiany parametrów urządzeń podrzędnych DP opartych na GSD typu fail-safe/ urządzeń I/O opartych na GSD
- Gdy konieczna jest ocena, czy wyprowadzane są wartości fail-safe czy dane procesowe

6.4.1 Nazwa i numer DB F-I/O

Nazwę DB F-I/O tworzą:

- stały przedrostek „F"
- adres początkowy F-I/O oraz nazwy wprowadzone we właściwościach F-I/O w *edytorze sprzętu i sieci* bądź w widoku urządzenia (maks. 24 pierwsze znaki)

Przykład: F00004_F-DI24xDC24V_1

Numer jest przypisywany w zakresie liczbowym zdefiniowanym w obszarze „Ustawienia" (strona 91) w *Safety Administration Editor*.

Opcja „Creates F-I/O DBs without prefix" (Tworzy DB F-I/O bez prefiksu) (S7-1200, S7-1500)

Po wybraniu opcji „Creates F-I/O DBs without prefix" (Tworzy DB F-I/O bez prefiksu) w obszarze „Ustawienia" (strona 91) w *Safety Administration Editor*, nazwa jest tworzona z:

- nazwy wprowadzonej we właściwościach F-I/O w *edytorze sprzętu i sieci* lub w widoku urządzenia (maks. 117 znaków)

Przykład: F-DI24xDC24V_1

Zmiana nazwy i numeru DB F-I/O

Nazwę zmienia się poprzez zmianę nazwy wprowadzonej we właściwościach F-I/O w *edytorze sprzętu i sieci* bądź w widoku urządzenia.

Numer zmienia się w zakładce „Properties”/”F-parameters” (Właściwości/Parametry bezpieczeństwa) powiązanego F-I/O.

6.4.2 Tagi DB F-I/O

Poniższa tabela zawiera zmienne dla DB F-I/O:

	Tag	Rodzaj danych	Funkcja	Wartość początkowa
Tagi, które można lub trzeba zapisać	PASS_ON	BOOL	1=aktywuj pasywację	0
	ACK_NEC	BOOL	1=zatwierdzenie do reintegracji wymagane w razie awarii F-I/O lub kanału	1
	ACK_REI	BOOL	1 = zatwierdzenie do reintegracji	0
	IPAR_EN	BOOL	Tag do ponownego przypisania parametrów urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD, lub, w przypadku SM 336; F-AI 6 x 0/4 ... 20 mA HART, do aktywacji komunikacji HART	0
	DISABLE*	BOOL	1=wyłącz F-I/O	0
Zaczniki, dla których można przeprowadzić ocenę	PASS_OUT	BOOL	Wyjście pasywacji	1
	QBAD	BOOL	1= Wartości fail-safe są wyprowadzane	1
	ACK_REQ	BOOL	1=Polecenie zatwierdzenia reintegracji	0
	IPAR_OK	BOOL	Tag do ponownego przypisania parametrów urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD, lub, w przypadku SM 336; F-AI 6 x 0/4 ... 20 mA HART, do aktywacji komunikacji HART	0
	DIAG	BYTE	Informacja o usłudze bez fail-safe	0
	DISABLED*	BOOL	1=F-I/O jest wyłączony	0
	QBAD_I_xx	BOOL	1=wartości fail-safe są wyprowadzane na kanał wejściowy xx (S7-300/400)	1
	QBAD_O_xx	BOOL	1=wartości fail-safe są wyprowadzane na kanał wyjściowy xx (S7-300/400)	1

* Od wersji systemu bezpieczeństwa Version 2.1 dla S7-1200/1500

Różnice w ocenie w F-CPU S7-1200/1500 oraz S7-300/400

Poniższa tabela opisuje różnice w ocenie tagów DB F-I/O oraz stanów wartości zależnie od zastosowanego F-I/O i F-CPU.

Tag w DB F-I/O lub stan wartości	F-I/O z profilem „RIOforFA-Safety" z F-CPU S7-1200/1500	F-I/O bez profilu „RIOforFA-Safety" z F-CPU S7-1200/1500	F-I/O z F-CPU S7-300/400
ACK_NEC	—[2]	x	x
QBAD[3]	x	x	x
PASS_OUT[3]	x	x	x
QBAD_I_xx[1]	—	—	x
QBAD_O_xx[1]	—	—	x
Stan zapisu[1]	x	x	—

[1] QBAD_I_xx i QBAD_O_xx wyświetlają ważność szczegłówej wartości kanału i odpowiadają tym stanowi odwróconej wartości z S7-1200/1500. Stan wartości lub QBAD_I_xx oraz QBAD_O_xx nie są dostępne dla urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe bez profilu „RIOforFA-Safety".

[2] W przypadku F-I/O obsługujących parametr kanału „Channel failure acknowledge" (Zatwierdzenie awarii kanału) (przykładowo moduły bezpieczeństwa S7-1500/ET 200MP lub moduły bezpieczeństwa S7-1200), zastępuje to zmienną ACK_NEC w bloku danych F-IO.

[3] Szczegóły charakterystyk, patrz „QBAD/PASS_OUT/DISABLED/QBAD_I_xx/QBAD_O_xx oraz stan wartości"

6.4.2.1 PASS_ON

Tag PASS_ON pozwala na włączenie pasywacji F-I/O, przykładowo, zależnie od różnych stanów w programie bezpieczeństwa.

Przy pomocy taga PASS_ON w DB F-I/O można pasywować F-I/O; szczegółowa pasywacja kanałów nie jest możliwa.

Dopóki PASS_ON = 1, **pasywacja** powiązanego F-I/O jest aktywna.

6.4.2.2 ACK_NEC

W przypadku wykrycia awarii F-I/O, występuje **pasywacja** odnośnego F-I/O. Jeśli zostanie wykryta awaria kanału i skonfigurowana jest szczegółowa pasywacja kanału, odnośne kanały są pasywowane. Jeśli ustawiono pasywację całego F-I/O, pasywacji ulegają wszystkie kanały odnośnego F-I/O. Po usunięciu awarii kanału lub całego F-I/O następuje **reintegracja odnośnego** F-I/O, zależnie od ACK_NEC:

- Przy ACK_NEC = 0 można przypisać **automatyczną reintegrację**.
- Przy ACK_NEC = 1 można przypisać **reintegrację** za pomocą **zatwierdzenia użytkownika**.

OSTRZEŻENIE

Przypisanie parametru znacznika ACK_NEC = 0 jest dozwolone jedynie, bit zgodności reintegracja jest dopuszczalna dla odnośnego procesu pod względem bezpieczeństwa. *(S010)*

Uwaga

Wartość początkowa do ACK_NEC to 1 po utworzeniu DB F-I/O. Jeśli nie jest wymagana automatyczna reintegracja, nie trzeba zapisywać ACK_NEC.

Zobacz także

Po usterce F-I/O lub kanału (strona 190)

6.4.2.3 ACK_REI

Gdy system bezpieczeństwa wykryje błąd komunikacji lub awarię F-I/O, odnośny F-I/O jest pasywowany. Jeśli zostanie wykryta awaria kanału i skonfigurowana jest szczegółowa pasywacja kanału, odnośne kanały są pasywowane. Jeśli ustawiono pasywację całego F-I/O, pasywacji ulegają wszystkie kanały odnośnego F-I/O. **Reintegracja** F-I/O / kanałów w F-I/O po usunięciu awarii wymaga **zatwierdzenia użytkownika** zboczem pozytywnym na zmiennej ACK_REI w DB F-I/O:

- Po każdym błędzie komunikacji
- Po usterce F-I/O lub kanału tylko z przypisaniem parametru „Zatwierdzenie awarii kanału - ręczne" lub ACK_NEC = 1

Reintegracja po awarii kanału obejmuje wszystkie kanały, których usterki zostały usunięte.

Zatwierdzenie nie jest możliwe, dopóki tag ACK_REQ = 1.

W programie bezpieczeństwa należy zapewnić zatwierdzenie użytkownika poprzez tag ACK_REI dla każdego F-I/O.

OSTRZEŻENIE

W przypadku zatwierdzenia użytkownika, należy połączyć tag ACK_REI z DB F-I/O z sygnałem generowanym na wejściu operatora. Wzajemne połączenie z automatycznie generowanym sygnałem nie jest dozwolone. *(S011)*

Uwaga

Alternatywnie można użyć instrukcji „ACK_GL" do wykonania reintegracji F-I/O po błędach komunikacji lub awarii F-I/O / kanału (ACK_GL: „Zatwierdzenie globalne wszystkich F-I/O w grupie F-runtime (STEP 7 Safety V16)" (strona 518)).

6.4.2.4 IPAR_EN

Tag IPAR_EN odpowiada tagowi iPar_EN_C w profilu magistrali PROFIsafe od wersji specyfikacji PROFIsafe V1.20 i wyższej.

Urządzenia podrzędne DP oparte na GSD typu fail-safe/ urządzenia I/O oparte na GSD

Aby określić, kiedy należy ustawić lub zresetować ten tag, gdy parametry urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD są ponownie przypisywane, należy zapoznać się ze specyfikacją PROFIsafe V1.20 lub nowszą bądź z dokumentacją powyższych urządzeń.

Należy pamiętać, że IPAR_EN = 1 nie wyzwala pasywacji odnośnego F-I/O.

Jeśli pasywacja ma wystąpić, gdy IPAR_EN = 1, należy również ustawić tag

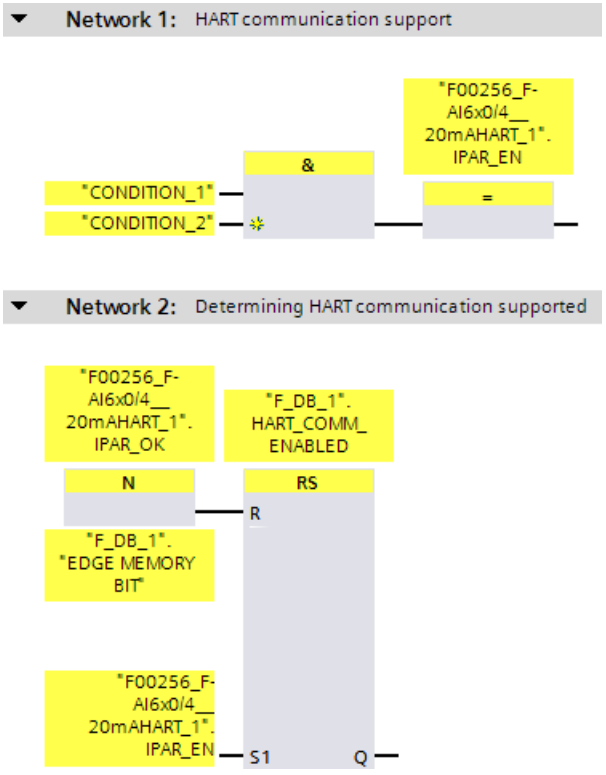
PASS_ON = 1. **Komunikacja HART z SM 336; F-AI 6 x 0/4 ... 20 mA HART**

W przypadku ustawienia taga IPAR_EN tag na „1", gdy przypisany jest parametr „HART_Tor" = „switchable" (możliwy do przełączenia) komunikacja HART do SM 336; F- AI 6 x 0/4 ... 20 mA HART jest aktywowana. Ustawienie tego taga na „0" spowoduje wyłączenie komunikacji HART. F-SM zatwierdza aktywną lub nieaktywną komunikację HART tagiem IPAR_OK = 1 lub 0.

Komunikację HART należy włączyć jedynie, gdy system jest w stanie, w którym ponowne przypisanie parametrów do powiązanych urządzeń HART można przeprowadzić bez stwarzania ryzyka.

Aby ocenić status „HART communication enabled" (Komunikacja HART włączona) w programie bezpieczeństwa, np. w celu zaprogramowania blokad, należy zgromadzić informacje przedstawione w poniższym przykładzie. Jest to konieczne do zapewnienia, że informacje są należycie dostępne nawet w razie wystąpienia błędu komunikacji, gdy komunikacja HART jest włączana z parametrem IPAR_EN = 1. Zmiana statusu taga IPAR_EN podczas tej oceny jest możliwa tylko, gdy nie wystąpiła pasywacja z powodu błędu komunikacji bądź awarii F-I/O / kanału.

Przykład aktywacji komunikacji HART



Dodatkowe informacje dotyczące komunikacji HART z SM 336; F-AI 6 x 0/4 ... 20 mA HART można znaleźć w podręczniku „System automatyki S7-300", podręczniku „System I/O ET 200M Distributed", podręczniku „Moduły sygnałowe typu fail-safe" (http://support.automation.siemens.com/WW/view/en/19026151) oraz w pomocy do modułu bezpieczeństwa.

6.4.2.5 DISABLE

Zmienna DISABLE pozwala na wyłączenie F-I/O.

Dopóki DISABLI = 1, powiązane F-I/O są **pasywowane**.

Wpisy diagnostyczne programu bezpieczeństwa nie mogą być dłużej wprowadzane w buforze diagnostycznym F-CPU dla tego F-I/O (przykładowo, ze względu na błąd komunikacji).

Istniejące wpisy diagnostyczne są oznaczane jako wychodzące.

6.4.2.6 QBAD/PASS_OUT/DISABLED/QBAD_I_xx/QBAD_O_xx oraz stan wartości

Poniższa tabela opisuje różnice w reakcji wartości kanałów oraz zmiennych QBAD, PASS_OUT, DISABLED, QBAD_I_xx/QBAD_O_xx oraz stanów wartości zależnie od zastosowanego F-I/O i F-CPU.

<table>
<tr><th>Wyjście wartości fail-safe po...</th><th>F-I/O z profilem „RIOforFA-Safety" z F-CPU S7-1200/1500</th><th>F-I/O bez profilu „RIOforFA-Safety" z F-CPU S7-1200/1500</th><th>F-I/O z F-CPU S7-300/400</th></tr>
<tr><td>Rozruch systemu</td><td colspan="2" rowspan="3">QBAD oraz PASS_OUT = 1
DISABLED

niezmienione Dla **wszystkich** kanałów:
Wartość kanału = wartość fail-safe (0) Stan wartości = 0*</td><td rowspan="3">QBAD oraz PASS_OUT = 1
Dla **wszystkich** kanałów:

Wartość kanału = wartość fail-safe (0)
QBAD_I_xx oraz QBAD_O_xx = 1*</td></tr>
<tr><td>Błędy komunikacji

Usterki F-I/O</td></tr>
<tr><td>Awarie kanałów w konfiguracji pasywacji dla całego F-I/O</td></tr>
<tr><td>Awarie kanałów podczas konfiguracji pasywacji szczegółowej kanałów</td><td>QBAD, PASS_OUT oraz DISABLED **niezmienione**
Dla **objętych** kanałów:
Wartość kanału = wartość fail-safe (0)
Stan wartości = 0</td><td>QBAD oraz PASS_OUT = 1
DISABLED **niezmienione** Dla **objętych** kanałów:
Wartość kanału = wartość fail-safe (0)
Stan wartości = 0*</td><td>QBAD oraz PASS_OUT = 1
Dla **objętych** kanałów: Wartość kanału = wartość fail-safe (0)
QBAD_I_xx oraz QBAD_O_xx = 1*</td></tr>
<tr><td>Dopóki pasywacja F-I/O jest aktywowana w DB F-I/O za pomocą PASS_ON = 1</td><td colspan="2">QBAD = 1, PASS_OUT oraz DISABLED **niezmienione** Dla **wszystkich** kanałów:
Wartość kanału = wartość fail-safe (0) Stan wartości = 0*</td><td>QBAD = 1, PASS_OUT **niezmienione**
Dla **wszystkich** kanałów:
Wartość kanału = wartość fail-safe (0)
QBAD_I_xx oraz QBAD_O_xx = 1*</td></tr>
<tr><td>Dopóki F-I/O jest dezaktywowane w DB F-I/O za pomocą DISABLE = 1</td><td colspan="2">QBAD, PASS_OUT oraz DISABLED = 1
Dla **wszystkich** kanałów:
Wartość kanału = wartość fail-safe (0) Stan wartości = 0*</td><td>-</td></tr>
</table>

* Stany wartości lub QBAD_I_xx oraz QBAD_O_xx nie są dostępne dla urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe bez profilu „RIOforFA-Safety".

6.4.2.7 ACK_REQ

Gdy system bezpieczeństwa wykryje błąd komunikacji lub awarię F-I/O / kanału F-I/O, odnośny F-I/O lub poszczególne kanały są pasywowane. ACK_REQ = 1 sygnalizuje, że **zatwierdzenie użytkownika** jest potrzebne do reintegracji odnośnego F-I/O lub kanałów F-I/O.

System bezpieczeństwa ustawia ACK_REQ = 1 gdy tylko usterka zostanie usunięta i możliwe jest zatwierdzenie użytkownika. W przypadku szczegółowej pasywacji kanałów, system bezpieczeństwa ustawia ACK_REQ = 1 gdy tylko usterka kanału zostanie usunięta. Jest dla niej możliwe zatwierdzenie użytkownika. Po zatwierdzeniu system bezpieczeństwa resetuje ACK_REQ do 0.

Uwaga

W przypadku F-I/O z wyjściami, zatwierdzenie po usterce F-I/O lub kanału jest możliwe kilka minut po usunięciu awarii, aż zostanie zastosowany niezbędny sygnał testowy (patrz *Instrukcje do F-I/O*).

6.4.2.8 IPAR_OK

Tag IPAR_OK odpowiada tagowi iPar_OK_S w profilu magistrali PROFIsafe od wersji specyfikacji PROFIsafe V1.20 i wyższej.

Urządzenia podrzędne DP oparte na GSD typu fail-safe/ urządzenia I/O oparte na GSD

Aby określić, jak wykonać ocenę tego taga, gdy parametry urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD są ponownie przypisywane, należy zapoznać się ze specyfikacją PROFIsafe V1.20 lub nowszą bądź z dokumentacją powyższych urządzeń.

Odnośnie komunikacji HART z SM 336; F-AI 6 x 0/4 ... 20 mA HART, patrz rozdział

„IPAR_EN" (strona 179).

6.4.2.9 DIAG

Tag DIAG zapewnia w celach serwisowych informacje nie-fail-safe (1 bajt) o błędach lub usterkach, które wystąpiły. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG są zapisywane do czasu wykonania zatwierdzenia przy pomocy taga ACK_REI lub wystąpienia automatycznej reintegracji.

Struktura DIAG

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Przekroczenie czasu wykryte przez F-I/O	Połączenie PROFIBUS/PROFINET pomiędzy F-CPU i F-I/O jest uszkodzone. Wartość czasu monitorowania bezpieczeństwa dla F-I/O jest zbyt niska. F-I/O odbierają nieprawidłowe dane przypisania parametrów lub	• Sprawdzić połączenie PROFIBUS/PROFINET i upewnić się, że nie ma zewnętrznych źródeł zakłóceń. • Sprawdzić przypisanie parametrów w F-I/O, W razie potrzeby ustawić wyższą wartość czasu monitorowania. Należy ponownie skompilować konfigurację sprzętową i pobrać ją do F-CPU. Ponownie skompilować program bezpieczeństwa. • Sprawdzić bufor diagnostyczny F-I/O. • Wyłączyć F-I/O i ponownie go włączyć.
		Wewnętrzna usterka F-I/O lub	Wymienić F-I/O
		Wewnętrzna usterka F-CPU	Wymienić F-CPU
Bit 1	Usterka F-I/O lub kanału wykryta przez F-I/O[1]	Patrz *Instrukcje do F-I/O*	Patrz *Instrukcje do F-I/O*
Bit 2	Błąd lub błąd numeru sekwencji wykryty przez F-I/O	Patrz opis do bitu 0	Patrz opis do bitu 0
Bit 3	Zastrzeżony	—	—
Bit 4	Przekroczenie czasu wykryte przez system bezpieczeństwa	Patrz opis do bitu 0	Patrz opis do bitu 0
Bit 5	Wykryto błąd numeru sekwencji przez system bezpieczeństwa[2]	Patrz opis do bitu 0	Patrz opis do bitu 0
Bit 6	Błąd CRC wykryty przez system bezpieczeństwa	Patrz opis do bitu 0	Patrz opis do bitu 0
Bit 7	Błąd adresowania[3]	—	Należy skontaktować się z działem obsługi

1 Nie dla F-I/O obsługującego profil „RIOforFA-Safety".

2 Tylko dla F-CPU S7-300/400

3 Tylko dla F-CPU S7-1200/1500

6.4.3 Dostęp do tagów DB F-I/O

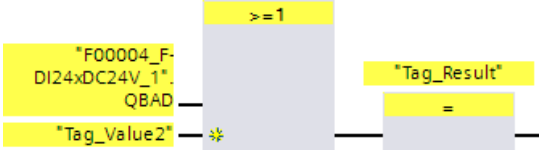
Zasada dostępu do tagów DB F-I/O

Dostęp do tagów DB F-I/O jest możliwy tylko z tej grupy F-runtime, z której możliwy jest dostęp do kanałów tego F-I/O (jeśli wprowadzono dostęp).

„W pełni kwalifikowany dostęp DB"

Dostęp do tagów DB F-I/O jest możlie poprzez „w pełni kwalifikowany dostęp DB" (czyli poprzez określenie nazwy DB F-I/O oraz określenie nazwy taga).

Przykład oceny taga QBAD



Zobacz także

F-I/O DB (strona 174)

6.5 Pasywacja i ponowna integracja F-I/O

Przegląd

Poniżej można znaleźć informacje dotyczące pasywacji i reintegracji F-I/O.

Wykresy sekwencji sygnałów

Sekwencje sygnałów przedstawione poniżej stanowią typowe sekwencja dla wskazanego zachowania.

Rzeczywiste sekwencje oraz, w szczególności, względne położenie zmiany stanu poszczególnych sygnałów może odbiegać od podanej sekwencji w zakresie znanych „rozmytych" czynników wykonywania progamu cyklicznego, zależących od następujących elementów:

- Stosowany F-I/O
- Stosowany F-CPU
- Czas cyklu (F-)OB, w którym wywoływana jest powiązana grupa F-runtime
- Czas rotacji celu PROFIBUS DP lub czas aktualizacji PROFINET IO

Uwaga

Przedstawiona sekwencja sygnałów odnosi się do stanu sygnałów w programie bezpieczeństwa utworzonym przez użytkownika.

6.5.1 Po uruchomieniu systemu

Zachowanie po uruchomieniu

Wyjście wartości fail-safe po uruchomieniu systemu bezpieczeństwa	**F-I/O z profilem „RIOforFA-Safety" z F-CPU S7-1200/1500**	**F-I/O bez profilu „RIOforFA-Safety" z F-CPU S7-1200/1500**	**Każdy F-I/O z F-CPU S7-300/400**
Pasywacja całego F-I/O następuje podczas rozruchu.	QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) Stan wartości = 0*		QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) QBAD_I_xx oraz QBAD_O_xx = 1*

* Stany wartości lub QBAD_I_xx oraz QBAD_O_xx nie są dostępne dla urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe bez profilu „RIOforFA-Safety".

Reintegracja F-I/O

Reintegracja F-I/O, tj. zapewnienie wartości procesowych w PII lub wyprowadzenie wartości procesowych zapewnionych w PIQ na wyjścia fail-safe, odbywa się **automatycznie**, niezależnie od ustawień w tagu ACK_NEC lub konfiguracji „Zatwierdzenie awarii kanału", nie wcześniej niż drugi cykl grupy F-runtime po uruchomieniu systemu bezpieczeństwa.

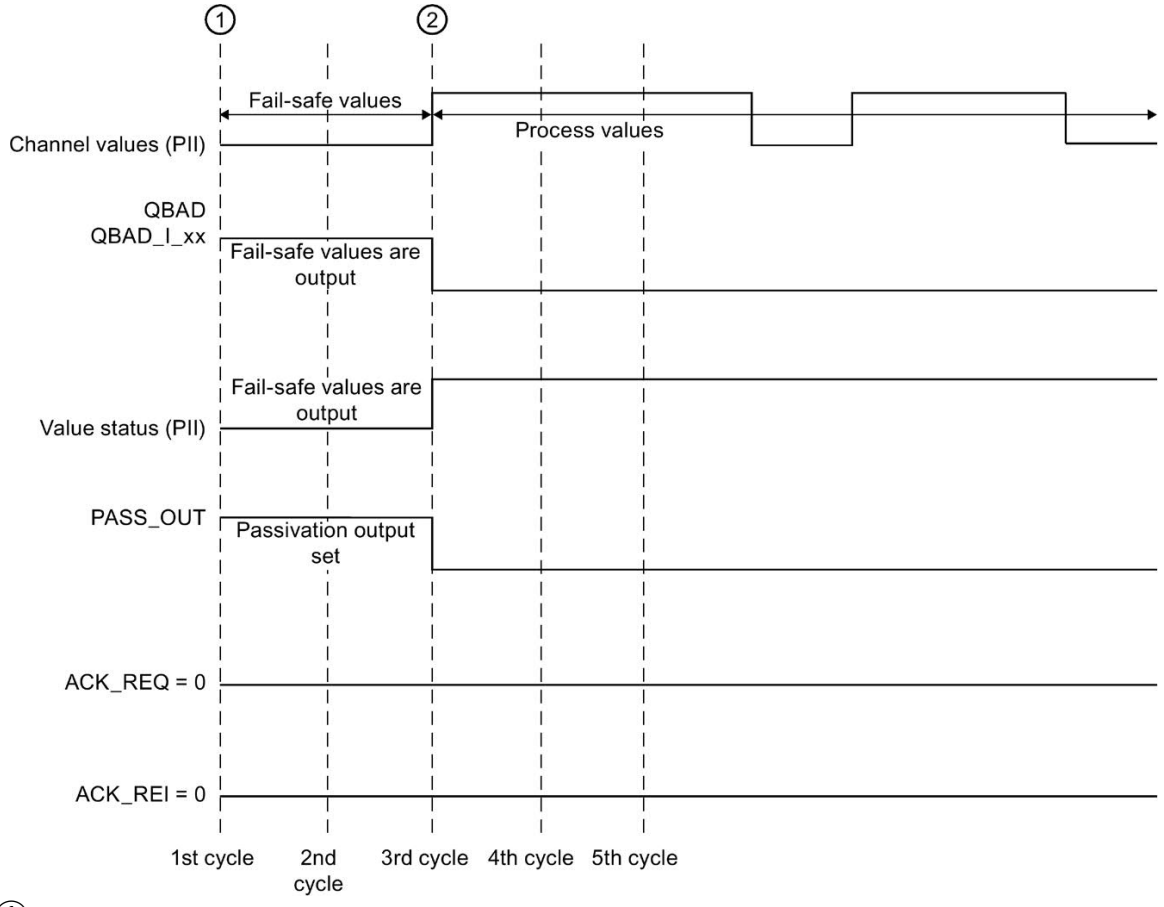
Dodatkowe informacje dotyczące oczekującej komunikacji bezpieczeństwa, błędów F-I/O lub kanałów podczas rozruchu systemu bezpieczeństwa można znaleźć w działach „Po błędach komunikacji" (strona188) oraz „Po usterce F-I/O lub kanału" (strona 190).

W przypadku urządzeń podrzędnych DP oparte na GSD typu fail-safe/ urządzeń I/O opartych na GSD z profilem „RIOforFA-Safety", należy odnieść się do odpowiedniej dokumentacji urządzeń.

Zależnie do stosowanego F-I/O i czasu cyklu grupy F-runtime oraz PROFIBUS DP/PROFINET IO, przed wystąpieniem reintegracji może upłynąć kilka cyklu grupy F-runtime.

Jeśli nawiązanie komunikacji pomiędzy F-CPU a F-I/O zajmuje więcej niż czas monitorowania bezpieczeństwa ustawiony we właściwościach F-I/O, automatyczna reintegracja nie jest wykonywana.

Sekwencja sygnałów do pasywacji i ponownej integracji F-I/O po uruchomieniu systemu bezpieczeństwa



① Rozruch systemu

② bezpieczeństwa/pasywacja

OSTRZEŻENIE

Po przełączeniu F-CPU z trybu STOP na RUN, standardowy program użytkownika uruchamia się w normalny sposób. Po uruchomieniu programu bezpieczeństwa wszystkie F-DB są inicjalizowane z wartościami z pamięci "load memory" – jak w przypadku zimnego restartu. Oznacza to, że zapisane informacje o błędach są kasowane.

System bezpieczeństwa automatycznie reintegruje F-I/O zgodnie z powyższym opisem.

Błąd roboczy lub wewnętrzny błąd również mogą wyzwolić uruchomienie programu bezpieczeństwa z wartościami z pamięci "load memory". Jeśli proces nie pozwala na taki rozruch, należy zaprogramować ochronę restartu/rozruchu w programie bezpieczeństwa: Wyjście danych procesowych musi być zablokowane do czasu ręcznego aktywowania. Aktywacja ta nie może wystąpić do chwili, gdy można bezpiecznie wyprowadzić dane procesowe, a usterki zostały skorygowane. *(S008)*

6.5.2 Po błędach komunikacji

Zachowanie po błędach komunikacji

Wyjście wartości fail-safe po błędach komunikacji	**F-I/O z profilem „RIOforFA-Safety" z F-CPU S7-1200/1500**	**F-I/O bez profilu „RIOforFA-Safety" z F-CPU S7-1200/1500**	**Każdy F-I/O z F-CPU S7-300/400**
Jeśli zostanie wykryty błąd komunikacji pomiędzy F-CPU a F-I/O, wszystkie kanały całego F-I/O są pasywowane.	QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) Stan wartości = 0*		QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) QBAD_I_xx oraz QBAD_O_xx = 1*

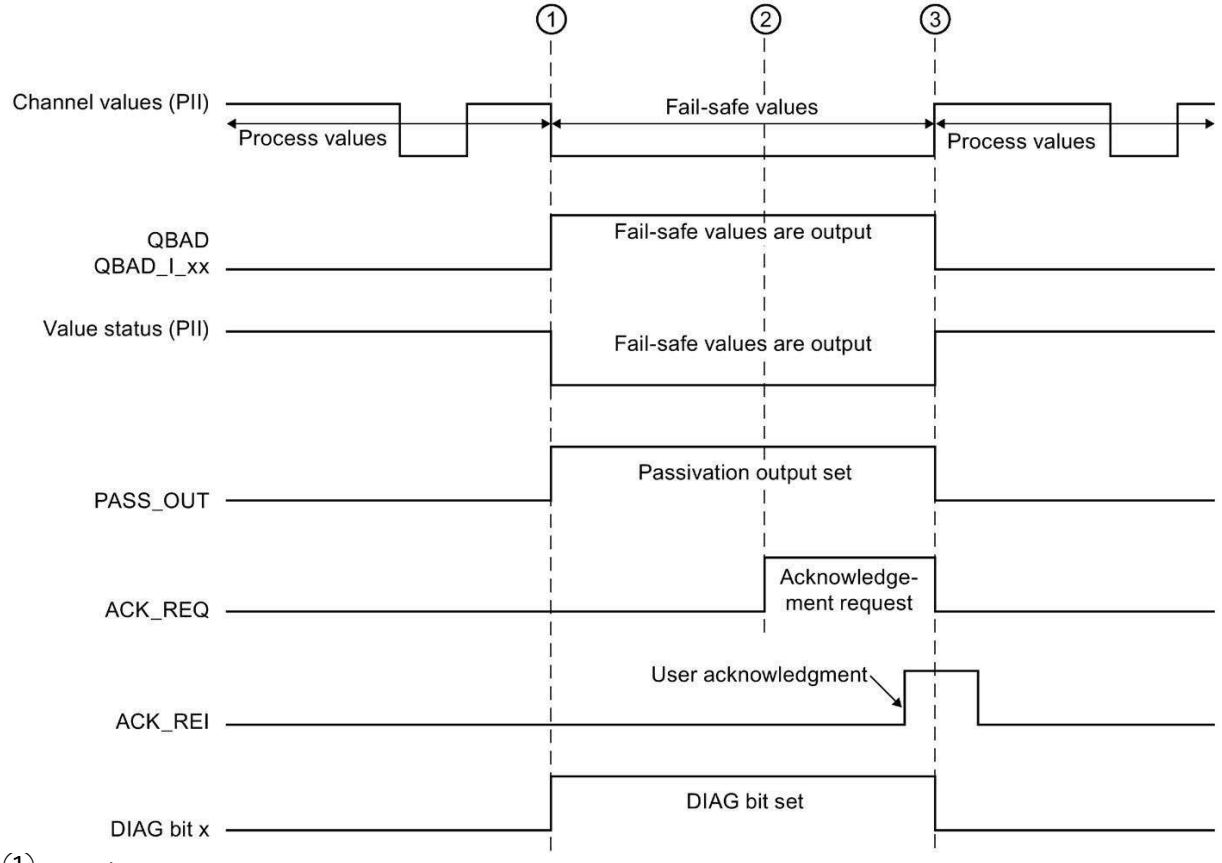
* Stany wartości lub QBAD_I_xx oraz QBAD_O_xx nie są dostępne dla urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe bez profilu „RIOforFA-Safety".

Reintegracja F-I/O

Reintegracja odnośnego F-I/O, czyli zapewnienie danych procesowych w PII lub wyprowadzenie danych dostępnych na PIQ do wyjść fail-safe, odbywa się tylko w następujących przypadkach:

- Wszystkie błędy komunikacji zostały usunięte, a system bezpieczeństwa ma ustawiony tag ACK_REQ = 1
- Wystąpiło **zatwierdzenie użytkownika** ze zboczem dodatnim:
  - Na tagu ACK_REI DB F-I/O (strona 178) lub
  - na wejściu ACK_REI_GLOB w instrukcji „ACK_GL" (ACK_GL: „Zatwierdzenie globalne wszystkich F-I/O w grupie F-runtime (STEP 7 Safety V16)" (strona 518))

Sekwencja sygnałów do pasywacji i ponownej integracji F-I/O po błędach komunikacji



① Błąd komunikacji/pasywacja

② Wszystkie błędy komunikacji zostały usunięte

③ Ponowna integracja

Zobacz także

Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia nadrzędnego DP lub sterownika IO (strona 196)

Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia I-slave lub I-device (strona 201)

6.5.3 Po usterce F-I/O lub kanału

Zachowanie po usterce

Wyjście wartości fail-safe po błędach F-I/O	**F-I/O z profilem „RIOforFA-Safety" z F-CPU S7-1200/1500**	**F-I/O bez profilu „RIOforFA-Safety" z F-CPU S7-1200/1500**	**Każdy F-I/O z F-CPU S7-300/400**
W przypadku wykrycia przez system bezpieczeństwa awarii F-I/O, występuje pasywacja wszystkich kanałów całego F-I/O.	QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) Stan wartości = 0*		QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) QBAD_I_xx oraz QBAD_O_xx = 1*

* Stany wartości lub QBAD_I_xx oraz QBAD_O_xx nie są dostępne dla urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe bez profilu „RIOforFA-Safety".

Zachowanie po usterce

Wyjście wartości fail-safe po usterce kanału	**F-I/O z profilem „RIOforFA-Safety" z F-CPU S7-1200/1500**	**F-I/O bez profilu „RIOforFA-Safety" z F-CPU S7-1200/1500**	**Każdy F-I/O z F-CPU S7-300/400**
Gdy skonfigurowana jest pasywacja **całego** F-I/O: W przypadku wykrycia przez system bezpieczeństwa awarii kanału, występuje pasywacja wszystkich kanałów całego F-I/O.	QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) Stan wartości = 0*		QBAD oraz PASS_OUT = 1 Dla **wszystkich** kanałów: Wartość kanału = wartość fail-safe (0) QBAD_I_xx oraz QBAD_O_xx = 1*
Przy konfiguracji pasywacji **szczegółowej kanału**: W przypadku wykrycia przez system bezpieczeństwa awarii kanału, występuje pasywacja wszystkich zakłóconych kanałów całego F-I/O.	QBAD i PASS_OUT **niezmienione** Dla **objętych** kanałów: Wartość kanału = wartość fail-safe (0) Stan wartości = 0	QBAD oraz PASS_OUT = 1 Dla **objętych** kanałów: Wartość kanału = wartość fail-safe (0) Stan wartości = 0*	QBAD oraz PASS_OUT = 1 Dla **objętych** kanałów: Wartość kanału = wartość fail-safe (0) QBAD_I_xx oraz QBAD_O_xx = 1*

* Stany wartości lub QBAD_I_xx oraz QBAD_O_xx nie są dostępne dla urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe bez profilu „RIOforFA-Safety".

Reintegracja F-I/O

Reintegracja odnośnego F-I/O lub odnośnych kanałów F-I/O, czyli zapewnienie danych procesowych w PII lub wyprowadzenie danych dostępnych na PIQ do wyjść fail-safe, odbywa się tylko w następujących przypadkach:

- Wszystkie awarie F-I/O lub kanałów zostały skorygowane.

W przypadku skonfigurowania pasywacji szczegółowej kanałów dla F-I/O, odnośne kanały są reintegrowane, gdy awaria zostanie usunięta; wszelkie uszkodzone kanały pozostają pasywowane.

Reintegracja jest wykonywana zależnie od ustawienia taga ACK_REI lub parametru „Zatwierdzenie awarii kanału" (konfiguracja modułu bezpieczeństwa S7-1500/ET 200MP oraz modułu bezpieczeństwa S7-1200

- Za pomocą ACK_NEC = 0 lub konfiguracją „Zatwierdzenie awarii kanału = automatyczne", wykonywana jest **automatyczna reintegracja** gdy tylko system bezpieczeństwa wykryje, że awaria została usunięta. W przypadku F-I/O z wejściami, reintegracja odbywa się natychmiastowo. W przypadku F-I/O z wyjściami lub F-I/O z wejściami i wyjściami, zależnie od stosowanego F-I/O, reintegracja może potrwać kilka minut; najpierw stosowane są niezbędne sygnały testowe, pozwalające na określenie, czy usterka została usunięta.
- Za pomocą ACK_NEC = 1 lub konfiguracja „Zatwierdzenie awarii kanału = ręczne", reintegracja jest wykonywana po zatwierdzeniu użytkownika zboczem dodatnim na tagu ACK_REI DB F-I/O DB lub na wejściu ACK_REI_GLOB instrukcji „ACK_GL". Zatwierdzenie można wykonać niezwłocznie po wykryciu przez system bezpieczeństwa, że usterka została usunięcia, a tag ACK_REQ = 1 został ustawiony.

  W przypadku urządzeń I/O opartych na GSD typu fail-safe z profilem „RIOforFA-Safety", należy odnieść się do odpowiedniej dokumentacji urządzenia.

OSTRZEŻENIE

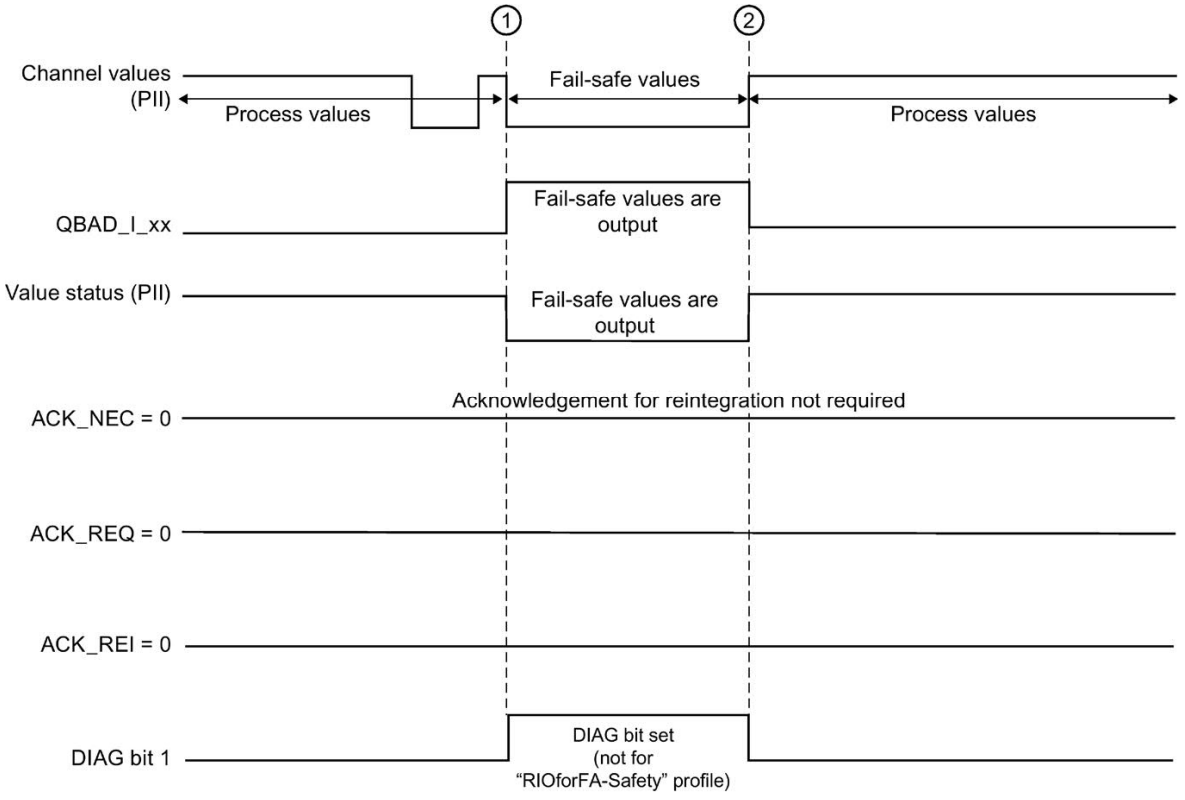
Po awarii zasilania F-I/O trwającej krócej niż wyznaczony czas monitorowania bezpieczeństwa dla F-I/O, automatyczna reintegracja może wystąpić niezależnie od ustawienia znacznika ACK_NEC lub parametru „Zatwierdzenie awarii kanału", zgodnie z opisem w przypadku, gdy ACK_NEC = 0 lub konfiguracja „Zatwierdzenie awarii kanału = automatyczne".

Jeśli automatyczna reintegracja nie jest dozwolona w odnośnym procesie, należy zaprogramować ochronę rozruchu, wykonując ocenę tagów QBAD lub QBAD_I_xx oraz QBAD_O_xx bądź stan wartości lub PASS_OUT.

W przypadku awarii zasilania F-I/O trwającej dłużej niż określony czas monitorowania bezpieczeństwa dla F-I/O, system bezpieczeństwa wykryje błąd komunikacji. *(S012)*

Sekwencja sygnałów do pasywacji i ponownej integracji F-I/O po awarii F-I/O lub kanału, gdy ACK_NEC = 0 lub konfiguracja „Zatwierdzenie awarii kanału = automatyczne" (dla pasywacji całego F-I/O po awarii kanałów)

Przykład do F-I/O z wejściami:



① Awaria kanału lub F-I/O
Pasywacja

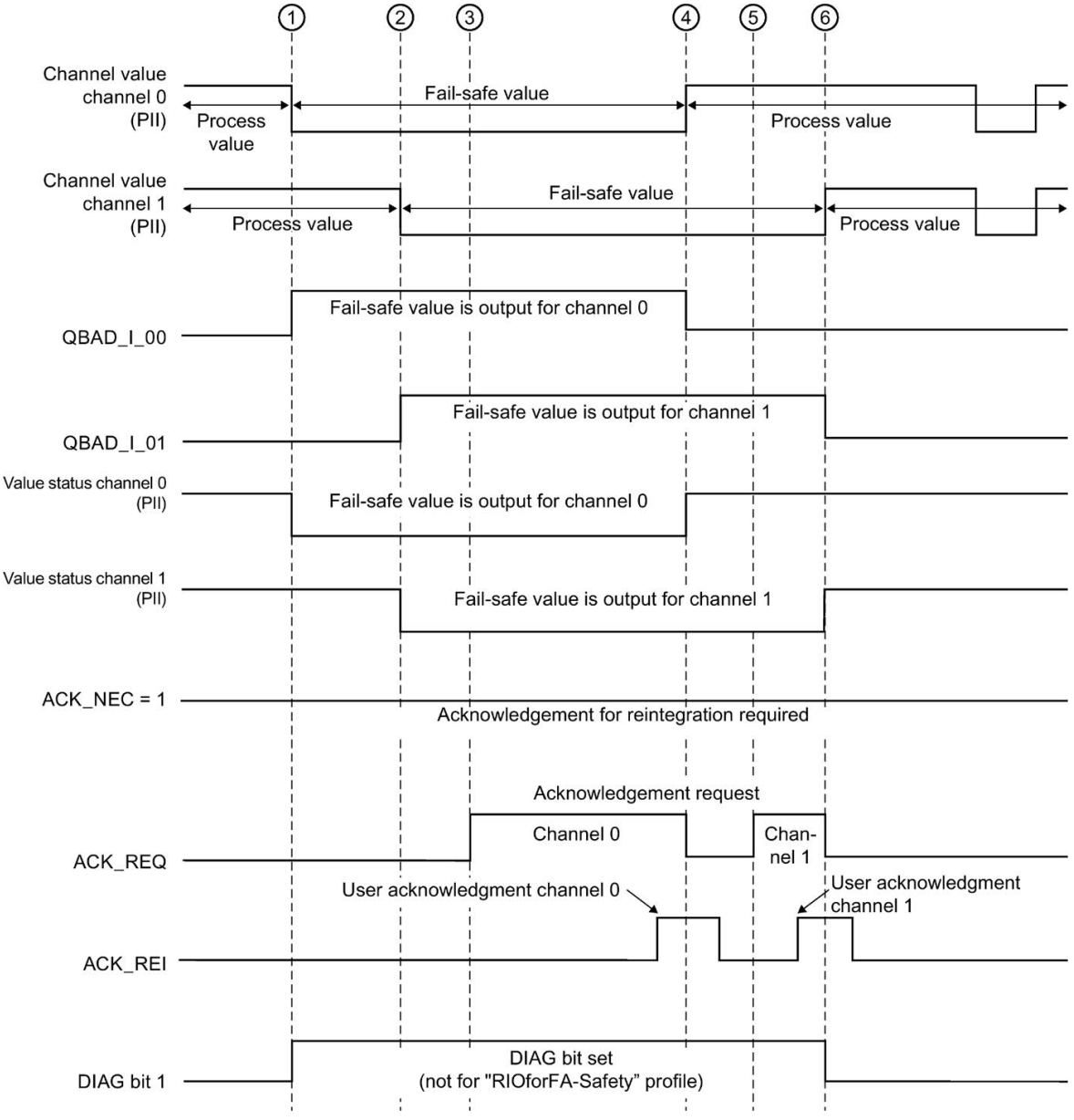
② Awaria kanału lub F-I/O skorygowana
Automatyczna reintegracja

Sekwencja sygnałów do pasywacji i ponownej integracji F-I/O po awarii F-I/O lub kanału, gdy ACK_NEC = 1 lub konfiguracja „Zatwierdzenie awarii kanału = ręczne" (dla pasywacji całego F-I/O po awarii kanałów)

Sekwencja sygnałów do pasywacja i ponownej integracji F-I/O po awarii F-I/O lub kanału, gdy ACK_NEC = 1 lub konfiguracja „Zatwierdzenie awarii kanału = ręczne" (wartość początkowa), patrz „Po błędach komunikacji" (strona 188).

Sekwencja sygnałów do pasywacji i ponownej integracji F-I/O po awarii kanału, gdy ACK_NEC = 1 lub konfiguracja „Zatwierdzenie awarii kanału = ręczne" (dla pasywacji szczegółowej kanału)

Przykład do F-I/O z wejściami:



① Awaria kanału 0/pasywacja kanału 0

② Awaria kanału 1/pasywacja kanału 1

③ Awaria kanału wyeliminowana dla kanału 0

④ Reintegracja kanału 0

⑤ Awaria kanału wyeliminowana dla kanału 1

⑥ Reintegracja kanału 1

6.5.4 Pasywacja grupy

Programowanie pasywacji grupy

Aby włączyć pasywację dodatkowego F-I/O podczas pasywowania F-I/O lub kanału w F-I/O przez systemy bezpieczeństwa, za pomocą tagów PASS_OUT/PASS_ON można wykonać **pasywację grupy** powiązanego F-I/O.

Pasywacja grupy za pomocą PASS_OUT/PASS_ON pozwala, przykładowo, do wymuszenia jednoczesnej reintegracji wszystkich F-I/O po uruchomieniu systemu bezpieczeństwa.

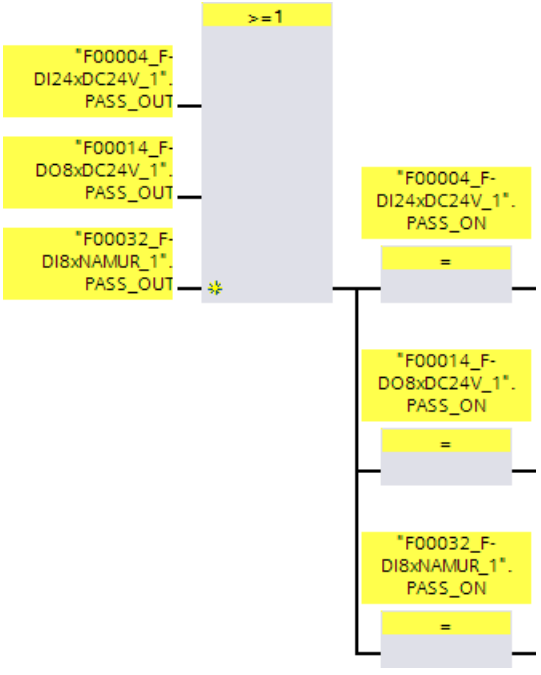
W przypadku pasywacji należy wykonać operację logiczną OR dla wszystkich tagów PASS_OUT z F-I/O w grupie i przypisać wynik do wszystkich tagów PASS_ON F-I/O w grupie.

Podczas korzystania z wartości fail-safe (0) ze względu na pasywację grupy za pomocą PASS_ON = 1, tag QBAD F-I/O tej grupy = 1.

Uwaga

Należy pamiętać o różnym zachowaniu PASS_OUT do F-I/O z/bez profili „RIOforFA-Safety (patrz tabela w dziale „QBAD/PASS_OUT/DISABLED/QBAD_I_xx/QBAD_O_xx i stan wartości (strona 181)).

Przykład pasywacji grupy

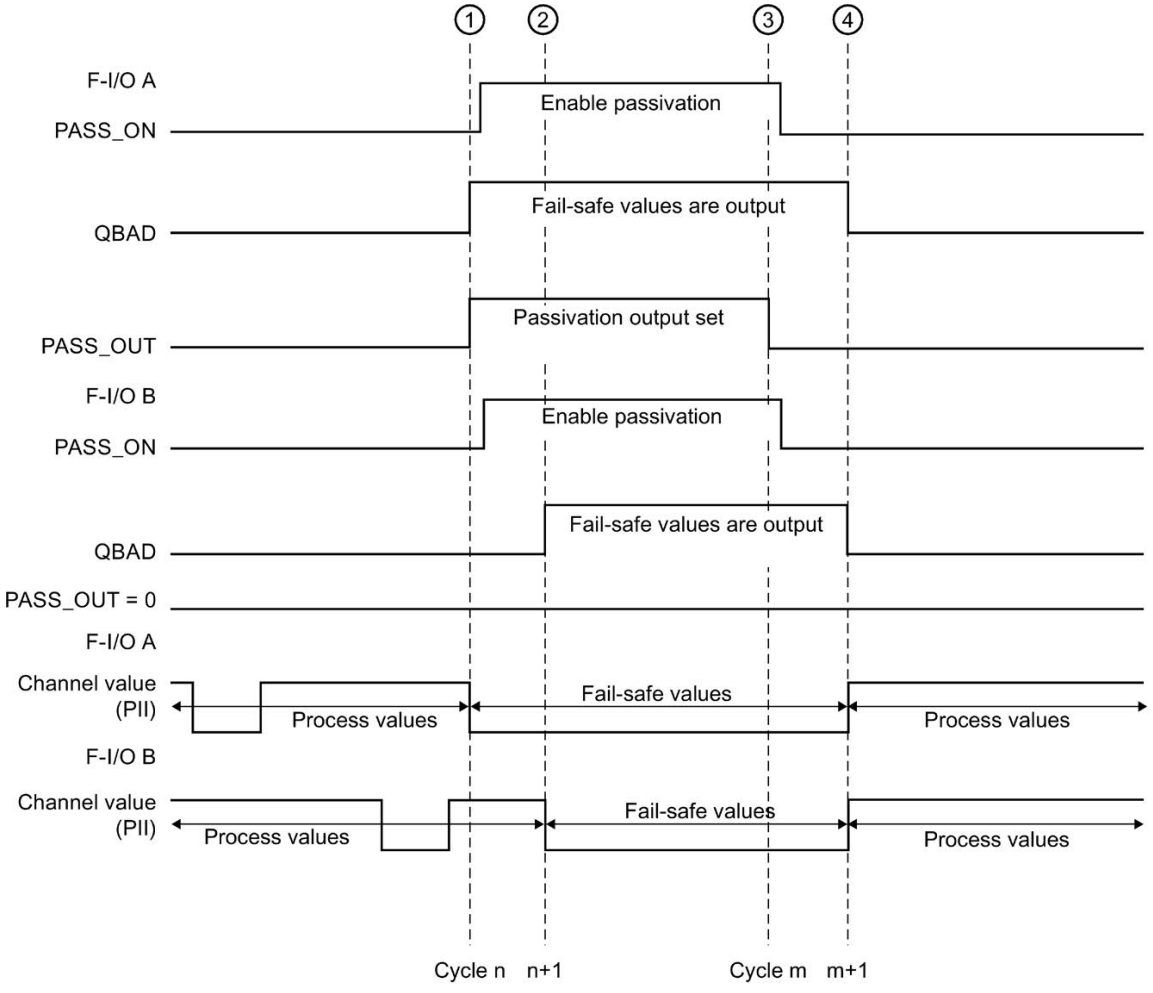


Reintegracja F-I/O

Reintegracja pasywowanego F-I/O przez pasywację grupy następuje **automatycznie**, jeśli reintegracja (**automatyczna** lub **przez zatwierdzenie użytkownika**) występuje dla F-I/O, który wyzwolił pasywację grupy (PASS_OUT = 0).

Sekwencja sygnałowa dla pasywacji grupy po błędzie komunikacji

Przykład do dwóch F-I/O z wejściami:



① Błąd komunikacji z F-I/O A
Pasywacja F-I/O A

② Pasywacja F-I/O B

③ Błąd komunikacji z F-I/O A skorygowany i zatwierdzony

④ Reintegracja F-I/O A i B

Wdrożenie zatwierdzenia użytkownika 7

7.1 Wdrażanie zatwierdzenia użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia nadrzędnego DP lub sterownika IO

Opcje zatwierdzenia przez użytkownika

Zależnie od wyniku analizy ryzyka, dostępne są następujące opcje wdrożenia zatwierdzenia przez użytkownika:

- Przycisk zatwierdzenia, podłączony do F-I/O z wejściami
- Przycisk zatwierdzenia, podłączony do standardowego I/O z wejściami
- System HMI

Zatwierdzenie przez użytkownika przy pomocy przycisku zatwierdzenia

---

Uwaga

W przypadku zastosowania zatwierdzenie przez użytkownika przy pomocy przycisku zatwierdzenia, oraz wystąpieniu błędu komunikacji, usterki F-I/O lub usterki kanału w F-I/O, do którego podłączony jest przycisk, nie będzie możliwe zatwierdzenie reintegracji danego F-I/O.

Takie "zablokowanie" można usunąć jedynie za pomocą przejścia STOP-to-RUN w F-CPU.

Wobec tego, zaleca się, by umożliwić zatwierdzenie za pomocą systemu HMI, aby zatwierdzić reintegrację F-I/O, do którego jest podłączony przycisk zatwierdzenia.

Zatwierdzenie przez użytkownika można wydać za pomocą przycisku zatwierdzenia podłączonego do standardowego I/O z wejściami, jeśli pozwala na to analiza ryzyka.

Zatwierdzenie przez użytkownika przy pomocy systemu HMI

Aby wprowadzić zatwierdzenie przez użytkownika przy pomocy systemu HMI, wymagana jest instrukcja ACK_OP: Zatwierdzenie typu fail-safe (STEP 7 Safety V16) (strona 619).

Procedura programowania zatwierdzenia przez użytkownika za pomocą systemu HMI (S7-300, S7-400)

1. Należy wybrać instrukcję „ACK_OP" w karcie zadań „Instrukcje" i umieścić ją w programie bezpieczeństwa. Sygnał zatwierdzenia do oceny zatwierdzeń użytkownika jest zapewniany przez wyjście OUT w ACK_OP.
2. W systemie HMI należy ustawić pole do ręcznego wprowadzania „acknowledgment value" (wartości zatwierdzenia) „6" (1. krok zatwierdzenia) oraz „wartość zatwierdzenia" „9" (2. krok zatwierdzenia).

   lub

   Należy przypisać przycisk funkcyjny 1 do jednokrotnego przeniesienia „acknowledgment value" (wartości zatwierdzenia) „6" (1. krok zatwierdzenia), oraz przycisk funkcyjny 2 do jednokrotnego przeniesienia „acknowledgment value" (wartości zatwierdzenia) „9" (2. krok zatwierdzenia). Konieczne jest przypisanie we/wy IN (obszar danych w instrukcji ACK_OP) do pola lub przycisków funkcyjnych.
3. Opcjonalnie: W systemie HMI należy ocenić wyjście Q w instancji DB w ACK_OP, by wskazać ramkę czasową, w ramach której musi wystąpić 2. krok zatwierdzenia, lub by wskazać, że 1. krok zatwierdzenia został wykonany.

Jeśli zatwierdzenie przez użytkownika ma być wykonywane wyłączenie z urządzenia programistycznego luib PC przy użyciu tabeli monitorowania (tag monitoruj/modyfikuj), bez konieczności wyłączania trybu bezpieczeństwa, należy przenieść argument (słowo pamięci lub DBW z DB standardowego programu użytkownika) na we/wy IN podczas wywoływania ACK_OP. Można następnie przenieś "wartości zatwierdzenia" „6" i „9" do urządzenia programistycznego lub PC poprzez zmodyfikowanie słowa pamięci lub DBW z DB. Słowo pamięci lub DBW z DB nie może być zapisywane przez program.

Uwaga

W przypadku podłączenia we/wy IN do słowa pamięci lub DBW z DB, należy użyć oddzielnego słowa pamięci lub DBW z DB ze standardowego programu użytkownika dla każdej instancji instrukcji ACK_OP na wejściu/wyjściu IN.

⚠ OSTRZEŻENIE

Dwa kroki zatwierdzenia **nie mogą** być wyzwalane przez jedną operację, przykładowo, przez automatyczne zapisanie ich wraz z warunkami czasowymi w programie, a następnie uruchamiane przez pojedynczy przycisk.
Zapewnienie dwóch oddzielnych kroków zatwierdzenia zapobiega również błędnemu wyzwoleniu zatwierdzenia w systemie HMI nieodpornym na uszkodzenia. *(S013)*

7.1 Wdrażanie zatwierdzenia użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia nadrzędnego DP lub sterownika IO

OSTRZEŻENIE

W przypadku systemów HMI i F-CPU, które są wzajemnie połączone i użycia instrukcji ACK_OP do zatwierdzenia typu fail-safe, należy upewnić się, że zamierzony F-CPU zostanie zaadresowany **przed** wykonaniem dwóch kroków zatwierdzenia.

- W tym celu należy zapisać nazwę unikalną w całej sieci* dla F-CPU e DB standardowego programu użytkownika dla każdego F-CPU.
- W systemie HMI należy ustawić pole, z którego można odczytać nazwę F-CPU dla DB online przed wykonaniem dwóch kroków zatwierdzenia.
- Opcjonalnie:

  W systemie HMI należy ustawić pole do trwałego zapisu nazwy F-CPU. Następnie można określić, czy zamierzony F-CPU jest adresowany poprzez zwykłe porównanie odczytu online nazwy F-CPU z trwale zapisaną nazwą. *(S014)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci.

Uwaga

Konfiguracja systemu kontroli operatorskiej i monitorowania nie ma wpływu na zbiorczy podpis bezpieczeństwa.

Procedura programowania zatwierdzenia przez użytkownika za pomocą systemu HMI (S7-1200, S7-1500)

1. Należy wybrać instrukcję „ACK_OP" w karcie zadań „Instrukcje" i umieścić ją w programie bezpieczeństwa. Sygnał zatwierdzenia do oceny zatwierdzeń użytkownika jest zapewniany przez wyjście OUT w ACK_OP.
2. Należy przypisać do wejścia ACK_ID identyfikator z zakresu od 9 do 30000 w celu
3. zatwierdzenia. Należy przypisać do we/wy IN słowo pamięci lub DBW z DB

   standardowego programu użytkownika.

   Uwaga

   Dla każdej instancji instrukcji ACK_OP należy zapewnić parametr we/wy IN z oddzielnym słowem pamięci lub DBW z DB standardowego programu użytkownika.

4. W systemie HMI należy ustawić pole do ręcznego wprowadzania „acknowledgment value" (wartości zatwierdzenia) „6" (1. krok zatwierdzenia) oraz „identyfikator" skonfigurowany na wejściu ACK_ID (2. krok zatwierdzenia).

   lub

   Przypisać przycisk funkcyjny 1 do jednorazowego transferu „wartości zatwierdzenia" „6" (1. krok zatwierdzenia) oraz przycisk funkcyjny 2 do jednorazowego transferu „identyfikatora" ustawionego w wejściu ACK_ID (2. krok zatwierdzenia).
   Konieczne jest przypisanie słowa pamięci lub DBW z DB standardowego programu użytkownika przypisanego do we/wy IN do pola lub przycisków funkcyjnych.

5. Opcjonalnie: W systemie HMI należy ocenić wyjście Q w instancji DB w ACK_OP, by wskazać ramkę czasową, w ramach której musi wystąpić 2. krok zatwierdzenia, lub by wskazać, że 1. krok zatwierdzenia został wykonany.

⚠ OSTRZEŻENIE

Dwa kroki zatwierdzenia **nie mogą** być wyzwalane przez jedną operację, przykładowo, przez automatyczne zapisanie ich wraz z warunkami czasowymi w programie, a następnie uruchamiane przez pojedynczy przycisk.
Zapewnienie dwóch oddzielnych kroków zatwierdzenia zapobiega również błędnemu wyzwoleniu zatwierdzenia w systemie HMI nieodpornym na uszkodzenia. *(S013)*

⚠ OSTRZEŻENIE

W przypadku systemów HMI i F-CPU, które są wzajemnie połączone i użycia instrukcji ACK_OP do zatwierdzenia typu fail-safe, należy upewnić się, że zamierzony F-CPU zostanie zaadresowany **przed** wykonaniem dwóch kroków zatwierdzenia.

Alternatywa 1:

- Wartość dla każdego identyfikatora zatwierdzenia (wejście ACK_ID; rodzaj danych: INT) można wybrać dowolnie z zakresu od 9 do 30000, lecz musi być unikalna w całej sieci* dla wszystkich instancji instrukcji ACK_OP.
  Należy doprowadzić wartości stałe do wejścia ACK_ID podczas wywoływania instrukcji. Bezpośredni dostęp do odczytu lub zapisu w powiązanej instancji DB jest niedozwolony w programie bezpieczeństwa!

Alternatywa 2:

- Należy zapisać nazwę unikalną w całej sieci* dla F-CPU e DB standardowego programu użytkownika dla każdego F-CPU.
- W systemie HMI należy ustawić pole, z którego można odczytać nazwę F-CPU dla DB online przed wykonaniem dwóch kroków zatwierdzenia.
- Opcjonalnie:

  W systemie HMI należy ustawić pole do trwałego zapisu nazwy F-CPU. Następnie można określić, czy zamierzony F-CPU jest adresowany przez zwykłe porównanie odczytu online nazwy F-CPU z trwale zapisaną nazwą. *(S047)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci.

Uwaga

Zasilenie wejścia/wyjścia IN instrukcji ACK_OP, a także skonfigurowanie systemu kontroli operatorskiej i monitorowania nie ma wpływu na zbiorczy podpis bezpieczeństwa, zbiorczy podpis F-SW czy podpis bloku, który wywołuje instrukcję ACK_OP.

Zmiany w zasileniu wejścia/wyjścia IN lub konfiguracji systemu kontroli operatorskiej i monitorowania nie skutkują zatem zmianą zbiorczego podpisu bezpieczeństwa / zbiorczego podpisu F-SW / podpisu bloku wywołującego.

Przykład procedury programowania zatwierdzenia przez użytkownika do reintregracji F-I/O

1. Opcjonalnie: należy ustawić tag ACK_NEC w odnośnym F-I/O DB (strona 177) na „0", jeśli automatyczna reintegracja (bez zatwierdzenia przez użytkownika) ma zostać wykonana po usterce F-I/O lub awarii kanału.

   OSTRZEŻENIE

   Przypisanie parametru znacznika ACK_NEC = 0 jest dozwolone jedynie, bit zgodności reintegracja jest dopuszczalna dla odnośnego procesu pod względem bezpieczeństwa. *(S010)*

2. Opcjonalnie: Można ocenić tagi QBAD lub QBAD_I_xx/QBAD_O_xx (S7-300/400) bądź status wartości (S7-1200, S7-1500) lub DIAG w odnośnym F-I/O DB, by wyzwolić lampkę sygnalizacyjną w razie wystąpienia błędu, i/lub wygenerować komunikaty o błędzie w systemie HMI standardowego programu użytkownika poprzez ocenę powyższych tagów lub statusu wartości. Komunikaty te można ocenić przed wykonaniem operacji zatwierdzania.
   Alternatywnie można ocenić bufor diagnostyczny F-CPU.
3. Opcjonalnie: Istnieje możliwość oceny taga ACK_REQ w odnośnym F-I/O DB, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy zatwierdzenie jest wymagane.
4. Należy przypisać wejście przycisku zatwierdzenia lub wyjście OUT instrukcji ACK_OP do taga ACK_REI w odnośnym F-I/O DB lub wejście ACK_REI_GLOB instrukcji ACK_GL (patrz powyżej).

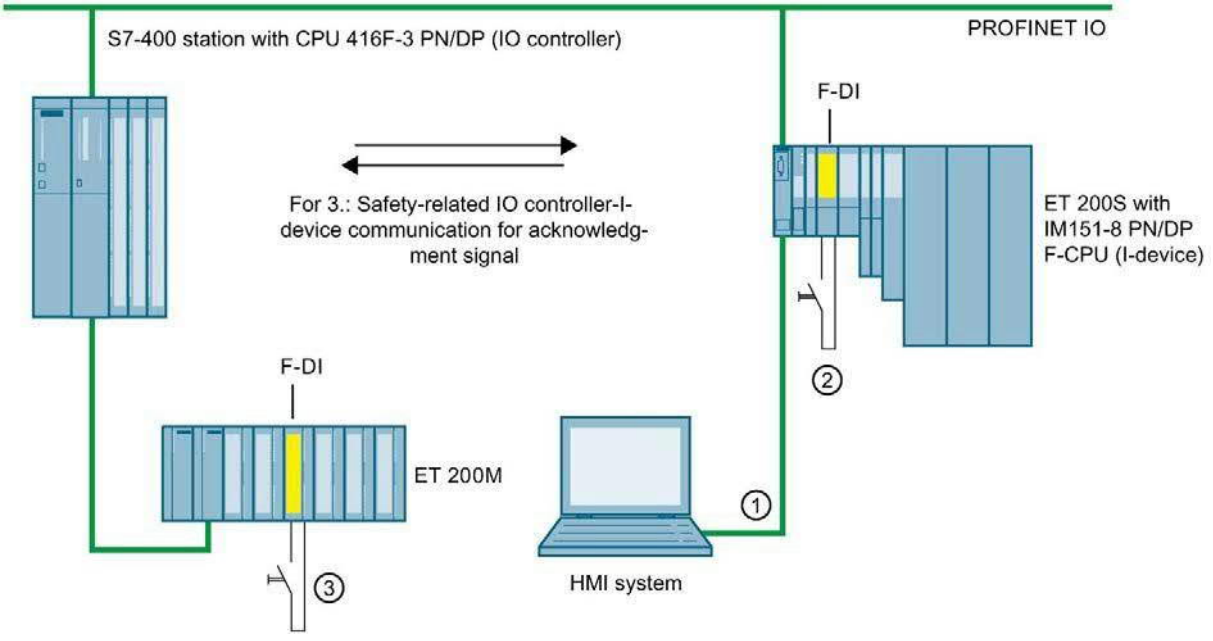
7.2 Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia I-slave lub I-device

Opcje zatwierdzenia przez użytkownika

Zatwierdzenie przez użytkownika można wprowadzić za pomocą:

- Systemu HMI, który pozwala na dostęp do F-CPU urządzenia I-slave/
- I-device
- Przycisku zatwierdzenia, podłączonego do F-I/O z wejściami przypisanymi do F-CPU urządzenia I-slave/ I-device

Te trzy opcje zostały zilustrowane poniżej.



1. Zatwierdzenie przez użytkownika przy pomocy systemu HMI, który pozwala na dostęp do F-CPU urządzenia I-slave/ I-device

ACK_OP: Instrukcja zatwierdzenia typu fail-safe (STEP 7 Safety V16) (strona 619) jest wymagana do wdrożenia zatwierdzenia przez użytkownika przy pomocy systemu HMI, który pozwala na dostęp do F-CPU urządzenia I-slave/ I-device.

Procedura programowania

Należy wykonać procedurę opisaną we „Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia nadrzędnego DP lub sterownika IO" (strona 196) pod hasłem „Procedura programowania...".

Z systemu HMI można uzyskać bezpośredni dostęp do instancji DB ACK_OP w urządzeniu I-slave/ I-device.

2. Zatwierdzenie przez użytkownika za pomocą przycisku zatwierdzenia w F-I/O z wejściami przypisanymi do F-CPU urządzenia I-slave/ I-device

Uwaga

W razie błędu komunikacji, usterki F-I/O lub awarii kanału w F-I/O, do którego podłączony jest przycisk zatwierdzenia, zatwierdzenie do reintegracji tego F-I/O nie jest możliwe.

Takie „zablokowanie" można usunąć jedynie za pomocą przejścia STOP-to-RUN w F-CPU I-device-slave/I-device.

Wobec tego, zaleca się, by umożliwić zatwierdzenie za pomocą systemu HMI, z pomocą którego możliwy jest dostęp do F-CPU urządzenia I-slave/ I-device, aby zatwierdzić reintegrację F-I/O, do którego jest podłączony przycisk zatwierdzenia (patrz 1).

3. Zatwierdzenie przez użytkownika za pomocą przycisku zatwierdzenia w F-I/O z wejściami przypisanymi do F-CPU urządzenia nadrzędnego DP/ sterownika IO

Aby użyć przycisku zatwierdzenia podłączonego przypisanego do F-CPU w urządzeniu nadrzędnym DP /sterowniku IO w celu wykonania zatwierdzenia przez użytkownika w programie bezpieczeństwa w F-CPU urządzenia I-slave/ I-device, należy przenieść sygnał zatwierdzenia z programu bezpieczeństwa w F-CPU urządzenia nadrzędnego DP /sterownika IO do programu bezpieczeństwa w F-CPU urządzenia I-slave/ I-device, korzystając z komunikacji urządzenie podrzędne - urządzenie nadrzędne / I-device - sterownik IO.

1. Umieścić instrukcję SENDDP (strona 631) w programie bezpieczeństwa w F-CPU urządzenia nadrzędnego DP/sterownika IO.
2. Umieścić instrukcję RCVDP (strona 631) w programie bezpieczeństwa w F-CPU urządzenia I-slave/ I-device.
3. Doprowadzić wejście przycisku zatwierdzenia do SD_BO_xx w SENDDP.

4. Sygnał zatwierdzenia do oceny potwierdzeń użytkownika jest dostępny na odnośnym wyjściu RD_BO_xx w RCVDP.

   Sygnał zatwierdzenia można teraz odczytać w sekcjach programu, w których będzie miało miejsce dalsze przetwarzanie z pełnym dostępem bezpośrednio w powiązanej instancji DB (przykładowo, "RCVDP_DB".RD_BO_02).

5. Należy zasilić odnośne wejście SUBBO_xx w RCVDP za pomocą wartości „FALSE" (wartość fail-safe 0), by zapewnić, iż zatwierdzenie przez użytkownika nie zostanie przypadkowo wyzwolone przed ustanowieniem komunikacji po raz pierwszy po uruchomieniu wysyłania i odbioru systemów bezpieczeństwa, lub w przypadku błędu komunikacji związanej z bezpieczeństwem.

Uwaga

W przypadku błędu komunikacji, usterki F-I/O lub awarii kanału w F-I/O, do którego podłączony jest przycisk zatwierdzenia, zatwierdzenie do reintegracji tego F-I/O nie jest możliwe.

Takie „zablokowanie" można usunąć jedynie za pomocą przejścia STOP-to-RUN w F-CPU urządzenia nadrzędnego DP/sterownika IO.

Wobec tego, zaleca się, by umożliwić zatwierdzenie za pomocą systemu HMI, z pomocą którego możliwy jest dostęp do F-CPU urządzenia nadrzędnego DP/sterownika IO, aby zatwierdzić reintegrację F-I/O, do którego jest podłączony przycisk zatwierdzenia.

Jeśli wystąpi błąd komunikacji urządzenie nadrzędne safety – urządzenie I-slave / sterownik IO – I-device, nie będzie możliwe przesłanie sygnału zatwierdzenia, a także zatwierdzenie do reintegracji komunikacji związanej z bezpieczeństwem nie jest możliwe.

Takie „zablokowanie" można usunąć jedynie za pomocą przejścia STOP-to-RUN w F-CPU urządzenia I-slave/I-device.

Wobec tego, zaleca się, by umożliwić zatwierdzenie za pomocą systemu HMI, z pomocą którego możliwy jest dostęp do F-CPU urządzenia I-slave/ I-device, aby zatwierdzić reintegrację komunikacji związanej z bezpieczeństwem do przekazywania sygnału zatwierdzenia (patrz 1).

Wymiana danych pomiędzy standardowym programem użytkownika a programem bezpieczeństwa

8

Dostępna jest opcja przenoszenia danych pomiędzy programem bezpieczeństwa a standardowym programem użytkownika. Przenoszenie tagów jest możliwe poprzez DB, F-DB oraz pamięć bitową:

	Ze standardowego programu użytkownika		**Z programu bezpieczeństwa**	
	Ochrona odczytu	**Ochrona zapisu**	**Ochrona odczytu**	**Ochrona zapisu**
Tag z DB	Dozwolone	Dozwolone	Tag z DB może być objęty ochroną odczytu *lub* ochroną zapisu	
Tag z F-DB	Dozwolone	**Niedozwolone**	Dozwolone	Dozwolone
Pamięć bitowa	Dozwolone	Dozwolone	Pamięć bitowa może być objęta ochroną odczytu *lub* ochroną zapisu	

Możliwy jest również dostęp do obrazu procesustandardowego I/O oraz F-I/O:

		Ze standardowego programu		**Z programu bezpieczeństwa**	
		Ochrona odczytu	**Ochrona zapisu**	**Ochrona**	**Ochrona zapisu**
Obraz procesu standardowego I/O	PII	Dozwolone	Dozwolone	Dozwolone	**Niedozwolone**
	PIQ	Dozwolone	Dozwolone	**Niedozwolone**	Dozwolone
Obraz procesu F-I/O	PII	Dozwolone	**Niedozwolone**	Dozwolone	**Niedozwolone**
	PIQ	Dozwolone	**Niedozwolone**	**Niedozwolone**	Dozwolone

Odłączanie programu bezpieczeństwa od standardowego programu

W przypadku wymiany danych pomiędzy standardowym programem użytkownika a programem bezpieczeństwa, zaleca się zdefiniowanie specjalnych bloków danych (bloków danych transferowych), w których zapisywane są dane do wymiany. Działanie to pozwala na oddzielenie bloków programu standardowego i bezpieczeństwa. Zmiany w standardowym programie nie wypływają na program bezpieczeństwa (i wzajemnie), o ile bloki nie zostaną zmodyfikowane.

8.1 Transfer danych z programu bezpieczeństwa do standardowego programu użytkownika

Transfer danych z programu bezpieczeństwa do standardowego programu użytkownika

Standardowy program użytkownika może odczytywać wszystkie dane programu bezpieczeństwa, na przykład przy użyciu dostępu symbolicznego (w pełni kwalifikowanego) w następujących elementach:

- Instancje DB dla F-FBs („Nazwa instancji".Signal_x)
- F-DB (przykładowo „Nazwa F_DB".Signal_1)
- Wejście obrazu procesuoraz wyjście F-I/O (przykładowo „Przycisk_Zatrzymania_Awaryjnego_1" (I 5.0))

Uwaga

Dla F-CPU S7-300/400

Wejście obrazu procesuF-I/O jest aktualizowane nie tylko na początku głównego bloku bezpieczeństwa, lecz także przez standardowy system operacyjny.

Aby odszukać czasy aktualizacji standardowego systemu operacyjnego, należy odnieść się do *pomocy STEP 7*, hasło „Wejście i wyjście obrazu procesowego". W przypadku F-CPU, które obsługują podział obrazu, należy pamiętać o czasach aktualizacji podczas korzystania z podziału obrazów procesowych. Z tego względu, podczas wykorzystywania wejścia obrazu procesuF-I/O w standardowym programie użytkownika, możliwe jest uzyskanie wartości innych niż w programie bezpieczeństwa. Różnica w wartościach może wystąpić z powodu:

- Różnych czasów aktualizacji
- Użycia wartości fail-safe w programie bezpieczeństwa

Aby uzyskać identyczne wartości w standardowym programie użytkownika i w programie bezpieczeństwa, nie należy otwierać wejścia obrazu procesuw standardowym programie aż do wykonania grupy F-runtime. W takim przypadku można również ocenić tag QBAD lub QBAD_I_xx tag w powiązanym F-I/O DB w standardowym programie użytkownika, aby sprawdzić, czy wejście obrazu procesuodbiera wartości fail-safe (0) lub dane procesowe. Podczas korzystania z podziału obrazu procesowego, należy również upewnić się, że obraz procesu nie został zaktualizowany przez standardowy program użytkownika lub przez instrukcję UPDAT_PI pomiędzy wykonaniem grupy F-runtime a oceną wejścia obrazu procesuw standardowym programie.

Uwaga

Dla F-CPU S7-1200/1500

Wejście obrazu procesuF-I/O jest aktualizowane przed przetworzeniem głównego bloku bezpieczeństwa.

Dane programu bezpieczeństwa można także zapisać bezpośrednio w standardowym programie użytkownika (patrz tabela obsługiwanych obszarów argumentów w: „Ograniczenia w językach programowania FBD/LAD" (strona 121)):

Blok danych/pamięć bitowa

Aby zapisać dane programu bezpieczeństwa bezpośrednio w standardowym programie użytkownika (np. wyjście DIAG, instrukcja SENDDP), można wykonać zapis do bloków danych standardowego programu z programu bezpieczeństwa. Jednakże, zapisywany tag nie może być odczytywany w samym programie bezpieczeństwa.

Możliwy jest również zapis do pamięci bitowej w programie bezpieczeństwa. Jednakże, zapisywana pamięć bitowa nie może być odczytywana w samym programie bezpieczeństwa.

Wyjście obrazu procesowego

Istnieje możliwość zapisu wyjścia obrazu procesu(PIQ) standardowego I/O w programie bezpieczeństwa, na przykład w celu wyświetlania go. PIQ nie może być odczytywane w programie bezpieczeństwa.

8.2 Transfer danych ze standardowego programu do programu bezpieczeństwa

Transfer danych ze standardowego programu do programu bezpieczeństwa

Podstawowa zasada stanowi, że jedynie dane typu fail-safe lub sygnały fail-safe z F-I/O oraz innych programów bezpieczeństwa (w innych F-CPU) mogą być przetwarzane w programie bezpieczeństwa, jako że standardowe tagi nie są bezpieczne.

Jeśli konieczne jest przetworzenie tagów ze standardowego programu użytkownika w programie bezpieczeństwa, można jednakże ocenić pamięć bitową ze standardowego programu użytkownika, tagi ze standardowego DB lub wejścia obrazu procesowego (PII) standardowego I/O w programie bezpieczeństwa (patrz tabela obsługiwanych obszarów argumentów w: „Ograniczenia w językach programowania FBD/LAD" (strona 121)).

Należy pamiętać, że zmiany strukturalne w standardowych blokach danych, używanych w programie bezpieczeństwa, prowadzą do niespójności w programie bezpieczeństwa i mogą spowodować konieczność wpisania hasła. W takim przypadku zbiorczy podpis bezpieczeństwa jest identyczny z oryginalnym po skompilowaniu. Aby nie dopuścić do takiego zdarzenia, należy użyć „bloków komunikacji międzyprocesowej" pomiędzy standardowym programem użytkownika a programem bezpieczeństwa.

OSTRZEŻENIE

Z powodu tego, że znaczniki nie są generowane w bezpieczny sposób, należy wykonać w programie bezpieczeństwa dodatkową kontrolę wykonalności określoną dla procesu, by zapewnić, iż nie wystąpi niebezpieczny stan. Jeśli pamięć bitowa, tag standardowego DB lub wejście standardowego I/O jest wykorzystywane w obu grupach F-runtime, należy wykonać kontrolę wykonalności oddzielnie dla każdej grupy F-runtime. *(S015)*

Aby ułatwić kontrolę, wszystkie tagi PLC ze standardowego programu użytkownika, które są oceniane w programie bezpieczeństwa, są ujęte w podsumowaniu bezpieczeństwa (strona 357).

Pamięć bitowa

Aby przetworzyć tagi standardowego programu użytkownika w programie bezpieczeństwa, można również odczytać pamięć bitową z programu bezpieczeństwa. Jednakże, odczytywana pamięć bitowa nie może być zapisywana w samym programie bezpieczeństwa.

Blok danych

Aby przetworzyć tagi standardowego programu użytkownika w programie bezpieczeństwa, można odczytać tagi z bloków danych standardowego programu użytkownika w programie bezpieczeństwa. Jednakże, odczytywany tag nie może być zapisywany w samym programie bezpieczeństwa.

Wejścia obrazu procesowego

Istnieje możliwość odczytu wejścia obrazu procesu(PII) standardowego I/O w programie bezpieczeństwa. PII nie może być zapisywane w programie bezpieczeństwa.

Przykłady: Programowanie kontroli wykonalności

- Przy pomocy instrukcji Porównania (strona 542) można sprawdzić, czy tagi ze standardowego programu użytkownika wykraczają lub nie dochodzą do dopuszczalnego limitu. Można zmodyfikować funkcję bezpieczeństwa, korzystając z wyniku porównania.
- Należy zastosować instrukcję ---(S)---: Wyjście set (STEP 7 Safety V16) (strona 425), ---(R)---: Wyjście reset (STEP 7 Safety V16) (strona 424) lub SR: Przerzutnik set/reset (STEP 7 Safety V16) (strona 427), przykładowo, ze tagami ze standardowego programu użytkownika, by umożliwić wyłączenie silnika, lecz nie jego włączenia.
- W przypadku sekwencji uruchomieniowych, należy żyć instrukcji operacji logicznych AND, przykładowo, by logicznie połączyć tagi ze standardowego programu użytkownika z warunkami włączenia, które wywodzą się ze tagów fail-safe.

Aby przetworzyć tagi ze standardowego programu użytkownika w programie bezpieczeństwa, należy pamiętać, że nie istnieje wystarczająco prosta metoda do sprawdzenia wykonalności wszystkich tagów.

Odczyt tagów ze standardowego programu użytkownika, które mogą ulec zmianie podczas wykonywania grupy F-runtime

Aby odczytać tagi ze standardowego programu użytkownika (pamięć bitowa, tagi standardowego DB lub PII standardowego I/O) w programie bezpieczeństwa, a mogą one ulec zmianie - poprzez standardowy program użytkownika lub system kontroli operatorskiej i monitorowania - podczas wykonywania grupy F-runtime, w której są odczytywane (na przykład z powodu przetwarzania standardowego programu użytkownika przez przerwanie cykliczne wyższego priorytetu), należy użyć pamięci bitowej lub tagów standardowego DB. Zalecane jest użycie standardowych FC do przetwarzania wstępnego

(strona 86) do F-CPU S7-1200/1500.

(S7-300/400) Należy zapisać pamięć bitową lub tagi standardowego DB ze tagami ze standardowego programu użytkownika niezwłocznie przed wywołaniem grupy F-runtime.

Uzyskuje się w ten sposób dostęp jedynie do tej pamięci bitowej lub tagów standardowego DB w programie bezpieczeństwa.

Należy również pamiętać, że **pamięć zegara**, zdefiniowana podczas konfiguracji F-CPU w zakładce „Properties" (Właściwości) może zmienić się podczas wykonania grupy F-runtime, ponieważ pamięć zegara działa asynchronicznie względem cyklu F-CPU.

Uwaga

F-CPU może przejść w stan STOP, jeśli nie zostanie to wykonane. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Komunikacja safety

9

9.1 Konfiguracja i programowanie komunikacji (S7-300, S7-400)

9.1.1 Przegląd komunikacji

Wstęp

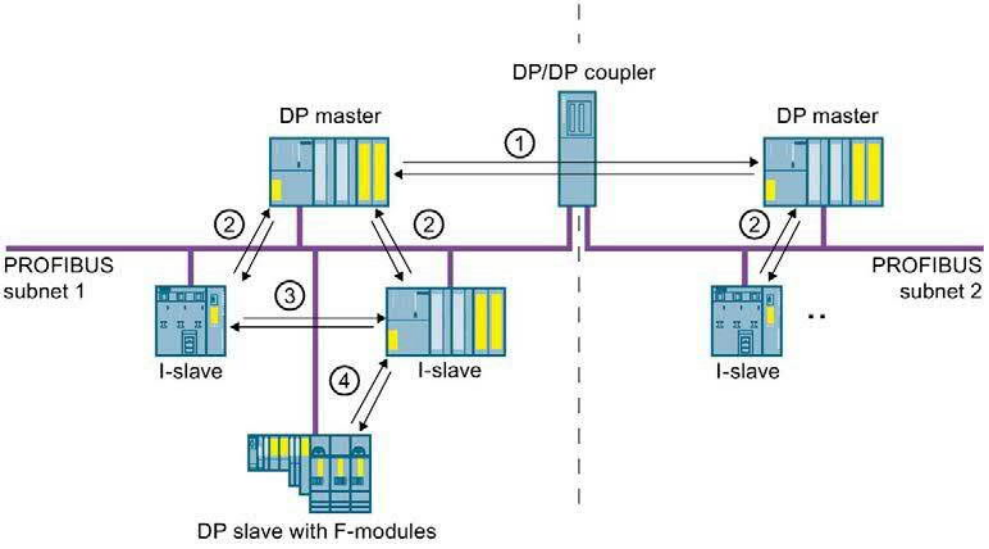
W tym dziale zamieszczono omówienie opcji komunikacji związanej z bezpieczeństwem w systemach bezpieczeństwa SIMATIC Safety.

Opcje komunikacji związanej z bezpieczeństwem

Komunikacja safety	Na podsieci	Wymagany dodatkowy sprzęt
Komunikacja urz. I-slave – urz. podrzędne	PROFIBUS DP	—
Komunikacja CPU safety – CPU:		
Komunikacja sterownik IO – sterownik IO	PROFINET IO	złącze PN/PN
Komunikacja urz. nadrzędne – urz. nadrzędne	PROFIBUS DP	złącze DP/DP
Komunikacja sterownik IO – I-device	PROFINET IO	—
Komunikacja urz. nadrzędne – urz. I-slave	PROFIBUS DP	—
Komunikacja urz. I-slave – urz. I-slave	PROFIBUS DP	—
Komunikacja sterownik IO – urz. I-slave	PROFINET IO i PROFIBUS DP	Połączenie IE/PB
Komunikacja safety poprzez połączenia S7	Przemysłowy Ethernet	—
Komunikacja sterownik IO – sterownik IO dla S7 Distributed Safety	PROFINET IO	złącze PN/PN
Komunikacja urz. nadrzędne – urządzenie nadrzędne do S7 Distributed Safety	PROFIBUS DP	złącze DP/DP
Komunikacja safety do S7 Distributed Safety lub systemów bezpieczeństwa S7 poprzez połączenia S7	Przemysłowy Ethernet	—

Omówienie komunikacji związanej z bezpieczeństwem poprzez PROFIBUS DP

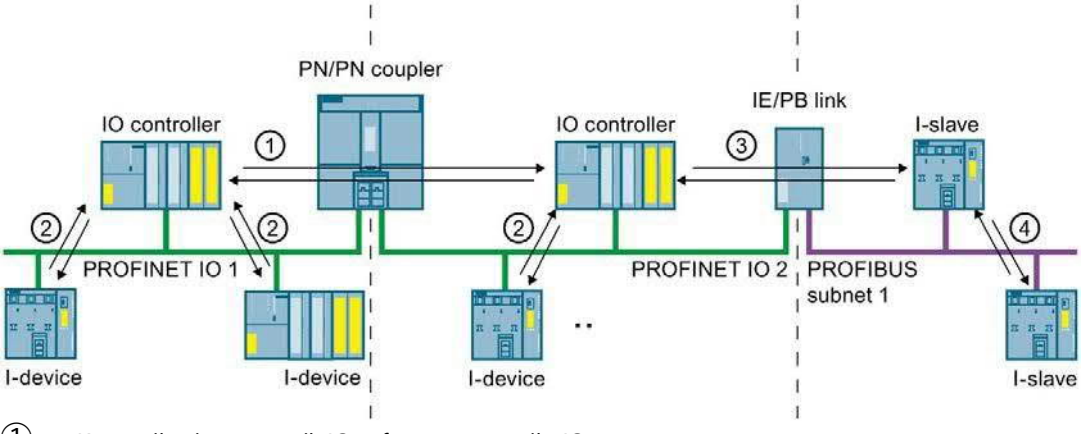
Poniższa ilustracja przedstawia omówienie 4 opcji komunikacji związanej z bezpieczeństwem poprzez PROFIBUS DP w systemach bezpieczeństwa SIMATIC Safety z F-CPU S7-300/400.



① Komunikacja urządzenie nadrzędne związane z bezpieczeństwem–urządzenie nadrzędne
② Komunikacja urządzenie nadrzędne związane z bezpieczeństwem–urządzenie podrzędne I
③ Komunikacja urządzenie podrzędne I związane z bezpieczeństwem–urządzenie I
④ Komunikacja urządzenie I-slave safety–urządzenie podrzędne

Omówienie komunikacji związanej z bezpieczeństwem poprzez PROFINET IO

Poniższa ilustracja przedstawia omówienie czterech opcji komunikacji związanej z bezpieczeństwem poprzez PROFINET IO w systemach bezpieczeństwa SIMATIC Safety z F-CPU S7-300/400. Jeśli stosowane jest połączenie IE/PB, możliwa jest komunikacja safety pomiędzy przypisanymi urządzeniami podrzędnymi I.



① Komunikacja sterownik IO safety – sterownik IO
② Komunikacja sterownik IO safety – I-device
③ Komunikacja sterownik IO safety – urządzenie I-slave
④ Komunikacja urządzenie I-slave safety – urządzenie I-slave, integrująca sterownik IO

Komunikacja CPU safety – CPU poprzez PROFIBUS DP lub PROFINET IO

W komunikacja CPU safety – CPU stała ilość danych typu fail-safe rodzaju BOOL lub INT jest przekazywana pomiędzy programami bezpieczeństwa w F-CPU urządzeń nadrzędnych DP/urządzeń I-slave lub sterownikami IO/urządzeniami I.

Dane są przesyłane przy użyciu instrukcji SENDDP do wysyłania oraz instrukcji RCVDP do odbierania. Dane są przechowywane w skonfigurowanych obszarach transferowych urządzeń. Każdy obszar transferu składa się z jednego obszaru adresowego wejścia i jednego wyjścia.

Komunikacja urządzenie I-slave safety – urządzenie podrzędne poprzez PROFIBUS DP

Komunikacja urządzenie I-slave safety – urządzenie podrzędne F-I/O jest możliwa w urządzeniu podrzędnym DP, które obsługuje komunikację urządzenie I-slave safety – urządzenie podrzędne, na przykład z wszystkim modułami bezpieczeństwa ET 200SP z IM 155-6 DP HF, wersja oprogramowania > V3.1, z wszystkimi modułami bezpieczeństwa ET 200SP z IM 151-1 HF, z wszystkimi modułami sygnałowymi S7-300 typu fail-safe z IM 153-2, od numeru zamówieniowego
6ES7153-2BA01-0XB0, wersja oprogramowania > V4.0.0.

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU urządzenia I-slave a F-I/O urządzenia podrzędnego DP odbywa się przy użyciu bezpośredniej wymiany danych, tak jak w standardowym programie. Do uzyskania dostępu do kanałów F-I/O w programie bezpieczeństwa F-CPU urządzenia I-slave wykorzystywany jest obraz procesu.

Komunikacja CPU safety – CPU poprzez przemysłowy Ethernet

Komunikacja CPU safety – CPU poprzez przemysłowy Ethernet jest możliwa z wykorzystaniem połączeń S7, zarówno do, jak i z następujących opcji:

- F-CPU S7-300 poprzez zintegrowany interfejs PROFINET
- F-CPU S7-400 poprzez zintegrowany interfejs PROFINET lub CP 443-1 bądź CP 443-1 Advanced-IT

W komunikacji związanej z bezpieczeństwem poprzez połączenia S7, określona ilość danych typu fail-safe rodzaju BOOL, INT, WORD, DINT, DWORD lub TIME jest przesyłana w sposób fail-safe pomiędzy programami bezpieczeństwa F-CPU połączonych przez połączenia S7.

Przesył danych wykorzystuje instrukcję SENDS7 do wysyłania oraz instrukcji RCVS7 do odbierania. Dane są wymieniane przy pomocy F-DB („DB komunikacji bezpieczeństwa") umieszczonego po stronie nadawcy i odbiorcy.

Komunikacja CPU safety – CPU do *S7 Distributed Safety* lub *systemów bezpieczeństwa*

Komunikacja safety jest możliwa z F-CPU w *SIMATIC Safety*
do F-CPU w *S7 Distributed Safety* lub *systemach bezpieczeństwa S7*.

9.1.2 Komunikacja sterownik IO safety – sterownik IO

9.1.2.1 Konfiguracja komunikacji sterownik IO safety – sterownik IO

Wstęp

Komunikacja safety pomiędzy programami bezpieczeństwa F-CPU sterowników IO odbywa się poprzez złącze PN/PN, który ustawia się pomiędzy F-CPU.

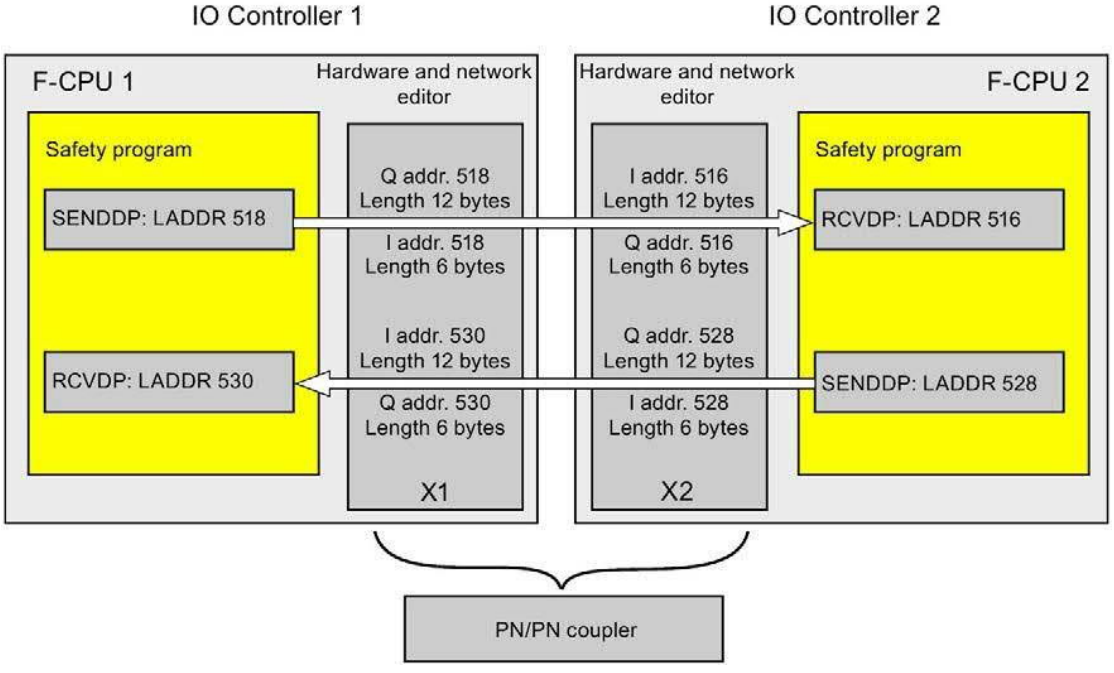
W przypadku F-CPU 416F-2 bez zintegrowanego interfejsu PROFINET, należy użyć CP 443-1 bądź CP 443-1 Advanced-IT.

Uwaga

Należy wyłączyć parametr „Data validity display DIA" (Wyświetlacz ważności danych DIA) we właściwościach złącza PN/PN w *edytorze sprzętu i sieci*. Jest to domyślne ustawienie. W przeciwnym razie komunikacja sterownik IO safety – sterownik IO nie jest możliwa.

Konfigurowanie obszarów transferu

Należy skonfigurować jeden obszar transferowy dla danych wyjściowych oraz jeden obszar dla danych wejściowych w *edytorze sprzętu i sieci* dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU w złączu PN/PN. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać **oraz** odbierać dane (komunikacja dwukierunkowa). Dla każdego z dwóch połączeń komunikacyjnych należy skonfigurować w złączu PN/PN jeden obszar transferowy dla danych wyjściowych oraz jeden dla danych wejściowych.



Zasady definiowania obszarów transferu

Obszar transferu dla danych wyjściowych oraz obszar dla danych wejściowych do **wysyłanych danych** muszą rozpoczynać się od tego samego adresu początkowego. Obszar transferu dla danych wyjściowych wymaga łącznie 12 bajtów (spójnych); obszar transferu dla danych wejściowych wymaga 6 bajtów (spójnych).

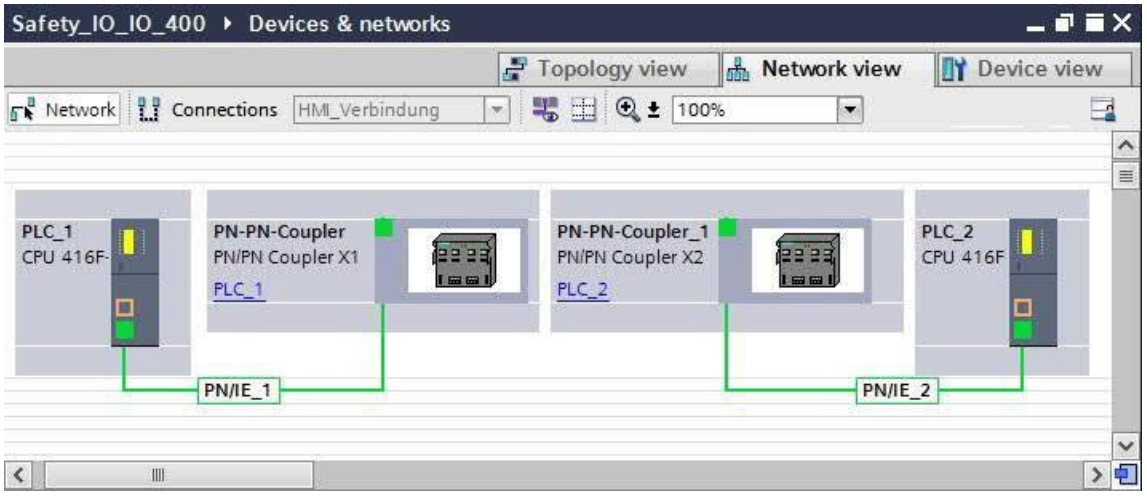
Obszar transferu dla danych wejściowych oraz obszar dla danych wyjściowych do **odbieranych danych** muszą rozpoczynać się od tego samego adresu początkowego. Obszar transferu do danych wejściowych wymaga łącznie 12 bajtów (spójnych); obszar transferu danych wyjściowych wymaga 6 bajtów (spójnych).

Procedura konfiguracji

Procedura konfiguracji komunikacja sterownik IO safety – sterownik IO przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Przełączyć na widok sieci w *edytorze sprzętu i sieci*.
3. Wybrać złącze PN/PN X1 oraz złącze PN/PN X2 z „Other field devices¥PROFINET IO¥Gateway¥Siemens AG¥PN/PN Coupler" w karcie zadań „Hardware catalog" (Katalog sprzętu) i wstawić je do widoku sieci w edytorze.
4. Połączyć interfejs PN F-CPU 1 z interfejsem PN złącza PN/PN X1 oraz interfejs PN F-CPU 2 z interfejsem PN złącza PN/PN X2.



5. Przełączyć na widok urządzenia dla złącza PN/PN X1 do połączeń komunikacji dwukierunkowej, tj. gdy F-CPU jednocześnie wysyła i odbiera dane. Wybrać następujące moduły z pola „IN/OUT" zakładki zadań „Hardware catalog" (Katalog sprzętu) (z aktywnym filtrem), po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń):
   - Jeden moduł „IN/OUT 6 bytes / 12 bytes" oraz
   - Jeden moduł „IN/OUT 12 bytes / 6 bytes"

6. We właściwościach modułu należy przypisać adresy poza obrazem procesowym w następujący sposób:

   W przypadku modułu „IN/OUT 6 bytes / 12 bytes" do wysyłania danych:

   – Adresy wejściowe: Adres początkowy 518

   – Adresy wyjściowe: Adres początkowy 518

   W przypadku modułu „IN/OUT 12 bytes / 6 bytes" do odbierania danych:

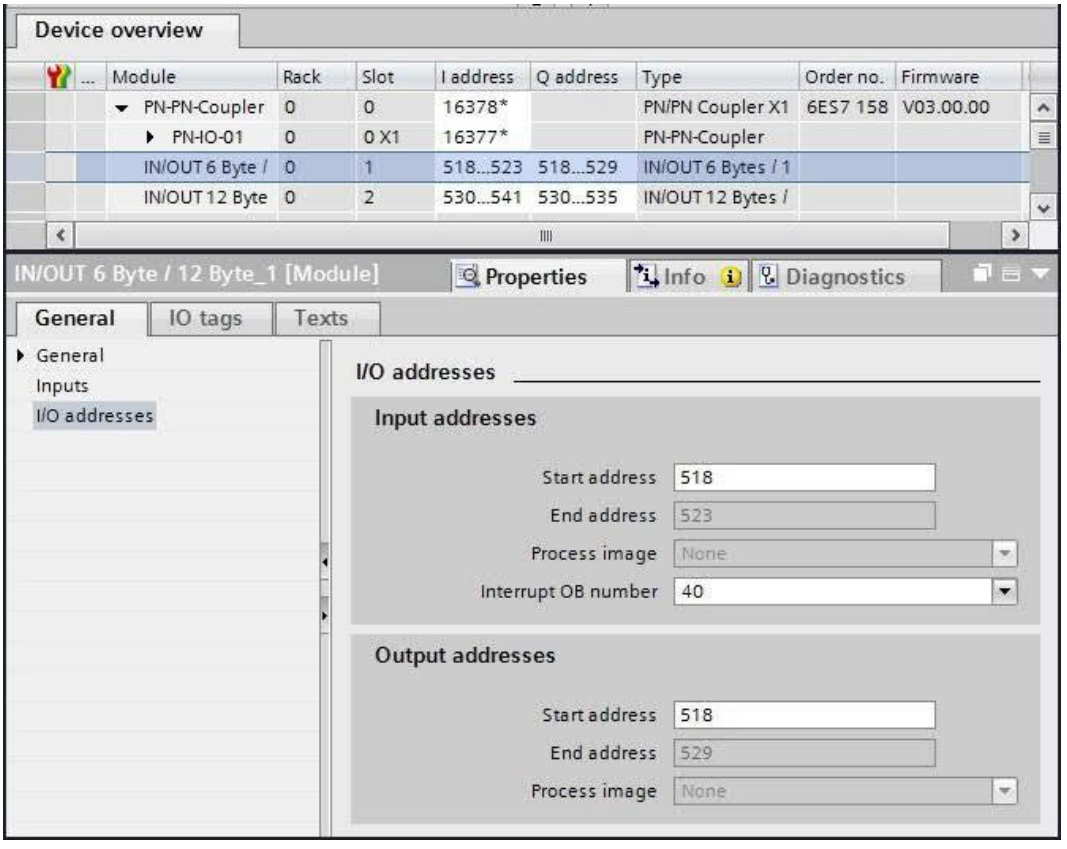
   – Adresy wejściowe: Adres początkowy 530

   – Adresy wyjściowe: Adres początkowy 530

Uwaga

Należy upewnić się, że przypisano identyczne adresy początkowe dla obszarów adresowych danych wejściowych i wyjściowych.

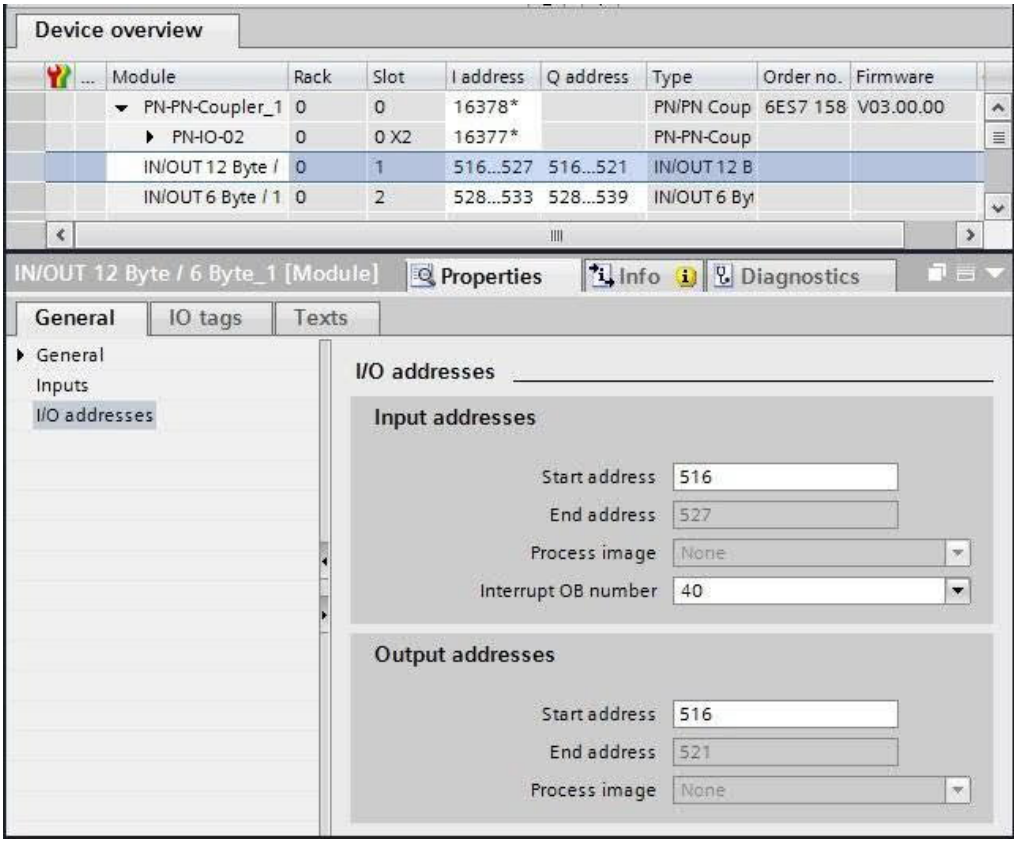
Wskazówka: Należy zanotować adresy początkowe obszarów transferu. Są one potrzebne do zaprogramowania bloków SENDDP i RCVDP (wejście LADDR).



7. Wybrać następujące moduły z pola „IN/OUT" w widoku urządzenia dla złącza PN/PN X2, po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń):
   - Jeden moduł „IN/OUT 12 bytes / 6 bytes" oraz
   - Jeden moduł „IN/OUT 6 bytes / 12 bytes"
8. We właściwościach modułu należy przypisać adresy poza obrazem procesowym w następujący sposób:

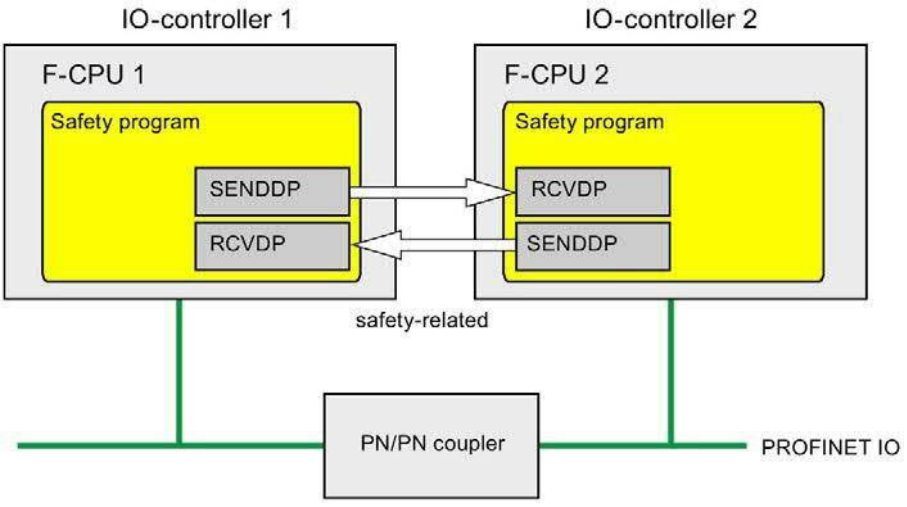
   W przypadku modułu „IN/OUT 12 bytes / 6 bytes" do odbierania danych:
   - Adresy wejściowe: Adres początkowy 516
   - Adresy wyjściowe: Adres początkowy 516

   W przypadku modułu „IN/OUT 6 bytes / 12 bytes" do wysyłania danych:
   - Adresy wejściowe: Adres początkowy 528
   - Adresy wyjściowe: Adres początkowy 528



9.1.2.2 Komunikacja sterownik IO safety – sterownik IO poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU sterowników IO wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych. Można wykorzystać je do wykonywania przesyłu typu fail-safe *stałych* ilość danych typu fail-safe rodzaju INT lub BOOL.

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.1.2.3 Programowanie komunikacji sterownik IO safety – sterownik IO

Wymogi do programowania

Należy skonfigurować obszary transferu do danych wejściowych i wyjściowych złącza PN/PN.

Procedura programowania

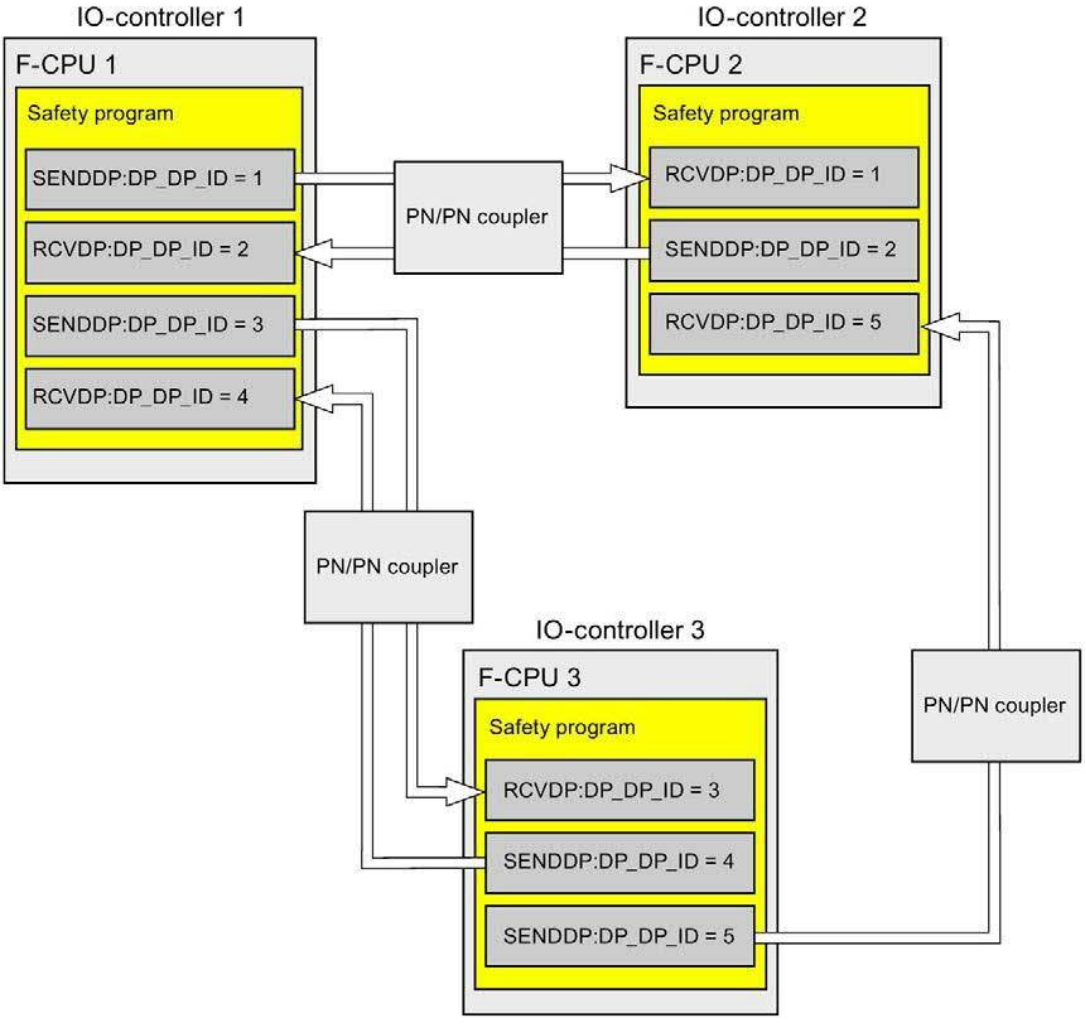
Komunikację sterownik IO safety – sterownik IO programuje się w następujący sposób:

1. W programie bezpieczeństwa, z którego dane będą wysyłane, należy wywołać instrukcję SENDDP (strona 631) w celu wysłania na końcu głównego bloku bezpieczeństwa.
2. W programie bezpieczeństwa, w którym dane będą odbierane, należy wywołać instrukcję RCVDP (strona 631) w celu odebrania na początku głównego bloku bezpieczeństwa.
3. Należy przypisać adresy początkowe obszarów transferu wyjść i wejść złącza PN/PN skonfigurowanego w *edytorze sprzętu i sieci* do odnośnych wejść LADDR.

   Należy wykonać to przypisanie dla każdego połączenia komunikacyjnego w każdym F-CPU.

4. Przypisać wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa do wejść DP_DP_ID. Pozwala to na ustalenie związku komunikacji pomiędzy instrukcją SENDDP w jednym F-CPU a instrukcją RCVDP w drugim F-CPU: Powiązane instrukcje otrzymują tę samą wartość dla DP_DP_ID.

   Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla 5 powiązań komunikacji sterownik IO safety – sterownik IO.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

5. Doprowadzić na wejścia SD_BO_xx i SD_I_xx w SENDDP sygnały wysyłania. Aby ograniczyć sygnały pośrednie podczas przesyłania bloków transferowych, można zapisać wartość bezpośrednio do instancji DB w SENDDP, korzystając z w pełni kwalifikowanego dostępu (przykładowo, "Name SENDDP_1".SD_BO_02) przed wywołaniem SENDDP.
6. Należy doprowadzić na wyjścia RD_BO_xx i RD_I_xx w RCVDP sygnały, które mają dalej być przetwarzane przez inne sekcje programu lub użyć w pełni kwalifikowanego dostępu, by odczytać otrzymane sygnały bezpośrednio z powiązanych instancji DB w sekcjach programu, które będą przetwarzane dalej (np. "Name RCVDP_1".RD_BO_02).
7. Należy zasilić odnośne wejścia SUBBO_xx i SUBI_xx w RCVDP za pomocą wartości fail-safe wyprowadzanej przez RCVDP zamiast danych procesowych, aż zostanie ustanowiona komunikacja po raz pierwszy po uruchomieniu wysyłania i odbioru systemów bezpieczeństwa, lub w przypadku błędu komunikacji związanej z bezpieczeństwem.

   – Specyfikacja stałych wartości fail-safe:

     W przypadku danych rodzaju INT, można wprowadzić stałe wartości fail-safe bezpośrednio jako stałe w wejściu SUBI_xx (wartość początkowa = "0"). Aby określić stałą wartość fail-safe „PRAWDA" dla danych rodzaju BOOL, należy zapewnić tag F_GOBDB".VKE1 dla wejścia SUBBO_xx (wartość początkowa = „FAŁSZ").

– Specyfikacja zmiennych wartości zastępczych:

Aby określić zmienne wartości zastępcze, należy zdefiniować tag obliczany poprzez program bezpieczeństwa w F-DB, po czym określić go (w pełni kwalifikowany) w wejściu SUBI_xx lub SUBBO_xx.

OSTRZEŻENIE

Uwaga: Logika programu do obliczania zmiennych wartości zastępczych może być wstawiona jedynie za wywołaniami RCVDP, ponieważ obszar przed nimi musi być wolny od operacji logicznych. Dlatego też, w pierwszym cyklu po uruchomieniu systemu bezpieczeństwa, we wszystkich instrukcjach RCVDP aktywne są wartości początkowe wartości zastępczych. Należy zatem przypisać do tych znaczników odpowiednie wartości początkowe. *(S017)*

8. Skonfigurować wejścia TIMEOUT instrukcji RCVDP i SENDDP, wprowadzając wymagany czas monitorowania.

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawce i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

9. Opcjonalnie: Istnieje możliwość oceny wyjścia ACK_REQ instrukcji RCVDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy zatwierdzenie jest wymagane.
10. Należy doprowadzić sygnał zatwierdzenia na wejście ACK_REI instrukcji RCVDP w celu przeprowadzenia reintegracji.
11. Opcjonalnie: Istnieje możliwość oceny wyjścia SUBS_ON instrukcji RCVDP lub SENDDP, by wykonać zapytanie, czy instrukcja RCVDP wyprowadza wartości fail-safe przypisane w wejściach SUBBO_xx i SUBI_xx.
12. Opcjonalnie: Istnieje możliwość oceny wyjścia ERROR instrukcji RCVDP lub SENDDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy wystąpił błąd komunikacji.
13. Opcjonalnie: Istnieje możliwość oceny wyjścia SENDMODE instrukcji RCVDP, by wykonać zapytanie, czy F-CPU z powiązaną instrukcją SENDDP znajduje się w wyłączonym trybie bezpieczeństwa (strona 360).

9.1.2.4 Komunikacja sterownik IO safety – sterownik IO – ograniczenia transferu danych

Uwaga

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć drugiego (lub trzeciego) wywołania SENDDP / RCVDP. Wymaga to skonfigurowania dodatkowego połączenia poprzez złącze PN/PN. To, czy jest to możliwe z pojedynczym złączem PN/PN, zależy od ograniczeń przepustowości tego złącza.

9.1.3 Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne

9.1.3.1 Konfiguracja komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne

Wstęp

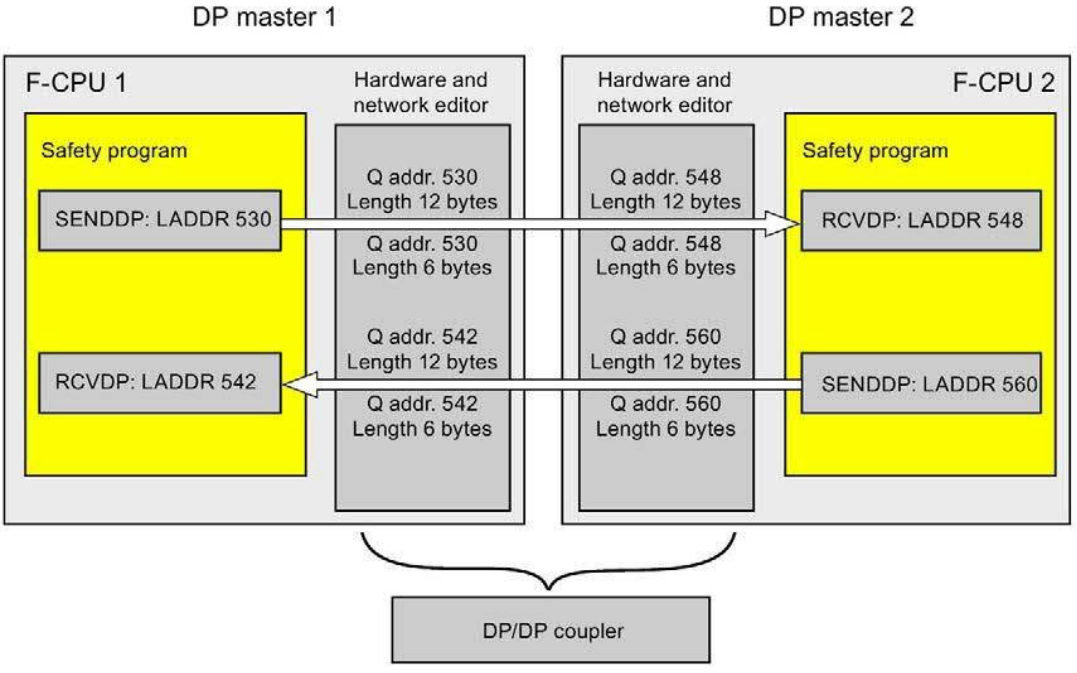
Komunikacja safety pomiędzy programami bezpieczeństwa F-CPU urządzeń nadrzędnych DP odbywa się poprzez złącze DP/DP.

Uwaga

Należy przełączyć wskaźnik ważności danych „DIA" na przełączniku DIP złącza DP/DP na „OFF" (wył). W przeciwnym razie komunikacja safety CPU – CPU nie jest możliwa.

Konfigurowanie obszarów transferu

Należy skonfigurować jeden obszar transferowy dla danych wyjściowych oraz jeden obszar dla danych wejściowych w *edytorze sprzętu i sieci* dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU w złączu DP/DP. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać oraz odbierać dane (komunikacja dwukierunkowa). Dla każdego z dwóch połączeń komunikacyjnych należy skonfigurować w złączu DP/DP jeden obszar transferowy dla danych wyjściowych oraz jeden dla danych wejściowych.



Zasady definiowania obszarów transferu

Obszar transferu dla danych wejściowych oraz obszar dla danych wyjściowych do **wysyłanych danych** muszą rozpoczynać się od tego samego adresu początkowego. Obszar transferu do danych wejściowych wymaga łącznie 6 bajtów (spójnych); obszar transferu danych wyjściowych wymaga 12 bajtów (spójnych).

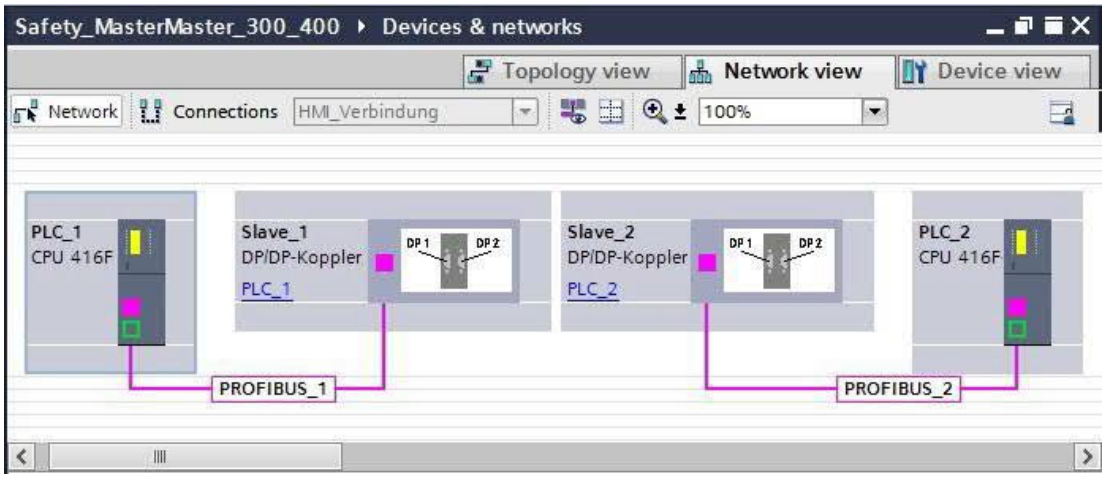
Obszar transferu dla danych wejściowych oraz obszar dla danych wyjściowych do **odbieranych danych** muszą rozpoczynać się od tego samego adresu początkowego. Obszar transferu do danych wejściowych wymaga łącznie 12 bajtów (spójnych); obszar transferu danych wyjściowych wymaga 6 bajtów (spójnych).

Procedura konfiguracji

Procedura konfiguracji komunikacji urządzenie nadrzędne safety
– urządzenie nadrzędne przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Przełączyć na widok sieci w *edytorze sprzętu i sieci*.
3. Wybrać złącze DP/DP z pozycji „Other field devices¥PROFIBUS DP¥Gateways¥Siemens AG¥DP/DP Coupler" w karcie zadań „Hardware catalog" (Katalog sprzętowy) i wstawić je do widoku sieci edytora sprzętu i sieci.
4. Wstawić drugie złącze DP/DP.
5. Podłączyć interfejs DP F-CPU 1 do interfejsu DP złącza DP/DP oraz interfejs DP F-CPU 2 do interfejsu DP drugiego złącza DP/DP.



6. Wolny adres PROFIBUS jest przypisywany automatycznie we właściwościach złącza DP/DP w widoku urządzenia. Należy ustawić ten adres na złączu DP/DP PLC 1, korzystając z przełącznika DIP na urządzeniu lub w konfiguracji złącza DP/DP (patrz podręcznik „Złącze DP/DP" (http://support.automation.siemens.com/WW/view/en/1179382)).
7. Przełączyć na widok urządzenia dla złącza DP/DP PLC1 do połączeń komunikacji dwukierunkowej, tj. gdy F-CPU jednocześnie wysyła i odbiera dane. Wybrać następujące moduły z zakładki zadań „Hardware catalog" (Katalog sprzętu) (z aktywnym filtrem), po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń):

   – Jeden moduł „6 bytes I/12 bytes Q consistent" oraz
   – Jeden moduł „12 bytes I/6 bytes Q consistent"

8. We właściwościach modułu należy przypisać adresy poza obrazem procesowym w następujący sposób:

   Przykładowo, dla modułu „6 bytes I/12 bytes Q consistent" do wysyłania danych:

   – Adresy wejściowe: Adres początkowy 530
   – Adresy wyjściowe: Adres początkowy 530

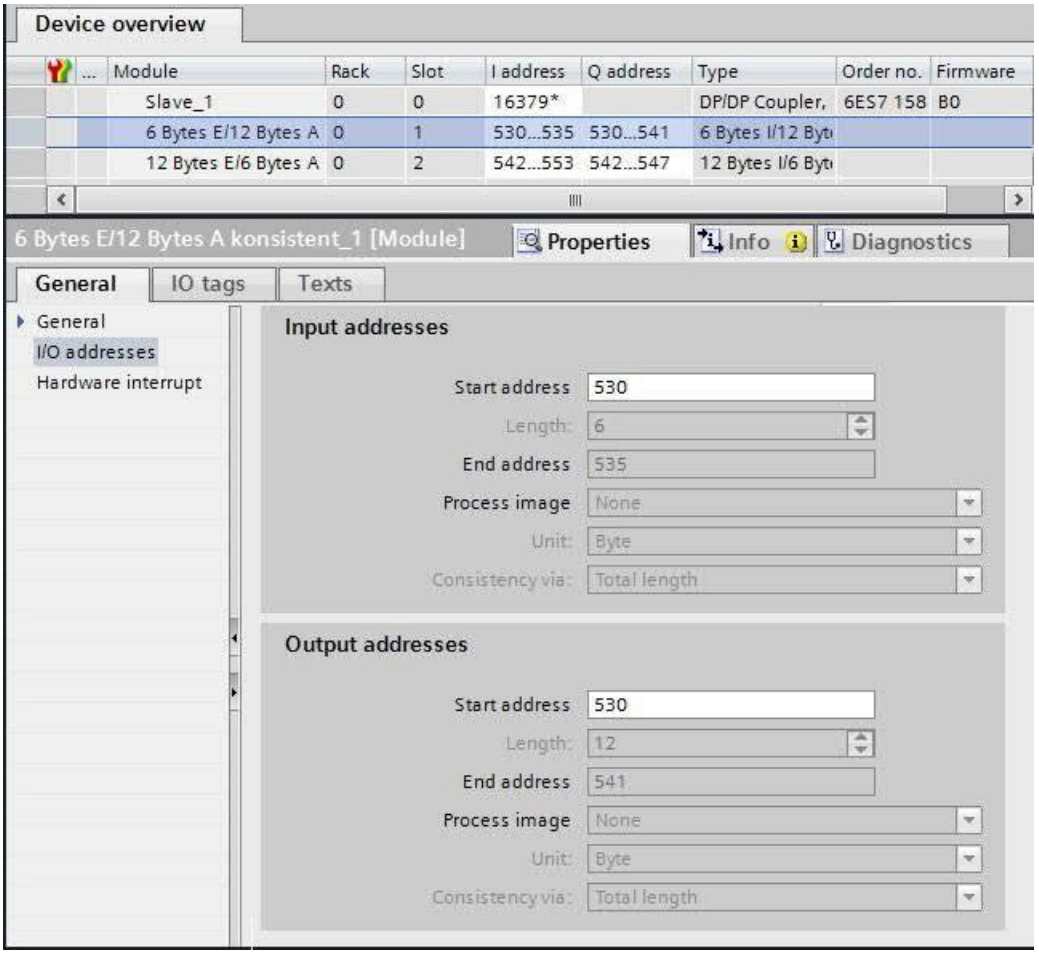
   Przykładowo, dla modułu „12 bytes I/6 bytes Q consistent" do odbierania danych:

   – Adresy wejściowe: Adres początkowy 542
   – Adresy wyjściowe: Adres początkowy 542

   Uwaga

   Należy upewnić się, że przypisano identyczne adresy początkowe dla obszarów adresowych danych wejściowych i wyjściowych.

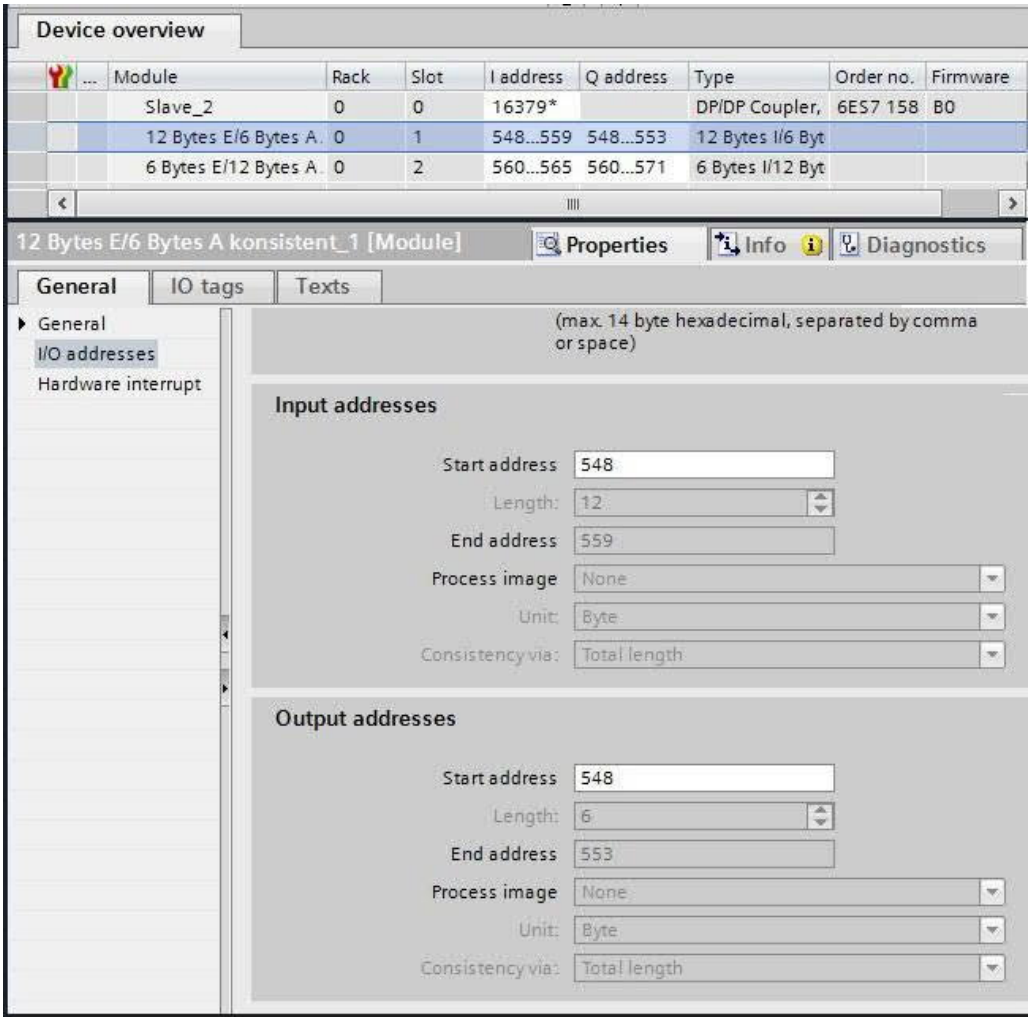
   Wskazówka: Należy zanotować adresy początkowe obszarów transferu. Są one potrzebne do zaprogramowania bloków SENDDP i RCVDP (wejście LADDR).



9. Wybrać następujące moduły z karty zadań „Hardware catalog (Katalog sprzętowy) (z aktywnym filtrem) w widoku urządzenia dla złącza DP/DP PLC2, po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń):
   - Jeden moduł „12 bytes I/6 bytes Q consistent" oraz
   - Jeden moduł „6 bytes I/12 bytes Q consistent"
10. We właściwościach modułu należy przypisać adresy poza obrazem procesowym w następujący sposób:

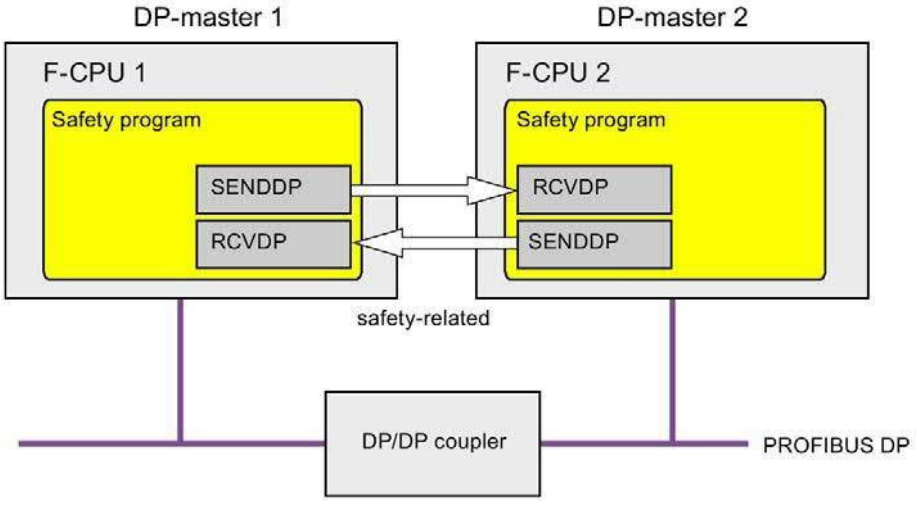
    Przykładowo, dla modułu „12 bytes I/6 bytes Q consistent" do odbierania danych:
   - Adresy wejściowe: Adres początkowy 548
   - Adresy wyjściowe: Adres początkowy 548

    Przykładowo, dla modułu „6 bytes I/12 bytes Q consistent" do wysyłania danych:
   - Adresy wejściowe: Adres początkowy 560
   - Adresy wyjściowe: Adres początkowy 560



9.1.3.2 Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU urządzenia nadrzędnego DP wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych. Można wykorzystać je do wykonywania przesyłu typu fail-safe *stałych* ilość danych typu fail-safe rodzaju INT lub BOOL.

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.1.3.3 Programowanie komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne

Wymogi do programowania

Należy skonfigurować obszary transferu do danych wejściowych i wyjściowych złącza DP/DP.

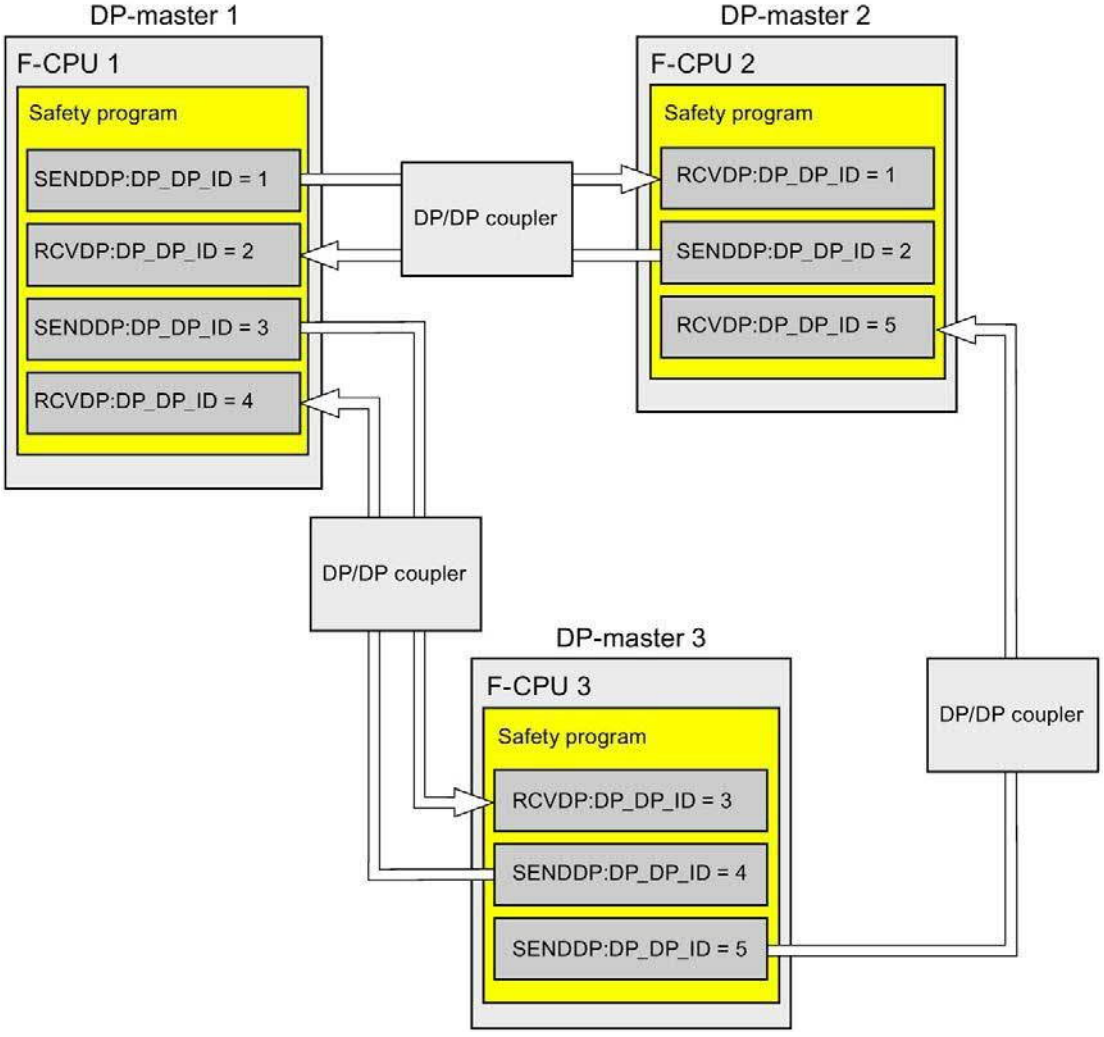
Procedura programowania

Komunikację urządzenie nadrzędne z bezpieczeństwem – urządzenie nadrzędne programuje się w następujący sposób:

1. W programie bezpieczeństwa, z którego dane będą wysyłane, należy wywołać instrukcję SENDDP (strona 631) w celu wysłania na końcu głównego bloku bezpieczeństwa.
2. W programie bezpieczeństwa, w którym dane będą odbierane, należy wywołać instrukcję RCVDP (strona 631) w celu odebrania na początku głównego bloku bezpieczeństwa.
3. Należy przypisać adresy początkowe obszarów transferu wyjść i wejść złącza DP/DP skonfigurowanego w *edytorze sprzętu i sieci* do odnośnych wejść LADDR.

   Należy wykonać to przypisanie dla każdego połączenia komunikacyjnego w każdym F-CPU.
4. Przypisać wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa do wejść DP_DP_ID. Pozwala to na ustalenie związku komunikacji pomiędzy instrukcją SENDDP w jednym F-CPU a instrukcją RCVDP w drugim F-CPU: Powiązane instrukcje otrzymują

Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla 5 powiązań komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

5. Doprowadzić na wejścia SD_BO_xx i SD_I_xx w SENDDP sygnały wysyłania. Aby ograniczyć sygnały pośrednie podczas przesyłania bloków transferowych, można zapisać wartość bezpośrednio do instancji DB w SENDDP, korzystając z w pełni kwalifikowanego dostępu (przykładowo, "Name SENDDP_1".SD_BO_02) przed wywołaniem SENDDP.
6. Należy doprowadzić na wyjścia RD_BO_xx i RD_I_xx w RCVDP sygnały, które mają dalej być przetwarzane przez inne sekcje programu lub użyć w pełni kwalifikowanego dostępu, by odczytać otrzymane sygnały bezpośrednio z powiązanych instancji DB w sekcjach programu, które będą przetwarzane dalej (np. "Name RCVDP_1".RD_BO_02).
7. Należy zasilić odnośne wejścia SUBBO_xx i SUBI_xx w RCVDP za pomocą wartości fail-safe wyprowadzanej przez RCVDP zamiast danych procesowych, aż zostanie ustanowiona komunikacja po raz pierwszy po uruchomieniu wysyłania i odbioru systemów bezpieczeństwa, lub w przypadku błędu komunikacji związanej z bezpieczeństwem.

   - Specyfikacja stałych wartości fail-safe:

     W przypadku danych rodzaju INT, można wprowadzić stałe wartości fail-safe bezpośrednio jako stałe w wejściu SUBI_xx (wartość początkowa = "0"). Aby określić stałą wartość fail-safe dla danych rodzaju BOOL, należy zapewnić tag "F_GLOBDB".VKE1 dla wejścia SUBBO_xx (wartość początkowa = „FAŁSZ").

   - Specyfikacja zmiennych wartości zastępczych:

     Aby określić zmienne wartości zastępcze, należy zdefiniować tag obliczany poprzez program bezpieczeństwa w F-DB, po czym określić go (w pełni kwalifikowany) w wejściu SUBI_xx lub SUBBO_xx.

⚠ OSTRZEŻENIE

Uwaga: Logika programu do obliczania zmiennych wartości zastępczych może być wstawiona jedynie za wywołaniami RCVDP, ponieważ obszar przed nimi musi być wolny od operacji logicznych. Dlatego też, w pierwszym cyklu po uruchomieniu systemu bezpieczeństwa, we wszystkich instrukcjach RCVDP aktywne są wartości początkowe wartości zastępczych. Należy zatem przypisać do tych znaczników odpowiednie wartości początkowe. *(S017)*

8. Skonfigurować wejścia TIMEOUT instrukcji RCVDP i SENDDP, wprowadzając wymagany czas monitorowania.

⚠ OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcze i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

9. Opcjonalnie: Istnieje możliwość oceny wyjścia ACK_REQ instrukcji RCVDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy zatwierdzenie jest wymagane.
10. Należy doprowadzić sygnał zatwierdzenia na wejście ACK_REI instrukcji RCVDP w celu przeprowadzenia reintegracji.
11. Opcjonalnie: Istnieje możliwość oceny wyjścia SUBS_ON instrukcji RCVDP lub SENDDP, by wykonać zapytanie, czy instrukcja RCVDP wyprowadza wartości fail-safe przypisane w wejściach SUBBO_xx i SUBI_xx.
12. Opcjonalnie: Istnieje możliwość oceny wyjścia ERROR instrukcji RCVDP lub SENDDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy wystąpił błąd komunikacji.
13. Opcjonalnie: Istnieje możliwość oceny wyjścia SENDMODE instrukcji RCVDP, by wykonać zapytanie, czy F-CPU z powiązaną instrukcją SENDDP znajduje się w wyłączonym trybie bezpieczeństwa (strona 360).

9.1.3.4 Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne: ograniczenia transferu danych

Uwaga

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć drugiego (lub trzeciego) wywołania SENDDP / RCVDP. Wymaga to skonfigurowania dodatkowego połączenia poprzez złącze DP/DP. To, czy jest to możliwe z pojedynczym złączem DP/DP, zależy od ograniczeń przepustowości tego złącza.

9.1.4 Komunikacja sterownika IO safety – I-device

9.1.4.1 Konfiguracja komunikacji związanej z bezpieczeństwem pomiędzy sterownikiem IO a I-device

Wstęp

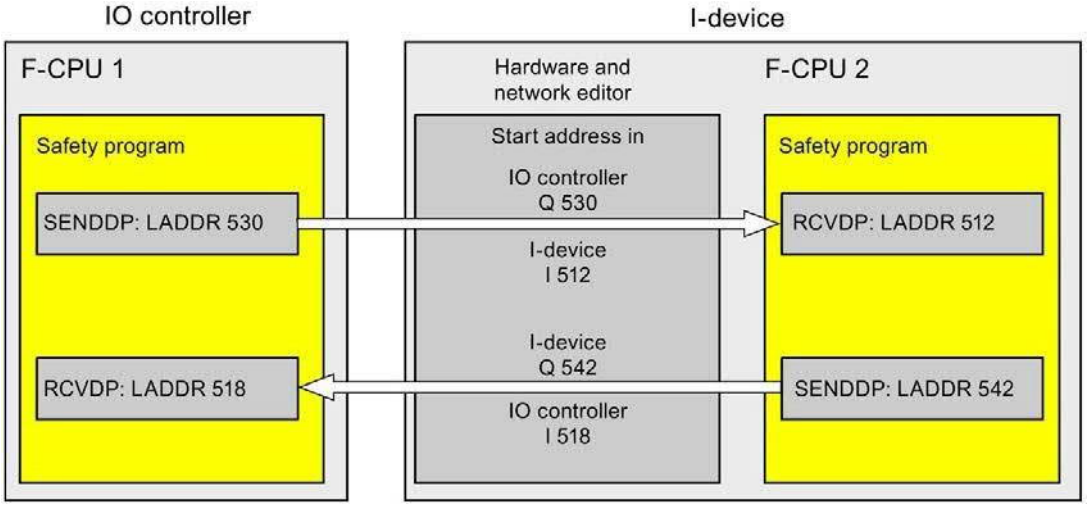
Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU sterownika IO a programem (programami) bezpieczeństwa F-CPU jednego lub kilku urządzeń I odbywa się poprzez połączenia sterownik IO – I-device (**F**-CD)
w PROFINET IO, tak jak w standardowych systemach.

Do komunikacji sterownik IO – I-device nie jest potrzebny dodatkowy sprzęt.

F-CPU wykorzystywany jako I-device musi obsługiwać tryb roboczy „urządzenie IO".

Konfigurowanie obszarów transferu

Dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU należy skonfigurować obszary transferu w *edytorze sprzętu i sieci*. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać oraz odbierać dane (komunikacja dwukierunkowa).



Podczas tworzenia obszaru transferu przypisywana jest do niego etykieta, pozwalająca na zidentyfikowanie go jako związku komunikacyjnego. Przykładowo, „F-CD_PLC_2 PLC_1_1" dla pierwszego połączenia F-CD pomiędzy F-CPU 1 sterownika IO a F-CPU 2 I-device.

Adresy początkowe obszarów transferu przypisuje się do wejścia LADDR instrukcji SENDDP i RCVDP w programach bezpieczeństwa.

Procedura konfiguracji

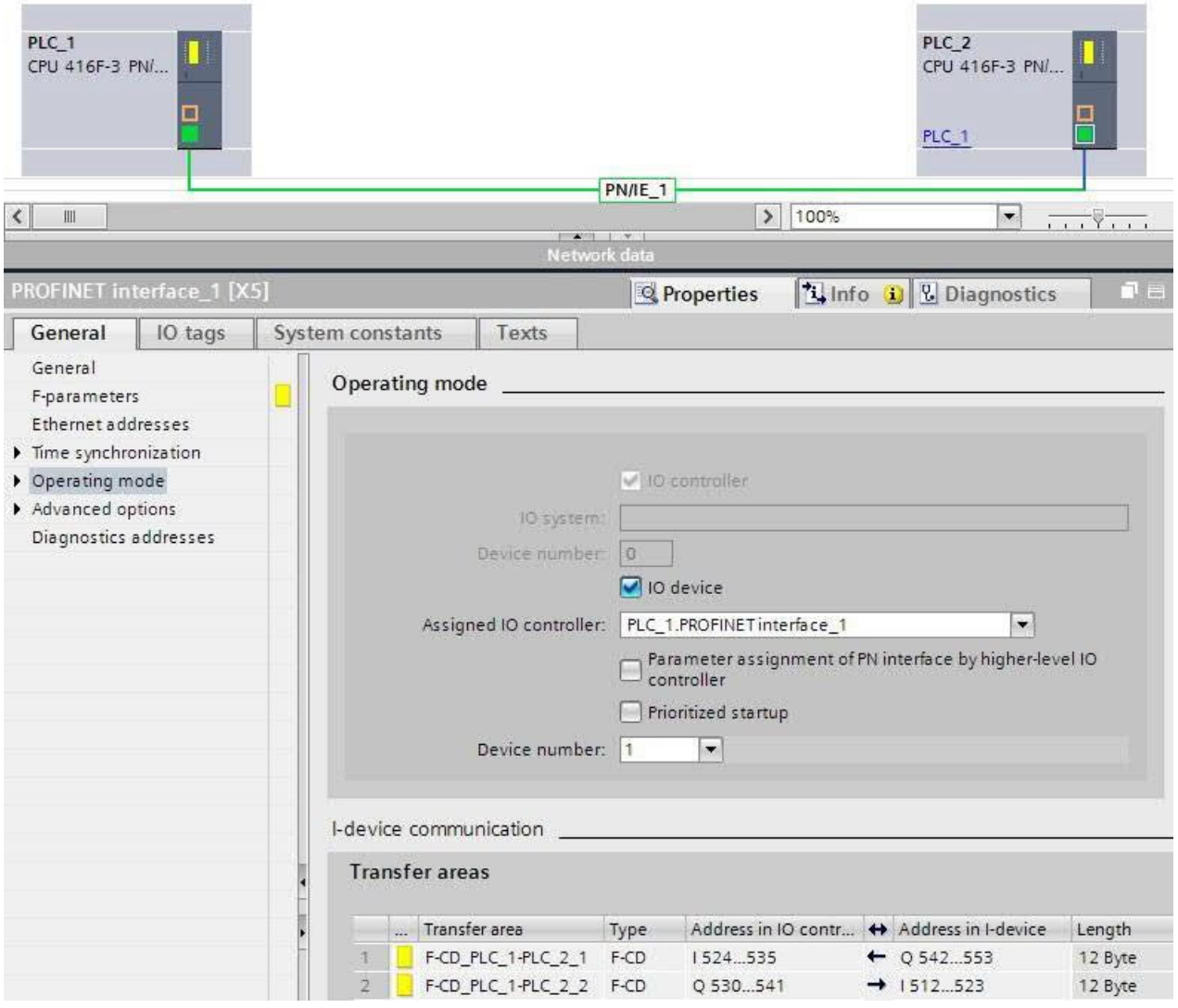
Procedura konfiguracji komunikacji sterownik IO safety – I-device przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Włączyć tryb „IO Device" dla F-CPU 2 we właściwościach jego interfejsu PN, po czym przypisać ten interfejs PN do interfejsu PN w F-CPU 1.
3. Wybrać interfejs PROFINET w F-CPU 2. Pod hasłem „Transfer areas" (Obszary transferu), tworzy się połączenie F-CD (typ „F-CD") do wysyłania do sterownika IO (←). Połączenie F-CD jest przedstawione na żółto w tabeli, ponadto wyświetlane są obszary adresowe w I-device oraz sterowniku IO przypisane na zewnątrz obrazu procesowego.

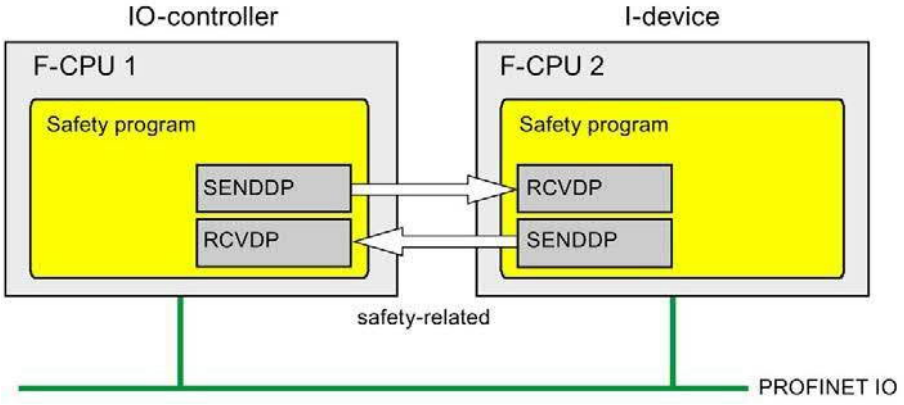
   Ponadto, dla każdego połączenia F-CD, automatycznie tworzone jest połączenie zatwierdzenia. (patrz „Szczegóły obszaru transferu").

4. Należy utworzyć dodatkowe połączenie F-CD do odbioru ze sterownika IO.
5. W nowo utworzonym obszarze transferu należy kliknąć na strzałkę, by zmienić kierunek przesyłu na odbiór ze sterownika IO (→).



9.1.4.2 Komunikacja sterownik IO safety – I-device poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU sterownika IO oraz I-device wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych.
Można wykorzystać je do wykonywania przesyłu typu fail-safe *stałych* ilość danych typu fail-safe rodzaju INT lub BOOL.

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.1.4.3 Programowanie komunikacji sterownik IO safety – I-device

Wymogi do programowania

Obszar transferu musi być skonfigurowany.

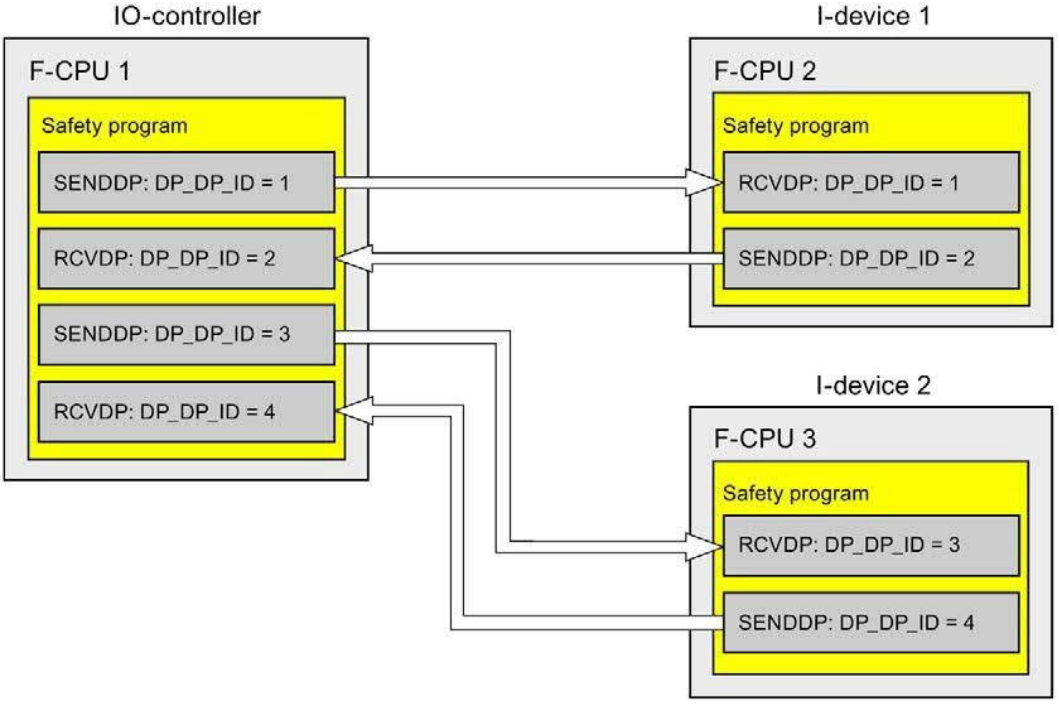
Procedura programowania

Procedura programowania komunikacji sterownik IO safety – I-device przebiega identycznie jak programowanie komunikacji sterownik IO safety – sterownik IO (patrz Komunikacja sterownik IO związany z bezpieczeństwem – sterownik IO (strona 217)).

Przypisanie adresów początkowych obszarów transferu do wejścia LADDR instrukcji SENDDP/RCVDP można pozyskać z następującej tabeli.

Instrukcja	Adres początkowy LADDR	
	Z wiersza	Z kolumny
SENDDP w sterowniku IO	→	Adres w sterowniku IO
RCVDP w sterowniku IO	←	Adres w sterowniku IO
SENDDP w I-device	←	Adres w urządzeniu IO
RCVDP w I-device	→	Adres w urządzeniu IO

Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla 4 powiązań komunikacji sterownik IO safety – I-device.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawce i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

9.1.4.4 Komunikacja sterownik IO safety – urządzenie IO – ograniczenia transferu danych

Ograniczenia transferu danych

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć dodatkowych instrukcji SENDDP/RCVDP. W tym celu należy skonfigurować dodatkowe obszary transferu. Należy pamiętać o maksymalnym limicie 1440 bajtów danych wejściowych lub 1440 bajtów danych wyjściowych dla transferu pomiędzy I-device a sterownikiem IO.

Poniższa tabela przedstawia ilości danych wyjściowych i wejściowych przypisanych w połączeniach komunikacji związanej z bezpieczeństwem:

Komunikacja safety	**Połączenie komunikacyjne**	**Przypisane dane wejściowe i wyjściowe**			
		W sterowniku IO		**W I-device**	
		Dane	**Dane**	**Dane**	**Dane**
Sterownik IO – I-device	**Wysyłanie:** I-device 1 do sterownika IO	6 bajtów	12 bajtów	12 bajtów	6 bajtów
	Odbiór: I-device 1 ze sterownika IO	12 bajtów	6 bajtów	6 bajtów	12 bajtów

Należy uwzględnić wszystkie dodatkowo skonfigurowane połączenia komunikacji standardowej oraz związanej z bezpieczeństwem (obszary transferu typu F-CD oraz CD) przy maksymalnym limicie 1440 bajtów danych wejściowych lub 1440 bajtów danych wyjściowych dla przesyłu pomiędzy I-device a sterownikiem IO. Ponadto, dane są przypisywane do celów wewnętrznych, wiec maksymalny limit może zostać osiągnięty wcześniej.

Po przekroczeniu limitu wyświetlany jest następujący komunikat o błędzie.

9.1.5 Komunikacja urządzenie nadrzędne safety – urządzenie I-slave

9.1.5.1 Konfiguracja komunikacji urządzenie nadrzędne safety – urządzenie I-slave

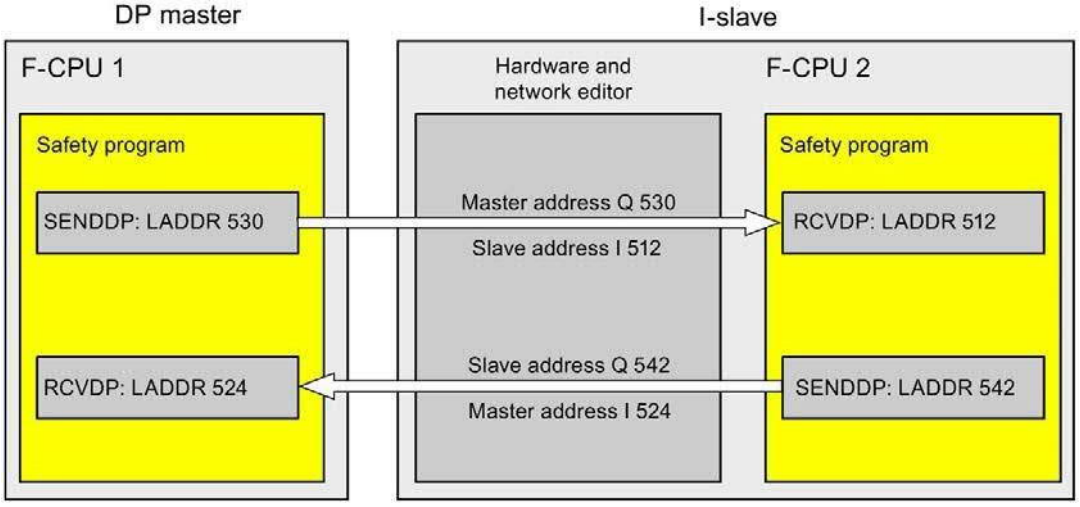
Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU urządzenia nadrzędnego DP a programem (programami) bezpieczeństwa F-CPU jednego lub kilku urządzeń I-slave odbywa się poprzez połączenia urządzenie nadrzędne – urządzenie I-slave (**F**-MS), tak jak w standardowych systemach.

Do takiej komunikacji nie jest potrzebne złącze DP/DP.

Konfigurowanie obszarów transferu

Dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU należy skonfigurować obszary transferu w *edytorze sprzętu i sieci*. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać oraz odbierać dane (komunikacja dwukierunkowa).



Podczas tworzenia obszaru transferu przypisywana jest do niego etykieta, pozwalająca na zidentyfikowanie go jako związku komunikacyjnego. Przykładowo, „F-MS_PLC_2 PLC_1_1" dla pierwszego połączenia F-MS pomiędzy F-CPU 1 urządzenia nadrzędnego DP a F-CPU 2 urządzenia I-slave.

Adresy początkowe obszarów transferu przypisuje się do wejścia LADDR instrukcji SENDDP i RCVDP w programach bezpieczeństwa.

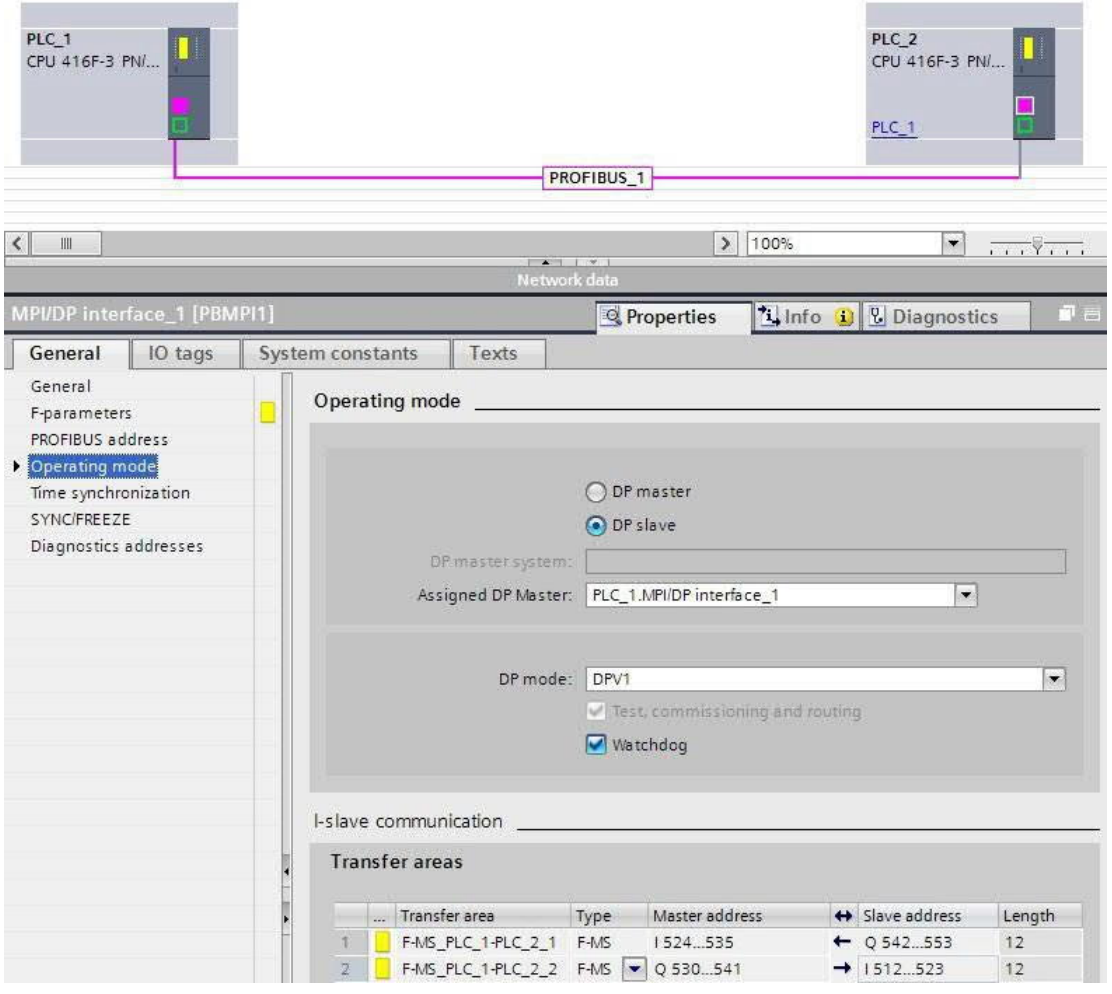
Procedura konfiguracji

Procedura konfiguracji komunikacji urządzenie nadrzędne safety – urządzenie I-slave przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

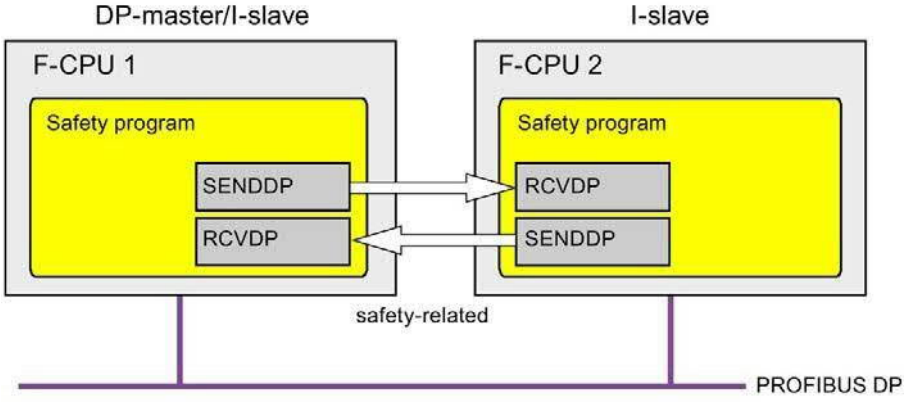
1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Włączyć tryb „DP slave" (urządzenie I-slave) dla F-CPU 2 we właściwościach jego interfejsu DP, po czym przypisać ten interfejs DP do interfejsu DP w F-CPU 1.
3. Wybrać interfejs PROFIBUS w F-CPU 2. Pod hasłem „Transfer areas" (Obszary transferu), tworzy się połączenie F-MS (typ „F-MS") do wysyłania do urządzenia nadrzędnego DP (←). Połączenie F-MS jest przedstawione na żółto w tabeli, ponadto wyświetlane są obszary adresowe w urządzeniu I-slave oraz urządzeniu nadrzędnym DP przypisane na zewnątrz obrazu procesowego.

   Ponadto, dla każdego połączenia F-MS, automatycznie tworzone jest połączenie zatwierdzenia. (patrz „Szczegóły obszaru transferu").
4. Należy utworzyć dodatkowe połączenie F-MS do odbioru z urządzenia nadrzędnego DP.
5. W nowo utworzonym obszarze transferu należy kliknąć na strzałkę, by zmienić kierunek przesyłu na odbiór z urządzenia nadrzędnego DP (→).



9.1.5.2 Komunikacja urządzenie nadrzędne safety – urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU urządzenia nadrzędnego DP oraz urządzenia I-slave lub F-COU wielu urządzeń I-slave wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych. Można wykorzystać je do wykonywania przesyłu typu fail-safe *stałych* ilość danych typu fail-safe rodzaju INT lub BOOL.

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.1.5.3 Programowanie komunikacji urządzenie nadrzędne safety – urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave

Wymogi

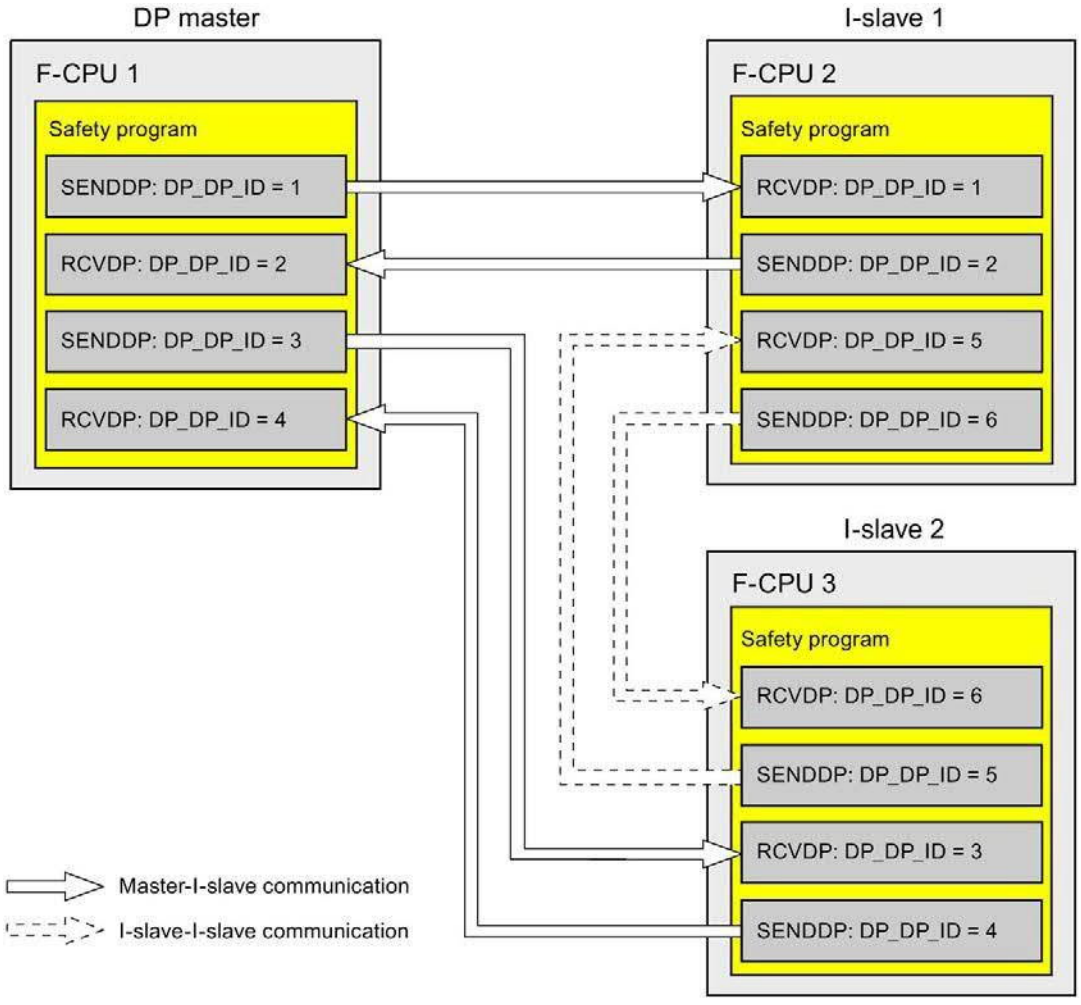
Obszar transferu musi być skonfigurowany.

Procedura programowania

Procedura programowania komunikacji urządzenie nadrzędne safety – urządzenie I-slave lub komunikacja urządzenie I-slave – I-slave przebiega identycznie jak programowanie komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne (patrz Programowanie komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne (strona 228)).

Instrukcja	**Adres początkowy LADDR**	
	Z wiersza	**Z kolumny**
SENDDP w urządzeniu nadrzędnym DP	→	Adres urządzenia
RCVDP w urządzeniu nadrzędnym DP	←	Adres urządzenia
SENDDP w urządzeniu I-slave	←	Adres urządzenia
RCVDP w urządzeniu I-slave	→	Adres urządzenia

Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla czterech powiązań komunikacji urządzenie nadrzędne safety – urządzenie I-slave oraz dwóch powiązań urządzenie I-slave – urządzenie I-slave.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcze i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

9.1.5.4 Ograniczenia transferu danych komunikacji urządzenie nadrzędne safety – urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave

Ograniczenia transferu danych

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć dodatkowych instrukcji SENDDP/RCVDP. W tym celu należy skonfigurować dodatkowe obszary transferu. Należy pamiętać o maksymalnym limicie 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych dla transferu pomiędzy urządzeniem I-slave a urządzeniem nadrzędnym DP.

Poniższa tabela przedstawia ilości danych wyjściowych i wejściowych przypisanych w połączeniach komunikacji związanej z bezpieczeństwem:

Komunikacja safety	**Połączenie komunikacyjne**	**Przypisane dane wejściowe i wyjściowe**					
		Urządzenie nadrzędne DP		**Urz. I-slave 1**		**Urz. I-slave 2**	
		Dane wyj.	**Dane wej.**	**Dane wyj.**	**Dane wej.**	**Dane wyj.**	**Dane wej.**
Urządzenie nadrzędne – urządzenie I-slave	**Wysyłanie:** Urz. podrz. I 1 do urz. podrz. DP	6 bajtów	12 bajtów	12 bajtów	6 bajtów	—	—
	Odbiór: Urz. podrz. I 1 z urz. nadrz. DP	12 bajtów	6 bajtów	6 bajtów	12 bajtów	—	—
Urządzenie I-slave – urządzenie I-slave	**Wysyłanie:** Urz. podrz. I 1 do urz. podrz. I 2	—	18 bajtów	12 bajtów	6 bajtów	6 bajtów	12 bajtów
	Odbiór: Urz. podrz. I 1 z urz. podrz. I 2	—	18 bajtów	6 bajtów	12 bajtów	12 bajtów	6 bajtów

Należy uwzględnić wszystkie dodatkowo skonfigurowane połączenia komunikacji standardowej oraz związanej z bezpieczeństwem (obszary transferu typu F-MS-, F-DX-, F-DX-Mod., MS-, DX- oraz DX-Mod) przy maksymalnym limicie 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych dla przesyłu pomiędzy I-device a urządzeniem nadrzędnym DP F-MS, F-DX, F-DX-Mod., MS, DX). Jeśli maksymalny limit 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych zostanie przekroczony, wyświetli się następujący komunikat o błędzie.

9.1.6 Komunikacja urządzenie I-slave safety – urządzenie I-slave

9.1.6.1 Konfiguracja komunikacji urządzenie I-slave safety – urządzenie I-slave

Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU urządzeń podrzędnych odbywa się przy użyciu bezpośredniej wymiany danych (**F**-DX) – identycznie jak w standardowych programach.

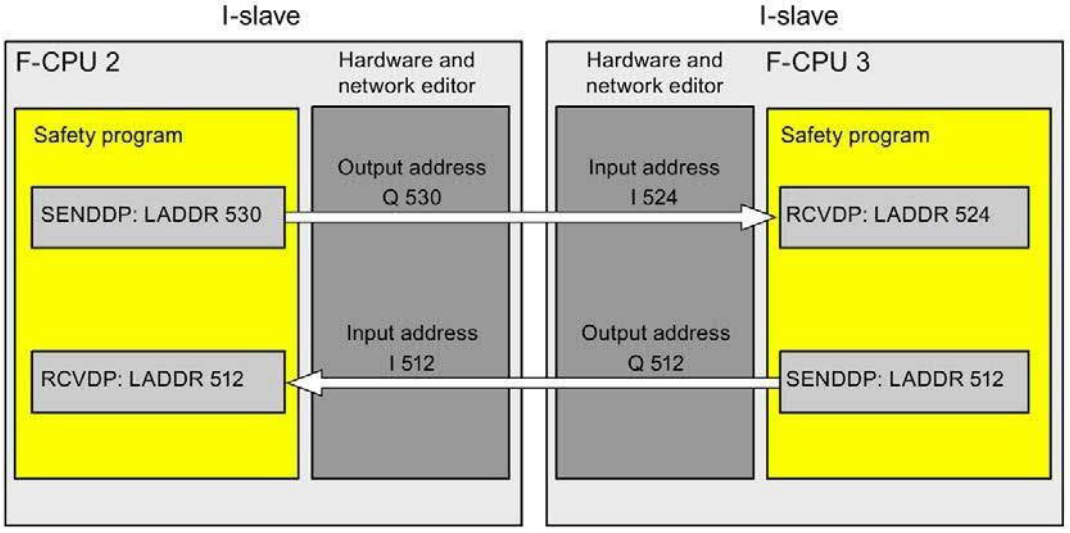
Do komunikacji urządzenie I-slave – urządzenie I-slave nie jest potrzebny dodatkowy sprzęt.

Możliwa jest również komunikacja urządzenie I-slave – urządzenie I-slave:

- Jeśli przypisane urządzenie nadrzędne DP jest standardowym CPU, który obsługuje bezpośrednią wymianę danych
- gdy zamiast urządzenia nadrzędnego DP, do sieci wstawiono sterownik IO współpracujący z urządzeniami podrzędnymi I poprzez połączenie IE/PB

Konfigurowanie obszarów transferu

Dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma urządzeniami podrzędnymi I należy skonfigurować obszary transferu w *edytorze sprzętu i sieci*. Na poniższej ilustracji oba urządzenia I-slave mogą wysyłać oraz odbierać dane (komunikacja dwukierunkowa).



Podczas tworzenia obszaru transferu przypisywana jest do niego etykieta, pozwalająca na zidentyfikowanie go jako związku komunikacyjnego. Przykładowo, „F-DX_PLC_2 PLC_1_1" dla pierwszego połączenia F-DX pomiędzy F-CPU 1 a F-CPU 2.

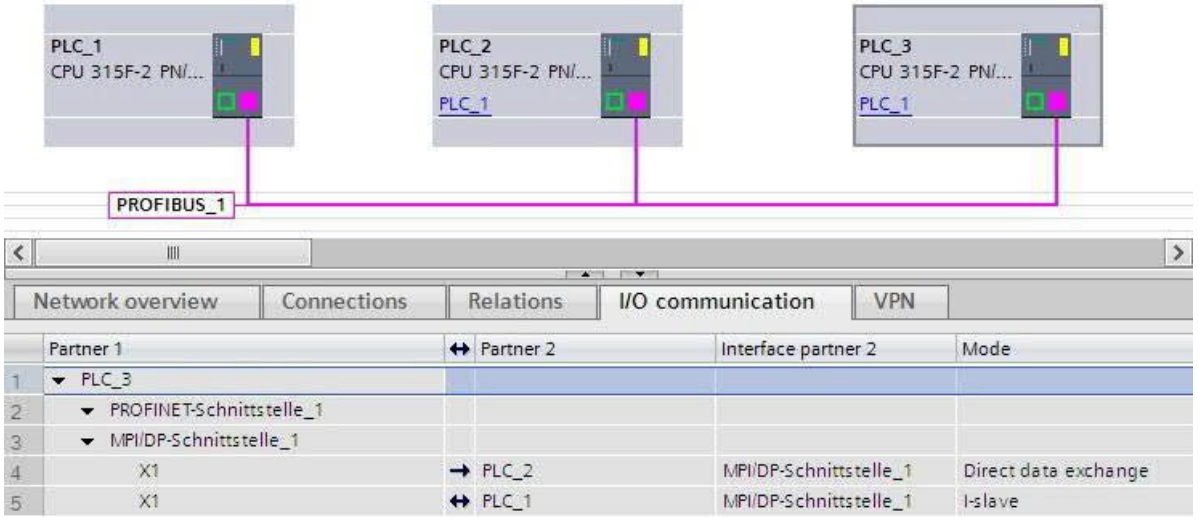
Adresy początkowe obszarów transferu przypisuje się do wejścia LADDR instrukcji SENDDP i RCVDP w programach bezpieczeństwa.

Procedura konfiguracji

Procedura konfiguracji komunikacji urządzenie I-slave – urządzenie I-slave przebiega identycznie jak w standardowym programie. Należy wykonać co następuje:

1. Wstawić trzy F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Włączyć tryb „DP slaves" (urządzenie I-slave) dla F-CPU 2 oraz F-CPU 3 we właściwościach ich interfejsu DP, po czym przypisać te interfejsy DP do interfejsu Dp w F-CPU 1.
3. Wybrać interfejs DP dla F-CPU 3 w widoku sieci.
4. Wybrać zakładkę „I/O communication" (Komunikacja I/O).
5. Korzystając z funkcjonalności przeciągnij-i-upuść w widoku sieci, przesunąć F-CPU 2 do kolumny „Partner 2" w zakładce „I/O-communication" (Komunikacja (I/O).

   Utworzy to linię z trybem „Direct data exchange" (Bezpośrednia wymiana danych) do wysyłania do urządzenia I-slave (F-CPU 2) (→).



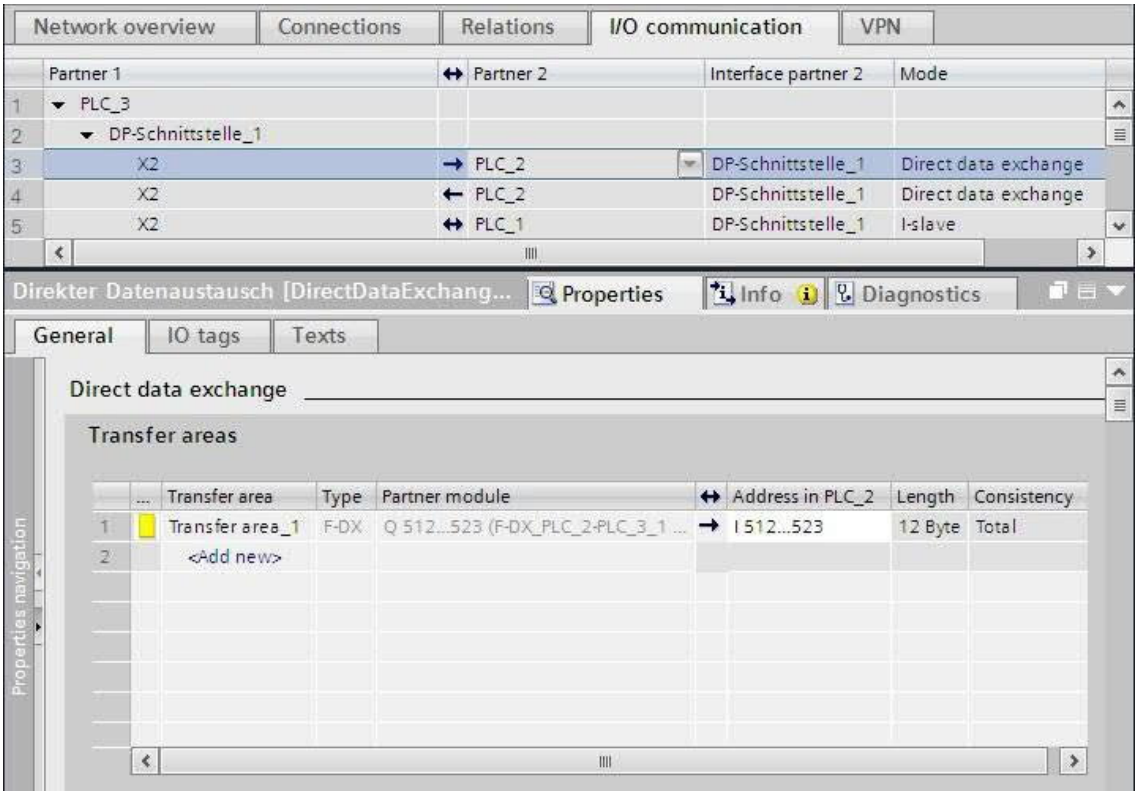
6. Kliknąć na nowo utworzoną linię (→).

7. W „Transfer areas" (Obszary transferu) (tabela „Direct data exchange" (Bezpośrednia wymiana danych)), należy utworzyć połączenie F-DX (rodzaj „F-DX") do wysyłania danych do urządzenia I-slave (F-CPU 2) (→). Połączenie F-DX jest przedstawione na żółto w tabeli, ponadto wyświetlane są obszary adresowe w urządzeniach I-slave przypisanych na zewnątrz obrazu procesu(PLC_2 i PLC_3).

   Ponadto, automatycznie zostanie utworzona linia z trybem „Direct data exchange" (Bezpośrednia wymiana danych) do odbioru z urządzenia I-slave (F-CPU 2) (→) w zakładce „I/O communication" (Komunikacja I/O), zaś połączenie zatwierdzenia (←, obszar transferu x_Ack) jest tworzony automatycznie w powiązanej tabeli „Direct data exchange" (Bezpośrednia wymiana danych).

   Jeden obszar transferu (rodzaj F-MS) dla CPU nadrzędnego (wyłączonego na wyświetlaczu) jest tworzony w „tabeli komunikacji urządzenia I-slave" dla każdego urządzenia I-slave.

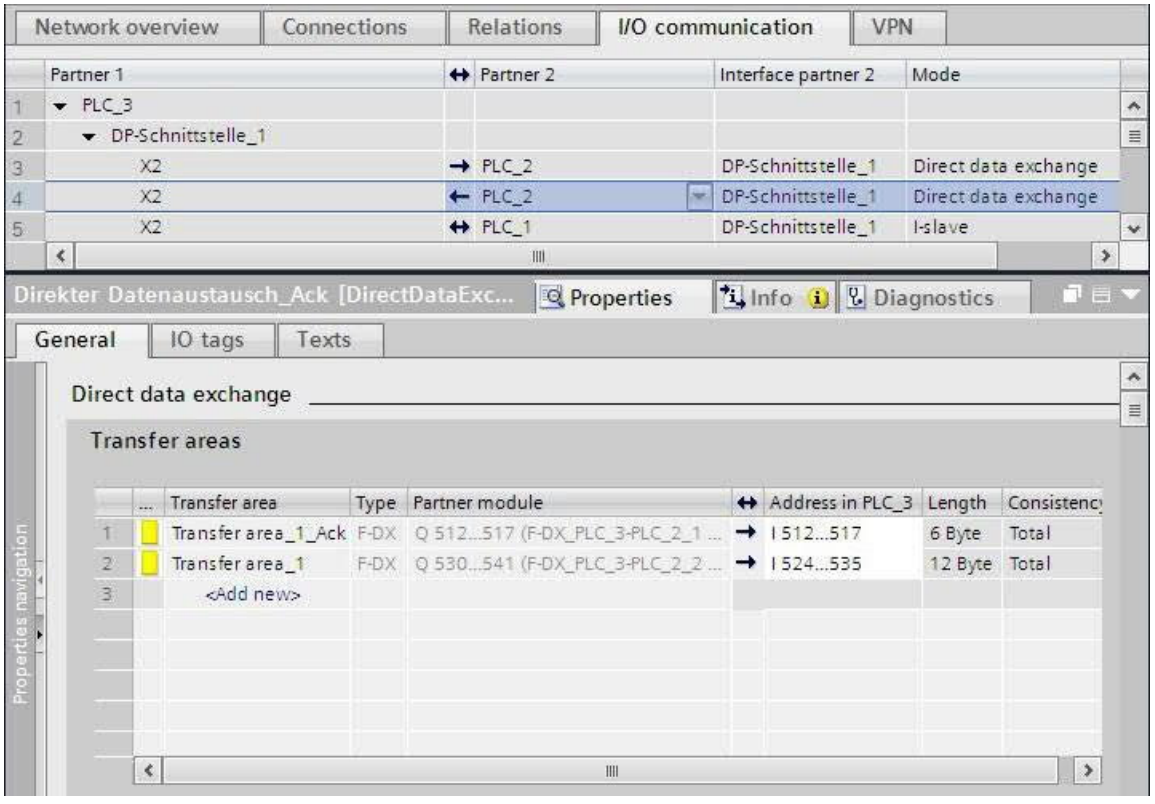
   Kończy to konfigurację wysyłania do F-CPU 2.



8. W zakładce „I/O communication" (Komunikacja I/O) należy wybrać automatycznie utworzoną linię z trybem „Direct data exchange" (Bezpośrednia wymiana danych) do odbioru z urządzenia I-slave (F-CPU 3) (←).
9. W „Obszarze transferu: (tabela „Direct data exchange" (Bezpośrednia wymiana danych)), należy utworzyć kolejne połączenie F-DX do odbioru z urządzenia I-slave (F-CPU 3).

   W takim przypadku również tworzone jest automatynicze połączenie zatwierdzenia (←, obszar transferu x_Ack) w „tabeli bezpośredniej wymiany danych", ponadto tworzone są dwa obszary transferu (rodzaj F-MS) dla CPU nadrzędnego (wyłączonego na wyświetlaczu) w tabeli „komunikacja urządzenia I-slave" dla obu urządzeń I-slave.

   Kończy to konfigurację odbioru z F-CPU 2.



Zmiana wyłączonych obszarów adresu lokalnego obszarów transferu

Aby zmienić wyłączony obszar adresu lokalnego dla „obszaru transferu x", należy zmienić obszar adresowy odnośnego połączenia zatwierdzenia „Transfer area x_Ack".

1. W „I/O communication" (Komunikacja I/O), należy wybrać linię ze strzałką skierowaną w tym samym kierunku co strzałka „Transfer area x" (Obszar transferu x) w tabeli „Direct data exchange" (Bezpośrednia wymiana danych).
2. Następnie należy wybrać linię z „Transfer area x_Ack" w tabeli „Direct data exchange" (Bezpośrednia wymiana danych).
3. Zmiana obszaru adresowania odbywa się w tym miejscu.

9.1.6.2 Komunikacja urządzenie I-slave safety – I-device poprzez SENDDP i RCVDP

Odniesienia

Opis komunikacji poprzez SENDDP i RCVDP dla komunikacji urządzenie I-slave safety – urządzenie I-slave można znaleźć w SENDDP i RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.1.6.3 Programowanie komunikacji urządzenie I-slave safety – urządzenie I-slave

Odniesienia

Opis programowania komunikacji urządzenie I-slave safety – urządzenie I-slave można znaleźć w Programowanie komunikacji urządzenie nadrzędne safety – urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave (strona 242).

Przypisanie adresów początkowych obszarów transferu do wejścia LADDR instrukcji SENDDP/RCVDP można pozyskać z następującej tabeli.

Instrukcja	Adres początkowy LADDR	
	Z wiersza	Z kolumny
SENDDP w 1. urządzeniu I-slave	→	Adres w <1. urządzeniu podrzędnym I> (w przykładzie kolumna „Address in PLC_2" (Adres w PLC_2))
RCVDP w 1. urządzeniu I-slave	←	Adres w <1. urządzeniu I-slave> (w przykładzie kolumna „Address in PLC_2" (Adres w PLC_2))
SENDDP w 2. urządzeniu I-slave	←	Adres w <2. urządzeniu I-slave> (w przykładzie kolumna „Address in PLC_3" (Adres w PLC_3))
RCVDP w 2. urządzeniu I-slave	→	Adres w <2. urządzeniu I-slave> (w przykładzie kolumna „Address in PLC_3" (Adres w PLC_3))

9.1.6.4 Ograniczenia transferu danych komunikacji urządzenie I-slave safety – urządzenie I-slave

Ograniczenia transferu danych

Opis programowania ograniczeń transferu danych komunikacji urządzenie I-slave safety – urządzenie I-slave można znaleźć w Ograniczenia transferu danych komunikacji urządzenie nadrzędne safety – urządzenie I-slave lub urządzenie I-slave – urządzenie I-slave (strona 245).

9.1.7 Komunikacja urządzenie I-slave safety – urządzenie podrzędne

9.1.7.1 Konfiguracja komunikacji urządzenie I-slave safety – urządzenie I-slave

Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU urządzenia I-slave a F-I/O urządzenia podrzędnego DP odbywa się przy użyciu bezpośredniej wymiany danych (**F**-DX-Mod), tak jak w standardowym programie.

Do komunikacji urządzenie I-slave – urządzenie podrzędne nie jest

potrzebny dodatkowy sprzęt. Możliwa jest również komunikacja

urządzenie I-slave – urządzenie podrzędne:

- gdy przypisane urządzenie nadrzędne DP jest standardowym CPU, który obsługuje bezpośrednią wymianę danych
- gdy zamiast urządzenia nadrzędnego DP, do sieci wstawiono sterownik IO współpracujący z urządzeniami podrzędnymi I poprzez połączenie IE/PB

DB F-I/O jest generowany automatycznie dla każdego F-I/O podczas jego konfiguracji w *edytorze sprzętu i sieci*; jest to wymagane dla dostępu F-I/O poprzez komunikację urządzenie I-slave safety – urządzenie podrzędne. DB F-I/O jest początkowo tworzony w programie bezpieczeństwa urządzenia nadrzędnego DP, o ile jest to F-CPU z aktywacją bezpieczeństwa. Jedynie po ustawieniu połączenia F-DX-Mod tworzony jest DB F-I/O w programie bezpieczeństwa urządzenia I-slave oraz usuwany w programie bezpieczeństwa urządzenia nadrzędnego DP.

Do uzyskania dostępu do kanałów F-I/O w programie bezpieczeństwa F-CPU urządzenia I-slave wykorzystywane jest wejście obrazu procesowy (patrz opis w Komunikacja urządzenie I-slave safety – urządzenie podrzędne – Dostęp F-I/O (strona 256)).

Ograniczenia

Uwaga

Komunikacja urządzenie I-slave safety – urządzenie podrzędne z F-I/O jest możliwa w urządzeniu podrzędnym DP, które obsługuje komunikację urządzenie I-slave safety – urządzenie podrzędne, na przykład
z wszystkimi modułami bezpieczeństwa ET 200SP z IM 155-6 DP HF, wersja oprogramowania > V3.1, z wszystkimi modułami bezpieczeństwa ET 200SP z IM 151-1 HF, z wszystkimi modułami sygnałowymi S7-300 typu fail-safe z IM 153-2, od numeru zamówieniowego 6ES7153-2BA01-0XB0, wersja oprogramowania > V4.0.0.

Uwaga

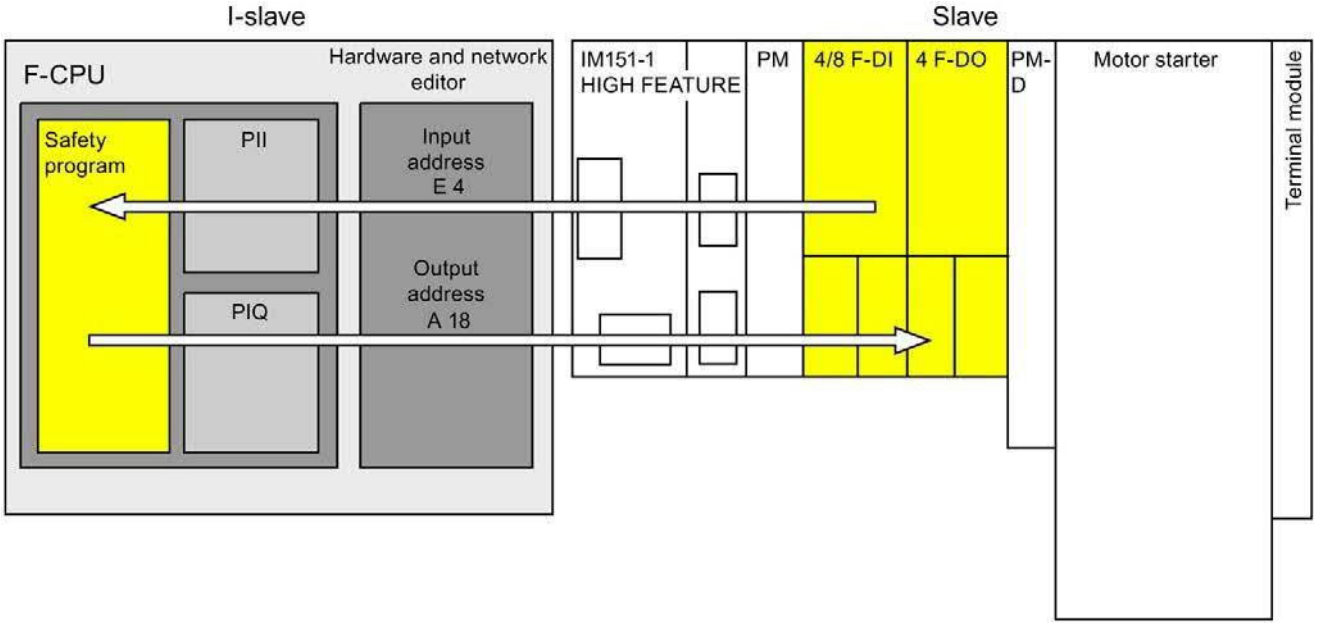
Przy komunikacji urządzenie I-slave safety – urządzenie podrzędne należy upewnić się, że CPU urządzenia nadrzędnego DP zostało zasilone przed F-CPU urządzenia I-slave.

W przeciwnym razie, zależnie od czasu monitorowania bezpieczeństwa określonego dla F-I/O, system bezpieczeństwa może wykryć błąd w komunikacji związanej z bezpieczeństwem (błąd komunikacji) pomiędzy F-CPU a F-I/O przypisanym do urządzenia I-slave. Oznacza to, że F-I/O nie są automatycznie reintegrowane po uruchomieniu systemu bezpieczeństwa. Zamiast tego są reintegrowane po zatwierdzeniu użytkownika przy pomocy zbocza dodatniego w tagu ACK_REI w DB I/O (zobacz również „Po błędach komunikacji" (strona 188) oraz „Po uruchomieniu systemu bezpieczeństwa" (strona 186)).

Konfigurowanie obszarów transferu

Dla każdej komunikacji związanej z bezpieczeństwem pomiędzy urządzeniem I-slave a urządzeniem podrzędnym należy skonfigurować obszary transferu w *edytorze sprzętu i sieci*.

Podczas tworzenia obszaru transferu przypisywana jest do niego etykieta, pozwalająca na zidentyfikowanie go jako związku komunikacyjnego. Przykładowo, „F-DX-Mod_PLC_2 PLC_1_1" dla pierwszego połączenia F-DX-Mod pomiędzy F-CPU 1 a F-CPU 2.

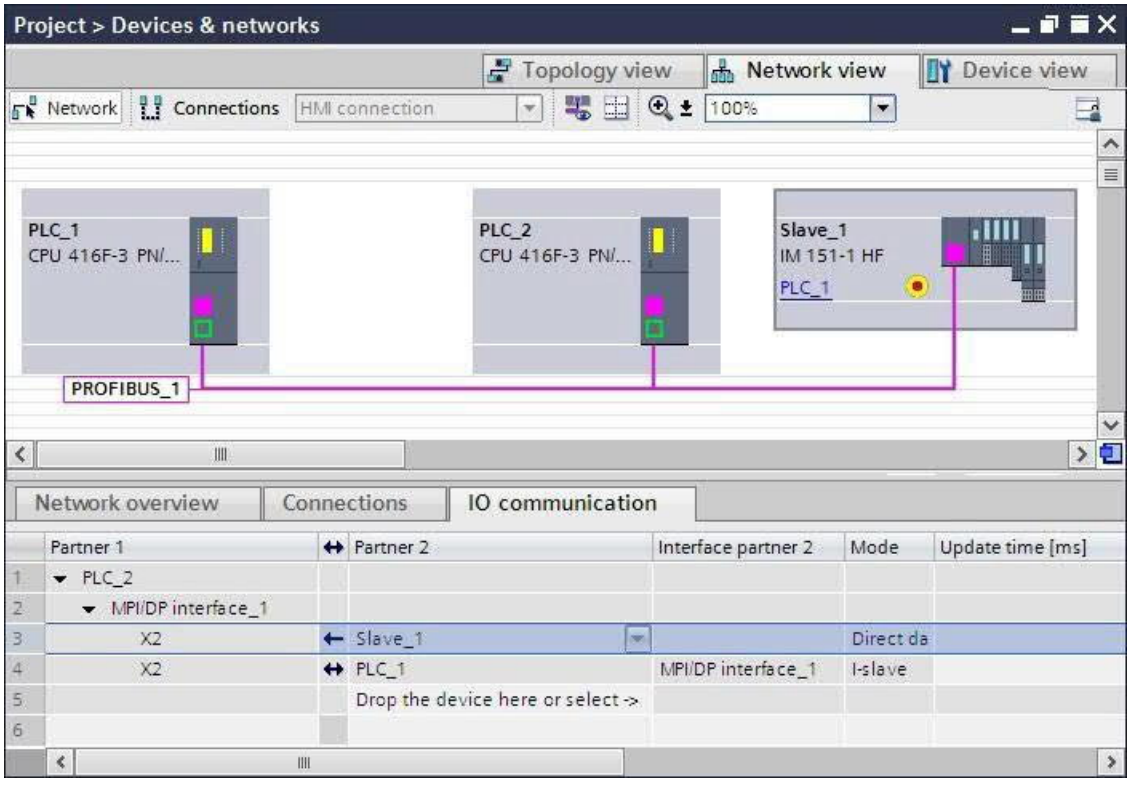


Procedura konfiguracji przy użyciu przykładu ET 200S. z modułami bezpieczeństwa w urządzeniu podrzędnym

Procedura konfiguracji komunikacji urządzenie podrzędne safety – urządzenie I-slave przebiega identycznie jak w standardowym programie.

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Należy wstawić odpowiednie urządzenie podrzędne DP, np. IM 151-1 HF, nr zamówieniowy 6ES7151-1BA0... z karty zadań „Hardware catalog" (Katalog sprzętowy) do widoku sieci w *edytorze sprzętu i sieci*.
3. Wstawić moduł zasilający, moduł 4/8 F-DI oraz moduł 4 F-DQ w widoku urządzenia ET 200S.
4. Włączyć tryb „DP slave" (urządzenie I-slave) dla F-CPU 2 we właściwościach jego interfejsu DP, po czym przypisać ten interfejs do F-CPU 1.
5. Przypisać interfejs DP IM 151-1 HF do urządzenia nadrzędnego DP (F-CPU 1).
6. Wybrać interfejs DP dla F-CPU 2 (urządzenie I-slave) w widoku sieci.
7. Wybrać zakładkę „I/O communication" (Komunikacja I/O).

8. Korzystając z funkcjonalności przeciągnij-i-upuść w widoku sieci, przesunąć ET 200S do kolumny „Partner 2" w zakładce „I/O-communication" (Komunikacja (I/O).

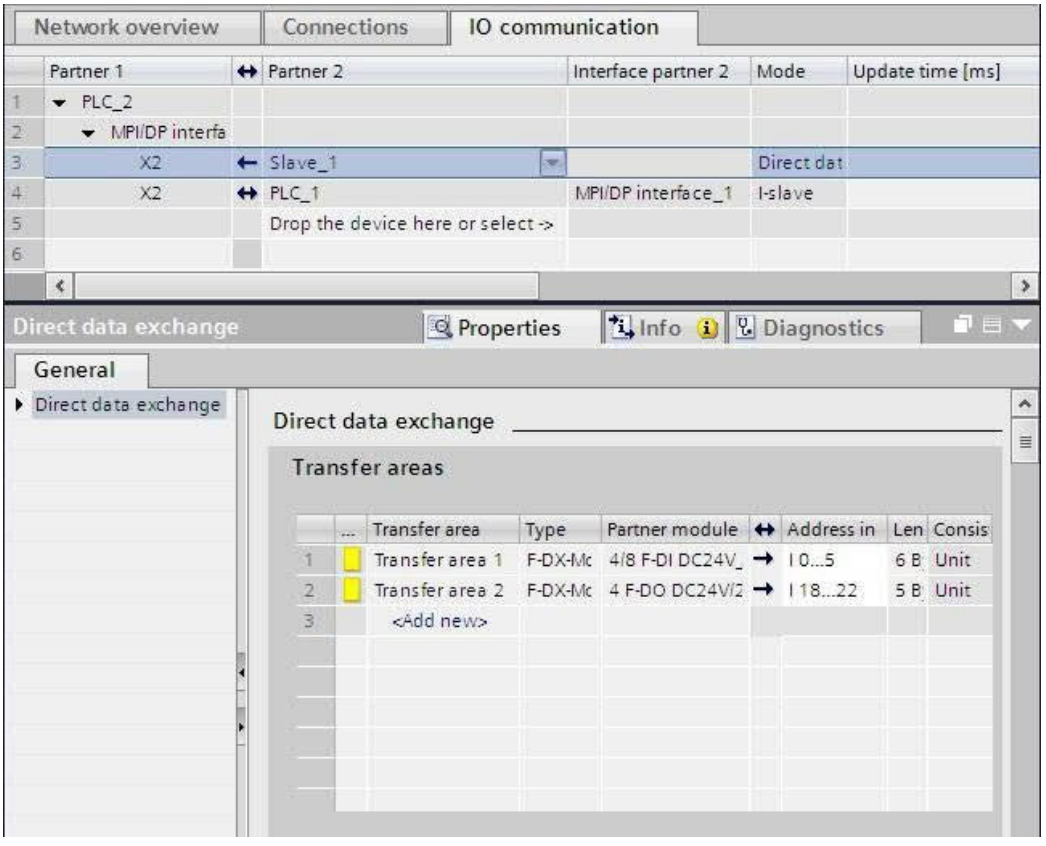


9. Kliknąć na nowo utworzoną linię
10. W „obszarach transferu" należy utworzyć połączenie F-DX-Mod (rodzaj „F-DX-Mod"). Połączenie F-DX-Mod jest oznaczone w tabeli żółtą linią. Wyświetlane są adresy dla „modułu partnerskiego" 4/8 F-DI w urządzeniu I-slave (PLC_2). Adresy można zmienić bezpośrednio w tabeli.

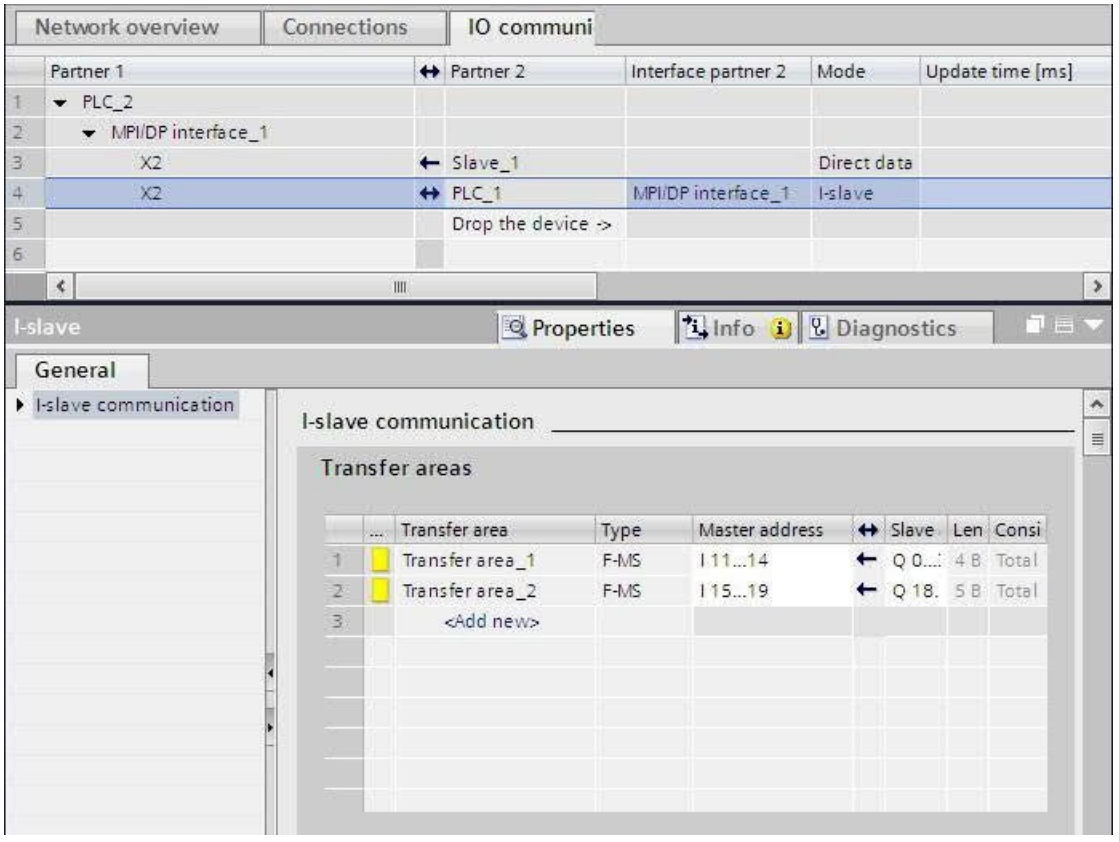
    Kończy to konfigurację dla modułu 4/8 F-DI.

11. W „obszarach transferu" należy utworzyć kolejne połączenie F-DX-Mod.
12. Należy zmienić moduł partnerski na moduł 4 F-DO, bezpośrednio w tabeli „obszary transferu" lub w szczegółach obszaru transferu 2, jeśli moduł 4 F-DO nie został jeszcze wybrany.

    Kończy to konfigurację dla modułu 4 F-DO.



W „tabeli komunikacji urządzenia I-slave" urządzenia I-slave tworzony jest obszar transferu (rodzaj F-MS) dla CPU nadrzędnego (wyłączonego na wyświetlaczu) dla każdego połączenia F-DX-Mod:



Zmiana w konfiguracji komunikacji urządzenie I-slave – urządzenie podrzędne

OSTRZEŻENIE

W przypadku dodania lub usunięcia komunikacji urządzenie I-slave – urządzenie podrzędne dla F-I/O, należy skompilować i pobrać konfigurację sprzętową urządzenia nadrzędnego DP, a także konfigurację sprzętową urządzenia I-slave.

Zbiorczy podpis bezpieczeństwa w F-CPU urządzenia I-slave oraz zbiorczy podpis bezpieczeństwa w F-CPU urządzenia nadrzędnego DP (jeśli tam też obecny jest program bezpieczeństwa) są ustawiane na „0”. Należy ponownie skompilować program(y) bezpieczeństwa. *(S019)*

9.1.7.2 Komunikacja urządzenie I-slave safety – urządzenie podrzędne – dostęp F-I/O

Dostęp poprzez obraz procesu

W komunikacji urządzenie I-slave safety – urządzenie podrzędne, obraz procesu (PII lub PIQ) pozwala na dostęp do F-I/O w programie bezpieczeństwa F-CPU urządzenia I-slave. Przebiega to identycznie jak dostęp F- I/O do F-I/O bezpośrednio przypisanego do urządzenia I-slave lub urządzenia nadrzędnego DP. W urządzeniu I-slave dostęp do F-I/O uzyskuje się za pomocą adresów przypisanych do połączenia F-DX-Mod w „obszarach transferu" (tabela „Direct data exchange" (Bezpośrednia wymiana danych)).

W tym przypadku należy zignorować wyświetlony obszar argumentów. Dostęp do F-I/O z wejściami jest możliwy, korzystając z PII oraz F-I/O z wyjściami, korzystając PIQ.

Informacje dotyczące dostępu I/O można znaleźć w dziale „Dostęp F-I/O" (strona 166).

9.1.7.3 Ograniczenia transferu danych komunikacji urządzenie I-slave safety – urządzenie I-slave

Ograniczenia transferu danych

Należy pamiętać o maksymalnym limicie 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych dla transferu pomiędzy urządzeniem I-slave a urządzeniem nadrzędnym DP.

Przykład wielkości danych wyjściowych i wejściowych, przypisanych do komunikacji związanej z bezpieczeństwem, przedstawiony jest w poniższej tabeli dla ET 200S 4/8 F-DI oraz ET 200S 4 F-DO:

Komunikacja safety	**Połączenie komunikacyjne**	**Przypisane dane wejściowe i wyjściowe***	
		Pomiędzy urządzeniem I-slave	
		Dane wyjściowe w urz. I-slave	**Dane wejściowe w urz. I-slave**
urządzenie I-slave – urządzenie podrzędne	Komunikacja urz I-slave – urz. podrzędne z 4/8 F-DI	4 bajtów	6 bajtów
	Komunikacja urz. I-slave – urz. podrzędne z 4 F-DO	5 bajtów	5 bajtów

* Przykład dla 4/8 F-DI oraz 4 F-DO w ET 200S

Należy uwzględnić wszystkie dodatkowo skonfigurowane połączenia komunikacji standardowej (połączenia F-MS, F-DX, F-DX-Mod., MS oraz DX) przy maksymalnym limicie 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych dla przesyłu pomiędzy urządzeniem I-slave a urządzeniem nadrzędnym DP. Jeśli maksymalny limit 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych zostanie przekroczony, wyświetli się następujący komunikat o błędzie.

9.1.8 Komunikacja sterownik IO safety – urządzenie I-slave

Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU sterownika IO a programem (programami) bezpieczeństwa F-CPU jednego lub kilku urządzeń I-slave odbywa się poprzez połączenia urządzenie kontroler – urządzenie I-slave (**F-**MS), tak jak w standardowych systemach.

Połączenie

W przypadku komunikacji sterownik IO safety – urządzenie I-slave, połączenie IE/PB jest niezbędne. Oba F-CPU są podłączone do połączenia IE/PB za pomocą interfejsu PROFIBUS DP lub PROFINET.

Uwaga

W przypadku korzystania z połączenia IE/PB, należy uwzględnić to podczas konfigurowania czasów monitorowania i odpowiedzi bezpieczeństwa oraz podczas obliczania maksymalnego czasu odpowiedzi systemu bezpieczeństwa (zobacz również „Czasy monitorowania i odpowiedzi" (strona 649)).

Należy pamiętać, że arkusz kalkulacyjny do obliczania czasów odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100) dla F-CPU S7-300/400 nie obsługuje wszystkich możliwych konfiguracji.

Odniesienia

Informacje dotyczące komunikacji urządzenie nadrzędne safety – urządzenie I-slave zamieszczone w dziale Komunikacja urządzenie nadrzędne – urządzenie I-slave (strona 239) również mają zastosowanie.

9.1.9 Komunikacja safety poprzez połączenia S7

9.1.9.1 Konfiguracja komunikacji związanej z bezpieczeństwem poprzez połączenia S7

Wstęp

Komunikacja safety pomiędzy programami bezpieczeństwa F- CPU poprzez połączenia S7 odbywa się za pomocą ustalonych połączeń S7 utworzonych w widoku sieci *edytora sprzętu i sieci* – identycznie jak w standardowych programach.

Ograniczenia

Uwaga

W SIMATIC Safety, połączenia S7 są ogólnie dozwolone jedynie poprzez przemysłowy

Ethernet.

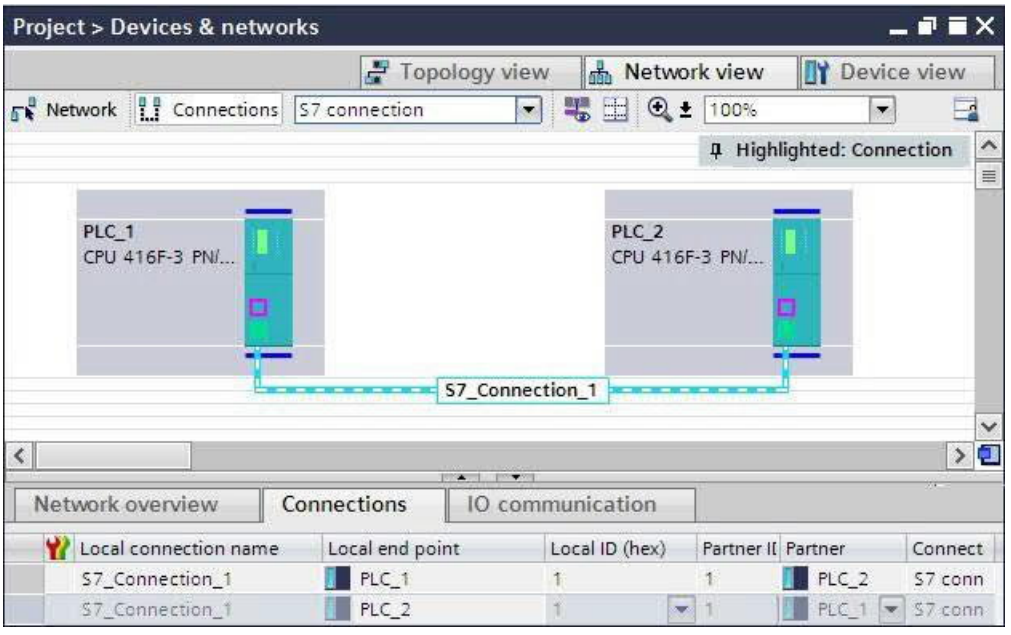
Komunikacja safety poprzez połączenia S7 jest możliwa z oraz do następujących F-CPU:

- F-CPU S7-300 poprzez zintegrowany interfejs PROFINET
- F-CPU S7-400 poprzez zintegrowany interfejs PROFINET lub CP 443-1 bądź CP 443-1 Advanced-IT

Tworzenie połączeń S7

Dla każdego połączenia pomiędzy dwoma F-CPU należy utworzyć połączenie S7 w widoku sieci *edytora sprzętu i sieci*.

Do każdego połączenia końcowego automatycznie przypisywany jest identyfikator lokalny oraz partnera, z perspektywy punktu końcowego (F-CPU). W razie potrzeby można zmienić oba identyfikatory w zakładce „Connections" (Połączenia). Lokalny identyfikatora przypisuje się do wejścia „ID" instrukcji SENDS7 i RCVS7 w programach bezpieczeństwa.

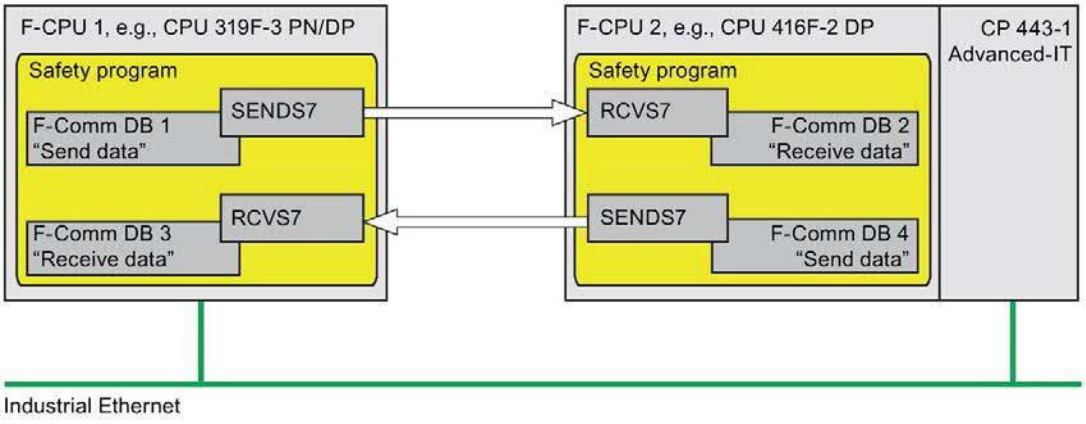


Procedura konfigurowania połączeń S7

Połączenia S7 do komunikacji związanej z bezpieczeństwem CPU – CPU konfiguruje się identycznie jak w przypadku *STEP 7 Professional* (patrz *pomoc do STEP 7 Professional* „Połączenia S7").

9.1.9.2 Komunikacja poprzez SENDS7, RCVS7, oraz DB komunikacji bezpieczeństwa

Komunikacja poprzez instrukcje SENDS7 i RCVS7



Instrukcje **SENDS7 i RCVS7** służą do bezpiecznego wysyłania i odbierania danych poprzez połączenia S7.

Instrukcje te mogą służyć do przesyłania określonych ilości danych fail-safe rodzaju BOOL, INT, WORD, DINT, DWORD oraz TIME w bezpieczny sposób. Dane fail-safe są przechowywane w utworzonych przez użytkownika F-DB (DB komunikacji bezpieczeństwa).

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVS7 **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDS7 **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane są wysyłane dopiero po wywołaniu instrukcji SENDS7 na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDS7 i RCVS7 można znaleźć w dziale SENDS7 oraz RCVS7: Komunikacja poprzez połączenia S7 (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 642).

DB komunikacji bezpieczeństwa

Dla każdego połączenia wysłane dane są przechowywane w F-DB (DBx komunikacji bezpieczeństwa), zaś otrzymane dane są przechowywane w F-DB (DBy komunikacji bezpieczeństwa).

W instrukcjach SENDS7 i RCVS7 można przypisać numery DB komunikacji bezpieczeństwa.

9.1.9.3 Programowanie komunikacji związanej z bezpieczeństwem poprzez połączenia S7

Wstęp

Programowanie komunikacja CPU safety – CPU poprzez połączenia S7 zostało opisane poniżej. W programach bezpieczeństwa odnośnych F- CPU należy ustawić następujące elementy:

- Utworzyć F-DB (DB komunikacji bezpieczeństwa), w którym zapisywane są dane wysyłane/odebrane dla komunikacji.
- Wywołać i przypisać parametry do instrukcji dla komunikacji z karty zadań „Instructions" (Instrukcje) w programie bezpieczeństwa.

Wymogi do programowania

Połączenia S7 pomiędzy odnośnymi F-CPU należy skonfigurować w widoku sieci w zakładce „Connections" (Połączenia) w *edytorze sprzętu i sieci*.

Tworzenie i edytowanie DB komunikacji bezpieczeństwa

DB komunikacji bezpieczeństwa to F-DB utworzone i edytowane w ten sam sposób co inne F-DB w drzewku projektu. W instrukcjach SENDS7 i RCVS7 można przypisać numery DB komunikacji bezpieczeństwa.

Uwaga

Długość i struktura DB komunikacji bezpieczeństwa po stronie odbiorcy muszą być zgodne z odnośnymi parametrami po stronie nadawcy.

Jeśli DB komunikacji bezpieczeństwa nie są zgodne, F-CPU może przejść w tryb STOP. Zdarzenie diagnostyczne jest wprowadzane do bufora diagnostycznego F-CPU.

Z tego względu zaleca się, by zastosować następującą procedurę:

1. Utworzyć DB komunikacji bezpieczeństwa w drzewku projektu lub poniżej w folderze „Program blocks" dla F-CPU po stronie nadawcy.
2. Określić odpowiednią strukturę DB komunikacji bezpieczeństwa, uwzględniając dane do przesłania.
3. Skopiować DB komunikacji bezpieczeństwa do drzewka projektu lub poniżej do folderu „Program blocks" dla F-CPU po stronie odbiorcy oraz zmienić nazwę, jeśli to konieczne.

Inne wymogi dla DB komunikacji bezpieczeństwa

DB komunikacji bezpieczeństwa musi spełniać również następujące właściwości:

- Nie mogą być instancją DB.
- Ich długość nie może przekraczać 100 bajtów.
- w DB komunikacji bezpieczeństwa można deklarować jedynie następujące rodzaje danych: BOOL, INT, WORD, DINT, DWORD oraz TIME.
- Rodzaje danych muszą być ułożone zgodnie z blokiem i w następującej kolejności: BOOL, rodzaj danych o długości bitowej 16 bitów (INT, WORD), oraz rodzaj danych o długości bitowej 32 bity (DINT, DWORD i TIME). W obrębie bloków danych o długości 16 i 32 bity, rodzaje danych mogą być ułożone dowolnie.
- Nie można zadeklarować więcej niż 128 elementów danych rodzaju BOOL.
- Ilość danych rodzaju BOOL zawsze musi być wielokrotnością liczby 16 (limit słowa). W razie konieczności należy dodać dane rezerwowe.

Jeśli te kryteria nie zostaną spełnione, *STEP 7 Safety Advanced* tworzy komunikat o błędzie podczas kompilacji.

Przypisanie wartości fail-safe

Wartości fail-safe są dostępne po stronie odbiorcy:

- Gdy połączenie pomiędzy partnerami komunikacji zostanie nawiązane po raz pierwszy po uruchomieniu systemów bezpieczeństwa
- Gdy wystąpi błąd komunikacji

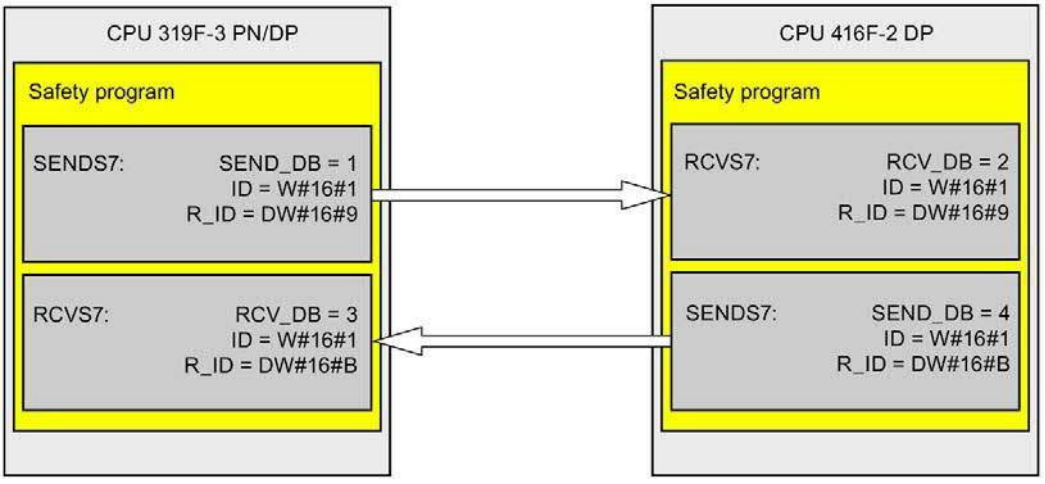
Wartości określone jako początkowe w DB komunikacji bezpieczeństwa po stronie odbiorcy zostaną udostępnione jako wartości początkowe.

Procedura programowania

Programowanie komunikacji związanej z bezpieczeństwem poprzez połączenia S7 odbywa się w następujący sposób:

1. Zasilić tagi w DB komunikacji bezpieczeństwa po stronie nadawcy sygnałami wysyłania, korzystając z w pełni kwalifikowanego dostępu (np. nazwa „Name of F-communication DB".tag („Nazwa DB komunikacji bezpieczeństwa".tag).
2. Odczytać tagi w DB komunikacji bezpieczeństwa po stronie odbiorcy (sygnału odebrania), które mają być dalej przetwarzane w innych sekcjach programu, korzystając z w pełni kwalifikowanego dostępu (np. nazwa „Name of F-communication DB".tag („Nazwa DB komunikacji bezpieczeństwa".tag).
3. W programie bezpieczeństwa, z którego dane będą wysyłane, należy wywołać instrukcję SENDS7 w celu wysłania na końcu głównego bloku bezpieczeństwa.
4. W programie bezpieczeństwa, w którym dane będą odbierane, należy wywołać instrukcję RCVS7 w celu odebrania na początku głównego bloku bezpieczeństwa.
5. Przypisać numery DB komunikacji bezpieczeństwa do wejścia SEND_DB w SENDS7 oraz do wejścia RCV_DB w RCVS7.
6. Przypisać lokalny identyfikator połączenia S7 (rodzaj danych: WORD) z perspektywy F-CPU skonfigurowanego w zakładce „Connections" (Połączenia) w widoku sieci do wejścia ID w SENDS7.

7. Przypisać lokalny identyfikator połączenia S7 (rodzaj danych: WORD) skonfigurowanego w zakładce „Connections" (Połączenia) w widoku sieci do wejścia ID w RCVS7.
8. Przypisać liczbę parzystą (rodzaj danych: DWORD) do wejść R_ID w SENDS7 i RCVS7. Pozwala to na określenie, czy instrukcja SENDS7 należy do instrukcji RCVS7. Powiązane instrukcje otrzymują tę samą wartość dla R_ID.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście R_ID; rodzaj danych: DWORD) można dobierać dowolnie; jednakże, muszą być nieparzyste i unikalne dla wszystkich połączeń komunikacji związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Wartość R_ID + 1 jest przypisywana wewnętrznie i nie należy z niej korzystać.

Należy doprowadzić wartości stałe do wejść ID oraz R_ID podczas wywoływania instrukcji. Bezpośredni dostęp do odczytu lub zapisu w powiązanej instancji DB jest niedozwolony w programie bezpieczeństwa! *(S020)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

9. Przypisać wejścia TIMEOUT instrukcji SENDS7 i RCVS7, wprowadzając wymagany czas monitorowania.

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcze i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

10. Aby zmniejszyć obciążenie magistrali, można tymczasowo wyłączyć komunikację pomiędzy F-CPU na wejściu EN_SEND instrukcji SENDS7. W tym celu należy doprowadzić na wejście EN_SEND wartość „0" (domyślnie = „PRAWDA"). W takim przypadku wysyłane dane nie są przesyłane do DB komunikacji bezpieczeństwa powiązanej instrukcji RCVS7, a odbiorca RCVS7 zapewnia wartości fail-safe przez ten okres (wartości początkowe DB komunikacji bezpieczeństwa). Jeśli pomiędzy partnerami nawiązana już była komunikacja, zostanie wykryty błąd komunikacji.
11. Opcjonalnie: Istnieje możliwość oceny wyjścia ACK_REQ instrukcji RCVS7, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy zatwierdzenie jest wymagane.
12. Doprowadzić na wejście ACK_REI instrukcji RCVS7 sygnał do zatwierdzenia w celu reintegracji.
13. Opcjonalnie: wykonać ocenę wyjścia SUBS_ON instruckji RCVS7 lub SENDS7 w celu określenia, czy instrukcja RCVS7 wyprowadza wartości fail-safe określone jako wartości początkowe w DB komunikacji bezpieczeństwa.
14. Opcjonalnie: Istnieje możliwość oceny wyjścia ERROR instrukcji RCVS7 lub SENDS7, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy wystąpił błąd komunikacji.
15. Opcjonalnie: Istnieje możliwość oceny wyjścia SENDMODE instrukcji RCVS7, by wykonać zapytanie, czy F-CPU z powiązaną instrukcją SENDS7 znajduje się w wyłączonym trybie bezpieczeństwa (strona 360).

Specjalne kwestie dla migrowanych projektów

W przypadku migrowania projektu z *S7 Distributed Safety V5.4 SP5* do *STEP 7 Safety Advanced,* w którym zaprogramowana jest komunikacja safety poprzez połączenia S7, należy mieć na uwadze następujące zagadnienia:

- Nie należy usuwać zmigrowanych instancji DB dla instrukcji SENDS7 i RCVS7 w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks".

W przeciwnym razie mogą wystąpić błędy komunikacji w odnośnych połączeniach

komunikacyjnych.

Migrowane instancje DB dla instrukcji SENDS7 i RCVS7 zostały usunięte, jeśli, po skompilowaniu programu bezpieczeństwa, „identyfikator definiowany przez użytkownika" w nowo utworzonych nie jest identyczny z „FRCVS7CL" lub „FSNDS7CL".

„Identyfikator definiowany przez użytkownika" bloku można znaleźć w jego właściwościach

w obszarze „Information" (Informacje).

9.1.9.4 Komunikacja safety poprzez połączenia S7 – ograniczenia transferu danych

Uwaga

Jeśli ilość danych do przesłania przekracza dozwoloną długość dla DB komunikacji bezpieczeństwa (100 bajtów), można utworzyć kolejny DB komunikacji bezpieczeństwa, który przenosi się do dodatkowych instrukcji SENDS7/RCVS7 ze zmodyfikowanym R_ID.

Należy pamiętać, że instrukcje USEND i URCV są wywoływane wewnętrzne przy każdym wywołaniu SENDS7 lub RCVS7 i korzystają z zasobów połączenia w F-CPU. Wpływa to na maksymalną liczbę dostępnych połączeń komunikacyjnych (*patrz podręcznik do F-CPU*).

Dodatkowe informacje dotyczące ograniczeń transferu danych dla połączeń S7 poszczególnych F-CPU są dostępne na stronie (http://support.automation.siemens.com/WW/view/en/38549114).

9.1.10 Komunikacja safety z innymi systemami bezpieczeństwa S7

9.1.10.1 Wstęp

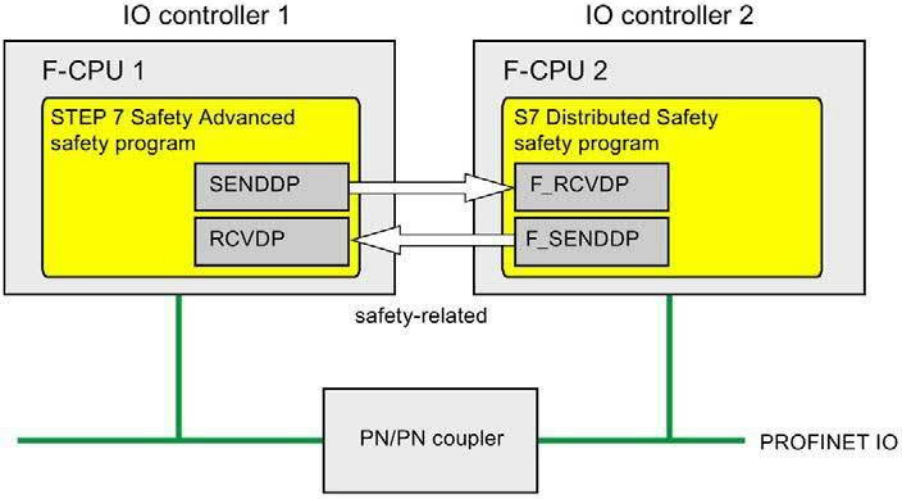
Komunikacja safety z F-CPU w SIMATIC Safety do F-CPU
w systemach bezpieczeństwa S7 Distributed Safety jest możliwa poprzez złącze PN/PN lub złącze DP/DP wykorzystywane pomiędzy dwoma F-CPU jako komunikacja sterownik IO – sterownik IO, komunikacja urządzenie nadrzędne – urządzenie nadrzędne bądź komunikacja poprzez ustalone połączenia S7.

Komunikacja safety z F-CPU w SIMATIC Safety do F-CPU

w systemach bezpieczeństwa S7 F/FH jest możliwa poprzez ustalone połączenia S7.

9.1.10.2 Komunikacja z S7 Distributed Safety za pomocą połączenia PN/PN (komunikacja sterownik IO – sterownik IO)

Funkcje komunikacyjne pomiędzy instrukcjami SENDDP/RCVDP na końcu *STEP 7 Safety Advanced* oraz bloki aplikacji bezpieczeństwa F_SENDDP/F_RCVDP na końcu *S7 Distributed Safety*:



Procedura na końcu *S7 Distributed Safety*

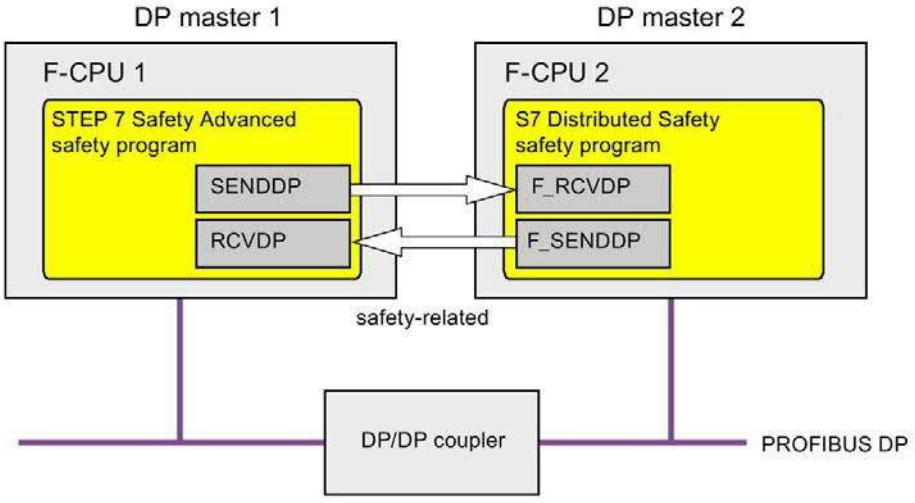
Na końcu *S7 Distributed Safety* należy postępować zgodnie z opisem w dziale „Komunikacja sterownik IO safety – sterownik IO" w podręczniku S7 Distributed Safety - Konfiguracja i programowanie (http://support.automation.siemens.com/WW/view/en/22099875).

Procedura na końcu *STEP 7 Safety Advanced*

Na końcu *STEP 7 Safety Advanced*, należy postępować zgodnie z opisem w Komunikacja sterownik IO safety – sterownik IO (strona 212).

9.1.10.3 Komunikacja z S7 Distributed Safety za pomocą połączenia DP/DP (komunikacja jednostka nadrzędna – jednostka nadrzędna)

Funkcje komunikacyjne pomiędzy instrukcjami SENDDP/RCVDP na końcu *STEP 7 Safety Advanced* oraz bloki aplikacji bezpieczeństwa F_SENDDP/F_RCVDP na końcu *S7 Distributed Safety*:



Procedura na końcu *S7 Distributed Safety*

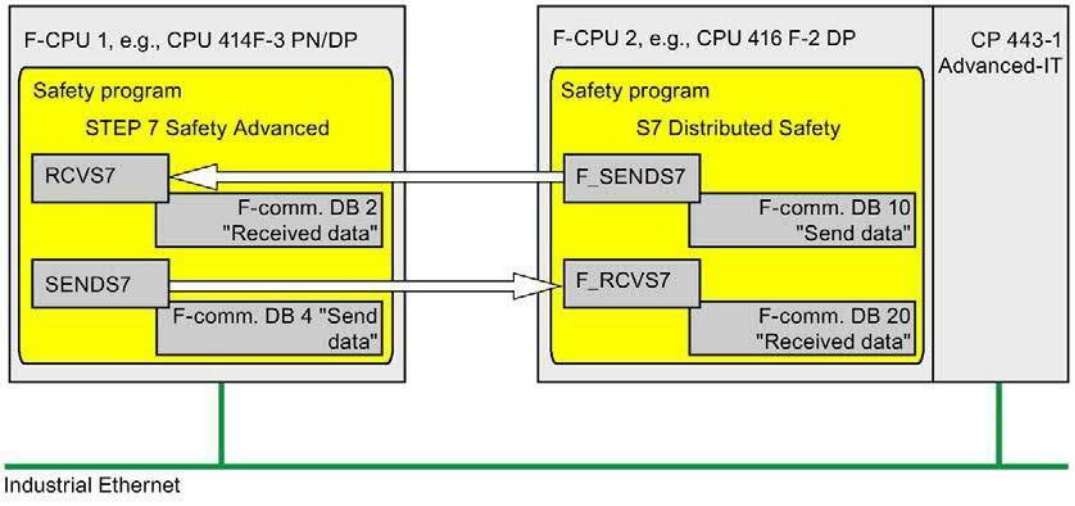
Na końcu *S7 Distributed Safety* należy postępować zgodnie z opisem w dziale „Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne" w podręczniku S7 Distributed Safety - Konfiguracja i programowanie (http://support.automation.siemens.com/WW/view/en/22099875).

Procedura na końcu *STEP 7 Safety Advanced*

Na końcu *STEP 7 Safety Advanced*, należy postępować zgodnie z opisem w Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne (strona 222).

9.1.10.4 Komunikacja z S7 Distributed Safety za pomocą połączeń S7

Funkcje komunikacyjne pomiędzy instrukcjami SENDS7/RCVS7 na końcu *STEP 7 Safety Advanced* oraz bloki aplikacji bezpieczeństwa F_SENDS7/F_RCVS7 na końcu *S7 Distributed Safety*:



Procedura na końcu *S7 Distributed Safety*

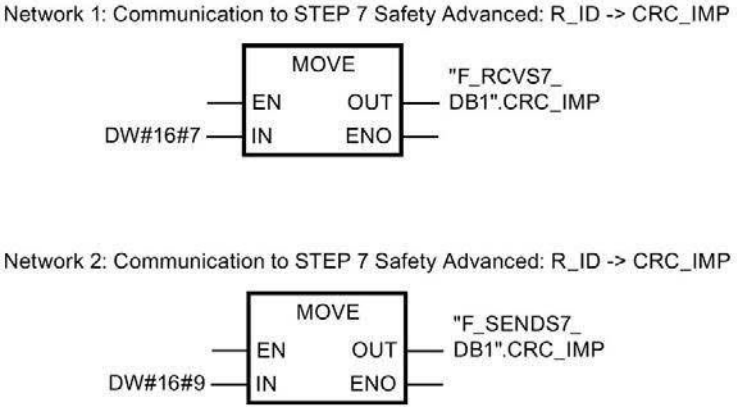
Na końcu *S7 Distributed Safety* należy postępować zgodnie z opisem w dziale „Komunikacja safety poprzez komunikację S7" w podręczniku S7 Distributed Safety - Konfiguracja i programowanie (http://support.automation.siemens.com/WW/view/en/22099875).

Jako że komunikacja safety poprzez połączenia S7 nie jest możliwa z nieokreślonymi partnerami w S7 Distributed Safety, należy najpierw utworzyć „wirtualną" stację SIMATIC w *S7 Distributed Safety*, w którym konfiguruje się F-CPU, stanowiący element pośredniczący dla F-CPU w *STEP 7 Safety Advanced* z jego adresem IP.

Następnie wstawia się połączenie S7 do tego F-CPU w tabeli połączeń. Zarówno połączenie lokalne, jak i zasoby połączenia partnerskiego (hex) są zatem stałe. Następnie należy ustawić te powiązane, nieokreślone połączenia S7, które zostały utworzone w *STEP 7 Professional*.

Ponadto, dla wszystkich połączeń komunikacyjnych do tego F-CPU, należy przesłać identyfikator komunikacji bezpieczeństwa, który został przypisany na wejściu R_ID powiązanych wywołań bloków aplikacji bezpieczeństwa F_SENDS7 i F_RCVS7, dodatkowo do taga CRC_IMP w instancji DB kolejno F_SENDS7 i F_RCVS7, w standardowym programie użytkownika tuż przed wywołaniem F-CALL.

Przykład programu:



Procedura na końcu *STEP 7 Safety Advanced*

Na końcu *STEP 7 Safety Advanced*, należy postępować zgodnie z opisem w Komunikacja safety poprzez połączenia S7 (strona 258).

Dla F-CPU w *S7 Distributed Safety* należy utworzyć i określić nieokreślone połączenie S7. Informacje dotyczące tego zagadnienia można znaleźć w pomocy *STEP 7* , pod hasłem „Tworzenie nieokreślonych połączeń" lub „Określanie nieokreślanych połączeń".

W tym celu należy ustawić lokalne i partnerskie zasoby połączenia (hex), które są stałe jako wynik powiązanego połączenia S7, które utworzono w *S7 Distributed Safety*.

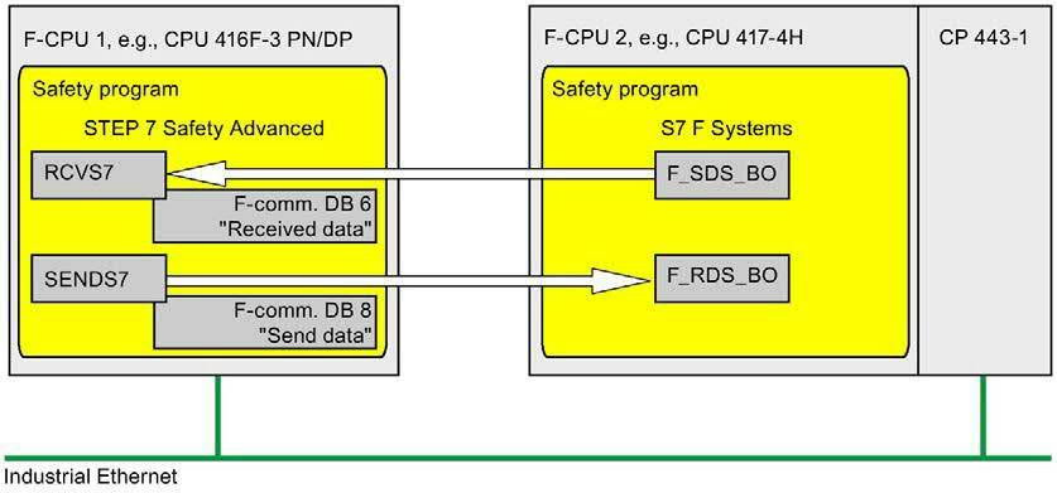
Jeśli zasoby połączenia lokalnego (hex) są zajęte przez istniejące połączenie, należy zmienić zasoby połączenia (hex) na nie.

Jeśli DB instancji SENDS7 i RCVS7, instrukcje, które służą do komunikacji z *S7 Distributed Safety* zostały przeniesione z *S7 Distributed Safety*, należy usunąć je w drzewku projektu w folderze „STEP 7 Safety", pod hasłem „Program blocks > System blocks" (Bloki programu > Bloki systemowe) (w przeciwieństwie do informacji w Programowanie komunikacji związanej z bezpieczeństwem poprzez połączenia S7 (strona 261), dział „Specjalne kwestie dla migrowanych projektów").

9.1.10.5 Komunikacja z systemami F/FH S7 za pomocą połączeń S7

Funkcje komunikacyjne pomiędzy instrukcjami SENDS7/RCVS7 na końcu *STEP 7 Safety Advanced* oraz bloki bezpieczeństwa F_SDS_BO/F_RDS_BO na końcu *systemów bezpieczeństwa S7*.

Możliwa jest wymiana maksymalnie 32 elementów danych rodzaju BOOL.



Procedura na końcu *systemów bezpieczeństwa S7*

Na końcu *systemów bezpieczeństwa S7* należy postępować zgodnie z opisem w dziale „Komunikacja safety pomiędzy F-CPU" w podręczniku „Systemy S7 F/FH - Konfiguracja i programowanie (http://support.automation.siemens.com/WW/view/en/16537972).

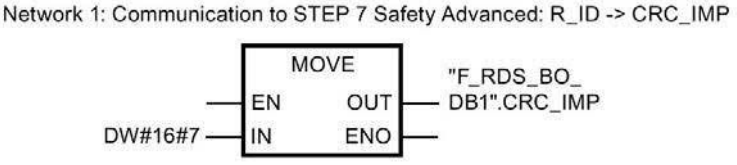
Jako że komunikacja safety poprzez połączenia S7 nie jest możliwa z nieokreślonymi partnerami w *systemach S7 F/FH*, należy najpierw utworzyć „wirtualną" stację SIMATIC w *systemach S7 F/FH*, w których konfiguruje się F-CPU, stanowiącą element pośredniczący dla F-CPU w *STEP 7 Safety Advanced* z jego adresem IP.

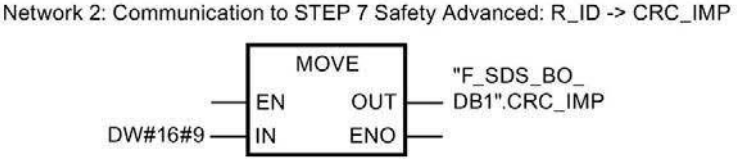
Następnie wstawia się połączenie S7 do tego F-CPU w tabeli połączeń. Zarówno połączenie lokalne, jak i zasoby połączenia partnerskiego (hex) są zatem stałe. Następnie należy ustawić te powiązane, nieokreślone połączenia S7, które zostały utworzone w *STEP 7*

Safety Advanced.

Ponadto należy wstawić funkcję w programie S7 (w obszarze zastrzeżonym w CFC dla innych aplikacji), w której, dla wszystkich połączeń komunikacyjnych tego F-CPU, przenosi się ID komunikacji bezpieczeństwa przypisany na wejściu R_ID do powiązanych wywołań bloków bezpieczeństwa F_SDS_BO oraz F_RDS_BO, dodatkowo do taga CRC_IMP w instancji DB, kolejno F_SDS_BO i F_RDS_BO. Numer DB instancji uzyskuje się z właściwości obiektu bloku w CFC. Należy przypisać nazwy opisowe do tych DB instancji. W przypadku wykonania kompresji w CFC, należy sprawdzić, czy numery instancji DB uległy zmianie.

Przykład programu:





Następnie należy zaimportować funkcję w CFC jako rodzaj bloku i wstawić standardowy program użytkownika do schematu. W sekwencji roboczej należy upewnić się, czy powiązana standardowa grupa runtime jest przetwarzana przed grupą F-runtime.

Procedura na końcu *STEP 7 Safety Advanced*

Na końcu *STEP 7 Safety Advanced*, należy postępować zgodnie z opisem w Komunikacja safety poprzez połączenia S7 (strona 258).

W szczególności: W *STEP 7 Safety Advanced* należy utworzyć DB komunikacji bezpieczeństwa z dokładnie 32 elementami danych rodzaju BOOL.

Dla F-CPU w *systemach S7 F/FH* należy utworzyć i określić nieokreślone połączenie S7. Informacje dotyczące tego zagadnienia można znaleźć w pomocy

STEP 7 , pod hasłem „Tworzenie nieokreślonych połączeń" lub „Określanie nieokreślanych połączeń".

W tym celu należy ustawić lokalne i partnerskie zasoby połączenia (hex), które są stałe jako wynik powiązanego połączenia S7, które utworzono w *systemach bezpieczeństwa S7*.

Jeśli zasoby połączenia lokalnego (hex) są zajęte przez istniejące połączenie, należy zmienić zasoby połączenia (hex) na nie.

9.2 Konfiguracja i programowanie komunikacji (S7-1200, S7-1500)

9.2.1 Przegląd komunikacji

Wstęp

W tym dziale zamieszczono omówienie opcji komunikacji związanej z bezpieczeństwem w systemach bezpieczeństwa SIMATIC Safety.

Opcje komunikacji związanej z bezpieczeństwem

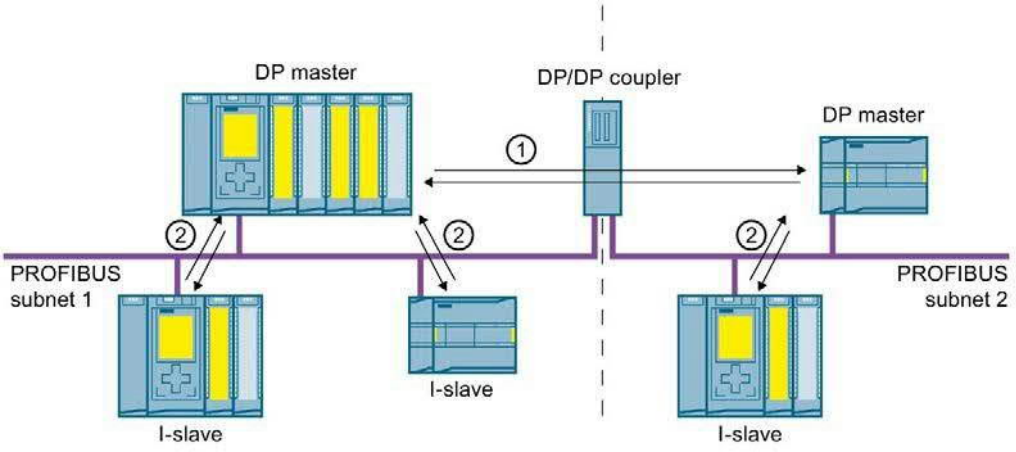
Komunikacja safety	**Na podsieci**	**Wymagany dodatkowy sprzęt**
Komunikacja CPU safety – CPU:		
Komunikacja sterownik IO – sterownik IO	PROFINET IO	złącze PN/PN
Komunikacja urz. nadrzędne – urz. nadrzędne	PROFIBUS DP	złącze DP/DP
Komunikacja sterownik IO – I-device	PROFINET IO	—
Komunikacja urz. nadrzędne – urz. I-slave	PROFIBUS DP	—
Komunikacja sterownik IO – urz. I-slave	PROFINET IO i PROFIBUS DP	Połączenie IE/PB
Komunikacja sterownik IO – sterownik IO do *S7 Distributed Safety*	PROFINET IO	złącze PN/PN
Komunikacja urządzenie nadrzędne – urządzenie nadrzędne do *S7 Distributed Safety*	PROFIBUS DP	złącze DP/DP

Uwaga

Komunikacja safety z F-CPU S7-1200 jest dozwolona jedynie od wersji oprogramowania V4.1.2.

Omówienie komunikacji związanej z bezpieczeństwem poprzez PROFIBUS DP

Poniższa ilustracja przedstawia omówienie opcji komunikacji związanej z bezpieczeństwem poprzez PROFIBUS DP w systemach bezpieczeństwa SIMATIC Safety z F-CPU S7-1200/1500.

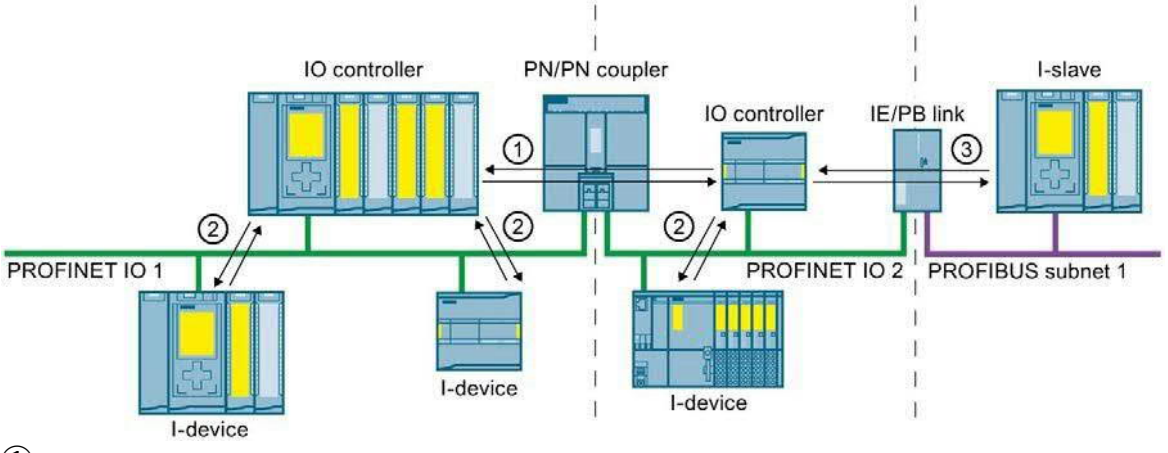


① Komunikacja urządzenie nadrzędne

② safety – urządzenie

Omówienie komunikacji związanej z bezpieczeństwem poprzez PROFINET IO

Poniższa ilustracja przedstawia omówienie opcji komunikacji związanej z bezpieczeństwem poprzez PROFINET IO w systemach bezpieczeństwa SIMATIC Safety z F-CPU S7-1200/1500.



① Komunikacja sterownik IO safety – sterownik IO

② Komunikacja sterownik IO safety – I-device

③ Komunikacja sterownik IO safety – urządzenie I-slave

Komunikacja CPU safety – CPU poprzez PROFIBUS DP lub PROFINET IO

W komunikacji CPU safety – CPU stała ilość danych rodzaju BOOL lub INT (alternatywnie DINT) jest przekazywana pomiędzy programami bezpieczeństwa w F-CPU urządzeń nadrzędnych DP/urządzeń I-slave lub sterownikami IO/urządzeniami I.

Dane są przesyłane przy użyciu instrukcji SENDDP do wysyłania oraz instrukcji RCVDP do odbierania. Dane są przechowywane w skonfigurowanych obszarach transferowych urządzeń. Identyfikator sprzętowy (identyfikator HW) definiuje skonfigurowane obszary transferu.

Komunikacja sterownik CPU safety – CPU do *S7 Distributed Safety*

Komunikacja safety jest możliwa z F-CPU w *SIMATIC Safety* do F-CPU w *S7 Distributed Safety*.

9.2.2 Komunikacja sterownik IO safety – sterownik IO

9.2.2.1 Konfiguracja komunikacji sterownik IO safety – sterownik IO

Wstęp

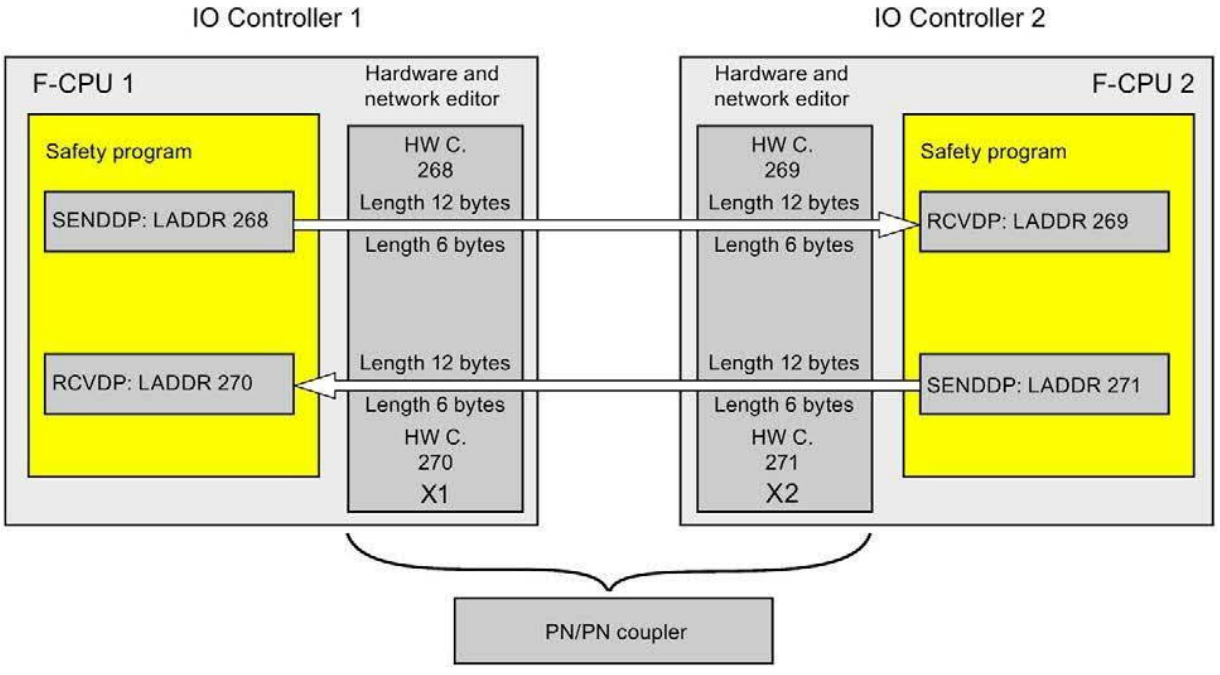
Komunikacja safety pomiędzy programami bezpieczeństwa F- CPU sterowników IO odbywa się poprzez złącze PN/PN, który ustawia się pomiędzy F- CPU.

Uwaga

Należy wyłączyć parametr „Data validity display DIA" (Wyświetlacz ważności danych DIA) we właściwościach złącza PN/PN w *edytorze sprzętu i sieci*. Jest to domyślne ustawienie. W przeciwnym razie komunikacja sterownik IO safety – sterownik IO nie jest możliwa.

Konfigurowanie obszarów transferu

Należy skonfigurować jeden obszar transferowy dla danych wyjściowych oraz jeden obszar dla danych wejściowych w *edytorze sprzętu i sieci* dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU w złączu PN/PN. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać **oraz** odbierać dane (komunikacja dwukierunkowa).



Zasady definiowania obszarów transferu

Dane do wysłania:

Obszar transferu dla danych wyjściowych wymaga łącznie 12 bajtów (spójnych); obszar transferu dla danych wejściowych wymaga 6 bajtów (spójnych).

Dane do odebrania:

Obszar transferu do danych wejściowych wymaga łącznie 12 bajtów (spójnych); obszar transferu danych wyjściowych wymaga 6 bajtów (spójnych).

Uwaga

Złącze PN/PN, numer zamówieniowy 6ES7158-3AD10-0XA0

Podczas konfigurowania obszarów transferu dla danych wyjściowych i wejściowych, należy postępować zgodnie z opisem w podręczniku „Złącze PN/PN połączeń magistrali SIMATIC (https://support.industry.siemens.com/cs/ww/en/view/44319532)", dział „Konfiguracja złącza PN/PN z STEP 7 TIA Portal".

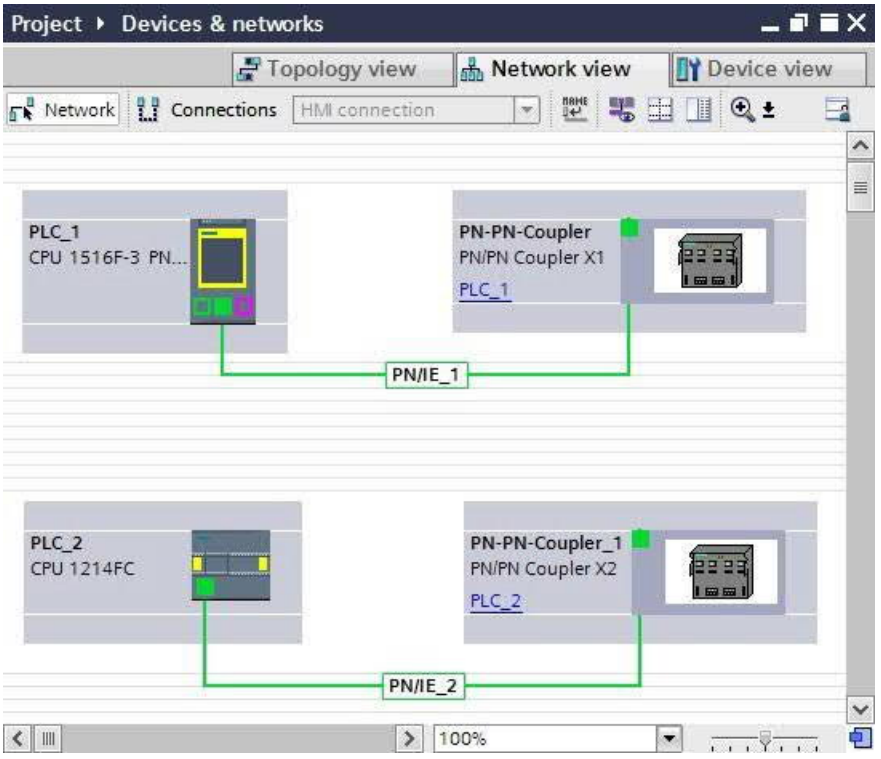
Procedura konfiguracji

Procedura konfiguracji komunikacja sterownik IO safety – sterownik IO przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Przełączyć na widok sieci w *edytorze sprzętu i sieci*.
3. Wybrać złącze PN/PN X1 oraz złącze PN/PN X2 z „Other field devices¥PROFINET IO¥Gateway¥Siemens AG¥PN/PN Coupler" w karcie zadań „Hardware catalog" (Katalog sprzętu) i wstawić je do widoku sieci w edytorze.

4. Połączyć interfejs PN F-CPU 1 z interfejsem PN złącza PN/PN X1 oraz interfejs PN F-CPU 2 z interfejsem PN złącza PN/PN X2.

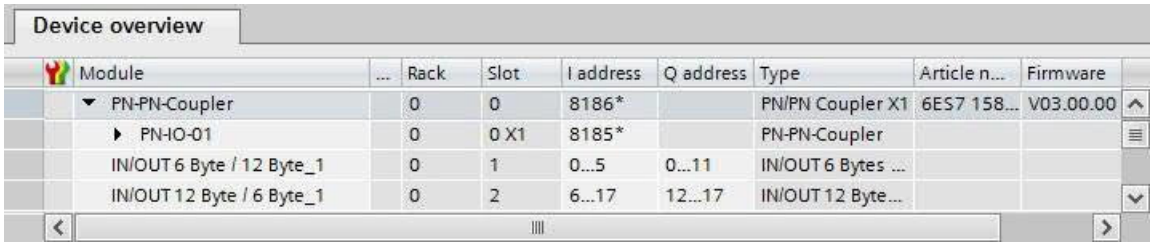


5. Przełączyć na widok urządzenia dla złącza PN/PN X1 do połączeń komunikacji dwukierunkowej, tj. gdy F-CPU jednocześnie wysyła i odbiera dane. Wybrać następujące moduły z pola „IN/OUT" zakładki zadań „Hardware catalog" (Katalog sprzętu) (z aktywnym filtrem), po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń):

   – Jeden moduł „IN/OUT 6 bytes / 12 bytes" oraz
   – Jeden moduł „IN/OUT 12 bytes / 6 bytes"

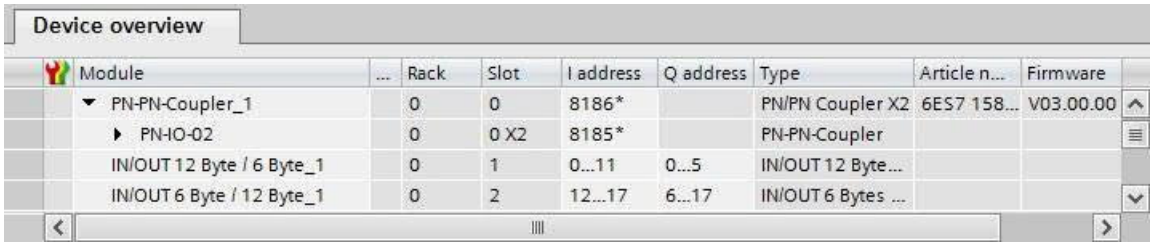
Uwaga

Obszary transferu są przypisywane na podstawie identyfikatora sprzętowego, który jest automatycznie przypisywany do modułów i urządzeń. Identyfikator jest potrzebny do zaprogramowania bloków SENDDP i RCVDP (wejście LADDR). Dla każdego identyfikatora obszaru transferu tworzona jest stała systemowa w odpowiadającym F-CPU. Możliwe jest przypisanie tych stałych symbolicznie do bloków SENDDP i RCVDP.



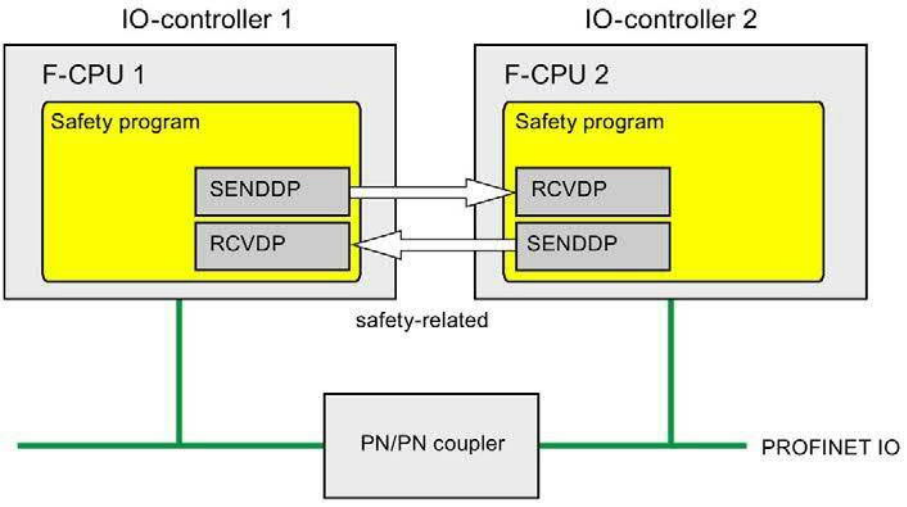
6. Wybrać następujące moduły z pola „IN/OUT" w widoku urządzenia dla złącza PN/PN X2, po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń):

   – Jeden moduł „IN/OUT 12 bytes / 6 bytes" oraz
   – Jeden moduł „IN/OUT 6 bytes / 12 bytes"



9.2.2.2 Komunikacja sterownik IO safety – sterownik IO poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU sterowników IO wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych. Można wykorzystać je do wykonywania przesyłu typu fail-safe *stałych* ilość danych typu fail-safe rodzaju BOOL lub INT (alternatywnie DINT).

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Możliwe jest również wywołanie instrukcji RCVDP i SENDDP w odrębnych F-FB/F-FC, które należy wywołać na początku lub na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.2.2.3 Programowanie komunikacji program sterownika IO związanego z bezpieczeństwem – sterownik IO

Wymogi do programowania

Należy skonfigurować obszary transferu do danych wejściowych i wyjściowych złącza PN/PN.

Procedura programowania

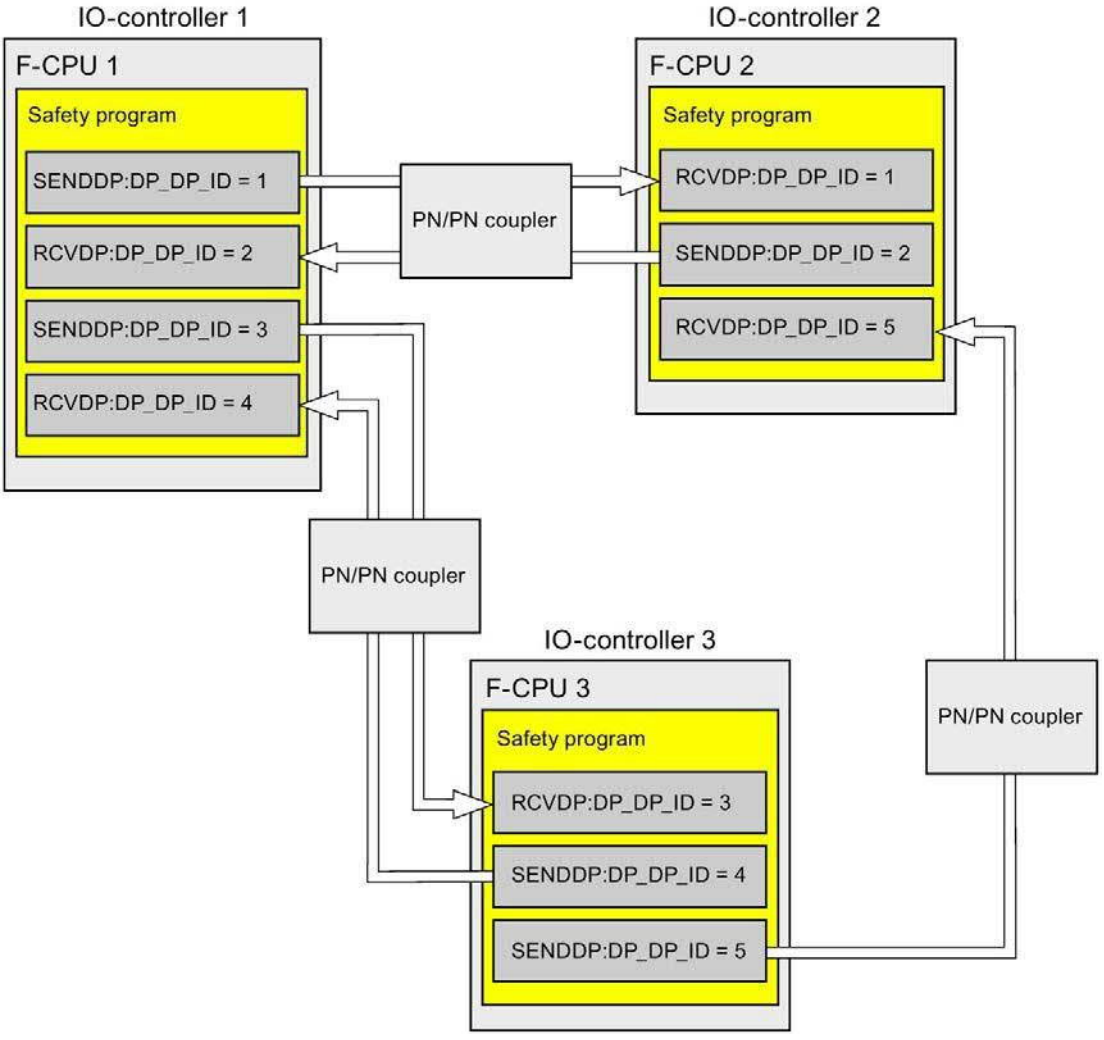
Komunikację program bezpieczeństwa – sterownik IO safety – sterownik IO programuje się w następujący sposób:

1. W programie bezpieczeństwa, z którego dane będą wysyłane, należy wywołać instrukcję SENDDP (strona 631) w celu wysłania na końcu głównego bloku bezpieczeństwa.
2. W programie bezpieczeństwa, w którym dane będą odbierane, należy wywołać instrukcję RCVDP (strona 631) w celu odebrania na początku głównego bloku bezpieczeństwa.
3. Należy przypisać odpowiednie identyfikatory sprzętowe wejść LADDR (stałe systemowe w domyślnej tabeli tagów) do obszarów transferu dla danych wyjściowych i wejściowych złącza PN/PN skonfigurowanego w edytorze sprzętu i sieci.

   Należy wykonać to przypisanie dla każdego połączenia komunikacyjnego w każdym F-CPU.

4. Przypisać wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa do wejść DP_DP_ID. Pozwala to na ustalenie związku komunikacji pomiędzy instrukcją SENDDP w jednym F-CPU a instrukcją RCVDP w drugim F-CPU: Powiązane instrukcje otrzymują tę samą wartość dla DP_DP_ID.

   Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla 5 powiązań komunikacji sterownik IO safety – sterownik IO.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie**; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości*** do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** S7-1200/1500: Od wersji V3.0 instrukcji SENDDP i RCVDP, nie jest nawiązywane połączenie na wejściu DP_DP_ID do identyfikatora komunikacji bezpieczeństwa „0".

*** S7-1200/1500: Od wersji V3.0 instrukcji the SENDDP i RCVDP, na wejście DP_DP_ID można również doprowadzać wartości zmienne z globalnego F-DB. W takim przypadku również należy skontrolować podczas odbioru programu bezpieczeństwa, czy zapewniona jest unikalność *przez cały czas*, sprawdzając algorytm do tworzenia wartości zmiennych. Jeśli nie można zagwarantować unikalnego identyfikatora komunikacji bezpieczeństwa podczas uruchomienia programu bezpieczeństwa, ponieważ jest on określany dopiero po uruchomieniu programu, należy upewnić się, że podczas tej fazy wartość na wejściu DP_DP_ID wynosi „0".

5. Doprowadzić na wejścia SD_BO_xx i SD_I_xx (alternatywnie SD_DI_00) w SENDDP sygnały wysyłania. Aby ograniczyć sygnały pośrednie podczas przesyłania bloków transferowych, można zapisać wartość bezpośrednio do instancji DB w SENDDP, korzystając z w pełni kwalifikowanego dostępu (przykładowo, "Name SENDDP_1".SD_BO_02) przed wywołaniem SENDDP.

6. Należy doprowadzić na wyjścia RD_BO_xx i RD_I_xx (alternatywnie RD_DI_00) w RCVDP sygnały, które mają dalej być przetwarzane przez inne sekcje programu lub użyć w pełni kwalifikowanego dostępu, by odczytać otrzymane sygnały bezpośrednio z powiązanych instancji DB w sekcjach programu, które będą przetwarzane dalej (np. "Name RCVDP_1".RD_BO_02).

7. Aby wysłać dane na wejściu SD_DI_00 zamiast danych na wejściach SD_I_00 i SD_I_01, należy doprowadzić na wejście DINTMODE (wartość początkowa = „FAŁSZ") w SENDDP wartość „PRAWDA".

8. Należy zasilić wejścia SUBBO_xx i SUBI_xx, lub alternatywnie SUBDI_00, w RCVDP za pomocą wartości fail-safe wyprowadzanej przez RCVDP zamiast danych procesowych, aż zostanie ustanowiona komunikacja po raz pierwszy po uruchomieniu wysyłania i odbioru systemów bezpieczeństwa, lub w przypadku błędu komunikacji związanej z bezpieczeństwem.

   – Specyfikacja stałych wartości fail-safe:

     W przypadku danych rodzaju INT/DINT, można wprowadzić stałe wartości fail-safe bezpośrednio jako stałe w wejściu SUBI_xx lub alternatywnie SUBDI_00 (wartość początkowa = "0"). Aby określić stałą wartość fail-safe „PRAWDA" dla danych rodzaju BOOL, należy ustawić „PRAWDA" dla wejścia SUBBO_xx (wartość początkowa = „FAŁSZ").

   – Specyfikacja zmiennych wartości zastępczych:

     Aby określić zmienne wartości zastępcze, należy zdefiniować tag obliczany poprzez program bezpieczeństwa w F-DB, po czym określić go (w pełni kwalifikowany) w wejściu SUBBO_XX lub SUBI_xx, bądź alternatywnie SUBDI_00.

OSTRZEŻENIE

Uwaga: Logika programu do obliczania zmiennych wartości zastępczych może być wstawiona jedynie za wywołaniami RCVDP, ponieważ obszar przed nimi musi być wolny od operacji logicznych. Dlatego też, w pierwszym cyklu po uruchomieniu systemu bezpieczeństwa, we wszystkich instrukcjach RCVDP aktywne są wartości początkowe wartości zastępczych. Należy zatem przypisać do tych znaczników odpowiednie wartości początkowe. *(S017)*

9. Skonfigurować wejścia TIMEOUT instrukcji RCVDP i SENDDP, wprowadzając wymagany czas monitorowania.

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcy i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

10. Opcjonalnie: Istnieje możliwość oceny wyjścia ACK_REQ instrukcji RCVDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy zatwierdzenie jest wymagane.
11. Należy doprowadzić sygnał zatwierdzenia na wejście ACK_REI instrukcji RCVDP w celu przeprowadzenia reintegracji.
12. Opcjonalnie: Istnieje możliwość oceny wyjścia SUBS_ON instrukcji RCVDP lub SENDDP, by wykonać zapytanie, czy instrukcja RCVDP wyprowadza wartości fail-safe przypisane w wejściach SUBBO_xx i SUBI_xx lub alternatywnie SUBDI_00.
13. Opcjonalnie: Istnieje możliwość oceny wyjścia ERROR instrukcji RCVDP lub SENDDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy wystąpił błąd komunikacji.
14. Opcjonalnie: Istnieje możliwość oceny wyjścia SENDMODE instrukcji RCVDP, by wykonać zapytanie, czy F-CPU z powiązaną instrukcją SENDDP znajduje się w wyłączonym trybie bezpieczeństwa (strona 360).

9.2.2.4 Komunikacja sterownik IO safety – sterownik IO – ograniczenia transferu danych

Uwaga

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć drugiego (lub trzeciego) wywołania SENDDP / RCVDP. Wymaga to skonfigurowania dodatkowego połączenia poprzez złącze PN/PN. To, czy jest to możliwe z pojedynczym złączem PN/PN, zależy od ograniczeń przepustowości tego złącza.

9.2.3 Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne

9.2.3.1 Konfiguracja komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne

Wstęp

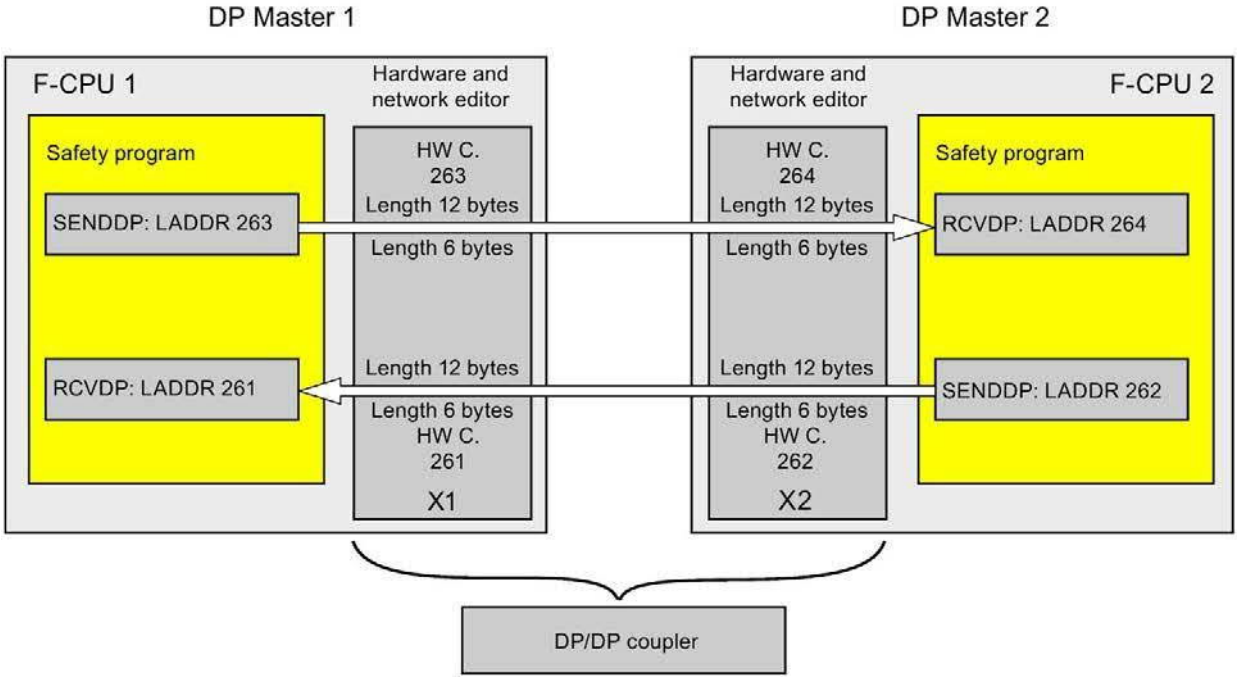
Komunikacja safety pomiędzy programami bezpieczeństwa F-CPU urządzeń nadrzędnych DP odbywa się poprzez złącze DP/DP.

Uwaga

Należy przełączyć wskaźnik ważności danych „DIA" na przełączniku DIP złącza DP/DP na „OFF" (wył). W przeciwnym razie komunikacja safety CPU – CPU nie jest możliwa.

Konfigurowanie obszarów transferu

Należy skonfigurować jeden obszar transferowy dla danych wyjściowych oraz jeden obszar dla danych wejściowych w *edytorze sprzętu i sieci* dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU w złączu DP/DP. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać oraz odbierać dane (komunikacja dwukierunkowa).



Zasady definiowania obszarów transferu

Dane do wysłania:

Obszar transferu dla danych wyjściowych wymaga łącznie 12 bajtów (spójnych); obszar transferu dla danych wejściowych wymaga 6 bajtów (spójnych).

Dane do odebrania:

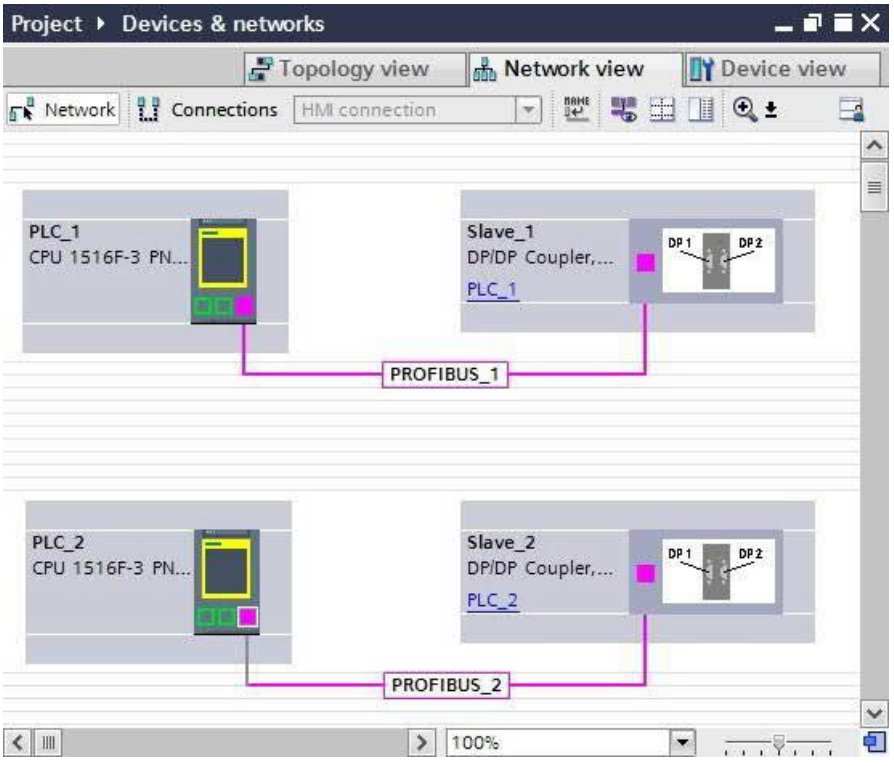
Obszar transferu do danych wejściowych wymaga łącznie 12 bajtów (spójnych); obszar transferu danych wyjściowych wymaga 6 bajtów (spójnych).

Procedura konfiguracji

Procedura konfiguracji komunikacji urządzenie nadrzędne safety
– urządzenie nadrzędne przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Przełączyć na widok sieci w *edytorze sprzętu i sieci*.
3. Wybrać złącze DP/DP z pozycji „Other field devices¥PROFIBUS DP¥Gateways¥Siemens AG¥DP/DP Coupler" w karcie zadań „Hardware catalog" (Katalog sprzętowy) i wstawić je do widoku sieci edytora sprzętu i sieci.
4. Wstawić drugie złącze DP/DP.
5. Podłączyć interfejs DP F-CPU 1 do interfejsu DP złącza DP/DP oraz interfejs DP F-CPU 2 do interfejsu DP drugiego złącza DP/DP.



6. Wolny adres PROFIBUS jest przypisywany automatycznie we właściwościach złącza DP/DP w widoku urządzenia. Należy ustawić ten adres na złączu DP/DP, korzystając z przełącznika DIP na urządzeniu lub w konfiguracji złącza DP/DP (patrz podręcznik „Złącze DP/DP" (http://support.automation.siemens.com/WW/view/en/1179382)).

7. Przełączyć na widok urządzenia dla złącza DP/DP PLC1 do połączeń komunikacji dwukierunkowej, tj. gdy oba F-CPU powinny jednocześnie wysyłać i odbierać dane. Wybrać następujące moduły z zakładki zadań „Hardware catalog" (Katalog sprzętu) (z aktywnym filtrem), po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń) złącza DP/DP:
   - Jeden moduł „6 bytes I/12 bytes Q consistent" oraz
   - Jeden moduł „12 bytes I/6 bytes Q consistent"

   Uwaga

   Obszary transferu są przypisywane na podstawie identyfikatora sprzętowego, który jest automatycznie przypisywany do modułów i urządzeń. Identyfikator jest potrzebny do zaprogramowania bloków SENDDP i RCVDP (wejście LADDR). Dla każdego identyfikatora obszaru transferu tworzona jest stała systemowa w odpowiadającym F-CPU. Możliwe jest przypisanie tych stałych symbolicznie do bloków SENDDP i RCVDP.

Device overview

...	Module	Rack	Slot	I address	Q address	Type	Article no.	Firmw...
	Slave_1	0	0 0	8186*		DP/DP Co...	6ES7 158-0AD01...	B0
	6 Bytes E/12 Bytes A konsist...	0	0 1	256...261	256...267	6 Bytes I/...		
	12 Bytes E/6 Bytes A konsist...	0	0 2	262...273	268...273	12 Bytes ...		
		0	3					

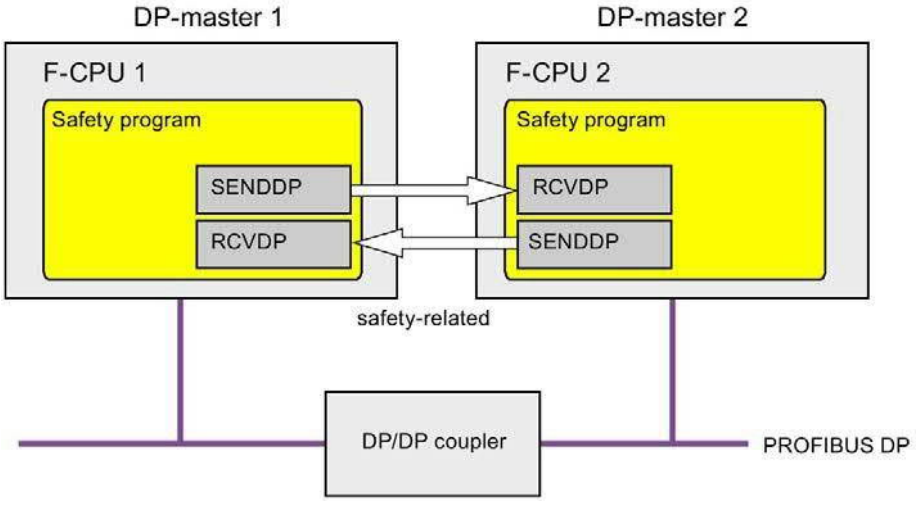
8. Wybrać następujące moduły z karty zadań „Hardware catalog (Katalog sprzętowy) (z aktywnym filtrem) w widoku urządzenia dla złącza DP/DP PLC2, po czym wstawić je do zakładki „Device overview" (Przegląd urządzeń):
   - Jeden moduł „12 bytes I/6 bytes Q consistent" oraz
   - Jeden moduł „6 bytes I/12 bytes Q consistent"

Device overview

...	Module	Rack	Slot	I address	Q address	Type	Article no.	Firmw...
	Slave_2	0	0 0	8186*		DP/DP Co...	6ES7 158-0AD01...	B0
	12 Bytes E/6 Bytes A konsist...	0	0 1	256...267	256...261	12 Bytes ...		
	6 Bytes E/12 Bytes A konsist...	0	0 2	268...273	262...273	6 Bytes I/...		
		0	3					

9.2.3.2 Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU urządzenia nadrzędnego DP wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych. Można wykorzystać je do wykonywania przesyłu typu fail-safe *stałych* ilość danych typu fail-safe rodzaju BOOL lub INT (alternatywnie DINT).

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Możliwe jest również wywołanie instrukcji RCVDP i SENDDP w odrębnych F-FB/F-FC, które należy wywołać na początku lub na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.2.3.3 Programowanie komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne

Wymogi do programowania

Należy skonfigurować obszary adresowania do danych wejściowych i wyjściowych złącza DP/DP.

Procedura programowania

Komunikację urządzenie nadrzędne z bezpieczeństwem – urządzenie nadrzędne programuje się w następujący sposób:

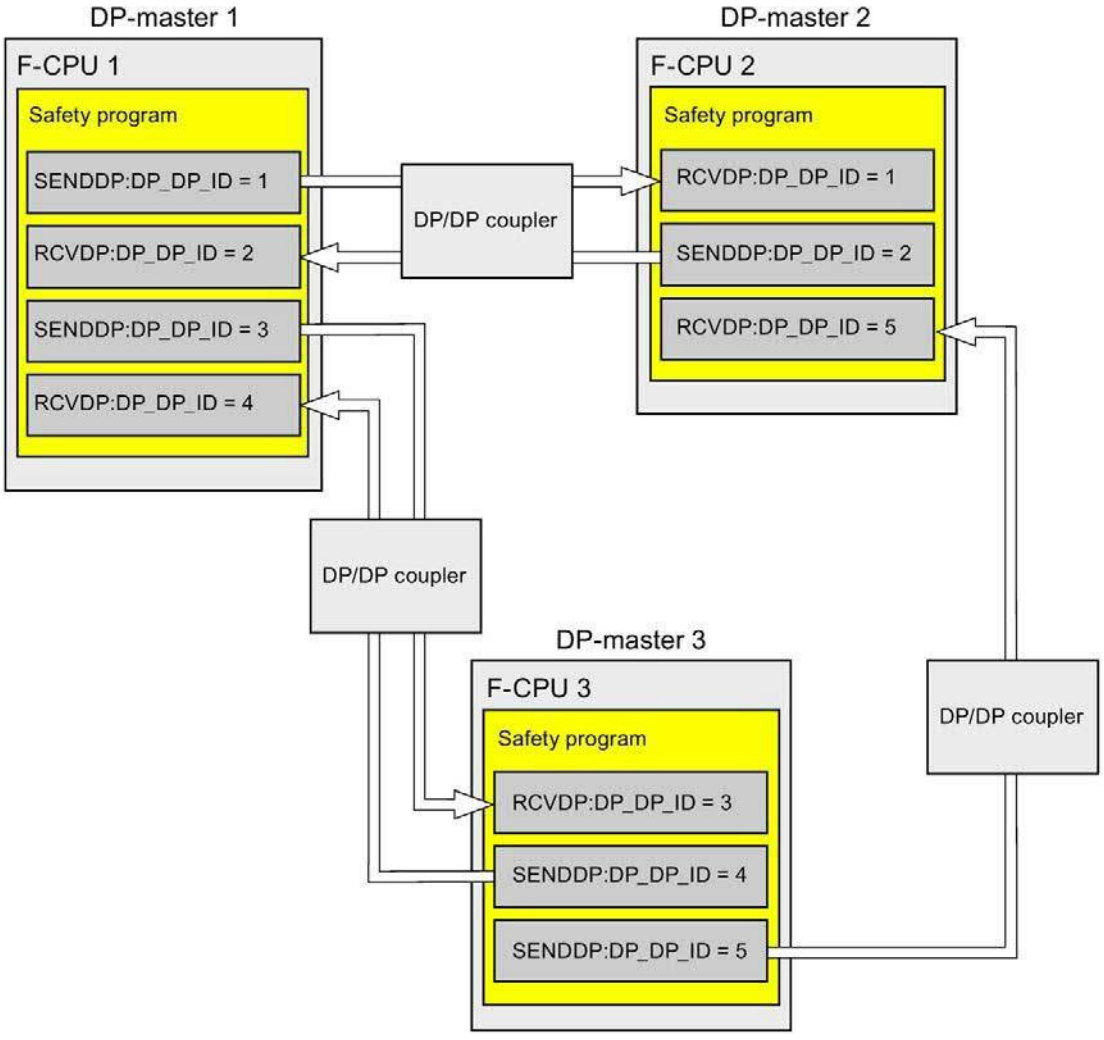
1. W programie bezpieczeństwa, z którego dane będą wysyłane, należy wywołać instrukcję SENDDP (strona 631) w celu wysłania na końcu głównego bloku bezpieczeństwa lub oddzielnego F-FC/F-FB.
2. W programie bezpieczeństwa, w którym dane będą odbierane, należy wywołać instrukcję RCVDP (strona 631) w celu odebrania na początku głównego bloku
3. bezpieczeństwa lub oddzielnego F-FC/F-FB.

   Należy przypisać identyfikatory HW danych wyjściowych i wejściowych złącza DP/DP skonfigurowanego w *edytorze sprzętu i sieci* (stałe w tabeli tagów) do odnośnych wejść LADDR.

   Należy wykonać to przypisanie dla każdego połączenia komunikacyjnego w każdym F-CPU.

4. Przypisać wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa do wejść DP_DP_ID. Pozwala to na ustalenie związku komunikacji pomiędzy instrukcją SENDDP w jednym F-CPU a instrukcją RCVDP w drugim F-CPU: Powiązane instrukcje otrzymują tę samą wartość dla DP_DP_ID.

   Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla 5 powiązań komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie**; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości*** do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** S7-1200/1500: Od wersji V3.0 instrukcji SENDDP i RCVDP, nie jest nawiązywane połączenie na wejściu DP_DP_ID do identyfikatora komunikacji bezpieczeństwa „0".

*** S7-1200/1500: Od wersji V3.0 instrukcji the SENDDP i RCVDP, na wejście DP_DP_ID można również doprowadzać wartości zmienne z globalnego F-DB. W takim przypadku również należy skontrolować podczas odbioru programu bezpieczeństwa, czy zapewniona jest unikalność *przez cały czas*, sprawdzając algorytm do tworzenia wartości zmiennych. Jeśli nie można zagwarantować unikalnego identyfikatora komunikacji bezpieczeństwa podczas uruchomienia programu bezpieczeństwa, ponieważ jest on określany dopiero po uruchomieniu programu, należy upewnić się, że podczas tej fazy wartość na wejściu DP_DP_ID wynosi „0".

5. Doprowadzić na wejścia SD_BO_xx i SD_I_xx (alternatywnie SD_DI_00) w SENDDP sygnały wysyłania. Aby ograniczyć sygnały pośrednie podczas przesyłania bloków transferowych, można zapisać wartość bezpośrednio do instancji DB w SENDDP, korzystając z w pełni kwalifikowanego dostępu (przykładowo, "Name SENDDP_1".SD_BO_02) przed wywołaniem SENDDP.
6. Należy doprowadzić na wyjścia RD_BO_xx i RD_I_xx (alternatywnie RD_DI_00) w RCVDP sygnały, które mają dalej być przetwarzane przez inne sekcje programu lub użyć w pełni kwalifikowanego dostępu, by odczytać otrzymane sygnały bezpośrednio z powiązanych instancji DB w sekcjach programu, które będą przetwarzane dalej (np. "Name RCVDP_1".RD_BO_02).
7. Aby wysłać dane na wejściu SD_DI_00 zamiast danych na wejściach SD_I_00 i SD_I_01, należy doprowadzić na wejście DINTMODE (wartość początkowa = „FAŁSZ") w SENDDP wartość „PRAWDA".
8. Należy zasilić wejścia SUBBO_xx i SUBI_xx, lub alternatywnie SUBDI_00, w RCVDP za pomocą wartości fail-safe wyprowadzanej przez RCVDP zamiast danych procesowych, aż zostanie ustanowiona komunikacja po raz pierwszy po uruchomieniu wysyłania i odbioru systemów bezpieczeństwa, lub w przypadku błędu komunikacji związanej z bezpieczeństwem.
   - Specyfikacja stałych wartości fail-safe:

     W przypadku danych rodzaju INT/DINT, można wprowadzić stałe wartości fail-safe bezpośrednio jako stałe w wejściu SUBI_xx lub alternatywnie SUBDI_00 (wartość początkowa = "0"). Aby określić stałą wartość fail-safe „PRAWDA" dla danych rodzaju BOOL, należy ustawić „PRAWDA" dla wejścia SUBBO_xx (wartość początkowa = „FAŁSZ").
   - Specyfikacja zmiennych wartości zastępczych:

     Aby określić zmienne wartości zastępcze, należy zdefiniować tag obliczany poprzez program bezpieczeństwa w F-DB, po czym określić go (w pełni kwalifikowany) w wejściu SUBBO_XX lub SUBI_xx, bądź alternatywnie SUBDI_00.

⚠ OSTRZEŻENIE

Uwaga: Logika programu do obliczania zmiennych wartości zastępczych może być wstawiona jedynie za wywołaniami RCVDP, ponieważ obszar przed nimi musi być wolny od operacji logicznych. Dlatego też, w pierwszym cyklu po uruchomieniu systemu bezpieczeństwa, we wszystkich instrukcjach RCVDP aktywne są wartości początkowe wartości zastępczych. Należy zatem przypisać do tych znaczników odpowiednie wartości początkowe. *(S017)*

9. Skonfigurować wejścia TIMEOUT instrukcji RCVDP i SENDDP, wprowadzając wymagany czas monitorowania.

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawce i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

10. Opcjonalnie: Istnieje możliwość oceny wyjścia ACK_REQ instrukcji RCVDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy zatwierdzenie jest wymagane.
11. Należy doprowadzić sygnał zatwierdzenia na wejście ACK_REI instrukcji RCVDP w celu przeprowadzenia reintegracji.
12. Opcjonalnie: Istnieje możliwość oceny wyjścia SUBS_ON instrukcji RCVDP lub SENDDP, by wykonać zapytanie, czy instrukcja RCVDP wyprowadza wartości fail-safe przypisane w wejściach SUBBO_xx i SUBI_xx lub alternatywnie SUBDI_00.
13. Opcjonalnie: Istnieje możliwość oceny wyjścia ERROR instrukcji RCVDP lub SENDDP, na przykład w standardowym programie użytkownika lub systemie HMI, by wykonać zapytanie lub wskazać, czy wystąpił błąd komunikacji.
14. Opcjonalnie: Istnieje możliwość oceny wyjścia SENDMODE instrukcji RCVDP, by wykonać zapytanie, czy F-CPU z powiązaną instrukcją SENDDP znajduje się w wyłączonym trybie bezpieczeństwa (strona 360).

9.2.3.4 Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne: ograniczenia transferu danych

Uwaga

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć drugiego (lub trzeciego) wywołania SENDDP / RCVDP. Wymaga to skonfigurowania dodatkowego połączenia poprzez złącze DP/DP. To, czy jest to możliwe z pojedynczym złączem DP/DP, zależy od ograniczeń przepustowości tego złącza.

9.2.4 Komunikacja sterownik IO safety – I-device

9.2.4.1 Konfiguracja komunikacji związanej z bezpieczeństwem pomiędzy sterownikiem IO a I-device

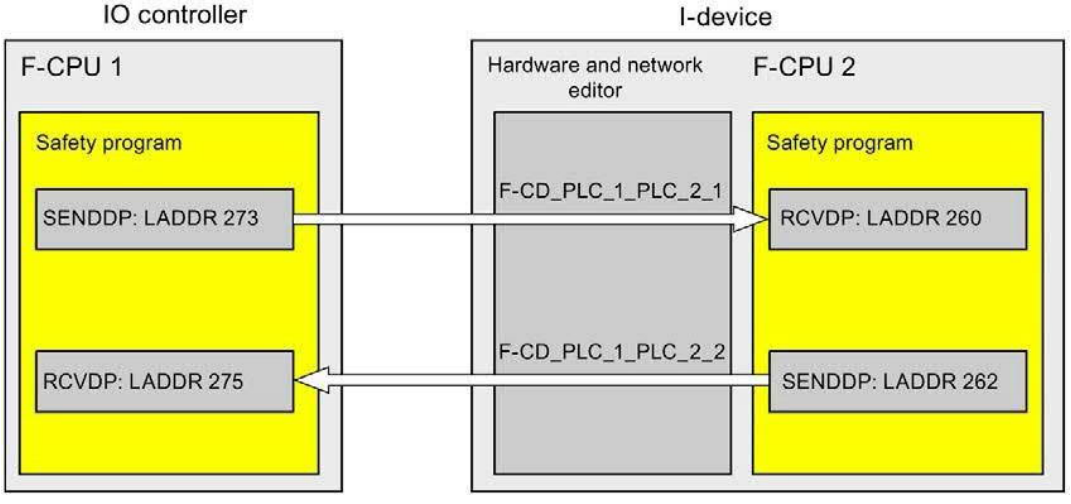
Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU sterownika IO a programem (programami) bezpieczeństwa F-CPU jednego lub kilku urządzeń I odbywa się poprzez połączenia sterownik IO – I-device (F-CD) w PROFINET IO, tak jak w standardowych systemach.

Do komunikacji sterownik IO – I-device nie jest potrzebny dodatkowy sprzęt.

Konfigurowanie obszarów transferu

Dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU należy skonfigurować obszary transferu w *edytorze sprzętu i sieci*. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać oraz odbierać dane (komunikacja dwukierunkowa).



Podczas tworzenia obszaru transferu przypisywana jest do niego etykieta, pozwalająca na zidentyfikowanie go jako związku komunikacyjnego. Przykładowo, „F-CD_PLC_2 PLC_1_1" dla pierwszego połączenia F-CD pomiędzy F-CPU 1 sterownika IO a F-CPU 2 I-device.

Podczas tworzenia obszaru transferu w F-CPU sterownika IO oraz w F-CPU I-device tworzona jest stała systemowa z nazwą obszaru transferu. Stała systemowa zawiera identyfikator sprzętowy obszaru transferu do odnośnego F-CPU.

Identyfikator sprzętowy (stałą systemową z tabeli tagów domyślnych) obszarów transferu przypisuje się symbolicznie do wejścia LADDR instrukcji SENDDP i RCVDP w programach bezpieczeństwa.

Procedura konfiguracji

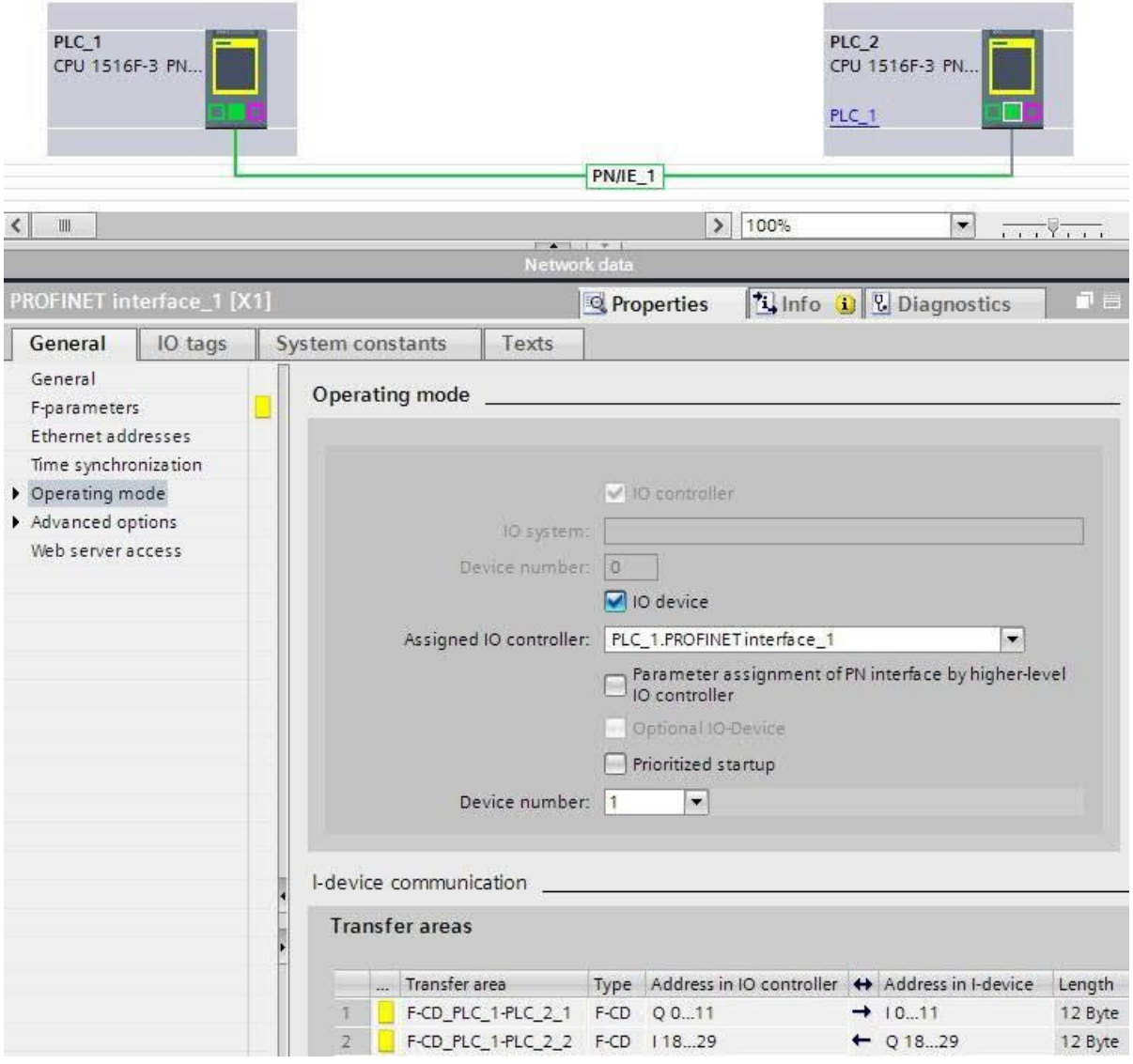
Procedura konfiguracji komunikacji sterownik IO safety – I-device przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Włączyć tryb „IO Device" dla F-CPU 2 we właściwościach jego interfejsu PN, po czym przypisać ten interfejs PN do interfejsu PN w F-CPU 1.
3. Wybrać interfejs PROFINET w F-CPU 2. Pod hasłem „Transfer areas" (Obszary transferu), tworzy się połączenie F-CD (typ „F-CD") do odbioru z urządzenia nadrzędnego IO (←). Połączenie F-CD jest przedstawione na żółto w tabeli, ponadto wyświetlane są obszary adresowe w I-device oraz sterowniku IO.

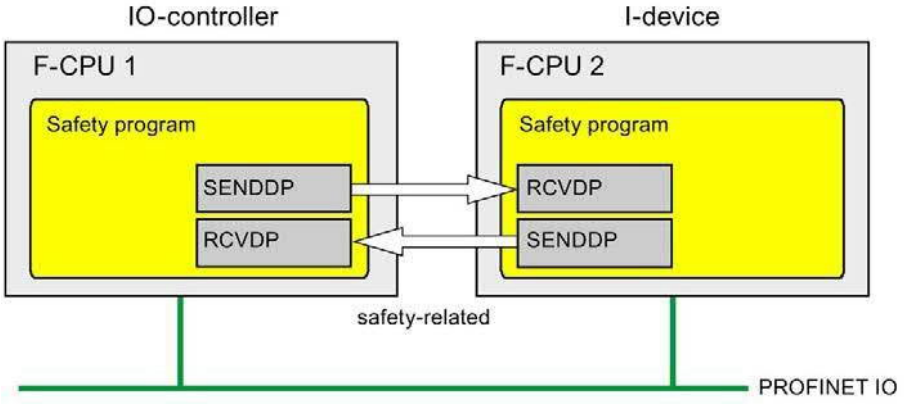
   Ponadto, dla każdego połączenia F-CD, automatycznie tworzone jest połączenie zatwierdzenia. (patrz „Szczegóły obszaru transferu").

4. Należy utworzyć dodatkowe połączenie F-CD do wysyłania do sterownika IO.
5. W nowo utworzonym obszarze transferu należy kliknąć na strzałkę, by zmienić kierunek przesyłu na wysyłanie do sterownika IO (←).



9.2.4.2 Komunikacja sterownik IO safety – I-device poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU sterownika IO oraz I-device wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych.
Można wykorzystać je do wykonywania przesyłu typu fail-safe *stałych* ilości danych typu rodzaju BOOL lub INT (alternatywnie DINT).

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Możliwe jest również wywołanie instrukcji RCVDP i SENDDP w odrębnych F-FB/F-FC, które należy wywołać na początku lub na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.2.4.3 Programowanie komunikacji sterownik IO safety – I-device

Wymogi do programowania

Obszar transferu musi być skonfigurowany.

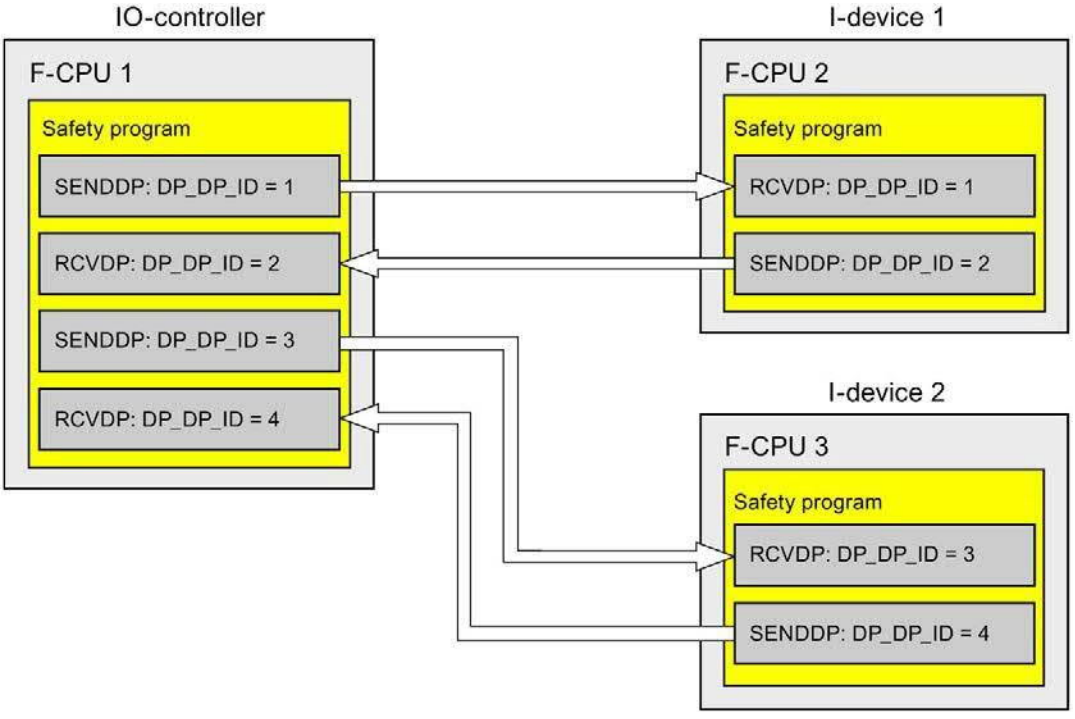
Procedura programowania

Procedura programowania komunikacji sterownik IO safety – I-device przebiega identycznie jak programowanie komunikacji sterownik IO safety – sterownik IO (patrz Komunikacja sterownik IO związany z bezpieczeństwem – sterownik IO (strona 281)).

Przypisanie identyfikatorów HW (stałe systemowe w standardowej tabeli tagów) obszarów transferu do wejścia LADDR instrukcji SENDDP/RCVDP można pozyskać z następującej tabeli.

Instrukcja	Identyfikator
SENDDP w sterowniku IO	Identyfikator sprzętowy obszaru transferu w sterowniku IO
RCVDP w sterowniku IO	Identyfikator sprzętowy obszaru transferu w sterowniku IO
SENDDP w I-device	Identyfikator sprzętowy obszaru transferu w I-device
RCVDP w I-device	Identyfikator sprzętowy obszaru transferu w I-device

Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla 4 powiązań komunikacji sterownik IO safety – I-device.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie**; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości*** do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** S7-1200/1500: Od wersji V3.0 instrukcji SENDDP i RCVDP, nie jest nawiązywane połączenie na wejściu DP_DP_ID do identyfikatora komunikacji bezpieczeństwa „0".

*** S7-1200/1500: Od wersji V3.0 instrukcji the SENDDP i RCVDP, na wejście DP_DP_ID można również doprowadzać wartości zmienne z globalnego F-DB. W takim przypadku również należy skontrolować podczas odbioru programu bezpieczeństwa, czy zapewniona jest unikalność *przez cały czas*, sprawdzając algorytm do tworzenia wartości zmiennych. Jeśli nie można zagwarantować unikalnego identyfikatora komunikacji bezpieczeństwa podczas uruchomienia programu bezpieczeństwa, ponieważ jest on określany dopiero po uruchomieniu programu, należy upewnić się, że podczas tej fazy wartość na wejściu DP_DP_ID wynosi „0".

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcy i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

9.2.4.4 Komunikacja sterownik IO safety – urządzenie IO – ograniczenia transferu danych

Ograniczenia transferu danych

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć dodatkowych instrukcji SENDDP/RCVDP. W tym celu należy skonfigurować dodatkowe obszary transferu. Należy pamiętać o maksymalnym limicie 1440 bajtów danych wejściowych lub 1440 bajtów danych wyjściowych dla transferu pomiędzy I-device a sterownikiem IO.

Poniższa tabela przedstawia ilości danych wyjściowych i wejściowych przypisanych w połączeniach komunikacji związanej z bezpieczeństwem:

Komunikacja safety	**Połączenie komunikacyjne**	**Przypisane dane wejściowe i wyjściowe**			
		W sterowniku IO		**W I-device**	
		Dane wyj.	**Dane wej.**	**Dane wyj.**	**Dane wej.**
Sterownik IO – I-device	**Wysyłanie:** I-device 1 do sterownika IO	6 bajtów	12 bajtów	12 bajtów	6 bajtów
	Odbiór: I-device 1 ze sterownika IO	12 bajtów	6 bajtów	6 bajtów	12 bajtów

Należy uwzględnić wszystkie dodatkowo skonfigurowane połączenia komunikacji standardowej oraz związanej z bezpieczeństwem (obszary transferu typu F-CD oraz CD) przy maksymalnym limicie 1440 bajtów danych wejściowych lub 1440 bajtów danych wyjściowych dla przesyłu pomiędzy I-device a sterownikiem IO. Ponadto, dane są przypisywane do celów wewnętrznych, wiec maksymalny limit może zostać osiągnięty wcześniej.

9.2.5 Komunikacja urządzenie nadrzędne safety – urządzenie I-slave

9.2.5.1 Konfiguracja komunikacji urządzenie nadrzędne safety – urządzenie I-slave

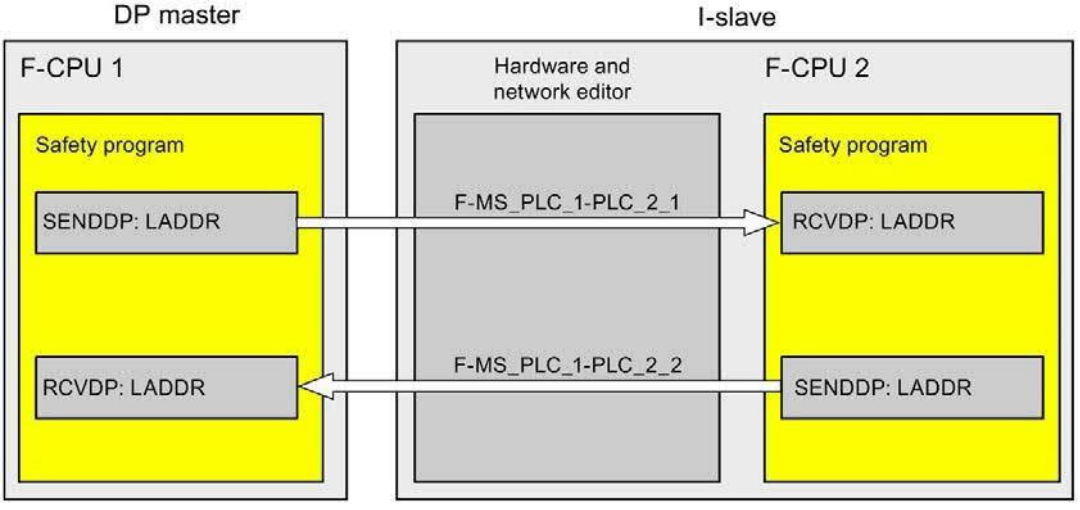
Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU urządzenia nadrzędnego DP a programem (programami) bezpieczeństwa F-CPU jednego lub kilku urządzeń I-slave odbywa się poprzez połączenia urządzenie nadrzędne – urządzenie I-slave (**F-**MS), tak jak w standardowych systemach.

Do takiej komunikacji nie jest potrzebne złącze DP/DP.

Konfigurowanie obszarów transferu

Dla każdej komunikacji związanej z bezpieczeństwem pomiędzy dwoma F-CPU należy skonfigurować obszary transferu w *edytorze sprzętu i sieci*. Poniższa ilustracja pokazuje, jak oba F-CPU mogą wysyłać oraz odbierać dane (komunikacja dwukierunkowa).



Podczas tworzenia obszaru transferu przypisywana jest do niego etykieta, pozwalająca na zidentyfikowanie go jako związku komunikacyjnego. Przykładowo, „F-MS_PLC_2 PLC_1_1" dla pierwszego połączenia F-MS pomiędzy F-CPU 1 urządzenia nadrzędnego DP a F-CPU 2 urządzenia I-slave.

Podczas tworzenia obszaru transferu w F-CPU urządzenia nadrzędnego DP oraz w F-CPU urządzenia I-slave tworzona jest stała systemowa z nazwą obszaru transferu. Stała systemowa zawiera identyfikator sprzętowy obszaru transferu do odnośnego F-CPU.

Identyfikator sprzętowy (stałą systemową z tabeli tagów domyślnych) obszarów transferu przypisuje się symbolicznie do wejścia LADDR instrukcji SENDDP i RCVDP w programach bezpieczeństwa.

Procedura konfiguracji

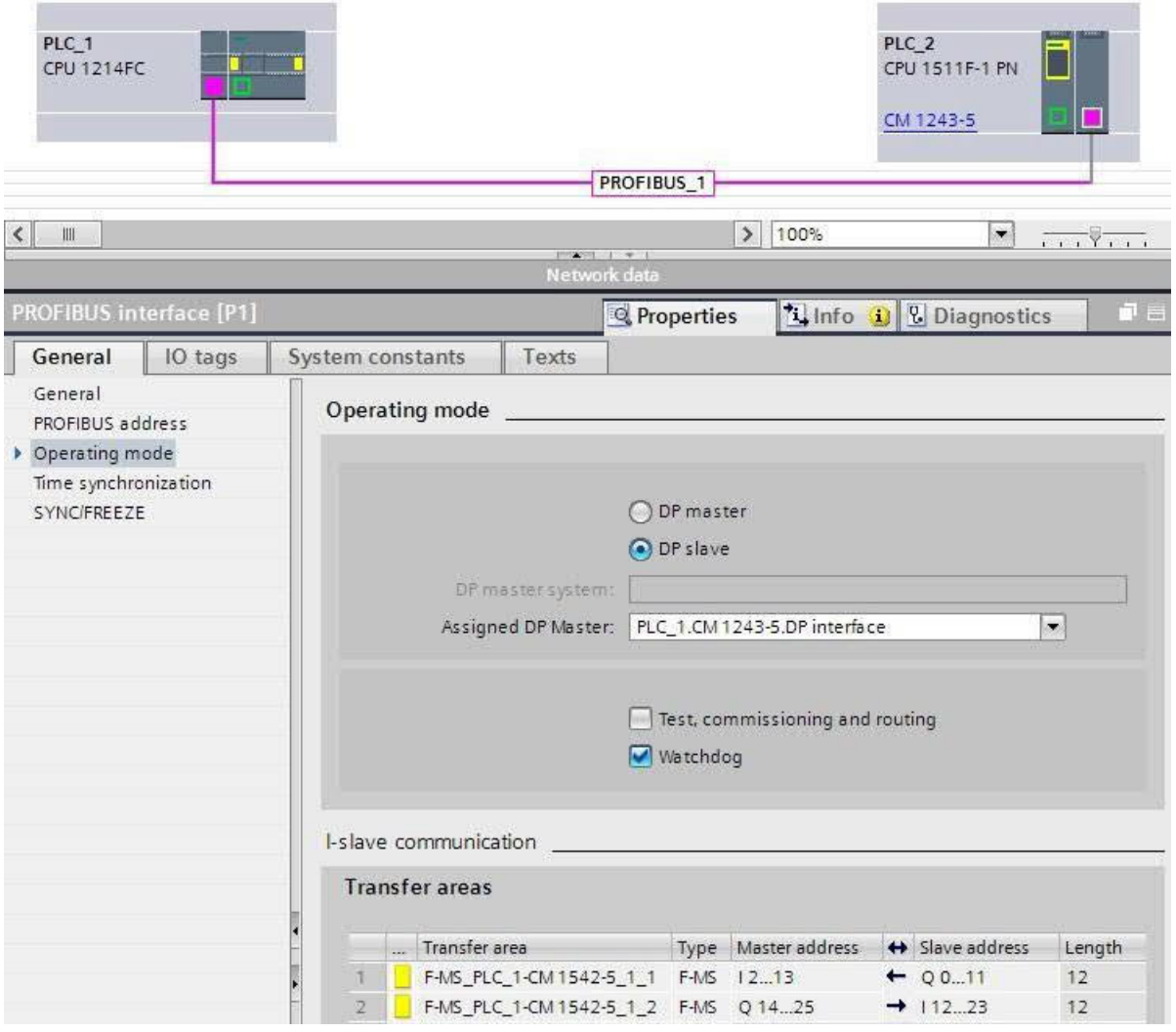
Procedura konfiguracji komunikacji urządzenie nadrzędne safety – urządzenie I-slave przebiega identycznie jak w standardowym programie.

Należy wykonać co następuje:

1. Wstawić dwa F-CPU z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu.
2. Jeśli F-CPU, który ma działać jako urządzenie nadrzędne DP (F-CPU 1), nie ma zintegrowanego inrerfejsu PROFIBUS, należy wstawić, przykładowo, PROFIBUS-CM.
3. Z widoku urządzenia F-CPU, które mają działać jako urządzenia I-slave (F-CPU 2), należy wstawić odpowiedni moduł CM DP lub moduł CP DP.
4. W razie potrzeby należy aktywować tryb „DP-slave" (I-slave) we właściwościach modułu CM/CP DP.
5. Przypisać interfejs DP CM/CP do interfejsu DP w F-CPU 1.
6. Wybrać interfejs PROFIBUS w F-CPU 2 lub w CM. Pod hasłem „Transfer areas" (Obszary transferu), tworzy się połączenie F-MS (typ „F-MS") do wysyłania do urządzenia nadrzędnego DP (←). Połączenie F-MS jest przedstawione na żółto w tabeli, ponadto wyświetlane są obszary adresowe w urządzeniu I-slave oraz urządzeniu nadrzędnym DP.

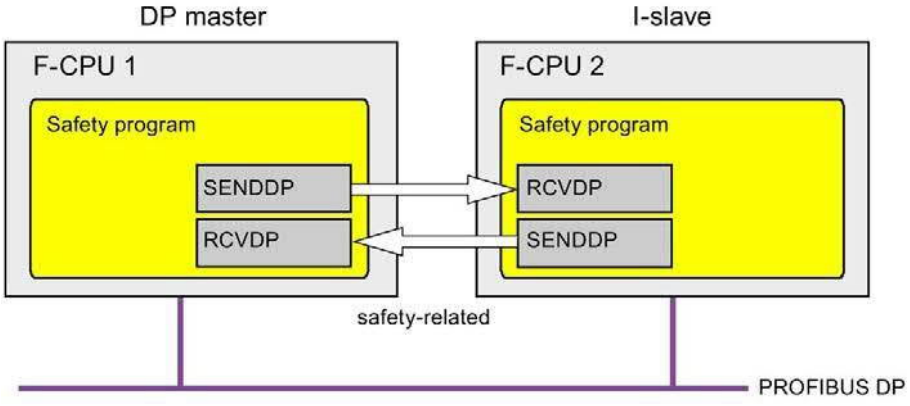
   Ponadto, dla każdego połączenia F-MS, automatycznie tworzone jest połączenie zatwierdzenia. (patrz „Szczegóły obszaru transferu").

7. Należy utworzyć dodatkowe połączenie F-MS do odbioru z urządzenia nadrzędnego DP.
8. W nowo utworzonym obszarze transferu należy kliknąć na strzałkę, by zmienić kierunek przesyłu na odbiór z urządzenia nadrzędnego DP (→).



9.2.5.2 Komunikacja urządzenie nadrzędne I safety – I-device poprzez SENDDP i RCVDP

Komunikacja poprzez instrukcje SENDDP i RCVDP



Komunikacja safety pomiędzy F-CPU urządzenia nadrzędnego DP oraz urządzenia I-slave wykorzystuje instrukcje SENDDP i RCVDP do kolejno wysyłania i odbierania danych. Można wykorzystać je do wykonywania przesyłu typu fail- safe *stałych* ilość danych typu fail-safe rodzaju BOOL lub INT (alternatywnie DINT).

Instrukcje te można znaleźć w karcie zadań „Instructions" (Instrukcje) pod hasłem „Communication" (Komunikacja). Instrukcja RCVDP **musi** zostać wywołana na początku głównego bloku bezpieczeństwa. Instrukcja SENDDP **musi** zostać wywołana na końcu głównego bloku bezpieczeństwa.

Możliwe jest również wywołanie instrukcji RCVDP i SENDDP w odrębnych F-FB/F-FC, które należy wywołać na początku lub na końcu głównego bloku bezpieczeństwa.

Należy pamiętać, że sygnały wysłane nie są wysyłane aż do wywołania instrukcji SENDDP na końcu wykonywania odnośnej grupy F-runtime.

Szczegółowy opis instrukcji SENDDP i RCVDP można znaleźć w dziale SENDDP oraz RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16) (strona 631).

9.2.5.3 Programowanie komunikacji urządzenie nadrzędne safety – urządzenie I-slave

Wymogi

Obszar transferu musi być skonfigurowany.

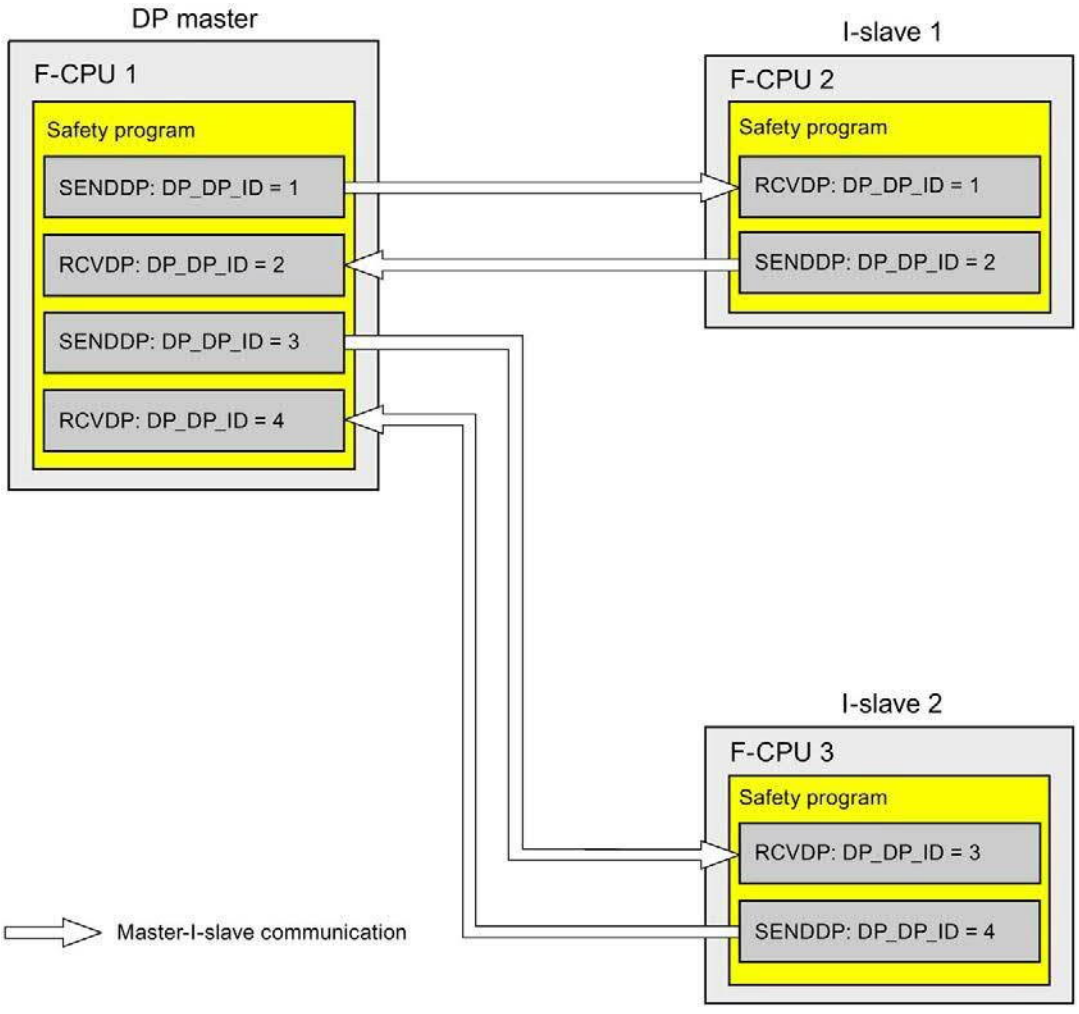
Procedura programowania

Procedura programowania komunikacji urządzenie nadrzędne safety – urządzenie I-slave przebiega identycznie jak programowanie komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne (patrz Programowanie komunikacji urządzenie nadrzędne safety – urządzenie nadrzędne (strona 285)).

Przypisanie identyfikatorów sprzętowych obszarów transferu do wejścia LADDR instrukcji SENDDP/RCVDP można pozyskać z następującej tabeli.

Instrukcja	Identyfikator
SENDDP w urządzeniu nadrzędnym DP	Identyfikator sprzętowy odnośnego obszaru transferu w urządzeniu nadrzędnym DP
RCVDP w urządzeniu nadrzędnym DP	Identyfikator sprzętowy odnośnego obszaru transferu w urządzeniu nadrzędnym DP
SENDDP w urządzeniu I-slave	Identyfikator sprzętowy obszaru transferu w urządzeniu I-slave
RCVDP w urządzeniu I-slave	Identyfikator sprzętowy obszaru transferu w urządzeniu I-slave

Poniższa ilustracja zawiera przykład sposobu określania identyfikatorów komunikacji bezpieczeństwa na wejściach instrukcji SENDDP i RCVDP dla czterech powiązań komunikacji urządzenie nadrzędne safety – urządzenie I-slave.



OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie**; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości*** do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** S7-1200/1500: Od wersji V3.0 instrukcji SENDDP i RCVDP, nie jest nawiązywane połączenie na wejściu DP_DP_ID do identyfikatora komunikacji bezpieczeństwa „0".

*** S7-1200/1500: Od wersji V3.0 instrukcji the SENDDP i RCVDP, na wejście DP_DP_ID można również doprowadzać wartości zmienne z globalnego F-DB. W takim przypadku również należy skontrolować podczas odbioru programu bezpieczeństwa, czy zapewniona jest unikalność *przez cały czas*, sprawdzając algorytm do tworzenia wartości zmiennych. Jeśli nie można zagwarantować unikalnego identyfikatora komunikacji bezpieczeństwa podczas uruchomienia programu bezpieczeństwa, ponieważ jest on określany dopiero po uruchomieniu programu, należy upewnić się, że podczas tej fazy wartość na wejściu DP_DP_ID wynosi „0".

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawce i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Informacje dotyczące obliczania czasów monitorowania można znaleźć w dziale „Czasy monitorowania i odpowiedzi" (strona 649).

9.2.5.4 Ograniczenia transferu danych komunikacji urządzenie nadrzędne I safety – urządzenie I-slave

Ograniczenia transferu danych

Jeśli ilość danych do przesyłu przekracza przepustowość powiązanych instrukcji SENDDP / RCVDP, można użyć dodatkowych instrukcji SENDDP/RCVDP. W tym celu należy skonfigurować dodatkowe obszary transferu. Należy pamiętać o maksymalnym limicie 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych dla transferu pomiędzy urządzeniem I-slave a urządzeniem nadrzędnym DP.

Poniższa tabela przedstawia ilości danych wyjściowych i wejściowych przypisanych w połączeniach komunikacji związanej z bezpieczeństwem:

Komunikacja safety	**Połączenie komunikacyjne**	**Przypisane dane wejściowe i wyjściowe**			
		Urządzenie nadrzędne DP		**Urządzenie I-slave**	
		Dane wyj.	**Dane wej.**	**Dane wyj.**	**Dane wej.**
Urządzenie nadrzędne – urządzenie I-slave	**Wysyłanie:** Urz. I-slave 1 do urz.nadrzędnego DP	6 bajtów	12 bajtów	12 bajtów	6 bajtów
	Odbiór: Urz. I-slave 1 z urz. nadrzędnego DP	12 bajtów	6 bajtów	6 bajtów	12 bajtów

Należy uwzględnić wszystkie dodatkowo skonfigurowane połączenia komunikacji standardowej oraz związanej z bezpieczeństwem (obszary transferu typu F-MS-, F-DX-, F-DX-Mod., MS-, DX- oraz DX-Mod) przy maksymalnym limicie 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych dla przesyłu pomiędzy I-device a urządzeniem nadrzędnym DP F-MS i MS). Jeśli maksymalny limit 244 bajtów danych wejściowych lub 244 bajtów danych wyjściowych zostanie przekroczony, wyświetli się następujący komunikat o błędzie.

9.2.6 Komunikacja sterownik IO safety – urządzenie I-slave

9.2.6.1 Komunikacja sterownik IO safety – urządzenie I-slave

Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU sterownika IO a programem (programami) bezpieczeństwa F-CPU jednego lub kilku urządzeń I-slave odbywa się poprzez połączenia urządzenie kontroler – urządzenie I-slave (**F-**MS), tak jak w standardowych systemach.

Połączenie

W przypadku komunikacji sterownik IO safety – urządzenie I-slave, połączenie IE/PB jest niezbędne. Oba F-CPU są podłączone do połączenia IE/PB za pomocą interfejsu PROFIBUS DP lub PROFINET.

Uwaga

W przypadku korzystania z połączenia IE/PB, należy uwzględnić to podczas konfigurowania czasów monitorowania i odpowiedzi bezpieczeństwa oraz podczas obliczania maksymalnego czasu odpowiedzi systemu bezpieczeństwa (zobacz również „Czasy monitorowania i odpowiedzi" (strona 649)).

Należy pamiętać, że arkusz kalkulacyjny do obliczania czasów odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100) dla F-CPU S7-300/400 nie obsługuje wszystkich możliwych konfiguracji.

Odniesienia

Informacje dotyczące komunikacji urządzenie nadrzędne safety – urządzenie I-slave zamieszczone w dziale Komunikacja urządzenie nadrzędne – urządzenie I-slave (strona 302) również mają zastosowanie.

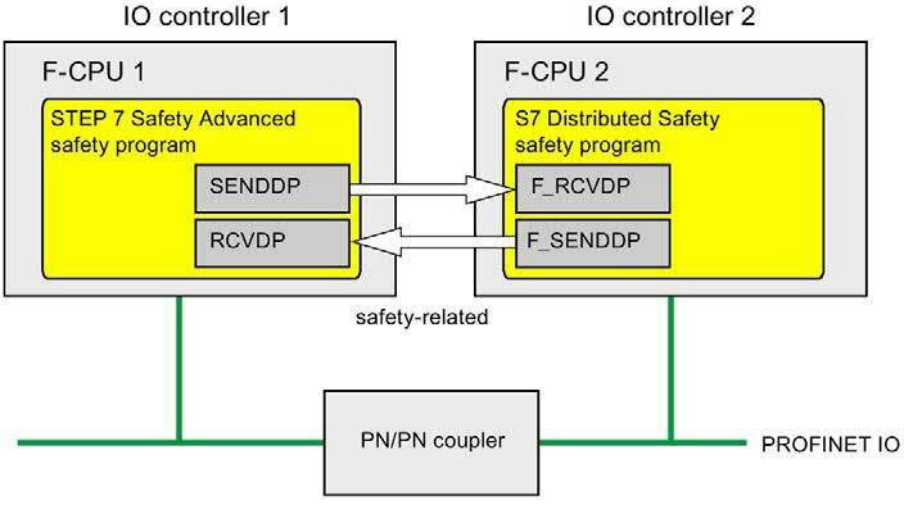
9.2.7 Komunikacja safety do systemu bezpieczeństwa S7 Distributed Safety

9.2.7.1 Wstęp

Komunikacja safety z F-CPU w SIMATIC Safety do F-CPU w systemach bezpieczeństwa S7 Distributed Safety jest możliwa poprzez złącze PN/PN lub złącze DP/DP wykorzystywane pomiędzy dwoma F-CPU jako komunikacja sterownik IO – sterownik IO lub komunikacja urządzenie nadrzędne – urządzenie nadrzędne.

9.2.7.2 Komunikacja z S7 Distributed Safety za pomocą połączenia PN/PN (komunikacja sterownik IO – sterownik IO)

Funkcje komunikacyjne pomiędzy instrukcjami SENDDP/RCVDP na końcu *STEP 7 Safety* oraz bloki aplikacji bezpieczeństwa F_SENDDP/F_RCVDP na końcu *S7 Distributed Safety*:



Procedura na końcu *S7 Distributed Safety*

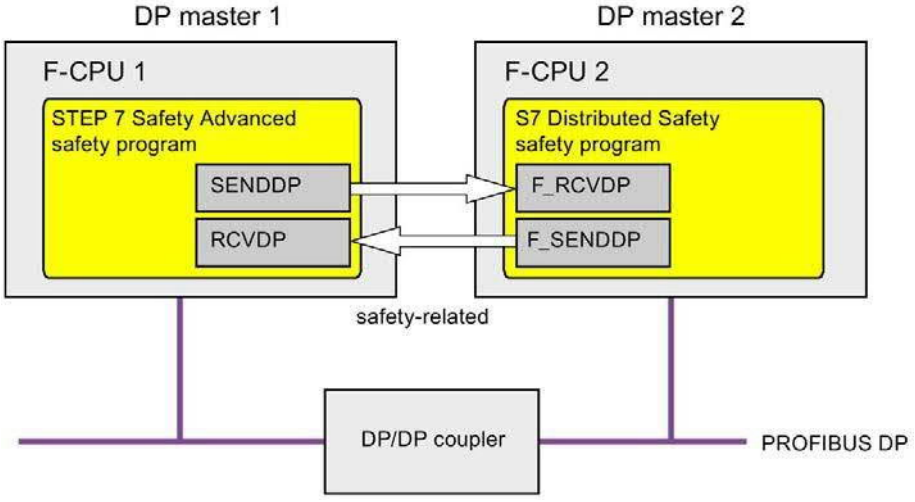
Na końcu *S7 Distributed Safety* należy postępować zgodnie z opisem w dziale „Komunikacja sterownik IO safety – sterownik IO" w podręczniku S7 Distributed Safety - Konfiguracja i programowanie (http://support.automation.siemens.com/WW/view/en/22099875).

Procedura na końcu *STEP 7 Safety*

Na końcu *STEP 7 Safety*, należy postępować zgodnie z opisem w Komunikacja sterownik IO safety – sterownik IO (strona 276).

9.2.7.3 Komunikacja z S7 Distributed Safety za pomocą połączenia DP/DP (komunikacja jednostka nadrzędna – jednostkanadrzędna)

Funkcje komunikacyjne pomiędzy instrukcjami SENDDP/RCVDP na końcu *STEP 7 Safety* oraz bloki aplikacji bezpieczeństwa F_SENDDP/F_RCVDP na końcu *S7 Distributed Safety*:



Procedura na końcu *S7 Distributed Safety*

Na końcu *S7 Distributed Safety* należy postępować zgodnie z opisem w dziale „Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne" w podręczniku S7 Distributed Safety - Konfiguracja i programowanie (http://support.automation.siemens.com/WW/view/en/22099875).

Procedura na końcu *STEP 7 Safety*

Na końcu *STEP 7 Safety*, należy postępować zgodnie z opisem w Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne (strona 285).

9.3 Konfiguracja i programowanie komunikacji z użyciem Flexible F-Link (S7-1200, S7-1500)

9.3.1 Flexible F-Link

Wstęp

W *STEP 7 Safety V15.1* dostępna jest nowa komunikacja CPU fail-safe – CPU, „Flexible F-Link" do F-CPU S7-1200 i S7-1500. Oznacza to, że dane typu fail-safe można łatwo wymieniać w postaci tablic fail-safe z wykorzystaniem standardowych mechanizmów komunikacji.

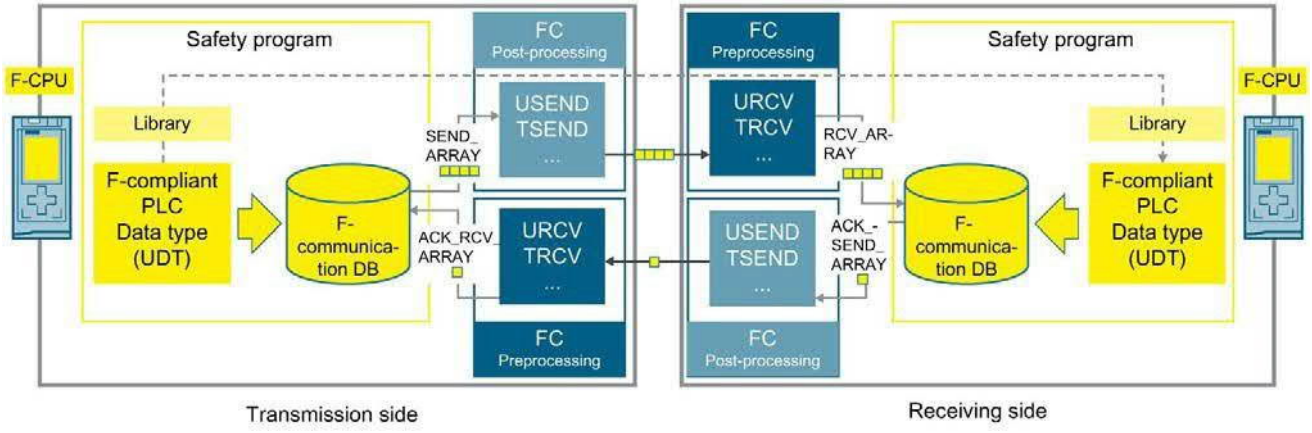
Flexible F-Link zapewnia szereg korzyści przy wymianie danych typu fail-safe:

- Gromadzenie danych typu fail-safe przekazywanych w rodzaju danych PLC zgodnych z bezpieczeństwem (UDT)
- Do 100 bajtów danych na obsługę UDT rodzaju danych fail-safe
- Łatwe przypisanie parametrów i automatyczne generowanie DB komunikacji typu fail-safe
- Transmisja danych typu fail-safe ze standardowymi blokami komunikacyjnymi również przez ograniczenia sieci
- Komunikacja grupy F-runtime (strona 98) do F-CPU S-1200/1500
- Zintegrowana z systemem oraz globalnie wystarczająco unikalna komunikacja bezpieczeństwa UUID
- Odrębne podpisy adresów komunikacji bezpieczeństwa dla łatwego wykrywania zmian w UUID komunikacji

Wymogi

- F-CPU S7-1500 z oprogramowaniem V2.0
- F-CPU S7-1200 z oprogramowaniem V4.2
- Od systemu bezpieczeństwa w wersji V2.2

Zasady komunikacji poprzez Flexible F-Link



Poniższe czynności należy wykonać **po stronie nadawcy**:

1. Utworzyć rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) dla danych do wysłania. Rozmiar może wynosić do 100 bajtów.
2. Utworzyć komunikację bezpieczeństwa z kierunkiem „Sending" (Wysyłanie) w Safety Administration Editor. Nowo utworzony DB komunikacji bezpieczeństwa dla tej komunikacji znajduje się pod ścieżką „Program blocks¥System blocks¥STEP 7 Safety¥F-communication DBs".
3. Ustawić czas monitorowania bezpieczeństwa (strona 655) dla komunikacji bezpieczeństwa.
4. W programie bezpieczeństwa należy połączyć tag danych wysyłanych (SEND_DATA) na DB komunikacji bezpieczeństwa (strona 98).
5. Aby przesłać zakodowane tablice fail-safe, należy utworzyć odpowiednie bloki komunikacyjne do wysyłania i odbierania (zatwierdzania) w standardowym programie. Aby przetwarzać wartości procesowe we właściwej kolejności chronologicznej, można użyć F-OB Przetwarzanie wstępne/końcowe (strona 86). Podczas korzystania ze standardowych bloków komunikacyjnych należy pamiętać, że tablice fail-safe są dostępne w sposób stały w czasie oceny oraz że przestrzegany jest czas monitorowania bezpieczeństwa (strona 655). Należy zwrócić uwagę na poniższą adnotację.

Poniższe czynności należy wykonać **po stronie odbiorcy**:

1. Utworzyć rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) o strukturze identycznej jak po stronie nadawcy.
2. W tym celu należy skopiować rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) ze strony nadawcy lub użyć biblioteki projektu bądź biblioteki globalnej.

   Utworzyć komunikację bezpieczeństwa z kierunkiem „Receiving" (Odbieranie) w Safety Administration Editor.

   Nowo utworzony DB komunikacji bezpieczeństwa dla tej komunikacji znajduje się pod ścieżką „Program blocks¥System blocks¥STEP 7 Safety¥F-communication DBs".
3. Skopiować UUID komunikacji bezpieczeństwa ze strony nadawcy.
4. Ustawić taki sam czas monitorowania bezpieczeństwa jak po stronie nadawcy.
5. W programie bezpieczeństwa należy połączyć tagi danych odbieranych (RCV_DATA) na DB komunikacji bezpieczeństwa (strona 98).
6. Aby przesłać zakodowane tablice fail-safe, należy utworzyć odpowiednie bloki komunikacyjne do wysyłania i odbierania (zatwierdzania) w standardowym programie. Aby przetwarzać wartości procesowe

we właściwej kolejności chronologicznej, można użyć F-OB Przetwarzanie wstępne/końcowe (strona 98). Podczas korzystania ze standardowych bloków komunikacyjnych należy pamiętać, że tablice fail-safe są dostępne w sposób stały w czasie oceny oraz że przestrzegany jest czas monitorowania bezpieczeństwa (strona 655). Należy zwrócić uwagę na poniższą adnotację.

7. W programie bezpieczeństwa należy połączyć tagi danych odbieranych (RCV_DATA) na DB komunikacji bezpieczeństwa (strona 98).

Uwaga

Podczas korzystania z niejednoznacznych protokołów komunikacji (np. TCP/IP), należy uwzględnić następujące zagadnienia:

- Zwiększone obciążenie komunikacji może istotnie pogorszyć dostępność aplikacji (czas działania czasu monitorowania bezpieczeństwa połączeń komunikacyjnych). Ma to szczególnie zastosowanie, gdy komunikacja OPC UA oraz Secure Open User Communication (OUC) są stosowane równolegle.
- Bufor komunikacyjny przepełnia się i może poważnie wpłynąć na dostępność aplikacji, czego należy unikać.

  Więcej przydatnych informacji można znaleźć poniższym przykładzie aplikacji: „Konfigurowanie komunikacji Flexible F-Link (https://support.industry.siemens.com/cs/ww/en/view/109768964)".

Uwaga

Podczas wykonywania symulacji przy pomocy *PLCSIM*, zegar generujący komunikat o błędzie po przekroczeniu czasu, gdy komunikacja z rzeczywistymi I/O zostanie zakłócona (np. przez ustawienie CPU w tryb STOP), nie jest wyzwalany. Dlatego w tym przypadku nie został wyświetlony komunikat o błędzie. Jest on wyświetlany niezwłocznie po przywróceniu połączenia. Po zatwierdzeniu użytkownika bieżące wartości są ponownie wysyłane i odbierane.

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawce i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania.
(S018)

OSTRZEŻENIE

W przypadku komunikacja CPU związany z bezpieczeństwem – CPU rodzaju Flexible F-Link należy uwzględnić następujące zagadnienia: Jeśli dane są wysyłane z F-CPU symulowanego za pomocą S7-PLCSIM, nie można zakładać, że dane są generowane w bezpieczny sposób. Należy następnie wdrożyć środki organizacyjne, takie jak monitorowanie pracy oraz ręczne wyłączenie bezpieczeństwa, by zapewnić bezpieczeństw w tych częściach systemu, na które wpływają wysyłane dane. Alternatywnie można wyprowadzić wartości zastępcze fail-safe zamiast odebranych danych w F-CPU, który otrzymuje dane, poprzez wykonanie oceny SENDMODE*.

* SENDMODE jest dostępny jako znacznik w DB komunikacji bezpieczeństwa.

(S086)

OSTRZEŻENIE

Gdy w Safety Administration Editor tworzona jest nowa komunikacja Flexible F-Link, unikalny UUID komunikacji bezpieczeństwa jest zapewniany przez system. Poprzez skopiowanie komunikacji w Safety Administration Editor w obrębie tabeli parametryzacji lub podczas kopiowania do innego F-CPU, UUID komunikacji bezpieczeństwa nie są ponownie generowane, przez co tracą swoją unikalność. Jeśli do konfigurowania nowego związku komunikacji wykorzystywana jest kopia, należy samodzielnie zapewnić unikalność. W tym celu należy wybrać dane UUID i wygenerować je ponownie poprzez menu kontekstowe „Generate UUID" (Wygeneruj UUID). Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas zatwierdzenia. *(S087)*

OSTRZEŻENIE

Podczas akceptacji należy skorzystać z podsumowania bezpieczeństwa, by sprawdzić, czy przesunięcia wszystkich elementów rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) są zgodne z wysyłanymi i odbieranymi danymi w ramce wiadomości bezpieczeństwa. Z tego względu wszystkie elementy i adresy są wyszczególnione w podsumowaniu bezpieczeństwa dla UDT. *(S088)*

Zobacz także

Komunikacja grupy F-runtime (S7-1200, S7-1500) (strona 154)

9.3.2 Interfejsy DB komunikacji bezpieczeństwa (S7-1200, S7-1500)

Interfejs DB komunikacji bezpieczeństwa do wysyłania

Poniższa tabela przedstawia interfejs bloku danych komunikacji bezpieczeństwa służącego do połączenia komunikacji z kierunkiem „wysyłanie":

Dział	Nazwa	Rodzaj danych	Wartość początkowa	Opis
Wejście	SEND_DATA	Rodzaj danych PLC zgodnych z bezpieczeństwem (UDT)	Jak w rodzaju danych PLC zgodnych z bezpieczeństwem	Dane użytkownika do wysłania:
	ACK_RCV_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	tablica z otrzymanymi nieprzetworzonymi danymi.
Wyjście	ERROR	BOOL	FALSE	Sygnalizuje aktywne błędy komunikacji lub błędy niezatwierdzone po stronie odbiorcy (nie w stanie początkowym). 1=Błąd komunikacji
	ACTIVATE_FV	BOOL	TRUE	Komunikacja pasywowana, w stanie początkowym (przykładowo, odbiornik nie jest aktywny), lub HOST wysyła ACTIVATE_FV. DEVICE wysyła bit stanu: FV_ACTVATED, lecz bez wartości zerowych. 1=Komunikacja wykorzystuje wartości fail-safe
	DIAG	Bajt	16#0	Bity błędu (przekroczenie czasu lub błąd CRC aktywne, bądź błąd komunikacji nie został depasywowany) Bit 3: Polecenie zatwierdzenia aktywne po stronie odbiorcy Bit 4: Wykryto przekroczenie czasu Bit 6: Wykryto błąd CRC
	SEND_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	Tablica z otrzymanymi nieprzetworzonymi danymi
	ACK_RCV_LENGTH	UInt	0	Informacja o długości dla ACK_RCV_ARRAY w bajtach
	SEND_LENGTH	UInt	0	Informacja o długości dla SEND_ARRAY w bajtach
InOut	—	—	—	—
Statyczny	—	—	—	—

Interfejs DB komunikacji bezpieczeństwa do odbierania

Poniższa tabela przedstawia interfejs bloku danych komunikacji bezpieczeństwa służącego do połączenia komunikacji z kierunkiem „odbieranie":

Dział	Nazwa	Rodzaj danych	Wartość początkowa	Opis
Wejście	PASS_ON	BOOL	FALSE	Pozwalana pasywację danych wyjściowych (wyjście wartości pasywowania) 1=Aktywuj pasywację
	ACK_REI	BOOL	FALSE	Reintegracja (w przypadku żądania reintegracji) za pomocą zbocza dodatniego 1=Zatwierdzenie reintegracji
	RCV_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	Tablica z otrzymanymi nieprzetworzonymi danymi
Wyjście	RCV_DATA	Rodzaj danych PLC zgodnych z bezpieczeństwem	Jak w rodzaju danych PLC zgodnych z bezpieczeństwem	Dane wyjściowe (PASS_VALUES lub otrzymane dane).
	ERROR	BOOL	FALSE	Sygnalizuje aktywne błędy komunikacji lub błędy niezatwierdzone (nie w stanie początkowym). 1=Błąd komunikacji
	PASS_OUT	BOOL	TRUE	Przy PASS_OUT=1, PASS_VALUES stanowią wyjście. Może przyjąć: ERROR, PASS_ON, przy początkowym uruchomieniu (np. nadawca nie jest uruchomiony) lub ACK_REQ oczekuje (błąd nie został zatwierdzony)
	ACK_REQ	BOOL	FALSE	Wymóg reintegracji (komunikacja stabilna po błędzie, wciąż wyprowadzane są wartości zastępcze) 1=Wymóg zatwierdzenia do reintegracji
	SENDMODE	BOOL	FALSE	MOD_MODE jest aktywny lub komunikacja z PLCSIM Advanced na nadawczym F-CPU 1=F-CPU z nadawcą w wyłączonej bezpiecznej pracy lub przy symulowanym CPU

Dział	Nazwa	Rodzaj danych	Wartość początkowa	Opis
	DIAG	Bajt	16#0	Bity błędów (przekroczenie czasu lub błąd CRC) Bit 0: Wykryto przekroczenie czasu po stronie nadawcy Bit 1: Błąd komunikacji aktywny po stronie nadawcy Bit 2: Wykryto błąd CRC po stronie nadawcy Bit 4: Wykryto przekroczenie czasu po stronie odbiorcy Bit 6: Wykryto błąd CRC po stronie odbiorcy
	ACK_SEND_ARRAY	Array [0..n] bajtów	Każdy element z 16#0	Tablica danych nieprzetworzonych do wysłania.
	RCV_LENGTH	UInt	0	Informacja o długości dla RCV_ARRAY w bajtach
	ACK_SEND_LENGTH	UInt	0	Informacja o długości dla ACK_SEND_ARRAY w bajtach
InOut	—	—	—	—
Statyczny	PASS_VALUES	Rodzaj danych PLC zgodnych z bezpieczeństwem (UDT)	Tak jako jak w rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) lub w DB I/O	Pasywacja lub wartości zastępcze

9.4 Konfiguracja i programowanie komunikacji pomiędzy F-CPU S7- 300/400 i S7-1200/1500

9.4.1 Przegląd komunikacji

Wstęp

W tym dziale dostępny jest przegląd opcji komunikacji związanej z bezpieczeństwem pomiędzy F-CPU S7-300/400 a S7-1200/1500 w systemach bezpieczeństwa SIMATIC Safety.

Opcje komunikacji związanej z bezpieczeństwem

Komunikacja safety	Na podsieci	Wymagany dodatkowy sprzęt
Komunikacja CPU safety – CPU:		
Kom. urz.nadrzędne – urz. nadrzędne	PROFIBUS DP	złącze DP/DP
Kom. urz nadrzędne – urz.I-slave	PROFIBUS DP	—
Komunikacja sterownik IO – sterownik IO	PROFINET IO	złącze PN/PN
Komunikacja sterownik IO – I-device	PROFINET IO	—
Komunikacja sterownik IO – urz. I-slave	PROFINET IO i PROFIBUS DP	Połączenie IE/PB

Podstawowa procedura konfiguracji i programowania

Konfiguracja i programowanie komunikacji związanej z bezpieczeństwem pomiędzy F-CPU S7-300/400 a F-CPU S7-1200/1500 powinna przebiegać zgodnie z opisem w „Konfiguracja i programowanie komunikacji (S7-300, S7-400)" (strona 209) oraz „Konfiguracja i programowanie komunikacji (S7-1200, S7-1500)" (strona 273) dla danej aplikacji.

Aby zaprogramować F-CPU S7-300/400, należy użyć adresu początkowego obszarów transferu. Aby zaprogramować F-CPU S7-1200/1500, należy użyć identyfikatorów sprzętowych obszarów transferu.

9.5 Konfigurowanie i programowanie komunikacji w kilku projektach

9.5.1 Komunikacja sterownik IO safety – I-device w kilku projektach

9.5.1.1 Konfiguracja komunikacji związanej z bezpieczeństwem pomiędzy sterownikiem IO a I-device

Wstęp

Komunikacja safety pomiędzy programem bezpieczeństwa F-CPU sterownika IO a programem (programami) bezpieczeństwa F-CPU jednego lub kilku urządzeń I odbywa się poprzez połączenia sterownik IO – I-device (F-CD) w PROFINET IO, tak jak w standardowych systemach.

Poniższy dział opisuje szczególne aspekty, gdy sterownik IO i urządzenie I-slave znajdują się w różnych projektach.

Wymogi

- Sterownik IO to F-CPU S7-1200/1500, który obsługuje funkcjonalność sterownika IO.
- I-device to F-CPU S7-300/400/1200/1500, który obsługuje funkcjonalność I-device.
- Projekt, w którym znajduje się I-device, musi być utworzony przy pomocy *S7 Distributed Safety V5.4*, *STEP 7 Safety V13* lub nowszym.

Konfiguracja

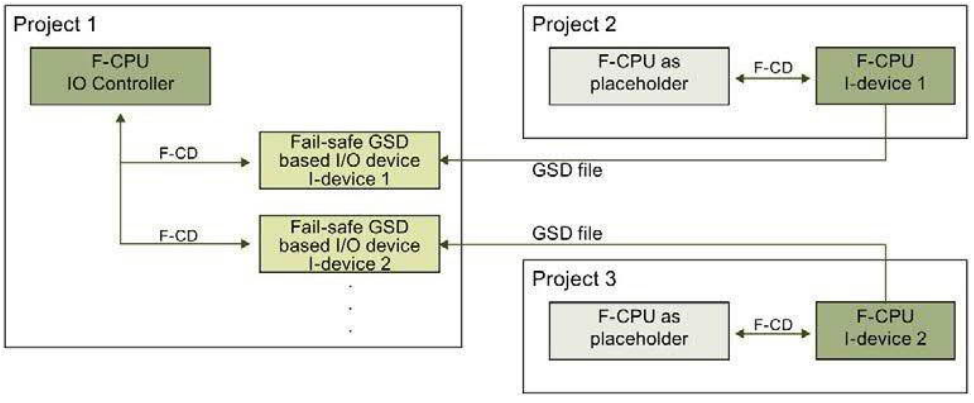
1. Skonfigurować komunikację związaną z bezpieczeństwem w projekcie z I-device zgodnie z opisem w "Komunikacji związanej z bezpieczeństwem pomiędzy sterownikiem IO a I-device" (strona 232) (S7-300/S7-400) lub „Komunikacji związanej z bezpieczeństwem pomiędzy sterownikiem IO a I-device" (strona 294) (S7-1200/S7-1500). W tym przypadku F-CPU 1 (sterownik IO) jest jedynie symbolem zastępczym dla F-CPU w projekcie sterownika IO.

   Uwaga

   Podczas tworzenia za pomocą *STEP 7 Safety* < V14 SP1, należy unikać dalszych zmian z obszarów transferu z CD do F-CD.

   Podczas tworzenia za pomocą *S7 Distributed Safety V5.4*, należy utworzyć obszary transferu aplikacji rodzaju adresu „Output" (Wyjście) i „Input" (Wejście) bezpośrednio po sobie.

2. Eksportować I-device jako plik GSD. Należy postępować zgodnie z opisem w pomocy *STEP 7* pod hasłem „Konfiguracja I-device".
3. Zaimportować plik GSD w projekcie ze sterownikiem IO. Postępować zgodnie z opisem w *pomocy do STEP 7* pod hasłem „Instalacja pliku GSD".
4. Wstawić I-device z karty zadań „Hardware catalog" (Katalog sprzętu) do projektu ze sterownikiem IO.
5. Przypisać F-CPU sterownika IO do I-device.



9.5.1.2 Programowanie komunikacji sterownik IO safety – I-device

Procedura programowania

Aby zaprogramować komunikację związaną z bezpieczeństwem pomiędzy sterownikiem IO a I-device dla F-CPU S7-300/400, należy analogicznie postępować zgodnie z procedurą opisaną w „Komunikacja sterownik IO safety – urządzenie I poprzez SENDDP i RCVDP" (strona 235) oraz „Programowanie komunikacji sterownik IO safety – I-device" (strona 236). Aby zaprogramować F-CPU S7- 300/400, należy użyć adresu początkowego obszarów transferu.

Aby zaprogramować komunikację związaną z bezpieczeństwem pomiędzy sterownikiem IO a I-device dla F-CPU S7-1200/1500, należy analogicznie postępować zgodnie z procedurą opisaną w „Komunikacja sterownik IO safety – urządzenie I poprzez SENDDP i RCVDP" (strona 297) oraz „Programowanie komunikacji sterownik IO safety – I-device" (strona 298). Aby zaprogramować F-CPU S7- 1200/1500, należy użyć identyfikatorów sprzętowych obszarów transferu.

Kompilowanie i finalizowanie programu 10

10.1 Kompilowanie programu bezpieczeństwa

Aby skompilować program bezpieczeństwa, należy wykonać tę samą podstawową procedurę co przy kompilacji standardowego programu użytkownika. Możliwe jest rozpoczęcie z różnych punktów w *STEP 7*, by to wykonać. Podstawy kompilowania programów użytkownika opisano w *pomocy do STEP 7*.

Uwaga

W przypadku zmiany związanej z bezpieczeństwem w konfiguracji sprzętowej należy pamiętać, że nie tylko ją, ale również program bezpieczeństwa należy ponownie skompilować i pobrać. Dotyczy to również zmian w F-I/O, które nie są wykorzystywane w programie bezpieczeństwa.

Uwaga

Program bezpieczeństwa nie jest kompilowany spójnie przy użyciu polecenia menu „Edit > Compile" (Edytuj > Kompiluj) lub ikony „Kompiluj" przy następujących warunkach:

- Po wybraniu folderu utworzonego przez użytkownika w drzewku projektu.
- Po wybraniu jednego lub kilku bloków (bezpieczeństwa) w folderze „Program blocks" (Bloki bezpieczeństwa) w drzewku projektu.

Należy skorzystać z tej procedury by sprawdzić, czy możliwe jest skompilowanie zmodyfikowanych bloków bezpieczeństwa.

Uwaga

Poniższe zagadnienia dotyczą F-CPU S7-300/400:

Aby skompilować blok bezpieczeństwa chronionej wiedzy technologicznej po zmianie, należy usunąć zabezpieczenie dla tego bloku, nim wykona się kompilację.

Zgłaszanie błędów kompilacji

Pomyślność kompilacji można rozpoznać po komunikacie w oknie inspektora „Info > Compile" (Informacje > Kompiluj), gdzie pojawiają się komunikaty o błędach i ostrzeżenia.

Więcej informacji odnośnie procedury, jaką należy wykonać w celu usunięcia błędów kompilacji, patrz „Usuwanie błędów kompilacji" w *pomocy do STEP 7*.

10.2 Wymogi pamięci roboczej programu bezpieczeństwa (S7-300, S7-400)

Szacowanie

Możliwe jest oszacowanie pamięci roboczej wymaganej dla programu bezpieczeństwa w następujący sposób:

Pamięć robocza(work memory) wymagana do programu bezpieczeństwa 32 KB dla bloków systemu

+ 4.4 KB dla komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime
+ 4.5 x pamięć robocza wymagana dla wszystkich F-FB/F-FC/głównych bloków
+ bezpieczeństwa
  4,5 x pamięć robocza wymagana dla wszystkich stosowanych instrukcji, które są przestawione na karcie zadań „Instructions" (Instrukcje) z ikoną bloku.
+ (za wyjątkiem SENDDP, RCVDP, SENDS7 oraz RCVS7)
  Pamięć robocza wymagana dla stosowanych instrukcji SENDDP i RCVDP (4,3 KB
+ każda)
  Pamięć robocza wymagana dla stosowanych instrukcji SENDS7 i RCVS7 (8,5 KB każda)

Pamięć robocza wymagana na dane

5 x pamięć robocza wymagana dla wszystkich F-DB (wraz z DB komunikacji bezpieczeństwa, lecz bez DB dla komunikacji grupy F-runtime) oraz I-DB do głównego bloku bezpieczeństwa/F-FB

+ 24 x pamięć robocza wymagana dla wszystkich DB do komunikacji grupy F-runtime
+ 2.3 x pamięć robocza wymagana dla wszystkich I-DB instrukcji (za wyjątkiem SENDDP, RCVDP, SENDS7 oraz RCVS7)
+ pamięć robocza wymagana dla wszystkich I-DB instrukcji SENDDP (0,2 KB), RCVDP (0,3 KB), SENDS7 (0,6 KB) oraz RCVS7 (1,0 KB)
+ 0,7 KB na F-FC
+ 0,7 KB na F-I/O (dla DB F-I/O itp.)
+ 4,5 KB

Rozmiar automatycznie generowanych bloków bezpieczeństwa

Nie należy wykorzystywać całego, maksymalnego rozmiaru bloku bezpieczeństwa, ponieważ automatycznie generowane bloki bezpieczeństwa są większe, wobec czego możliwe jest przekroczenie maksymalnego dopuszczalnego rozmiaru w F-CPU. Przekroczenie rozmiaru bloku powoduje wyzwolenie odnośnego komunikatu o błędzie z informacją, które bloki bezpieczeństwa są zbyt duże. Należy je podzielić, jeśli to konieczne.

10.3 Pobieranie danych projektu

10.3.1 Pobieranie danych projektu do F-CPU

Wstęp

Po pomyślnym skompilowaniu programu bezpieczeństwa można pobrać go wraz ze standardową aplikacją do F-CPU. Aby pobrać program bezpieczeństwa, należy wykonać te same czynności co w przypadku standardowego programu użytkownika, z różnych punktów początkowych w *STEP 7*.

- W oknie „Load preview" (Podgląd wgrywania) należy wprowadzić dane (np. hasło do F-CPU) i ustawić wymagania do pobrania (np. czy F-CPU został przełączony do trybu STOP przed pobraniem).
- Okno „Load results" (Wynik wczytywania) przedstawia wynik po pobraniu.

Opcje pobierania programu bezpieczeństwa zostaną przedstawione później. Podstawowe informacje dotyczące pobierania można znaleźć w *pomocy do STEP 7*.

Zasady pobierania programu bezpieczeństwa do F-CPU

⚠OSTRZEŻENIE

Jeśli w sieci dostępnych jest **kilka F-CPU** (np. poprzez Ethernet) przy pomocy **tego samego urządzenia programistycznego lub PC**, należy podjąć następujące działania, by zagwarantować, iż dane projektu są pobierane do właściwego F-CPU:

Hasła użytkownika określone dla danego F-CPU, takie jak jednolite hasło do F-CPU z przypisanym do niego adresem ethernetowym.

Należy mieć na uwadze następuje zagadnienia:

- Aby aktywować ochronę dostępu do F-CPU podczas wczytywania konfiguracji sprzętowej po raz pierwszy, należy użyć połączenia dwupunktowego (podobnie jak w przypadku przypisywania adresu MPI do F-CPU po raz pierwszy).
- Przed pobraniem programu bezpieczeństwa do F-CPU, najpierw należy cofnąć istniejące zezwolenie na dostęp dla innych F-CPU.
- Ostatnie pobranie programu bezpieczeństwa przed przełączeniem na operację produkcyjną należy wykonać z aktywną ochroną dostępu. *(S021)*

Uwaga

Pobranie spójnego programu bezpieczeństwa jest możliwe tylko w trybie STOP.

Uwaga

Jeśli *STEP 7 Safety* wykryje niespójność programu bezpieczeństwa podczas rozruchu F-CPU,
nie będzie możliwe jego uruchomienie, o ile F-CPU obsługuje tę funkcję detekcji (patrz informacje o produkcie dla danego F-CPU S7-300/400). Jest ona zawsze obsługiwana w F-CPU S7-1200/1500). Odpowiednie zdarzenie diagnostyczne jest wprowadzane do bufora diagnostycznego F-CPU.

Jeśli F-CPU nie obsługuje tej funkcji detekcji, może przejść do trybu STOP, jeśli niespójny program bezpieczeństwa zostanie wykonany przy aktywnym trybie bezpieczeństwa.

Podczas pobierania programu bezpieczeństwa należy upewnić się, że działanie „Consistent download" (Spójne pobieranie) zostało ustawione dla wyboru „Safety program" (Program bezpieczeństwa) w oknie „Load preview" (Podgląd wczytywania).

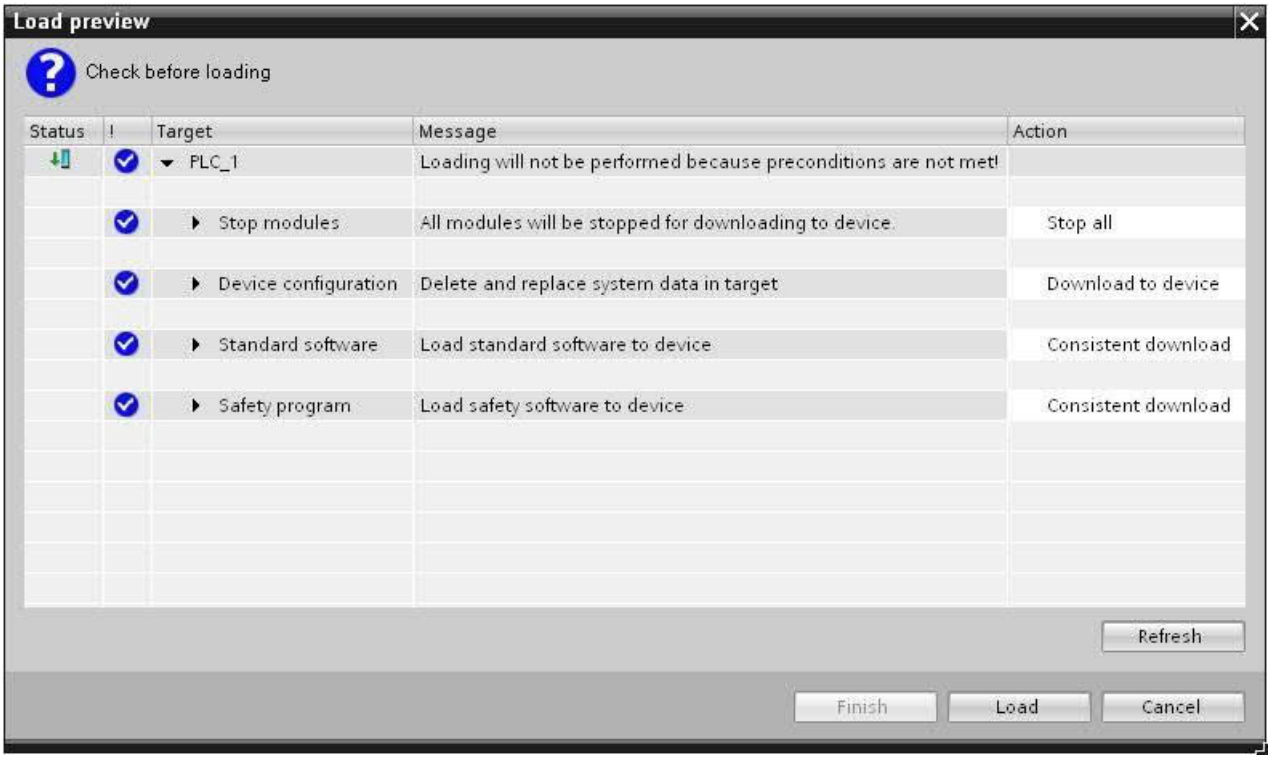
Niespójne pobieranie jest możliwe tylko przy wyłączonym trybie bezpieczeństwa.

Wpisywanie hasła przed pobraniem do F-CPU

Jeśli przypisano poziom ochrony dla F-CPU (strona 109) (we właściwościach F-CPU, zakładka „Protection" (Ochrona)),w oknie „Load preview" (Podgląd wczytywania) należy wpisać odpowiednie hasło. Bez wpisania hasła możliwe jest wykonanie jedynie tych czynności, które są dozwolone bez hasła. Po spełnieniu warunków do pobrania przycisk „Load" (Wczytaj) staje się aktywny.

Okno „Load preview" (Podgląd wczytywania)

W przypadku F-CPU, okno „Load preview" (Podgląd wczytywania) zawiera również dział „Safety program" (Program bezpieczeństwa).



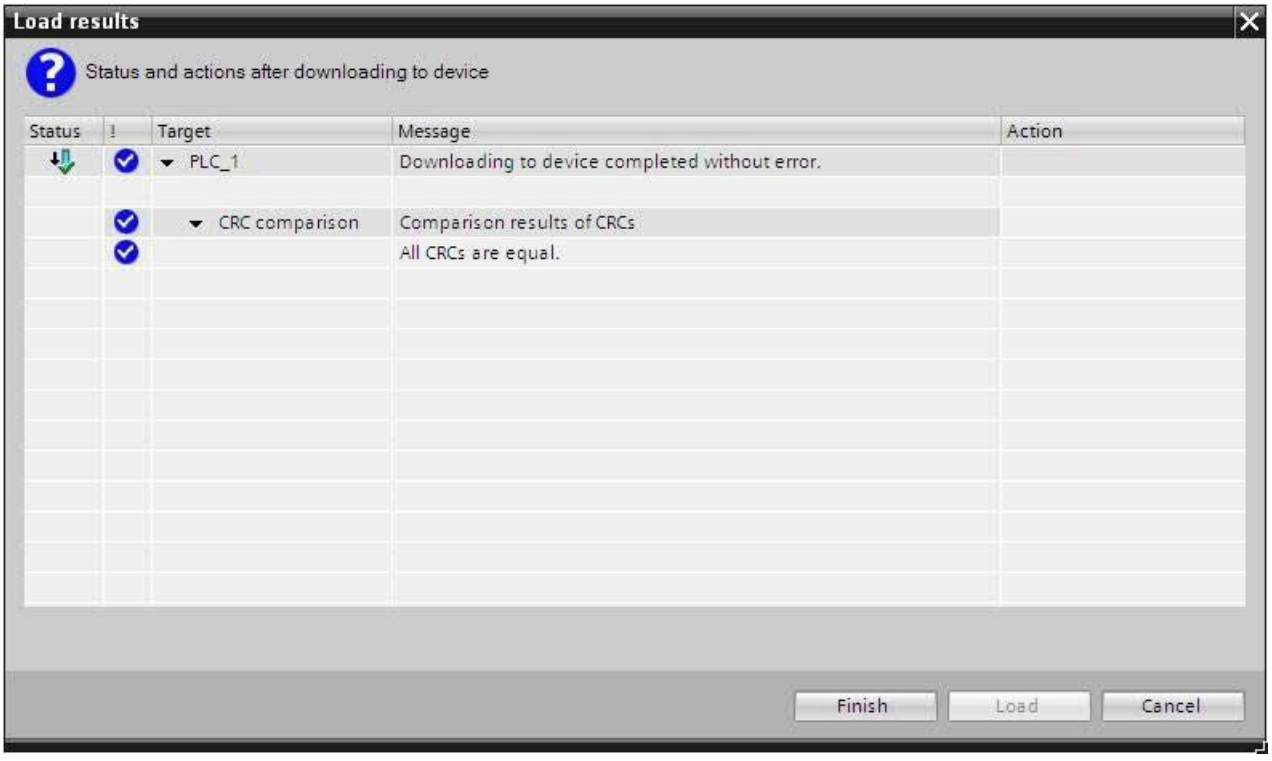
Należy wybrać następujący element:

- Aby pobrać spójny program bezpieczeństwa, należy wybrać działanie „Consistent download" (Spójne pobieranie) pod punktem „Safety program" (Program bezpieczeństwa).
- (S7-300, S7-400) Aby pobrać selektywnie indywidualne bloki bezpieczeństwa (strona 331), należy wybrać działanie „Download selection" (Wybór pobierania) pod punktem „Safety program" (Program bezpieczeństwa), a następnie wybrać wymagane bloki bezpieczeństwa. W razie potrzeby konieczne będzie wyłączenie trybu bezpieczeństwa w „Disable safety mode" (Wyłącz tryb bezpieczeństwa). To ustawienie służy jedynie do testu online poszczególnych bloków bezpieczeństwa.
- (S7-300, S7-400) Aby pobrać jedynie program bezpieczeństwa, należy wybrać działanie „Consistent download" (Spójne pobieranie) pod punktem „Safety program" (Program bezpieczeństwa) oraz działanie „Download selection" (Wybór pobierania) pod punktem „Standard software" (Standardowe oprogramowanie), po czym wybrać jedynie te bloki bezpieczeństwa, które wywołują główny blok bezpieczeństwa.
- (S7-300, S7-400) Aby pobrać program bezpieczeństwa, przykładowo, z powodu nieznajomości hasła do F-CPU, należy wybrać działanie „No action" (Brak działania) pod punktem „Safety program" (Program bezpieczeństwa).

W przypadku F-CPU S7-1200/1500, możliwa jest tylko wartość „Consistent download" (Spójne pobieranie) jako działanie w oknie „Load preview" (Podgląd wczytywania). Nie jest możliwe wybranie oddzielnego wczytywania standardowego programu lub programu bezpieczeństwa. Kompletny program użytkownika jest automatycznie i spójnie pobierany gdy tylko zostaną wprowadzone zmiany w programie standardowym i programie bezpieczeństwa.

Okno „Load results" (Wynik wczytywania)

Po pobraniu do F-CPU, otworzy się okno „Load results" (Wynik wczytywania). W oknie pojawi się status oraz niezbędne czynności po pobraniu.



Należy sprawdzić, czy w oknie pojawił się komunikat „Downloading of safety program completed without errors." (Pobieranie programu bezpieczeństwa ukończone bez błędów.) Jeśli nie, należy powtórzyć operację pobierania.

10.3.1.1 Pobieranie danych projektu do F-CPU S7-300/400 z włożoną kartą pamięci (karta pamięci SIMATIC Memory Card lub karta flash)

Podczas pobierania danych projektu do F-CPU S7-300/400 z włożoną kartą pamięci (karta pamięci SIMATIC Memory Card do S7-300 lub karta flash do S7-400), należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zastosować poniższą procedurę podczas pobierania programu bezpieczeństwa do
F-CPU z **urządzeniem programistycznym/PC**, by zapewnić, iż F-CPU nie zawiera „starego" programu bezpieczeństwa:

- Należy pobrać program bezpieczeństwa do F-CPU.
- Wykonać identyfikację programu (np. sprawdzić, czy zbiorcze podpisy bezpieczeństwa są zgodne online i offline).
- Należy wykonać reset pamięci F-CPU, korzystając z przełącznika trybu lub poprzez urządzenie programistyczne/PC. Po usunięciu pamięci roboczej programu bezpieczeństwa jest ponownie przesyłany z pamięci "load memory" (karta pamięci, karta SIMATIC Micro do F-CPU S7-300, karta flash do F-CPU S7-400) do pamięci roboczej. *(S022)*

10.3.1.2 Pobieranie danych projektu do F-CPU S7-400 bez włożonej karty flash

Podczas pobierania danych projektu do F-CPU S7-400 bez włożonej karty flash, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zastosować poniższą procedurę podczas pobierania programu bezpieczeństwa do
F-CPU z **urządzeniem programistycznym/PC**, by zapewnić, iż F-CPU nie zawiera „starego" programu bezpieczeństwa:

- Należy wykonać reset pamięci F-CPU, korzystając z **przełącznika trybu** lub poprzez **urządzenie programistyczne/PC**.
- Należy pobrać konfigurację sprzętową i program bezpieczeństwa do F-CPU.
- Wykonać identyfikację programu (np. sprawdzić, czy zbiorcze podpisy bezpieczeństwa są zgodne online i offline). *(S023)*

10.3.1.3 Pobieranie danych projektu do WinAC RTX F

Podczas pobierania danych projektu do WinAC RTX F, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Należy zastosować się do poniższej procedury podczas pobierania programu bezpieczeństwa do WinAC RTX F z urządzeniem programistycznym/PC, aby zagwarantować, iż WinAC RTX F nie zawiera „starego" programu bezpieczeństwa:

1. Wykonać reset pamięci WinAC RTX F (patrz podręcznik Windows Automation Center RTX WinAC RTX (F) 2010 (http://support.automation.siemens.com/WW/view/en/43715176)).
2. Pobrać dane projektu (strona 325) do WinAC RTX F.

   Jeśli test funkcyjny programu bezpieczeństwa nie zostanie wykonany w docelowym WinAC RTX F, należy także wykonać punkty 3 i 4:
3. Wykonać identyfikację programu. Oznacza to sprawdzenie, czy zbiorcze podpisy bezpieczeństwa są zgodne online i offline.
4. Wykonać rozruch systemu bezpieczeństwa.

Pomiędzy identyfikacją programu online a rozruchem systemu bezpieczeństwa nie należy zamykać WinAC RTX F (przykładowo, w wyniku ponownego uruchomienia).

(S024)

10.3.1.4 Pobieranie poszczególnych bloków bezpieczeństwa do F-CPU S7-300/400

Pobieranie bloków bezpieczeństwa w wyłączonym trybie bezpieczeństwa.

Możliwe jest jednoczesne pobieranie bloków bezpieczeństwa i standardowych bloków do F-CPU poprzez drzewko projektu. Jednakże, gdy tylko bloki bezpieczeństwa zostaną pobrane, wykonywana jest kontrola w celu sprawdzenia, czy F-CPU jest w trybie STOP lub z wyłączonym trybem bezpieczeństwa. Jeśli nie, dostępna jest opcja przełączenia na wyłączony tryb bezpieczeństwa lub przełączenie F-CPU w tryb STOP.

Aby pobrać poszczególne bloki bezpieczeństwa do F-CPU, przykładowo, by przetestować zmiany, należy upewnić się, że nie wybrano folderu „Program blocks" (Bloki bezpieczeństwa) lub F-CPU w drzewku projektu, lecz jedynie te bloki, które mają zostać pobrane.

Dopiero wtedy, w oknie „Load preview" (Podgląd wczytywania), konieczne będzie wyłączenie trybu bezpieczeństwa po zmianie opcji z „Consistent download" (Spójne pobieranie) na „Download selection" (Wybór pobierania) oraz zmianie opcji „Stop modules" (Zatrzymaj moduły) na „No action" (Brak działania).

W przypadku pominięcia tego wyboru bloku zostaną pobrane bez wyłączenia trybu bezpieczeństwa, co spowoduje przejście F-CPU w tryb STOP.

Wyłączenie trybu bezpieczeństwa jest również możliwe w *Safety Administration Editor* przed rozpoczęciem pobierania.

Należy pamiętać, że spójność programu bezpieczeństwa w F-CPU po pobraniu poszczególnych bloków bezpieczeństwa nie może być gwarantowana. Aby osiągnąć spójny program bezpieczeństwa, zawsze należy pobierać cały program do F-CPU.

Zasady pobierania poszczególnych bloków bezpieczeństwa

Poniższe zasady dotyczą pobierania poszczególnych bloków bezpieczeństwa:

- Pobieranie jest możliwe jedynie przy wyłączonym trybie bezpieczeństwa lub gdy F-CPU jest w trybie STOP.
- Bloki bezpieczeństwa można pobrać jedynie do F-CPU, do którego pobrano już program bezpieczeństwa.

Oznacza to, że należy pobrać cały program bezpieczeństwa podczas jego początkowego pobierania oraz po zmianie hasła do programu bezpieczeństwa.

Uwaga

W przypadku pobierania jedynie bloków bezpieczeństwa, bloki, w których wywoływane są główne bloki bezpieczeństwa (np. przerwanie cykliczne OB 35) nie są pobierane. W tym celu należy wybrać opcję „Selection" (Wybór) pod punktem „Standard software" (Standardowe oprogramowanie) w oknie podglądu i wybrać niezbędne bloki.

Uwaga

Pobieranie poszczególnych bloków bezpieczeństwa służy jedynie do ich testowania. Przed przejściem do trybu produkcyjnego należy pobrać spójny program bezpieczeństwa do F-CPU.

10.3.1.5 Pobieranie danych projektu do F-CPU S7-1200 bez włożonej karty programu

Podczas pobierania danych projektu do F-CPU S7-1200 bez włożonej karty programu, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zastosować poniższą procedurę podczas pobierania programu bezpieczeństwa do
F-CPU z **urządzeniem programistycznym/PC**, by zapewnić, iż F-CPU nie zawiera „starego" programu bezpieczeństwa:

- Należy pobrać program bezpieczeństwa do F-CPU.
- Wykonać identyfikację programu (np. sprawdzić, czy zbiorcze podpisy bezpieczeństwa są zgodne online i offline). *(S042)*

10.3.1.6 Pobieranie danych projektu do F-CPU S7-1200 z włożoną kartą programu

Podczas pobierania danych projektu do F-CPU S7-1200 z włożoną kartą programu, należy przestrzegać następującego ostrzeżenia:

⚠ OSTRZEŻENIE

Należy przestrzegać poniższej procedury, by zapewnić, iż we wewnętrznej pamięci "load memory" F-CPU nie ma „starego" programu bezpieczeństwa, gdy wkładana jest karta programu do F-CPU S7-1200:

1. Należy sprawdzić, czy **dioda LED STOP/RUN (pomarańczowa) oraz dioda LED konserwacji migają podczas rozruchu przez 3 sekundy na F-CPU bez karty pamięci**. Jeśli tak jest, wewnętrzna pamięć "load memory" F-CPU została już usunięta (przykładowo, gdy F-CPU działał z kartą programu jako zewnętrzną pamięcią "load memory") i można pominąć krok 3.
2. Włożyć kartę programu do F-CPU.

   Jeśli F-CPU jest w trybie RUN, przełączy się na STOP. Dioda LED konserwacji na F-CPU zacznie migać, wskazując, ze karta programu jest oceniania lub że należy usunąć wewnętrzną pamięć "load memory".
3. Do usunięcia wewnętrznej pamięci "load memory" można użyć jednej z poniższych metod:
   - Wyłączyć F-CPU i ponownie go włączyć.
   - Przełączyć F-CPU z trybu STOP na RUN.
   - Wykonać funkcję „Memory reset" (Reset pamięci) (MRES).

   Po ponownym uruchomieniu i usunięciu wewnętrznej pamięci "load memory", **dioda LED STOP/RUN (pomarańczowa) oraz dioda LED konserwacji muszą migać**. Wewnętrzna pamięć "load memory" F-CPU została usunięta i nie zawiera już „starego" programu bezpieczeństwa.
4. Do oceny karty programu można użyć jednej z poniższych metod:
   - Wyłączyć F-CPU i ponownie go włączyć.
   - Przełączyć F-CPU z trybu STOP na RUN.
   - Wykonać funkcję „Memory reset" (Reset pamięci)

   (MRES). F-CPU uruchomi się ponownie i wykona

   ocenę karty programu.

   F-CPU następnie przejdzie w tryb rozruchu (RUN lub STOP), który został ustawiony dla F-CPU. *(S061)*

W przypadku F-CPU S7-1200 bez włożonej karty pamięci SIMATIC Memory Card oraz z usuniętą wewnętrzną pamięcią "load memory", diody LED statusu przybiorą konfigurację opisaną w poniższej tabeli.

Opis	**STOP/RUN** **Pomarańczowa/Zielona**	**ERROR Czerwona**	**MAINT Pomarańczowa**
Wewnętrzna pamięć "load memory" usunięta i karta pamięci SIMATIC Memory Card **nie** włożona.	Migająca (pomarańczowa) (przez 3 sekundy podczas rozruchu)	Wyłączona	Migająca (przez 3 sekundy podczas rozruchu)

OSTRZEŻENIE

W przypadku wykorzystywania urządzenia programistycznego/PC do pobierania bloków bezpieczeństwa do F-CPU S7-1200 z włożoną kartą programu (zewnętrzna pamięć "load memory"), należy upewnić się, że przesył jest wykonywany na kartę. Można to wykonać za pomocą następujących środków:

- Sprawdzić, czy karta programu jest włożona poprawnie.
- Włożyć kartę programu, której rozmiar pamięci jest inny niż rozmiar wewnętrznej pamięci "load memory". Sprawdzić w drzewku projektu „Online & Diagnostics > Diagnostics > Memory" (Online i diagnostyka > Diagnostyka > Pamięć), czy rozmiar pamięci wyświetlany dla pamięci "load memory" odpowiada wielkości karty programu. *(S058)*

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zastosować poniższą procedurę podczas pobierania programu bezpieczeństwa do
F-CPU z **urządzeniem programistycznym/PC**, by zapewnić, iż F-CPU nie zawiera „starego" programu bezpieczeństwa:

- Należy pobrać program bezpieczeństwa do F-CPU.
- Wykonać identyfikację programu (np. sprawdzić, czy zbiorcze podpisy bezpieczeństwa są zgodne online i offline). *(S042)*

10.3.1.7 Pobieranie danych projektu do F-CPU S7-1500

Podczas pobierania danych projektu do F-CPU S7-1500, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zastosować poniższą procedurę podczas pobierania programu bezpieczeństwa do
F-CPU z **urządzeniem programistycznym/PC**, by zapewnić, iż F-CPU nie zawiera „starego" programu bezpieczeństwa:

- Należy pobrać program bezpieczeństwa do F-CPU.
- Wykonać identyfikację programu (np. sprawdzić, czy zbiorcze podpisy bezpieczeństwa są zgodne online i offline). *(S042)*

10.3.1.8 Pobieranie danych projektu do sterownika programowego S7-1500 F

Podczas pobierania danych projektu do sterownika programowego S7-1500 F, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zastosować poniższą procedurę podczas pobierania programu bezpieczeństwa do
F-CPU z **urządzeniem programistycznym/PC**, by zapewnić, iż F-CPU nie zawiera „starego" programu bezpieczeństwa:

- Należy pobrać program bezpieczeństwa do F-CPU.
- Wykonać identyfikację programu (np. sprawdzić, czy zbiorcze podpisy bezpieczeństwa są zgodne online i offline). *(S042)*

OSTRZEŻENIE

Ze względów bezpieczeństwa, hasło sterownika programowego S7-1500 F, oprócz pamięci "load memory", jest również przechowywane w odrębnej pamięci.

W przeciwieństwie do pamięci "load memory", ta odrębna pamięć nie jest usuwana. Oznacza to, że poprzednie hasła są ponownie aktywne po usunięciu sterownika programowego S7-1500 F i następującego uruchomienia.

Z tego względu należy mieć na uwadze następuje zagadnienia:

- Sterownik programowy S7-1500 F jest usuwany w przypadku następujących sytuacji pobierania stacji PC:
  - Pobieranie stacji PC ze zmodyfikowanym przypisaniem interfejsu.
  - Pobieranie stacji PC ze zmodyfikowanym miejscem zapisu danych retentywnych.
- Dlatego zaleca się, by nie ustawiać ochrony dostępu bezpieczeństwa przed wykonaniem odbioru technicznego. Jeśli wymagana jest zmiana przypisania interfejsu stacji PC lub miejsca zapisu danych retentywnych, nie trzeba wprowadzać hasła bezpieczeństwa podczas kolejnego obowiązkowego pobierania sterownika programowego S7-1500 F.
- Zaleca się, by usunąć ochronę dostępu bezpieczeństwa ze sterownika programowego S7-1500 F, który nie jest już używany. W przypadku zapomnienia hasła bezpieczeństwa do sterownika programowego S7-1500 F, można usunąć je poprzez deinstalację/instalację lub wczytanie nowego obrazu. *(S076)*

Zobacz także

Pobieranie danych projektu do F-CPU (strona 325)

Sterownik programowy

(http://support.automation.siemens.com/WW/view/en/109249299)

10.3.2 Pobieranie danych projektu do karty pamięci i wkładanie karty

Należy postępować tak jak w przypadku standardowych bloków, by pobrać dane projektu z F-CPU do karty pamięci (karta flash dla S7-400, karta SIMATIC Micro do S7-300 lub SIMATIC Memory Card do S7-1200/1500). Należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny danych projektu nie zostanie wykonany w F-CPU docelowym, należy zagwarantować, iż poprawne dane projektu znajdują się na karcie pamięci po ich pobraniu.

Należy wykonać następujące kroki:

1. Upewnić się, że użyto pustej karty pamięci.
2. Pobrać dane projektu na kartę.
3. Wyraźnie oznakować kartę unikalną nazwą (np. ze zbiorczym podpisem bezpieczeństwa).

Podana procedura musi zostać zapewniona poprzez środki organizacyjne. *(S043)*

Po włożeniu karty pamięci (karta flash dla S7-400, karta SIMATIC Micro do S7-300 lub SIMATIC Memory Card do S7-1200/1500) z danymi projektu z F-CPU, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zagwarantować poprzez identyfikację programu online lub inne stosowne środki (np. sprawdzenie oznakowania karty), że włożona karta pamięci zawiera poprawny program bezpieczeństwa. *(S025)*

10.3.2.1 Wkładanie karty pamięci SIMATIC Memory Card lub karty flash do F-CPU S7-300/400

Po włożeniu karty pamięci (karta flash do S7-400 lub karta SIMATIC Micro do S7-300) do F-CPU S7-300/400 F-CPU, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

Jeśli test funkcjonalny programu bezpieczeństwa nie zostanie wykonany w F-CPU docelowym, należy zastosować poniższą procedurę podczas wkładania karty, by upewnić się, iż F-CPU nie zawiera „starego" programu bezpieczeństwa:

- Wyłączyć zasilanie F-CPU. W przypadku F-CPU z awaryjnym zasilaniem bateryjnym (np. CPU 416F-2), wyjąć baterię. (Aby upewnić się, że F-CPU jest pozbawiony zasilania, należy odczekać przez czas bufora stosowanego zasilacza, lub jeśli nie jest on znany, wyjąć F-CPU.)
- Wyjąć kartę pamięci ze starym programem bezpieczeństwa z F-CPU.
- Włożyć kartę pamięci z nowym programem bezpieczeństwa do F-CPU.
- Włączyć F-CPU. W przypadku F-CPU z awaryjnym zasilaniem bateryjnym (np. CPU 416F-2), włożyć baterię.

(S026)

10.3.2.2 Wkładanie karty transferowej do F-CPU S7-1200

Podczas wkładanie karty transferowej do F-CPU S7-1200, należy przestrzegać następującego ostrzeżenia:

⚠OSTRZEŻENIE

Należy przestrzegać poniższej procedury, by zapewnić, iż we wewnętrznej pamięci "load memory" nie ma „starego" programu bezpieczeństwa, gdy dane projektu są kopiowane do F-CPU S7-1200 przy pomocy karty transferowej:

1. Należy sprawdzić, czy **dioda LED STOP/RUN (pomarańczowa) oraz dioda LED konserwacji migają podczas rozruchu przez 3 sekundy na F-CPU bez karty pamięci**. W takim przypadku wewnętrzna pamięć "load memory" F-CPU została już usunięta i można pominąć krok 3.
2. Włożyć kartę transferową do F-CPU.

   Jeśli F-CPU jest w trybie RUN, przełączy się na STOP. Dioda LED konserwacji na F-CPU zacznie migać, wskazując, ze karta transferowa jest oceniania lub że należy usunąć wewnętrzną pamięć "load memory".
3. Do usunięcia wewnętrznej pamięci "load memory" można użyć jednej z poniższych metod:
   - Wyłączyć F-CPU i ponownie go włączyć.
   - Przełączyć F-CPU z trybu STOP na RUN.
   - Wykonać funkcję „Memory reset" (Reset pamięci) (MRES).

   Po ponownym uruchomieniu i usunięciu wewnętrznej pamięci "load memory", **dioda LED STOP/RUN (pomarańczowa) oraz dioda LED konserwacji muszą migać**. Wewnętrzna pamięć "load memory" F-CPU została usunięta i nie zawiera już „starego" programu bezpieczeństwa.
4. Należy użyć jednej z poniższych metod do oceny karty transferowej (transfer z karty do wewnętrznej pamięci "load memory"):
   - Wyłączyć F-CPU i ponownie go włączyć.
   - Przełączyć F-CPU z trybu STOP na RUN.
   - Wykonać funkcję „Memory reset" (Reset pamięci) (MRES).

   Po ponownym uruchomieniu i wykonaniu oceny karty SIMATIC Memory Card, F-CPU kopiuje dane projektu do wewnętrznej pamięci "load memory". Po zakończeniu kopiowania dioda LED konserwacji na F-CPU zacznie migać, wskazując, że można wyjąć kartę.
5. Wyjąć kartę transferową z F-CPU.
6. Do oceny wewnętrznej pamięci "load memory" można użyć jednej z poniższych metod:
   - Wyłączyć F-CPU i ponownie go włączyć.
   - Przełączyć F-CPU z trybu STOP na RUN.
   - Wykonać funkcję „Memory reset" (Reset pamięci) (MRES).

   F-CPU następnie przejdzie w tryb rozruchu (RUN lub STOP), który został ustawiony dla F-CPU. *(S059)*

W przypadku F-CPU S7-1200 bez włożonej karty pamięci SIMATIC Memory Card oraz z usuniętą wewnętrzną pamięcią "load memory", diody LED statusu przybiorą konfigurację opisaną w poniższej tabeli.

Opis	**STOP/RUN Pomarańczowa/Zielona**	**ERROR Czerwona**	**MAINT Pomarańczowa**
Wewnętrzna pamięć "load memory" usunięta i karta pamięci SIMATIC Memory Card **nie** włożona.	Migająca (pomarańczowa) (przez 3 sekundy podczas rozruchu)	Wyłączona	Migająca (przez 3 sekundy podczas rozruchu)

10.3.3 Pobieranie danych projektu F-CPU S7-1200 z wewnętrznej pamięci roboczej do pustej karty SIMATIC Memory Card

Podczas pobierania danych projektu z wewnętrznej pamięci "load memory" F-CPU S7-1200 do pustej karty SIMATIC Memory Card, należy przestrzegać następującego ostrzeżenia:

⚠OSTRZEŻENIE

Aby zagwarantować, iż program bezpieczeństwa został pobrany z wewnętrznej pamięci "load memory" F-CPU do karty SIMATIC Memory Card po podłączeniu jej do F-CPU S7-1200 oraz że wewnętrzna pamięć "load memory" zostanie następnie usunięta, należy wykonać następującą procedurę:

1. Należy upewnić się, że wykorzystywana jest pusta karta SIMATIC Memory Card, przykładowo, sprawdzając w eksploratorze Windows, czy folder „SIMATIC.S7S" oraz plik „S7_JOB.S7S" zostały usunięte.
2. Włożyć pustą kartę SIMATIC Memory Card do F-CPU.

   Jeśli F-CPU jest w trybie RUN, przełączy się na STOP. Dioda LED konserwacji na F- CPU miga, wskazując, że można skopiować program z wewnętrznej pamięci "load memory" na kartę SIMATIC Memory Card oraz że pamięć wewnętrzna jest następnie kasowana.
3. Do rozpoczęcia kopiowania z pamięci wewnętrznej na kartę SIMATIC Memory Card i następnego wykasowania pamięci należy użyć jednej z poniższych metod:
   - Wyłączyć F-CPU i ponownie go włączyć.
   - Przełączyć F-CPU z trybu STOP na RUN.
   - Wykonać funkcję „Memory reset" (Reset pamięci) (MRES).

   Po zrestartowaniu i skopiowaniu programu z wewnętrznej pamięci "load memory" do karty SIMATIC Memory Card oraz opróżnieniu wewnętrznej pamięci, **dioda LED STOP/RUN (pomarańczowa) oraz dioda LED konserwacji muszą migać**. Wewnętrzna pamięć "load memory" F-CPU została usunięta i nie zawiera już programu bezpieczeństwa. Karta SIMATIC Memory Card jest teraz kartą programu.
4. Do oceny karty programu można użyć jednej z poniższych metod:
   - Wyłączyć F-CPU i ponownie go włączyć.
   - Przełączyć F-CPU z trybu STOP na RUN.
   - Wykonać funkcję „Memory reset" (Reset pamięci)

   (MRES). F-CPU uruchomi się ponownie i wykona

   ocenę karty programu.

   F-CPU następnie przejdzie w tryb rozruchu (RUN lub STOP), który został ustawiony dla F-CPU. *(S057)*

Uwaga

Należy również zastosować się do ustawienia „Disable copying from internal load memory to external load memory" „Wyłącz kopiowanie z wewnętrznej pamięci obciążenia do zewnętrznej pamięci" w konfiguracji sprzętowej F-CPU.

10.3.4 Aktualizacja danych projektu na F-CPU S7-1200 przy użyciu karty transferowej

Podczas aktualizacji danych projektu na F-CPU S7-1200 przy pomocy karty transferu, należy przestrzegać następującego ostrzeżenia:

OSTRZEŻENIE

W przypadku wykonania aktualizacji programu bezpieczeństwa w F-CPU S7-1200 przy pomocy karty transferowej, należy upewnić się, że transfer do wewnętrznej pamięci "load memory" odbył się poprawnie, za pomocą dalszej identyfikacji programu. *(S060)*

10.3.5 Przywracania kopii zapasowej programu bezpieczeństwa do F-CPU S7-300/1200/1500

Dostępna jest opcja wykonania kopii dla F-CPU w taki sam sposób jak przy standardowym CPU, a następnie przywrócenie jej. Informacje dotyczące wykonywania kopii dla CPU można znaleźć w *pomocy do STEP 7* pod hasłem „Tworzenie kopii zapasowej S7-CPU",

Podczas przywracania konfiguracja programowej i sprzętowej do F-CPU należy mieć na uwadze następuje zagadnienia:

OSTRZEŻENIE

Po przywróceniu kopii dla F-CPU należy wykonać identyfikację programu.
(S055)

Uwaga

Zaleca się, by do identyfikacji programu użyć zbiorczego podpisu bezpieczeństwa, który jest ujęty w nazwie pliku zapasowego. W takim przypadku nie wolno zmieniać zbiorczego podpisu bezpieczeństwa w nazwie.

OSTRZEŻENIE

(S7-1200/1500) Jeśli wiele F-CPU z aktywnym serwerem sieciowym jest dostępnych dla tego samego urządzenia programistycznego lub PC, należy zastosować dodatkowe środki, by upewnić się, że program bezpieczeństwa jest przywracany do właściwego F-CPU.

Do praw „Administrator bezpieczeństwa" na serwerze sieciowym należy wykorzystywać hasła określone dla CPU. Przykładowo, należy wybrać jednolite hasło z dołączonym adresem IP (np. Password_192.168.0.8) dla każdego F-CPU. *(S065)*

10.3.6 Funkcje specjalne podczas tworzenia i importowania obrazów sterownika programowego S7-1500 F

Tworzenie obrazu

OSTRZEŻENIE

Podczas tworzenia obrazu z programem bezpieczeństwa należy zastosować się do następujących punktów:

- Należy ograniczyć dostęp do sterownika programowego S7-1500 F poprzez ochronę dostępu dla osób, które są upoważnione do tworzenia obrazów.
- Przed utworzeniem obrazu należy użyć identyfikacji programu do upewnienia się, że w sterowniku programowym S7-1500 F zainstalowany jest właściwy program bezpieczeństwa.
- Obrazy z programem bezpieczeństwa należy tworzyć na pustym nośniku danych (opróżnionym lub sformatowanym) lub istniejący obraz musi zostać całkowicie usunięty.
- Po utworzeniu obrazu należy wyjąć nośnik z nim.
- Wyraźnie oznakować nośnik danych nazwą (np. ze zbiorczym podpisem bezpieczeństwa). *(S073)*

UWAGA

Jeśli program bezpieczeństwa w obrazie oraz stary program bezpieczeństwa sterownika programowego S7-1500 F nie są identyczne, zaimportowany program nie uruchomi się. W takim przypadku należy ponownie pobrać program bezpieczeństwa do F-CPU. Można to zrobić, na przykład, za pomocą TIA Portal. Dlatego też kopie bezpieczeństwa zawsze powinny być aktualne.

W taki sam sposób można uruchomić program bezpieczeństwa z innej karty CFast, możliwe jest również wgranie i uruchomienie obrazu utworzonego przez inne urządzenie lub nośnik danych.

Import obrazu

OSTRZEŻENIE

Podczas importowania obrazu z programem bezpieczeństwa należy zastosować się do następujących punktów:

- Należy ograniczyć dostęp do sterownika programowego S7-1500 F poprzez ochronę dostępu dla osób, które są upoważnione do importowania obrazów.
- Importując obraz poprzez LAN, zdalny dostęp lub porównywalny dostęp, należy zapewnić ochronę dostępu (np. poprzez zezwolenie administratora Windows (ADMIN)). Należy pamiętać, że jedynie upoważnione osoby są ustawiane jako użytkownicy.
- Aby zapewnić, że obraz jest zapisywany do właściwego sterownika programowego S7-1500 F, podczas importowania obrazu poprzez LAN należy upewnić się, że tylko jeden sterownik programowy jest dostępny w sieci. Można to osiągnąć na przykład przez usunięcie fizycznych połączeń oraz opcji trasowania do innych sterowników programowych S7-1500 F.
- Należy upewnić się, że w obrazie znajduje się właściwy program bezpieczeństwa, na przykład, poprzez unikalną identyfikację nośnika danych.
- Należy usunąć obraz i wszelkie kopie po zaimportowaniu ich na sterownik programowy S7-1500 F.
- Po zaimportowaniu obrazu należy użyć identyfikacji programu do upewnienia się, przykładowo, za pomocą panelu że w sterowniku programowym S7-1500 F zainstalowany jest właściwy program bezpieczeństwa. *(S074)*

10.3.7 Wczytywanie danych projektu z F-CPU do urządzenia programującego /PC

Wczytywanie danych projektu (w tym dane projektu safety) do urządzenia programistycznego / PC (S7-1500)

Funkcja „Upload from device (software)" (Wczytaj z urządzenia (oprogramowanie)) lub „Upload device as new station (hardware and software)" (Wczytaj urządzenie jako nową stację (sprzęt i oprogramowanie)) jest dostępna tylko dla F-CPU S7-1500, jeśli opcja „Enable consistent upload from the F-CPU" (Włącz spójne wczytywanie z F-CPU) jest aktywna dla F-CPU w *Safety Administration Editor,* a dane projektu zostały następnie wgrane do F-CPU.

Aby wczytać dane projektu (w tym dane projektu safety) do urządzenia programistycznego / PC, należy postępować jak przy standardowych blokach.

Jeśli w sieci dostępnych jest kilka F-CPU (np. poprzez przemysłowy Ethernet) przy pomocy tego samego urządzenia programistycznego lub PC, należy zagwarantować, iż dane projektu są pobierane z właściwego F-CPU. Przykład: „Online & diagnostics" > "Online accesses " > "Flash LED" (Online i diagnostyka > Dostęp online > Migająca LED).

Po pomyślnym wczytaniu z urządzenia można kontynuować pracę jak z projektem utworzonym offline.

OSTRZEŻENIE

Aby wykonać zatwierdzenie danych projektu wczytanych do urządzenia programistycznego / PC lub wykonać zmiany w danych projektu związanych z bezpieczeństwem, a F-CPU jest w trybie STOP, należy przełączyć go w tryb RUN przed wgraniem ich do urządzenia programistycznego / PC. W ten sposób można zagwarantować, że program bezpieczeństwa jest wykonalny. Jeśli F-CPU pozostaje w trybie STOP, nie jest możliwe wykonanie zatwierdzenia zmian w danych projektu związanych z bezpieczeństwem. *(S080)*

Możliwe jest wczytanie poszczególnych bloków bezpieczeństwa do urządzenia programistycznego / PC niezależnie od opcji „Zezwól na spójne wgrywanie z F-CPU".

Nie jest możliwe wgrywanie do urządzenia programistycznego / PC poszczególnych bloków bezpieczeństwa chronionej wiedzy technologicznej.

Uwaga

Hasło offline jest zastępowane lub usuwanie przez hasło online programu

Zobacz także

Obszar „ustawienia" (strona 91)

10.3.8 Wczytywanie stacji PC poprzez plik konfiguracyjny

Dostępna jest opcja zapisania konfiguracji systemu PC w pliku konfiguracyjnym, przeniesienie go i wczytanie do systemu docelowego. Cała konfiguracja stacji PC jest zapisywana w pliku konfiguracyjnym o rozszerzeniu *.psc z TIA Portal.

Zapisywanie i wczytywanie pliku konfiguracyjnego jest obsługiwane od:

- *STEP 7 Safety V15*
- Sterownik programowy S7-1500 F V2.5

Przykład

Szczegółowy przykład dostępny jest na stronie (https://support.industry.siemens.com/cs/ww/en/view/109759142).

Parametry identyfikacyjne

Parametry identyfikacyjne obejmują:

- Nazwę pliku
- Informacje w projekcie i stacji zapisane z TIA Portal w pliku PSC w metadanych.

  Przykładowo:

  - Wersja projektu
  - Przeznaczenie instalacji
  - Komentarz stacji

Parametry identyfikacyjne należy zapisać w pliku, jeśli to konieczne, który jest zapisany w systemie docelowym.

Do oceny i testowania tych parametrów identyfikacyjnych poprzez skrypt, należy zapisać te informacje bezpośrednio w skrypcie lub zapisać parametry identyfikacyjne w odrębnym pliku, który zostanie zapisany w systemie docelowym.

10.3.8.1 Tworzenie pliku konfiguracyjnego

1. W TIA Portal należy utworzyć nowy plik konfiguracyjny w „Project > Memory Card file > New > PC system configuration file (.psc)".

   Plik konfiguracyjny jest tworzony w drzewku projektu pod hasłem „Card reader/USB memory".
2. Przy pomocy zbiorczego podpisu bezpieczeństwa należy sprawdzić w SAE, czy wybrano poprawny projekt/stację.
3. Przy pomocy myszy należy przeciągnąć wybraną stację PC do pliku konfiguracyjnego.

   Spowoduje to wczytanie stacji PC do pliku konfiguracyjnego.

⚠ OSTRZEŻENIE

Zamiast identyfikacji programu online, można użyć unikalnej nazwy do pliku konfiguracyjnego *.psc (**P**C **S**tation **C**onfiguration), aby upewnić się, że poprawny program bezpieczeństwa został umieszczony w pliku konfiguracyjnego.

Ponadto, należy zastosować poniższe uwagi podczas tworzenia pliku konfiguracyjnego:

Podczas tworzenia pliku konfiguracyjnego z programem bezpieczeństwa nie można korzystać z istniejącego pliku. Należy utworzyć nowy plik.

Należy również usunąć pliki konfiguracyjne z wadliwym programem z nośnika danych.

Należy ograniczyć dostęp do pliku konfiguracyjnego (*.pcs) poprzez wstrzymanie dostępu do obszaru do osób, które są upoważnione do importowania i modyfikowania pliku. *(S081)*

10.3.8.2 Importowanie pliku konfiguracyjnego

Dostępne są następujące opcje importowania pliku konfiguracyjnego:

- Poprzez menu panelu stacji PC (import plikukonfiguracyjnego)
- Za pomocą skryptu

Import poprzez menu panelu stacji PC

Wymogi

Aby rozpocząć importowanie pliku konfiguracyjnego poprzez menu w panelu stacji PC S7-150xS(P) F, wykonujący je użytkownik musi być w grupie „Operatorzy fail-safe".

Procedura

OSTRZEŻENIE

Jeśli operacja importu przebiegła pomyślnie, wyświetli się pomyślny komunikat. Jeśli nie pojawił się pomyślny komunikat, należy przyjąć, iż import nie powiódł się i wciąż obecny jest stary program bezpieczeństwa.

Podczas importowania pliku konfiguracyjnego stacji PC poprzez menu panelu z programem bezpieczeństwa, należy zastosować następujące środki:

- Użyć unikalnej nazwy pliku, by sprawdzić, czy wybrano wymagany plik.
- Aby zapewnić, że import jest wykonywany do właściwego sterownika programowego S7-1500 F, podczas importowania konfiguracji poprzez LAN należy upewnić się, że zaadresowano właściwy sterownik programowy. W tym celu należy wykonać jedną z poniższych czynności:
  – Usunąć fizyczne połączenia oraz opcje trasowania do innych sterowników programowych S7-1500 F.
  – Użyć unikalnych nazw komputera i loginów użytkowników bądź innych opcji identyfikacji. *(S084)*

Import za pomocą skryptu

⚠OSTRZEŻENIE

Należy sprawdzić w skrypcie opartym na konkretnych parametrach identyfikacyjnych, czy import pliku konfiguracyjnego jest dozwolony dla odnośnego systemu docelowego (np. poprzez wykonanie oceny nazwy F-CPU, nazwy projektu lub korzystając z przeznaczenia instalacji).

Ponadto może być konieczne lub użyteczne sprawdzenie odnośnych instancji systemu docelowego, co oznacza wszechstronną kontrolę adresowania i/lub kontrolę wersji pliku konfiguracyjnego. Przykładowo, jedynie wyższe wersje lub wyjątki w postaci konkretnych wersji (czarna lista). Należy zawczasu przygotować te informacje na systemie docelowym.

Przykład kontroli odnośnej wersji pod kątem ważności:

- Skrypt ocenia informacje dotyczące wersji i zezwala, przykładowo, tylko na pliki konfiguracyjne wyższej wersji.

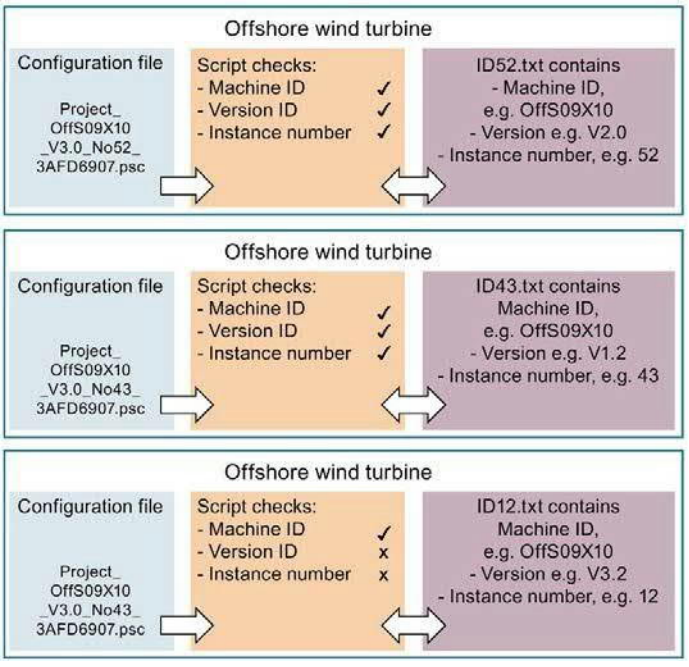
Jak producent maszyn, użytkownik musi zagwarantować, iż skrypt jest chroniony przed nieupoważnioną manipulacją (zmianą zawartości lub nazwy).

Jeśli jako producent maszyn użytkownik musi jedynie udostępnić pliki konfiguracyjne, należy upewnić się, że nie zaimportowano niewłaściwego pliku konfiguracyjnego, stosując środki techniczne (rozszerzona kontrola skryptu) oraz szkolenie operatorów maszyn. *(S082)*

Skrypt sprawdza:

- Pasujące identyfikatory maszyny
- Wersje identyfikatorów wyższe niż bieżący. W przypadku wykrycia, nowa wersja jest zapisywana do pliku txt.

Poniższa ilustracja zawiera omówienie systematyczne kontroli pliku konfiguracyjnego w skrypcie przy pomocy parametrów identyfikacyjnych zapisanych w odrębnym pliku (przedstawione na fioletowo na ilustracji):



OSTRZEŻENIE

Pomyślne zaimportowanie programu bezpieczeństwa poprzez skrypt określa się, oceniając odnośną wartość zwrotną (0x51A3). Jeśli odnośna wartość zwrotna nie została zwrócona przed polecenie skryptu PCSystem_Control, import nie powiódł się i stary program może wciąż być obecny.

Aby zapewnić, że wartość zwrotna nie pochodzi z poprzedniego importowania, należy zresetować wartość do 0x3FF („PCSystem_Control /ImportConfig" bez wprowadzania nazwy pliku) przed wykonaniem importu i następnie sprawdzić, czy wartość zwrotna została zresetowana do 0x3FF (wprowadzić „PCSystem_Control /GetStatus /ImportConfig", po czym wpisać „echo %errorlevel%". Ta instrukcja musi zwrócić wartość 0x3FF).

Jeśli operacja importu jest wyzwalana przez serwer, konieczna jest informacja o pozytywnej wartości zwrotnej.

Dla zapewnienia możliwości śledzenia zaleca się, by udokumentować operację importu w

pliku rejestru.

Jeśli plik konfiguracyjny jest importowany ręcznie poprzez linię poleceń Windows (poprzez polecenie skryptu), należy wykonać jedną z następujących czynności:

- Zresetować wartość zwrotną do 0x3FF przed zaimportowaniem i sprawdzić ją (patrz powyżej).
  - Wykonać import.
  - Ocenić wartość zwrotną (wprowadzić „PCSystem_Control /GetStatus /ImportConfig", po czym wpisać „echo %errorlevel%". Ta instrukcja musi zwrócić wartość 0x51A3).
- Wykonać import.
  - Wykonać ręczną identyfikację programu, np. poprzez panel na F-CPU.

(S083)

Uwaga

Pozytywna wartość zwrotna podczas importowania pliku konfiguracyjnego poprzez skrypt to „0x51A3" dla sterownika programowego S7-1500 F, w odróżnieniu od sterownika programowego S7-1500, dla którego jest to „0x0000".

Gdy plik jest importowany przez skrypt, należy przenieść do niego autoryzację. Oznacza to, że użytkownik wykonawczy nie wymaga wyższego upoważnienia, ponieważ skrypt udostępniony przez producenta maszyn zawiera niezbędne autoryzacje (grupa użytkowników „Operatorzy fail-safe").

Prawa są przypisywane poprzez skrypt jako przypisanie usługi Windows do odpowiedniej grupy użytkowników. Ta początkowa instalacja musi zostać wykonana zawczasu przez administratora Windows na każdym komputerze z S7-150xS(P) F. Usługa Windows może zostać wywołana przez użytkownika wykonawczego, po czym usługa Windows wykona skrypt.

10.4 Identyfikacja programu

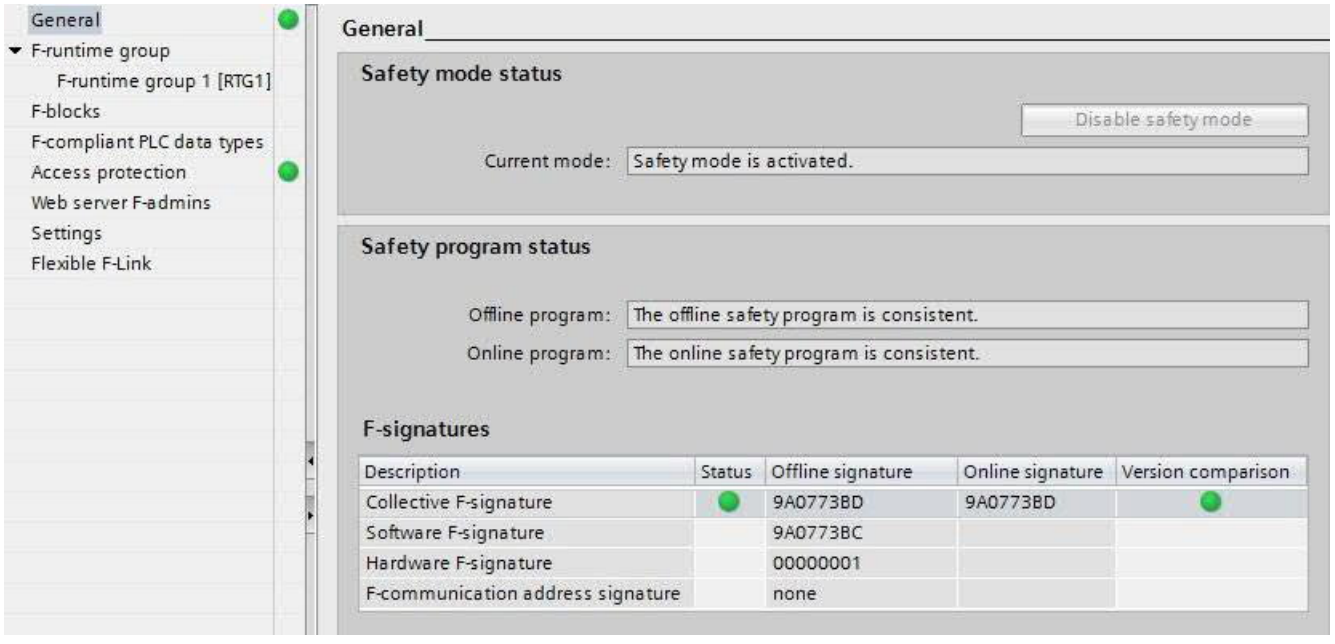
Identyfikacja programu pozwala na określenie, czy do F-CPU pobrano właściwy program bezpieczeństwa. W tym celu należy porównać zbiorcze podpisy bezpieczeństwa programu bezpieczeństwa oraz przypisanie praw „administrator bezpieczeństwa" online z oczekiwanymi wartościami. Oczekiwaną wartością może być, przykładowo, zbiorczy podpis bezpieczeństwa programu offline z *Safety Administration Editor* lub z podsumowania bezpieczeństwa. Przypisanie praw „administratora bezpieczeństwa" należy sprawdzić w *Safety Administration Editor*.

Przy pomocy środków organizacyjnych, podczas identyfikacji programu należy upewnić się, że program bezpieczeństwa nie został pobrany przez inny TIA Portal (na innym urządzeniu programistycznym lub PC).

Za pomocą *Safety Administration Editor*

W przypadku identyfikacji programu za pomocą *Safety Administration Editor*, należy

1. Otworzyć *Safety Administration Editor* F-CPU, który ma zostać sprawdzony.
2. Połączyć się online z F-CPU, który ma zostać sprawdzony.
3. Porównać zbiorczy podpis bezpieczeństwa wyświetlany online z oczekiwaną wartością w dziale „General" (Ogólne).
4. Sprawdzić, czy programy offline i online są spójne (strona 393).
5. Sprawdzić, czy w kolumnie „status" oraz „Version comparison" (Porównanie wersji) wyświetlany jest zielony symbol.



6. Sprawdzić w dziale „Web server F-admins" (Administratorzy bezpieczeństwa serwera sieciowego), czy jedynie upoważnieni użytkownicy mają dostęp do praw „administrator bezpieczeństwa" offline i online.

Za

W przypadku identyfikacji programu za pomocą HMI, należy wykonać następujące kroki:

1. Odczytać zbiorczy podpis bezpieczeństwa programu bezpieczeństwa z taga F_PROG_SIG globalnego F-DB (strona 157) (S7-300, S7-400) lub taga F_SYSINFO.F_PROG_SIG DB informacji o grupie F-runtime (strona 158) (S7-1200, S7-1500).
2. Należy porównać wartość taga F_PROG_SIG z oczekiwaną wartością.

Za pomocą wyświetlacza F-CPU S7-1500

W przypadku identyfikacji programu za pomocą wyświetlacza na CPU, należy wykonać następujące kroki:

1. W menu wyświetlacza należy przejść do „Overview > Fail-safe" (Przegląd > Fail-safe).
2. Porównać wyświetlony zbiorczy podpis bezpieczeństwa z oczekiwaną wartością.

Za pomocą serwera sieciowego F-CPU S7-1200/1500

W przypadku identyfikacji programu za pomocą serwera sieciowego CPU S7-1200/1500, należy wykonać następujące kroki:

1. Odczytać zbiorczy podpis bezpieczeństwa na stronie domowej serwera sieciowego.
2. Porównać wyświetlony zbiorczy podpis bezpieczeństwa z oczekiwaną wartością.

Zobacz także

Safety Administration Editor (strona 79)

10.5 Porównywanie programów bezpieczeństwa

Porównywanie programów bezpieczeństwa jak w wersji standardowej

Za pomocą *edytora porównania* w *STEP 7* można wykonać porównanie offline-online lub offline-offline dla programów bezpieczeństwa. Procedura jest identyczna jak dla standardowego programu użytkownika. Zawartość bloków bezpieczeństwa również jest porównywana do porównania programów bezpieczeństwa. Wynik porównania offline-offline można zastosować do zatwierdzenia zmian (strona 396). Porównanie włącza się, zaznaczając kryterium porównania „Safety" (Bezpieczeństwo) i wyłączając inne kryteria porównania.

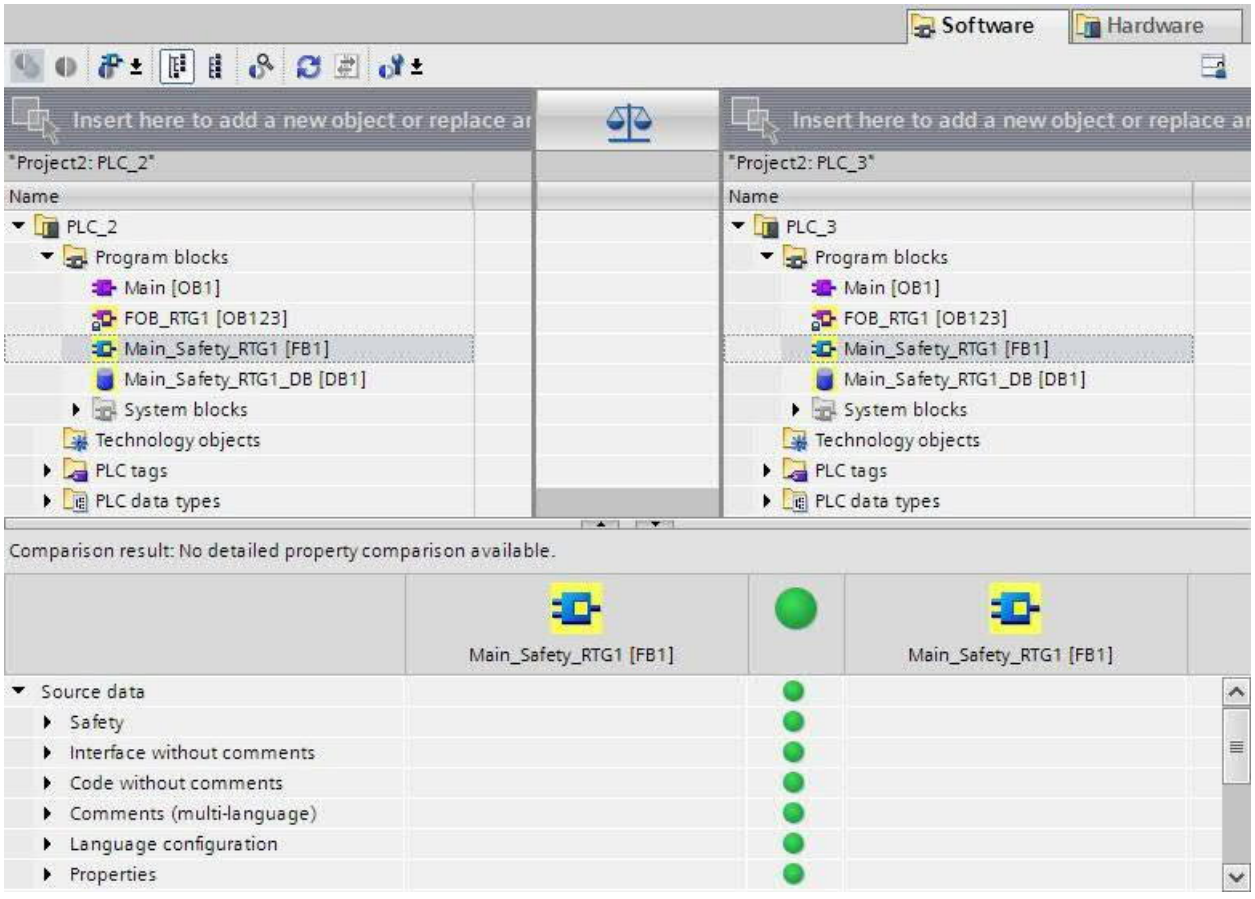
Uwaga

Nie należy wykorzystywać *edytora porównania* do wykrywania zmian offline-online w programie bezpieczeństwa/konfiguracji F-I/O podczas zatwierdzania zmian. Do tego celu służy jedynie porównanie offline-offline. Aby zaakceptować zmiany, należy wykonać czynności opisane w dziale „Zatwierdzenie zmian" (strona 396).

Wynik porównania dla programów bezpieczeństwa

Przedstawienie wyników porównania odpowiada przedstawieniu *STEP 7*.

Po kliknięciu na folder „Program blocks" (Bloki programu) po lewej stronie edytora porównania, widoczny jest zbiorczy podpis bezpieczeństwa programu bezpieczeństwa wyświetlanego pod hasłem „Comparison result" (Wynik porównania). Otrzymuje się informacje o tym, czy program bezpieczeństwa jest spójny.



Po kliknięciu na blok bezpieczeństwa, oprócz standardowych informacji, widoczny jest odnośny podpis oraz podpisy interfejsu.

Uwaga

W razie przerwania połączenia do F-CPU podczas porównania online/offline, jego wynik będzie niepoprawny.

Opcje filtra porównania

Za pomocą filtrów w *edytorze porównania* można ograniczyć wynik porównania do następujących grup bloków:

- Porównaj tylko bloki bezpieczeństwa
- Porównaj tylko bloki bezpieczeństwa istotne dla certyfikacji
- Porównaj jedynie bloki standardowe

Dostępne są również opcje filtra *STEP 7* , „Show only objects with differences" (Pokaż jedynie obiekty ze zmianami" oraz „Show identical and different objects" (Pokaż identyczne i różne obiekty).

Przy porównaniu programów bezpieczeństwa istotne są również bloki bezpieczeństwa w folderze „System blocks" (Bloki systemowe).

Kryteria porównania

Należy upewnić się, że pod jedynie kryterium porównania „Safety" jest aktywne.

Klasyfikacja wyświetlonych zmian

Niezależnie od tego, czy wykonano porównanie offline/online czy offline/offline, następujące zmiany mogą być wskazane jako zmian w automatycznie generowanych blokach bezpieczeństwa:

- Zmiana w maksymalnym czasie cyklu grupy F-runtime oraz czasie cyklu ostrzeżenia grupy F-runtime
- Zmiana w parametrach bezpieczeństwa dla F-CPU
- zmieniona wersja systemu bezpieczeństwa lub zmiana w konfiguracji sprzętowej (S7-1200/1500: Wyświetlana jako zmiana bloku „F_SystemInfo_DB").
- (S7-300/400) Zmiana w komunikacji grupy F-runtime, przykładowo, zmiana liczby DB do komunikacji grupy F-runtime
- Zmiana w głównym bloku bezpieczeństwa, F-FB, F-FC, F-DB
- Zmiana w konfiguracji sprzętowej dla F-I/O adresowanego w programie bezpieczeństwa

Możliwe jest, że blok jest wyświetlany jako zmieniony, lecz żadne zmiany nie zostały wyświetlone w szczegółowym porównaniu zawartości bloku. Nie jest to problem z wyświetlaniem, lecz oznacza, że zmiany, przykładowo, adresów w tabeli tagów, mają wpływ na ten blok. W razie wątpliwości należy przetestować ten blok.

Drukowanie wyniku porównania

Wynik porównania można wydrukować za pomocą opcji „Project > Print" (Projekt > Drukuj) w pasku menu lub korzystając z przycisku druku na pasku narzędziowym. Wybrać „Print objects/area", „All" (Drukuj obiekty/obszar, Wszystko) oraz „Properties", „All" (Właściwości, Wszystko).

Należy upewnić się, że wszystkie strony zostały wydrukowane w całości. Niekompletne wydruki (np. z powodu niskiego poziomu tuszu) nie mogą zostać wykorzystane do zatwierdzenia zmian.

10.6 Drukowanie danych projektu

Drukowanie

Możliwe jest wydrukowanie wszystkich istotnych danych projektu (konfiguracja sprzętowa dla F-CPU i F-I/O, program bezpieczeństwa). Uzyskuje się tym „podsumowanie bezpieczeństwa", które, wraz z dokumentacją, stanowi podstawę do badania poprawności poszczególnych elementów systemu.

Poprawność jest warunkiem wstępnym dla zatwierdzenia systemu.

Specyfikacja zbiorczego podpisu bezpieczeństwa w stopce wydruku zapewnia, iż wydruk jest jednoznacznie powiązany z programem bezpieczeństwa.

Podsumowanie bezpieczeństwa

Podsumowanie bezpieczeństwa zapewnia dokumentację danych projektu związanych z bezpieczeństwem, pomagającą wykonać zatwierdzenie systemu.

Procedura tworzenia podsumowania bezpieczeństwa

Aby utworzyć podsumowanie bezpieczeństwa,

1. W drzewku projektu należy wybrać *Safety Administration Editor* F-CPU, dla którego ma zostać utworzone podsumowanie bezpieczeństwa.
2. Wybrać opcję „Print" (Drukuj) w menu „Project > Print" (Projekt > Drukuj) w pasku menu lub korzystając z przycisku druku na pasku narzędziowym.

   W wyświetlonym oknie można wprowadzić ustawienia układu wydruku oraz, między innymi, określić jego zakres (wszystko/podzbiór).
3. W „Document information" (Informacje dokumentu) należy wybrać jeden z formatów ISO, np. „DocuInfo_ISO_A4_Portait".
4. Należy wybrać opcję „All" (Wszystko), jeśli na wydruku mają zostać przedstawione bloki bezpieczeństwa i rodzaje danych PLC zgodne z bezpieczeństwem. Jest to konieczne, do udokumentowania kodu programu do zatwierdzenia (patrz „Zatwierdzenie systemu" (strona 376)). Wybrać opcję „Compact" (Kompaktowy), by wykluczyć kod źródłowy z wydruku.
5. Kliknąć na przycisk „Print" (Drukuj).

W wyniku otrzymuje się podsumowanie bezpieczeństwa dla F-CPU.

Należy upewnić się, że wszystkie strony zostały wydrukowane w całości. Niekompletne wydruki (np. z powodu niskiego poziomu tuszu) nie mogą zostać wykorzystane do zatwierdzenia zmian.

Zawartość podsumowania w omówieniu

Zagadnienia ujęte w podsumowaniu obejmują następujące elementy:

- Ogólne informacje dotyczące identyfikacji programu, podpisów, wersji oprogramowania, ustawień programu bezpieczeństwa (z obszaru roboczego „Settings" (Ustawienia) w *Safety Administration Editor*), na przykład wersja systemu bezpieczeństwa.
- Elementy biblioteki systemowej użyte w programie bezpieczeństwa (z karty zadań „Instructions" (Instrukcje)) wraz z ich wersjami
- Informacje o grupach F-runtime (np. limit ostrzeżenia czasu cyklu grupy F-runtime, maksymalny czas cyklu grupy F-runtime)
- Lista bloków bezpieczeństwa w folderze „Program blocks" (Bloki programu) (np. nazwa, funkcja, powiązana grupa F-runtime, podpis)
- (S7-1200, S7-1500) Lista bloków bezpieczeństwa chronionej wiedzy technologicznej zastosowanych w programie bezpieczeństwa (np. nazwa, podpis, stosowana wersja systemu bezpieczeństwa, stosowane instrukcje lub wywoływane bloki bezpieczeństwa).
- (S7-1200, S7-1500) Lista rodzaju danych PLC zgodnych z bezpieczeństwem (UDT), jeśli występują one w programie bezpieczeństwa.
- Dane ze standardowego programu użytkownika, oceniane w programie bezpieczeństwa
- Parametry bloku komunikacji CPU safety – CPU
- (S7-300, S7-400) Adresy bezwzględne i nazwy tagów DB współdzielonych typu F, do których dostęp jest możliwy ze standardowego programu użytkownika
- Informacje o sprzęcie (stosowane F-I/O, wersja CPU, adresy)
- Informacje dotyczące wydruku (data wydruku, liczba stron)

Zawartość stopki wydruku

Na podstawie stopki wydruku można określić:

- Czy wydrukowane dane projektu safety są spójne oraz czy wszystkie strony należą do tego samego programu i tej samej wersji (ten sam zbiorczy podpis bezpieczeństwa: w stopce na każdej stronie oznacza, że wydruk należy do jednego programu bezpieczeństwa z tym zbiorczym podpisem).

Stopka jest dodawana do kodu źródłowego bloków bezpieczeństwa tylko jeśli zaznaczono opcję „All" (Wszystkie) w podsumowaniu bezpieczeństwa.

Jeśli bloki bezpieczeństwa zostaną wydrukowane w inny sposób, stopka jest pomijana, przez co nie jest możliwe łatwe zidentyfikowanie, czy wydruk bloku należy do bieżącej wersji programu.

Drukowanie migrowanego projektu

Wydrukowanie podsumowania bezpieczeństwa dla projektu migrowanego z *S7 Distributed Safety V5.4 SP5* jest możliwe jedynie, jeśli projekt został skompilowany przy pomocy *STEP 7 Safety Advanced,* a struktura nowego programu (główny blok bezpieczeństwa) została w ten sposób zatwierdzona. W przeciwnym razie wydruk nie jest możliwy i wystąpi odpowiedni komunikat błędu.

Zaleca się wydrukowanie projektu w *S7 Distributed Safety V5.4 SP5* przed wykonaniem migracji.

10.7 Testowanie programu bezpieczeństwa

10.7.1 Przegląd testowania programu bezpieczeństwa

Kompletny test funkcji lub test zmian

Po utworzeniu programu bezpieczeństwa należy wykonać kompletny test funkcji zgodnie z zadaniem automatyzacji.

W przypadku zmian wprowadzonych w programie bezpieczeństwa, który przeszedł już kompletny test funkcji, wymagane jest sprawdzenie jedynie tych zmian oraz upewnienie się, że nie mają one wpływu na inne części programu.

Monitorowanie

Funkcje testu tylko do odczytu (takie jak monitorowanie tagów programu bezpieczeństwa) są dostępne standardowo dla programów.

Modyfikacja

Funkcje testu odczytu i zapisu (takie jak kontrolowanie tagów programu bezpieczeństwa) są dostępne w ograniczonym zakresie dla programów i tylko przy wyłączonym trybie bezpieczeństwa.

Symulacja poprzez *S7-PLCSIM*

Przy pomocy *S7-PLCSIM* można przetestować program bezpieczeństwa. Obsługa *S7-PLCSIM* przebiega identycznie jak dla standardowego programu użytkownika.

Symulację w *S7-PLCSIM* uruchamia się za pomocą elementu „Online > Simulation > Start"

(Online > Symulacja > Start).

Zasady testowania

- Wymuszenie wejść i wyjść F-I/O nie jest możliwe.
- Kontrolowanie wyjść F-I/O w połączeniu z funkcją „Enabling F-I/O outputs" (Aktywacja wyjść F-I/O) nie jest możliwe.
- Ustawienie punktów przerwania w standardowym programie użytkownika spowoduje błędy w programie bezpieczeństwa (zobacz także „Testowanie programu bezpieczeństwa" (strona 363)).
- Zmiany w konfiguracji F-I/O lub komunikacji CPU safety – CPU można przetestować jedynie po zapisaniu i pobraniu konfiguracji sprzętowej, oraz po tym, jak program bezpieczeństwa został skompilowany i pobrany do F-CPU.

Zobacz także

Wyłączanie trybu bezpieczeństwa (strona 360)

10.7.2 Wyłączanie trybu bezpieczeństwa

Wstęp

Program bezpieczeństwa zazwyczaj działa F-CPU w trybie bezpieczeństwa. Oznacza to, że wszystkie środki kontroli awarii są aktywne. W trybie bezpieczeństwa nie jest możliwa modyfikacja programu bezpieczeństwa podczas pracy (w trybie RUN). Należy wyłączyć tryb bezpieczeństwa, by, przykładowo, zmodyfikować tagi w programie bezpieczeństwa w trybie RUN. Tryb bezpieczeństwa pozostaje wyłączony do czasu, aż F-CPU zostanie ponownie przełączony z trybu STOP do RUN.

Zasady wyłączania trybu bezpieczeństwa

OSTRZEŻENIE

Jako że zmiany w programie bezpieczeństwa można wykonać w trybie RUN, gdy tryb bezpieczeństwa jest wyłączony, należy uwzględnić następujące zagadnienia:

- Wyłączenie trybu bezpieczeństwa jest przeznaczone do celów testowych, odbioru technicznego itp. Gdy jest on wyłączony, bezpieczeństwo systemu należy zagwarantować innymi środkami organizacyjnymi, takimi jak monitorowana praca, ręczne wyłączenie bezpieczeństwa oraz ograniczenia dostępu do określonych obszarów.
- Wyłączenie trybu bezpieczeństwa musi zostać wyświetlone.

  Należy użyć taga MODE w globalnym F-DB ("F_GLOBDB".MODE) do F-CPU S7-300/400 lub w DB informacji o grupie F-runtime (np. RTG1SysInfo.F_SYSINFO.MODE) do F-CPU S7-1200/1500, które pozwalają na ocenę odczytu trybu roboczego (1 = wyłączony tryb bezpieczeństwa). Oznacza to nie tylko, że wyłączony tryb bezpieczeństwa jest wyświetlany na urządzeniu programistycznym lub PC w oknie wyłączenia trybu bezpieczeństwa, lecz jest także wskazywane za pomocą lampki sygnalizacyjnej sterowanej przez standardowy program użytkownika lub przy pomocy komunikatu do systemu HMI generowanego poprzez ocenę wspomnianego wyżej taga „Wyłączony tryb bezpieczeństwa" w DB współdzielonym typu F.
- Musi być możliwe zweryfikowanie, czy tryb bezpieczeństwa został wyłączony. Wymagany jest rejestr, jeśli to możliwe, rejestrujący i archiwizujący alarmy systemu kontroli operatorskiej i monitorowania, lub, jeśli to konieczne, rejestr w postaci środków organizacyjnych. Ponadto zaleca się, by wyłączenie trybu bezpieczeństwa było wskazywane w systemie HMI.
- Tryb bezpieczeństwa jest wyłączany w obrębie całego F-CPU. Należy jednakże uwzględnić następujące elementy w komunikacji CPU safety – CPU: Jeśli F-CPU wysyłający dane ma wyłączony tryb bezpieczeństwa, nie można zakładać, że wysyłane dane są generowane w bezpieczny sposób. Należy zapewnić bezpieczeństwo w tych jednostkach, na które wpływają wysyłane dane, stosują środki organizacyjne lub wyprowadzić bezpieczne wartości zastępcze zamiast otrzymywanych danych, wykonując ocenę SENDMODE*.

* SENDMODE jest dostępny jako wyjście instrukcji RCVDP lub RCVS7 w przypadku komunikacji poprzez Flexible F-Link jako tag w DB komunikacji bezpieczeństwa.

(S027)

Procedura wyłączania trybu bezpieczeństwa

Aby wyłączyć program bezpieczeństwa,

1. Otworzyć *Safety Administration Editor* dla odnośnego F-CPU.
2. Otworzyć obszar roboczy „General" (Ogólne) (strona 82) w nawigacji obszaru.
3. Sprawdzić, czy status trybu bezpieczeństwa jest wyświetlany jako aktywny.

   Jeśli tak, należy przejść do następnego kroku; jeśli nie, należy zatrzymać proces, ponieważ tryb bezpieczeństwa jest już wyłączony lub nie można go wyłączyć.
4. Kliknąć na przycisk „Disable safety mode" (Wyłącz tryb bezpieczeństwa).
5. Wprowadzić hasło do programu bezpieczeństwa online.

   Po wpisaniu właściwego hasła pojawi się kolejne okno, zawierające zbiorczy podpis bezpieczeństwa w F-CPU. Należy sprawdzić, czy jest to spodziewany podpis. Jeśli są zgodne, należy zatwierdzić okno.
6. Wprowadzić hasło dla F-CPU.

   Po wpisaniu właściwego hasła dla F-CPU, tryb bezpieczeństwa zostanie wyłączony.

   Jeśli hasło jest nieprawidłowe, tryb bezpieczeństwa pozostanie aktywny.

   (S7-300, S7-400) W przypadku pobierania poszczególnych bloków bezpieczeństwa, warunek „Disable safety mode" (Wyłącz tryb bezpieczeństwa) jest automatycznie umieszczany w oknie „Load preview" (Podgląd wczytywania). Z tego względu nie jest konieczne odrębne wyłączanie trybu bezpieczeństwa przed pobraniem każdego bloku bezpieczeństwa.

Uwaga

Jeśli zbiorczy podpis bezpieczeństwa lub hasła nie są zgodne dla programu bezpieczeństwa online i offline, oznacza to że:

- Program bezpieczeństwa offline został zmodyfikowany po ostatnim pobraniu, lub
- Zaadresowano niewłaściwy F-CPU. Należy sprawdzić drugą kwestię w zbiorczym podpisie bezpieczeństwa online.

Włączanie trybu bezpieczeństwa

Uwaga

Aby włączyć tryb bezpieczeństwa, F-CPU musi przełączyć się z trybu STOP na RUN.

Przełączenie F-CPU z trybu STOP na RUN zawsze włącza tryb bezpieczeństwa, nawet jeśli program bezpieczeństwa został zmodyfikowany lub nie jest spójny. Tag MODE w DB współdzielonym bezpieczeństwa dla F-CPU S7-300/400 lub DB informacji grupy F-runtime jest ustawiany na „0" dla F-CPU S7-1200/1500.

Jeśli zmieniono program bezpieczeństwa, lecz nie skompilowano i pobrano go, F-CPU może wrócić do trybu STOP.

Ocena trybu bezpieczeństwa/wyłączonego trybu bezpieczeństwa

Aby ocenić tryb bezpieczeństwa/wyłączony tryb bezpieczeństwa w programie bezpieczeństwa, można wykonać ocenę taga „MODE" w DB współdzielonym typu F dla F-CPU S7-300/400 lub DB informacji o grupie F-runtime dla F-CPU S7-1200/1500 (1 = wyłączony tryb bezpieczeństwa). Dostęp do tego taga jest możliwy poprzez w pełni kwalifikowany dostęp (np. "F_GLOBDB".MODE lub RTG1SysInfo.MODE).

Ocena ta pozwala, przykładowo, na pasywowanie F-I/O gdy program bezpieczeństwa jest wyłączonym trybie bezpieczeństwa. W tym celu należy przypisać tag „MODE" w DB współdzielonym typu F lub DB informacji o grupie F-runtime do wszystkich tagów „PASS_ON" w DB tego F-I/O, który ma zostać pasywowany.

OSTRZEŻENIE

Gdy program bezpieczeństwa jest w wyłączonym trybie bezpieczeństwa, znacznik „MODE" w DB współdzielonym typu F lub DB informacji o grupie F-runtime również jest oceniany w tym trybie.

Nawet jeśli F-I/O są pasywowane przy wyłączonym trybie bezpieczeństwa wskutek oceny znacznika „MODE", należy zapewnić, że system jest w wyłączonym trybie bezpieczeństwa poprzez inne środki organizacyjne, takie jak monitorowanie pracy czy ręczne wyłączenie bezpieczeństwa. *(S028)*

Zobacz także

DB współdzielone bezpieczeństwa (S7-300, S7-400) (strona 157)

DB informacji grupy F-runtime (S7-1200, S7-1500) (strona 158)

Komunikacja (strona 631)

10.7.3 Testowanie programu bezpieczeństwa

Wstęp

Tagi programu bezpieczeństwa można monitorować w dowolnej chwili.

Kontrolowanie tagów programu bezpieczeństwa jest możliwe tylko przy wyłączonym trybie bezpieczeństwa, jako że niektóre domyślne środki kontroli programu muszą być do tego celu wyłączone.

Możliwe jest kontrolowanie następujących tagów programu bezpieczeństwa:

- Wejścia i wyjścia F-I/O (wartości kanałów i stan wartości (S7-1200, S7-1500))
- Tagi w globalnym F-DB (za wyjątkiem DB do komunikacji grupy F-runtime)
- Tagi w instancji DB do F-FB
- Tagi w DB F-I/O (dozwolone tagi, patrz „F-I/O DB" (strona 174))

Procedura monitorowania tagów programu bezpieczeństwa

Monitorowanie wymaganych tagów programu bezpieczeństwa jest możliwa z otwartej tabeli kontroli lub z

edytora programu (status programu).

1. Należy postępować jak standardowym programie. Dodatkowe informacje można znaleźć w *pomocy do STEP 7* pod hasłem „Testowanie programów użytkownika".

Procedura kontrolowania tagów programu bezpieczeństwa

Kontrola wymaganych tagów programu bezpieczeństwa jest możliwa z otwartej tabeli kontroli:

1. Do modyfikacji, należy wyłączyć tryb bezpieczeństwa (strona 360) a automatycznie otwieranym oknie.
2. Należy zakończyć istniejące polecenia modyfikacji po zakończeniu testowania, nim uruchomi się tryb bezpieczeństwa.

Wartość w F-DB można modyfikować tylko online w F-CPU. Jeśli wartość należy również zmienić offline, należy zrobić to, edytując wartość początkową offline i kompilując program bezpieczeństwa.

W przypadku kontroli tagów F-I/O należy wykonać co następuje:

1. Utworzyć oddzielny wiersz dla każdej wartości kanału oraz stanu wartości (S7-1200, S7-1500) do zmodyfikowania. Wartość kontrolna musi odpowiadać wartości kanału lub stanowi wartości.
2. Ustawić „start of scan cycle" (start cyklu skanowania) lub „end of scan cycle" (koniec cyklu skanowania) oraz „permanent" (stały) lub „once" (raz).

   Niezależnie od ustawionego punktu wyzwolenia, polecenia modyfikacji wejść (PII) w F-I/O zawsze aktywują się przed wykonaniem głównego bloku bezpieczeństwa, zaś polecenia modyfikacji wyjść (PIQ) aktywują się po wykonaniu głównego bloku bezpieczeństwa.
3. (S7-300, S7-400) Należy utworzyć dodatkową tabelę kontroli, jeśli nadzorem ma być objętych więcej niż 5 wejść/wyjść.

Uwaga

F-I/O można modyfikować tylko w trybie RUN F-CPU.

Nie jest możliwe zmodyfikowanie skonfigurowanego F-I/O, z którego wartość kanału, stan wartości (S7-1200, S7-1500) lub dowolny tag z powiązanego DB F-I/O został użyty w programie bezpieczeństwa. W programie bezpieczeństwa należy używać co najmniej jednego taga z powiązanego DB F-I/O lub co najmniej jednej wartości kanału lub stanu wartości (S7-1200, S7-1500) z F-I/O, który ma zostać zmodyfikowany.

Dla wejść (PII), polecenia modyfikacji mają pierwszeństwo na wyjściem wartości fail-safe, zaś dla wyjść (PIQ), wartość fail-safe ma pierwszeństwo nad poleceniami modyfikacji. Dla wyjść (kanałów), które nie zostały aktywowane we właściwościach F-I/O, polecenia modyfikacji wpływają tylko na PIQ, nie na F-I/O.

Uwaga

Poniższe zagadnienia dotyczą F-CPU S7-1200/1500:

Aby uniknąć niedozwolonych połączeń wartości kanału i stanu

- Stan wartości jest ustawiany automatycznie przez system bezpieczeństwa na 1 podczas ustawiania wartości kanału na wartość <> wartość fail-safe 0
- Wartość fail-safe 0 jest ustawiana automatycznie na wyjście po ustawieniu stanu wartości na 0 w powiązanej wartości kanału

---

⚠ OSTRZEŻENIE

Należy konkretnie zresetować polecenia modyfikacji stałych w tabeli nadzoru przy wyłączonym trybie bezpieczeństwa.

Należy pamiętać, że polecenia modyfikacji stałych, które nie zostaną poprawnie zresetowane, mogą pozostać aktywne w tle nawet po przejściu F-CPU z trybu STOP na RUN.

Ze względu na to, że F-CPU ponownie jest w trybie bezpieczeństwa po przejściu STOP/RUN, polecenia modyfikacji stałych już nie obowiązują i nie są widoczne w tabeli nadzoru.

Polecenie aktywuje się przy ponownym wyłączeniu trybu bezpieczeństwa.

Za pomocą resetu pamięci F-CPU można upewnić się, że żadne polecenie nie pozostało aktywne w tle. *(S029)*

Test okablowania przy pomocy tabeli nadzoru

Test okablowania dla wejścia można wykonać, zmieniając sygnał wejściowy sprawdzając, czy nowa wartość pojawi się na PII.

Test okablowania dla wyjścia można wykonać, zmieniając wyjście za pomocą funkcji

„Modify" (Modyfikuj) i sprawdzając, czy wymagany element wykonawczy zareagował na to.

Podczas testu okablowania należy pamiętać, ze program bezpieczeństwa musi działać na F-CPU, z co najmniej jedną wartością kanału lub stanem wartości (S7-1200, S7-1500) na monitorowanym F-I/O; można także zastosować tag z powiązanego DB F-I/O.

W przypadku F-I/O, które mogą działać również jako standardowe I/O (np. moduły sygnałowe typu fail-safe S7-300), możliwe jest także wykonanie test okablowania dla wyjść, stosując funkcję „Modify" (Modyfikuj) w trybie STOP, obsługują F-I/O jak standardowy I/O zamiast w trybie bezpieczeństwa.

Dodatkowe zasady testowania (S7-300/400/1500)

Ustawienie punktów przerwania w standardowym programie użytkownika spowoduje wystąpienie następujących błędów w programie bezpieczeństwa:

- Przekroczenie monitorowanie czasu cyklu bezpieczeństwa
- Błąd podczas komunikacji z F-I/O

  (S7-1500) Moduły fail-safe przełączą się w tryb bezpieczeństwa po upłynięciu zadanego czasu monitorowania bezpieczeństwa.
- Błąd podczas komunikacji CPU związany z
- bezpieczeństwem – CPU Wewnętrzna awaria CPU

Aby mimo to użyć punktów przerwania do testu, należy najpierw wyłączyć tryb bezpieczeństwa. Będzie skutkować to następującymi błędami:

- Błąd podczas komunikacji z F-I/O
- Błąd podczas komunikacji CPU safety – CPU Różnica

pomiędzy F-CPU S7-1500 a F-CPU S7-300/400:

- Jeśli punkt przerwania zostanie aktywowany i osiągnięty, F-CPU przejdzie bezpośrednio

  w tryb STOP po trybie HOLD.
- Aby przełączyć go na tryb RUN po trybie HOLD w celu dalszego testowania standardowego programu użytkownika, można zasymulować to w S7-PLCSIM.

Brak ochrony dostępu jest wstępnie konieczny do celów testów, odbioru technicznego itp. Oznacza to, że można wykonywać wszelkie czynności offline i online bez ochrony, tj. bez wpisywania hasła.

Zobacz także

„Zmiana programu bezpieczeństwa w trybie RUN (S7-300, S7-400)" (strona 371);

Pobieranie danych projektu do F-CPU (strona 325)

10.7.4 Testowanie programu bezpieczeństwa z S7-PLCSIM

Program bezpieczeństwa można przetestować wraz ze standardowym programem przy pomocy symulowanego CPU w *S7-PLCSIM*, bez konieczności posiadania sprzętu. Należy zwrócić uwagę na ostrzeżenie S030 w dziale „Uwagi dotyczące trybu bezpieczeństwa programu bezpieczeństwa" (strona 401).

Obsługa *S7-PLCSIM* do systemów bezpieczeństwa SIMATIC Safety przebiega identycznie jak w przypadku standardowych systemów S7. Należy mieć na uwadze następujące specjalne elementy:

Tryb bezpieczeństwa/wyłączony tryb bezpieczeństwa

Zaleca się, by wykonać test programu bezpieczeństwa w trybie bezpieczeństwa, by wykryć, czy F-CPU przechodzi w tryb STOP w fazie testowej programu w *S7-PLCSIM* wskutek, przykładowo, wyników instrukcji, które znalazły się poza dopuszczalnym zakresem dla rodzaju danych.

Poniższą symulację można wykonać w *S7-PLCSIM*, tak jak na rzeczywistym F-CPU, z wyłączonym trybem bezpieczeństwa.

- Modyfikacja tagów w F-DB i DB F-I/O.

F-CPU może przejść w stan STOP w *S7-PLCSIM*, jeśli ten wymóg zostanie pominięty. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

(S7-1200, S7-1500) Aby nie dopuścić do niezamierzonej modyfikacji tagów w F-DB i DB F-I/O w trybie bezpieczeństwa, zaleca się, by nie korzystać z przycisku „Activate/deactivate modification of non-inputs

(Włącz/wyłącz modyfikację elementów innych niż wejścia) w *S7-PLCSIM*

Podczas symulacji w *S7-PLCSIM* , monitorowanie maksymalnego czasu cyklu grupy F-runtime oraz limit ostrzeżenie czasu cyklu grupy F-runtime (S7-1200, S7-1500) są wyłączone.

Symulacja wejść F-I/O

Modyfikacja wejść (wartości kanałów) w *S7-PLCSIM:*

Wejścia (wartości kanałów) w F-I/O modyfikuje się tak jak wejścia w standardowym I/O w *S7-PLCSIM*.

Modyfikacja wejść (stan wartości) w *S7-PLCSIM:*

(S7-1200, S7-1500) Poprzez modyfikację wejść (stany wartości) w F-I/O można zasymulować wchodzące i wychodzące awarie kanałów/F-I/O. Należy pamiętać o następujących uwagach/ograniczeniach:

- Aby realistycznie symulować zachowanie F-I/O, należy zwrócić uwagę na połączenie pomiędzy wartością kanału a stanem wartości rzeczywistego F-I/O. Połączenie stan wartości = 0 oraz wartość kanału <> wartość fail-safe (0) jest nieprawidłowa, przez co wynik symulacji będzie odbiegać od zachowania rzeczywistego F-CPU.
- Podczas przejścia CPU ze STOP do RUN w *S7-PLCSIM*, wszystkie wejścia F-I/O (stany wartości) są inicjowane z 1. Oznacza to, że można rozpocząć modyfikację wejść (wartości kanałów) bez symulowania wejść (stanu wartości).
- Modyfikacja wejść (stan wartości) w *S7-PLCSIM* nie ma wpływu na tagi QBAD i PASS_OUT w DB F-I/O. Należy pamiętać, że w rzeczywistych F-I/O, QBAD i PASS_OUT mogą przybrać wartość 1 niezwłocznie po osiągnięciu stanu wartości 0 na co najmniej jednym kanale F-I/O. (patrz tagi do DB F-I/O: PASS_OUT/QBAD/QBAD_I_xx/QBAD_O_xx oraz stan wartości (strona 181)).
- Dla F-I/O skonfigurowanego z „Zachowanie po usterce kanału" = „Pasywacja kompletnego F-I/O", należy użyć tag PASS_ON w DB F-I/O do symulacji pasywacji kompletnego F-I/O w przypadku awarii kanału / F-I/O. Pasywacja jedynie poszczególnych wejść (wartość kanału obejmująca stan wartości) w symulacji, zachowanie symulacji będzie odbiegać od rzeczywistego F-CPU.
- Możliwe jest również użycie taga PASS_ON w DB F-I/O DB do F-I/O bez stanu wartości do symulowania pasywacji całego F-I/O w przypadku awarii F-I/O lub kanału.
- Należy zmodyfikować wejścia (wartość kanału) na $7FFF_H$ (dla przekroczenia wartości) lub 8000_H (dla niedostatecznej wartości), by zasymulować awarię F-I/O / kanału SM 336; AI 6 x 13Bit lub SM 336; F-AI 6 x 0/4...20 mA HART z konfiguracją „Zachowanie po usterce kanału" = „Pasywuj kanał".
- W przypadku F-I/O, który nie obsługuje profilu „RIOforFA-Safety", należy wykonać zatwierdzenie z dodatnim zboczem na tagu ACK_REI DB F-I/O, tak jak w rzeczywistym F-I/O, by wykonać reintegrację po zmianie stanu wartości z 0 na 1 lu gdy wartość kanału uległa zmianie z $7FFF_H/8000_H$ na nierówność $7FFF_H/8000_H$ (patrz powyżej), gdy ACK_NEC = 1 dla DB F-I/O. Reintegracja odbywa się automatycznie we wszystkich innych przypadkach mogących wynikać z rzeczywistego F-I/O.

Czasy aktualizacji

Należy pamiętać, że stan wejść (wartości kanałów lub stan wartości (S7-1200/1500)) monitorowany w tabeli SIM w *S7-PLCSIM* jest jedynie identyczny ze stanem przetwarzanym w programie bezpieczeństwa, jeśli nastąpiła pasywacja powiązanego F-I/O.

Przy pasywacji F-I/O, program bezpieczeństwa operuje na wartościach fail-safe (wartość kanału oraz stan wartości (S7-1200/1500) = 0).

Instrukcje do komunikacji pomiędzy F-CPU

Poniższe zagadnienia dotyczą instrukcji SENDDP/RCVDP (S7-300/400) oraz instrukcji SENDDP/RCVDP w wersji < 3.0 (S7-1200/1500):

Nie jest możliwe zasymulowanie komunikacji pomiędzy F-CPU z instrukcjami SENDDP i RCVDP w *S7-PLCSIM*. Można jednakże użyć instrukcji SENDDP i RCVDP w połączeniu z *S7-PLCSIM*. Podczas symulacji w *S7-PLCSIMW* instrukcja RCVDP wyprowadza wartości fail-safe oczekujące na jej wejściach SUBBO_xx oraz SUBI_xx ((S7-1200/1500) lub alternatywnie SUBDI_00). Instrukcje SENDDP i RCVDP sygnalizują to wartością 1 na wyjściu SUBS_ON.

W przypadku instrukcji SENDDP/RCVDP o wersji >= 3.0, mają zastosowanie poniższe

zasady:

Podczas symulacji w *S7-PLCSIM* możliwe jest zasymulowanie danych otrzymywanych oraz informacji „Wyłączony tryb bezpieczeństwa" (RCVDP) lub kolejno informacji „Wyjście wartości zastępczych" (SENDDP) w odpowiednich obszarach transferu dla wejść. Należy mieć na uwadze poniższe uwagi:

- Symulowane wartości nie są aktywne do czasu ustawienia po raz pierwszy bitu SIMULATION w odnośnym słowie kontroli symulacji (patrz poniższa tabela) po uruchomieniu systemu bezpieczeństwa. Przed ustawieniem bitu SIMULATION instrukcja RCVDP wyprowadza wartości fail-safe oczekujące na jej wejściach SUBBO_xx oraz SUBI_yy ((S7-1200/1500) lub alternatywnie SUBDI_00).
- Ustawienie bitu SEND_MODE w słowie kontroli symulacji spowoduje ustawienie wyjścia SENDMORE dla instrukcji RCVDP.
- Ustawienie bitu STATUS_SUBS w słowie kontroli symulacji spowoduje ustawienie wyjścia SUBS_ON dla instrukcji SENDDP.
- Bity zarezerwowane w słowie kontrolnym symulacji zawsze muszą być 0.
- Podczas przejścia STOP/RUN z *S7-PLCSIM*, zachowywane są najczęściej symulowane wartości w obszarze transferu dla wejść.

Adres(y) początkowy(e) skonfigurowanego obszaru transferu dla danych wejściowych i wyjściowych można znaleźć w stosownej konfiguracji (zobacz również „Konfiguracja i programowanie komunikacji (S7-1200, S7-1500)" (strona 273)).

Tabela 10-1 Struktura odnośnego obszaru transferu dla wejść słowa kontrolnego symulacji (instrukcja RCVDP)

Bajt	Znaczenie	Komentarz
0	RD_BO_15 ... RD_BO_08	
1	RD_BO_07 ... RD_BO_00	
	DINTMODE=0:	
2	RD_I_00	Słowo RD_I_00, MSB[1] jako pierwsze
3		
4	RD_I_01	Słowo RD_I_01, MSB[1] jako pierwsze
5		
	Alternatywny DINTMODE=1:	
2	RD_DI_00	High Wordz RD_DI_00, MSB[1] jako pierwsze
3		
4		Low Word z RD_DI_00 **XOR 0x8000**, MSB[1] jako pierwsze
5		
6	Słowo sterujące symulacji (bajt wysoki)	Bit 0...6: Zastrzeżony Bit 7: SIMULATION: Aktywacja symulacji RCVDP
7	Słowo sterujące symulacji (bajt niski)	Bit 0: SEND_MODE: Wyjście ustawiające SENDMODE Bit 1...7: Zastrzeżony
8 ... 11	Zastrzeżony	

[1] MSB: najbardziej

Tabela 10-2 Struktura odnośnego obszaru transferu dla wejść słowa kontrolnego symulacji (instrukcja SENDDP)

Bajt	Znaczenie	Komentarz
0	Słowo sterujące symulacji (bajt wysoki)	Bit 0: STATUS_SUBS: Wyjście ustawiające SUBS_ON Bit 1...6: Zastrzeżony Bit 7: SIMULATION: Aktywacja symulacji SENDDP
1	Słowo sterujące symulacji (bajt niski)	Bit 0...7: Zastrzeżony
2 ... 5	Zastrzeżony	

OSTRZEŻENIE

W przypadku komunikacja CPU związany z bezpieczeństwem – CPU rodzaju Flexible F-Link należy uwzględnić następujące zagadnienia: Jeśli dane są wysyłane z F-CPU symulowanego za pomocą S7-PLCSIM, nie można zakładać, że dane są generowane w bezpieczny sposób. Należy następnie wdrożyć środki organizacyjne, takie jak monitorowanie pracy oraz ręczne wyłączenie bezpieczeństwa, by zapewnić bezpieczeństw w tych częściach systemu, na które wpływają wysyłane dane. Alternatywnie można wyprowadzić wartości zastępcze fail-safe zamiast odebranych danych w F-CPU, który otrzymuje dane, poprzez wykonanie oceny SENDMODE*.

* SENDMODE jest dostępny jako znacznik w DB komunikacji bezpieczeństwa.

(S086)

(S7-300, S7-400) Nie jest możliwe zasymulowanie komunikacji pomiędzy F-CPU z instrukcjami SENDS7 i RCVS7 w *S7-PLCSIM*. Można jednakże użyć instrukcji SENDS7 i RCVS7 w połączeniu z *S7-PLCSIM*.

Podczas symulacji w *S7-PLCSIM*, instrukcja RCVS7 wyprowadza wartości początkowe określone w DB komunikacji jako wartości fail-safe. Instrukcje SENDS7 i RCVS7 sygnalizują to wartością 1 na wyjściu SUBS_ON.

Niespójny program bezpieczeństwa (S7-1200, S7-1500)

Jeśli CPU przejdzie w tryb STOP w *S7-PLCSIM* z wpisem diagnostycznym „Safety program: inconsistent" (Program bezpieczeństwa: niespójny), F-CPU nie jest poprawnie inicjalizowany w *S7-PLCSIM*. Należy wykonać reset pamięci the F-CPU w *S7-PLCSIM* i pobrać ponownie program do CPU w *S7-PLCSIM*.

10.7.5 Zmiana programu bezpieczeństwa w trybie RUN (S7-300, S7-400)

Wstęp

Zmiany w programie bezpieczeństwa podczas pracy (w trybie RUN) są możliwe tylko przy wyłączonym trybie bezpieczeństwa (strona 360). Zmiany offline bloków bezpieczeństwa w *edytorze programu* wykonuje się identycznie jak przy standardowym programie. Nie jest możliwa zmiana bloków bezpieczeństwa online.

Uwaga

Jeśli zmiany w programie bezpieczeństwa **nie** mają być wykonywane podczas pracy, patrz „Tworzenie bloków bezpieczeństwa w FBD / LAD" (strona 160).

Procedura zmiany programu bezpieczeństwa w trybie RUN

Aby zmienić program bezpieczeństwa, należy

1. Zmiany w głównym bloku bezpieczeństwa lub F-FB i jego powiązanej instancji DB, F-FC lub F-DB należy wprowadzać w *edytorze programu*.
2. Pobrać zmieniony blok bezpieczeństwa do F-CPU (procedura, patrz „Pobieranie danych projektu do F-CPU (strona 325)). Cały program zostanie automatycznie skompilowany.
3. Jeśli tryb bezpieczeństwa jest aktywny, pojawi się okno „Load preview" (Podgląd wczytywania) z poleceniem wyłączenia trybu bezpieczeństwa i wprowadzenia hasła do programu bezpieczeństwa.

Uwaga

Podczas pobierania w wyłączonym trybie bezpieczeństwa, możliwe jest jedynie pobranie bloków fail-safe utworzonych przez użytkownika (główny blok bezpieczeństwa, F-FB, F-FC lub F-DB), bloków aplikacji bezpieczeństwa bądź standardowych bloków i ich powiązanych instancji DB. W przypadku pobrania automatycznie dodanych bloków bezpieczeństwa (F-DB lub automatycznie generowane bloki bezpieczeństwa oraz powiązane instancje DB, DB współdzielone typu F), F-CPU może przejść w tryb STOP lub uruchomi się tryb bezpieczeństwa.

Dlatego też należy wybierać poszczególne bloki jedynie podczas pobierania w wyłączonym trybie bezpieczeństwa.

Sekwencja do pobierania zmian

Zmiany w programie bezpieczeństwa w trybie RUN, gdy tryb bezpieczeństwa jest wyłączone, mogą, przykładowo, spowodować zmianę stanu elementu wykonawczego wskutek zmian w programie.

Po wprowadzeniu zmian należy zacząć od pobrania programu bezpieczeństwa, a następnie włączyć funkcję standardowego programu użytkownika monitorowaną przez program bezpieczeństwa.

Ograniczenia komunikacji CPU safety – CPU

Podczas pracy (w trybie RUN), nie można nawiązać nowej komunikacji CPU safety – CPU za pomocą nowych instrukcji SENDDP/RCVDP lub SENDS7/RCVS7.

Aby nawiązać nowe połączenie komunikacji CPU safety – CPU, zawsze należy pobrać odnośny program bezpieczeństwa w spójny sposób z F-CPU, gdy ten jest w trybie STOP, po wstawieniu nowej instrukcji SENDDP, SENDS7, RCVDP lub RCVS7.

Ograniczenia komunikacji grupy F-runtime

Nie można wprowadzać zmian w komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime w trybie RUN. Oznacza to, że nie jest możliwe przypisywanie, usuwanie lub zmiana żadnych DB dla komunikacji grupy F-runtime.

Po wprowadzeniu zmian w komunikacji grupy F-runtime, należy pobrać program bezpieczeństwa do F-CPU w trybie STOP.

Ograniczenia dostępu F-I/O

Jeśli podczas pracy (w trybie RUN) wstawi się dostęp F-I/O do F-I/O bez wartości pojedynczego kanału lub tag z powiązanego DB F-I/O został już użyty w programie bezpieczeństwa, dostęp F-I/O jest możliwy jedynie, gdy program bezpieczeństwa zostanie spójnie pobrany do F-CPU.

Zmiana standardowego programu użytkownika

Pobranie zmian w standardowym programie użytkownika jest możliwe, gdy F-CPU działa w trybie RUN, niezależnie od tego, czy tryb bezpieczeństwa jest włączony.

⚠ OSTRZEŻENIE

(S7-300, S7-400) W trybie bezpieczeństwa, dostęp za pomocą hasła CPU nie może być autoryzowany podczas wprowadzania zmian w standardowym programie użytkownika, ponieważ pozwoliłoby to na zmiany w programie bezpieczeństwa. Aby wykluczyć taką możliwość, należy ustawić poziom zabezpieczenia „Write protection for fail-safe blocks" (Ochrona zapisu dla bloków fail-safe) i skonfigurować hasło dla F-CPU. Jeśli tylko jedna osoba jest upoważniona do zmiany standardowego programu użytkownika oraz programu bezpieczeństwa, należy ustawić poziom zabezpieczenia „Write protection" (Ochrona zapisu) lub „Read/write protection" (Ochrona odczytu/zapisu), by inne osoby miały jedynie ograniczony dostęp lub brak dostępu do całego programu użytkownika (programów standardowego i bezpieczeństwa). *(S001)*

Procedura wprowadzania zmian do programu bezpieczeństwa

W przypadku pobrania poszczególnych bloków bezpieczeństwa do F-CPU podczas pracy (w trybie RUN),
bloki systemu bezpieczeństwa (F-DB) oraz automatycznie generowane bloki bezpieczeństwa nie są aktualizowane ani pobierane, skutkując niespójnością programu w F-CPU. Przy pomocy poniższej procedury można wprowadzić zmiany w programie bezpieczeństwa:

1. Należy pobrać program bezpieczeństwa spójnie do F-CPU, po czym aktywować tryb bezpieczeństwa, przełączając F-CPU z trybu STOP na RUN (procedura dostępna w dziale „Pobieranie danych projektu do F-CPU (strona 325)).
2. Należy wykonać kroki opisane w dziale „Zatwierdzenie zmian" (strona 396).

10.7.6 Zmiana standardowego programu użytkownika w trybie RUN (S7-1200, S7-1500)

Zmiana standardowego programu użytkownika

Pobranie zmian w standardowym programie użytkownika jest możliwe, gdy F-CPU działa w trybie RUN, niezależnie od tego, czy tryb bezpieczeństwa jest włączony.

10.8 Historia zmian bezpieczeństwa

Rejestrowanie zmian w programie bezpieczeństwa włącza się za pomocą opcji „Enable F-change history" (Włącz historię zmiany bezpieczeństwa) w *Safety Administration Editor*. Historia zmian bezpieczeństwa zachowuje się jak standardowa historia zmian.

Historia zmian bezpieczeństwa jest tworzona dla każdego F-CPU w nawigacji projektu pod hasłem „Common data/logs" (Wspólne dane/rejestry).

Poniższe elementy są rejestrowane w historii zmian bezpieczeństwa:

- Zbiorczy podpis bezpieczeństwa
- Nazwa użytkownika
- Skompilowany znacznik czasowy
- Pobranie programu bezpieczeństwa ze znacznikiem czasowym
- Skompilowane bloki bezpieczeństwa z podpisem i znacznikiem

Historia zmian bezpieczeństwa może zawierać maksymalnie 5000 wejść na F-CPU. Po przekroczeniu 5000 wpisów, tworzona jest nowa historia zmian bezpieczeństwa, z wykorzystaniem schematu nazewnictwa „Historia zmian bezpieczeństwa <nazwa CPU> YYYY-MM-DD hh:mm:ss".

Po aktualizacji projektu funkcja „Przejdź do" nie jest dłużej obsługiwana dla historii zmian bezpieczeństwa projektu w przypadku wpisów utworzonych przed *STEP 7 Safety V15.1*.

UWAGA

Połączenie pomiędzy F-CPU a powiązaną historią zmian bezpieczeństwa jest wykonywane poprzez nazwę historii.

Dlatego nie należy zmieniać nazwy F-CPU i historii zmian bezpieczeństwa. W przypadku zmiany nazwy F-CPU lub historii zmian bezpieczeństwa, zostanie utworzona nowa historia z bieżącą nazwą F-CPU.

Uwaga

Nie można wykorzystać historii zmian bezpieczeństwa do rozpoznawania zmian w programie bezpieczeństwa/w konfiguracji F-I/O podczas zatwierdzania zmian.

Aby zaakceptować zmiany, należy wykonać czynności opisane w dziale „Zatwierdzenie zmian" (strona 396).

Uwaga

Zaleca się aktywowanie historii zmian bezpieczeństwa przed przejściem w operację produkcyjną.

Zatwierdzenie systemu 11

11.1 Przegląd zatwierdzenia systemu

Wstęp

Podczas wykonywania testu zatwierdzenia systemu, należy spełnić wszystkie normy i wytyczne (przykładowo, „Wytyczne instalacji PROFINET) dotyczące konkretnej aplikacji. Dotyczy to również systemów, które nie „podlegają zatwierdzeniu". Podczas zatwierdzania należy uwzględnić wymogi w raporcie certyfikacji (http://support.automation.siemens.com/WW/view/en/49368678/134200).

Ogólną zasadą jest, że zatwierdzenie systemu bezpieczeństwa wykonuje niezależny ekspert. Wymagana niezależność musi zostać zdefiniowana w planie bezpieczeństwa i zależy od wymaganego PL/SIL.

Należy przestrzegać wszystkich ostrzeżeń w niniejszym podręczniku.

OSTRZEŻENIE

Konfiguracja F-CPU oraz F-I/O, a także programowanie bloków bezpieczeństwa musi odbywać się z TIA Portal w sposób opisany w niniejszej dokumentacji. Należy przestrzegać wszystkich kwestii opisanych w dziale „Zatwierdzenie systemu" (strona 376), aby zagwarantować bezpieczne działanie systemu SIMATIC Safety. Inne procedury nie są dozwolone. *(S056)*

Dowód poprawnego wdrożenia danych projektu związanych z bezpieczeństwem

Aby możliwe było przyznanie zatwierdzenia systemu, należy dokonać oceny i udokumentować poprawność poszczególnych elementów. Aby móc udokumentować charakterystyki elementów, należy utworzyć podsumowanie bezpieczeństwa.

Należy ująć następujące charakterystyki:

- Poprawność programu bezpieczeństwa, w tym konfiguracja sprzętowa (obejmuje testowanie) (strona 378)
- Kompletność podsumowania bezpieczeństwa (strona 379)
- Zgodność elementów biblioteki systemowej użytej w programie bezpieczeństwa z Załącznikiem 1 raportu do certyfikacji TÜV (strona 380)
- Zgodność bloków bezpieczeństwa chronionej wiedzy technologicznej stosowanych w programie bezpieczeństwa z ich dokumentacją bezpieczeństwa.(strona 381)
- Kompletność i poprawność konfiguracji sprzętowej (strona 383) Poprawność ikompletność konfiguracji komunikacji (strona 391) Identyfikacja programu online i offline (strona 393)
- Pozostałe charakterystyki (strona 394), takie jak wersja oprogramowania, użycie danych ze standardowego programu użytkownika

Po zatwierdzeniu należy zarchiwizować wszystkie odnośne dokumenty oraz dane projektu, aby zatwierdzony projekt był dostępny jako odniesienie dla kolejnych zatwierdzeń.

Podsumowanie

Podsumowanie bezpieczeństwa (strona 357) do dokumentacja projektu wymagana do zatwierdzenia systemu.

11.2 Poprawność programu bezpieczeństwa, w tym konfiguracja sprzętowa (obejmuje testowanie)

Poprawności oprogramowania nie można zapewnić jedynie poprzez testy i weryfikację podczas odbioru technicznego, lecz wymaga ona stosowania szeregu różnych środków podczas tworzenia. Zobacz również ostrzeżenie S062 w rozdziale „Przegląd" (strona 21).

Weryfikacja/test funkcji

Już podczas tworzenia wykonuje się testy (strona 359) programu bezpieczeństwa oraz powiązanej konfiguracji sprzętowej. Należy wykonać te testy zgodnie ze specyfikacją funkcji bezpieczeństwa i udokumentować je, nim przeprowadzi się zatwierdzenie systemu.

Aby umożliwić wykonać przeglądu kodu programu bezpieczeństwa i udokumentowanie zatwierdzonego kodu, kod źródłowy wszystkich bloków bezpieczeństwa jest drukowany jako część podsumowania (strona 357), o ile zaznaczono opcję „All" (Wszystko) dla wydruku.

Aby wykonać test funkcji po załadowaniu, należy wykonać identyfikację programu. Dodatkowe informacje dostępne są w dziale „Pobieranie danych projektu" (strona 325).

Poprawne działanie programu bezpieczeństwa musi zostać zagwarantowane przez wypełnienie wszystkich kroków z rozdziału „Przegląd zatwierdzenia systemu" (strona 376) przed zastosowaniem go w produkcji. Podczas korzystania z kontroli konfiguracji (zarządzania opcjami), należy zapewnić poprawne działanie programu bezpieczeństwa dla wszystkich możliwych opcji stacji, wykonując odpowiednie testy funkcjonalne. Należy dołączyć wyniki testów do podsumowania bezpieczeństwa w dokumentacji zatwierdzenia.

Czasy, na przykład czasy monitorowania (strona 649) oraz opóźnienia można skontrolować tylko w ograniczonym zakresie, korzystając z testów funkcjonalnych (strona 325). Należy selektywnie sprawdzić te czasy, by określić, czy zostały prawidłowo dobrane, korzystając, przykładowo, z podsumowania bezpieczeństwa.

Niektóre z tych czasów są specjalnie wyszczególnione w podsumowaniu, na przykład czas monitorowania bezpieczeństwa (dla komunikacji pomiędzy F-CPU a F-I/O) oraz czas
monitorowania komunikacja CPU safety – CPU (wejście TIMEOUT). W przypadku czasów odbiegających od normalnych warunków, dostępny jest arkusz kalkulacyjny do obliczania czasu odpowiedzi
(http://support.automation.siemens.com/WW/view/en/49368678/133100).
Należy uwzględnić je wraz z praktycznie określanymi warunkami aplikacji. Należy pamiętać, że czasy monitorowania mają wpływ na czasy odpowiedzi funkcji bezpieczeństwa.

Spójność programu bezpieczeństwa

Należy sprawdzić dział „Informacje ogólne" podsumowania bezpieczeństwa, by określić, czy program bezpieczeństwa został rozpoznany jako „spójny".

Dotyczy to F-CPU S7-300/400 tylko, jeśli poniższe podpisy również są identyczne:

- Zbiorczy podpis bezpieczeństwa (dział „Informacje ogólne", „Zbiorczy podpis bezpieczeństwa")
- „Podpis bloków bezpieczeństwa z atrybutem F" (dział „Informacje ogólne", „Bieżąca kompilacja")

Spójność programu bezpieczeństwa jest wymagana do zatwierdzenia. Jeśli podpisy nie są identyczne, możliwe jest ustalenie spójności poprzez ponowne skompilowanie programu bezpieczeństwa oraz nowe utworzenie podsumowania bezpieczeństwa.

11.3 Kompletność podsumowania bezpieczeństwa

Wstęp

Jeśli program bezpieczeństwa zawierający konfigurację sprzętową jest gotowy do zatwierdzenia, należy wykonać i udokumentować dodatkową kontrolę na podstawie podsumowania bezpieczeństwa, by zagwarantować, iż podsumowanie jest kompletne, a części programu bezpieczeństwa mogą zostać zatwierdzone.

Procedura tworzenia podsumowania bezpieczeństwa

Aby wygenerować podsumowanie bezpieczeństwa, należy wykonać procedurę opisaną w dziale „Drukowanie danych projektu" (strona 357).

W trakcie jej wykonywania należy zaznaczyć opcję „All" (Wszystko), by ująć kod źródłowy bloków bezpieczeństwa w wydruku.

Sprawdzenie podsumowania bezpieczeństwa pod kątem kompletności

Aby użyć istniejącego podsumowania, którego kompletność nie jest znana, należy je sprawdzić, by określić, czy w stopce na wszystkich stronach wydruku znajduje się ten sam zbiorczy podpis bezpieczeństwa. Pozwoli to na zapewnienie, iż wszystkie wydrukowane arkusza należą do tego samego projektu.

W dziale „Informacje dodatkowe" można znaleźć między innymi liczbę stron w podsumowaniu bezpieczeństwa. Dzięki temu można sprawdzić, czy wydrukowano wszystkie strony podsumowania. Niekompletne wydruki (np. z powodu niskiego poziomu tuszu) nie mogą zostać wykorzystane do zatwierdzenia.

Jeśli utworzono podsumowanie bezpieczeństwa z opcją „All" (Wszystko), kod źródłowych wszystkich bloków bezpieczeństwa zostanie wydrukowany. Wydruk tego kodu również zawiera stopkę, pozwalającą na łatwe przypisanie go do konkretnego podsumowania.

Powiązanie z programem bezpieczeństwa

W dziale „Informacje ogólne" podsumowania bezpieczeństwa należy sprawdzić, czy zbiorczy podpis bezpieczeństwa odpowiada podpisowi programu bezpieczeństwa do zatwierdzenia w obszarze roboczym *Safety Administration Editor* w „General" (Ogólne). Jeśli nie są identyczne, podsumowanie i program nie będą zgodne.

11.4 Zgodność elementów biblioteki systemowej użytej w programie bezpieczeństwa z Załącznikiem 1 raportu do certyfikacji TÜV

Wstęp

STEP 7 Safety zawiera instrukcje LAD/FBD do programowania programu bezpieczeństwa, a także bloki systemu bezpieczeństwa to tworzenia wykonywalnego programu bezpieczeństwa, który został utworzony i przetestowany przez firmę SIEMENS oraz przeszedł certyfikację TÜV. Bloki systemu bezpieczeństwa są automatycznie wstawiane przez system bezpieczeństwa w oparciu o jego ustawioną wersję (patrz dział „Ustawienia" (strona 91)).

Aby umożliwić sprawdzenie, czy używane instrukcje LAD/FBD oraz bloki systemu bezpieczeństwa odpowiadają Załącznikowi 1 raportu do certyfikacji TÜV oraz wersjom, które mają zostać użyte, zostały one wyszczególnione w podsumowaniu bezpieczeństwa.

Procedura

Aby dokonać kontroli, należy pobrać aktualny Załącznik 1 raportu do certyfikacji TÜV „SIMATIC Safety" z internetu (http://support.automation.siemens.com/WW/view/en/49368678/134200).

Aby dokonać kontroli, należy wykonać co następuje:

OSTRZEŻENIE

- (S7-1200, S7-1500) Wersje różnych instrukcji LAD/FBD wyszczególnione w podsumowaniu w dziale „Elementy biblioteki systemowej zastosowane w programie bezpieczeństwa" muszą być zgodne z wersjami w Załączniku 1 raportu do certyfikacji TÜV.
- (S7-300, S7-400) Wersje, podpisy i podpisy wartości początkowych różnych instrukcji LAD/FBD oraz bloków systemu bezpieczeństwa wyszczególnione w podsumowaniu w dziale „Elementy biblioteki systemowej zastosowane w programie bezpieczeństwa" muszą być zgodne z wersjami, podpisami i podpisami wartości początkowych w Załączniku 1 raportu do certyfikacji TÜV.
- Wersje określonych instrukcji LAD/FBD wyszczególnionych w podsumowaniu bezpieczeństwa muszą spełniać wymogi bezpieczeństwa danej aplikacji. Należy pamiętać o możliwych różnicach w funkcjonalności różnych wersji określonych w dziale dla odpowiedniej instrukcji.
- Wersja systemu bezpieczeństwa podana na liście w podsumowaniu pod hasłem „Ustawienia programu bezpieczeństwa" musi być zgodna z wersją w Załączniku 1 raportu do certyfikacji TÜV. *(S054)*

W razie rozbieżności należy ponownie sprawdzić, czy dostępna jest poprawna wersja.

(S7-300 / 400) Różnice mogą wystąpić, gdy w programie są bloki bezpieczeństwa / instrukcje, które nie są używane.

11.5 Zgodność bloków bezpieczeństwa chronionej wiedzy technologicznej stosowanych w programie bezpieczeństwa z ich dokumentacją bezpieczeństwa.

11.5 Zgodność bloków bezpieczeństwa chronionej wiedzy technologicznej stosowanych w programie bezpieczeństwa z ich dokumentacją bezpieczeństwa.

W przypadku korzystania z bloków bezpieczeństwa chronionej wiedzy technologicznej do programowania programu (np. z bibliotek), kod źródłowy tych bloków nie jest drukowany w podsumowaniu.

F-CPU S7-300/400

- Podpis i podpis wartości początkowej bloku bezpieczeństwa chronionej
- wiedzy technologicznej
- Wersje wszystkich zastosowanych instrukcji LAD/FDB.

Podczas wykonywania zatwierdzenia systemu należy przeprowadzić następujące kontrole, korzystając z podsumowania bezpieczeństwa:

- Podpis i wartość początkowa każdego bloku bezpieczeństwa chronionej wiedzy technologicznej wyszczególnione w podsumowaniu w dziale „Bloki bezpieczeństwa w programie bezpieczeństwa" muszą być identyczne z podpisem i wartością początkową udokumentowaną przez autora.
- Wersje różnych instrukcji LAD/FBD wyszczególnione w podsumowaniu w dziale „Elementy biblioteki systemowej zastosowane w programie bezpieczeństwa" muszą być zgodne z wersjami bloków wiedzy specjalistycznej udokumentowanymi przez autora lub muszą być funkcjonalnie identycznie z nimi.
- Podpisy i wartość początkowa bloków bezpieczeństwa chronionej wiedzy technologicznej wyszczególnione w podsumowaniu w dziale „Bloki bezpieczeństwa w programie bezpieczeństwa" muszą być identyczne z podpisami i wartością początkową podpisów (wywoływanych bloków bezpieczeństwa) udokumentowaną przez autora.

W przypadku różnic, należy ustawić udokumentowaną (lub funkcjonalnie identyczną) wersję i zastosować bloki bezpieczeństwa z udokumentowanymi podpisami oraz wartościami początkowymi. Jeśli nie można wyeliminować konfliktów wersji ze względu na różne zależności, należy skontaktować się z autorem bloku chronionej wiedzy technologicznej w celu uzyskania kompatybilnej, zatwierdzonej wersji.

F-CPU S7-1200/1500

- Podpis bloku bezpieczeństwa chronionej wiedzy technologicznej
- Wersja systemu bezpieczeństwa ustawiona podczas ustawiania ochrony
- wiedzy technologicznej Wersje wszystkich zastosowanych instrukcji
- LAD/FDB.

Podczas wykonywania zatwierdzenia systemu należy przeprowadzić następujące kontrole, korzystając z podsumowania bezpieczeństwa:

- Podpis każdego bloku bezpieczeństwa chronionej wiedzy technologicznej wyszczególnione w podsumowaniu w dziale „Bloki bezpieczeństwa chronionej wiedzy technologicznej w programie bezpieczeństwa" muszą być identyczne z podpisem udokumentowanym przez autora.
- Wersja systemu bezpieczeństwa bloku bezpieczeństwa chronionej wiedzy technologicznej wyszczególniona w podsumowaniu pod hasłem „Bloki bezpieczeństwa chronionej wiedzy technologicznej w programie bezpieczeństwa" musi być zgodna z
- jedną z wersji podaną w Załączniku 1 raportu do certyfikacji TÜV.

  Wersje różnych instrukcji LAD/FBD bloku bezpieczeństwa chronionej wiedzy technologicznej wyszczególnione w podsumowaniu w dziale „Bloki bezpieczeństwa chronionej wiedzy technologicznej w programie bezpieczeństwa" muszą być zgodne z wersjami bloków wiedzy specjalistycznej udokumentowanymi przez autora lub muszą
- być funkcjonalnie identycznie z nimi.

  Podpisy bloków bezpieczeństwa wywoływanych w bloku bezpieczeństwa chronionej

W przypadku różnic, należy ustawić udokumentowaną (lub funkcjonalnie identyczną) wersję i zastosować bloki bezpieczeństwa z udokumentowanymi podpisami. Jeśli nie można wyeliminować konfliktów wersji ze względu na różne zależności, należy skontaktować się z autorem bloku chronionej wiedzy technologicznej w celu uzyskania kompatybilnej, zatwierdzonej wersji.

11.6 Kompletność i poprawność konfiguracji sprzętowej

Wstęp

Konfiguracja sprzętowa jest istotnym elementem projektu, który należy zatwierdzić. Za pomocą konfiguracji sprzętu ustawia się właściwości, które mogą wpływać na bezpieczeństwo sygnałów. Należy udokumentować te ustawienia w podsumowaniu bezpieczeństwa, by zagwarantować, iż spełnione zostały wymogi aplikacji.

Służy do tego dział „Konfiguracja sprzętowa F-I/O" w podsumowaniu bezpieczeństwa. Dział ten zawiera kilka tabel:

- Tabela z informacjami o F-CPU oraz zakresy stosowanych adresów docelowych bezpieczeństwa i „centralny adres źródłowy bezpieczeństwa" dla F-CPU.
- Tabela przeglądu zastosowanych F-I/O.
- Tabela dla każdego F-I/O z informacjami o F-I/O i wszystkich parametrach ze skonfigurowanymi wartościami.

Jako że zarządzanie użytkownika serwerem sieciowym również stanowi część konfiguracji sprzętowej, wymagana jest autoryzacja z prawami „administrator bezpieczeństwa". Więcej informacji można znaleźć w dziale „Administratorzy bezpieczeństwa serwera sieciowego (S7-1200, S7-1500)" (strona 90).

Uwaga

Należy pamiętać, że F-I/O adresowany poprzez komunikację urządzenie I-slave safety – urządzenie podrzędne znajduje się w podsumowaniu F-CPU urządzenia I-slave, nie w podsumowaniu F-CPU powiązanego urządzenia nadrzędnego DP.

Podsumowanie bezpieczeństwa dla F-CPU urządzenia nadrzędnego DP obejmuje uwagę dla tego F-CPU w tabeli omówienia, wskazującą, że F-I/O nie jest przypisany do tego F-CPU.

Uwaga

Podczas korzystania ze współdzielonych urządzeń:

F-I/O adresowany we współdzielonym urządzeniu można znaleźć w podsumowaniu F-CPU sterownika IO, do którego jest przypisany.

Podsumowanie bezpieczeństwa F-CPU innych sterowników IO pomiędzy którymi dzielone jest urządzenie, wskazuje uwagę w tabeli omówienia dla tego F-I/O, że nie jest przypisany do danego F-CPU.

Procedura sprawdzania kompletności konfiguracji sprzętowej

Należy upewnić się, że wszystkie skonfigurowane F-I/O zostały ujęte w podsumowaniu bezpieczeństwa. Należy także sprawdzić, czy nie ma F-I/O, który nie został skonfigurowany jako należący do danego F-CPU.

Uwaga

Jeśli wykorzystywana jest kontrola konfiguracji (zarządzanie opcjami), podsumowanie bezpieczeństwa musi zawierać wszystkie urządzenia F-I/O maksymalnej konfiguracji. Należy wykonać poniższe kontrole dla wszystkich F-I/ maksymalnej konfiguracji.

Procedura sprawdzania poprawności konfiguracji sprzętowej przy użyciu podsumowania bezpieczeństwa

1. Sprawdzić w dziale „Konfiguracja sprzętowa F-IO" unikalność adresów PROFIsafe.

   Patrz działy „Adresy PROFIsafe do F-I/O typu adresowania PROFIsafe 1" (strona 66) lub „Adresy PROFIsafe do F-I/O typu adresowania PROFIsafe 2" (strona 68) „Specjalne przypadki konfiguracji urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe" (strona 76) i „Zalecenia dotyczące przypisywania adresu PROFIsafe" (strona 63).

   – Sprawdzić, czy parametr „Centralny adres źródłowy bezpieczeństwa" poszczególnych F-CPU różni się w całej sieci. F-CPU, do których przypisane są wyłącznie F-I/O typy adresu PROFIsafe 1, nie muszą być uwzględniane podczas tej kontroli.
   – W przypadku F-I/O d adresu PROFIsafe typu 1 należy sprawdzić, czy adresy docelowe bezpieczeństwa są zgodne z poniższym ostrzeżeniem:

   *Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza

   OSTRZEŻENIE

   F-I/O do typu adresowania PROFIsafe 1 są unikalnie adresowane przez ich adresy docelowe bezpieczeństwa (np. za pomocą ustawienia przełącznika adresowego).

   Adres docelowy bezpieczeństwa (a zatem również ustawienie przełącznika adresowego) dla F-I/O musi być unikalny w całej sieci* oraz w obrębie CPU (w obrębie systemu) **dla całego** F-I/O. Należy również uwzględnić F-I/O typu adresowania PROFIsafe 2. *(S051)*

   ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

   ** „W obrębie CPU" oznacza wszystkie F-I/O przypisane do F-CPU: Centralny F-I/O tego F-CPU, a także F-I/O, dla których F-CPU to urządzenie nadrzędne DP/sterownik IO oraz przypisane F-I/O we współdzielonym urządzeniu. F-I/O adresowany przy pomocy komunikacji urządzenie I-slave – urządzenie podrzędne jest przypisywany do F-CPU urządzenia I-slave, a nie do F-CPU urządzenia nadrzędnego DP / sterownika IO.

   Uwaga

   Więcej informacji dotyczących przypisywania adresów PROFIsafe unikalnych dla CPU oraz sieci, sprawdź FAQ (https://support.industry.siemens.com/cs/ww/en/view/109740240).

– W przypadku F-I/O d adresu PROFIsafe typu 2 należy sprawdzić, czy adresy docelowe bezpieczeństwa są zgodne z poniższym ostrzeżeniem:

⚠ OSTRZEŻENIE

F-I/O typu adresowania PROFIsafe 2 jest adresowany unikalnie przy pomocy połączenia adresu źródłowego bezpieczeństwa (parametr „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) przypisanego F-CPU) oraz adresu docelowego bezpieczeństwa.

Połączenie adresu źródłowego bezpieczeństwa oraz adresu docelowego bezpieczeństwa dla każdego F-I/O musi być unikalne w całej sieci* oraz w obrębie CPU** (w obrębie systemu). Ponadto, adres docelowy bezpieczeństwa nie może być zajmowany przez F-I/O typu adresowania PROFIsafe 1.

Aby zapewnić, że adresy są unikalne dla F-CPU dla obsługiwanych konfiguracji (strona 64), należy upewnić się, iż parametr „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) dla wszystkich F-CPU jest unikalny w całej sieci*. Osiąga się to poprzez różne ustawienia parametru „Centralny adres źródłowy bezpieczeństwa" dla F-CPU. *(S052)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** „W obrębie CPU" oznacza wszystkie F-I/O przypisane do F-CPU: Centralny F-I/O tego F-CPU, a także F-I/O, dla których F-CPU to urządzenie nadrzędne DP/sterownik IO oraz przypisane F-I/O we współdzielonym urządzeniu. F-I/O adresowany przy pomocy komunikacji urządzenie I-slave – urządzenie podrzędne jest przypisywany do F-CPU urządzenia I-slave, a nie do F-CPU urządzenia nadrzędnego DP / sterownika IO.

Uwaga

Więcej informacji dotyczących przypisywania adresów PROFIsafe unikalnych dla CPU oraz sieci, sprawdź FAQ (https://support.industry.siemens.com/cs/ww/en/view/109740240).

- Sprawdzić, czy adresy PROFIsafe urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD spełniają wymogi poniższego ostrzeżenia:

> **OSTRZEŻENIE**
>
> Należy sprawdzić dokumentację urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD typu fail-safe, aby określić ważny typ adresu PROFIsafe. W przypadku braku niezbędnych informacji, należy przyjąć typ adresu PROFIsafe 1. Należy postępować zgodnie z opisem w dziale Adresy PROFIsafe do F-I/O typu adresowania PROFIsafe 1 (strona 66) lub Adresy PROFIsafe do F- I/O typu adresowania PROFIsafe 2 (strona 68).
>
> Należy ustawić adres źródłowy bezpieczeństwa dla urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD typu fail-safe zgodnie ze specyfikacją producenta. Jeśli adres źródłowy bezpieczeństwa musi odpowiadać parametrowi „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) dla F-CPU (typ adresu PROFIsafe 2), można znaleźć go w zakładce „Properties" (Właściwości) F-CPU. W takim przypadku należy również sprawdzić w podsumowaniu bezpieczeństwa, czy wartość F-CPU dla parametru „Central F-source address" (Centralny adres źródłowy bezpieczeństwa) jest zgodny z wartością adresu źródłowego bezpieczeństwa dla urządzenia podrzędnego DP opartego na GSD typu fail-safe/urządzenia I/O opartego na GSD typu fail-safe. *(S053)*

2. Sprawdzić parametry safety (w tym czas monitorowania bezpieczeństwa F_WD_Time) wszystkich skonfigurowanych F-I/O.

   Parametry te znajdują się w dziale „Konfiguracja sprzętowa F-I/O", w tabeli poświęconej F-I/O.

   Tabela składa się z dwóch części:

   – Lewa część zawiera parametry, które odnoszą się do samego F-I/O („dane modułu).
   – Prawa część zawiera parametry poszczególnych kanałów („parametry kanałów").

   Parametry te muszą być ustawione zgodnie z wymogami bezpieczeństwa aplikacji.

   W przypadku korzystania z urządzeń podrzędnych DP oparte na GSD typu fail-safe/urządzeń I/O opartych na GSD, należy sprawdzić odnośne dokumenty pod katem możliwych dodatkowych parametrów (technologicznych) związanych z bezpieczeństwem.

Uwaga

F-I/O, do których mają zostać przypisane te same parametry safety (za wyjątkiem adresów PROFIsafe) można skopiować podczas konfiguracji. Za wyjątkiem adresów PROFIsafe, nie ma konieczności sprawdzania poszczególnych parametrów związanych z bezpieczeństwem. Wystarczy porównać
„Podpis parametrów bezpieczeństwa (bez adresów)" w dziale „Konfiguracja sprzętowa F-I/O" w tabeli omówienia. Dotyczy to również urządzeń podrzędnych DP opartych na GSD typu fail-safe/ urządzeń I/O opartych na GSD bez parametrów i. W przypadku urządzeń podrzędnych DP opartych na GSD / urządzeń I/O opartych na GSD z parametrami i, możliwe jest, iż „Podpis parametru bezpieczeństwa (bez adresów) nie jest zgodny, mimo iż wszystkie parametry safety, za wyjątkiem adresów PROFIsafe, są zgodne. W takim przypadku należy porównać wszystkie parametry safety.

Wyjątek:

Dla F-I/O, które nie obsługują profilu „RIOforFA-Safety", należy wykonać porównanie parametru „Zachowanie po usterce kanału", dodatkowo do „Podpis parametru bezpieczeństwa (bez adresów)".

3. Sprawdzić, czy numery zamówieniowe F-I/O w podsumowaniu bezpieczeństwa odpowiadają numerom rzeczywistego F-I/O w systemie. Jeśli numery różnią się, istniejący F-I/O musi być częścią kompatybilną z F-I/O wyszczególnionym w podsumowaniu bezpieczeństwa.

4. W przypadku nieobsługiwanej konfiguracji należy zapoznać się z działem „Konfiguracje obsługiwane przez system bezpieczeństwa SIMATIC Safety" (strona 64).

OSTRZEŻENIE

Korzystając z konfiguracji, które nie są uwzględnione w obsługiwanych, należy mieć na uwadze następuje zagadnienia:

- Należy upewnić się, że F-I/O tej konfiguracji występuje w podsumowaniu bezpieczeństwa oraz że DB dla F-I/O został utworzony. W przeciwnym razie nie można wykorzystać F-I/O w tej konfiguracji. (Należy skontaktować się z działem obsługi klienta.)
- Dla F-I/O w środowisku PROFINET IO**, należy sprawdzić parametr trybu pracy PROFIsafe (F_Par_Version) z podsumowaniem bezpieczeństwa, by upewnić się, że jest on poprawny. W środowisku PROFINET IO musi być ustawiony tryb V2. F-I/O obsługujące jedynie tryb V1 nie mogą być zastosowane w środowisku PROFINET IO.
- Należy upewnić się, że przypisanie adresów PROFIsafe jest unikalne w obrębie CPU* oraz w całej sieci***:
  - Należy sprawdzić poprawność adresów PROFIsafe, korzystając z podsumowania bezpieczeństwa.
  - Za pomocą podsumowania bezpieczeństwa można sprawdzić, czy adres źródłowy bezpieczeństwa odpowiada parametrowi „Centralny adres źródłowy bezpieczeństwa" F-CPU dla F-I/O typu adresowania PROFIsafe 2.
  - Dla F-I/O typu adresowania PROFIsafe 1, lub jeśli nie można ustawić adresu źródłowego bezpieczeństwa zgodnie z parametrem F-CPU „Centralny adres źródłowy bezpieczeństwa", konieczne jest zagwarantowanie unikalności adresu PROFIsafe wyłącznie poprzez przypisanie unikalnego adresu docelowego bezpieczeństwa.

  Należy sprawdzić unikalność adresu docelowego bezpieczeństwa indywidualnie dla każdego F-I/O, który znajduje się w konfiguracji, która nie jest obsługiwana, korzystając z podsumowania bezpieczeństwa. *(S050)*

* „W obrębie CPU" oznacza wszystkie F-I/O przypisane do F-CPU: Centralny F-I/O tego F-CPU, a także F-I/O, dla których F-CPU to urządzenie nadrzędne DP/sterownik IO oraz przypisane F-I/O we współdzielonym urządzeniu. F-I/O adresowany przy pomocy komunikacji urządzenie I-slave – urządzenie podrzędne jest przypisywany do F-CPU urządzenia I-slave, a nie do F-CPU urządzenia nadrzędnego DP / sterownika IO.

** F-I/O znajduje się w „środowisku PROFINET IO", jeśli co najmniej część komunikacji związanej z bezpieczeństwem z F-CPU odbywa się poprzez PROFINET IO. Jeśli F-I/O jest podłączony poprzez komunikację urządzenie I-slave – urządzenie podrzędne, należy uwzględnić linię komunikacyjną do urządzenia nadrzędnego DP / sterownika IO.

*** Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

Uwaga

Więcej informacji dotyczących przypisywania adresów PROFIsafe unikalnych dla CPU oraz sieci, sprawdź FAQ (https://support.industry.siemens.com/cs/ww/en/view/109740240).

5. Sprawdzić, czy jedynie upoważnione osoby posiadają prawa „Admistrator bezpieczeństwa" w *Safety Administration Editor* lub na standardowym wydruku danych projektu.

OSTRZEŻENIE

Upoważnienie „F-Admin" (Administrator bezpieczeństwa) dla serwera sieciowego bez zabezpieczenia hasłem (użytkownik „Everybody" (Wszyscy)) jest przeznaczone jedynie do testów, odbioru technicznego itp. Dotyczy to zatem systemu, który nie wykonuje operacji produkcyjnej. W takim przypadku należy zagwarantować bezpieczeństwo systemu poprzez inne środki organizacyjne, na przykład, zabezpieczając dostęp do określonych obszarów.

Przed przejściem do operacji produkcyjnej należy usunąć prawa „F-Admin" (administratora bezpieczeństwa) dla użytkownika „Everybody" (Wszyscy).

Jedynie upoważniony personel może mieć dostęp do hasła użytkownika serwera sieciowego z prawami „F-Admin" (Administrator bezpieczeństwa). Po pobraniu konfiguracji sprzętowej należy sprawdzić, czy jedynie upoważnieni użytkownicy serwera sieciowego mają prawo „F-Admin" na F-CPU. W tym celu należy użyć widoku online w *Safety Administration Editor*.

Zapisanie loginu i hasła serwera sieciowego w przeglądarce jest dozwolone jedynie, gdy dostęp nieupoważnionych osób jest ograniczony poprzez inne środki organizacyjne (np. ochronę dostępu do PG/PC). *(S064)*

11.7 Kompletność i poprawność konfiguracji komunikacji

Wstęp

Komunikacja safety jest oparta na mechanizmach standardowej komunikacji *STEP 7*.

Aby zapewnić, iż wykryte zostaną błędy niedostrzeżone przez standardową komunikację, komunikacja safety pomiędzy F-CPU jest zabezpieczona. Konieczne są do tego dodatkowe parametry, które należy udokumentować i sprawdzić podczas zatwierdzenia.

Do tego celu służą działy „Parametry bloków komunikacji CPU safety – CPU" oraz „Przegląd komunikacji poprzez Flexible F-Link" w podsumowaniu bezpieczeństwa. Dział „Parametry bloków komunikacji CPU safety – CPU" zawiera dwie tabele (dla komunikacji poprzez PROFIBUS DP lub PROFINET IO oraz dla komunikacji poprzez połączenia S7). Dział „Przegląd komunikacji poprzez Flexible F- Link" zawiera tabelę z omówieniem konfiguracji połączeń oraz tabelę „Komunikacja poprzez Flexible F-Link do UDT" dla każdego zastosowanego rodzaju danych PLC zgodnych z bezpieczeństwem (UDT).

Nie wszystkie rodzaje komunikacji związanej z bezpieczeństwem są dostępne dla wszystkich F-CPU. Więcej informacji można znaleźć w dziale „Komunikacja safety" (strona 209).

Procedura sprawdzania poprawności konfiguracji komunikacji

Aby sprawdzić poprawność konfiguracji komunikacji, należy wykonać co następuje:

⚠ OSTRZEŻENIE

Podczas akceptacji należy skorzystać z podsumowania bezpieczeństwa, by sprawdzić, czy przesunięcia wszystkich elementów rodzaju danych PLC zgodnych z bezpieczeństwem (UDT) są zgodne z wysyłanymi i odbieranymi danymi w ramce wiadomości bezpieczeństwa. Z tego względu wszystkie elementy i adresy są wyszczególnione w podsumowaniu bezpieczeństwa dla UDT. *(S088)*

⚠ OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście R_ID; rodzaj danych: DWORD) można dobierać dowolnie; jednakże, muszą być nieparzyste i unikalne dla wszystkich połączeń komunikacji związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Wartość R_ID + 1 jest przypisywana wewnętrznie i nie należy z niej korzystać.

Należy doprowadzić wartości stałe do wejść ID oraz R_ID podczas wywoływania instrukcji. Bezpośredni dostęp do odczytu lub zapisu w powiązanej instancji DB jest niedozwolony w programie bezpieczeństwa! *(S020)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

Aby sprawdzić poprawność komunikacji poprzez Flexible F-Link, należy wykonać następujące kroki:

OSTRZEŻENIE

Gdy w Safety Administration Editor tworzona jest nowa komunikacja Flexible F-Link, unikalny UUID komunikacji bezpieczeństwa jest zapewniany przez system. Poprzez skopiowanie komunikacji w Safety Administration Editor w obrębie tabeli parametryzacji lub podczas kopiowania do innego F-CPU, UUID komunikacji bezpieczeństwa nie są ponownie generowane, przez co tracą swoją unikalność. Jeśli do konfigurowania nowego związku komunikacji wykorzystywana jest kopia, należy samodzielnie zapewnić unikalność. W tym celu należy wybrać dane UUID i wygenerować je ponownie poprzez menu kontekstowe „Generate UUID" (Wygeneruj UUID). Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas zatwierdzenia. *(S087)*

11.8 Identyfikacja programu online i offline

Po sprawdzeniu wszystkich właściwości programu bezpieczeństwa offline, należy upewnić się, że jest on identyczny na F-CPU, na którym ma być wykonywany.

1. Połączyć się online z F-CPU. Jeśli w sieci dostępnych jest kilka F-CPU (np. poprzez przemysłowy Ethernet) przy pomocy urządzenia programistycznego lub PC, należy upewnić się, że połączono z właściwym F-CPU: Przykład: „Online & diagnostics" > "Online accesses " > "Flash LED" (Online i diagnostyka > Dostęp online > Migająca LED).
2. Otworzyć *Safety Administration Editor*.
3. Sprawdzić, czy zbiorcze podpisy bezpieczeństwa online i offline są zgodne z podpisami z podsumowania bezpieczeństwa.
4. Następnie sprawdzić w dziale „Ogólne" pod hasłem „Status programu bezpieczeństwa", czy programy bezpieczeństwa są identyczne w wersji online i offline.

   Przy pomocy „Status" oraz „Porównanie wersji" można sprawdzić bieżącą sytuację i, w razie potrzeby, wykonać zalecane środki:

Status	Porównanie wersji	Komunikat	Środek
	nieistotne	Programy bezpieczeństwa różnią się.	• Upewnić się, że podłączony jest wymagany F-CPU. • Należy pobrać program bezpieczeństwa do F-CPU
		Programy bezpieczeństwa są identyczne, lecz stosowane są różne wersje bloków bezpieczeństwa.	Program bezpieczeństwa musi zostać pobrany do F-CPU w najnowszej wersji, by był skuteczny.
		Programy bezpieczeństwa są identyczne.	Brak

Należy pamiętać, że jedynie porównanie zmian stanowi rzetelne źródło informacji o tym, czy programy bezpieczeństwa są identyczne. Wyświetlanie podpisów służy do szybkiej identyfikacji zmian.

11.9 Pozostałe charakterystyki

Wstęp

Należy również sprawdzić kilka innych charakterystyk, które są istotne do zatwierdzenia projektu.

Kontrola wykonalności transmisji danych ze standardowego programu do programu bezpieczeństwa

Należy sprawdzić, czy kontrola wykonalności została zaprogramowana dla wszystkich danych przekazywanych ze standardowego programu użytkownika do programu bezpieczeństwa. W tym celu dział „Dane ze standardowego programu użytkownika." wyszczególnia wszystkie tagi standardowego programu użytkownika odczytywane w programie bezpieczeństwa. Tagi standardowego program użytkownika zapisywane w programie bezpieczeństwa nie są tu wyszczególnione, ponieważ kontrola wykonalności nie jest dla nich wymagana. Więcej informacji dostępnych jest w ostrzeżeniu S015 w dziale „Transfer danych ze standardowego programu do programu bezpieczeństwa" (strona 207).

Sprawdzanie wersji programu

Należy sprawdzić, czy wersja *STEP 7 Safety* użyta do utworzenia podsumowania (w stopce wydruku) jest co najmniej równa wersji użytej do skompilowania programu bezpieczeństwa. Drugą wersję można znaleźć w dziale „Informacje ogólne" podsumowania bezpieczeństwa, pod hasłem „Zastosowane wersje". Obie wersje muszą być wyszczególnione w Załączniku 1 raportu do certyfikacji TÜV.

Możliwość wyłączenia trybu bezpieczeństwa

Należy upewnić się, że nie jest możliwe wyłączenie trybu bezpieczeństwa. Więcej informacji na ten temat można znaleźć w dziale „Informacje ogólne", pod hasłem „Ustawienia programu bezpieczeństwa". Ustawienia te zapewniają, iż nie jest możliwe przypadkowe wyłączenie trybu bezpieczeństwa programu. Więcej informacji można znaleźć w ostrzeżeniu S027 dziale „Wyłączanie trybu bezpieczeństwa" (strona 360).

Ochrona dostępu

Należy sprawdzić dział „Informacje ogólne" pod hasłem „Ochrona dostępu", by określić, czy dozwolone są ustawienia dla ochrony dostępu. Należy mieć na uwadze poniższe ostrzeżenie.

W przeciwnym razie nie można zatwierdzić projektu, ponieważ program bezpieczeństwa w F-CPU nie jest chroniony przed nieupoważnionym dostępem.

OSTRZEŻENIE

(S7-300, S7-400) W trybie bezpieczeństwa, dostęp za pomocą hasła CPU nie może być autoryzowany podczas wprowadzania zmian w standardowym programie użytkownika, ponieważ pozwoliłoby to na zmiany w programie bezpieczeństwa. Aby wykluczyć taką możliwość, należy ustawić poziom zabezpieczenia „Write protection for fail-safe blocks" (Ochrona zapisu dla bloków fail-safe) i skonfigurować hasło dla F-CPU. Jeśli tylko jedna osoba jest upoważniona do zmiany standardowego programu użytkownika oraz programu bezpieczeństwa, należy ustawić poziom zabezpieczenia „Write protection" (Ochrona zapisu) lub „Read/write protection" (Ochrona odczytu/zapisu), by inne osoby miały jedynie ograniczony dostęp lub brak dostępu do całego programu użytkownika (programów standardowego i bezpieczeństwa). *(S001)*

OSTRZEŻENIE

(S7-1200, S7-1500) W trybie bezpieczeństwa, program bezpieczeństwa musi być zabezpieczony hasłem. W tym celu należy ustawić poziom zabezpieczenia co najmniej „Full access (no protection)" (Pełny dostęp (brak ochrony)) i przypisać hasło do „Full access incl. fail-safe (no protection)" (Pełny dostęp wraz z fail-safe (brak ochrony)). Ten poziom zabezpieczenia pozwala jedynie na pełny dostęp do standardowego programu użytkownika, nie do bloków bezpieczeństwa.

W przypadku wybrania wyższego poziomu, na przykład w celu zabezpieczenia standardowego programu użytkownika, należy przypisać dodatkowe hasło do opcji „Full access (no protection)" (Pełny dostęp (brak ochrony)).

11.10 Zatwierdzenie zmian

Wstęp

Ogólnie rzecz biorąc, można przyjąć takie samo podejście do zatwierdzenia zmian jak w początkowym zatwierdzeniu (patrz „Przegląd zatwierdzenia systemu" (strona 376)).

Należy sprawdzić wszystkie dane projektu safety (program bezpieczeństwa oraz odpowiednią konfigurację sprzętową) pod kątem zmian.

OSTRZEŻENIE

W przypadku zatwierdzenia zmian, należy sprawdzić, czy zamierzone zmiany zostały wprowadzone poprawnie i w pełni.

Należy również sprawdzić, czy nie doszło do niezamierzonych zmian w innym miejscu (przykładowo, dodane I/O lub instrukcje). *(S072)*

Aby uniknąć konieczności zatwierdzania całego systemu w przypadku nieistotnych zmian, *STEP 7 Safety* pozwala na zidentyfikowanie tych części programu bezpieczeństwa, które uległy zmianie.

- Kontrola zmienionych lub nowo dodanych bloków bezpieczeństwa.
- Kontrola zmienionych lub nowo dodanych instrukcji i bloków systemu
- bezpieczeństwa. Kontrola parametrów związanych z bezpieczeństwem w
- zmienionych lub nowo dodanych F-I/O.
- Kontrola struktury konfiguracji sprzętowej związanej z bezpieczeństwem (np. położenie
- gniazd lub adresów początkowych F-I/O).

Następnie wykonuje się test funkcji bloków bezpieczeństwa/F-I/O objętych zmianą.

Należy sprawdzić, czy zmiany nie mają wpływu na niezmienione części danych projektu związanych z bezpieczeństwem, zwłaszcza w przypadku usuniętych bloków bezpieczeństwa lub usuniętych F-I/O.

Uwaga

Zatwierdzenie zmian nie jest możliwe po migracji CPU.

⚠OSTRZEŻENIE

Wykonując zmiany, w których przypisanie adresów wejść/wyjść i okablowanie może się zmienić, należy wykonać test podłączenia (strona 363).

Przykładami takich zmian są:

- Dodanie F-I/O
- Zmiana adresu początkowego F-I/O
- Zmiana pozycji gniazda F-I/O
- Zmiana
  - rack'a
  - adresu urządzenia podrzędnego
  - podsieci PROFIBUS DP/PROFINET IO
  - adresu IP
  - nazwy urządzenia

(S071)

Wykrywanie zmian w danych projektu związanych z bezpieczeństwem

Do identyfikacji istotnych zmian potrzebne są dwa projekty TIA:

- Projekt odniesienia: Zawiera początkowo zaakceptowane dane projektu. Stanowią one punkt początkowy dalszego porównania.
- Projekt do zatwierdzenia: Zawiera bieżące dane projektu safety. Jest to wynik projektu odniesienia oraz wprowadzonych na nim zmian.

Aby wykryć zmiany, konieczne jest porównanie danych projektu związanych z bezpieczeństwem z projektu odniesienia z danymi projektu do zatwierdzenia.

Zbiorczy podpis bezpieczeństwa to szybki krok pozwalający na określenie, czy wprowadzono istotne zmiany. Jeśli podpis uległ zmianie, w danych projektu wystąpią znaczące zmiany.

(S7-1200, S7-1500) Można użyć zbiorczego podpisu F-SW, zbiorczego podpisu F-HW oraz podpisu adresu komunikacji bezpieczeństwa do określenia, czy zmiany obejmują program bezpieczeństwa (zmieniony zbiorczy podpis F-SW) i/lub dane projektu safety (zbiorczy podpis F-HW) i/lub dane komunikacji (z Flexible F-Link, podpis adresu komunikacji bezpieczeństwa).

Wykrywanie zmian w programie bezpieczeństwa

Szybką opcją do wykrywania zmian w programie bezpieczeństwa jest porównanie zbiorczego podpisu F-SW danych projektu związanych z bezpieczeństwem w projekcie odniesienia ze zbiorczym podpisem F-SW w danych projektu do zatwierdzenia. Jeśli się różnią, oznacza to, że w programie do zatwierdzenia powstały zmiany.

Aby odszukać zmiany w programie bezpieczeństwa, należy wykonać porównanie offline-offline pomiędzy programem bezpieczeństwa projektu do zatwierdzenia a programem projektu odniesienia (patrz „Porównywanie programów bezpieczeństwa" (strona 354)). Należy użyć ustawienia filtra „Compare only F-blocks relevant for certification" (Porównaj tylko bloki bezpieczeństwa istotne dla certyfikacji). Ogranicza to wynik porównania jedynie do tych bloków bezpieczeństwa, które należy uwzględnić przy zatwierdzaniu zmian.

⚠ OSTRZEŻENIE

Należy upewnić się, że kryterium porównania „Safety" (Bezpieczeństwo) zostało włączone, by uwzględnić kryteria istotne dla zatwierdzenia zmian. *(S069)*

Wyłączając pozostałe kryteria porównania, można odznaczyć te różnice, które są nieistotne dla zatwierdzenia zmian (np. znacznik czasowy).

Stan porównania pomaga zidentyfikować, które bloki bezpieczeństwa uległy zmianie.

Wykrywanie zmian w konfiguracji sprzętowej związanej z bezpieczeństwem

Szybką opcją do wykrywania zmian w konfiguracji sprzętowej związanej z bezpieczeństwem jest porównanie zbiorczego podpisu F-HW danych projektu związanych z bezpieczeństwem w projekcie odniesienia ze zbiorczym podpisem F-HW w danych projektu do zatwierdzenia. Jeśli się różnią, oznacza to, że w konfiguracji sprzętowej do zatwierdzenia powstały zmiany.

Jeśli zbiorczy podpis F-HW uległ zmianie, a wszystkie urządzenia F-I/O pozostały niezmienne, wskazuje to, że uległy zmianie parametry safety F- CPU bądź struktura konfiguracji sprzętowej związanej z bezpieczeństwem; przykładowo, może chodzić o pozycję gniazd.

Możliwe są dwa sposoby lokalizacji zmian dotyczących bezpieczeństwa w konfiguracji sprzętowej:

- Porównanie w edytorze porównania
- Porównanie oparte na dwóch podsumowaniach bezpieczeństwa

Porównanie w edytorze porównania

Projekt odniesienia i projekt do zatwierdzenia muszą być spójne i skompilowane, by móc wykonać porównanie. Aby wykonać porównanie, patrz „Porównywanie programów bezpieczeństwa" (strona 354).

1. Przejść w wyniku porównania do folderu „System blocks > STEP 7 Safety > F-I/O DBs". Wszystkie bloki danych wyszczególnione w tym folderze to DB F-I/O i są przypisane do F-I/O.
   - Jeśli DB F-I/O w wyniku porównania są identyczne, oznacza to, że konfiguracja safety przypisanych F-I/O nie została zmieniona.

     Standardowe parametry mogły ulec zmianie.
   - Jeśli DB F-I/O w wyniku porównania nie są identyczne, oznacza to, że konfiguracja safety przypisanych F-I/O została zmieniona.
   - Jeśli DB F-I/O w wyniku porównania zostały oznaczone jako „nieistniejące", powiązane urządzenia F-I/O mogły zostać usunięte, dodane lub nazwa adresów początkowych urządzeń F-I/O została zmieniona. W takim przypadku można odszukaćprzypisanie DB F-I/O do określonego F-I/O w podsumowaniu bezpieczeństwa pod hasłem „Konfiguracja sprzętowa F-I/O".
2. W przypadku odszukania zmienionego F-I/O, można sprawdzić zmienione parametry w podsumowaniu bezpieczeństwa w sposób opisany poniżej.

Porównanie oparte na dwóch podsumowaniach bezpieczeństwa

Porównanie oparte na dwóch podsumowaniach bezpieczeństwa należy wykonać w

następujący sposób:

1. W dziale „Konfiguracja sprzętowa F-I/O" należy porównać adresy początkowe (adresy I/O), parametr „Zachowanie po usterce kanału" oraz gniazdo F-I/O.
2. W tabeli omówienia w dziale „Konfiguracja sprzętowa F-I/O" należy porównać CRC parametru F-I/O z tymi w podsumowaniu bezpieczeństwa zatwierdzonego F-CPU.
   - Jeśli „Podpis parametru (bez adresów)" różni się dla F-I/O, wskazuje to na istnienie zmian związanych z bezpieczeństwem w parametrach bezpieczeństwa F-I/O. Ponadto, adresy PROFIsafe również mogły ulec zmianie.

     W takim przypadku należy sprawdzić odnośną tabelę szczegółów parametrów związanych z bezpieczeństwem F-I/O i zweryfikować unikalność adresów PROFIsafe.
   - Jeśli „Podpis parametru (bez adresów)" jest identyczny, jedynie adresy PROFIsafe mogły ulec zmianie.

     W takim przypadku wystarczy potwierdzić unikalność adresów PROFIsafe.

Należy wykonać kontrolę zgodnie z opisem w dziale „Kompletność i poprawność konfiguracji sprzętowej: (strona 383).

(S7-1200, S7-1500) Wykrywanie zmian w komunikacji z Flexible F-Link

Szybką opcją do wykrywania zmian w konfiguracji komunikacji z Flexible F-Link jest porównanie podpisu adresu komunikacji bezpieczeństwa danych projektu związanych z bezpieczeństwem w projekcie odniesienia z podpisem adresu komunikacji bezpieczeństwa danych projektu do zatwierdzenia. Jeśli się różnią, oznacza to, że w konfiguracji komunikacji (tylko UUID) z Flexible F-Link do zatwierdzenia powstały zmiany. Pozostałe parametry komunikacji, takie jak przekroczenie czasu lub kierunek transmisji są obejmowane przez zbiorczy podpis F-SW (patrz „Wykrywanie zmian w programie bezpieczeństwa" powyżej).

Aby zlokalizować zmiany w konfiguracji komunikacji z Flexible F-Link, należy porównać tabelę „Przegląd komunikacji poprzez Flexible F-Link" projektu odniesienia w odpowiednim podsumowaniu z tabelą w projekcie do zatwierdzenia.

Zobacz także

Dostęp do tagów DB F-I/O (strona 184)

Obsługa i konserwacja

12

12.1 Uwagi dotyczące trybu bezpieczeństwa

Wstęp

Należy uwzględnić poniższe ważne uwagi dotyczące trybu bezpieczeństwa programu bezpieczeństwa.

Użycie urządzeń/programów symulacyjnych

⚠OSTRZEŻENIE

Użycie urządzeń/programów symulacyjnych w instalacjach

W przypadku korzystania z urządzeń lub programów symulacyjnych generujących ramki komunikatów bezpieczeństwa, przykładowo, opartych na PROFIsafe, i udostępniania ich do systemu bezpieczeństwa SIMATIC Safety poprzez system magistrali (np. PROFIBUS DP lub PROFINET IO), należy zapewnić bezpieczeństwo systemu poprzez zastosowanie środków organizacyjnych, takich jak monitorowanie operacyjne oraz ręczne wyłączenie bezpieczeństwa.
Należy pamiętać, że analizator protokołu nie może wykonywać żadnych funkcji, które powielają zarejestrowane sekwencje ramek komunikatów z poprawnym zachowaniem czasowym.

Wersja *S7-PLCSIM* < 15.1 lub *wersja S7-PLCSIM Advanced* < 2.0 SP1 oraz wersja systemu bezpieczeństwa < 2.2

W przypadku korzystania z *S7-PLCSIM* (strona 359) do symulowania programów bezpieczeństwa, środki określone powyżej nie są wymagane, ponieważ S7-PLCSIM nie jest w stanie ustanowić połączenia online z rzeczywistym elementem.

Wersja *S7-PLCSIM* ≥ 15.1 lub *wersja S7-PLCSIM Advanced* ≥ 2.0 SP1 oraz wersja systemu bezpieczeństwa ≥ 2.2

Należy zagwarantować bezpieczeństwo systemu poprzez środki organizacyjne, np. poprzez monitorowanie operacji oraz ręczne wyłączenie bezpieczeństwa.

Ponadto, załadowanie programu bezpieczeństwa z systemem bezpieczeństwa w wersji 2.2 i wyższej do *S7-PLCSIM* jest dozwolone jedynie od *S7-PLCSIM* V15.1 lub *S7-PLCSIM Advanced* V2.0 SP1. *(S030)*

Uwaga

W przypadku *S7-PLCSIM* przed V15.1 lub *S7-PLCSIM Advanced* przed V2.0 SP1 oraz wersji systemu bezpieczeństwa 2.2 lub wyższej, program bezpieczeństwa przechodzi w tryb STOP i tworzone jest stosowne zdarzenie diagnostyczne.

Przełączenie F-CPU w tryb STOP

OSTRZEŻENIE

STOP, przykładowo, poprzez urządzenie programistyczne/PC, przełącznik trybu, funkcję komunikacyjną lub instrukcję „STP"

Uruchomienie trybu STOP, przykładowo, za pomocą urządzenia programistycznego/PC, przełącznika trybu, funkcji komunikacyjnej lub instrukcji „STP", a także utrzymanie tego trybu nie jest powiązane z bezpieczeństwem. Taki stan STOP można łatwo (i nieumyślnie) cofnąć, przykładowo, korzystając z urządzenia programistycznego/PC.

Po przełączeniu F-CPU z trybu STOP na RUN, standardowy program użytkownika uruchamia się w normalny sposób. Po uruchomieniu programu bezpieczeństwa wszystkie F-DB są inicjalizowane z wartościami z pamięci "load memory" – jak w przypadku zimnego restartu. Oznacza to, że zapisane informacje o błędach są kasowane. System bezpieczeństwa automatycznie reintegruje F-I/O.

Jeśli proces nie pozwala na taki rozruch, należy zaprogramować ochronę restartu/rozruchu w programie bezpieczeństwa: Wyjście danych procesowych musi być zablokowane do czasu ręcznego aktywowania. Aktywacja ta nie może wystąpić do chwili, gdy można bezpiecznie wyprowadzić dane procesowe, a usterki zostały skorygowane (patrz „Programowanie zabezpieczenia rozruchu" (strona 165)). *(S031)*

Błąd CRC w komunikacji związanej z bezpieczeństwem

Uwaga

Błąd CRC w komunikacji związanej z bezpieczeństwem

W przypadku, gdy F-CPU wymaga ręcznego zatwierdzenia błędu CRC więcej niż raz w okresie 100 godzin, i powtarza się to wielokrotnie, należy sprawdzić, czy zostały zastosowane wytyczne instalacyjne dla PROFINET lub PROFIBUS.

Wystąpił błąd CRC, jeśli:

- Tag ACK_REQ dla DB F-I/O jest ustawiony, a tag DIAG dla DB F-I/O (bit 2 lub bit 6) wskazuje błędy CRC

  lub
- błąd CRC został wprowadzany do bufora diagnostycznego F-CPU

W takim przypadku, wartości prawdopodobieństwa awarii (https://support.industry.siemens.com/cs/ww/en/view/109481784) (PFD_{avg}/PFH) dla komunikacji związanej z bezpieczeństwem nie mają dłużej zastosowania.

Informacje dotyczące wytycznych instalacji dla PROFINET oraz PROFIBUS można znaleźć pod adresem:

- Wytyczne instalacji PROFIBUS (www.profibus.com/PBInstallationGuide)
- Technologia łączeniowa PROFIBUS (http://www.profibus.com/nc/downloads/downloads/profibus-interconnection-technology/display/)
- Wytyczne instalacji PROFINET (www.profibus.com/PNInstallationGuide)
- Technologia łączeniowa i okablowania PROFINET (http://www.profibus.com/nc/downloads/downloads/profinet-cabling-and-interconnection-technology/display/)
- Wymogi środowiskowe PROFIsafe (www.profibus.com/PROFIsafeRequirements)

Gdy ocena wskazuje, że wytyczne konfiguracji dla PROFIBUS i PROFINET zostały spełnione, należy skontaktować się z działem obsługi klienta.

12.2 Wymiana elementów programowych i sprzętowych

Wymiana elementów programowych

Podczas wymiany elementów programowych w urządzeniu programistycznym lub PC, np. na nową wersję *STEP 7*, należy przestrzegać informacji dotyczących kompatybilności wstępnej i zstępnej w dokumentacji oraz plikach readme danych produktów (np. *STEP 7 Safety*).

Podczas wymiany *STEP 7 Safety* należy sprawdzić, czy wersja *STEP 7 Safety* została ujęta na liście w Załączniku 1 raportu do certyfikacji TÜV.

Wymiana elementów sprzętowych

Elementy sprzętowe SIMATIC Safety (F-CPU, F-I/O, baterie itp.) wymienia się identycznie jak w standardowym systemie automatyzacji.

Wymiana sterowników programowych S7-1500

⚠ OSTRZEŻENIE

Po wymianie modułu CPU (np. nowy PC z nośnikiem danych ze starego PC) lub wymianie nośnika danych (np. nośnik danych z programem bezpieczeństwa 1 został zastąpiony nośnikiem z programem bezpieczeństwa 2), przy pomocy Panelu należy sprawdzić, wyświetlany jest poprawny zbiorczy podpis bezpieczeństwa lub wykonać identyfikację programu. *(S066)*

Usuwanie i wstawianie F-I/O podczas pracy

Jeśli usunięcie i wstawienie jest możliwe dla standardowego I/O podczas pracy, jest również możliwe dla odnośnego F-I/O. Należy jednak pamiętać, że wymiana modułu F-I/O podczas pracy może spowodować błąd komunikacji w F-CPU.

Należy zatwierdzić błąd komunikacji w programie bezpieczeństwa w tagu ACK_REI dla DB F-I/O (strona 174) lub, alternatywnie, przy pomocy instrukcji „ACK_GL" (strona 518). Bez zatwierdzenia F-I/O pozostanie pasywowany.

Aktualizacja oprogramowania CPU

Należy sprawdzić system operacyjny CPU dla zatwierdzenia bezpieczeństwa: Korzystając z nowego systemu operacyjnego CPU (aktualizacji oprogramowania), należy sprawdzić, czy wykorzystywany system operacyjny CPU jest zatwierdzony do użytku w systemie bezpieczeństwa.

Minimalne wersje systemu operacyjnego CPU z gwarantowaną kompatybilnością zostały podane w załączniku do certyfikacji. Należy uwzględnić tę informację oraz wszelkie uwagi dotyczące nowego systemu operacyjnego CPU.

Aktualizacja oprogramowania modułu interfejsu

Wykorzystując nowy system operacyjny do modułu interfejsu, np. IM 151-1 HIGH FEATURE ET 200S (aktualizacja oprogramowania), należy zastosować następujące zalecenia:

Jeśli wybrano opcję „Activate firmware after update" (Aktywuj oprogramowanie po aktualizacji) dla aktualizacji oprogramowania (patrz *pomoc do STEP 7*, „Online i diagnostyka"), IM zostanie automatycznie zresetowany po pomyślnym pobraniu, a następnie uruchomi się na nowej wersji systemu operacyjnego. Należy pamiętać, że aktualizacja oprogramowania modułu interfejsu podczas pracy generuje błąd komunikacji w F-CPU.

Należy zatwierdzić błąd komunikacji w programie bezpieczeństwa w tagu ACK_REI dla DB F-I/O (strona 174) lub, alternatywnie, przy pomocy instrukcji „ACK_GL" (strona 518). Bez zatwierdzenia F-I/O pozostanie pasywowany.

Konserwacja zapobiegawcza (test odporności)

Test odporności złożonych podzespołów elektronicznych oznacza zazwyczaj wymianę na nowe, nieużywane elementy.

Wartości PFD_{avg} i PFH dla F-CPU S7-300/400 oraz F-I/O

Lista wartości prawdopodobieństwa awarii (wartości PFD_{avg}, PFH) dla elementów stosowanych w systemie SIMATIC Safety dostępna jest w internecie (https://support.industry.siemens.com/cs/ww/en/view/109481784).

Wartości PFD_{avg} i PFH dla F-CPU S7-1200/1500-I/O

Poniżej zamieszczono wartości prawdopodobieństwo uszkodzenia (wartości PFD_{avg}, PFH) dla F-CPU S7-1200/1500 o trwałości użytkowej 20 lat i czasie użytkowania 100 godzin:

Tryb rzadkiego przywołania do działania **Zgodnie z IEC 61508:2010:** **PFD_{avg} = Średnie prawdopodobieństwo uszkodzenia przy przywołaniu do działania**	**Tryb wysokiego zapotrzebowania/tryb ciągły** **Zgodnie z IEC 61508:2010:** **PFH = Średnia częstotliwość niebezpiecznego uszkodzenia [h^{-1}]**
< 2E-05	< 1E-09

Wartości PFD_{avg} i PFH dla komunikacji związanej z bezpieczeństwem

Poniżej zamieszczono wartości prawdopodobieństwa uszkodzenia (wartości PFD_{avg}, PFH) dla komunikacji związanej z bezpieczeństwem:

Tryb rzadkiego przywołania do działania **Zgodnie z IEC 61508:2010:** **PFD_{avg} = Średnie prawdopodobieństwo uszkodzenia przy przywołaniu do działania**	**Tryb wysokiego zapotrzebowania/tryb ciągły** **Zgodnie z IEC 61508:2010:** **PFH = Średnia częstotliwość niebezpiecznego uszkodzenia [h^{-1}]**
< 1E-05*	< 1E-09*

*** Uwaga dla F-CPU S7-300/400:**

Wartość PFH obowiązuje przy założeniu, że w funkcji bezpieczeństwa działa maksymalnie 100 F-I/O. W przypadku wykorzystywania więcej niż 100 F-I/O, należy dodać 4E-12 na F-I/O dla funkcji bezpieczeństwa.
Wartość PFD_{avg} obowiązuje dla czasu użytkowania 20 lat oraz przy założeniu, że w funkcji bezpieczeństwa działa maksymalnie 25 F-I/O. W przypadku wykorzystywania więcej niż 25 F-I/O, należy dodać 3,5E-7 na F-I/O dla funkcji bezpieczeństwa.

12.3 Przewodnik po diagnostyce (S7-300, S7-400)

Wstęp

Poniżej zamieszczono zestawienie możliwości diagnostycznych, które można ocenić w razie wystąpienia błędu systemu. Większość możliwości diagnostycznych jest identycznych jak w standardowych systemach automatyki. Kolejność kroków przedstawia zalecenia.

Kroki oceny możliwości diagnostycznych

Poniższa tabela przedstawia kroki do oceny możliwości diagnostycznych.

Krok	Procedura	Odniesienia
1	**Ocena LED na sprzęcie (F-CPU, F-I/O):** • LED BUSF na F-CPU: Miga, gdy wystąpił błąd komunikacji na PROFIBUS DP/PROFINET IO: Włączona, jeśli błąd programowania wystąpi, gdy OB 85 oraz OB 121 zostały zaprogramowanie (np. instancja DB nie została wczytana) • LED STOP LED na F-CPU: zapala się, gdy F-CPU przechodzi w tryb STOP • LED usterki na F-I/O: np. SF-LED (LED błędu grupy) włącza się, gdy wystąpi usterka indywidualnego F-I/O	*Instrukcje obsługi do F-CPU i F-I/O*
2	**Ocena bufora diagnostycznego modułów:** Bufor diagnostyczny modułu (F-CPU, F-I/O, CP) odczytuje się w jego widoku online i diagnostycznym w grupie „Diagnostic buffer" (Bufor diagnostyczny) w folderze „Online & Diagnostics".	*Pomoc do STEP 7 oraz instrukcje obsługi do F-CPU i F-I/O*
3	**Ocena stosów F-CPU:** gdy F-CPU jest w trybie STOP, należy odczytać kolejno: • Stos bloku: Należy sprawdzić, czy tryb STOP w F-CPU został wyzwolony przez blok bezpieczeństwa programu bezpieczeństwa • Stos przerwania • Stos danych lokalnych	*Pomoc do STEP 7*

Krok	Procedura	Odniesienia
4	**Ocenić tag diagnostyczny DB F-I/O, korzystając z funkcji testowania i odbioru technicznego, za pomocą systemu kontroli operatorskiej i monitorowania, lub w standardowym programie użytkownika:** Ocenić tag DIAG w DB F-I/O	Dostęp F-I/O (strona 166)
5	**Ocenić wyjścia diagnostyczne instancji DB instrukcji, korzystając z funkcji testowania i odbioru technicznego, za pomocą systemu kontroli operatorskiej i monitorowania, lub w standardowym programie użytkownika:** • Ocenić następujące elementy dla MUTING, EV1oo2DI, TWO_H_EN, MUT_P, ESTOP1, FDBACK, SFDOOR w przypisanej instancji DB: – Wyjście DIAG • Ocenić następujące elementy dla SENDDP lub RCVDP w przypisanej instancji DB: – Wyjście RET_DPRD/RET_DPWR – Wyjście DIAG • Ocenić następujące elementy dla SENDS7 lub RCVS7 w przypisanej instancji DB: – Wyjście STAT_RCV – Wyjście STAT_SND – Wyjście DIAG	Instrukcje

Wskazówki dotyczące RET_DPRD/RET_DPWR

Informacje diagnostyczne wyjść RET_DPRD/RET_DPWR instrukcji SENDDP lub RCVDP odpowiadają informacjom diagnostycznym wartości zwrotnej RETVAL z instrukcji „DPRD_DAT" oraz „DPWR_DAT". Opis instrukcji „DPRD_DAT" oraz „DPWR_DAT" można znaleźć w pomocy do *STEP 7*.

Wskazówka: STAT_RCV oraz STAT_SND

Informacje diagnostyczne wyjścia STAT_RCV instrukcji SENDS7 lub RCVS7 odpowiadają informacjom diagnostycznym wyjścia STATUS z instrukcji „URCV". Informacje diagnostyczne wyjścia STAT_SND instrukcji SENDS7 lub RCVS7 odpowiadają informacjom diagnostycznym wyjścia STATUS z instrukcji „USEND". Opis instrukcji „UCRV" oraz „USEND" można znaleźć w pomocy do *STEP 7*.

12.4 Przewodnik po diagnostyce (S7-1500)

Szczegółowe informacje dotyczące diagnostyki F-CPU S7-1500 można znaleźć w instrukcji funkcji „Diagnostyka" (http://support.automation.siemens.com/WW/view/en/59192926).

12.5 Przewodnik po diagnostyce (S7-1200)

Szczegółowe informacje dotyczące diagnostyki F-CPU S7-1200 można znaleźć w instrukcji „Bezpieczeństwo funkcjonalne S7-1200" (http://support.automation.siemens.com/WW/view/en/104547552).

Instrukcje do STEP 7 Safety

13

Przegląd instrukcji do programu bezpieczeństwa

Podczas programowania bloku bezpieczeństwa, wszystkie instrukcje dostępne do programowania w LAD lub FBD ze skonfigurowanym F-CPU można znaleźć w karcie zadań „Instructions" (Instrukcje).

Oprócz instrukcji znanych z programowania standardowego bloku, dostępne są również specjalne funkcje bezpieczeństwa, np. do monitorowania oburęcznego, analizy rozbieżności, mutingu, zatrzymania/wyłączenia awaryjnego, monitorowania drzwi bezpieczeństwa oraz monitorowania sygnału zwrotnego oraz instrukcji do komunikacji CPU związany z bezpieczeństwem – CPU.

Należy mieć na uwadze następujące zagadnienia

Uwaga

Nie można połączyć włączonego wejścia EN oraz włączonego wyjścia ENO. Wyjątek:

(S7-1200, S7-1500) Przy użyciu poniższych instrukcji można zaprogramować wykrywanie nadmiernego przepływu poprzez podłączenie włączonego wyjścia ENO:

- ADD: Dodawanie (STEP 7 Safety V16) (strona 554)
- SUB: Odejmowanie (STEP 7 Safety V16) (strona 557)
- MUL: Mnożenie (STEP 7 Safety V16) (strona 560)
- DIV: Dzielenie (STEP 7 Safety V16) (strona 563)
- NEG: Tworzenie uzupełnienia dwójkowego(STEP 7 Safety V16) (strona 567)
- ABS: Tworzenie wartości bezwzględnej (STEP 7 Safety V16) (S7-1200, S7-1500) (strona 570)
- CONVERT: Konwertowanie wartości (STEP 7 Safety V16) (strona 584)

13.1 Ogólne

13.1.1 LAD

13.1.1.1 Nowa sieć (STEP 7 Safety V16)

Wymogi

Blok bezpieczeństwa jest otwarty.

Procedura

Aby wstawić nowy blok, należy wykonać następujące kroki:

1. Należy wybrać sieć, po której ma zostać wstawiona nowa sieć.
2. Wybrać polecenie „Insert network" (Wstaw sieć) z menu skrótów.

Uwaga

W przypadku wstawienia elementu do ostatniej pustej sieci bloku bezpieczeństwa w programie LAD, poniżej zostanie automatycznie wstawiona nowa pusta sieć.

Wynik

Do bloku bezpieczeństwa zostanie wstawiona nowa pusta sieć.

13.1.1.2 Puste pole (STEP 7 Safety V16)

Wymogi

Dostępna sieć.

Procedura

Aby wstawić instrukcję LAD do sieci przy użyciu pustego pola, należy wykonać następujące kroki:

1. Otworzyć kartę zadania „Instructions" (Instrukcje).
2. Przejść do „Basic instructions > General > Empty box" (Instrukcje podstawowe > Ogólne > Puste pole).
3. Korzystając z funkcjonalności przeciągnij-i-upuść, przesunąć element „Empty box" (Puste pole) do żądanego miejsca w sieci.
4. Przesunąć kursor nad żółty trójkąt w prawym górnym narożniku pustego pola. Wyświetli się rozwijana lista.
5. Wybrać wymaganą instrukcję z rozwijanej listy.

Jeśli instrukcja działa jak blok funkcyjny (FB) w systemie, otworzy się okno „Call options" (Opcje wywołania). W tym oknie można utworzyć blok danych instancji dla bloku funkcyjnego, zarówno jako pojedynczą instancję, jak i, w razie potrzeby instancję wielokrotną, w której przechowywane są dane wstawionych instrukcji. Po utworzeniu nowego bloku, znajduje się on w folderze „Program resources" w drzewku projektu pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe). W przypadku wybrania instancji wielokrotnej, jest ona dostępna w interfejsie bloku, w dziale „Static" (Statyczny).

Wynik

Puste pole jest zamieniane na odpowiednią instrukcję. Dla parametrów wstawiane są symbole zastępcze.

13.1.1.3 Otwieranie rozgałęzienia (STEP 7 Safety V16)

Opis

Za pomocą rozgałęzień można zaprogramować połączenia równoległe w języku programowania LAD. Rozgałęzienia są wstawiane do głównej ścieżki bieżącej. Możliwe jest wstawienie kilku styków na odgałęzieniu, tworząc tym połączenie równoległe z połączeń szeregowych. W ten sposób można zaprogramować skomplikowane schematy drabinkowe.

Wymogi

- Dostępna sieć.
- Sieć zawiera elementy.

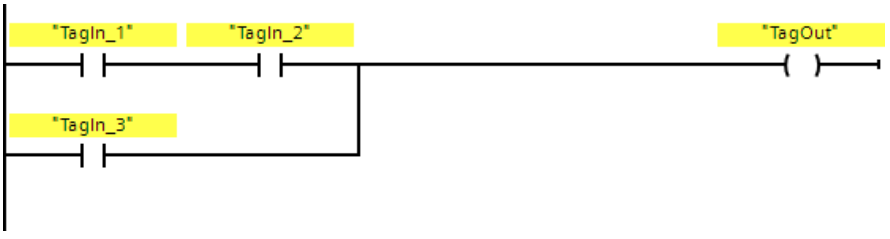
Procedura

Aby wstawić nowe rozgałęzienie do sieci, należy wykonać następujące kroki:

1. Otworzyć kartę zadania „Instructions" (Instrukcje).
2. Przejść do „Basic instructions > General > Open branch" (Instrukcje podstawowe > Ogólne > Otwórz rozgałęzienie).
3. Korzystając z funkcjonalności przeciągnij-i-upuść, przesunąć element do żądanego miejsca w sieci.
4. Aby podłączyć nowe rozgałęzienie do szyny zasilającej, należy przeciągnąć element do szyny.

Przykład

Na poniższej ilustracji znajduje się przykład sposobu użycia rozgałęzień:



13.1.1.4 Zamykanie rozgałęzienia (STEP 7 Safety V16)

Opis

Rozgałęzienia muszą zostać zamknięte w odpowiednich miejscach. W razie potrzeby można ustawić je tak, by nie przecinały się wzajemnie.

Wymogi

Dostępne rozgałęzienie.

Procedura

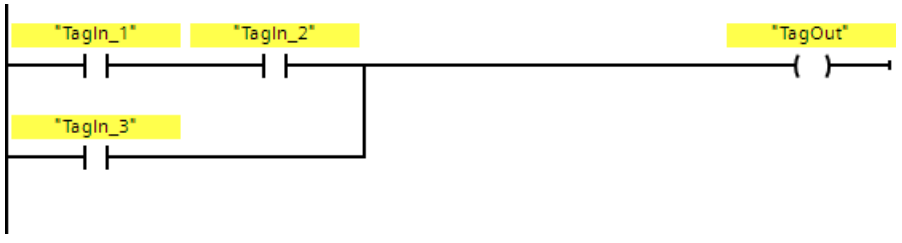
Aby zamknąć otwarte rozgałęzienie, należy wykonać następujące kroki:

1. Wybrać otwarte rozgałęzienie.
2. Wcisnąć i przytrzymać lewy przycisk myszy.

   Po przesunięciu kursora pojawi się przerywana linia.
3. Przeciągnąć linię w odpowiednie miejsce sieci. Dozwolone połączenia są wskazywane zielonymi liniami.
4. Zwolnić przycisk myszy.

Przykład

Na poniższej ilustracji znajduje się przykład sposobu użycia rozgałęzień:



13.1.2 FBD

13.1.2.1 Nowa sieć (STEP 7 Safety V16)

Wymogi

Blok bezpieczeństwa jest otwarty.

Procedura

Aby wstawić nowy blok, należy wykonać następujące kroki:

1. Należy wybrać sieć, po której ma zostać wstawiona nowa sieć.
2. Wybrać polecenie „Insert network" (Wstaw sieć) z menu

Uwaga

W przypadku wstawienia elementu do ostatniej pustej sieci bloku bezpieczeństwa w programie FBD, poniżej zostanie automatycznie wstawiona nowa pusta sieć.

Wynik

Do bloku bezpieczeństwa zostanie wstawiona nowa pusta sieć.

13.1.2.2 Puste pole (STEP 7 Safety V16)

Wymogi

Dostępna sieć.

Procedura

Aby wstawić elementy FBD do sieci przy użyciu pustego pola, należy wykonać następujące kroki:

1. Otworzyć kartę zadania „Instructions" (Instrukcje).
2. Przejść do „Basic instructions > General > Empty box" (Instrukcje podstawowe > Ogólne > Puste pole).
3. Korzystając z funkcjonalności przeciągnij-i-upuść, przesunąć element „Empty box" (Puste pole) do żądanego miejsca w sieci.
4. Przesunąć kursor nad żółty trójkąt w prawym górnym narożniku pustego pola. Wyświetli się rozwijana lista.
5. Wybrać żądany element FBD z rozwijanej listy.

Jeśli instrukcja działa jak blok funkcyjny (FB) w systemie, otworzy się okno „Call options" (Opcje wywołania). W tym oknie można utworzyć blok danych instancji dla bloku funkcyjnego, zarówno jako pojedynczą instancję, jak i, w razie potrzeby instancję wielokrotną, w której przechowywane są dane wstawionych instrukcji. Po utworzeniu nowego bloku, znajduje się on w folderze „Program resources" w drzewku projektu pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe).
W przypadku wybrania instancji wielokrotnej, jest ona dostępna w interfejsie bloku, w dziale „Static" (Statyczny).

Wynik

Puste pole jest zamieniane na odpowiednią instrukcję. Dla parametrów wstawiane są symbole zastępcze.

13.1.2.3 Otwieranie rozgałęzienia (STEP 7 Safety V16)

Opis

Rozgałęzienia, wstawiane pomiędzy polami, pozwalają na zaprogramowanie połączeń równoległych w języku programowania schematu bloków funkcyjnych (FBD). W rozgałęzieniu można wstawiać dodatkowe pola, tworząc tym złożone schematy bloków funkcyjnych.

Wymogi

Dostępna sieć.

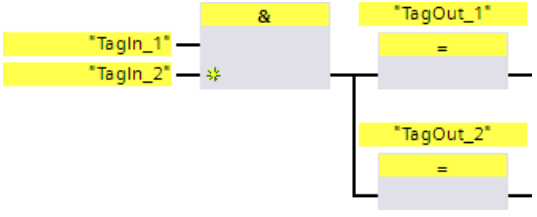
Procedura

Aby wstawić nowe rozgałęzienie do sieci, należy wykonać następujące kroki:

1. Otworzyć kartę zadania „Instructions" (Instrukcje).
2. Przejść do panelu „Basic instructions > General > Branch" (Instrukcje podstawowe > Ogólne > Rozgałęzienie).
3. Korzystając z funkcjonalności przeciągnij-i-upuść, przesunąć element do żądanego miejsca na linii łączącej dwa pola.

Przykład

Na poniższej ilustracji znajduje się przykład sposobu użycia rozgałęzień:



13.1.2.4 Wstawianie wejścia binarnego (STEP 7 Safety

Opis

Przy pomocy instrukcji „Insert binary input" (Wstaw wejście binarne) można rozszerzyć pole jednej z poniższych instrukcji o wejście binarne:

- „AND logic operation" (operacja logiczna AND)
- „OR logic operation" (operacja logiczna OR)
- „EXCLUSIVE OR logic operation" (Operacja logiczna EXCLUSIVE OR)

Można wykonać zapytanie o stan sygnału kilku argumentów, rozszerzając pole instrukcji.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wejście	BOOL	Argument wskazuje bit, stan sygnału którego zostanie sprawdzony.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:

Pole instrukcji „AND logic operation" (operacja logiczna AND) rozstało rozszerzone przez dodatkowe wejście binarne, na którym wykonywane jest zapytanie o stan sygnału argumentu
„TagIn_3". Wyjście „TagOut" jest ustawiane, gdy stan sygnału argumentów „TagIn_1", „TagIn_2" oraz „TagIn_3" to „1".

Zobacz także

Operacja logiczna AND (STEP 7 Safety V16) (strona 439)

Operacja logiczna OR (STEP 7 Safety V16) (strona 441)

X:Operacja logiczna EXCLUSIVE OR (STEP 7 Safety V16) (strona 442)

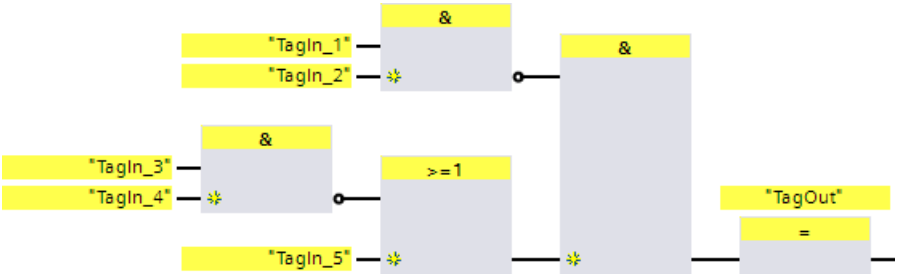
13.1.2.5 Odwrócenie RLO (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Invert RLO" można odwrócić wynik operacji logicznej (RLO).

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione

- Wejście „TagIn_1" i/lub „TagIn_2" ma stan sygnału „0".
- Wejście „TagIn_3" lub „TagIn_4" ma stan sygnału „0" wejście „TagIn_5" ma stan sygnału „1".

13.2 Operacje na bitach logicznych

13.2.1 LAD

13.2.1.1 ---| |---: Styk NO (STEP 7 Safety V16)

Opis

Aktywacja styku normalnie otwartego zależy od stanu sygnału powiązanego argumentu. Jeśli argument ma stan sygnału „1", styk normalnie otwarty jest zamknięty. Energia przepływa z lewej szyny zasilającej przez styk normalnie otwarty do prawej szyny, a stan sygnału na wyjściu instrukcji jest ustawiany na „1".

Jeśli argument ma stan sygnału „0", styk normalnie otwarty jest nie jest aktywowany. Przepływ energii do prawej szyny jest przerywany, a stan sygnału na wyjściu instrukcji jest resetowany do „0".

Dwa lub więcej styków normalnie otwartych jest połączonych kolejno przez „AND", gdy są połączone szeregowo. Przy połączeniu szeregowym, prąd przepływa po zamknięciu wszystkich styków.

Styki normalnie otwarte są połączone przez „OR" gdy są połączone równolegle. Przy połączeniu równoległym, prąd przepływa po zamknięciu jednego ze styków.

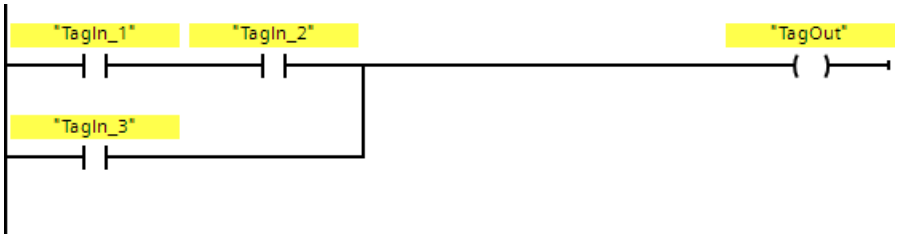
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wejście	BOOL	Argument, stan sygnału którego jest sprawdzany.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument TagOut" jest ustawiany, gdy zostanie spełniony jeden z następujących warunków:

- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".
- Stan sygnału przy argumentzie „TagIn_3" to „1".

13.2.1.2 ---| / |---: Styk NC (STEP 7 Safety V16)

Opis

Aktywacja styku normalnie zamkniętego zależy od stanu sygnału powiązanego argumentu. Jeśli argument ma stan sygnału "1", styk normalnie zamknięty jest otwarty, a stan sygnału na wyjściu instrukcji jest resetowany do „0".

Jeśli argument ma stan sygnału "0", styk normalnie zamknięty nie jest aktywowany, a stan sygnału na wyjściu instrukcji jest ustawiany na „1".

Dwa lub więcej styków normalnie zamkniętych jest połączonych kolejno przez „AND", gdy są połączone szeregowo. Przy połączeniu szeregowym, prąd przepływa po zamknięciu wszystkich styków.

Styki normalnie zamknięte są połączone przez „OR" gdy są połączone równolegle. Przy połączeniu równoległym, prąd przepływa po zamknięciu jednego ze styków.

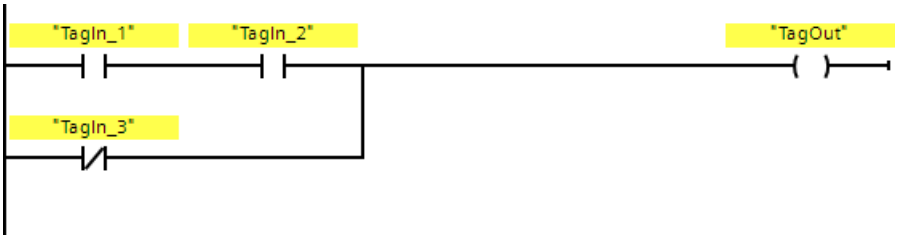
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wejście	BOOL	Argument, stan sygnału którego jest sprawdzany.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument TagOut" jest ustawiany, gdy zostanie spełniony jeden z następujących warunków:

- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".
- Stan sygnału przy argumentzie „TagIn_3" to „0".

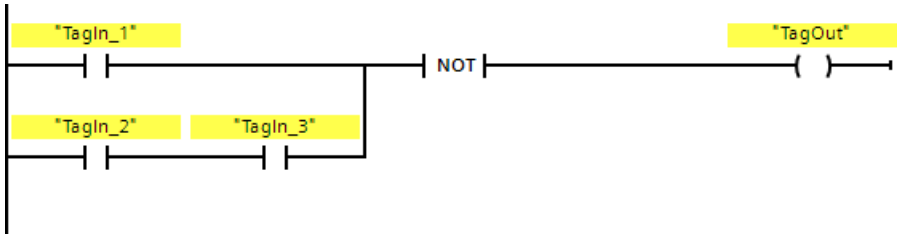
13.2.1.3 --|NOT|--: Odwrócenie RLO (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Invert RLO" można odwrócić stan sygnału wyniku operacji logicznej (RLO). Gdy stan sygnału to „1" na wejściu instrukcji, wyjście instrukcji ma stan sygnału „0". Gdy stan sygnału to „0" na wejściu instrukcji, wyjście ma stan sygnału „1".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument TagOut" jest resetowany, gdy zostanie spełniony jeden z następujących warunków:

- Argument „TagIn_1" ma stan sygnału „1".
- Argumenty „TagIn_2" oraz „TagIn_3" mają stan sygnału „1".

13.2.1.4 ---( )---: Przypisanie (STEP 7 Safety V16)

Opis

Możliwe jest użycie instrukcji „Assignment" (Przypisanie) do ustawienia bitu określonego argumentu. Gdy wynik operacji logicznej (RLO) na wejściu cewki to „1", określony argument jest ustawiany na stan sygnału „1". Gdy stan sygnału to „0" na wejściu cewki, bit określonego argumentu jest resetowany do „0".

Ta instrukcja nie wpływa na RLO. RLO na wejściu cewki jest wysyłany bezpośrednio na wyjście.

Instrukcja „Assignment" może być umieszczona w dowolnym miejscu w sieci.

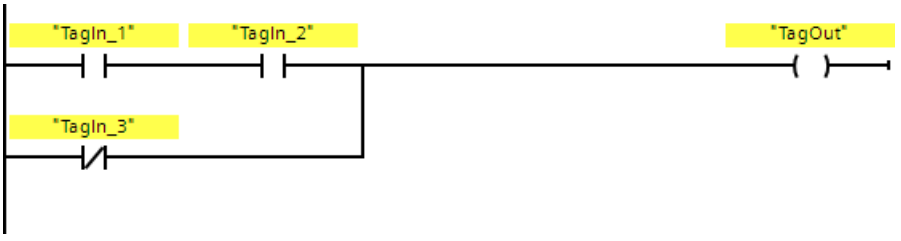
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wyjście	BOOL	Argument, do którego przypisano RLO.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument TagOut" jest ustawiany, gdy zostanie spełniony jeden z następujących warunków:

- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".
- Stan sygnału przy argumentzie „TagIn_3" to „0".

13.2.1.5 ---(R)---: Wyjście reset (STEP 7 Safety V16)

Opis

Możliwe jest użycie instrukcji „Reset output" (Zresetuj wyjście) do zresetowania stanu sygnału określonego argumentu na „0".

Jeśli prąd przypływa do cewki (RLO wynosi „1"), określony argument jest ustawiany na „0". Jeśli wynik operacji logicznej na wejściu cewki to „0" (brak przepływu sygnału do cewki), stan sygnału określonego argumentu pozostaje niezmienny.

Ta instrukcja nie wpływa na RLO. RLO na wejściu cewki jest wysyłany bezpośrednio do wyjścia cewki.

Uwaga

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do argumentów instrukcji, najpierw należy zainicjować bit danych lokalnych.

Uwaga

Nie można używać obszarów argumentów „obraz procesu wejść", „obraz procesu wyjść" ze standardowego I/O oraz „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

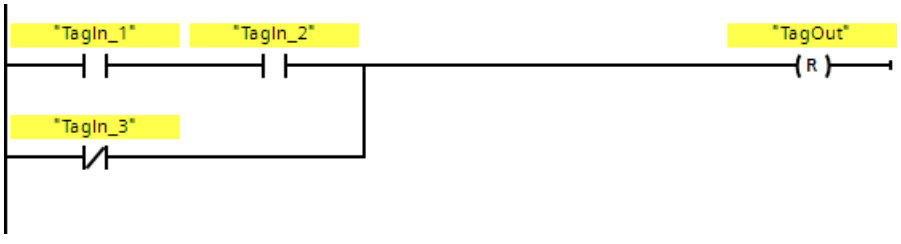
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wyjście	BOOL	Argument, który jest resetowany, gdy RLO = „1".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument TagOut" jest resetowany, gdy zostanie spełniony jeden z następujących warunków:

- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".
- Stan sygnału argumentu „TagIn_3" to „0".

13.2.1.6 ---(S)---: Wyjście set (STEP 7 Safety V16)

Opis

Możliwe jest użycie instrukcji „Set output" (Wyjście set) do ustawienia stanu sygnału określonego argumentu na „1".

Jeśli prąd przypływa do cewki (RLO wynosi „1"), określony argument jest ustawiany na „1". Jeśli wynik operacji logicznej na wejściu cewki to „0" (brak przepływu sygnału do cewki), stan sygnału określonego argumentu pozostaje niezmienny.

Ta instrukcja nie wpływa na RLO. RLO na wejściu cewki jest wysyłany bezpośrednio do wyjścia cewki.

Uwaga

Instrukcja nie jest wykonywana, jeśli zostanie zastosowana do wyjścia F-I/O, który jest pasywowany (np. podczas uruchomienia systemu bezpieczeństwa). Dlatego też dobrze jest uzyskiwać dostęp do wyjść F-I/O jedynie poprzez instrukcję „Assignment" (Przypisanie).

Wyjście F-I/O jest pasywowane, jeśli QBAD lub QBAD_O_xx = 1 bądź stan wartości = 0 zostanie ustawiony w odnośnym DB F-I/O.

Uwaga

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do argumentów instrukcji, najpierw należy zainicjować bit danych lokalnych.

Uwaga

Nie można używać obszarów argumentów „obraz procesu wejść", „obraz procesu wyjść" ze standardowego I/O oraz „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

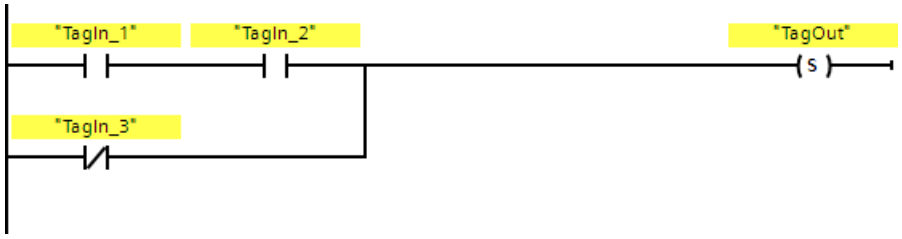
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wyjście	BOOL	Argument ustawiony, gdy RLO = „1".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument TagOut" jest ustawiany, gdy zostanie spełniony jeden z następujących warunków:

- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".
- Stan sygnału argumentu „TagIn_3" to „0".

13.2.1.7 SR: Przerzutnik set/reset (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Set/reset flip-flop" Przerzutnik set/reset) można ustawić lub zresetować bit określonego argumentu w oparciu o stan sygnału wejść S i R1. Jeśli stan sygnału na wejściu S to „1", a stan sygnału na wejściu R1 to „0", określony argument jest ustawiany na „1". Jeśli stan sygnału na wejściu S to „0", a stan sygnału na wejściu R1 to „1", określony argument jest resetowany do „0".

Wejście R1 ma pierwszeństwo na wejściem S. Jeśli stan sygnału na obu wejściach to „1", stan sygnału określonego argumentu jest resetowany do „0".

Instrukcja nie jest wykonywana, jeśli stan sygnału na wejściach S i R1 to „0". Stan sygnału argumentu pozostaje wtedy niezmieniony.

Bieżący stan sygnału argumentu jest przenoszony na wyjście Q i może być stamtąd pobrany.

Uwaga

Aby użyć parametru formalnego z F-FC do argumentu instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do argumentów instrukcji, najpierw należy zainicjować bit danych lokalnych.

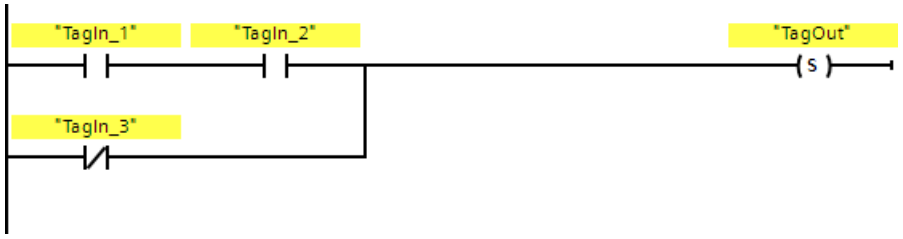
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
S	Wejście	BOOL	Aktywuje opcję set
R1	Wejście	BOOL	Aktywuje opcję reset
<Argument>	Wyjście	BOOL	Argument, który jest ustawiany lub resetowany.
Q	Wyjście	BOOL	Stan sygnału argumentu

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argumenty „F_DB_1".TagSR" oraz „TagOut" są ustawiane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „1".
- Argument „TagIn_2" ma stan sygnału „0".

Argumenty „F_DB_1".TagSR" oraz „TagOut" są resetowane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „0", a argument „TagIn_2" ma stan sygnału „1".
- Oba argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".

13.2.1.8 RS: Przerzutnik reset/set (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Reset/set flip-flop" Przerzutnik reset/set) można zresetować lub ustawić bit określonego argumentu w oparciu o stan sygnału wejść R i S1. Gdy stan sygnału to „1" na wejściu R oraz „0" na wejściu S1, określony argument jest resetowany do „0". Gdy stan sygnału to „0" na wejściu R oraz „1" na wejściu S1, określony argument jest ustawiany na „1".

Wejście S1 ma pierwszeństwo na wejściem R. Jeśli stan sygnału na obu wejściach to „1", stan sygnału określonego argumentu jest ustawiany na „1".

Instrukcja nie jest wykonywana, jeśli stan sygnału na wejściach R i S1 to „0". Stan sygnału argumentu pozostaje wtedy niezmieniony.

Bieżący stan sygnału argumentu jest przenoszony na wyjście Q i może być stamtąd pobrany.

Uwaga

Aby użyć parametru formalnego z F-FC do argumentu instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do argumentów instrukcji, najpierw należy zainicjować bit danych lokalnych.

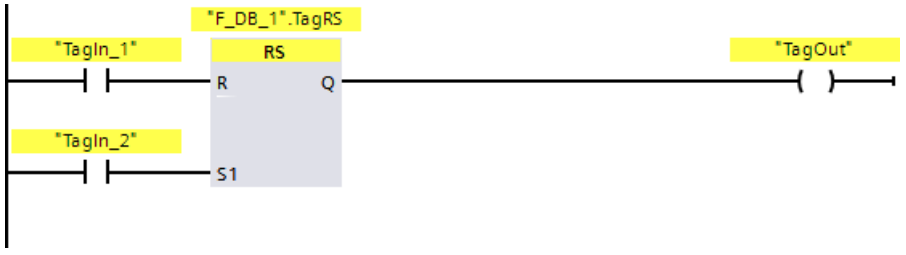
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
R	Wejście	BOOL	Aktywuje opcję reset
S1	Wejście	BOOL	Aktywuje opcję set
<Argument>	Wyjście	BOOL	Argument, który jest resetowany lub ustawiany.
Q	Wyjście	BOOL	Stan sygnału argumentu

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argumenty „F_DB_1".TagRS" oraz „TagOut" są resetowane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „1".
- Argument „TagIn_2" ma stan sygnału „0".

Argumenty „F_DB_1".TagRS" oraz „TagOut" są ustawiane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „0", a argument „TagIn_2" ma stan sygnału „1".
- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".

13.2.1.9 --|P|--: Skanowanie argumentu pod kątem narastającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan argument for positive signal edge" (Skanuj argument pod kątem narastającego zbocza sygnału) można określić, czy występuje zmiana z „0" na „1" w stanie sygnału określonego argumentu (<Argument1>). Instrukcja porównuje bieżący stan sygnału
<Argument1> ze stanem sygnału poprzedniego zapytania zapisanego w <Argument2>. Jeśli instrukcja wykryje zmianę w wyniku operacji logicznej z „0" na „1", występuje dodatnie zbocze narastające.

W przypadku wykrycia zbocza narastającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Argument, dla którego ma zostać wykonane zapytanie (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Bit pamięci zbocza (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument2> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument2> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument2> instrukcji, najpierw należy zainicjować bit danych lokalnych.

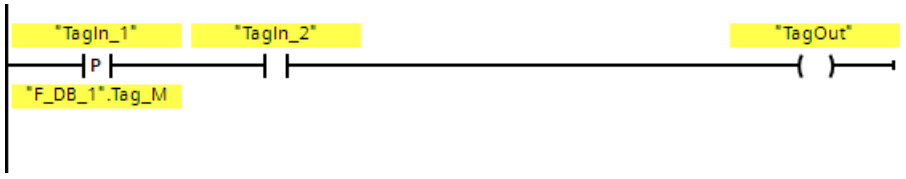
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument1>	Wejście	BOOL	Sygnał, dla którego zostanie wykonane zapytanie
<Argument2>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest stan sygnału z poprzedniego zapytania.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument „TagOut" jest ustawiany, gdy zostaną spełnione następujące warunki:

- Występuje zbocze narastające na wejściu „TagIn_1". Stan sygnału z poprzedniego zapytania jest zapisywany w bicie pamięci zbocza „"F_DB_1".Tag_M".
- Stan sygnału argumentu „TagIn_2" to „1".

13.2.1.10 --|N|--: Skanowanie argumentu pod kątem opadającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan argument for negative signal edge" (Skanuj argument pod kątem opadającego zbocza sygnału) można określić, czy występuje zmiana z „1" na „0" w stanie sygnału określonego argumentu. Instrukcja porównuje bieżący stan sygnału <Argument1> ze stanem sygnału poprzedniego zapytania zapisanego w <Argument2>. Jeśli instrukcja wykryje zmianę w wyniku operacji logicznej z „1" na „0", występuje ujemne zbocze opadające.

W przypadku wykrycia zbocza opadającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Argument, dla którego ma zostać wykonane zapytanie (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Bit pamięci zbocza (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument2> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument2> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument2> instrukcji, najpierw należy zainicjować bit danych lokalnych.

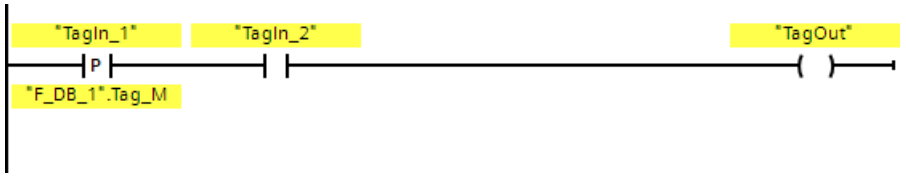
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument1>	Wejście	BOOL	Sygnał, dla którego zostanie wykonane zapytanie
<Argument2>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest stan sygnału z poprzedniego zapytania.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument „TagOut" jest ustawiany, gdy zostaną spełnione następujące warunki:

- Występuje zbocze opadające na argumentzie „TagIn_1". Stan sygnału z poprzedniego zapytania jest zapisywany w bicie pamięci zbocza „"F_DB_1".Tag_M".
- Stan sygnału argumentu „TagIn_2" to „1".

13.2.1.11 P_TRIG: Skanowanie RLO pod kątem narastającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan RLO for positive signal edge" (Skanuj RLO pod kątem narastającego zbocza sygnału) można wykonać zapytanie o zmianę w stanie sygnału wyniku operacji logicznej z „0" na „1". Instrukcja porównuje bieżący stan sygnału wyniku operacji logicznej (RLO) ze stanem sygnału z poprzedniego zapytania, który zapisany jest w bicie pamięci zbocza (<Argument>). Jeśli instrukcja wykryje zmianę w RLO z „0" na „1", występuje dodatnie zbocze narastające.

W przypadku wykrycia zbocza narastającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument> instrukcji, najpierw należy zainicjować bit danych lokalnych.

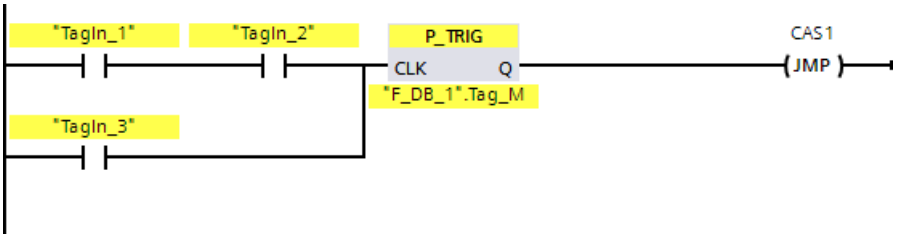
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
CLK	Wejście	BOOL	Bieżący RLO
<Argument>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest RLO z poprzedniego zapytania.
Q	Wyjście	BOOL	Wynik oceny zbocza

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



RLO z poprzedniej operacji na bitach logicznych jest zapisywany w bicie pamięci zbocza „"F_DB_1".Tag_M". W przypadku wykrycia zmiany stanu sygnału RLO z „0" na „1", program przeskakuje do etykiety skoku CAS1.

13.2.1.12 N_TRIG: Skanowanie RLO pod kątem opadającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan RLO for negative signal edge" (Skanuj RLO pod kątem opadającego zbocza sygnału) można wykonać zapytanie o zmianę w stanie sygnału wyniku operacji logicznej z „1" na „0". Instrukcja porównuje bieżący stan sygnału wyniku operacji logicznej ze stanem sygnału z poprzedniego zapytania, który zapisany jest w bicie pamięci zbocza (<Argument>). Jeśli instrukcja wykryje zmianę w RLO z „1" na „0", występuje ujemne zbocze opadające.

W przypadku wykrycia zbocza opadającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument> instrukcji, najpierw należy zainicjować bit danych lokalnych.

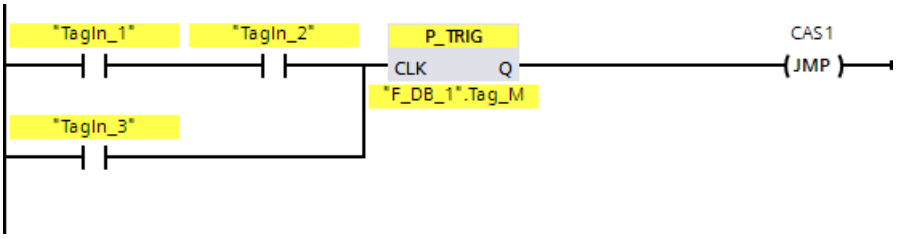
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
CLK	Wejście	BOOL	Bieżący RLO
<Argument>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest RLO z poprzedniego zapytania.
Q	Wyjście	BOOL	Wynik oceny zbocza

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



RLO poprzedniej operacji na bitach logicznych jest zapisywany w bicie pamięci zbocza „"F_DB_1".Tag_M". W przypadku wykrycia zmiany stanu sygnału RLO z „1" na „0", program przeskakuje do etykiety skoku CAS1.

13.2.2 FBD

13.2.2.1 Operacja logiczna AND (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „AND logic operation" (Operacja logiczna AND) można wykonać zapytanie o stany sygnałów dwóch lub więcej określonych argumentów oraz ocenę ich zgodnie z matrycą logiczną AND.

Jeśli stan sygnału wszystkich argumentów to „1", warunki zostały spełnione, a instrukcja zwraca wynik „1". Jeśli stan sygnału jednego z argumentów to „0", warunki nie zostały spełnione, a instrukcja generuje wynik „0".

Jeśli instrukcja „AND logic operation" (operacja logiczna OR) jest pierwszą instrukcją w ciągu logicznym, zapisuje wynik zapytania stanu sygnału w bicie RLO.

Każda instrukcja „AND logic operation" (operacja logiczna OR), która nie jest pierwszą instrukcją w ciągu logicznym, łączy logicznie wynik stanu sygnału z wartością zapisaną w bicie RLO. Ta kombinacja logiczna jest wykonywana zgodnie z matrycą logiczną AND.

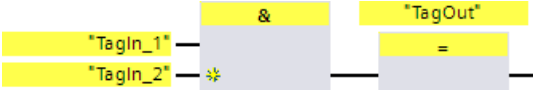
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wejście	BOOL	Argument wskazuje bit, stan sygnału którego zostanie sprawdzony.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy stan sygnału argumentów „TagIn_1" oraz „TagIn_2" to „1".

Matryca logiczna AND

Poniższa tablica przedstawia wyniki łączenia dwóch argumentów w operacji logicznej AND:

Stan sygnału pierwszego argumentu	Stan sygnału drugiego argumentu	Wynik operacji logicznej
1	1	1
0	1	0
1	0	0
0	0	0

Zobacz także

Wstawianie wejścia binarnego (STEP 7 Safety V16) (strona 418)

13.2.2.2 Operacja logiczna OR (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „OR logic operation" (Operacja logiczna OR) można wykonać uzyskać stany sygnałów dwóch lub więcej określonych argumentów oraz ocenę ich zgodnie z matrycą logiczną AND.

Jeśli stan sygnału co najmniej jednego argumentu to „1", warunki zostały spełnione, a instrukcja zwraca wynik „1". Jeśli stan sygnału wszystkich argumentów to „0", warunki nie zostały spełnione, a instrukcja generuje wynik „0".

Jeśli instrukcja „OR logic operation" (operacja logiczna OR) jest pierwszą instrukcją w ciągu logicznym, zapisuje wynik zapytania stanu sygnału w bicie RLO.

Każda instrukcja „OR logic operation" (operacja logiczna OR), która nie jest pierwszą instrukcją w ciągu logicznym, łączy logicznie wynik stanu sygnału z wartością zapisaną w bicie RLO. Ta kombinacja logiczna jest wykonywana zgodnie z matrycą logiczną OR.

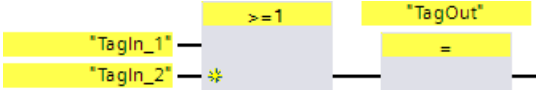
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wejście	BOOL	Argument wskazuje bit, stan sygnału którego zostanie sprawdzony.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy stan sygnału argumentu „TagIn_1" lub „TagIn_2" to „1".

Matryca logiczna OR

Poniższa tablica przedstawia wyniki łączenia dwóch argumentów w operacji logicznej OR:

Stan sygnału pierwszego argumentu	Stan sygnału drugiego argumentu	Wynik operacji logicznej
1	0	1
0	1	1
1	1	1
0	0	0

Zobacz także

Wstawianie wejścia binarnego (STEP 7 Safety V16) (strona 418)

13.2.2.3 X: Operacja logiczna EXCLUSIVE OR (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „EXCLUSIVE OR logic operation" (Operacja logiczna EXCLUSIVE OR) można uzyskać wynik zapytania o stan sygnału zgodnie z matrycą logiczną EXCLUSIVE OR.

Przy użyciu instrukcji „EXCLUSIVE OR logic operation", stan sygnału to „1", gdy stan sygnału jednego z dwóch określonych argumentów to „1". Gdy wykonywane jest zapytanie dla więcej niż dwóch argumentów, całkowity wynik operacji logicznej to „1", jeśli nieparzysta liczba argumentów zwraca wynik „1".

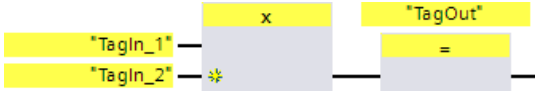
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wejście	BOOL	Argument wskazuje bit, stan sygnału którego zostanie sprawdzony.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy stan sygnału jednego z dwóch argumentów „TagIn_1" oraz „TagIn_2" to „1". Gdy oba argumenty mają stan sygnału „1" lub „0", wyjście „TagOut" jest resetowane.

Matryca logiczna EXCLUSIVE OR

Poniższa tablica przestawia wyniki połączenia dwóch argumentów w operacji EXCLUSIVE OR:

Stan sygnału pierwszego argumentu	Stan sygnału drugiego argumentu	Wynik operacji logicznej
1	0	1
0	1	1
1	1	0
0	0	0

Poniższa tablica przestawia wyniki połączenia trzech argumentów w operacji EXCLUSIVE OR:

Stan sygnału pierwszego argumentu	Stan sygnału drugiego argumentu	Stan sygnału trzeciego argumentu	Wynik operacji logicznej
1	0	0	1
0	1	1	0
0	1	0	1
1	0	1	0
0	0	1	1
1	1	0	0
1	1	1	1
0	0	0	0

Zobacz także

Wstawianie wejścia binarnego (STEP 7 Safety V16) (strona 418)

13.2.2.4 =: Przypisanie (STEP 7 Safety V16)

Opis

Możliwe jest użycie instrukcji „Assignment" (Przypisanie) do ustawienia bitu określonego argumentu. Jeśli wynik operacji logicznej (RLO) na wejściu pola ma stan sygnału „1" lub wejście pola dla F-CPU S7-1200/1500 nie jest podłączone, określony argument jest ustawiany na stan sygnału „1". Jeśli stan sygnału na wejściu pola to „0" bit określonego argumentu jest resetowany do „0".

Ta instrukcja nie wpływa na RLO. RLO na wejściu pola jest przypisywany bezpośrednio do argumentu znajdującego się powyżej pola przypisania.

Instrukcja „Assignment" może być umieszczona w dowolnym miejscu w sekwencji operacji logicznych.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wyjście	BOOL	Argument, do którego przypisano RLO.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:

Argument „TagOut" na wyjściu instrukcji „Assignment" jest ustawiany, gdy zostanie spełniony jeden z następujących warunków:

- Wejścia „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".
- Stan sygnału na wejściu „TagIn_3" to „0".

13.2.2.5 R: Wyjście reset (STEP 7 Safety V16)

Opis

Możliwe jest użycie instrukcji „Reset output" (Zresetuj wyjście) do zresetowania stanu sygnału określonego argumentu na „0".

Jeśli wejście pola ma stan sygnału „1" lub wejście pola dla F-CPU S7-1200/1500 nie jest podłączone, określony argument jest resetowany do „0". Jeśli na wejściu pola znajduje się wynik operacji logicznej „0", stan sygnału określonego argumentu pozostaje niezmieniony.

Ta instrukcja nie wpływa na RLO. RLO z wejścia pola jest przenoszony bezpośrednio na wyjście pola.

Uwaga

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do argumentów instrukcji, najpierw należy zainicjować bit danych lokalnych.

Uwaga

Nie można używać obszarów argumentów „obraz procesu wejść", „obraz procesu wyjść" ze standardowego I/O oraz „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

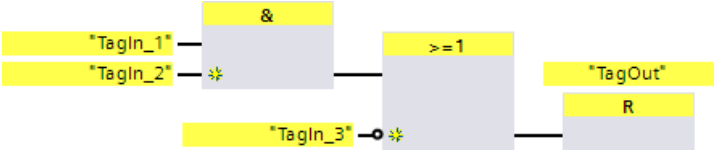
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wyjście	BOOL	Argument, który jest resetowany przy RLO = „1".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argument TagOut" jest resetowany, gdy zostanie spełniony jeden z następujących warunków:

- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".
- Stan sygnału argumentu „TagIn_3" to „0".

13.2.2.6 S: Wyjście set (STEP 7 Safety V16)

Opis

Możliwe jest użycie instrukcji „Set output" (Wyjście set) do ustawienia stanu sygnału określonego argumentu na „1".

Jeśli wejście pola ma stan sygnału „1" lub wejście pola dla F-CPU S7-1200/1500 nie jest podłączone, określony argument jest ustawiany na „1". Jeśli na wejściu pola znajduje się wynik operacji logicznej „0", stan sygnału określonego argumentu pozostaje niezmieniony.

Ta instrukcja nie wpływa na RLO. RLO z wejścia pola jest przenoszony bezpośrednio na wyjście pola.

Uwaga

Instrukcja nie jest wykonywana, jeśli zostanie zastosowana do wyjścia F-I/O, który jest pasywowany (np. podczas uruchomienia systemu bezpieczeństwa). Dlatego też dobrze jest uzyskiwać dostęp do wyjść F-I/O jedynie poprzez instrukcję „Assignment" (Przypisanie).

Wyjście F-I/O jest pasywowane, jeśli QBAD lub QBAD_O_xx = 1 bądź stan wartości = 0 zostanie ustawiony w odnośnym DB F-I/O.

Uwaga

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do argumentów instrukcji, najpierw należy zainicjować bit danych lokalnych.

Uwaga

Nie można używać obszarów argumentów „obraz procesu wejść", „obraz procesu wyjść" ze standardowego I/O oraz „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument>	Wyjście	BOOL	Argument ustawiony, gdy RLO = „1”.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:

Argument TagOut” jest ustawiany, gdy zostanie spełniony jeden z następujących warunków:

- Argumenty „TagIn_1” oraz „TagIn_2” mają stan sygnału „1”.
- Stan sygnału argumentu „TagIn_3” to „0”.

13.2.2.7 SR: Przerzutnik set/reset (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Set/reset flip-flop" Przerzutnik set/reset) można ustawić lub zresetować bit określonego argumentu w oparciu o stan sygnału wejść S i R1. Jeśli stan sygnału na wejściu S to „1", a stan sygnału na wejściu R1 to „0", określony argument jest ustawiany na „1". Jeśli stan sygnału na wejściu S to „0", a stan sygnału na wejściu R1 to „1", określony argument jest resetowany do „0".

Wejście R1 ma pierwszeństwo na wejściem S. Jeśli stan sygnału na obu wejściach to „1", stan sygnału określonego argumentu jest resetowany do „0".

Instrukcja nie jest wykonywana, jeśli stan sygnału na wejściach S i R1 to „0". Stan sygnału argumentu pozostaje wtedy niezmieniony.

Bieżący stan sygnału argumentu jest przenoszony na wyjście Q i może być stamtąd pobrany.

Uwaga

Aby użyć parametru formalnego z F-FC do argumentu instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza instrukcji, najpierw należy zainicjować bit danych lokalnych.

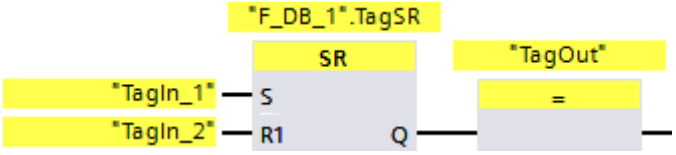
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
S	Wejście	BOOL	Aktywuje opcję set
R1	Wejście	BOOL	Aktywuje opcję reset
<Argument>	Wyjście	BOOL	Argument, który jest ustawiany lub resetowany.
Q	Wyjście	BOOL	Stan sygnału argumentu

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argumenty „F_DB_1".TagSR" oraz „TagOut" są ustawiane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „1".
- Argument „TagIn_2" ma stan sygnału „0".

Argumenty „F_DB_1".TagSR" oraz „TagOut" są resetowane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „0", a argument „TagIn_2" ma stan sygnału „1".
- Oba argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".

13.2.2.8 RS: Przerzutnik reset/set (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Reset/set flip-flop" Przerzutnik reset/set) można zresetować lub ustawić bit określonego argumentu w oparciu o stan sygnału wejść R i S1. Gdy stan sygnału to „1" na wejściu R oraz „0" na wejściu S1, określony argument jest resetowany do „0". Gdy stan sygnału to „0" na wejściu R oraz „1" na wejściu S1, określony argument jest ustawiany na „1".

Wejście S1 ma pierwszeństwo na wejściem R. Jeśli stan sygnału na obu wejściach to „1", stan sygnału określonego argumentu jest ustawiany na „1".

Instrukcja nie jest wykonywana, jeśli stan sygnału na wejściach R i S1 to „0". Stan sygnału argumentu pozostaje wtedy niezmieniony.

Bieżący stan sygnału argumentu jest przenoszony na wyjście Q i może być stamtąd pobrany.

Uwaga

Aby użyć parametru formalnego z F-FC do argumentu instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla argumentów instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza instrukcji, najpierw należy zainicjować bit danych lokalnych.

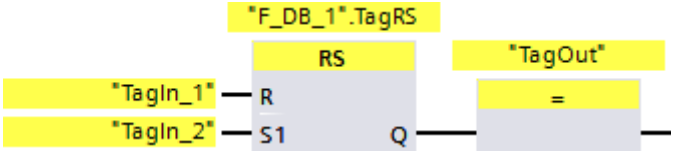
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
R	Wejście	BOOL	Aktywuje opcję reset
S1	Wejście	BOOL	Aktywuje opcję set
<Argument>	Wyjście	BOOL	Argument, który jest resetowany lub ustawiany.
Q	Wyjście	BOOL	Stan sygnału argumentu

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Argumenty „F_DB_1".TagRS" oraz „TagOut" są resetowane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „1".
- Argument „TagIn_2" ma stan sygnału „0".

Argumenty „F_DB_1".TagRS" oraz „TagOut" są ustawiane, gdy zostaną spełnione następujące warunki:

- Argument „TagIn_1" ma stan sygnału „0", a argument „TagIn_2" ma stan sygnału „1".
- Argumenty „TagIn_1" oraz „TagIn_2" mają stan sygnału „1".

13.2.2.9 P: Skanowanie argumentu pod kątem narastającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan argument for positive signal edge" (Skanuj argument pod kątem narastającego zbocza sygnału) można określić, czy występuje zmiana z „0" na „1" w stanie sygnału określonego argumentu (<Argument1>). Instrukcja porównuje bieżący stan sygnału
<Argument1> ze stanem sygnału poprzedniego zapytania zapisanego w <Argument2>. Jeśli instrukcja wykryje zmianę w wyniku operacji logicznej z „0" na „1", występuje dodatnie zbocze narastające.

W przypadku wykrycia zbocza narastającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Argument, dla którego ma zostać wykonane zapytanie (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Bit pamięci zbocza (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument2> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument2> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument2> instrukcji, najpierw należy zainicjować bit danych lokalnych.

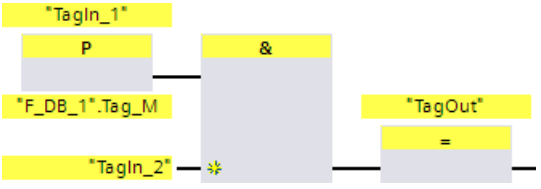
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument1>	Wejście	BOOL	Sygnał, dla którego zostanie wykonane zapytanie
<Argument2>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest stan sygnału z poprzedniego zapytania.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



„TagOut" jest ustawiany, gdy zostaną spełnione następujące warunki:

- Występuje zbocze narastające na wejściu „TagIn_1".
- Stan sygnału argumentu „TagIn_2" to „1".

13.2.2.10 N: Skanowanie argumentu pod kątem opadającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan argument for negative signal edge" (Skanuj argument pod kątem opadającego zbocza sygnału) można określić, czy występuje zmiana z „1" na „0" w stanie sygnału określonego argumentu. Instrukcja porównuje bieżący stan sygnału <Argument1> ze stanem sygnału poprzedniego zapytania zapisanego w <Argument2>. Jeśli instrukcja wykryje zmianę w wyniku operacji logicznej z „1" na „0", występuje ujemne zbocze opadające.

W przypadku wykrycia zbocza opadającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Argument, dla którego ma zostać wykonane zapytanie (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Bit pamięci zbocza (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument2> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument2> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument2> instrukcji, najpierw należy zainicjować bit danych lokalnych.

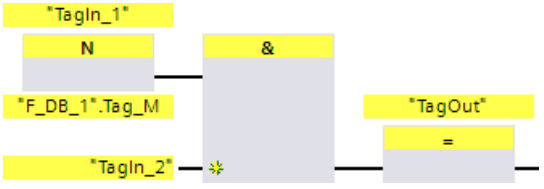
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Argument1>	Wejście	BOOL	Sygnał, dla którego zostanie wykonane zapytanie
<Argument2>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest stan sygnału z poprzedniego zapytania.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione następujące warunki:

- Występuje zbocze opadające na wejściu „TagIn_1".
- Stan sygnału argumentu „TagIn_2" to „1".

13.2.2.11 P_TRIG: Skanowanie RLO pod kątem narastającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan RLO for positive signal edge" (Skanuj RLO pod kątem narastającego zbocza sygnału) można wykonać zapytanie o zmianę w stanie sygnału wyniku operacji logicznej z „0" na „1". Instrukcja porównuje bieżący stan sygnału wyniku operacji logicznej ze stanem sygnału z poprzedniego zapytania, który zapisany jest w bicie pamięci zbocza (<Argument>). Jeśli instrukcja wykryje zmianę w RLO z „0" na „1", występuje dodatnie zbocze narastające.

W przypadku wykrycia zbocza narastającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument> instrukcji, najpierw należy zainicjować bit danych lokalnych.

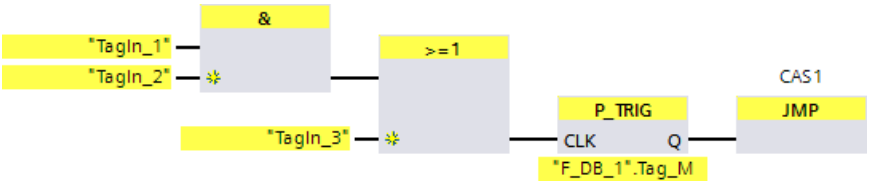
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
CLK	Wejście	BOOL	Bieżący RLO
<Argument>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest RLO z poprzedniego zapytania.
Q	Wyjście	BOOL	Wynik oceny zbocza

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



RLO z poprzedniej operacji na bitach logicznych jest zapisywany w bicie pamięci zbocza „"F_DB_1".Tag_M". W przypadku wykrycia zmiany stanu sygnału RLO z „0" na „1", program przeskakuje do etykiety skoku CAS1.

13.2.2.12 N_TRIG: Skanowanie RLO pod kątem opadającego zbocza sygnału (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Scan RLO for negative signal edge" (Skanuj RLO pod kątem opadającego zbocza sygnału) można wykonać zapytanie o zmianę w stanie sygnału wyniku operacji logicznej z „1" na „0". Instrukcja porównuje bieżący stan sygnału wyniku operacji logicznej ze stanem sygnału z poprzedniego zapytania, który zapisany jest w bicie pamięci zbocza (<Argument>). Jeśli instrukcja wykryje zmianę w RLO z „1" na „0", występuje ujemne zbocze opadające.

W przypadku wykrycia zbocza opadającego, wyjście instrukcji daje stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu instrukcji to „0".

Uwaga

Adres bitu pamięci zbocza nie może być używany więcej niż raz w programie, w przeciwnym razie zostanie on nadpisany. Wpłynie to na ocenę zbocza, a wynik nie będzie dłużej jednoznaczny.

Uwaga

Aby użyć parametru formalnego z F-FC do bitu pamięci zbocza <Argument> instrukcji, należy go zadeklarować jako parametr wejściowy/wyjściowy.

Uwaga

Nie można używać obszarów argumentów „obraz procesu", „standardowy DB" i „pamięć bitowa" dla bitu pamięci zbocza <Argument> instrukcji.

Jeśli obszar argumentów „local data (temp)" (Dane lokalne (tymczasowe)) jest wykorzystywany do bitu pamięci zbocza <Argument> instrukcji, najpierw należy zainicjować bit danych lokalnych.

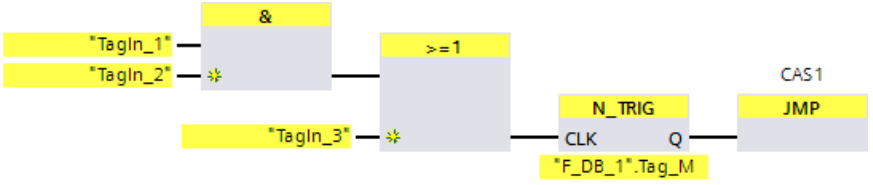
Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
CLK	Wejście	BOOL	Bieżący RLO
<Argument>	InOut	BOOL	Bit pamięci zbocza, w którym zapisany jest RLO z poprzedniego zapytania.
Q	Wyjście	BOOL	Wynik oceny zbocza

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



RLO poprzedniej operacji na bitach logicznych jest zapisywany w bicie pamięci zbocza „"F_DB_1".Tag_M". W przypadku wykrycia zmiany stanu sygnału RLO z „1" na „0", program przeskakuje do etykiety skoku CAS1.

13.3 Funkcje bezpieczeństwa

13.3.1 ESTOP1: Zatrzymanie/wyłączenie awaryjne do kategorii zatrzymania 1 (STEP 7 Safety V16)

Opis

Ta instrukcja wprowadza zatrzymanie/wyłączenie awaryjne z zatwierdzeniem dla kategorii zatrzymania 0 oraz 1.

Sygnał aktywacji Q jest resetowany do 0, gdy tylko wejście E_STOP przyjmie stan sygnału 0 (kategoria zatrzymania 0). Sygnał aktywacji Q_DELAY jest resetowany do 0 po czasie opóźnienia ustawionym na wejściu TIME_DEL (kategoria zatrzymania 1).

Sygnał aktywacji Q jest resetowany do 1 nie wcześniej, aż wejście E_STOP przyjmie stan sygnału 1 i wystąpi zatwierdzenie. Zatwierdzenie aktywacji odbywa się zgodnie z przypisaniem parametru na wejściu ACK_NEC:

- Jeśli ACK_NEC = 0, zatwierdzenie odbywa się automatycznie.
- Jeśli ACK_NEC = 1, należy użyć zbocza narastającego na wejściu ACK do zatwierdzenia aktywacji.

Wyjście ACK_REQ sygnalizuje, że zatwierdzenie użytkownika jest wymagane na wejściu ACK do zatwierdzenia. Instrukcja ustawia wyjście ACK_REQ na 1, gdy tylko wejście E_STOP = 1.

Po zatwierdzeniu instrukcja resetuje ACK_REQ do 0.

Każde wywołanie instrukcji „Emergency STOP/Emergency OFF up to Stop Category 1" (Zatrzymanie/wyłączenie awaryjne do kategorii zatrzymania 1) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. ESTOP1_DB_1) lub wiele instancji (np. ESTOP1_Instance_1) dla instrukcji „Emergency STOP/Emergency OFF up to Stop Category 1" (Zatrzymanie/wyłączenie awaryjne do kategorii zatrzymania 1). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku.

Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

OSTRZEŻENIE

Do znacznika ACK_NEC nie można przypisać wartości 0, o ile automatyczny restart danego procesu nie jest w inny sposób wykluczony. *(S033)*

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Uwaga: W przypadku dwóch kanałów zgodnych z kategorią 3,4 normy ISO 13849-1:2015 lub EN ISO 13849-1:2015, monitorowanie rozbieżności dwóch styków NC ZATRZYMANIA AWARYJNEGO/WYŁĄCZENIA AWARYJNEGO musi odbywać się w F-I/O. Należy odpowiednio skonfigurować F-I/O (ocena czujnika: dwukanałowa, równoważna), zaś wynik oceny musi być połączony z wejściem E_STOP. Aby nie dopuścić do wpływu czasu rozbieżności na czas reakcji, należy przypisać „Supply value 0" (Wartość zasilania 0) dla zachowania rozbieżności podczas konfiguracji.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
E_STOP	Wejście	BOOL	ZATRZYMANIE/WYŁĄCZENIE AWARYJNE
ACK_NEC	Wejście	BOOL	1=Niezbędne zatwierdzenie
ACK	Wejście	BOOL	1=Zatwierdzenie
TIME_DEL	Wejście	TIME	Opóźnienie
Q	Wyjście	BOOL	1=Aktywuj
Q_DELAY	Wyjście	BOOL	Aktywacja ma opóźnione wyłączenie
ACK_REQ	Wyjście	BOOL	1=Niezbędne zatwierdzenie
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Wersja 1.0 wymaga, by blok F_TOF z numerem FB 186 był dostępny w drzewku projektu w folderze „Program blocks/System blocks/STEP 7 Safety". Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji. Uniknie się dzięki temu niezgodności w numeracji.
1,1	x	—	-—	Te wersje są funkcjonalnie identyczne z wersją V1.0, lecz nie wymagają, by blok F_TOF miał określony numer.
1,2	x	—	o	
1,3	x	o	o	
1,4	x	o	o	
1,5	x	x	x	
1,6	x	x	x	Reakcja czasu opóźnienia TIME_DEL dla F-CPU S7-1200/1500 została przystosowana do reakcji F-CPU S7-300/400: Jeśli wejście ESTOP (0 -> 1 (w tym zatwierdzenie) -> 0) ulega zmianie podczas trwania czasu opóźnienia, czas opóźnienia jest restartowany.

o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Charakterystyka rozpoczęcia pracy

Po uruchomieniu systemu bezpieczeństwa, gdy ACK_NEC = 1, należy zatwierdzić instrukcję, korzystając ze zbocza narastającego na wejściu ACK.

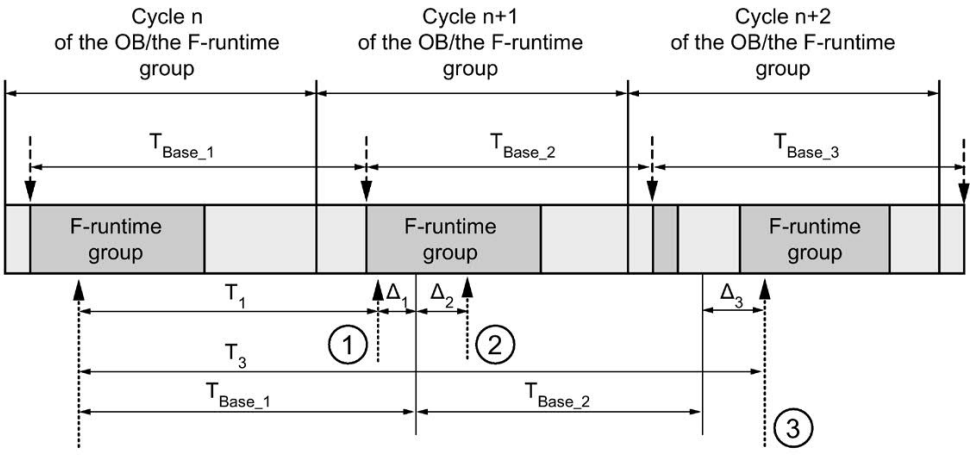
Wyjście DIAG

Wyjście DIAG zapewnia w celach serwisowych informacje nie fail-safe na temat błędów. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG 4 i 5 są zapisywane aż do zatwierdzenia na wejściu ACK.

Struktura DIAG

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Nieprawidłowa nastawa	Nastawa opóźnienia < 0	Ustawić opóźnienie > 0
Bit 1	Zastrzeżony	—	—
Bit 2	Zastrzeżony	—	—
Bit 3	Zastrzeżony	—	—
Bit 4	Zatwierdzenie nie jest możliwe, ponieważ zatrzymanie/wyłączenie awaryjne jest wciąż aktywne	Przycisk zatrzymania/ wyłączenia awaryjnego jest zablokowany	Zwolnić przycisk zatrzymania/wyłączenia awaryjnego
		Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O przycisku zatrzymania/ wyłączenia awaryjnego	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
		Przycisk zatrzymania /wyłączenia awaryjnego jest uszkodzony	Sprawdzić przycisk zatrzymania/wyłączenia awaryjnego
		Usterka okablowania	Sprawdzić okablowanie przycisku zatrzymania /wyłączenia awaryjnego
Bit 5	Jeśli brak aktywacji: wejście ACK ma permanentny stan sygnału 1	Uszkodzony przycisk zatwierdzenia	Sprawdzić przycisk zatwierdzenia
		Usterka okablowania	Sprawdzić okablowanie przycisku zatwierdzenia
Bit 6	Wymagane zatwierdzenie (= stan ACK_REQ)	—	—
Bit 7	Stan wyjścia Q	—	—

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



⁃⁃⁃⁃► = Time base update

┈┈┈► = Call time of an instruction with time processing

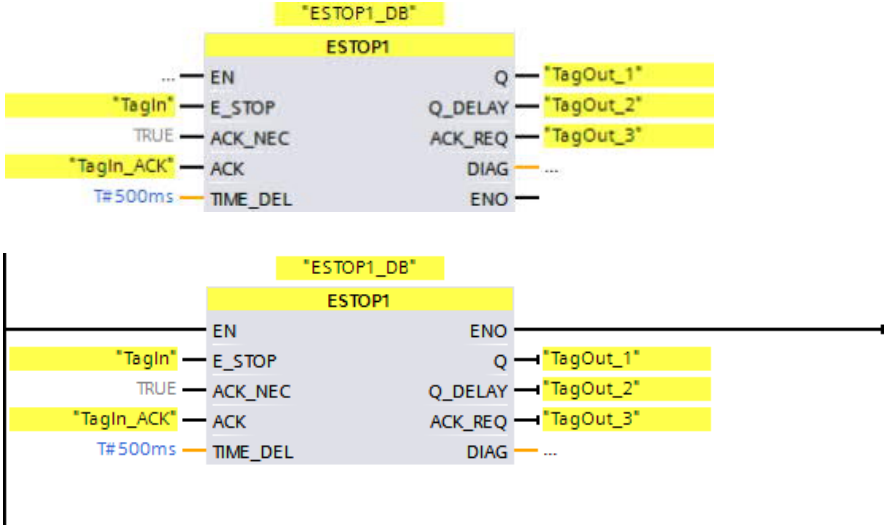
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



13.3.2 TWO_HAND: Monitorowanie oburęczne (STEP 7 Safety Advanced V16) (S7-300, S7-400)

Opis

Ta instrukcja wprowadza monitorowanie oburęczne.

Uwaga

Ta instrukcja jest dostępna jedynie dla F-CPU S7-300 i S7-400. W przypadku F-CPU S7-1200/1500, należy użyć instrukcji „Two-hand monitoring with enable" (Monitorowanie oburęczne z aktywacją). Aplikacja „Two-hand monitoring with enable" (Monitorowanie oburęczne z aktywacją) zastępuje instrukcję „Two-hand monitoring" (Monitorowanie oburęczne) z kompatybilnymi funkcjami.

Jeśli przyciski IN1 i IN2 zostaną aktywowane w obrębie dozwolonego czasu rozbieżności DISCTIME ≤ 500 ms (IN1/IN2 = 1) (aktywacja synchroniczna), sygnał wyjścia Q jest ustawiany na 1. Jeśli różnica czasu pomiędzy aktywacją przycisku IN1 i IN2 jest większa niż DISCTIME, należy zwolnić przyciski i wcisnąć je ponownie.

Q jest resetowane do 0 gdy tylko jeden z przycisków zostanie zwolniony (IN1/IN2 = 0). Sygnał aktywacji Q może zostać zresetowany do 1 tylko, jeśli drugi przycisk został zwolniony, a następnie oba zostaną wciśnięte w czasie rozbieżności. Sygnał aktywacji Q nie może być ustawiony na 1, jeśli czas rozbieżności został ustawiony na wartości poniżej 0 lub większe niż 500 ms.

Każde wywołanie instrukcji „Two-hand monitoring" (Monitorowanie oburęczne) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. TWO_HAND_DB_1) lub wiele instancji (np. TWO_HAND_Instance_1) dla instrukcji „Two-hand monitoring" (Monitorowanie oburęczne). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Instrukcje obsługują wymogi zgodnie z EN 574:1996 + A1:2008.

Uwaga: W instrukcji można ocenić jedynie jeden sygnał na przycisk. Monitorowanie rozbieżności styków NC i NO przycisków IN1 i IN2 jest wykonywane bezpośrednio podczas odpowiedniej konfiguracji (ocena czujnika: ocena 1oo2, nierównoważna) bezpośrednio przez F-I/O z wejściami. Styk zwierny musi być podłączony w taki sposób, by doprowadzał użyteczny sygnał (patrz instrukcji wykorzystywanego F-I/O). Aby nie dopuścić do wpływu czasu rozbieżności na czas reakcji, należy przypisać „Supply value 0" (Wartość zasilania 0) dla zachowania rozbieżności podczas konfiguracji. W przypadku wykrycia rozbieżności, wartość fail-safe 0 jest wprowadzana do obrazu procesuwejść (PII) dla przycisku oraz QBAD lub QBAD_I_xx = 1 jest ustawiane w odnośnym DB F-I/O. (Zobacz również „Dostęp F-I/O" (strona 166))

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

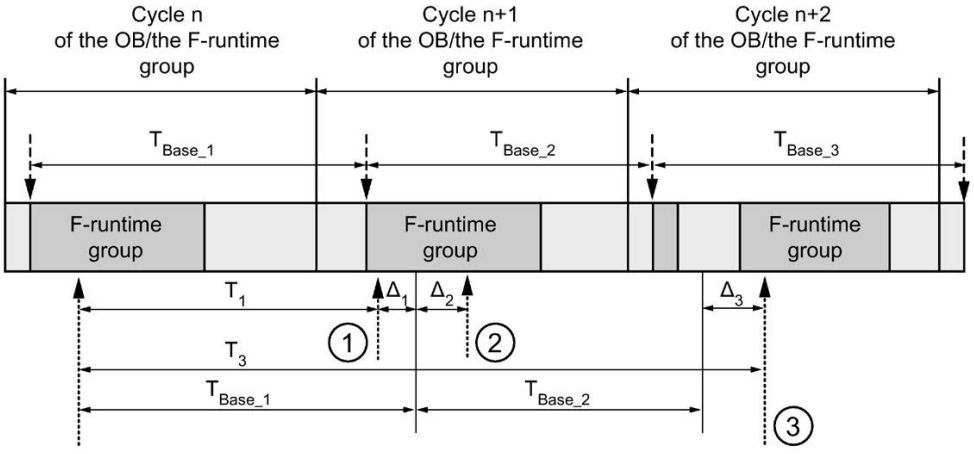
Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN1	Wejście	BOOL	Przycisk 1
IN2	Wejście	BOOL	Przycisk 2
DISCTIME	Wejście	TIME	Czas rozbieżności (0 – 500 ms)
Q	Wyjście	BOOL	1=Aktywuj

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



----► = Time base update

·····► = Call time of an instruction with time processing

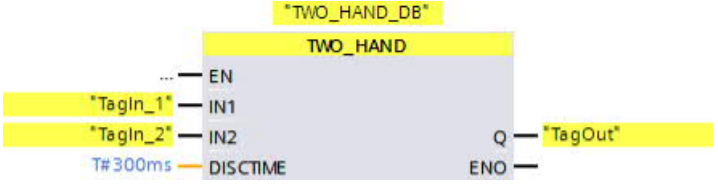
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

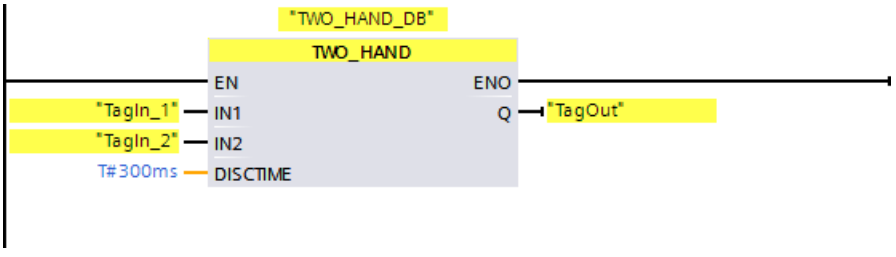
② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:





13.3.3 TWO_H_EN: Monitorowanie oburęczne z aktywacją (STEP 7 Safety V16)

Opis

Ta instrukcja wprowadza monitorowanie oburęczne z aktywacją.

Jeśli przyciski IN1 i IN2 zostaną aktywowane w obrębie dozwolonego czasu rozbieżności DISCTIME ≤ 500 ms (IN1/IN2 = 1) (aktywacja synchroniczna), sygnał wyjścia Q jest ustawiany na 1, gdy istnieje ENABLE = 1. Jeśli różnica czasu pomiędzy aktywacją przycisku IN1 i IN2 jest większa niż DISCTIME, należy zwolnić przyciski i wcisnąć je ponownie.

Q jest resetowane do 0 gdy tylko jeden z przycisków zostanie zwolniony (IN1/IN2 = 0) lub ENABLE = 0. Sygnał aktywacji Q może zostać zresetowany do 1 tylko, jeśli drugi przycisk został zwolniony, a następnie oba zostaną wciśnięte w czasie rozbieżności przy istniejącym ENABLE = 1.

Każde wywołanie instrukcji „Two-hand monitoring with enable" (Monitorowanie oburęczne z aktywacją) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. TWO_H_EN_DB_1) lub wiele instancji (np. TWO_H_EN_Instance_1) dla instrukcji „Two-hand monitoring with enable" (Monitorowanie oburęczne z aktywacją). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Instrukcje obsługują wymogi zgodnie z EN 574:1996 + A1:2008.

Uwaga: W instrukcji można ocenić jedynie jeden sygnał na przycisk. Monitorowanie rozbieżności styków NC i NO przycisków IN1 i IN2 jest wykonywane bezpośrednio podczas odpowiedniej konfiguracji (ocena czujnika: ocena 1oo2, nierównoważna) bezpośrednio przez F-I/O z wejściami. Styk zwierny musi być podłączony w taki sposób, by doprowadzał użyteczny sygnał (patrz instrukcji wykorzystywanego F-I/O). Aby nie dopuścić, by czas rozbieżności wpływał na czas odpowiedzi, podczas konfigurowania zachowania rozbieżności, należy skonfigurować „Supply value 0" (Wartość zasilania 0).

W przypadku wykrycia rozbieżności, wartość fail-safe 0 jest wprowadzana do obrazu procesuwejść (PII) dla przycisku oraz QBAD lub QBAD_I_xx = 1 lub kolejno stan wartości = 0 jest ustawiane w odnośnym DB F-I/O.

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN1	Wejście	BOOL	Przycisk 1
IN2	Wejście	BOOL	Przycisk 2
ENABLE	Wejście	BOOL	Wejście aktywacji
DISCTIME	Wejście	TIME	Czas rozbieżności (0 – 500 ms)
Q	Wyjście	BOOL	1=Aktywuj
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	x	x	

o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

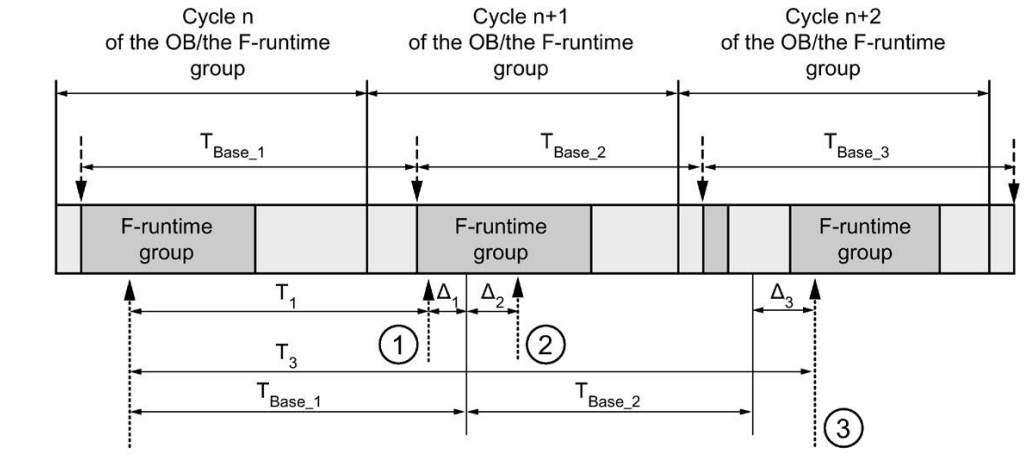
Wyjście DIAG

Wyjście DIAG zapewnia w celach serwisowych informacje nie fail-safe na temat błędów. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG 0 do 5 są zapisywane do czasu usunięcia przyczyny wystąpienia błędu.

Struktura DIAG

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Nieprawidłowa nastawa czasu rozbieżności DISCTIME	Nastawa czasu rozbieżności jest < 0 lub > 500 ms	Ustawić czas rozbieżności w zakresie 0 – 500 ms
Bit 1	Czas rozbieżności upłynął	Nastawa czasu rozbieżności jest zbyt niska	W razie potrzeby należy ustawić wyższy czas rozbieżności
		Przyciski nie zostały aktywowane w czasie rozbieżności	Zwolnić przyciski i aktywować je w obrębie czasu rozbieżności
		Usterka okablowania	Sprawdzić okablowanie przycisków
		Uszkodzone przyciski	Sprawdzić przyciski
		Przyciski są podłączone do innego F-I/O oraz usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
Bit 2	Zastrzeżony	—	—
Bit 3	Zastrzeżony	—	—
Bit 4	Nieprawidłowa sekwencja aktywacji	Jeden przycisk nie został zwolniony	Zwolnić przyciski i aktywować je w obrębie czasu rozbieżności
		Uszkodzone przyciski	Sprawdzić przyciski
Bit 5	ENABLE nie istnieje	ENABLE = 0	Ustawić ENABLE = 1, zwolnić przycisk i aktywować go w czasie rozbieżności
Bit 6	Zastrzeżony	—	—
Bit 7	Stan wyjścia Q	—	—

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



----► = Time base update

·····► = Call time of an instruction with time processing

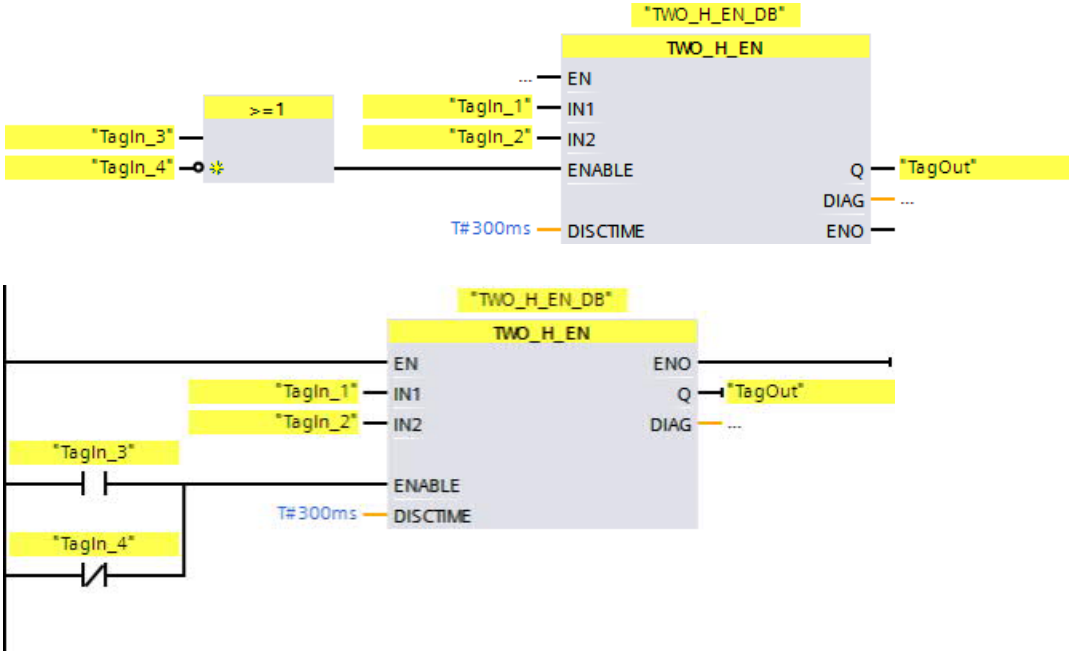
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



13.3.4 MUTING: Muting (STEP 7 Safety Advanced V16) (S7-300, S7-400)

Opis

Ta instrukcja wykonuje równoległe tłumienie z dwoma lub czterema czujnikami mutingu.

Uwaga

Ta instrukcja jest dostępna jedynie dla F-CPU S7-300 i S7-400. W przypadku F-CPU S7-1200/1500, należy użyć instrukcji „Parallel muting" (Muting równoległy) (strona 485). Instrukcja „Parallel muting" (Muting równoległy) zastępuje instrukcję „Muting" z kompatybilnymi funkcjami.

Muting to zdefiniowane tłumienie funkcji zabezpieczającej kurtyn świetlnych. Muting kurtyn świetlnych można wykorzystać do wprowadzenia towarów lub przedmiotów do obszaru niebezpiecznego monitorowanego przez kurtynę bez spowodowania zatrzymania maszyny.

Aby móc użyć funkcji mutingu, potrzebne są co najmniej dwa niezależnie podłączone czujniki mutingu. Użycie dwóch lub czterech czujników mutingu oraz poprawne wprowadzenie ich do sekwencji produkcyjnej musi gwarantować, iż nikt nie może wejść do niebezpiecznego obszaru podczas tłumienia kurtyny świetlnej.

Każde wywołanie instrukcji „Muting" musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. MUTING_DB_1) lub wiele instancji (np. MUTING_Instance_1) dla instrukcji „Muting". Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

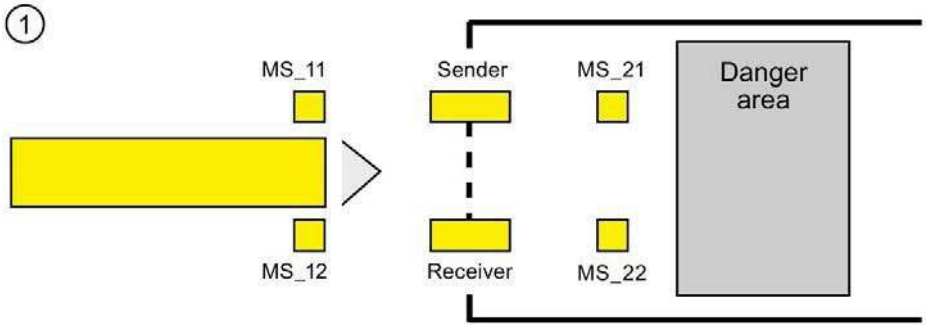
Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
MS_11	Wejście	BOOL	Czujnik mutingu 1 lub para czujników 1
MS_12	Wejście	BOOL	Czujnik mutingu 2 lub para czujników 1
MS_21	Wejście	BOOL	Czujnik mutingu 1 lub para czujników 2
MS_22	Wejście	BOOL	Czujnik mutingu 2 lub para czujników 2
STOP	Wejście	BOOL	1=Układ przenośnika zatrzymany
FREE	Wejście	BOOL	1=Kurtyna świetlna niezakłócona
QBAD_MUT	Wejście	BOOL	Sygnał QBAD z F-I/O lub sygnał QBAD_O_xx kanału kontrolki mutingu
DISCTIM1	Wejście	TIME	Czas rozbieżności pary czujników 1 (0 – 3 s)
DISCTIM2	Wejście	TIME	Czas rozbieżności pary czujników 2 (0 – 3 s)
TIME_MAX	Wejście	TIME	Maksymalny czas tłumienia (0 – 10 min)
ACK	Wejście	BOOL	Zatwierdzenie blokowania restartu
Q	Wyjście	BOOL	1= Aktywne, nie wyłączone
MUTING	Wyjście	BOOL	Wyświetlanie mutingu jest aktywne
ACK_REQ	Wyjście	BOOL	Niezbędne zatwierdzenie
FAULT	Wyjście	BOOL	Błąd grupy
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Sekwencja schematyczna procedury tłumienia wolnej od błędów przy użyciu 4 czujników mutingu (MS_11, MS_12, MS_21, MS_22)



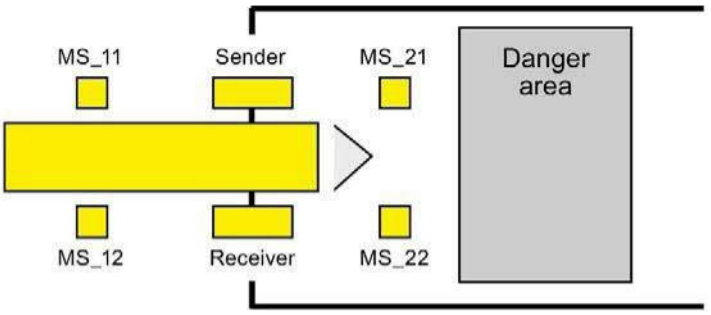
- Jeśli oba czujniki mutingu MS_11 i MS_12 zostaną aktywowane przez produkt w obrębie DISCTIM1 (zastosuj stan sygnału = 1), instrukcja uruchamia funkcję MUTING. Sygnał aktywacji Q pozostaje w stanie 1, nawet gdy wejście FREE = 0 (kurtyna świetlna zakłócona przez produkt). Wyjście MUTING do ustawiania kontrolki mutingu przełącza się na 1.

Uwaga

Kontrolkę mutingu można monitorować przy pomocy wejścia QBAD_MUT. W tym celu należy podłączyć kontrolkę mutingu do wyjścia z monitorowaniem przerwania przewodu w F-I/O i zasilić wejście QBAD_MUT sygnałem QBAD z powiązanego F-I/O lub sygnałem QBAD_O_xx z powiązanego kanału. Jeśli QBAD_MUT = 1, muting jest kończony przez instrukcję. Jeśli monitorowanie kontrolki mutingu nie jest konieczne, nie trzeba doprowadzać sygnału do wejścia QBAD_MUT.

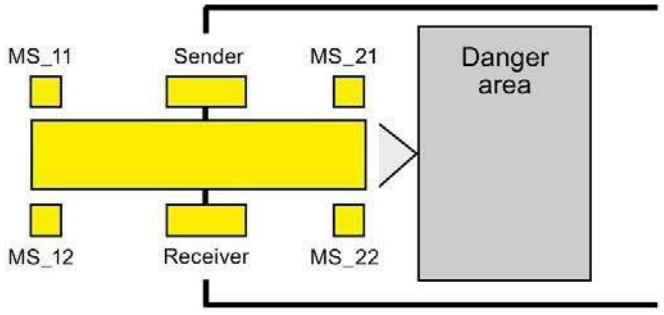
Należy zastosować F-I/O, który może szybko wykryć uszkodzenie w postaci przerwania przewodu po aktywacji operacji mutingu (*patrz instrukcja obsługi określonego F-I/O*).

②



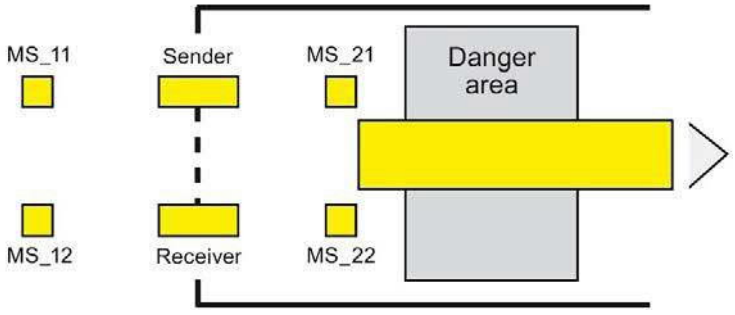
- Dopóki oba czujniki mutingu MS_11 i MS_12 są aktywne, funkcja MUTING instrukcji powoduje utrzymanie wartości 1 na wyjściu Q oraz utrzymaniu 1 dla funkcji MUTING (aby produkt mógł przejść przez kurtynę bez spowodowania zatrzymania maszyny).

③



- Dwa czujniki mutingu MS_21 i MS_22 muszą zostać aktywowane (w obrębie DISCTIM2), nim czujniki mutingu MS_11 i MS_12 zostaną wyłączone (zastosuj sygnał stanu 0). W ten sposób instrukcja utrzymuje funkcję MUTING. (Q = 1, MUTING = 1).

④

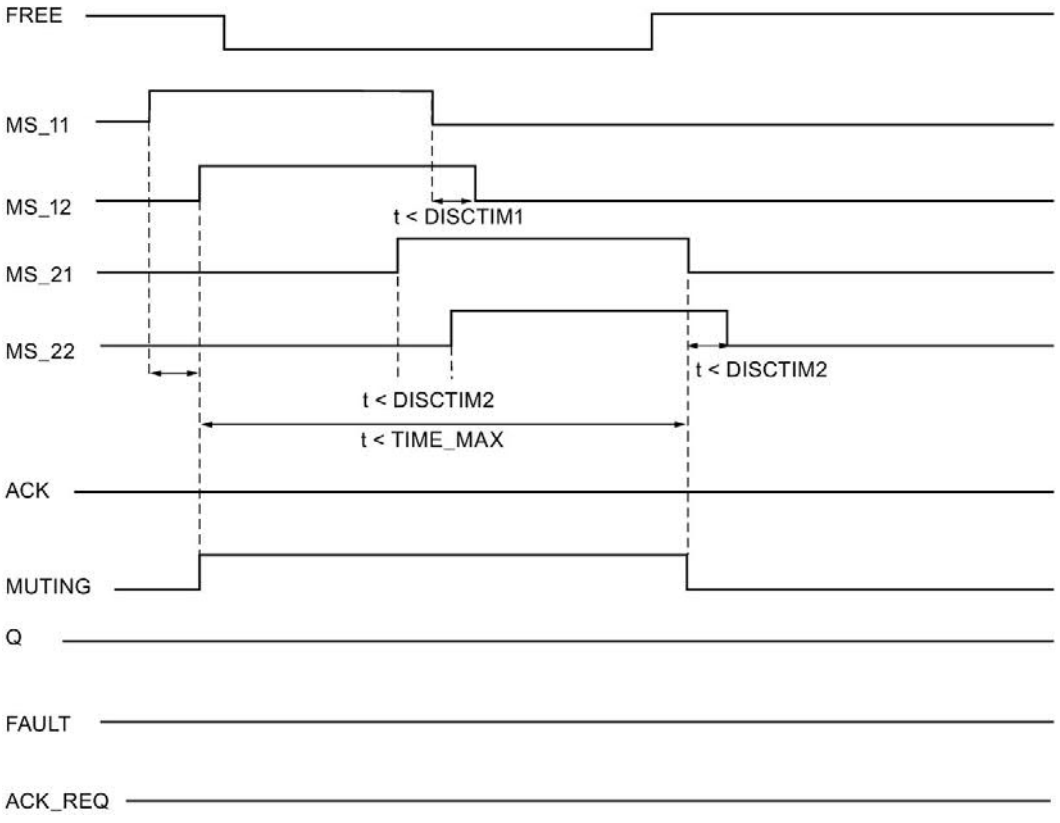


- Jeśli tylko jedne z dwóch czujników mutingu MS_21 i MS_22 zostanie wyłączony (produkt aktywuje czujniki) funkcja MUTING jest kończona (Q = 1, MUTING = 0). Maksymalny czas aktywacji funkcji MUTING to czas ustawiony na wejściu TIME_MAX.

Uwaga

Funkcja MUTING jest również uruchamiana, jeśli produkt przejdzie przez kurtynę świetlną w odwrotnym kierunku, a czujniki mutingu są wobec tego aktywowane w odwrotnej kolejności.

Schematy taktowania dla procedury tłumienia wolnej od błędów przy użyciu 4 czujników mutingu

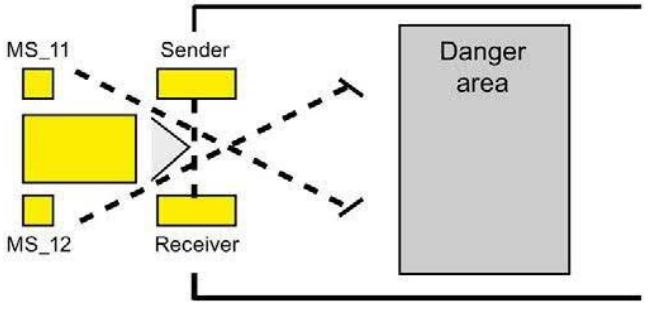


Sekwencja schematyczna procedury tłumienia z refleksyjnymi kurtynami świetlnymi

Jeśli za czujniki mutingu służą refleksyjne kurtyny świetlne, są one zazwyczaj ustawione po przekątnej.

Na ogół takie ułożenie refleksyjnych kurtyn świetlnych jako czujników mutingu wymaga jedynie dwóch kurtyn, przy czym tylko MS_11 i MS_12 są wzajemnie połączone.

Sekwencja jest podobna do procedury mutingu z 4 czujnikami. Pomijany jest krok 3. W kroku 4 należy zastąpić MS_21 i MS_22 kolejno MS_11 i MS_12.



Blokowanie restartu po zakłóceniu kurtyny świetlnej (jeśli MUTING nie jest aktywny), po wystąpieniu błędów oraz podczas rozruchu systemu bezpieczeństwa

Sygnał aktywacji Q nie może być ustawiony na 1 lub przejść do 0, jeśli:

- Kurtyna świetlna zostanie przerwana (np. przez osobę lub transport materiału), gdy funkcja MUTING nie jest aktywna
- Funkcja monitorowania kontrolki mutingu odpowiada na wejściu QBAD_MUT
- Para czujników 1 (MS_11 i MS_12) lub para czujników 2 (MS_21 i MS_22) nie została aktywowana lub dezaktywowana w czasie rozbieżności, kolejno DISCTIM1 lub DISCTIM2
- Funkcja MUTING jest aktywna dłużej niż maksymalny czas mutingu TIME_MAX
- Czasy rozbieżności DISCTIM1 oraz DISCTIM2 ustawiono na wartości < 0 lub > 3 s
- Maks. czas mutingu TIME_MAX został ustawiony na wartość < 0 lub > 10 min

W zidentyfikowanych przypadkach wyjście FAULT (błąd grupy) jest ustawiane na 1 (blokowanie restartu). Jeśli funkcja MUTING została uruchomiona, zostanie zakończona, a wyjście mutingu przybierze wartość 0.

OSTRZEŻENIE

Gdy ważna kombinacja czujników mutingu zostanie wykryta podczas rozruchu systemu bezpieczeństwa (przykładowo, ze względu na to, że czujniki są połączone z wejściami standardowego I/O, który natychmiastowo zapewnia wartości procesowe podczas rozruchu),
funkcja MUTING jest niezwłocznie uruchamiana, a wyjście MUTING oraz sygnał aktywacji Q są ustawiane na 1. Wyjście FAULT (błąd grupy) nie jest ustawiane na 1 (brak blokowania restartu!). *(S035)*

Zatwierdzenie blokowania restartu

Sygnał aktywacji Q przybiera ponownie

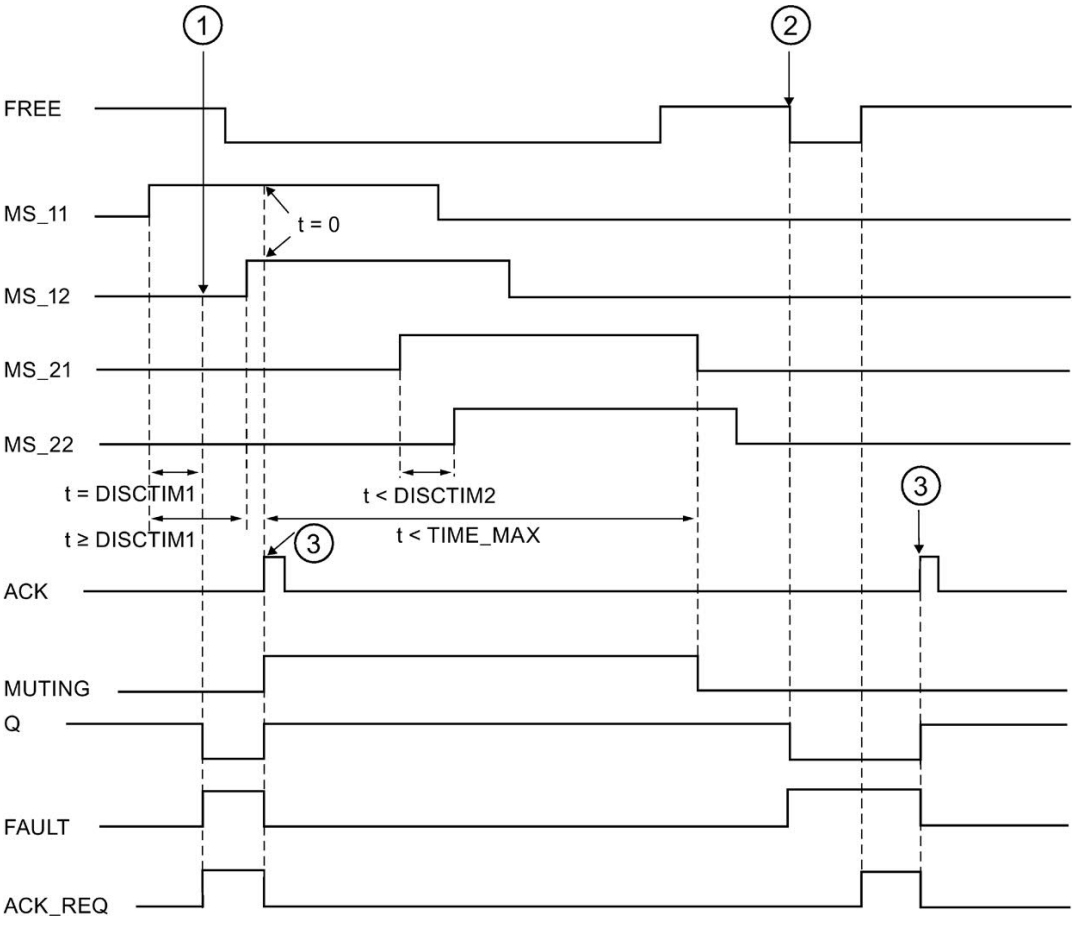
- Kurtyna świetlna nie jest zakłócona
- Występujące błędy zostały usunięte (patrz wyjście DIAG) oraz
- Zatwierdzenie użytkownika ze zboczem dodatnim występuje na wejściu ACK (zobacz również „Wdrożenie rozpoznawania użytkownika" (strona 196)).

Wyjście FAULT jest ustawione na 0. Wyjście ACK_REQ = 1 sygnalizuje, że na wejściu ACK wymagane jest zatwierdzenie użytkownika w celu usunięcia blokady restartu. Instrukcja ustawia ACK_REQ = 1 gdy kurtyna świetlna nie jest zakłócona lub usunięto błędy. Po zatwierdzeniu instrukcja resetuje ACK_REQ do 0.

Uwaga

W przypadku błędów rozbieżności i po przekroczeniu maksymalnego czasu mutingu, ACK_REQ jest niezwłocznie ustawiane na 1. Gdy tylko zostanie wykonane zatwierdzenie użytkownika na wejściu ACK, czasy rozbieżności DISCTIM1 i DISCTIM2 oraz maksymalny czas mutingu TIME_MAX są resetowane.

Schematy taktowania dla błędów rozbieżności na parze czujników 1 lub dla zakłócenia kurtyny świetlnej (jeśli MUTING nie jest aktywny)



① Para czujników 1 (MS_11 i MS_12) nie została aktywowana w czasie rozbieżności DISCTIM1.

② Kurtyna świetlna została naruszona mimo iż funkcja MUTING nie jest aktywna.

③ Zatwierdzenie

Zachowanie z zatrzymanym urządzeniem przenośnikowym

Jeśli, w stanie zatrzymanego urządzenia przenośnikowego, konieczne jest wyłączenie monitowania z jednego z poniższych powodów:

- Aby zapewnić zgodność z czasem rozbieżności DISCTIM1 lub DISCTIM2
- Aby zapewnić zgodność maksymalnym czasem mutingu TIME_MAX

należy doprowadzić na wejście STOP sygnał „1" przez cały czas zatrzymania urządzenia przenośnikowego. Gdy tylko urządzenie przenośnikowe wznowi pracę (STOP = 0), czasy rozbieżności DISCTIM1 i DISCTIM2 oraz maksymalny czas mutingu TIME_MAX są resetowane.

⚠ OSTRZEŻENIE

Gdy STOP = 1, monitorowanie rozbieżności jest wyłączone. W tym czasie, jeśli wejścia MSx1/MSx2 pary czujników przybiorą stan sygnału 1 wskutek niewykrytego błędu, np. oba czujniki mutingu zablokują się na 1, błąd nie będzie wykrywany, a funkcja MUTING może zostać niezamierzenie aktywowana. *(S036)*

Wyjście DIAG

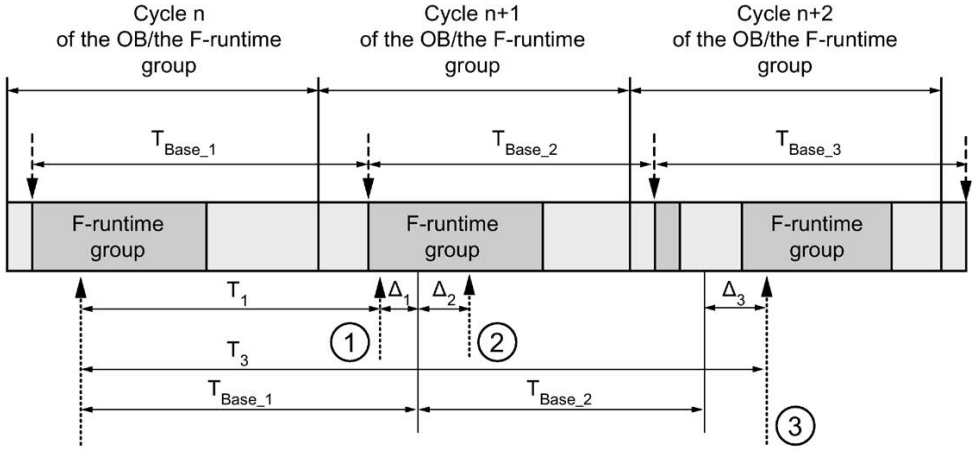
Wyjście DIAG zapewnia w celach serwisowych informacje nie fail-safe na temat błędów. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG są zapisywane aż do zatwierdzenia na wejściu ACK.

Struktura DIAG

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Błąd rozbieżności lub nieprawidłowe ustawienie czasu rozbieżności DISCTIM 1 dla pary czujników 1	Usterka w sekwencji produkcyjnej	Usterka w sekwencji produkcyjnej usunięta
		Uszkodzony czujnik	Sprawdzić czujniki
		Usterka okablowania	Sprawdzić okablowanie czujników
		Czujniki są podłączone do innego F-I/O oraz usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
		Nastawa czasu rozbieżności jest zbyt niska	W razie potrzeby należy ustawić wyższy czas rozbieżności
		Nastawa czasu rozbieżności to < 0 s lub > 3 s	Ustawić czas rozbieżności w zakresie pomiędzy 0 a 3 s
Bit 1	Błąd rozbieżności lub nieprawidłowe ustawienie czasu rozbieżności DISCTIM 2 dla pary czujników 2	Tak samo jak bit 0	Tak samo jak bit 0
Bit 2	Przekroczony maksymalny czas mutingu lub nieprawidłowe ustawienie czasu mutingu TIME_MAX	Usterka w sekwencji produkcyjnej	Usterka w sekwencji produkcyjnej usunięta
		Nastawa maksymalnego czasu mutingu jest zbyt niska	W razie potrzeby należy ustawić wyższy maksymalny czas mutignu
		Nastawa czasu mutingu to < 0 s lub > 10 min	Ustawić czas mutingu w zakresie między 0 s a 10 min
Bit 3	Przerwana kurtyna świetlna bez aktywnego mutingu	Uszkodzona kurtyna świetlna	Sprawdzić kurtynę świetlną
		Usterka okablowania	Sprawdzić okablowanie kurtyny świetlnej (wejście FREE)
		Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O kurtyny świetlnej (wejście FREE)	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
		Patrz inne bity DIAG	
Bit 4	Kontrolka mutingu jest uszkodzona lub nie można jej ustawić	Kontrolka mutingu jest uszkodzona	Wymienić kontrolkę mutingu
		Usterka okablowania	Sprawdzić okablowanie kontrolki
		Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O kontrolki mutingu	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
Bit 5	Zastrzeżony	—	—

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 6	Zastrzeżony	—	—
Bit 7	Zastrzeżony	—	—

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



----► = Time base update

·····► = Call time of an instruction with time processing

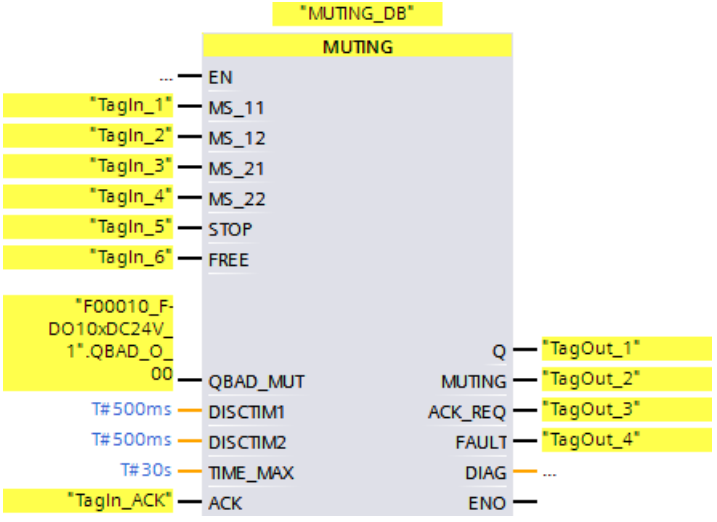
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

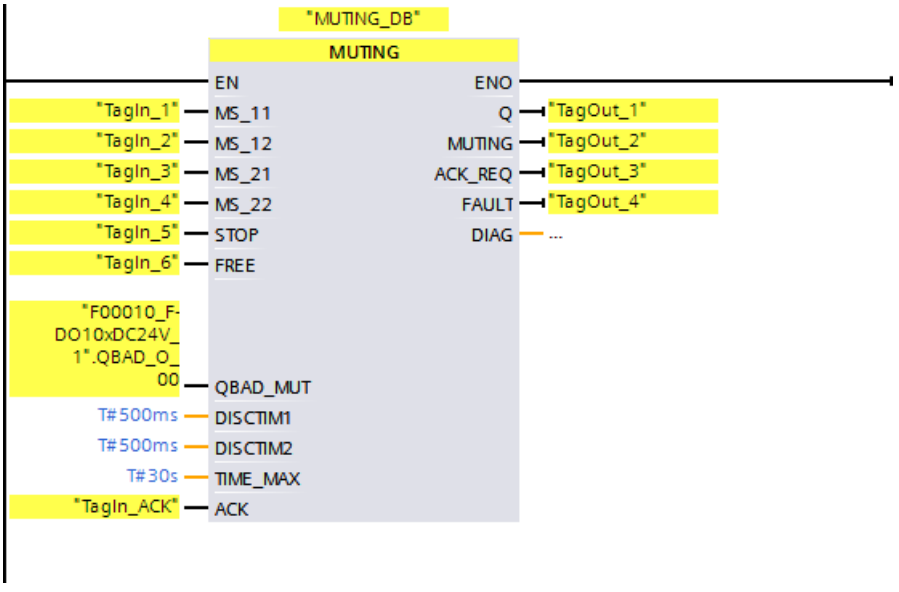
② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:





13.3.5 MUT_P: Muting równoległy (STEP 7 Safety V16)

Opis

Ta instrukcja wykonuje równoległe tłumienie z dwoma lub czterema czujnikami mutingu.

Muting to zdefiniowane tłumienie funkcji zabezpieczającej kurtyn świetlnych. Muting kurtyn świetlnych można wykorzystać do wprowadzenia towarów lub przedmiotów do obszaru niebezpiecznego monitorowanego przez kurtynę bez spowodowania zatrzymania maszyny.

Aby móc użyć funkcji mutingu, potrzebne są co najmniej dwa niezależnie podłączone czujniki mutingu. Użycie dwóch lub czterech czujników mutingu oraz poprawne wprowadzenie ich do sekwencji produkcyjnej musi gwarantować, iż nikt nie może wejść do niebezpiecznego obszaru podczas tłumienia kurtyny świetlnej.

Każde wywołanie instrukcji „Parallel muting" (Muting równoległy) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. MUT_P_DB_1) lub wiele instancji (np. MUT_P_Instance_1) dla instrukcji „Parallel muting" (Muting równoległy). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
MS_11	Wejście	BOOL	Czujnik mutingu 11
MS_12	Wejście	BOOL	Czujnik mutingu 12
MS_21	Wejście	BOOL	Czujnik mutingu 21
MS_22	Wejście	BOOL	Czujnik mutingu 22
STOP	Wejście	BOOL	1=Układ przenośnika zatrzymany
FREE	Wejście	BOOL	1=Kurtyna świetlna niezakłócona
ENABLE	Wejście	BOOL	1=Aktywuj MUTING
QBAD_MUT	Wejście	BOOL	Sygnał QBAD z F-I/O lub sygnał QBAD_O_xx / odwrócony stan wartości kanału kontrolki
ACK	Wejście	BOOL	Zatwierdzenie blokowania restartu
DISCTIM1	Wejście	TIME	Czas rozbieżności pary czujników 1 (0 – 3 s)
DISCTIM2	Wejście	TIME	Czas rozbieżności pary czujników 2 (0 – 3 s)
TIME_MAX	Wejście	TIME	Maksymalny czas tłumienia (0 – 10 min)
Q	Wyjście	BOOL	1= Aktywne, nie wyłączone
MUTING	Wyjście	BOOL	Wyświetlanie mutingu jest aktywne
ACK_REQ	Wyjście	BOOL	Niezbędne zatwierdzenie
FAULT	Wyjście	BOOL	Błąd grupy
DIAG	Wyjście	WORD	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x*	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x*	—	—	Te wersje mają identyczne funkcje jak wersja V1.0. Wyjście DIAG może zostać poprawnie połączone z argumentem o rodzaju danych WORD.
1,2	x*	—	o	
1,3	x*	o	o	
1,4	x	x	x	

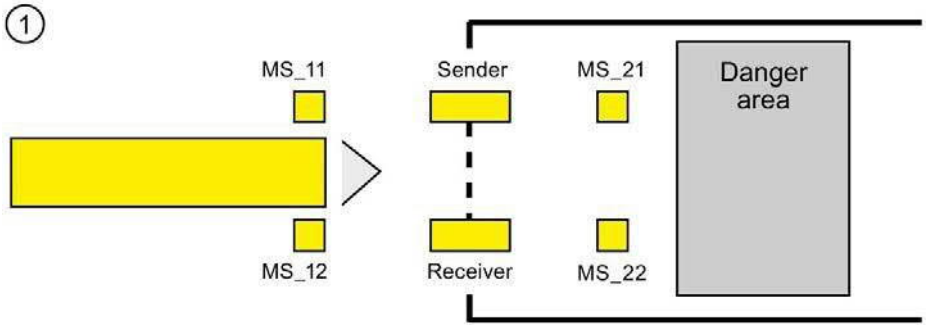
o Ta wersja nie jest już obsługiwana.

* S7-300/400: Gdy obecna jest blokada restartu (wyjście FAULT = 1) oraz ENABLE = 1, wyjście ACK_REQ jest ustawiane na 1, nawet jeśli nawet jeden czujnik mutingu nie został aktywowany. Więcej informacji dostępnych w DIAG bity 5 i 6.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Sekwencja schematyczna procedury tłumienia wolnej od błędów przy użyciu 4 czujników mutingu (MS_11, MS_12, MS_21, MS_22)



- Jeśli oba czujniki mutingu MS_11 i MS_12 zostaną aktywowane przez produkt w obrębie DISCTIM1 (zastosuj stan sygnału = 1), a MUTING został włączony przez ustawienie wejścia ENABLE na 1, instrukcja uruchamia funkcję MUTING. Sygnał aktywacji Q pozostaje w stanie 1, nawet gdy wejście FREE = 0 (kurtyna świetlna zakłócona przez produkt). Wyjście MUTING do ustawiania kontrolki mutingu przełącza się na 1.

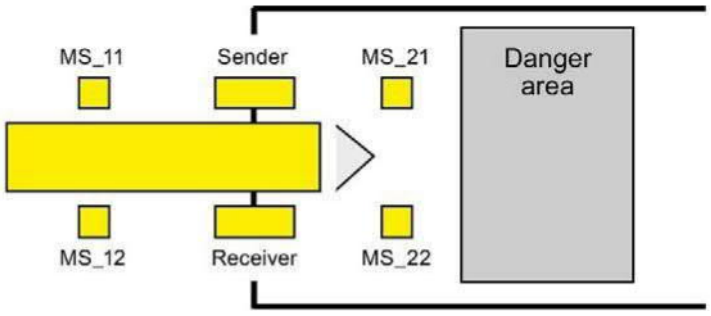
Uwaga

Kontrolkę mutingu można monitorować przy pomocy wejścia QBAD_MUT. W tym celu należy podłączyć kontrolkę mutingu do wyjścia z monitorowaniem przerwania przewodu w F-I/O i zasilić wejście QBAD_MUT sygnałem QBAD z powiązanego F-I/O lub sygnałem QBAD_O_xx /
odwróconego stanu sygnału powiązanego kanału. Jeśli QBAD_MUT = 1, muting jest kończony przez instrukcję. Jeśli monitorowanie kontrolki mutingu nie jest konieczne, nie trzeba doprowadzać sygnału do wejścia QBAD_MUT.

Należy zastosować F-I/O, który może szybko wykryć uszkodzenie w postaci przerwania przewodu po aktywacji operacji mutingu (*patrz instrukcja obsługi określonego F-I/O*).

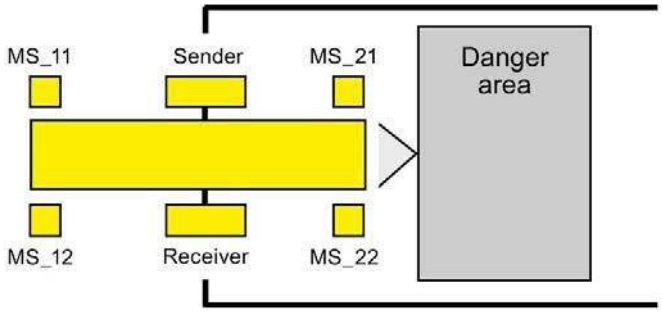
---

②



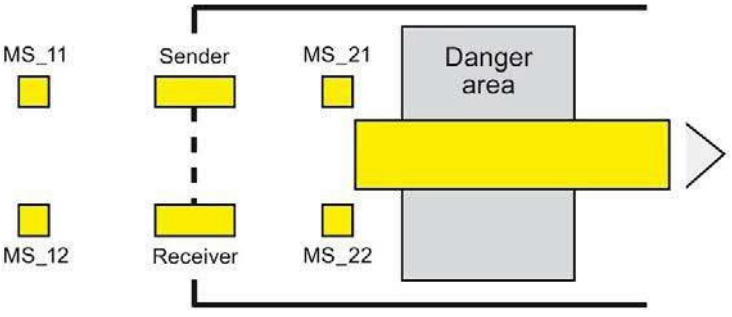
- Dopóki oba czujniki mutingu MS_11 i MS_12 są aktywne, funkcja MUTING instrukcji powoduje utrzymanie wartości 1 na wyjściu Q oraz utrzymaniu 1 dla funkcji MUTING (aby produkt mógł przejść przez kurtynę bez spowodowania zatrzymania maszyny). Oba czujniki mutingu MS_11 i MS_12 mogą zostać wyłączone (t < DISCTIM1) przez krótki czas (zastosuj stan sygnału 0).

③



- Oba czujniki mutingu MS_21 i MS_22 muszą zostać aktywowane (w obrębie DISCTIM2), nim czujniki mutingu MS_11 i MS_12 zostaną wyłączone (zastosuj sygnał stanu 0). W ten sposób instrukcja utrzymuje funkcję MUTING. (Q = 1, MUTING = 1).

④

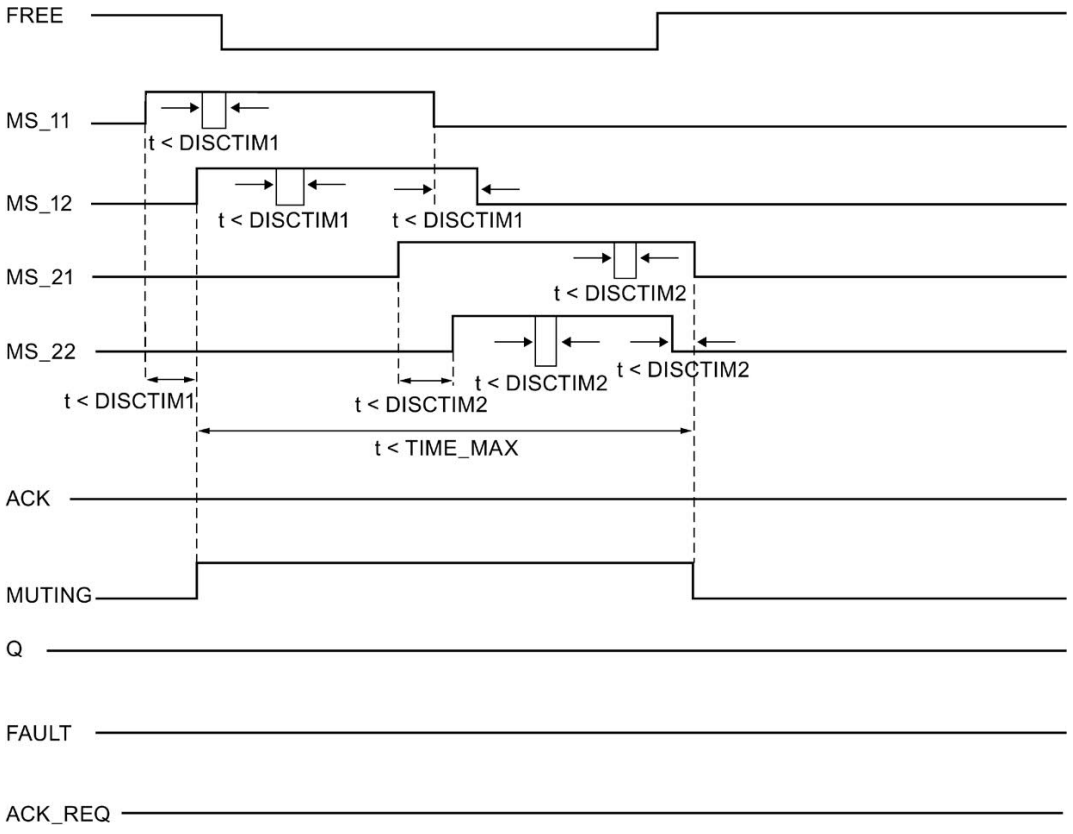


Jeśli tylko czujniki mutingu MS_21 i MS_22 zostaną wyłączone (produkt aktywuje czujniki) funkcja MUTING jest kończona (Q = 1, MUTING = 0). Maksymalny czas aktywacji funkcji MUTING to czas ustawiony na wejściu TIME_MAX.

Uwaga

Funkcja MUTING jest również uruchamiana, jeśli produkt przejdzie przez kurtynę świetlną w odwrotnym kierunku, a czujniki mutingu są wobec tego aktywowane w odwrotnej kolejności.

Schematy taktowania dla procedury tłumienia wolnej od błędów przy użyciu 4 czujników mutingu

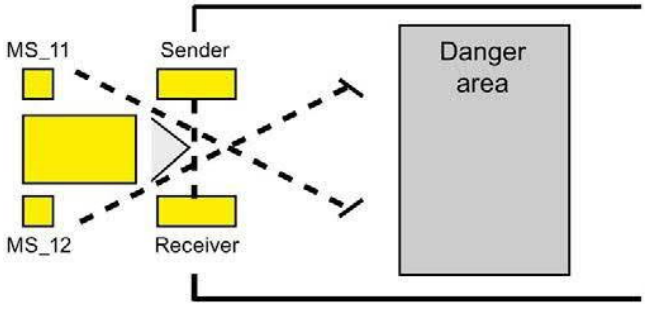


Sekwencja schematyczna procedury tłumienia z refleksyjnymi kurtynami świetlnymi

Jeśli za czujniki mutingu służą refleksyjne kurtyny świetlne, są one zazwyczaj ustawione po przekątnej.

Na ogół takie ułożenie refleksyjnych kurtyn świetlnych jako czujników mutingu wymaga jedynie dwóch kurtyn, przy czym tylko MS_11 i MS_12 są wzajemnie połączone.

Sekwencja jest podobna do procedury mutingu z 4 czujnikami. Pomijany jest krok 3. W kroku 4 należy zastąpić MS_21 i MS_22 kolejno MS_11 i MS_12.



Blokowanie restartu po zakłóceniu kurtyny świetlnej (jeśli MUTING nie jest aktywny), po wystąpieniu błędów oraz podczas rozruchu systemu bezpieczeństwa

Sygnał aktywacji Q nie może być ustawiony na 1 lub przejść do 0, jeśli:

- Kurtyna świetlna zostanie przerwana (np. przez osobę lub transport materiału), gdy funkcja MUTING nie jest aktywna
- Kurtyna świetlna została (jest) zakłócona, a monitorowanie kontrolki mutingu na wejściu QBAD_MUT jest ustawione na 1
- Kurtyna świetlna została (jest) zakłócona, a funkcja MUTING nie została włączona poprzez ustawienie wejścia ENABLE na 1.
- Para czujników 1 (MS_11 i MS_12) lub para czujników 2 (MS_21 i MS_22) nie została aktywowana lub dezaktywowana w czasie rozbieżności, kolejno DISCTIM1 lub DISCTIM2
- Funkcja MUTING jest aktywna dłużej niż maksymalny czas mutingu TIME_MAX
- Czasy rozbieżności DISCTIM1 oraz DISCTIM2 ustawiono na wartości < 0 lub > 3 s
- Maksymalny czas mutingu TIME_MAX został ustawiony na wartość < 0 lub > 10 min
- System bezpieczeństwa uruchamia się (niezależnie od tego, czy kurtyna świetlna została naruszona, ponieważ F-I/O jest pasywowany po rozruchu systemu, wobec czego na wejście FREE jest początkowo podawana wartość 0)

W zidentyfikowanych przypadkach wyjście FAULT (błąd grupy) jest ustawiane na 1 (blokowanie restartu). Jeśli funkcja MUTING została uruchomiona, zostanie zakończona, a wyjście mutingu przybierze wartość 0.

Zatwierdzenie użytkownika do blokowania restartu (czujnik mutingu nie jest aktywny lub ENABLE = 0)

- Kurtyna świetlna nie jest zakłócona
- Występujące błędy zostały usunięte (patrz wyjście DIAG) oraz
- Zatwierdzenie użytkownika ze zboczem dodatnim występuje na wejściu ACK (zobacz również „Wdrożenie rozpoznawania użytkownika" (strona 196)).

Wyjście FAULT jest ustawione na 0. Wyjście ACK_REQ = 1 (oraz bit DIAG 6) sygnalizuje, że na wejściu ACK wymagane jest zatwierdzenie użytkownika w celu usunięcia blokady restartu. Instrukcja ustawia ACK_REQ = 1 gdy kurtyna świetlna nie jest zakłócona lub usunięto błędy. Po zatwierdzeniu instrukcja resetuje ACK_REQ do 0.

Zatwierdzenie użytkownika do blokowania restartu (czujnik mutingu jest aktywny i ENABLE = 1)

Sygnał aktywacji Q przybiera ponownie wartość 1, gdy:

- Występujące błędy zostały usunięte (patrz wyjście DIAG)
- FREE występuje aż do wykrycia poprawnej kombinacji czujników mutingu

Wyjście FAULT jest ustawione na 0. Funkcja MUTING jest resetowana w razie potrzeby, a wyjście MUTING przybiera wartość 1, jeśli zostanie wykryta poprawna kombinacja czujników mutingu. Gdy ENABLE = 1, wyjście ACK_REQ = 1 (oaz bit DIAG 5) sygnalizuje, że FREE jest niezbędne do usunięcia błędu oraz do zdjęcia blokady restartu. *Po pomyślnym FREE, ACK_REQ jest resetowane do 0 przez instrukcję.

Uwaga

Po przekroczeniu maksymalnego czasu mutingu, TIME_MAX jest resetowane gdy tylko funkcja MUTING zostanie zresetowana.

Funkcja FREE

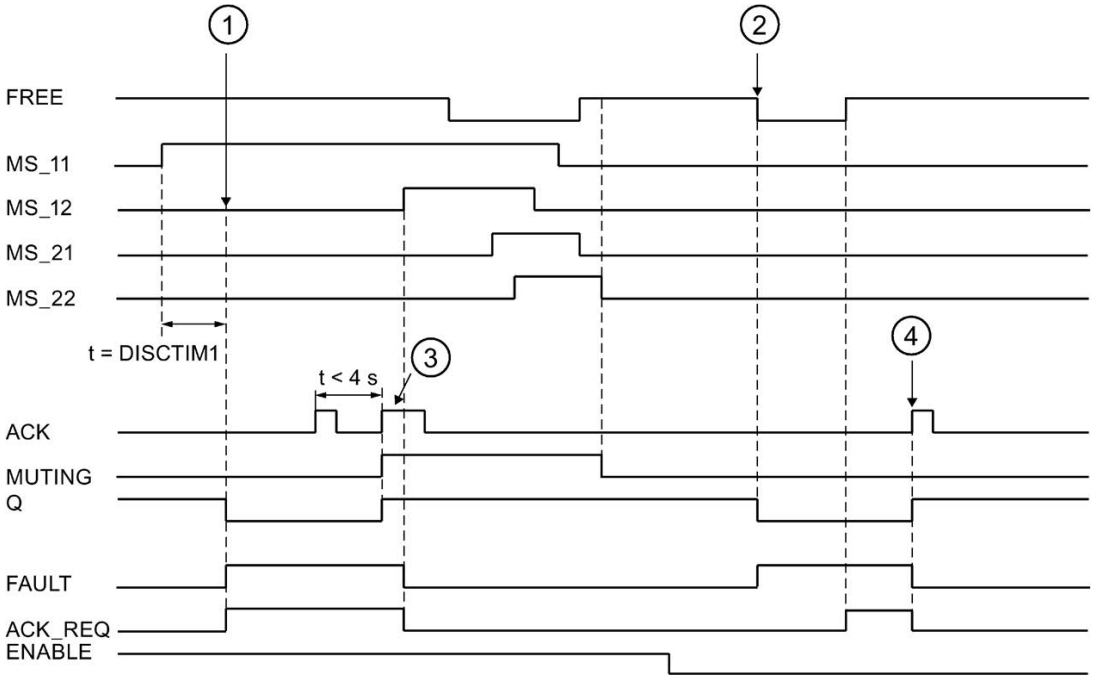
Jeśli nie jest możliwe natychmiastowe usunięcie błędu, funkcja FREE pozwala na zwolnienie zakresu mutingu. Sygnał aktywacji Q oraz wyjście MUTING = 1 tymczasowo. Funkcja FREE może zostać użyta, jeśli:

- ENABLE = 1
- Co najmniej jeden czujnik mutingu został aktywowany
- Zatwierdzenie użytkownika ze zboczem narastającym na wejściu ACK wystąpi dwukrotnie w ciągu 4 s, a drugie zatwierdzenie na wejściu ACK utrzymuje się na stanie sygnału 1 (przycisk zatwierdzenia pozostaje aktywny)

⚠ OSTRZEŻENIE

Podczas korzystania z funkcji FREE, należy kontrolować działanie. Musi być możliwe przerwanie w dowolnej chwili niebezpiecznej sytuacji poprzez zwolnienie przycisku zatwierdzenia. Przycisk zatwierdzenia musi być zamontowany w sposób pozwalający na obserwowanie całego niebezpiecznego obszaru. *(S037)*

Schematy taktowania dla błędów rozbieżności na parze czujników 1 lub dla zakłócenia kurtyny świetlnej (MUTING nie jest aktywny)



① Para czujników 1 (MS_11 i MS_22) nie została aktywowana w czasie rozbieżności DISCTIM1.

② Kurtyna świetlna została naruszona, mimo iż brak jest aktywacji (ENABLE=0)

③ Funkcja FREE

④ Zatwierdzenie

Zachowanie z zatrzymanym urządzeniem przenośnikowym

Jeśli, w stanie zatrzymanego urządzenia przenośnikowego, konieczne jest wyłączenie monitowania z jednego z poniższych powodów:

- Aby zapewnić zgodność z czasem rozbieżności DISCTIM1 lub DISCTIM2
- Aby zapewnić zgodność maksymalnym czasem mutingu TIME_MAX

Należy doprowadzić na wejście STOP sygnał „1" przez cały czas zatrzymania urządzenia przenośnikowego. Gdy tylko urządzenie przenośnikowe wznowi pracę (STOP = 0), czasy rozbieżności DISCTIM1 i DISCTIM2 oraz maksymalny czas mutingu TIME_MAX są resetowane.

⚠ OSTRZEŻENIE

Gdy STOP = 1 lub ENABLE = 0, monitorowanie rozbieżności jest wyłączone. W tym czasie, jeśli wejścia MSx1/MSx2 pary czujników przybiorą stan sygnału 1 wskutek niewykrytego błędu, np. oba czujniki mutingu zablokują się na 1, błąd nie będzie wykrywany, a funkcja MUTING może zostać niezamierzenie aktywowana (gdy ENABLE = 1). *(S038)*

Wyjście DIAG

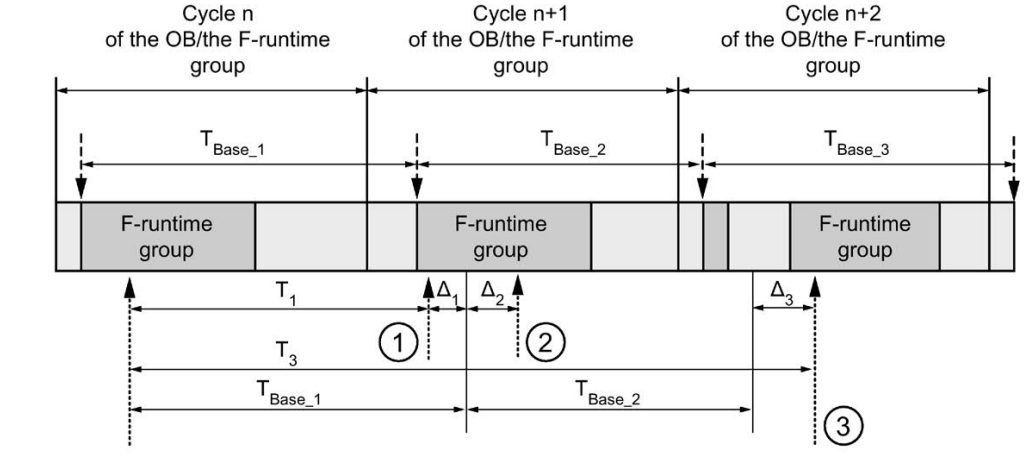
Wyjście DIAG zapewnia w celach serwisowych informacje nie fail-safe na temat błędów. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG 0 do 6 są zapisywane aż do zatwierdzenia na wejściu ACK.

Struktura DIAG

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Błąd rozbieżności lub nieprawidłowa nastawa czasu rozbieżności DISCTIM 1 dla pary czujników 1	Usterka w sekwencji produkcyjnej	Usterka w sekwencji produkcyjnej usunięta
		Uszkodzony czujnik	Sprawdzić czujniki
		Usterka okablowania	Sprawdzić okablowanie czujników
		Czujniki są podłączone do innego F-I/O oraz usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
		Nastawa czasu rozbieżności jest zbyt niska	W razie potrzeby należy ustawić wyższy czas rozbieżności
		Nastawa czasu rozbieżności to < 0 s lub > 3 s	Ustawić czas rozbieżności w zakresie pomiędzy 0 a 3 s
Bit 1	Błąd rozbieżności lub nieprawidłowa nastawa czasu rozbieżności DISCTIM 2 dla pary czujników 2	Tak samo jak bit 0	Tak samo jak bit 0
Bit 2	Przekroczony maksymalny czas mutingu lub nieprawidłowe ustawienie czasu mutingu TIME_MAX	Usterka w sekwencji produkcyjnej	Usterka w sekwencji produkcyjnej usunięta
		Nastawa maksymalnego czasu mutingu jest zbyt niska	W razie potrzeby należy ustawić wyższy maksymalny czas mutignu
		Nastawa czasu mutingu to < 0 s lub > 10 min	Ustawić czas mutingu w zakresie między 0 s a 10 min
Bit 3	Przerwana kurtyna świetlna bez aktywnego mutingu	ENABLE = 0	Ustaw ENABLE = 1
		Uszkodzona kurtyna świetlna	Sprawdzić kurtynę świetlną
		Usterka okablowania	Sprawdzić okablowanie kurtyny świetlnej (wejście FREE)
		Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O kurtyny świetlnej (wejście FREE)	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
		Rozruch systemu bezpieczeństwa	DIa FREE, patrz DIAG Bit 5
		Patrz inne bity DIAG	
Bit 4	Kontrolka mutingu jest uszkodzona lub nie można jej ustawić	Kontrolka mutingu jest uszkodzona	Wymienić kontrolkę mutingu
		Usterka okablowania	Sprawdzić okablowanie kontrolki
		Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O kontrolki mutingu	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 5	FREE jest konieczne	Patrz inne bity DIAG	Dwa zbocza narastające na ACK w ciągu 4 s, aktywacja przycisku zatw. aż do chwili ACK_REQ = 0
Bit 6	Niezbędne zatwierdzenie	—	—
Bit 7	Stan wyjścia Q	—	—
Bit 8	Stan wyjścia MUTING	—	—
Bit 9	FREE aktywne	—	—
Bit 10	Zastrzeżony	—	—
...			
Bit 15	Zastrzeżony	—	—

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



----► = Time base update

·····► = Call time of an instruction with time processing

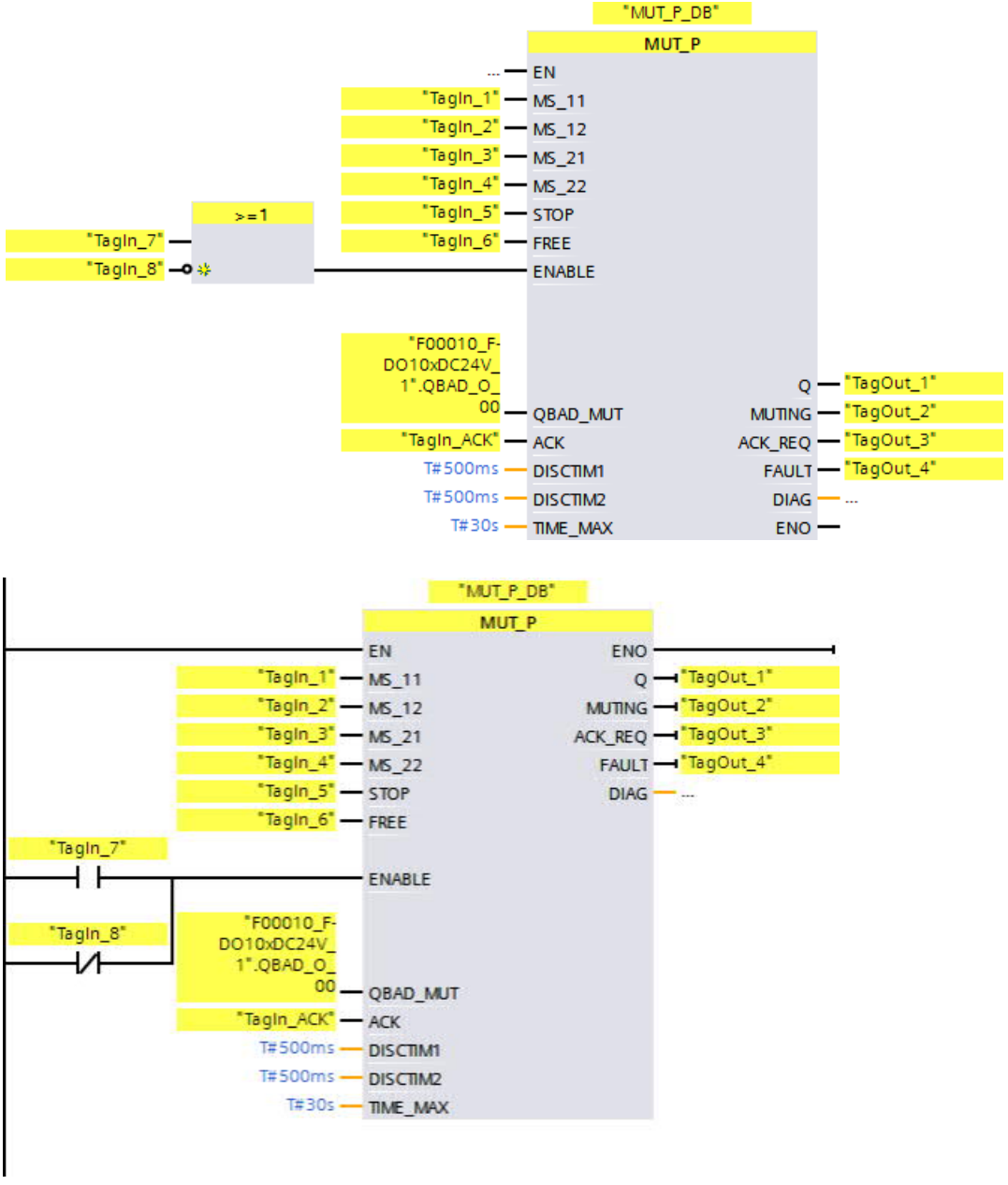
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



13.3.6 EV1oo2DI: Ocena 1oo2 z analizą rozbieżności (STEP7 Safety V16)

Opis

Ta instrukcja wprowadza ocenę 1oo2 dwóch jednokanałowych czujników w połączeniu z analizą rozbieżności.

Wyjście Q jest ustawiane na 1, jeśli stan sygnału wejść IN1 i IN2 jest równy 1 i nie ma zapisanych błędów rozbieżności DISC_FLT. Jeśli stan sygnału jednego lub obu wejść to 0, wyjście Q jest ustawiane na 0.

Gdy tylko stany sygnału wejść IN1 i IN2 zaczną się różnić, uruchamiany jest czas rozbieżności DISCTIME. Jeśli stany sygnału obu wejść wciąż są różne po upłynięciu czasu rozbieżności, wykrywany jest błąd rozbieżności, a DISC_FLT jest ustawiane na 1 (blokada restartu).

Jeśli rozbieżność pomiędzy wejściami IN1 i IN2 nie jest już wykrywana, błąd rozbieżności jest zatwierdzany zgodnie z przypisaniem parametru ACK_NEC:

- Jeśli ACK_NEC = 0, zatwierdzenie odbywa się automatycznie.
- Jeśli ACK_NEC = 1, należy użyć zbocza narastającego na wejściu ACK do zatwierdzenia błędu rozbieżności.

Wyjście ACK_REQ = 1 sygnalizuje, że na wejściu ACK wymagane jest zatwierdzenie użytkownika w celu zatwierdzenia błędu rozbieżności (anulowania blokady restartu). Instrukcja ustawia ACK_REQ = 1 w chwili braku wykrywania rozbieżności. Po zatwierdzeniu lub, jeśli przed nim ponownie wystąpi rozbieżność pomiędzy wejściami IN1 i IN2, instrukcja resetuje ACK_REQ do 0.

Wyjście Q nigdy nie może być ustawione na 1, jeśli nastawa czasu rozbieżności jest < 0 lub > 60 s. W takim przypadku wyjście DISC_FLT również jest ustawiane na 1 (blokada restartu). Interwał wywołania programu bezpieczeństwa (np. OB 35) musi być mniejszy niż nastawa czasu rozbieżności.

Każde wywołanie instrukcji „1oo2 evaluation with discrepancy analysis" (Ocena 1oo2 z analizą rozbieżności) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. EV1oo2DI_DB_1) lub wiele instancji (np. EV1oo2DI_Instance_1) dla instrukcji „1oo2 evaluation with discrepancy analysis" (Ocena 1oo2 z analizą rozbieżności). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

OSTRZEŻENIE

Do znacznika ACK_NEC nie można przypisać wartości 0, o ile automatyczny restart danego procesu nie jest w inny sposób wykluczony. *(S033)*

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN1	Wejście	BOOL	Czujnik 1
IN2	Wejście	BOOL	Czujnik 2
DISCTIME	Wejście	TIME	Czas rozbieżności (0 – 60 s)
ACK_NEC	Wejście	BOOL	1 = niezbędne zatwierdzenie dla błędu rozbieżności
ACK	Wejście	BOOL	Zatwierdzenie błędu rozbieżności
Q	Wyjście	BOOL	Wyjście
ACK_REQ	Wyjście	BOOL	1= wymagane zatwierdzenie
DISC_FLT	Wyjście	BOOL	1 = błąd rozbieżności
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	x	x	

o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

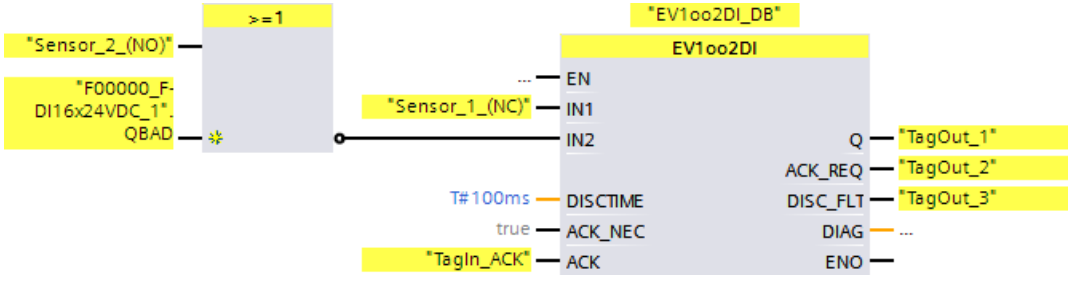
Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

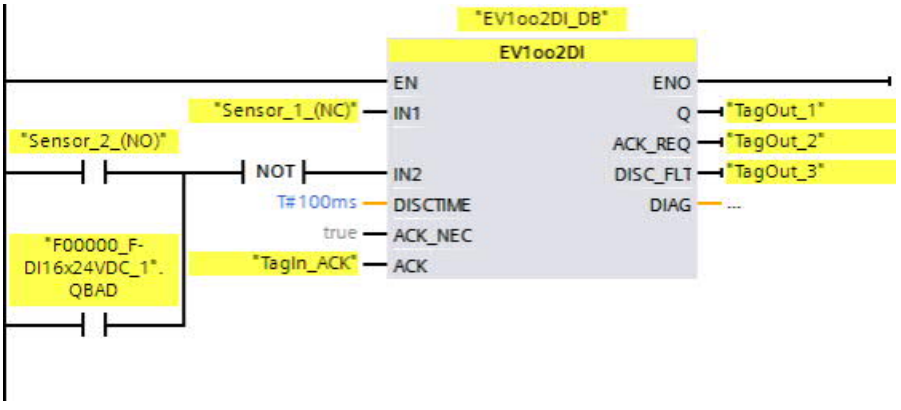
Aktywacja wejść IN1 i IN2

Wejścia IN1 i IN2 muszą być aktywowane w taki sposób, by ich bezpieczny stan wynosił 0.

Przykład z sygnałem QBAD lub QBAD_I_xx

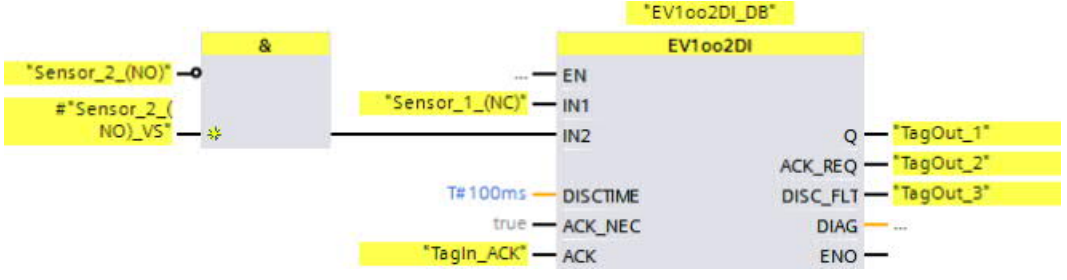
W przypadku nierównoważnych sygnałów, należy wykonać operację OR na wejściu (IN1 i IN2), do którego przypisano sygnał enkodera do bezpiecznego stanu 1, wraz sygnałem QBAD powiązanego F-I/O lub sygnał QBAD_I_xx powiązanego kanału (z F-CPU S7-300/400), po czym zanegować wynik. Stan sygnału 0 na wejściu IN1 lub IN2, gdy wartości fail-safe są wyprowadzane.

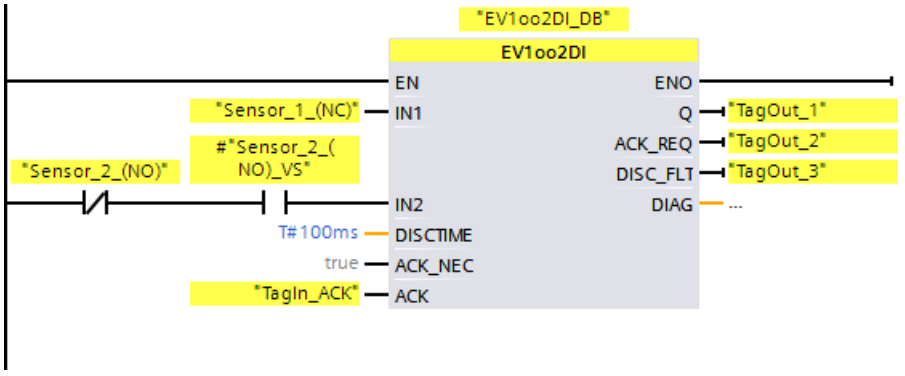




Przykład ze stanem wartości

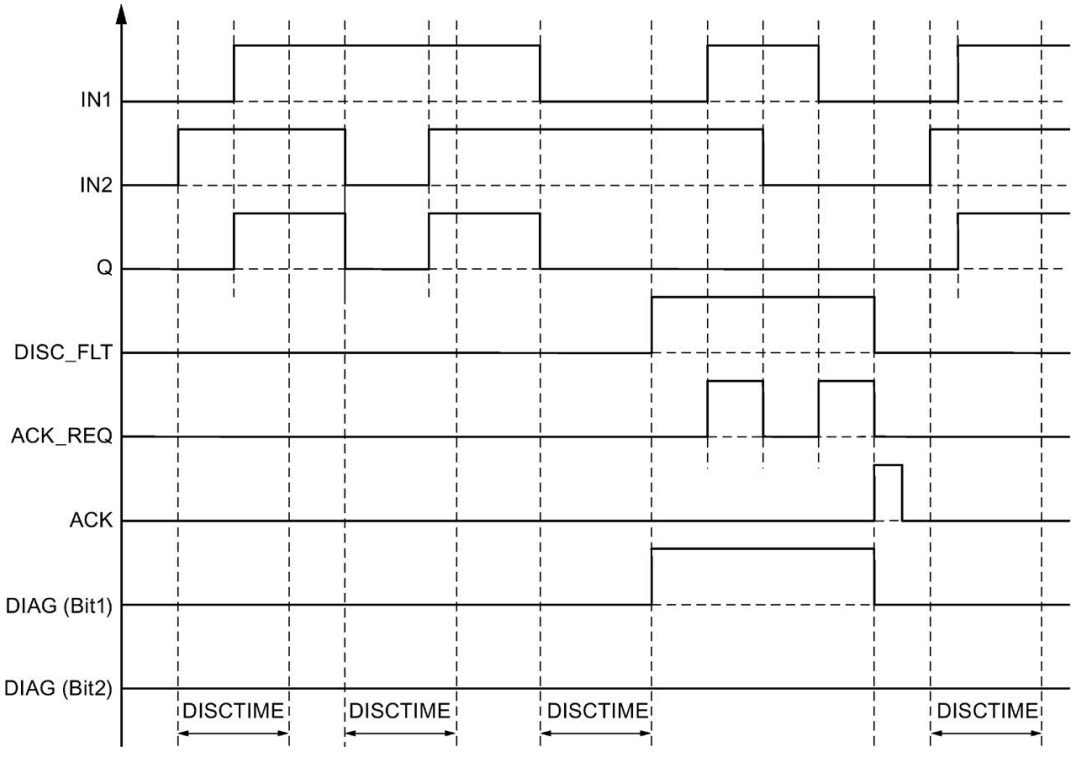
W przypadku nierównoważnych sygnałów, należy zanegować wejście (IN1 lub IN2), do którego przypisano sygnał enkodera do bezpiecznego stanu 1, po czym wykonać operację AND ze stanem wartości powiązanego kanału. Stan sygnału 0 na wejściu IN1 lub IN2, gdy wartości fail-safe są wyprowadzane.





Schematy taktowania EV1oo2DI

Jeśli ACK_NEC = 1:



Charakterystyka rozpoczęcia pracy

Uwaga

Jeśli czujniki na wejściach IN1 i IN2 są przypisane do różnych F-I/O, możliwe jest, by wartości fail-safe były wyprowadzane dla różnych czasów po uruchomieniu systemu bezpieczeństwa ze względu na charakterystykę rozpoczęcia pracy F-I/O. Jeśli stany sygnału wejść IN1 i IN2 pozostają różne po upłynięciu czasu rozbieżności DISCTIME, po uruchomieniu systemu bezpieczeństwa wykrywany jest błąd rozbieżności.

Jeśli ACK_NEC = 1, należy zatwierdzić błąd rozbieżności za pomocą zbocza narastającego na wejściu ACK.

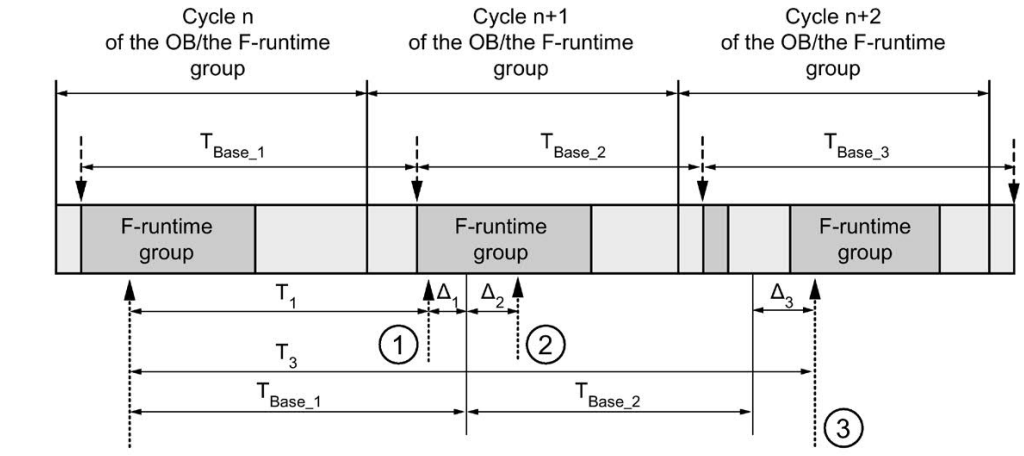
Wyjście DIAG

Wyjście DIAG zapewnia w celach serwisowych informacje nie fail-safe na temat błędów. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG są zapisywane aż do zatwierdzenia na wejściu ACK.

Struktura DIAG

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Błąd rozbieżności lub nieprawidłowa nastawa czasu rozbieżności (= stan DISC_FLT)	Uszkodzony czujnik	Sprawdzić czujniki
		Usterka okablowania	Sprawdzić okablowanie czujników
		Czujniki są podłączone do innego F-I/O oraz usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
		Nastawa czasu rozbieżności jest zbyt niska	W razie potrzeby należy ustawić wyższy czas rozbieżności
		Nastawa czasu rozbieżności to < 0 s lub > 60 s	Ustawić czas rozbieżności w zakresie pomiędzy 0 a 60 s
Bit 1	W przypadku błędów rozbieżności: ostatnia zmiana stanu sygnału na wejściu IN1	—	—
Bit 2	W przypadku błędów rozbieżności: ostatnia zmiana stanu sygnału na wejściu IN2	—	—
Bit 3	Zastrzeżony	—	—
Bit 4	Zastrzeżony	—	—
Bit 5	W przypadku błędów rozbieżności: wejście ACK ma permanentny stan sygnału 1	Uszkodzony przycisk zatwierdzenia	Wymienić przycisk zatwierdzenia
		Usterka okablowania	Sprawdzić okablowanie przycisku zatwierdzenia
Bit 6	Niezbędne zatwierdzenie	—	—
Bit 7	Stan wyjścia Q	—	—

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



----► = Time base update

·····► = Call time of an instruction with time processing

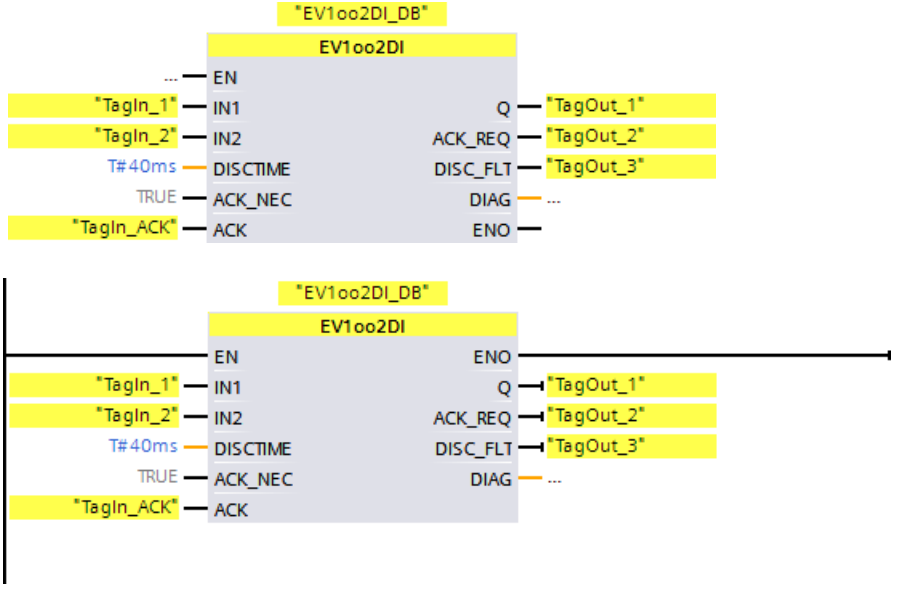
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



13.3.7 FDBACK: Monitorowanie sygnału zwrotnego (STEP 7 Safety

Opis

Ta instrukcja wprowadza monitorowanie sygnału zwrotnego.

Sprawdzany jest stan sygnału wyjścia Q, by określić, czy odpowiada on stanowi odwróconego sygnału wejścia sygnału zwrotnego FEEDBACK.

Wyjście Q jest ustawiane na 1, gdy tylko wejście ON = 1. Wymogiem dla tego warunku jest to, by wejście sygnału zwrotnego FEEDBACK = 1 oraz brak zapisanego błędu sygnału zwrotnego.

Wyjście Q jest resetowane do 0, gdy tylko wejście ON = 0 lub zostanie wykryty błąd sygnału zwrotnego.

Błąd sygnału zwrotnego ERROR = 1 jest wykrywany, gdy odwrócony stan sygnału wejścia sygnału zwrotnego FEEDBACK (do wyjścia Q) nie występuje za stanem sygnału wyjścia Q w maksymalnym dopuszczalnym czasie sygnału zwrotnego. Zapisywany jest błąd sygnału zwrotnego.

W przypadku wykrycia rozbieżności pomiędzy wejściem sygnału zwrotnego FEEDBACK a wyjściem Q po wystąpieniu błędu sygnału zwrotnego, błąd ten jest zatwierdzany zgodnie z przypisaniem parametru do ACK_NEC:

- Jeśli ACK_NEC = 0, zatwierdzenie odbywa się automatycznie.
- Jeśli ACK_NEC = 1, należy zatwierdzić błąd sygnału zwrotnego za pomocą zbocza narastającego na wejściu ACK.

Wyjście ACK_REQ = 1 sygnalizuje, że zatwierdzenie użytkownika jest wymagane na wejściu ACK do zatwierdzenia błędu sygnału zwrotnego. Po zatwierdzeniu instrukcja resetuje ACK_REQ do 0.

Aby uniknąć wykrywania błędów sygnału zwrotnego i konieczności ich zatwierdzania, gdy F-I/O sterowane przez wyjście Q są pasywowane, konieczne jest doprowadzenie na wejście QBAD_FIO sygnału QBAD z powiązanego F-I/O lub sygnału QBAD_O_xx / odwróconego stanu sygnału powiązanego kanału.

Każde wywołanie instrukcji „Feedback monitoring" (Monitorowanie sygnału zwrotnego) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. FDBACK_DB_1) lub wiele instancji (np. FDBACK_Instance_1) dla instrukcji „Feedback monitoring" (Monitorowanie sygnału zwrotnego). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

OSTRZEŻENIE

Do znacznika ACK_NEC nie można przypisać wartości 0, o ile automatyczny restart danego procesu nie jest w inny sposób wykluczony. *(S033)*

⚠OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ON	Wejście	BOOL	1= Włączone wyjście
FEEDBACK	Wejście	BOOL	Wejście sygnału zwrotnego
QBAD_FIO	Wejście	BOOL	Sygnał QBAD z F-I/O lub sygnał QBAD_O_xx / odwrócony stan wartości wyjścia Q
ACK_NEC	Wejście	BOOL	1=Niezbędne zatwierdzenie
ACK	Wejście	BOOL	Zatwierdzenie
FDB_TIME	Wejście	TIME	Czas sygnału zwrotnego
Q	Wyjście	BOOL	Wyjście
ERROR	Wyjście	BOOL	Błąd sygnału zwrotnego
ACK_REQ	Wyjście	BOOL	Żądane zatwierdzenie
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

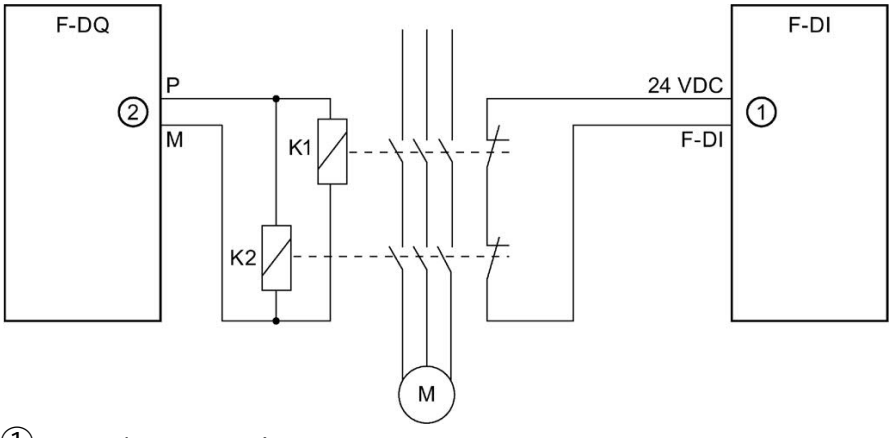
Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Wersja 1.0 wymaga, by blok F_TOF z numerem FB 186 był dostępny w drzewku projektu w folderze „Program blocks/System blocks/STEP 7 Safety". Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji. Uniknie się dzięki temu niezgodności w numeracji.
1,1	x	—	—	Te wersje są funkcjonalnie identyczne z wersją V1.0, lecz nie wymagają, by blok F_TOF miał określony numer.
1,2	x	—	o	
1,3	x	o	o	
1,4	x	o	o	
1,5	x	x	x	

o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępnawersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład wzajemnego połączenia



① Wysłanie do wejścia FEEDBACK instrukcji

② z wyjścia Q

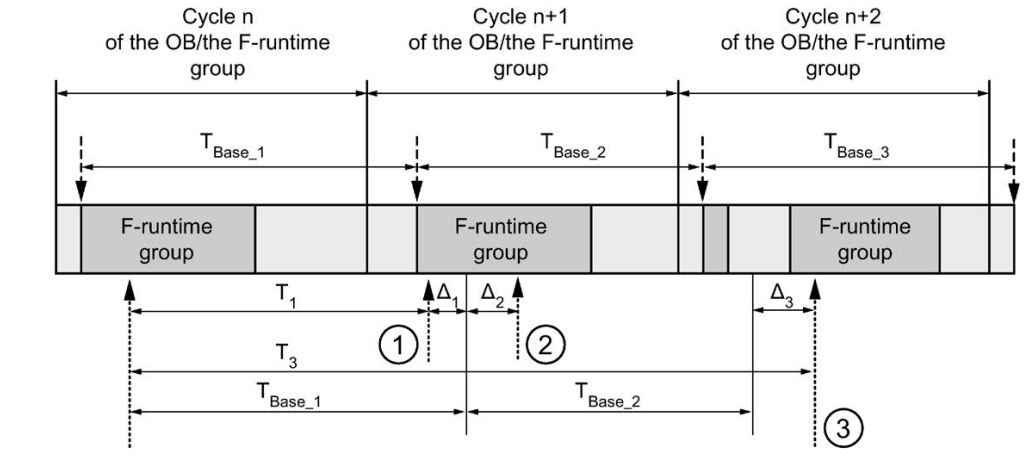
Wyjście DIAG

Wyjście DIAG zapewnia w celach serwisowych informacje nie fail-safe na temat błędów. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG 0, 2 i 5 są zapisywane aż do zatwierdzenia na wejściu ACK.

Struktura DIAG

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Błąd sygnału zwrotnego lub nieprawidłowa nastawa czasu sygnału zwrotnego (= stan ERROR)	Nastawa czasu sygnału zwrotnego	Ustawić czas sygnału zwrotnego > 0
		Nastawa czasu sygnału zwrotnego jest zbyt niska	W razie potrzeby należy ustawić wyższy czas sygnału zwrotnego
		Usterka okablowania	Sprawdzić okablowanie elementu wykonawczego i styk sygnału
		Element wykonawczy lub styk sygnału zwrotnego uszkodzony	Sprawdzić element wykonawczy i styk sygnału zwrotnego
		Usterka I/O lub usterka kanału wejścia sygnału zwrotnego	Sprawdzić I/O
Bit 1	Pasywacja kanału F-I/O sterowanego przez wyjście Q (= stan QBAD_FIO)	Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
Bit 2	Po błędzie sygnału zwrotnego: wejście sygnału zwrotnego ma permanentny stan sygnału 0	Usterka F-I/O lub usterka kanału wejścia sygnału zwrotnego	Sprawdzić I/O
		Styk sygnału zwrotnego uszkodzony	Sprawdzić styk sygnału zwrotnego
		Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O wejścia sygnału zwrotnego	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
Bit 3	Zastrzeżony	—	—
Bit 4	Zastrzeżony	—	—
Bit 5	W przypadku błędu sygnału zwrotnego: wejście ACK ma permanentny stan sygnału 1	Uszkodzony przycisk zatwierdzenia	Sprawdzić przycisk zatwierdzenia
		Usterka okablowania	Sprawdzić okablowanie przycisku zatwierdzenia
Bit 6	Wymagane zatwierdzenie (= stan ACK_REQ)	—	—
Bit 7	Stan wyjścia Q	—	—

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



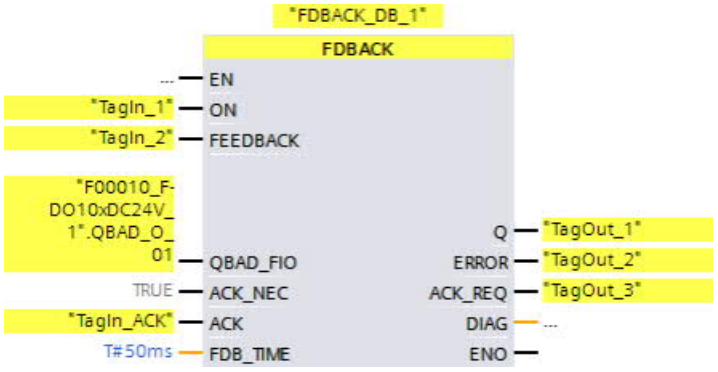
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

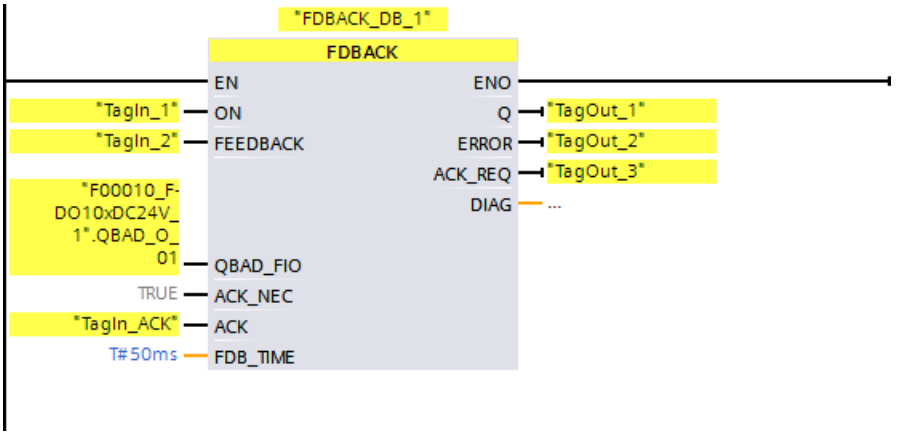
② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

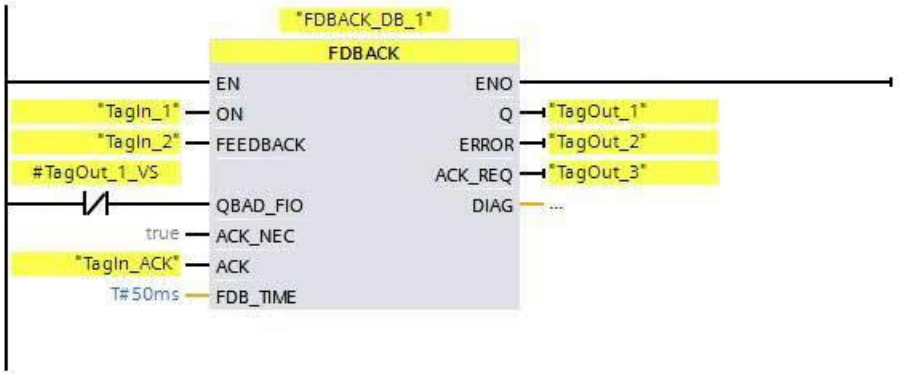
Przykład

Poniższy przykład przedstawia sposób działa instrukcji dla F-CPU S7-300/400:





Poniższy przykład przedstawia sposób działa instrukcji dla F-CPU S7-1200/1500:


"FDBACK_DB_1"
FDBACK
EN
ENO
"TagIn_1"
ON
Q
"TagOut_1"
"TagIn_2"
FEEDBACK
ERROR
"TagOut_2"
#TagOut_1_VS
ACK_REQ
"TagOut_3"
QBAD_FIO
DIAG
...
true
ACK_NEC
"TagIn_ACK"
ACK
T#50ms
FDB_TIME

13.3.8 SFDOOR: Monitorowanie drzwi bezpieczeństwa (STEP 7 Safety V16)

Opis

Ta instrukcja wprowadza monitorowanie drzwi bezpieczeństwa.

Sygnał aktywacji Q jest resetowany do 0, gdy tylko jedno z wejść IN1 lub IN2 przyjmie stan sygnału 0 (drzwi bezpieczeństwa są otwarte). Sygnał aktywacji można zresetować do 1,

- Wejścia IN1 i IN2 przyjmą stan sygnału 0 przed otwarciem drzwi (drzwi bezpieczeństwa zostały całkowicie otwarte)
- Wejścia IN1 i IN2 przyjmą stan sygnału 1 (drzwi bezpieczeństwa zamknięte)
- Występuje zatwierdzenie

Zatwierdzenie aktywacji odbywa się zgodnie z przypisaniem parametru na wejściu ACK_NEC:

- Jeśli ACK_NEC = 0, zatwierdzenie odbywa się automatycznie.
- Jeśli ACK_NEC = 1, należy użyć zbocza narastającego na wejściu ACK do zatwierdzenia aktywacji.

Wyjście ACK_REQ = 1 sygnalizuje, że zatwierdzenie użytkownika jest wymagane na wejściu ACK do zatwierdzenia. Instrukcja ustawia ACK_REQ = 1 w chwili zamknięcia drzwi. Po zatwierdzeniu instrukcja resetuje ACK_REQ do 0.

Aby instrukcja mogła rozpoznać, czy wejścia IN1 i IN2 mają wartość 0 jedynie z powodu pasywacji powiązanego F-I/O, należy doprowadzić na wejścia QBAD_IN1 lub QBAD_IN2 sygnał QBAD powiązanego F-I/O lub sygnał QBAD_I_xx / odwrócony stan sygnału powiązanego kanału. Pozwoli to, między innymi, na uniemożliwienie całkowitego otwarcia drzwi bezpieczeństwa przed zatwierdzeniem w razie pasywowania F-I/O.

Każde wywołanie instrukcji „Safety door monitoring" (Monitorowanie drzwi bezpieczeństwa) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. SFDOOR_DB_1) lub wiele instancji (np. SFDOOR_Instance_1) dla instrukcji „Safety door monitoring" (Monitorowanie drzwi bezpieczeństwa). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

⚠ OSTRZEŻENIE

Do znacznika ACK_NEC nie można przypisać wartości 0, o ile automatyczny restart danego procesu nie jest w inny sposób wykluczony. *(S033)*

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN1	Wejście	BOOL	Wejście 1
IN2	Wejście	BOOL	Wejście 2
QBAD_IN1	Wejście	BOOL	Sygnał QBAD z F-I/O lub sygnał QBAD_O_xx / stan wartości odwróconej kanału wejścia IN1
QBAD_IN2	Wejście	BOOL	Sygnał QBAD z F-I/O lub sygnał QBAD_O_xx / stan wartości odwróconej kanału wejścia IN2
OPEN_NEC	Wejście	BOOL	1 = Otwarcie konieczne przy rozruchu
ACK_NEC	Wejście	BOOL	1=Niezbędne zatwierdzenie
ACK	Wejście	BOOL	Zatwierdzenie
Q	Wyjście	BOOL	1 = Aktywne, drzwi bezpieczeństwa zamknięte
ACK_REQ	Wyjście	BOOL	Żądane zatwierdzenie
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	x	x	

o Ta wersja nie jest już obsługiwana.

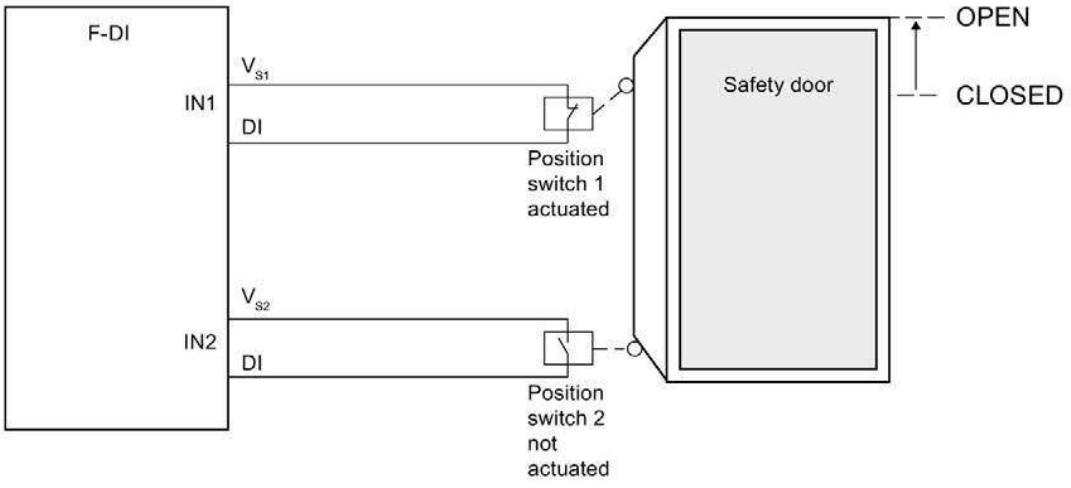
Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

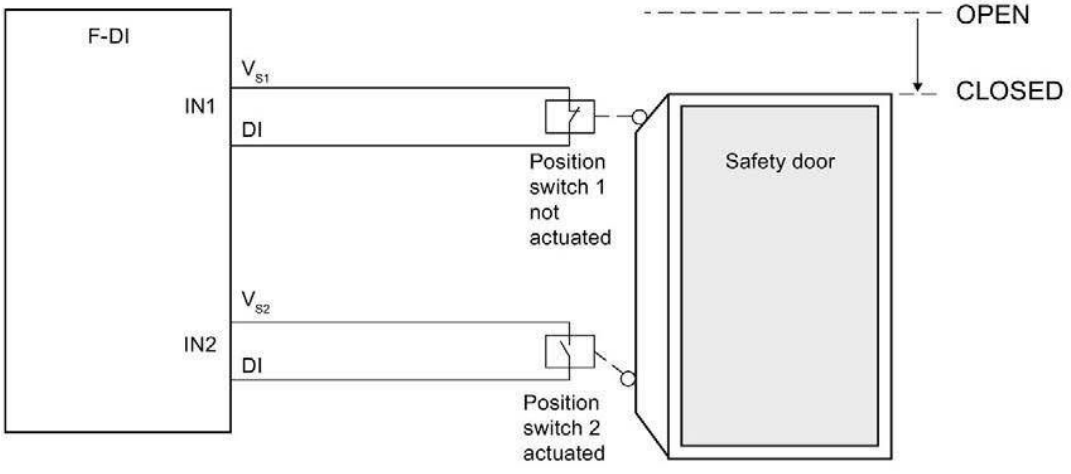
Przykład wzajemnego połączenia

Należy połączyć styk NC wyłącznika pozycyjnego 1 drzwi bezpieczeństwa z wejściem IN1, oraz styk NO wyłącznika pozycyjnego 2 z wejściem IN2. Wyłącznik pozycyjny 1 musi być zamontowany w taki sposób, by był aktywowany po otwarciu drzwi bezpieczeństwa. Wyłącznik pozycyjny 2 musi być zamontowany w taki sposób, by był aktywowany po zamknięciu drzwi bezpieczeństwa.

Safety door open:



Safety door closed:



Charakterystyka rozpoczęcia pracy

Po uruchomieniu systemu bezpieczeństwa sygnał aktywacji Q jest resetowany do 0. Zatwierdzenie aktywacji odbywa się zgodnie z przypisaniem parametru na wejściach OPEN_NEC oraz ACK_NEC:

- Gdy OPEN_NEC = 0, automatyczne zatwierdzenie występuje **niezależnie** od ACK_NEC, gdy tylko dwa wejścia IN1 i IN2 przyjmą stan sygnału 1 po raz pierwszy po reintegracji powiązanego F-I/O (drzwi bezpieczeństwa zostały zamknięte).
- Gdy OPEN_NEC = 1 **lub** gdy co najmniej jedno z wejść IN1 i IN2 wciąż ma stan sygnału 0 po reintegracji powiązanego F-I/O, automatyczne zatwierdzenie przebiega **zgodnie** z ACK_NEC lub należy użyć zbocza narastającego na wejściu ACK w celu aktywacji. Przed zatwierdzeniem wejścia IN1 i IN2 muszą przyjąć stan sygnału 0 (drzwi bezpieczeństwa zostały całkowicie otwarte), a następnie stan sygnału 1 (drzwi bezpieczeństwa zostały zamknięte).

OSTRZEŻENIE

Do znacznika OPEN_NEC nie można przypisać wartości 0, o ile automatyczny restart danego procesu nie jest w inny sposób wykluczony. *(S039)*

Wyjście DIAG

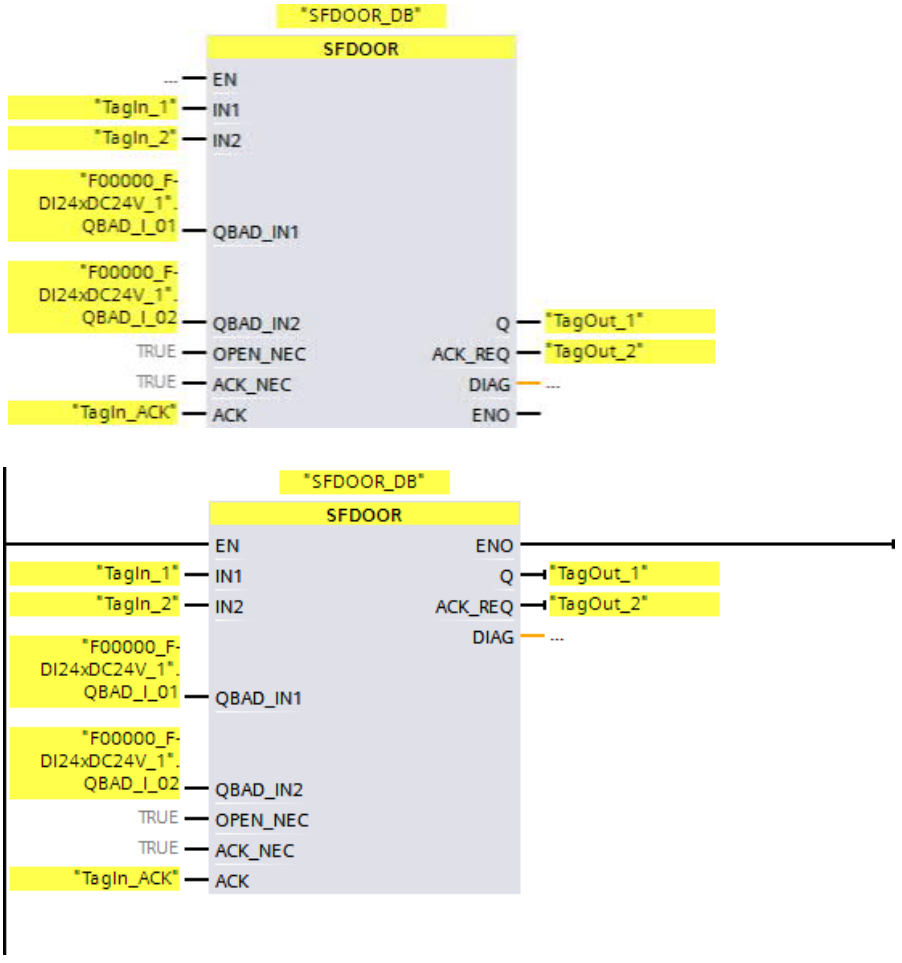
Wyjście DIAG zapewnia w celach serwisowych informacje nie fail-safe na temat błędów. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika.

Struktura DIAG

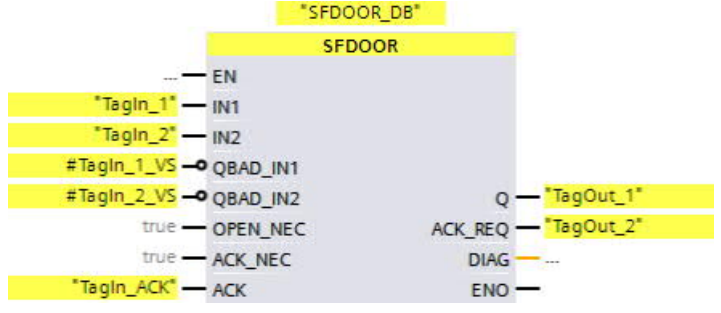
Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Zastrzeżony	—	—
Bit 1	Brak stanu sygnału 0 na wejściach IN1 oraz IN2	Drzwi bezpieczeństwa nie były całkowicie otwarte, gdy OPEN_NEC = 1 po uruchomieniu systemu bezpieczeństwa	W pełni otworzyć drzwi bezpieczeństwa
		Otwarte drzwi bezpieczeństwa nie były całkowicie otwarte	W pełni otworzyć drzwi bezpieczeństwa
		Usterka okablowania	Sprawdzić okablowanie wył. poz.
		Wyłącznik pozycyjny jest	Sprawdzić wyłącznik pozycyjny
		Wyłącznik pozycyjny jest nieprawidłowo wyregulowany	Wyregulować wyłącznik pozycyjny
Bit 2	Brak stanu sygnału 1 na wejściach IN1 oraz IN2	Drzwi bezp. nie były zamknięte	Zamknąć drzwi bezpieczeństwa
		Usterka okablowania	Sprawdzić okablowanie wył. poz.
		Wyłącznik pozycyjny jest	Sprawdzić wyłącznik pozycyjny
		Wyłącznik pozycyjny jest nieprawidłowo wyregulowany	Wyregulować wyłącznik pozycyjny
Bit 3	QBAD_IN1 i/lub QBAD_IN2 = 1	Usterka F-I/O, usterka kanału, błąd komunikacji lub pasywacja za pomocą PASS_ON w F-I/O lub kanale IN1 i/lub IN2	Rozwiązanie można znaleźć w dziale „Struktura DIAG", bity 0 do 6 w DIAG (strona 183)
Bit 4	Zastrzeżony	—	—
Bit 5	Jeśli brak aktywacji: wejście ACK ma permanentny stan sygnału 1	Uszkodzony przycisk zatwierdzenia	Sprawdzić przycisk zatwierdzenia
		Usterka okablowania	Sprawdzić okablowanie przycisku zatwierdzenia
Bit 6	Wymagane zatwierdzenie (= stan ACK_REQ)	—	—
Bit 7	Stan wyjścia Q	—	—

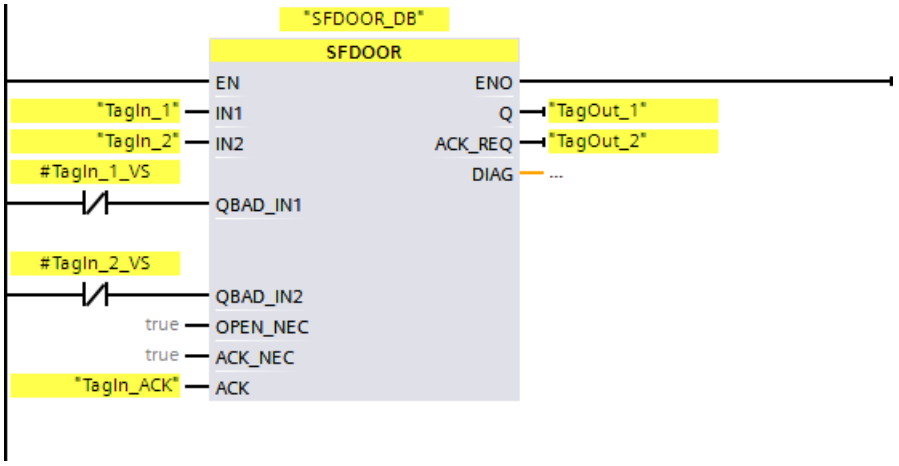
Przykład

Poniższy przykład przedstawia sposób działa instrukcji dla F-CPU S7-300/400:



Poniższy przykład przedstawia sposób działa instrukcji dla F-CPU S7-1200/1500:




"SFDOOR_DB"
SFDOOR
EN
ENO
"TagIn_1"
IN1
Q
"TagOut_1"
"TagIn_2"
IN2
ACK_REQ
"TagOut_2"
#TagIn_1_VS
DIAG
...
QBAD_IN1
#TagIn_2_VS
QBAD_IN2
true
OPEN_NEC
true
ACK_NEC
"TagIn_ACK"
ACK

13.3.9 ACK_GL: Zatwierdzenie globalne wszystkich F-I/O w grupie F-runtime (STEP 7 Safety V16)

Opis

Te instrukcje tworzą zatwierdzenie dla jednoczesnej reintegracji wszystkich F-I/O lub kanałów F-I/O grupy F-runtime po błędach komunikacji, błędach F-I/O lub usterkach kanałów.

Zatwierdzenie użytkownika (strona 196) ze zboczem dodatnim na wejściu AKC_GLOB jest konieczne do wykonania reintegracji. Zatwierdzenie przebiega analogicznie do zatwierdzenia użytkownika poprzez tag ACK_REI DB F-I/O (strona 178), lecz działa jednocześnie na wszystkie F-I/O grupy F-runtime, w której wywoływana jest instrukcja.

W przypadku korzystania z instrukcji ACK_GL, nie jest konieczne zapewnianie zatwierdzenia dla każdego F-I/O grupy F-runtime poprzez tag ACK_REI DB F-I/O.

Każde wywołanie instrukcji „Global acknowledgment of all F-I/O of a runtime group" (Zatwierdzenie globalne wszystkich F-I/O w grupie F-runtime) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. ACK_GL_DB_1) lub wiele instancji (np. ACK_GL_Instance_1) dla instrukcji „Global acknowledgment of all F-I/O of a runtime group" (Zatwierdzenie globalne wszystkich F-I/O w grupie F-runtime). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku.

Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Uwaga

Zatwierdzenie poprzez instrukcję ACK_GL jest możliwe jedynie, gdy tag ACK_REI DB F- I/O = 0. Analogicznie, zatwierdzenie poprzez tag ACK_REI DB F-I/O jest możliwe jedynie, jeśli wejście ACK_GLOB instrukcji = 0.

Instrukcję można wywołać tylko raz na grupę F-runtime.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ACK_GLOB	Wejście	BOOL	1 = zatwierdzenie do reintegracji

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	x	x	

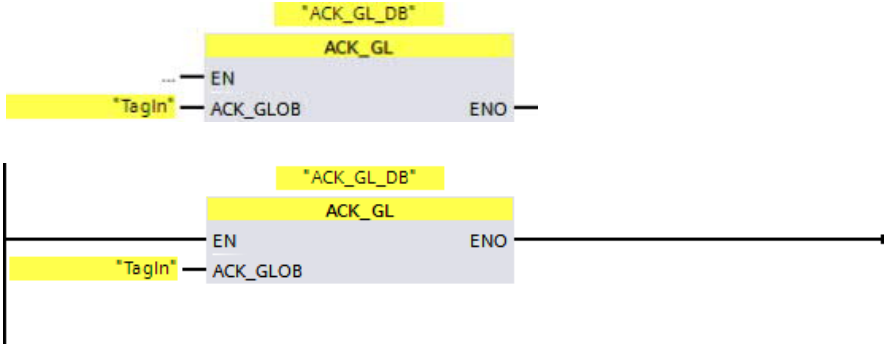
o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



13.4 Operacje czasowe

13.4.1 TP: Generowanie impulsu (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Generate impulse" (Generowanie impulsu) można ustawić wyjście Q na zaprogramowany okres. Instrukcja jest uruchamiana, jeśli wynik operacji logicznej (RLO) zmieni się z „0" na „1" (zbocze dodatnie) na wejściu IN. Zaprogramowany okres PT rozpoczyna się wraz z uruchomieniem instrukcji. Wyjście Q jest ustawiane na okres PT niezależnie od dalszej sekwencji sygnału wejściowego. Ponadto, wykrycie nowego zbocza sygnału dodatniego nie wpływa na stan sygnału na wyjściu Q przez czas trwania PT.

Możliwe jest wykonanie zapytania dla bieżącej wartości czasu na wyjściu ET. Wartość czasu rozpoczyna się od T#0s i kończy się po osiągnięciu wartości okresu PT. Jeśli okres PT uległ zakończeniu, a stan sygnału na wejściu IN to „0", wyjście ET jest resetowane.

Każde wywołanie instrukcji „Generate impulse" (Generowanie impulsu) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. F_IEC_Timer_DB_1) lub wiele instancji (np. F_IEC_Timer_Instance_1) dla instrukcji „Generate impulse" (Generowanie impulsu). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w *pomocy do STEP 7*.

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

System operacyjny resetuje instancje instrukcji „Generate impulse" (Generowanie impulsu) podczas uruchamiania systemu bezpieczeństwa.

Uwaga

Funkcjonalność tej instrukcji różni się od odnośnej standardowej instrukcji TP w następujących punktach:

- Jeśli instrukcja jest wywoływana, gdy czas działa z PT = 0 ms, wyjścia Q i ET są resetowane.
- Jeśli instrukcja jest wywoływana z PT < 0 ms, wyjścia Q i ET są resetowane.

Aby zrestartować impuls, wymagane jest nowe zbocze sygnału narastającego na wejściu IN, gdy PT ponownie będzie większy od 0.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	BOOL	Wejście startowe
PT	Wejście	TIME	Czas trwania impulsu; musi być dodatni
Q	Wyjście	BOOL	Wyjście impulsu
ET	Wyjście	TIME	Bieżąca wartość czasu

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	o	o	
1,4	x	x	x	

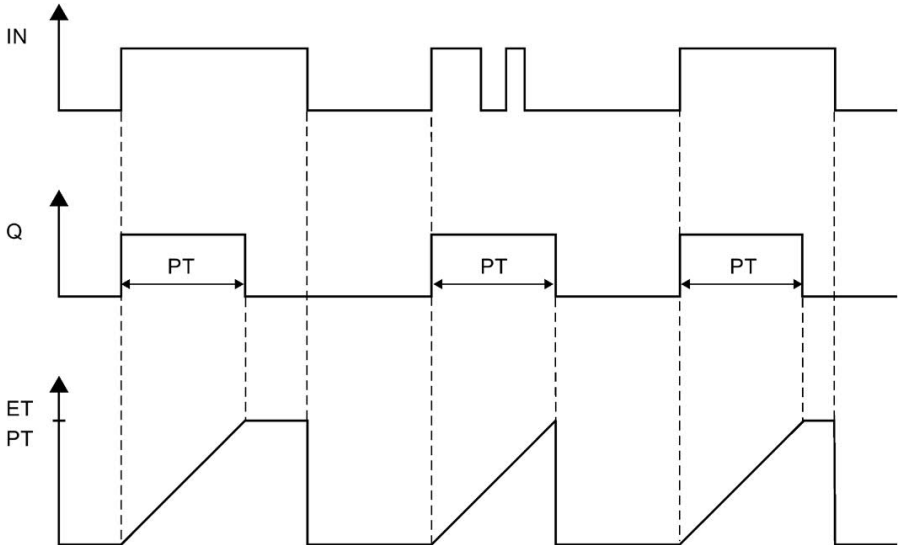
o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

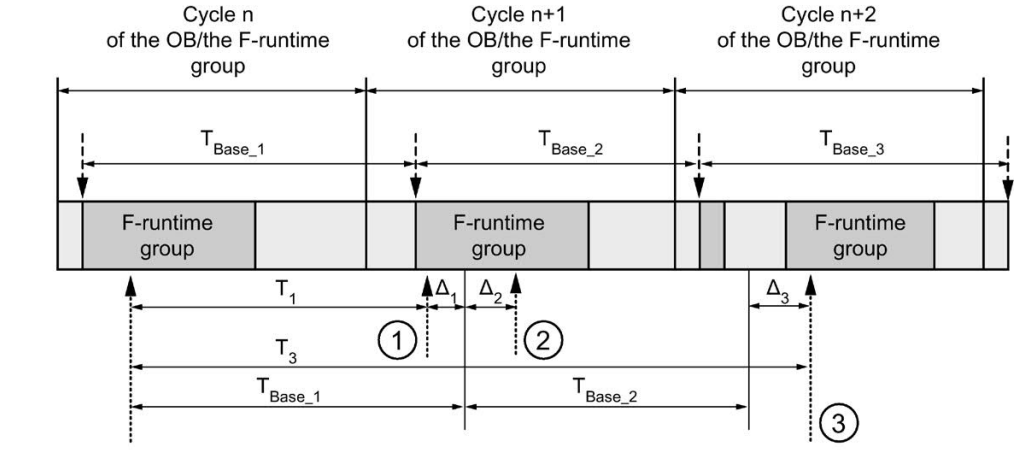
Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Schemat impulsów

Poniższa ilustracja przedstawia schemat impulsów instrukcji „Generate impulse" (Generowanie impulsu):



Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



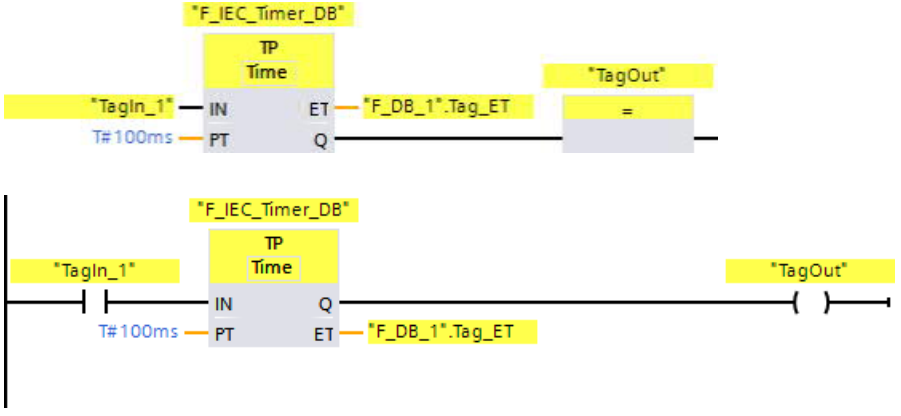
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Jeśli stan sygnału argumentu „TagIn_1" zmieni się z „0" na „1", uruchamiana jest instrukcja „Generate impulse" (Generowanie impulsu) i rozpoczyna się okres wyznaczony na wejściu PT (100 ms), niezależnie od dalszego przebiegu argumentu
„TagIn_1".

Argument „TagOut" na wyjściu Q ma stan sygnału „1" do czasu upłynięcia danego okresu. Argument „"F_DB_1".Tag_ET" zawiera bieżącą wartość czasu.

13.4.2 TON: Generowanie opóźnienia załączenia

Opis

Instrukcja „Generate on-delay" (Generowanie opóźnienia załączenia) służy do opóźniania ustawienia wyjścia Q przez określony okres PT. Instrukcja jest uruchamiana, jeśli wynik operacji logicznej (RLO) zmieni się z „0" na „1" (zbocze dodatnie) na wejściu IN. Zaprogramowany okres PT rozpoczyna się wraz z uruchomieniem instrukcji. Po upłynięciu okresu PT wyjście Q jest ustawiane na stan sygnału „1". Wyjście Q pozostaje ustawione dopóki wejście startowe nie zostanie ustawione na „1". Gdy stan sygnału na wejściu startowym zmieni się z „1" na „0", wyjście Q jest resetowane. Funkcja czasu jest restartowana, gdy na wejściu startowym zostanie wykryte nowe zbocze sygnału dodatniego.

Możliwe jest wykonanie zapytania dla bieżącej wartości czasu na wyjściu ET. Wartość czasu rozpoczyna się od T#0s i kończy się po osiągnięciu wartości okresu PT. Wyjście ET jest resetowane, gdy tylko stan sygnału na wejściu IN zmieni się na „0".

Każde wywołanie instrukcji „Generate on-delay" (Generowanie opóźnienia załączenia) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. F_IEC_Timer_DB_1) lub wiele instancji (np. F_IEC_Timer_Instance_1) dla instrukcji „Generate on-delay" (Generowanie opóźnienia załączenia). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w *pomocy do STEP 7*.

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

System operacyjny resetuje instancje instrukcji „Generate on-delay" (Generowanie opóźnienia załączenia) podczas uruchamiania systemu bezpieczeństwa.

Uwaga

Funkcjonalność tej instrukcji różni się od odnośnej standardowej instrukcji TON w następujących punktach:

- Jeśli instrukcja jest wywoływana, gdy czas działa z PT = 0 ms, wyjście ET jest resetowane.
- Jeśli instrukcja jest wywoływana z PT < 0 ms, wyjścia Q i ET są resetowane.

Aby zrestartować opóźnienie załączenia, wymagane jest nowe zbocze sygnału narastającego na wejściu IN, gdy PT ponownie będzie większy od 0.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	BOOL	Wejście startowe
PT	Wejście	TIME	Czas trwania opóźnienia załączenia; musi być dodatni
Q	Wyjście	BOOL	Wyjście ustawiane po upłynięciu czasu PT.
ET	Wyjście	TIME	Bieżąca wartość czasu

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	o	o	
1,4	x	x	x	

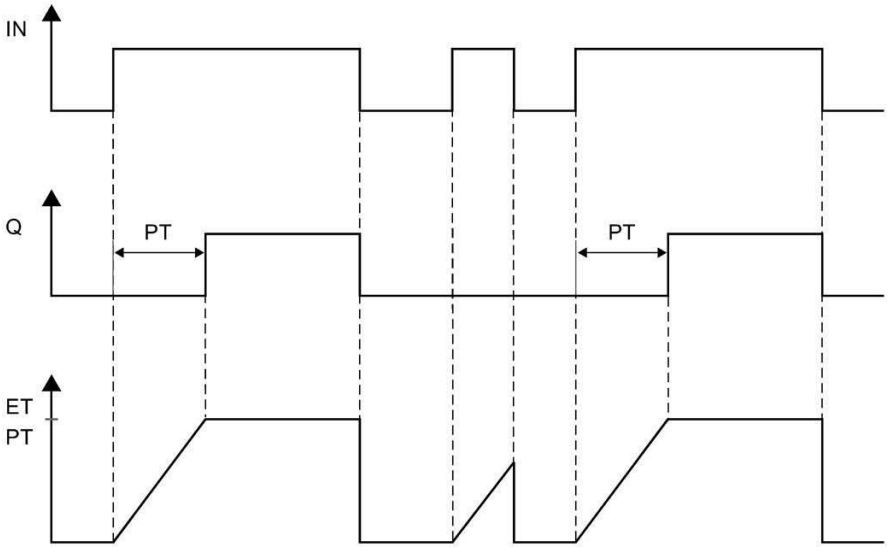
o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

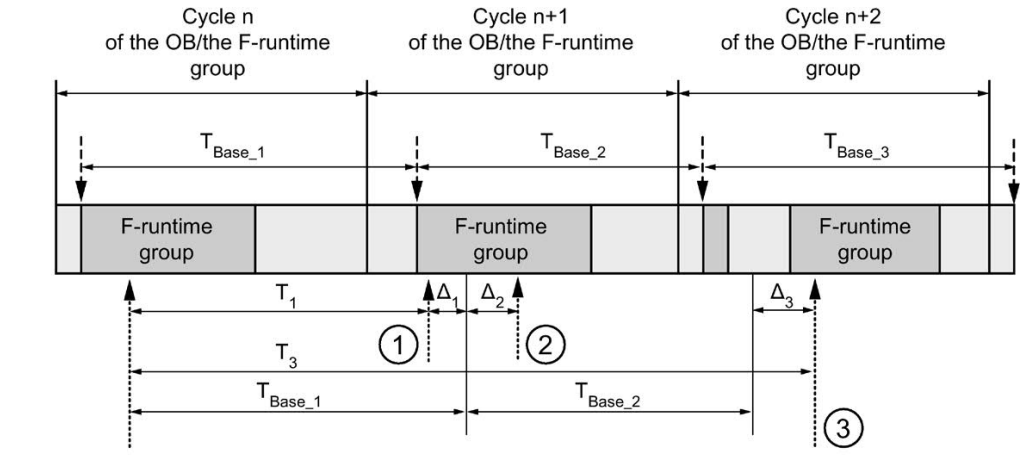
Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Schemat impulsów

Poniższa ilustracja przedstawia schemat impulsów instrukcji „Generate on-delay" (Generowanie opóźnienia załączenia):



Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



----► = Time base update

·····► = Call time of an instruction with time processing

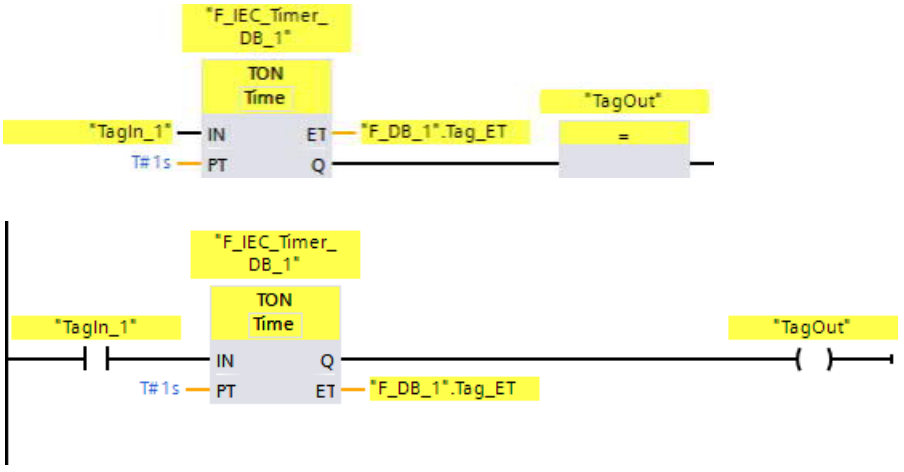
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gdy stan sygnału argumentu „TagIn_1" zmieni się z „0" na „1", uruchamiana jest instrukcja „Generate on-delay" (Generowanie opóźnienia załączenia) i rozpoczyna się okres wyznaczony na wejściu PT (1 ms).

Argument „TagOut" na wyjściu Q podaje stan sygnału „1", gdy upłynie zadany okres i pozostaje tak ustawione, dopóki „TagIn_1" podaje stan sygnału „1". Argument „"F_DB_1".Tag_ET" zawiera bieżącą wartość czasu.

13.4.3 TOF: Generowanie opóźnienia wyłączenia

Opis

Instrukcja „Generate off-delay" (Generowanie opóźnienia wyłączenia) służy do opóźniania resetowania wyjścia Q przez określony okres PT. Wyjście Q jest ustawiane, jeśli wynik operacji logicznej (RLO) zmieni się z „0" na „1" (zbocze dodatnie) na wejściu IN. Gdy stan sygnału na wejściu IN wróci do „0", rozpoczyna się zaprogramowany okres PT. Wyjście Q pozostaje ustawione przez czas trwania okresu PT. Po upłynięciu okresu PT, wyjście Q jest resetowane. Jeśli stan sygnału na wejściu IN zmieni się na „1" przed upłynięciem okresu PT, czas jest resetowany. Stan sygnału na wyjściu Q pozostaje na poziomie „1".

Możliwe jest wykonanie zapytania dla bieżącej wartości czasu na wyjściu ET. Wartość czasu rozpoczyna się od T#0s i kończy się po osiągnięciu wartości okresu PT. Po upłynięciu czasu PT wyjście ET pozostaje na bieżącej wartości do chwili zmiany wejścia IN z powrotem na „1". Jeśli wejście IN zmieni się na „1" przed upłynięciem czasu PT, wyjście ET jest resetowane do wartości T#0.

Każde wywołanie instrukcji „Generate off-delay" (Generowanie opóźnienia wyłączenia) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. F_IEC_Timer_DB_1) lub wiele instancji (np. F_IEC_Timer_Instance_1) dla instrukcji „Generate off-delay" (Generowanie opóźnienia wyłączenia). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku.

Więcej informacji dostępnych w *pomocy do STEP 7*.

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

System operacyjny resetuje instancje instrukcji „Generate off-delay" (Generowanie opóźnienia wyłączenia) podczas uruchamiania systemu bezpieczeństwa.

Uwaga

Funkcjonalność tej instrukcji różni się od odnośnej standardowej instrukcji TOF w następujących punktach:

- Jeśli instrukcja jest wywoływana, gdy czas działa z PT = 0 ms, wyjścia Q i ET są resetowane.
- Jeśli instrukcja jest wywoływana z PT < 0 ms, wyjścia Q i ET są resetowane.

Aby zrestartować opóźnienie wyłączenia, wymagane jest kolejne zbocze sygnału opadającego na wejściu IN, gdy PT ponownie będzie większy od 0.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	BOOL	Wejście startowe
PT	Wejście	TIME	Czas trwania opóźnienia wyłączenia; musi być dodatni
Q	Wyjście	BOOL	Wyjście resetowane po upłynięciu czasu PT.
ET	Wyjście	TIME	Bieżąca wartość czasu

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	o	o	
1,4	x	x	x	

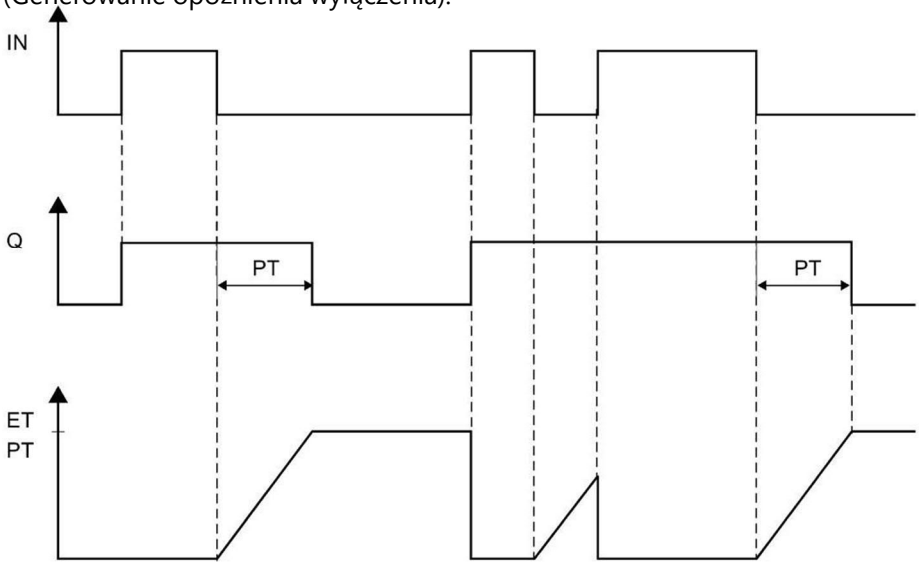
o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

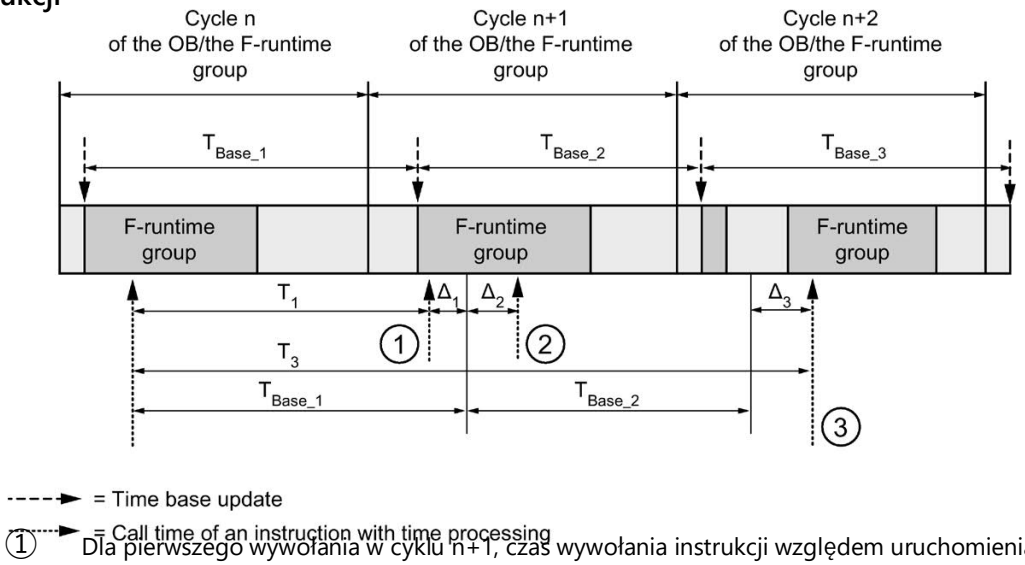
Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Schemat impulsów

Poniższa ilustracja przedstawia schemat impulsów instrukcji „Generate off-de lay" (Generowanie opóźnienia wyłączenia):



Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



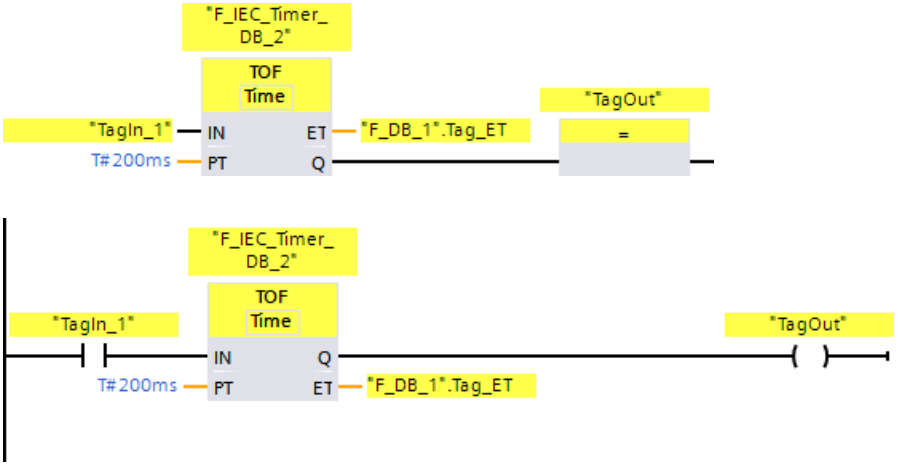
① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Jeśli stan sygnału argumentu „TagIn_1" zmieni się z „0" na „1", stan sygnału argumentu „TagOut" na wyjściu Q zostanie ustawiony na „1".

Jeśli stan sygnału argumentu „TagIn_1" zmieni się z powrotem na „0", rozpocznie się okres wyznaczony na wejściu PT (200 ms).

Argument „TagOut" na wyjściu Q jest ustawiany z powrotem na „0" po upłynięciu tego czasu. Argument „"F_DB_1".Tag_ET" zawiera bieżącą wartość czasu.

13.5 Operacje licznika

13.5.1 CTU: Zliczanie w górę (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Count up" (Zliczanie w górę) można zwiększyć wartość na wyjściu CV. Gdy stan sygnału na wejściu CU zmieni się z „0" na „1" (dodatnie zbocze sygnału), wykonywana jest instrukcja, a bieżący stan na wyjściu CV jest zwiększany o jeden. Wartość stanu jest zwiększana po każdym wykryciu narastającego zbocza sygnału aż do osiągnięcia górnego limitu rodzaju danych określonego na wyjściu CV. Po osiągnięciu górnego limitu stan sygnału na wejściu CU nie wpływa na instrukcję.

Status licznika można sprawdzić za pomocą wyjścia Q. Stan sygnału na wyjściu Q jest określany przez parametr PV. Gdy bieżąca wartość licznika jest większa lub równa wartości parametru PV, wyjście Q jest ustawiane na stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu Q to „0".

Wartość na wyjściu CV jest resetowana do zera, gdy stan sygnału na wejściu R zmieni się na „1". Dopóki utrzymuje się stan sygnału „1" na wejściu R, stan sygnału na wejściu CU nie ma wpływu na instrukcję.

Każde wywołanie instrukcji „Count up" (Zliczanie w górę) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. F_IEC_Counter_DB_1) lub wiele instancji (np. F_IEC_Counter_Instance_1) dla instrukcji „Count up" (Zliczanie w górę). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w *pomocy do STEP 7*.

System operacyjny resetuje instancje instrukcji „Count up" (Zliczanie w górę) podczas uruchamiania systemu bezpieczeństwa.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
CU	Wejście	BOOL	Wejście licznika
R	Wejście	BOOL	Wejście reset
PV	Wejście	INT	Wartość, dla której ustawiane jest wyjście Q
Q	Wyjście	BOOL	Status licznika
CV	Wyjście	INT	Bieżąca wartość licznika

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	x	x	

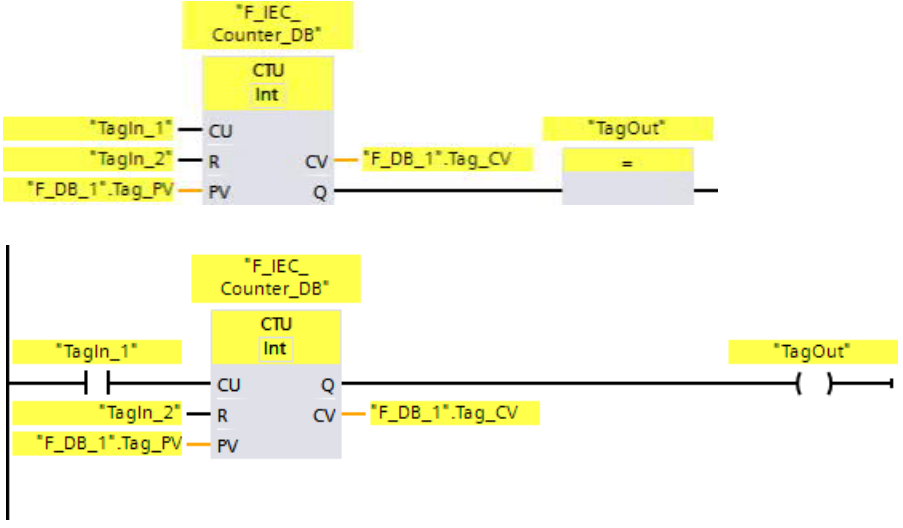
o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gdy stan sygnału na wejściu „CU" zmieni się z „0" na „1", wykonywana jest instrukcja „Count up" (Zliczanie w górę), a bieżący stan na wyjściu „CV" jest zwiększany o jeden. Wartość stanu jest zwiększana po każdym dodatkowym wykryciu narastającego zbocza sygnału aż do osiągnięcia górnego limitu rodzaju danych (32767).

Wartość parametru PV jest stosowana jako limit w celu określenia argumentu „TagOut" na wyjściu Q. Wyjście Q zwraca stan sygnału „1" tak długo, jak bieżąca wartość licznika jest większa lub równa wartości argumentu „PV". We wszystkich pozostałych przypadkach, wyjście „Q" ma stan sygnału „0".

13.5.2 CTD: Zliczanie w dół (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Count down" (Zliczanie w dół) można zwiększyć wartość na wyjściu CV. Gdy stan sygnału na wejściu CD zmieni się z „0" na „1" (dodatnie zbocze sygnału), wykonywana jest instrukcja, a bieżący stan na wyjściu CV jest zmniejszany o jeden. Wartość stanu jest zmniejszana po każdym wykryciu narastającego zbocza sygnału aż do osiągnięcia dolnego limitu określonego rodzaju danych. Po osiągnięciu dolnego limitu stan sygnału na wejściu CD nie wpływa na instrukcję.

Status licznika można sprawdzić za pomocą wyjścia Q. Gdy bieżąca wartość licznika jest mniejsza lub równa zeru, wyjście Q jest ustawiane na stan wartości „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu Q to „0".

Wartość na wyjściu CV jest ustawiana na wartość parametru „PV", gdy stan sygnału na wejściu LD zmieni się na „1". Dopóki utrzymuje się stan sygnału „1" na wejściu LD, stan sygnału na wejściu CD nie ma wpływu na instrukcję.

Każde wywołanie instrukcji „Count down" (Zliczanie w dół) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. F_IEC_Counter_DB_1) lub wiele instancji (np. F_IEC_Counter_Instance_1) dla instrukcji „Count down" (Zliczanie w dół). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w *pomocy do STEP 7*.

System operacyjny resetuje instancje instrukcji „Count down" (Zliczanie w dół) podczas uruchamiania systemu bezpieczeństwa.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
CD	Wejście	BOOL	Wejście licznika
LD	Wejście	BOOL	Wejście obciążenia
PV	Wejście	INT	Wartość na wyjściu CV, gdy ustawiane jest LD = 1
Q	Wyjście	BOOL	Status licznika
CV	Wyjście	INT	Bieżąca wartość licznika

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	x	x	

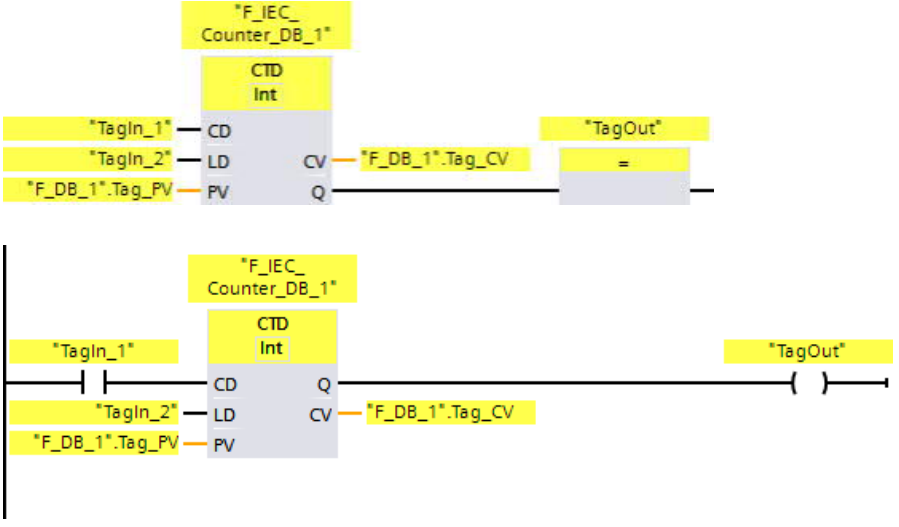
o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gdy stan sygnału na wejściu „CD" zmieni się z „0" na „1", wykonywana jest instrukcja „Count down" (Zliczanie w dół), a bieżący stan na wyjściu „CV" jest zmniejszany o jeden. Wartość stanu jest zmniejszana po każdym wykryciu narastającego zbocza sygnału aż do osiągnięcia dolnego limitu rodzaju danych (-32768).

Wyjście Q zwraca stan sygnału „1" tak długo, jak bieżąca wartość licznika jest mniejsza lub równa zeru. We wszystkich pozostałych przypadkach, wyjście „Q" ma stan sygnału „0".

13.5.3 CTUD: Zliczanie w górę i w dół (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Count up and down" (Zliczanie w górę i w dół) można zwiększyć wartość na wyjściu CV. Jeśli stan sygnału na wejściu CU zmieni się z „0" na „1" (dodatnie zbocze sygnału), bieżący stan na wyjściu CV jest zwiększany o jeden. Jeśli stan sygnału na wejściu CD zmieni się z „0" na „1" (dodatnie zbocze sygnału), bieżący stan na wyjściu CV jest zmniejszany o jeden. Jeśli na wejściach CU i CD obecny jest dodatni sygnał zbocza w jednym cyklu programu, bieżąca wartość licznika na wyjściu CV pozostaje niezmieniona.

Wartość stanu może być zwiększana aż do osiągnięcia górnego limitu rodzaju danych określonego na wyjściu CV. Po osiągnięciu górnego limitu wartość nie jest zwiększana przy dodatnim zboczu sygnału. Po osiągnięciu dolnego limitu określonego rodzaju danych, wartość zliczania nie jest dalej zmniejszana.

Gdy stan sygnału na wejściu LD zmieni się na „1", wartość zliczania na wyjściu CV jest ustawiana na wartość parametru PV. Dopóki utrzymuje się stan sygnału „1" na wejściu LD, stan sygnału na wejściach CU i CD nie ma wpływu na instrukcję.

Wartość licznika jest ustawiana na zero, gdy stan sygnału na wejściu R zmieni się na „1". Dopóki utrzymuje się stan sygnału „1" na wejściu R, stan sygnału na wejściach CU, CD i LD nie ma wpływu na instrukcję „Count up and down" (Zliczanie w górę i w dół).

Stan zliczania w górę można sprawdzić na wyjściu QU. Gdy bieżąca wartość licznika jest większa lub równa wartości parametru PV, wyjście QU zapewnia stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu QU to „0".

Stan zliczania w dół można sprawdzić na wyjściu QD. Gdy bieżąca wartość licznika jest mniejsza lub równa zeru, wyjście QD jest ustawiane na stan sygnału „1". We wszystkich pozostałych przypadkach, stan sygnał na wyjściu QD to „0".

Każde wywołanie instrukcji „Count up and down" (Zliczanie w górę i w dół) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. F_IEC_Counter_DB_1) lub wiele instancji (np. F_IEC_Counter_Instance_1) dla instrukcji „Count up and down" (Zliczanie w górę i w dół). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w *pomocy do STEP 7*.

System operacyjny resetuje instancje instrukcji „Count up and down" (Zliczanie w górę i w dół) podczas uruchamiania systemu bezpieczeństwa.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
CU	Wejście	BOOL	Wejście zliczania w górę
CD	Wejście	BOOL	Wejście zliczania w dół
R	Wejście	BOOL	Wejście reset
LD	Wejście	BOOL	Wejście obciążenia
PV	Wejście	INT	Wartość ustawiana na wyjściu QU/ na którym wyjście CV jest ustawiane na LD = 1.
QU	Wyjście	BOOL	Status licznika w górę
QD	Wyjście	BOOL	Status licznika w dół
CV	Wyjście	INT	Bieżąca wartość licznika

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	o	o	
1,3	x	x	x	

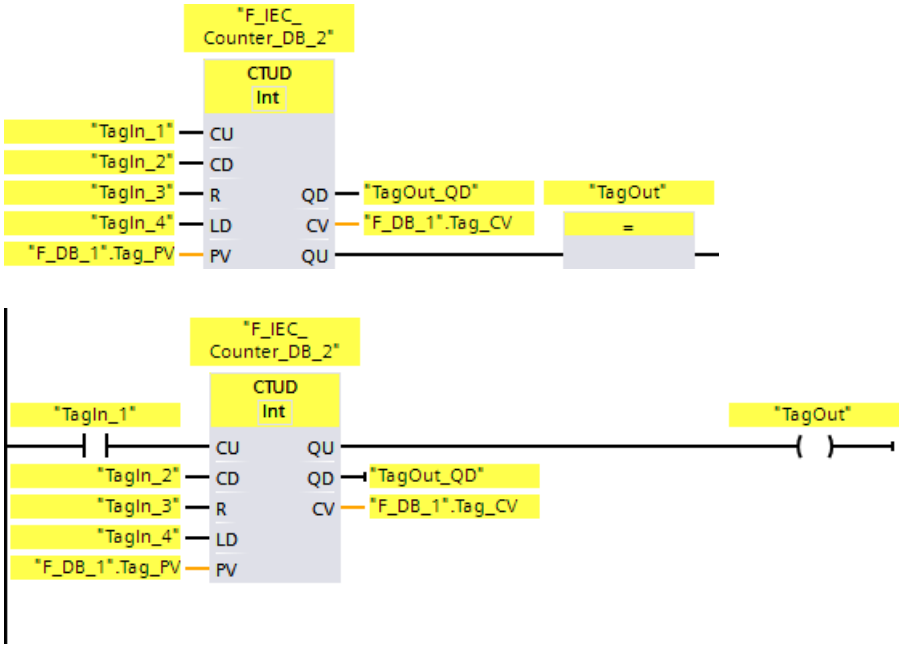
o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gdy stan sygnału na wejściu „CU" lub na wejściu „CD" zmieni się z „0" lub „1" (dodatnie zbocze sygnału), instrukcja „Count up and down" (Zliczanie w górę i w dół) jest wykonywana. Gdy na wejściu „CU" obecne jest dodatnie zbocze sygnału, bieżąca wartość zliczania wyjścia „CV" jest zwiększana o jeden. Gdy na wejściu „CD" obecne jest dodatnie zbocze sygnału, bieżąca wartość zliczania wyjścia „CV" jest zmniejszana o jeden. Wartość zliczania jest zwiększana przy każdym dodatnim zboczu sygnału na wejściu CU aż do osiągnięcia górnego limitu 32767. Wartość zliczania jest zmniejszana przy każdym dodatnim zboczu sygnału na wejściu CD aż do osiągnięcia dolnego limitu -32768.

Wyjście „QU" zwraca stan sygnału „1" tak długo, jak bieżąca wartość licznika jest większa lub równa wartości na wejściu „PV". We wszystkich pozostałych przypadkach, wyjście QU ma stan sygnału „0".

Wyjście „QU" zwraca stan sygnału „1" tak długo, jak bieżąca wartość licznika jest mniejsza lub równa zeru. We wszystkich pozostałych przypadkach, wyjście QD ma stan sygnału „0".

13.6 Operacje komparatora

13.6.1 CMP ==: Równe (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Equal" (Równe) można określić, czy pierwsza wartość porównywana (IN1 lub

<Argument1>) jest równa drugiej wartości porównywanej (IN2 lub <Argument2>).

Jeśli warunek porównania zostanie spełniony, instrukcja zwraca wynik (RLO) „1". Jeśli warunek porównania nie zostanie spełniony, instrukcja zwraca wynik RLO „0".

Dla LAD:

RLO instrukcji jest połączony z RLO całej bieżącej ścieżki w następujący sposób:

- Poprzez AND, gdy instrukcja porównania jest połączona szeregowo.
- Poprzez OR, gdy instrukcja porównania jest połączona równolegle.

Pierwszą wartość porównania (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Drugą wartość porównania (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Parametry

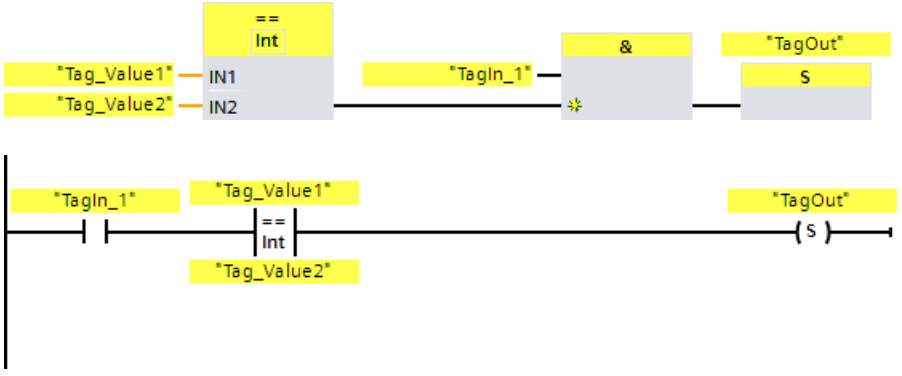
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
FBD: IN1 LAD: <Argument1>	Wejście	INT, DINT, TIME, WORD, (S7-300/400) DWORD	Pierwsza wartość do porównania
FBD: IN2 LAD: <Argument2>	Wejście	INT, DINT, TIME, WORD, (S7-300/400) DWORD	Druga wartość do porównania

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione

- „Tag_In1" ma stan sygnału „1".
- Warunek instrukcji porównania jest spełniony („Tag_Value1" = „Tag_Value2").

13.6.2 CMP <>: Nierówne (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Not equal" (Nierówne) można określić, czy pierwsza wartość porównywana (IN1 lub <Argument1>) nie jest równa drugiej wartości porównywanej (IN2 lub
<Argument2>).
Jeśli warunek porównania zostanie spełniony, instrukcja zwraca wynik (RLO) „1". Jeśli warunek porównania nie zostanie spełniony, instrukcja zwraca wynik RLO „0".

Dla LAD:

RLO instrukcji jest połączony z RLO całej bieżącej ścieżki w następujący sposób:

- Poprzez AND, gdy instrukcja porównania jest połączona szeregowo.
- Poprzez OR, gdy instrukcja porównania jest połączona równolegle.

Pierwszą wartość porównania (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Drugą wartość porównania (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Parametry

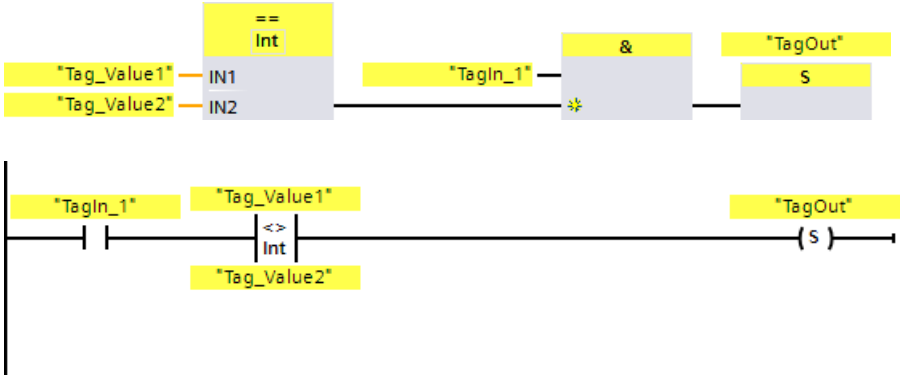
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
FBD: IN1 LAD: <Argument1>	Wejście	INT, DINT, TIME, WORD, (S7-300/400) DWORD	Pierwsza wartość do porównania
FBD: IN2 LAD: <Argument2>	Wejście	INT, DINT, TIME, WORD, (S7-300/400) DWORD	Druga wartość do porównania

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione

- „Tag_In1" ma stan sygnału „1".
- Warunek instrukcji porównania jest spełniony („Tag_Value1" <> „Tag_Value2").

13.6.3 CMP >=: Większe lub równe (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Greater or equal" (Większe lub równe) można określić, czy pierwsza wartość porównywana (IN1 lub <Argument1>) jest większa bądź równa drugiej wartości porównywanej (IN2 lub <Argument2>). Obie wartości do porównania muszą być tego samego rodzaju.

Jeśli warunek porównania zostanie spełniony, instrukcja zwraca wynik (RLO) „1". Jeśli warunek porównania nie zostanie spełniony, instrukcja zwraca wynik RLO „0".

Dla LAD:

RLO instrukcji jest połączony z RLO całej bieżącej ścieżki w następujący sposób:

- Poprzez AND, gdy instrukcja porównania jest połączona szeregowo.
- Poprzez OR, gdy instrukcja porównania jest połączona równolegle.

Pierwszą wartość porównania (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Drugą wartość porównania (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Parametry

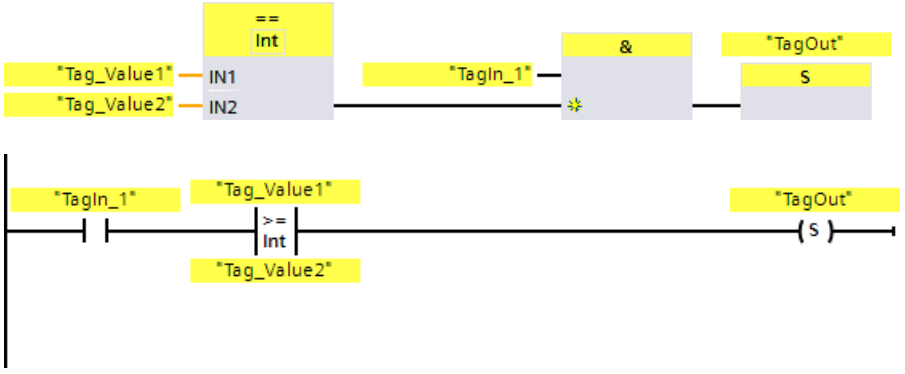
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
FBD: IN1 LAD: <Argument1>	Wejście	INT, DINT, TIME	Pierwsza wartość do porównania
FBD: IN2 LAD: <Argument2>	Wejście	INT, DINT, TIME	Druga wartość do porównania

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione

- „Tag_In1" ma stan sygnału „1".
- Warunek instrukcji porównania jest spełniony („Tag_Value1" >= „Tag_Value2").

13.6.4 CMP <=: Mniejsze lub równe (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Less or equal" (Mniejsze lub równe) można określić, czy pierwsza wartość porównywana (IN1 lub <Argument1>) jest mniejsza bądź równa drugiej wartości porównywanej (IN2 lub <Argument2>). Obie wartości do porównania muszą być tego samego rodzaju.

Jeśli warunek porównania zostanie spełniony, instrukcja zwraca wynik (RLO) „1". Jeśli warunek porównania nie zostanie spełniony, instrukcja zwraca wynik RLO „0".

Dla LAD:

RLO instrukcji jest połączony z RLO całej bieżącej ścieżki w następujący sposób:

- Poprzez AND, gdy instrukcja porównania jest połączona szeregowo.
- Poprzez OR, gdy instrukcja porównania jest połączona równolegle.

Pierwszą wartość porównania (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Drugą wartość porównania (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Parametry

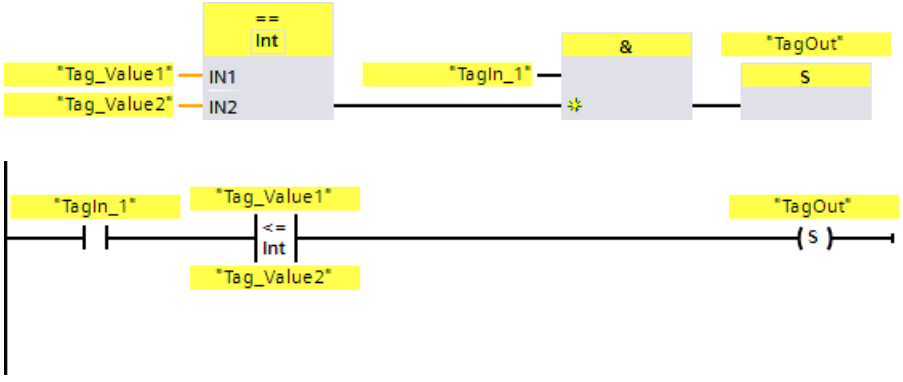
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
FBD: IN1 LAD: <Argument1>	Wejście	INT, DINT, TIME	Pierwsza wartość do porównania
FBD: IN2 LAD: <Argument2>	Wejście	INT, DINT, TIME	Druga wartość do porównania

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione

- „Tag_In1" ma stan sygnału „1".
- Warunek instrukcji porównania jest spełniony („Tag_Value1" <= „Tag_Value2").

13.6.5 CMP >: Większe niż (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Greater than" (Większe niż) można określić, czy pierwsza wartość porównywana (IN1 lub <Argument1>) jest większa od drugiej wartości porównywanej (IN2 lub <Argument2>). Obie wartości do porównania muszą być tego samego rodzaju.

Jeśli warunek porównania zostanie spełniony, instrukcja zwraca wynik (RLO) „1". Jeśli warunek porównania nie zostanie spełniony, instrukcja zwraca wynik RLO „0".

Dla LAD:

RLO instrukcji jest połączony z RLO całej bieżącej ścieżki w następujący sposób:

- Poprzez AND, gdy instrukcja porównania jest połączona szeregowo.
- Poprzez OR, gdy instrukcja porównania jest połączona równolegle.

Pierwszą wartość porównania (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Drugą wartość porównania (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Parametry

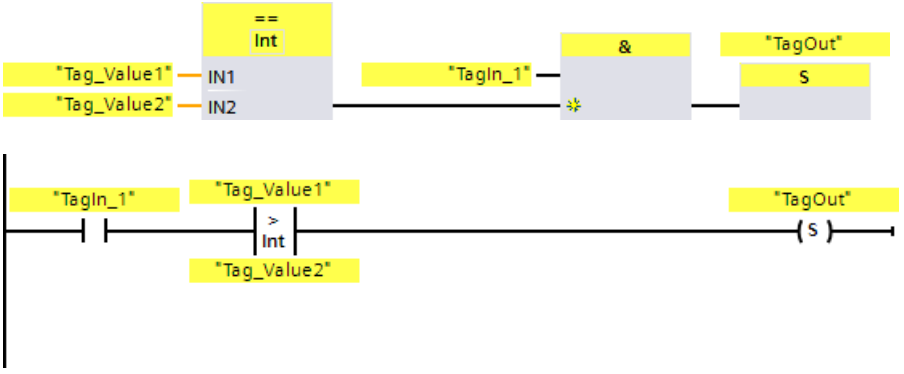
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
FBD: IN1 LAD: <Argument1>	Wejście	INT, DINT, TIME	Pierwsza wartość do porównania
FBD: IN2 LAD: <Argument2>	Wejście	INT, DINT, TIME	Druga wartość do porównania

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione

- „Tag_In1" ma stan sygnału „1".
- Warunek instrukcji porównania jest spełniony („Tag_Value1" > „Tag_Value2").

13.6.6 CMP <: Mniejsze niż (STEP 7 Safety

Opis

Za pomocą instrukcji „Less than" (Mniejsze niż) można określić, czy pierwsza wartość porównywana (IN1 lub <Argument1>) jest mniejsza od drugiej wartości porównywanej (IN2 lub <Argument2>). Obie wartości do porównania muszą być tego samego rodzaju.

Jeśli warunek porównania zostanie spełniony, instrukcja zwraca wynik (RLO) „1". Jeśli warunek porównania nie zostanie spełniony, instrukcja zwraca wynik RLO „0".

Dla LAD:

RLO instrukcji jest połączony z RLO całej bieżącej ścieżki w następujący sposób:

- Poprzez AND, gdy instrukcja porównania jest połączona szeregowo.
- Poprzez OR, gdy instrukcja porównania jest połączona równolegle.

Pierwszą wartość porównania (<Argument1>) należy wprowadzić w miejsce symbolu zastępczego argumentu powyżej instrukcji. Drugą wartość porównania (<Argument2>) należy wprowadzić w miejsce symbolu zastępczego argumentu poniżej instrukcji.

Parametry

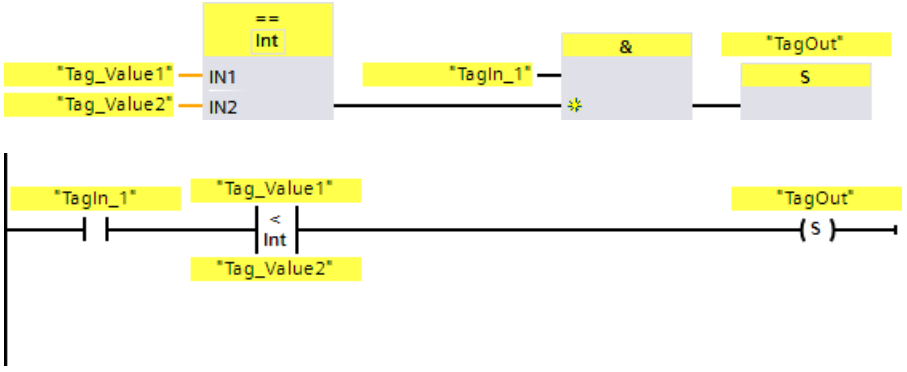
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
FBD: IN1 LAD: <Argument1>	Wejście	INT, DINT, TIME	Pierwsza wartość do porównania
FBD: IN2 LAD: <Argument2>	Wejście	INT, DINT, TIME	Druga wartość do porównania

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wyjście „TagOut" jest ustawiane, gdy zostaną spełnione

- „Tag_In1" ma stan sygnału „1".
- Warunek instrukcji porównania jest spełniony („Tag_Value1" < „Tag_Value2").

13.7 Funkcje matematyczne

13.7.1 ADD: Dodawanie (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Add" (Dodawanie) można dodać wartość na wejściu IN1 i wartość na wejściu IN2, po czym wyprowadzić wynik na wyjście OUT (OUT = IN1 + IN2).

Nie można połączyć włączonego wejścia „EN" lub (S7-300, S7-400) włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Uwaga

Gdy wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, F-CPU może przełączyć się w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Dlatego też należy przestrzegać dopuszczalnego zakresu dla rodzaju danych podczas tworzenia programu!

(S7-1200, S7-1500) Można uniknąć przejścia F-CPU w tryb STOP, podłączając włączone wyjście ENO, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Jeśli wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, włączone wejście ENO zwraca stan sygnału „0".
- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

(S7-300, S7-400) Można uniknąć przejścia F-CPU w tryb STOP, wstawiając instrukcję „Get status bit OV" do następnej sieci, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Sieć z instrukcją „Get status bit OV" nie możne zawierać żadnych etykiet skoku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Wydawane jest ostrzeżenie, jeśli nie wstawiono instrukcji „Get status bit OV".
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

Parametry

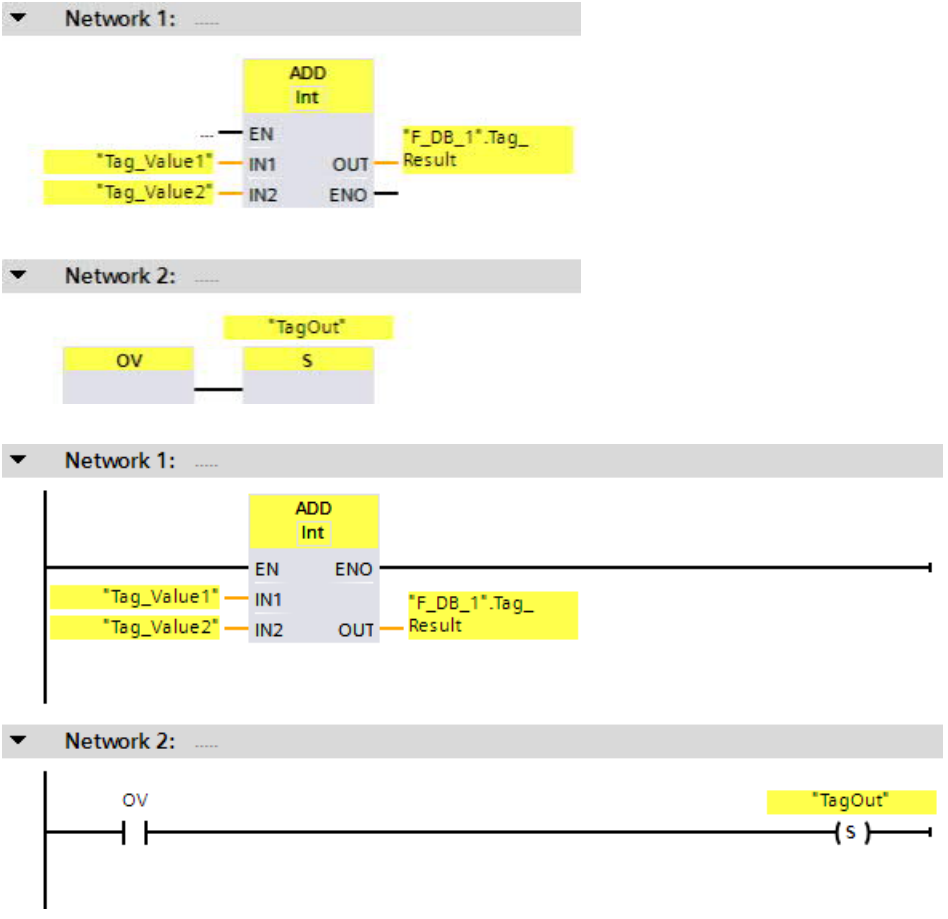
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ENO	Wyjście	BOOL	(S7-1200, S7-1500) Włączone wyjście
IN1	Wejście	INT, DINT	Pierwszy dodajnik
IN2	Wejście	INT, DINT	Drugi dodajnik
OUT	Wyjście	INT, DINT	Suma

Rodzaj danych instrukcji wybiera się z listy rozwijanej „<???>" w polu instrukcji.

Przykład dla F-CPU S7-300/400

Poniższy przykład pokazuje sposób działania instrukcji:



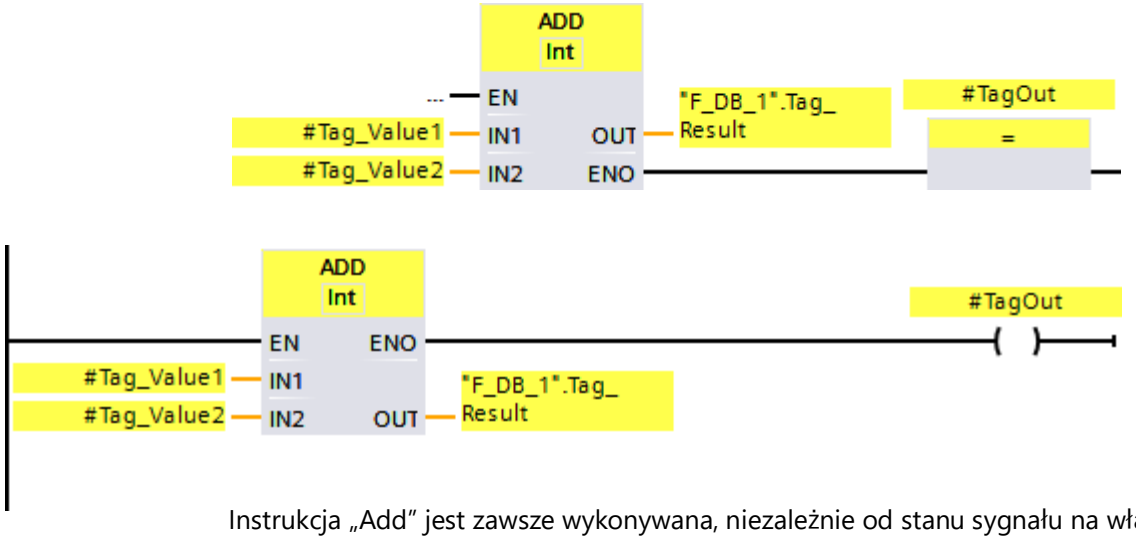
Instrukcja „Add" jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN. Wartość argumentu „Tag_Value1" jest dodawana do wartości argumentu „Tag_Value2". Wynik dodawania jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

W razie potrzeby można również zapisać stan sygnału włączonego wyjścia ENO w F-DB, po czym centralnie ocenić, czy wystąpiło przepełnienie dla wszystkich bądź jednej grupy instrukcji z detekcją przepełnienia.

W przypadku wykrycia przekroczenia wartości podczas wykonywania instrukcji „Add", bit stanu OV jest ustawiany na „1". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

Przykład dla F-CPU S7-1200/1500

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Add" jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „#Tag_Value1" jest dodawana do wartości argumentu „#Tag_Value2". Wynik dodawania jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

Jeśli podczas wykonywania instrukcji „Add" (Dodawanie) nie występuje przekroczenie wartości, włączone wyjście ENO ma stan sygnału „1" oraz ustawiany jest argument „#TagOut".

W razie potrzeby można również zapisać stan sygnału włączonego wyjścia ENO w (F-)DB, po czym centralnie ocenić, czy wystąpiło przepełnienie dla wszystkich bądź jednej grupy instrukcji z detekcją przepełnienia.

Zobacz także

---| |--- OV:Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 627)

---| / |--- OV:Pozyskiwanie zanegowanego bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 629)

13.7.2 SUB: Odejmowanie (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Substract" (Odejmowanie) można odjąć wartość na wejściu IN2 od wartości na wejściu IN1, po czym wyprowadzić wynik na wyjście OUT (OUT = IN1 - IN2).

Nie można połączyć włączonego wejścia „EN" lub (S7-300, S7-400) włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Uwaga

Gdy wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, F-CPU może przełączyć się w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Dlatego też należy przestrzegać dopuszczalnego zakresu dla rodzaju danych podczas tworzenia programu!

(S7-1200, S7-1500) Można uniknąć przejścia F-CPU w tryb STOP, podłączając włączone wyjście ENO, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Jeśli wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, włączone wejście ENO zwraca stan sygnału „0".
- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

(S7-300, S7-400) Można uniknąć przejścia F-CPU w tryb STOP, wstawiając instrukcję „Get status bit OV" do następnej sieci, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Sieć z instrukcją „Get status bit OV" nie możne zawierać żadnych etykiet skoku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Wydawane jest ostrzeżenie, jeśli nie wstawiono instrukcji „Get status bit OV".
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

Parametry

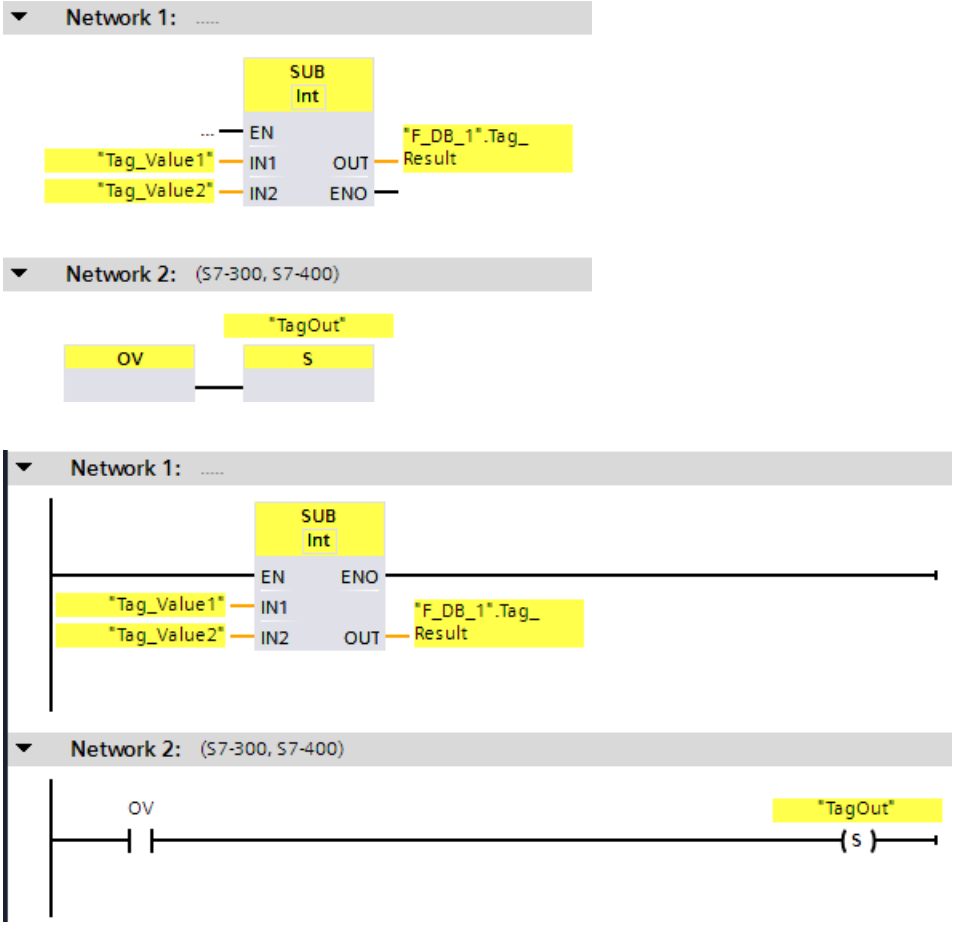
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ENO	Wyjście	BOOL	(S7-1200, S7-1500) Włączone wyjście
IN1	Wejście	INT, DINT	Odjemna
IN2	Wejście	INT, DINT	Odjemnik
OUT	Wyjście	INT, DINT	Różnica

Rodzaj danych instrukcji wybiera się z listy rozwijanej „<???>” w polu instrukcji.

Przykład dla F-CPU S7-300/400

Poniższy przykład pokazuje sposób działania instrukcji:



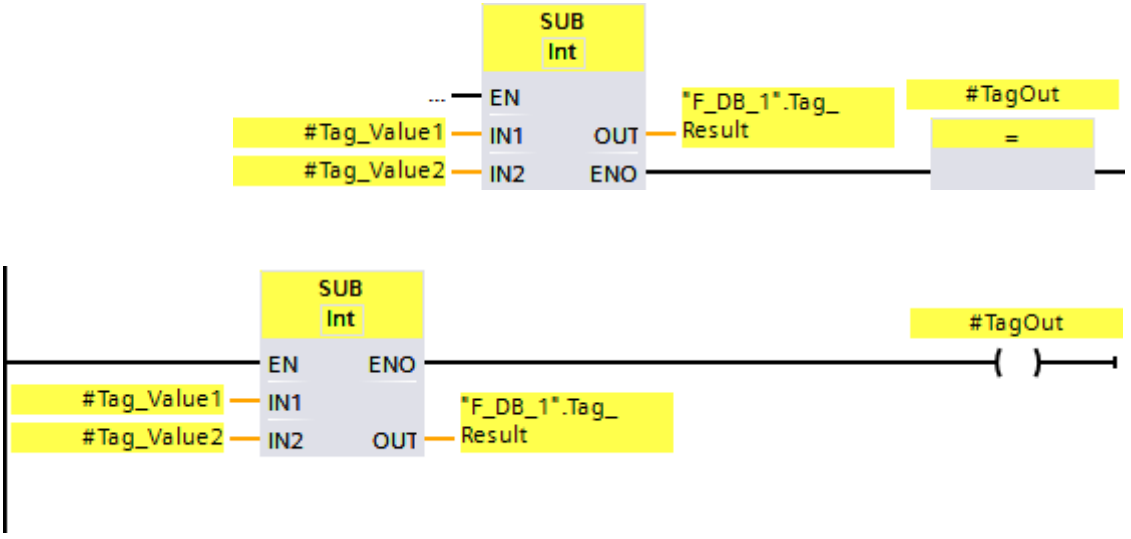
Instrukcja „Substract” jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „Tag_Value2" jest odejmowana od wartości argumentu „Tag_Value1". Wynik dodawania jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

W przypadku wykrycia przekroczenia wartości podczas wykonywania instrukcji „Substract" (Odejmowanie), bit stanu OV jest ustawiany na „1". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

Przykład dla F-CPU S7-1200/1500

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Substract" jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „#Tag_Value2" jest odejmowania od wartości argumentu „#Tag_Value1". Wynik dodawania jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

Jeśli podczas wykonywania instrukcji „Substract" (Odejmowanie) nie występuje przekroczenie wartości, włączone wyjście ENO ma stan sygnału „1" oraz ustawiany jest argument „#TagOut".

Zobacz także

---| |--- OV:Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 627)

---| / |--- OV:Pozyskiwanie zanegowanego bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 629)

13.7.3 MUL: Mnożenie (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Multiply" (Mnożenie) można pomnożyć wartość na wejściu IN1 przez wartość na wejściu IN2, po czym wyprowadzić wynik na wyjście OUT (OUT = IN1 × IN2).

Nie można połączyć włączonego wejścia „EN" lub (S7-300, S7-400) włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Uwaga

Gdy wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, F-CPU może przełączyć się w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Dlatego też należy przestrzegać dopuszczalnego zakresu dla rodzaju danych podczas tworzenia programu!

(S7-1200, S7-1500) Można uniknąć przejścia F-CPU w tryb STOP, podłączając włączone wyjście ENO, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Jeśli wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, włączone wejście ENO zwraca stan sygnału „0".
- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

(S7-300, S7-400) Można uniknąć przejścia F-CPU w tryb STOP, wstawiając instrukcję „Get status bit OV" do następnej sieci, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku. Sieć z
- instrukcją „Get status bit OV" nie możne zawierać żadnych etykiet skoku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi
- (http://support.automation.siemens.com/WW/view/en/49368678/133100)). Wydawane
- jest ostrzeżenie, jeśli nie wstawiono instrukcji „Get status bit OV".

  Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

Parametry

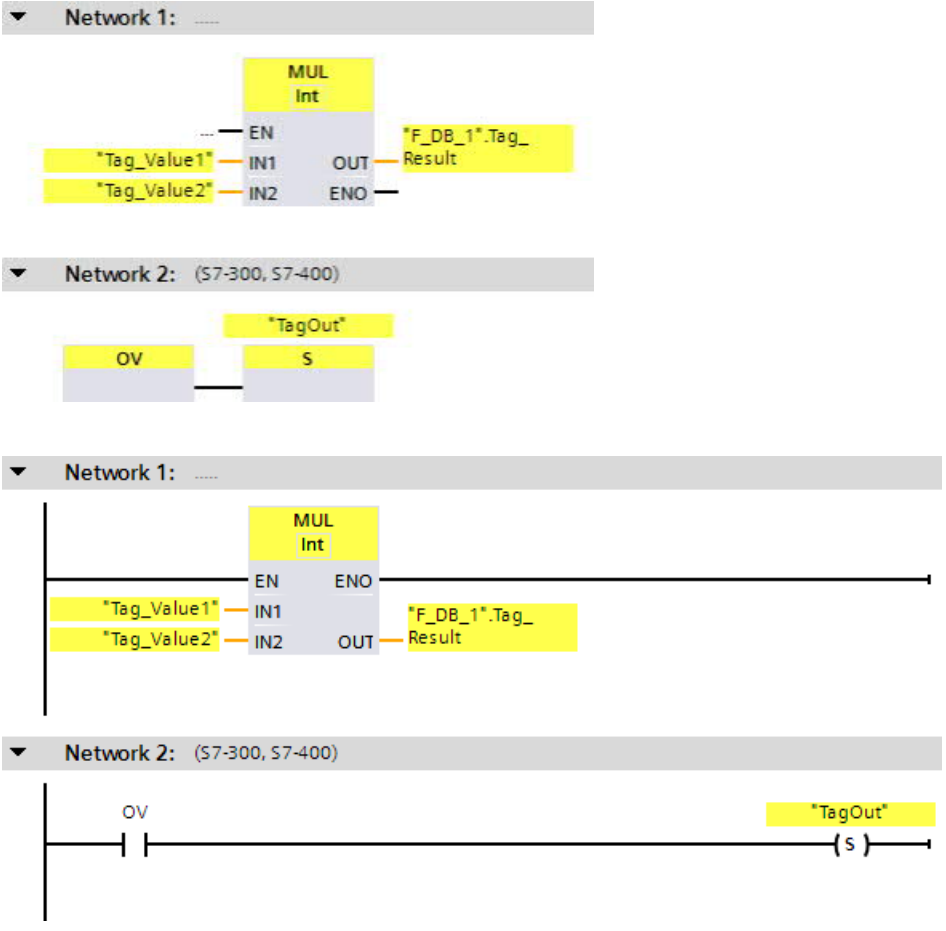
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ENO	Wyjście	BOOL	(S7-1200, S7-1500) Włączone wyjście
IN1	Wejście	INT, DINT	Mnożnik
IN2	Wejście	INT, DINT	Mnożna
OUT	Wyjście	INT, DINT	Produkt

Rodzaj danych instrukcji wybiera się z listy rozwijanej „<???>" w polu instrukcji.

Przykład dla F-CPU S7-300/400

Poniższy przykład pokazuje sposób działania instrukcji:



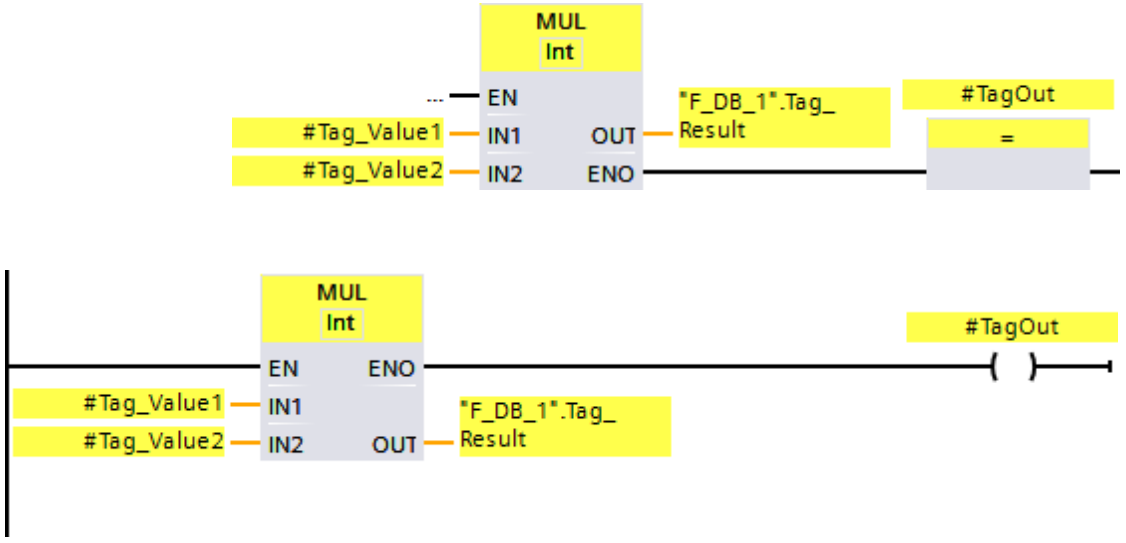
Instrukcja „Multiply" jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „Tag_Value1" jest mnożona przez wartość argumentu „Tag_Value2". Wynik mnożenia jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

W przypadku wykrycia przekroczenia wartości podczas wykonywania instrukcji „Multiply" (Mnożenie), bit stanu OV jest ustawiany na „1". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

Przykład dla F-CPU S7-1200/1500

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Multiply" jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „#Tag_Value1" jest mnożona przez wartość argumentu „#Tag_Value2". Wynik mnożenia jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

Jeśli podczas wykonywania instrukcji „Multiply" (Mnożenie) nie występuje przekroczenie wartości, włączone wyjście ENO ma stan sygnału „1" oraz ustawiany jest argument „#TagOut".

Zobacz także

---| |--- OV:Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 627)

---| / |--- OV:Pozyskiwanie zanegowanego bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 629)

13.7.4 DIV: Dzielenie (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Divide" (Dzielenie) można podzielić wartość na wejściu IN1 przez wartość na wejściu IN2, po czym wyprowadzić wynik na wyjście OUT (OUT = IN1 / IN2).

Nie można połączyć włączonego wejścia „EN" lub (S7-300, S7-400) włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Uwaga

Gdy wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, F-CPU może przełączyć się w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Dlatego też należy przestrzegać dopuszczalnego zakresu dla rodzaju danych podczas tworzenia programu!

(S7-1200, S7-1500) Można uniknąć przejścia F-CPU w tryb STOP, podłączając włączone wyjście ENO, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Jeśli wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, włączone wejście ENO zwraca stan sygnału „0".
- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

(S7-300, S7-400) Można uniknąć przejścia F-CPU w tryb STOP, wstawiając instrukcję „Get status bit OV" do następnej sieci, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Sieć z instrukcją „Get status bit OV" nie możne zawierać żadnych etykiet skoku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Wydawane jest ostrzeżenie, jeśli nie wstawiono instrukcji „Get status bit OV".
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

Uwaga

S7-300/400, S7-1200/1500 (włączone wyjście ENO podłączone):

Jeśli dzielnik (wejście IN2) instrukcji DIV = 0, iloraz (wynik dzielenia na wyjściu OUT) = 0. Wynik reaguje jak analogiczna instrukcja w standardowym bloku. F-CPU *nie* przechodzi w tryb STOP.

S7-1200/1500 (włączone wyjście ENO nie jest podłączone):

Jeśli dzielnik (wejście IN2) instrukcji DIV = 0, F-CPU przechodzi w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU. Zaleca się, by wykluczyć dzielnik (wejście IN2) = 0 podczas tworzenia programu.

Parametry

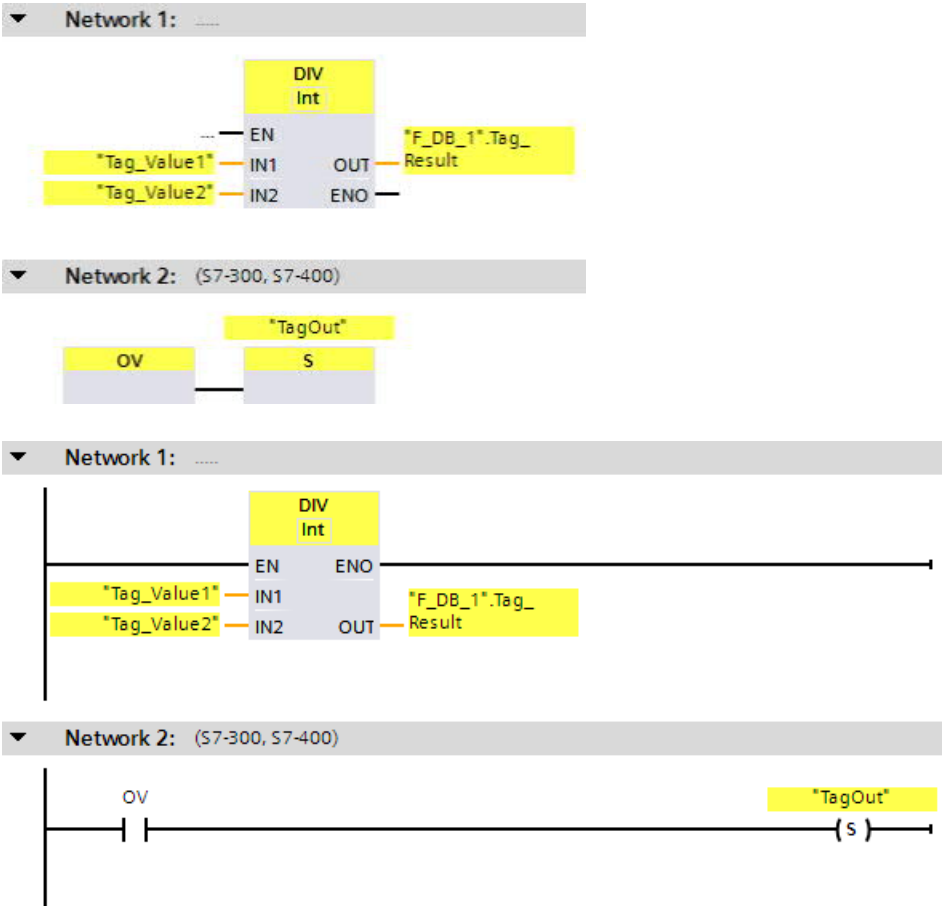
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ENO	Wyjście	BOOL	(S7-1200, S7-1500) Włączone wyjście
IN1	Wejście	INT, DINT	Dzielna
IN2	Wejście	INT, DINT	Dzielnik
OUT	Wyjście	INT, DINT	Iloraz

Rodzaj danych instrukcji wybiera się z listy rozwijanej „<???>” w polu instrukcji.

Przykład dla F-CPU S7-300/400

Poniższy przykład pokazuje sposób działania instrukcji:



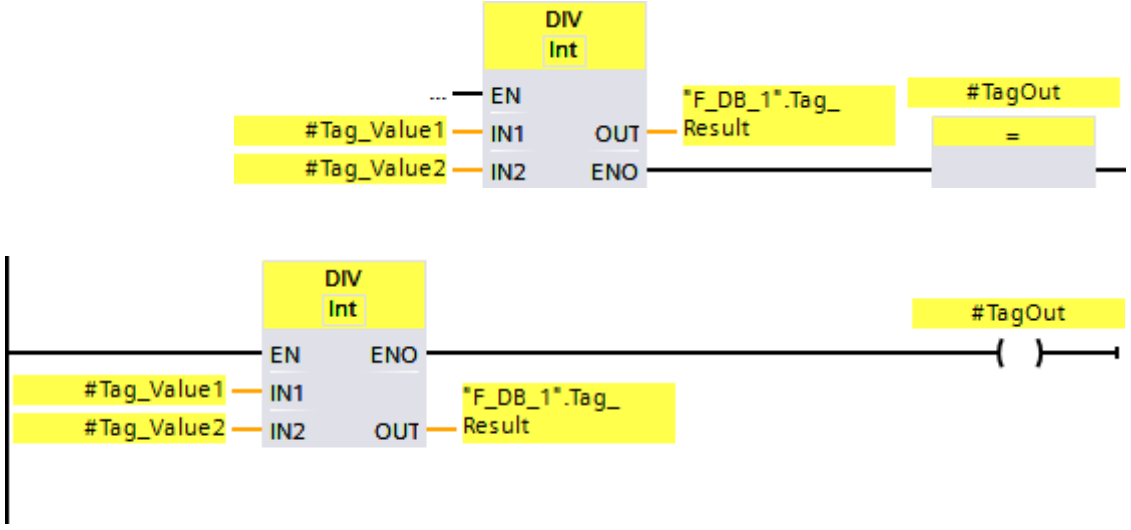
Instrukcja „Divide" jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „Tag_Value1" jest dzielona przez wartość argumentu „Tag_Value2". Wynik dzielenia jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

W przypadku wykrycia przekroczenia wartości podczas wykonywania instrukcji „Divide" (Dzielenie), bit stanu OV jest ustawiany na „1". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

Przykład dla F-CPU S7-1200/1500

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Divide" jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „#Tag_Value1" jest dzielona przez wartość argumentu „#Tag_Value2". Wynik dzielenia jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

Jeśli podczas wykonywania instrukcji „Divide" (Dzielenie) nie występuje przekroczenie wartości, włączone wyjście ENO ma stan sygnału „1" oraz ustawiany jest argument „#TagOut".

Zobacz także

---| |--- OV:Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 627)

---| / |--- OV:Pozyskiwanie zanegowanego bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 629)

13.7.5 NEG: Tworzenie uzupełnienia dwójkowego(STEP 7 Safety V16)

Opis

Instrukcja „Create twos complement" (Tworzenie uzupełnienia dwójkowego) pozwala na zmianę znaku wartości na wejściu IN i sprawdzenie wyniku na wyjściu OUT. W przypadku, przykładowo, dodatniej wartości na wejściu IN, ujemny odpowiednik tej wartości jest wysyłany na wyjście OUT.

Nie można połączyć włączonego wejścia „EN" lub (S7-300, S7-400) włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Uwaga

Gdy wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, F-CPU może przełączyć się w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Dlatego też należy przestrzegać dopuszczalnego zakresu dla rodzaju danych podczas tworzenia programu!

(S7-1200, S7-1500) Można uniknąć przejścia F-CPU w tryb STOP, podłączając włączone wyjście ENO, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Jeśli wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, włączone wejście ENO zwraca stan sygnału „0".
- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

(S7-300, S7-400) Można uniknąć przejścia F-CPU w tryb STOP, wstawiając instrukcję „Get status bit OV" do następnej sieci, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Sieć z instrukcją „Get status bit OV" nie możne zawierać żadnych etykiet skoku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Wydawane jest ostrzeżenie, jeśli nie wstawiono instrukcji „Get status bit OV".
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

Parametry

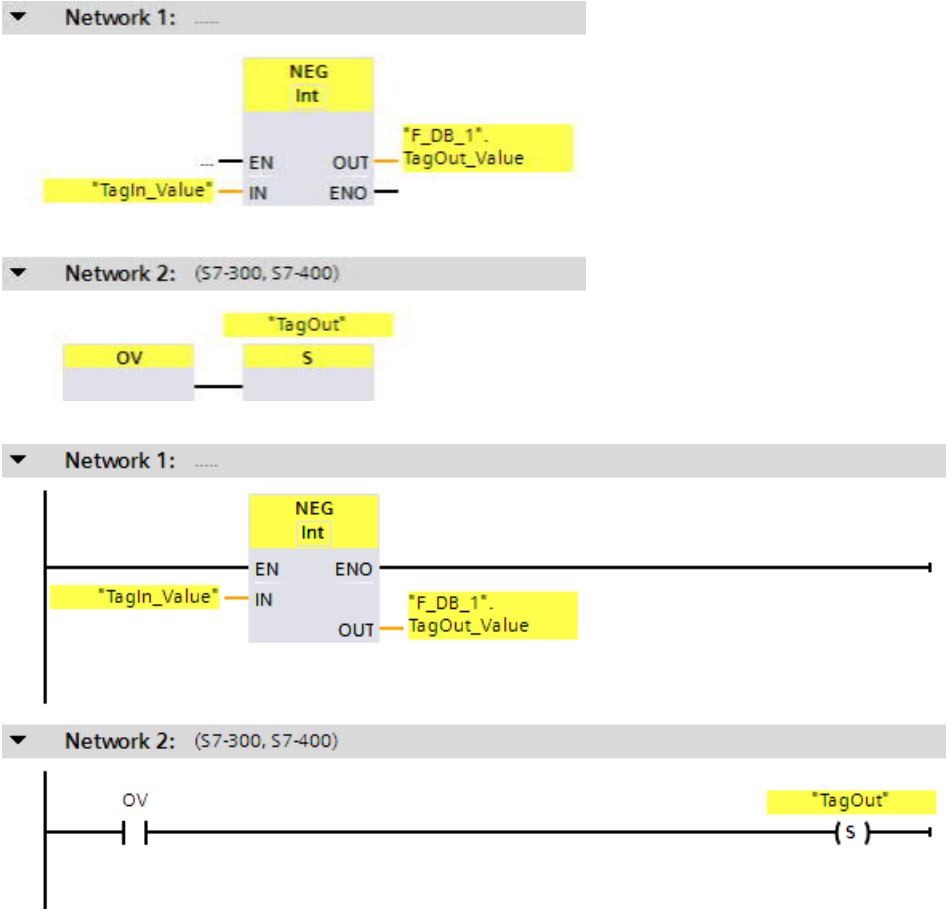
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ENO	Wyjście	BOOL	(S7-1200, S7-1500) Włączone wyjście
IN	Wejście	INT, DINT	Wartość wejściowa
OUT	Wyjście	INT, DINT	Uzupełnienie dwójkowe wartości wejściowej

Rodzaj danych instrukcji wybiera się z listy rozwijanej „<???>" w polu instrukcji.

Przykład dla F-CPU S7-300/400

Poniższy przykład pokazuje sposób działania instrukcji:



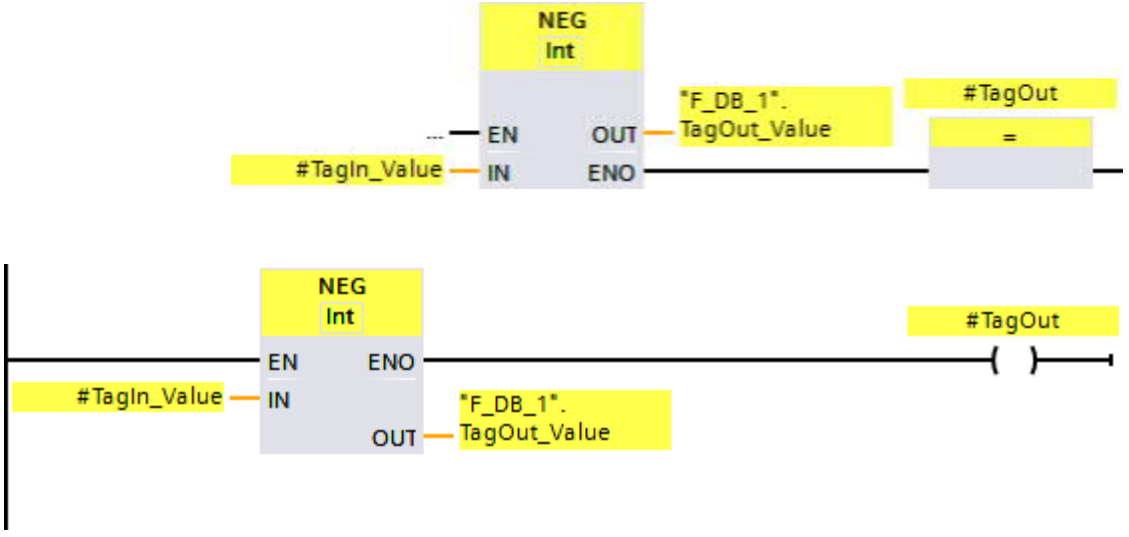
Instrukcja „Create two's complement" (Tworzenie uzupełnienia dwójkowego) jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Znak argumentu „TagIn_Value" jest zmieniany, a wynik jest zapisywany w argumentzie „"F_DB_1".TagOut_Value".

W przypadku wykrycia przekroczenia wartości podczas wykonywania instrukcji „Create two's complement" (Tworzenie uzupełnienia dwójkowego), bit stanu OV jest ustawiany na „1". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

Przykład dla F-CPU S7-1200/1500

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Create two's complement" (Tworzenie uzupełnienia dwójkowego) jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Znak argumentu „#TagIn_Value" jest zmieniany, a wynik jest zapisywany w argumentzie „"F_DB_1".TagOut_Value".

Jeśli podczas wykonywania instrukcji „Create two's complement" (Tworzenie uzupełnienia dwójkowego) nie występuje przekroczenie wartości, włączone wyjście ENO ma stan sygnału
„1" oraz ustawiany jest argument „TagOut".

Zobacz także

---| |--- OV:Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 627)

---| / |--- OV:Pozyskiwanie zanegowanego bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400) (strona 629)

13.7.6 ABS: Tworzenie wartości bezwzględnej (STEP 7 Safety V16) (S7-1200, S7-1500)

Opis

Za pomocą instrukcji „Form absolute value" (Tworzenie wartości bezwzględnej) można obliczyć wielkość bezwzględną wartości określonej na wejściu „IN". Wynik instrukcji jest wyprowadzany na wyjście OUT, skąd można go pozyskać.

Nie można połączyć włączonego wejścia „EN" lub (S7-300, S7-400) włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Uwaga

Gdy wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, F-CPU może przełączyć się w tryb STOP. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Dlatego też należy przestrzegać dopuszczalnego zakresu dla rodzaju danych podczas tworzenia programu!

Można uniknąć przejścia F-CPU w tryb STOP, podłączając włączone wyjście ENO, programując tym detekcję nadmiernego przepływu.

Należy mieć na uwadze następuje zagadnienia:

- Jeśli wynik instrukcji plasuje się poza dopuszczalnym zakresem dla tego rodzaju danych, włączone wejście ENO zwraca stan sygnału „0".
- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.
- Czas wykonania instrukcji jest wydłużany (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).
- Pamięć robocza wymagana dla programu bezpieczeństwa jest zwiększana.

Parametry

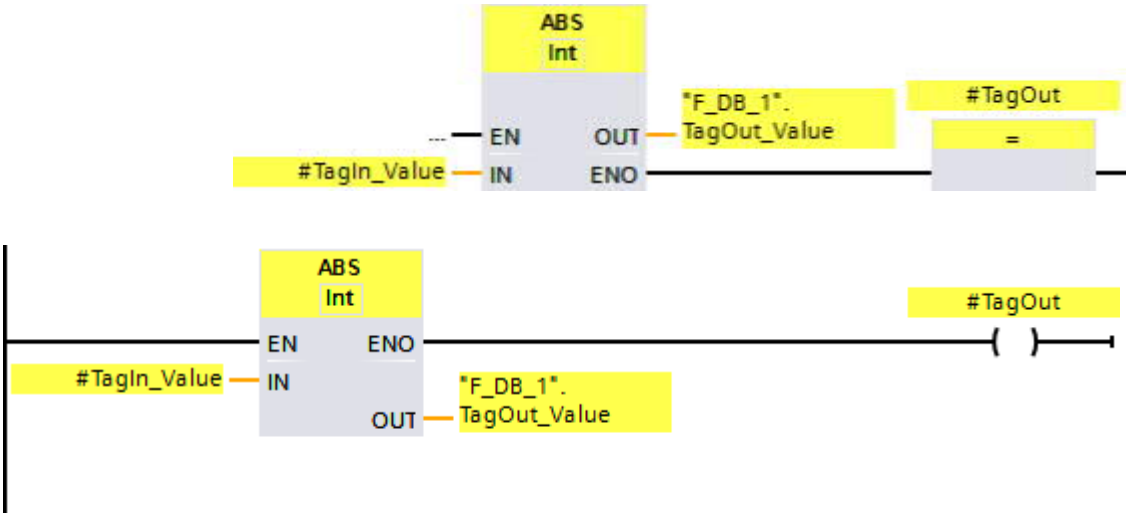
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ENO	Wyjście	BOOL	(S7-1200, S7-1500) Włączone wyjście
IN	Wejście	INT, DINT	Wartość wejściowa
OUT	Wyjście	INT, DINT	Wartość bezwzględna wartości wejściowej

Rodzaj danych instrukcji wybiera się z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Form absolute value" (Tworzenie wartości bezwzględnej) jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Wartość bezwzględna wartości na argumentzie „TagIn_Value" jest obliczana, a wynik jest zapisywany w argumentzie „"F_DB_1".TagOut_Value".

Jeśli podczas wykonywania instrukcji „Form absolute value" (Tworzenie wartości bezwzględnej) nie występuje przekroczenie wartości, włączone wyjście ENO ma stan sygnału „1" oraz ustawiany jest argument „#TagOut".

13.8 Operacje przenoszenia

13.8.1 MOVE: Przenoszenie wartości (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „Move value" (Przenoszenie wartości) można przenieść zawartość argumentu na wejściu IN do argumentu na wyjściu OUT1.

Na wejściu IN oraz wyjściu OUT1 można określić jedynie argumenty o identycznej szerokości oraz identycznej strukturze danych.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

(S7-1200, S7-1500) W stanie podstawowym pole instrukcji zawiera wyjście (OUT1). Możliwe jest rozszerzenie liczby wyjść. Wstawione wyjścia są numerowane w kolejności rosnącej. Podczas wykonywania, zawartość argumentu na wejściu IN jest przenoszona do dostępnych wyjść. Pole instrukcji nie może zostać rozszerzone, jeśli przenoszone są argumenty z rodzajem danych PLC zgodnych z bezpieczeństwem (UDT).

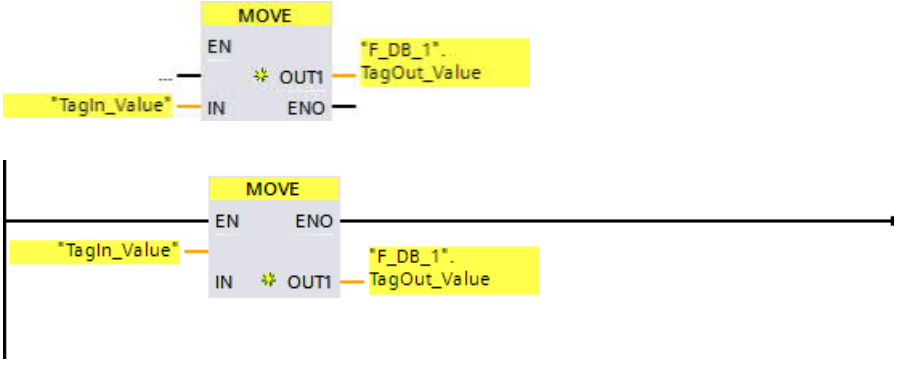
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	INT, DINT, WORD, (S7-300/400) DWORD, TIME, rodzaj danych PLC zgodnych z bezpieczeństwem (UDT)	Wartość źródłowa
OUT1	Wyjście	INT, DINT, WORD, (S7-300/400) DWORD, TIME, rodzaj danych PLC zgodnych z bezpieczeństwem (UDT)	Adres docelowy

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN". Instrukcja kopiuje treść argumentu „TagIn_Value" do argumentu „"F_DB_1".TagOut_Value".

13.8.2 RD_ARRAY_I: Odczytaj z INT F-array (STEP 7 Safety V16) (S7-1500)

Opis

Instrukcja „Read value from INT F-array" (Odczytaj z INT F-array) służy do odczytu elementu z tablicy na wejściu ARRAY, który odnosi się do indeksu na wejściu INDEX, po czym zapisuje swoją wartość na wyjściu OUT. Jeśli podczas uzyskiwania dostępu do tablicy wystąpi błąd, jest on wyświetlany na wyjściu ERROR.

Tablica musi być utworzona w globalnym DB bezpieczeństwa i może zawierać tylko jeden wymiar. Elementy ARRAY muszą być danymi rodzaju INT. Poniższe zasady dotyczą limitów tablicy:

- Dolny limit musi wynosić 0.
- Górny limit to maksymalnie 10000.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	
ARRAY	Wejście	VARIANT	Tablica, z której jest odczytywany
INDEX	Wejście	DINT	Element odczytywany w tablicy. Specyfikacja: stała lub tag.
OUT	Wyjście	INT	Wartość odczytywana i wyprowadzana.
ERROR	Wyjście	BOOL	Informacja błędu Parametr ERROR jest ustawiany, gdy wystąpi błąd podczas przetwarzania instrukcji.

Parametr ARRAY

Oprócz bezpośredniego połączenia z tablicą w globalnym DB fail-safe, to wejście może zostać również połączone z INOUT rodzaju danych ARRAY[*] INT. Umożliwia to rozprzęgnięcie danych i logiki programu w celu, przykładowo, utworzenia funkcji biblioteki bez istniejących połączeń dla dedykowanego bloku danych.

Parametr ERROR

Poniższa tabela przedstawia znaczenie wartości parametru ERROR:

Wartość	Opis
FALSE	Brak błędu
TRUE	Wartość na parametrze INDEX wykracza poza wartość graniczną ARRAY.

Wersje instrukcji

Dla tej instrukcji dostępna jest jedna wersja:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	—	—	x[1]	

[1] obsługiwana od wersji oprogramowania V2.0

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

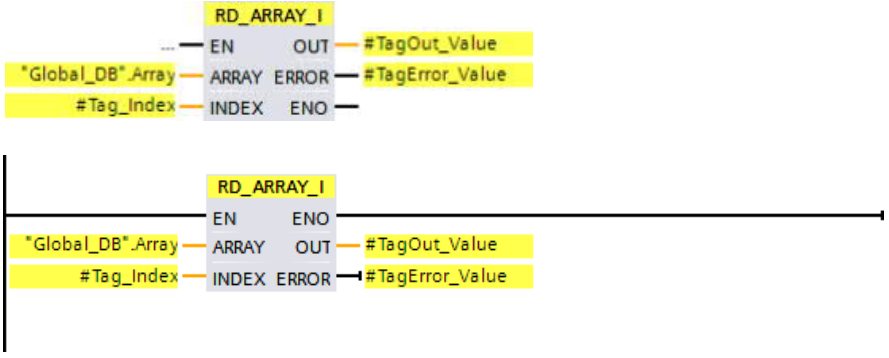
Reakcja na błędy

Jeśli wartość na wejściu INDEX wykracza poza limity tablicy, ustawiane jest wyjście ERROR = 1, a wartość tablicy elementu z indeksem = 0 jest wyprowadzana na wyjście OUT, niezależnie od wartości przekazywanej na wejście INDEX.

Dlatego też należy ustawić wartość elementu z indeksem = 0 jako wartość zastępcza fail-safe.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Poniższa tabela pokazuje, jak działa instrukcja, korzystając z określonych wartości argumentów:

Parametr	Argument	Wartość
ARRAY	"Global_DB".Array	Argument "Global_DB".Array to ARRAY rodzaju danych Array[0..10] INT
INDEX	#Tag_Index	2
OUT	#TagOut_Value	Wartość elementu w położeniu tablicy [2]
ERROR	#TagError_Value	Fałsz

Instrukcja „Read value from INT F-array" (Odczytajz INT F-array) jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Zawartość 2. elementu argumentu „Global_DB.Array" jest wyprowadzana na wyjście „#TagOut_Value".

13.8.3 RD_ARRAY_DI: Odczytaj z DINT F-array (STEP 7 Safety V16) (S7-1500)

Opis

Instrukcja „Read value from DINT F-array" (Odczytajz INT F-array) służy do odczytu elementu z tablicy na wejściu ARRAY, który odnosi się do indeksu na wejściu INDEX, po czym zapisuje swoją wartość na wyjściu OUT. Jeśli podczas uzyskiwania dostępu do tablicy wystąpi błąd, jest on wyświetlany na wyjściu ERROR.

Tablica musi być utworzona w globalnym DB bezpieczeństwa i może zawierać tylko jeden wymiar. Elementy tablicy muszą być danymi rodzaju DINT. Poniższe zasady dotyczą limitów tablicy:

- Dolny limit musi wynosić 0.
- Górny limit to maksymalnie 10000.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ARRAY	Wejście	VARIANT	Tablica, z której jest odczytywany
INDEX	Wejście	DINT	Element odczytywany w tablicy. Specyfikacja: stała lub znacznik.
OUT	Wyjście	DINT	Wartość odczyt. i wyprowadzana.
ERROR	Wyjście	BOOL	Informacja błędu Parametr ERROR jest ustawiany, gdy wystąpi błąd podczas przetwarzania instrukcji

Parametr ARRAY

Oprócz bezpośredniego połączenia z tablicą w globalnym DB fail-safe, to wejście może zostać również połączone z INOUT rodzaju danych ARRAY[*] DINT. Umożliwia to rozprzęgnięcie danych i logiki programu w celu, przykładowo, utworzenia funkcji biblioteki bez istniejących połączeń dla dedykowanego bloku danych.

Parametr ERROR

Poniższa tabela przedstawia znaczenie wartości parametru ERROR:

Wartość	Opis
FALSE	Brak błędu
TRUE	Wartość na parametrze INDEX wykracza poza wartość graniczną ARRAY.

Wersje instrukcji

Dla tej instrukcji dostępna jest jedna

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	—	—	x[1]	

[1] obsługiwana od wersji oprogramowania V2.0

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępnawersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

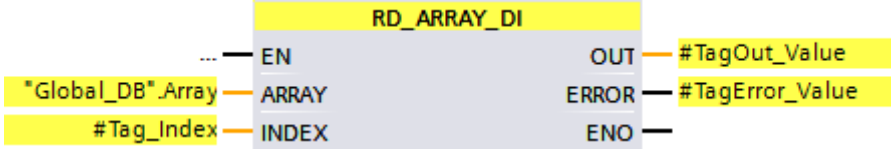
Reakcja na błędy

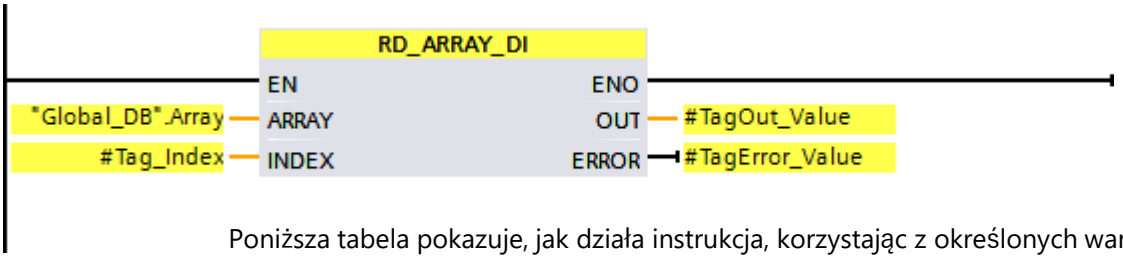
Jeśli wartość na wejściu INDEX wykracza poza limity tablicy, ustawiane jest wyjście ERROR = 1, a wartość tablicy elementu z indeksem = 0 jest wyprowadzana na wyjście OUT, niezależnie od wartości przekazywanej na wejście INDEX.

Dlatego też należy ustawić wartość elementu z indeksem = 0 jako wartość zastępcza fail-

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:





Poniższa tabela pokazuje, jak działa instrukcja, korzystając z określonych wartości argumentów:

Parametr	Argument	Wartość
ARRAY	"Global_DB".Array	Argument "Global_DB".Array to ARRAY rodzaju danych Array[0..10] DINT
INDEX	#Tag_Index	2
OUT	#TagOut_Value	Wartość elementu w położeniu tablicy [2]
ERROR	#TagError_Value	FALSE

Instrukcja „Read value from DINT F-array" (Odczytajz INT F-array) jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN".

Zawartość 2. elementu argumentu „Global_DB.Array" jest wyprowadzana na wyjście „#TagOut_Value".

13.8.4 WR_FDB: Zapis wartości pośrednio do F-DB (STEP 7 Safety V16) (S7-300, S7-400)

Opis

Instrukcja zapisuje wartość określoną na wejściu IN do taga adresowanego przez INI_ADDR oraz OFFSET w F-DB.

Adres tagów adresowanych przy użyciu INI_ADDR oraz OFFSET musi znajdować się w zakresie adresowym zdefiniowanym przez adresy INI_ADDR oraz END_ADDR.

Jeśli F-CPU przeszedł w tryb STOP ze zdarzeniem diagnostycznym ID 75E2, należy sprawdzić, czy ten warunek został spełniony.

Adres początkowy obszaru w F-DB, do którego zapisywana jest wartość z wejścia IN, jest przenoszony przy użyciu wejścia INI_ADDR. Powiązana korekcja w tym obszarze jest przenoszona przy użyciu wejścia OFFSET.

Adres przenoszony w wejściu INI_ADDR lub END_ADDR musi wskazywać na tag wybranego rodzaju danych w F-DB. Jedynie tagi wybranego rodzaju danych są dozwolone pomiędzy adresami INI_ADDR i END_ADDR. Adres INI_ADDR musi być mniejszy niż adres END_ADDR.

Jak przedstawiono w poniższym przykładzie, adresy INI_ADDR oraz END_ADDR muszą być przenoszone z pełną kwalifikacją jako "DBx".DBWy lub w odnośnej reprezentacji symbolicznej. Przenoszenia w innej formie nie są dozwolone.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	INT, DINT	Wartość do zapisu do F-DB
INI_ADDR	Wejście	POINTER	Adres początkowy obszaru w F-DB
END_ADDR	Wejście	POINTER	Adres końcowy obszaru w F-DB
OFFSET	Wejście	INT	Korekcja

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykłady przypisania parametrów INI_ADDR, END_ADDR oraz OFFS

Nazwa	Rodzaj	Wartość	Komentarz
Statyczny			
VAR_BOOL10	BOOL	fałsz	
VAR_BOOL11	BOOL	fałsz	
VAR_BOOL12	BOOL	fałsz	
VAR_BOOL13	BOOL	fałsz	
VAR_TIME10	TIME	T#0MS	
VAR_TIME11	TIME	T#0MS	
VAR_INT10	INT	0	<- INI ADDR = "F-DB 1".VAR INT10 Przykład 1
VAR_INT11	INT	0	
VAR_INT12	INT	0	
VAR_INT13	INT	0	<- OFFSET = 3
VAR_INT14	INT	0	
VAR_INT15	INT	0	<- END ADDR = "F-DB 1".VAR INT15
VAR_BOOL20	BOOL	fałsz	
VAR_BOOL21	BOOL	fałsz	
VAR_BOOL22	BOOL	fałsz	
VAR_BOOL23	BOOL	fałsz	
VAR_INT20	INT	0	<- INI ADDR = "F-DB 1".VAR INT20 Przykład 2
VAR_INT21	INT	0	
VAR_INT22	INT	0	
VAR_INT23	INT	0	<- END ADDR = "F-DB 1".VAR INT23
VAR_INT30	INT	0	<- INI ADDR = "F-DB 1".VAR INT30 Przykład 3
VAR_INT31	INT	0	<- OFFSET = 1
VAR_INT32	INT	0	
VAR_INT33	INT	0	
VAR_INT34	INT	0	<- END ADDR = "F-DB".VAR INT34
VAR_TIME20	TIME	T#0MS	
VAR_DINT10	DINT	0	<- INI ADDR = "F-DB 1".VAR DINT10 Przykład 4
VAR_DINT11	DINT	0	
VAR_DINT12	DINT	0	<- OFFSET = 2
VAR_DINT13	DINT	0	<- END ADDR = "F-DB 1".VAR DINT13

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:

13.8.5 RD_FDB: Odczyt wartości pośrednio z F-DB (STEP 7 Safety V16) (S7-300, S7-400)

Opis

Ta instrukcja odczytuje tag zaadresowany poprzez INI_ADDR oraz OFFSET w F-DB i przekazuje je na wyjście OUT.

Adres tagów adresowanych przy użyciu INI_ADDR oraz OFFSET musi znajdować się w zakresie adresowym zdefiniowanym przez adresy INI_ADDR oraz END_ADDR.

Jeśli F-CPU przeszedł w tryb STOP ze zdarzeniem diagnostycznym ID 75E2, należy sprawdzić, czy ten warunek został spełniony.

Adres początkowy obszaru w F-DB, z którego odczytywany jest tag, jest przenoszony przy użyciu wejścia INI_ADDR. Powiązana korekcja w tym obszarze jest przenoszona przy użyciu wejścia OFFSET.

Adres przenoszony w wejściu INI_ADDR lub END_ADDR musi wskazywać na tag wybranego rodzaju danych w F-DB. Jedynie tagi wybranego rodzaju danych są dozwolone pomiędzy adresami INI_ADDR i END_ADDR. Adres INI_ADDR musi być mniejszy niż adres END_ADDR.

Adresy INI_ADDR oraz END_ADRR muszą być przenoszone z pełną kwalifikacją jako "DBx".DBWy lub w odnośnej reprezentacji symbolicznej. Przenoszenia w innej formie nie są dozwolone. Przykłady przypisania parametrów INI_ADDR, END_ADDR oraz OFFSET są zawarte w WR_FDB:Zapis wartości pośrednio do F-DB (STEP 7 Safety V16) (S7-300, S7-400) (strona 579).

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametry

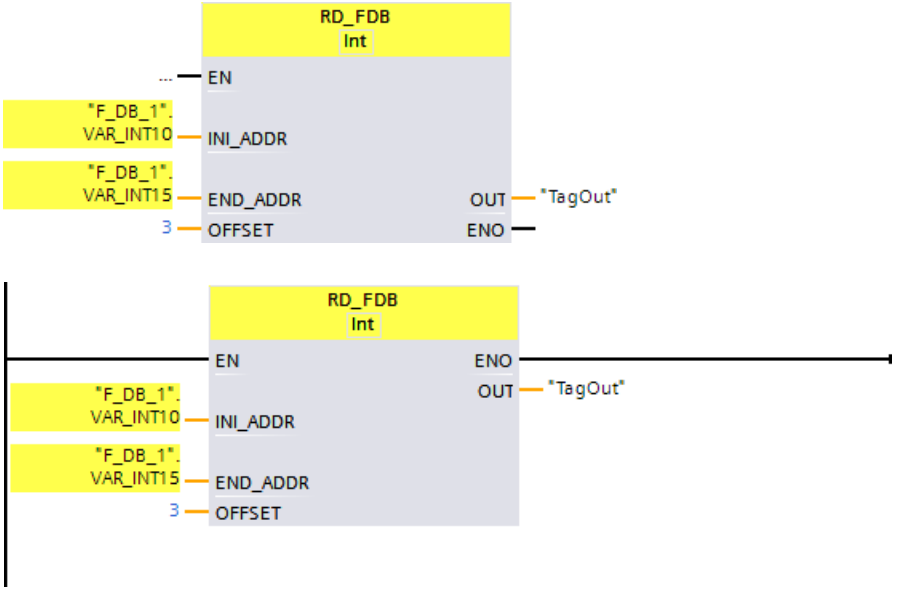
W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
INI_ADDR	Wejście	POINTER	Adres początkowy obszaru w F-DB
END_ADDR	Wejście	POINTER	Adres końcowy obszaru w F-DB
OFFSET	Wejście	INT	Korekcja
OUT	Wyjście	INT, DINT	Wartość do odczytu z F-DB

Rodzaj danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



13.9 Operacje konwertowania

13.9.1 CONVERT: Konwertowanie wartości (STEP 7 Safety V16)

Opis

Instrukcja „Convert value" (Konwertowanie wartości) odczytuje zawartość parametru IN i przekształca ją zgodnie rodzajem danych wybranym w polu instrukcji. Przekształcona wartość jest wyprowadzana na wyjście OUT.

Podłączenie włączonego wejścia „EN" nie jest możliwe. Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN"). Podłączenie włączonego wyjścia „ENO" jest możliwe i wymagane tylko podczas konwertowania z rodzaju danych „DINT" na „INT".

Uwaga

Podczas konwertowania z „DINT" na „INT", konieczne jest podłączenie włączonego wyjścia ENO i wobec tego zaprogramowanie detekcji przekroczenia wartości.

Należy mieć na uwadze następuje zagadnienia:

- Jeśli wartość na wejściu wykracza poza zakres INT, ENO zwraca 0.
- Wynik instrukcji reaguje jak analogiczna instrukcja w standardowym bloku.

Parametry

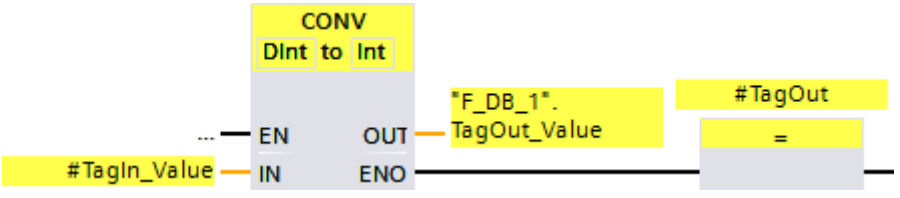
W poniższej tabeli znajdują się parametry instrukcji:

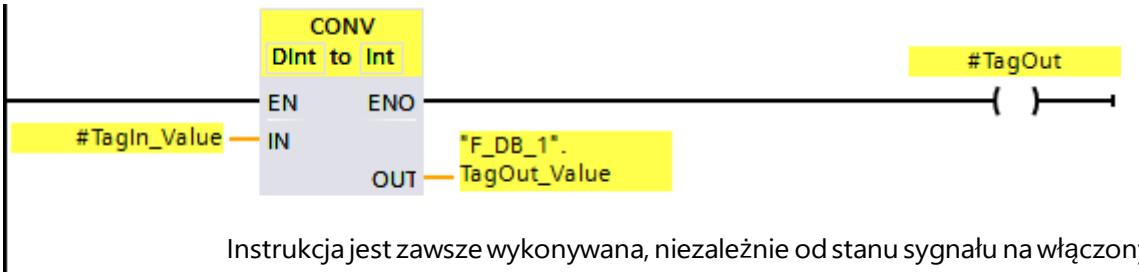
Parametr	Deklaracja	Rodzaj danych	Opis
ENO	Wyjście	BOOL	Włączone wyjście
IN	Wejście	INT, DINT	Wartość do przekształcenia.
OUT	Wyjście	INT, DINT	Wynik przekształcenia

Rodzaje danych instrukcji można wybrać z listy rozwijanej „<???>" w polu instrukcji. Obsługiwane przekształcenia obejmują z „INT na DINT" oraz „DINT na INT".

Przykład

Poniższy przykład przedstawia sposób działania instrukcji „Convert value „DINT to INT"" (Przekształcenie wartości „DINT na INT") dla F-CPU S7-1200/1500:





Instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu EN.

Wartość argumentu „TagIn_Value" jest przekształcana na liczbę całkowitą (16-bitową), a wynik jest zapisywany w argumentzie „"F_DB_1".TagOut_Value".

Jeśli podczas wykonywania instrukcji „Convert value „DINT to INT"" (Przekształcenie wartości „DINT na INT") nie występuje przekroczenie wartości, włączone wyjście ENO ma stan sygnału „1" oraz ustawiany jest argument„TagOut".

W razie potrzeby można również zapisać stan sygnału włączonego wyjścia ENO w (F-)DB, po czym centralnie ocenić, czy wystąpiło przepełnienie dla wszystkich bądź jednej grupy instrukcji z detekcją przepełnienia.

Zobacz także

s7cotia.xls (http://support.automation.siemens.com/WW/view/en/49368678/133100)

13.9.2 BO_W: Przekształcenie 16 elementów danych rodzaju BOOL na element danych rodzaju WORD (STEP 7 Safety V16)

Opis

Ta instrukcja przekształca 16 wartości rodzaju danych BOOL na wejścia od IN0 do IN15 dla wartości rodzaju WORD, która jest następnie dostępna na wyjściu OUT. Konwertowanie odbywa się w następujący sposób: I-ty bit wartości WORD jest ustawiany na 0 (lub 1), jeśli wartość na wejściu INi = 0 (lub 1).

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN0	Wejście	BOOL	Bit 0 wartości WORD
IN1	Wejście	BOOL	Bit 1 wartości WORD
...			...
IN15	Wejście	BOOL	Bit 15 wartości WORD
OUT	Wyjście	WORD	Wartość WORD składająca się z IN0 – IN15

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	o	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	—	o	
1,3	x	o	o	
1,4	x	x	x	
2,0	x	x[1]	x[2]	

o Ta wersja nie jest już obsługiwana.

1 obsługiwane dla wersji oprogramowania V4.2 i wyższej

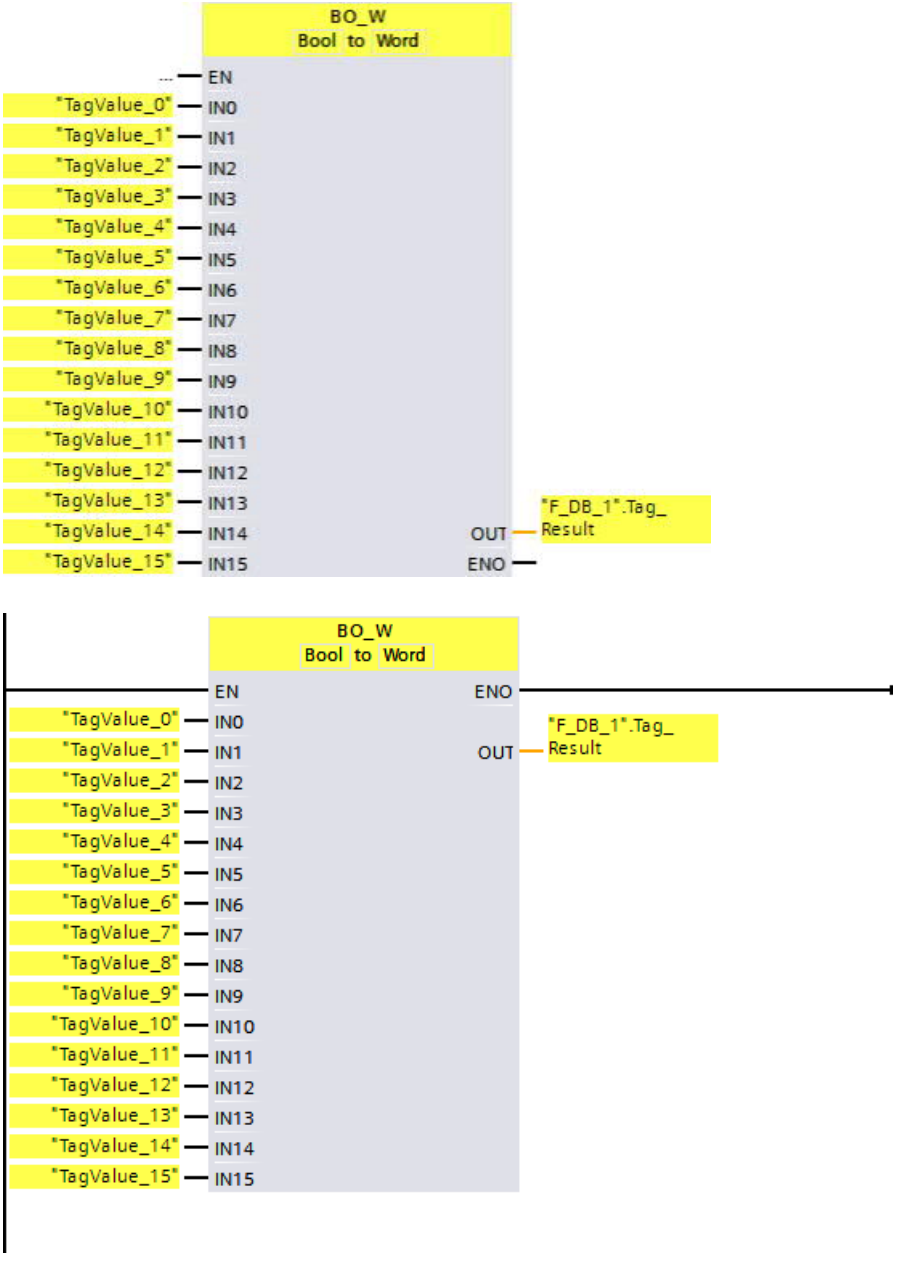
2 obsługiwane dla wersji oprogramowania V2.0 i wyższej

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Poniższa tabela pokazuje, jak działa instrukcja, korzystając z określonych wartości argumentów:

Parametr	Argument	Wartość
IN0	TagValue_0	FALSE
IN1	TagValue_1	FALSE
...		...
IN13	TagValue_13	FALSE
IN14	TagValue_14	TRUE
IN15	TagValue_15	TRUE
OUT	"F_DB_1".Result	W#16#C000

Wartości argumentów od „TagValue_0" do „TagValue_15" są łączone w wartość rodzaju WORD i przypisywane do argumentu „"F_DB_1".TagResult".

13.9.3 W_BO: Przekształcenie elementu danych rodzaju WORD na 16 elementów danych rodzaju BOOL (STEP 7 Safety V16)

Opis

Ta instrukcja przekształca wartości rodzaju danych WORD na wejściu IN na 16 wartości rodzaju BOOL, które jest następnie dostępne na wyjściach od OUT0 do OUT15. Konwertowanie odbywa się w następujący sposób: Wyjście OUTi jest ustawiane na 0 (lub 1), jeśli i-ty bit wartości WORD to 0 (lub 1).

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	WORD	Wartość WORD
OUT0	Wyjście	BOOL	Bit 0 wartości WORD
OUT1	Wyjście	BOOL	Bit 1 wartości WORD
...			...
OUT15	Wyjście	BOOL	Bit 15 wartości WORD

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	o	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	—	o	
1,3	x	o	o	
1,4	x	x	x	
2,0	x	x[1]	x[2]	

o Ta wersja nie jest już obsługiwana.

1 obsługiwane dla wersji oprogramowania V4.2 i wyższej

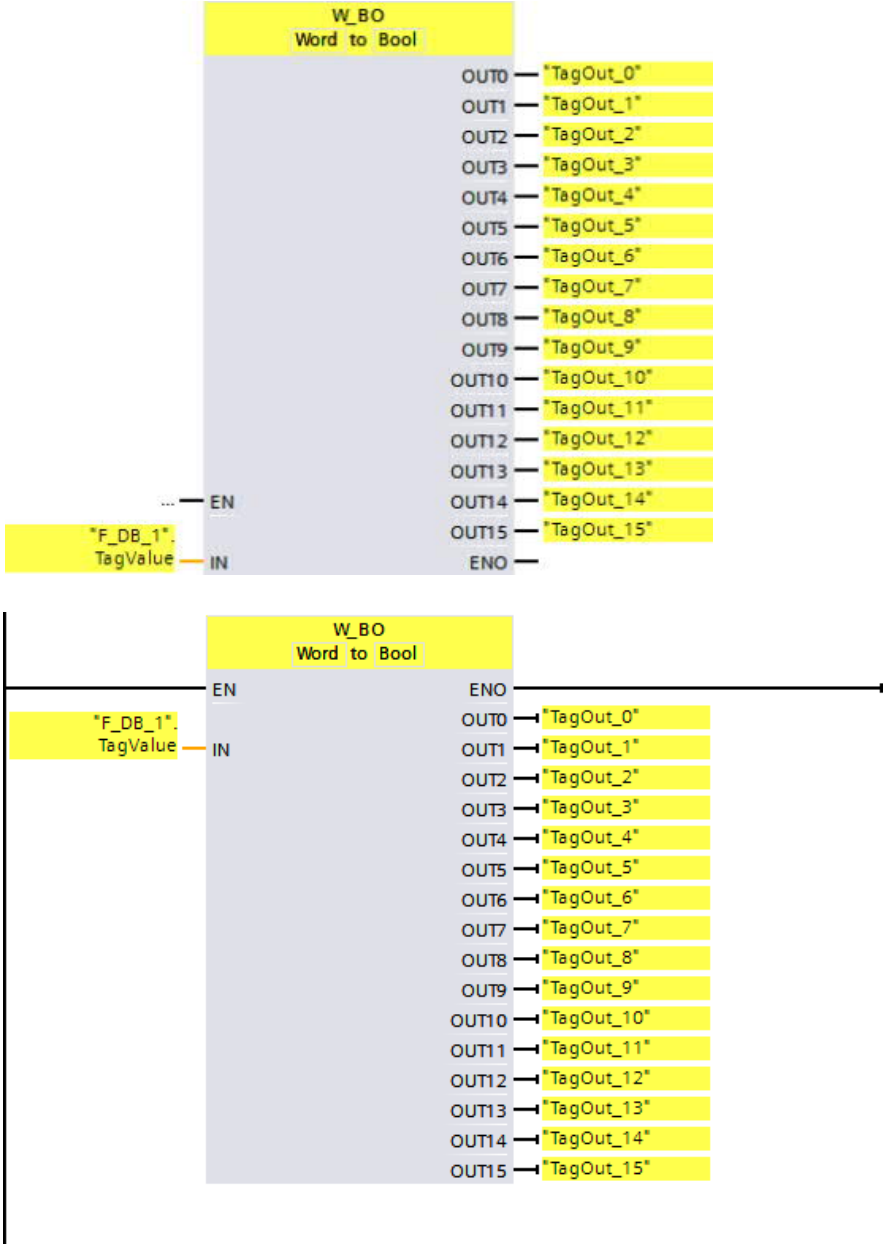
2 obsługiwane dla wersji oprogramowania V2.0 i wyższej

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Poniższa tabela pokazuje, jak działa instrukcja, korzystając z określonych wartości argumentów:

Parametr	Argument	Wartość
IN	"F_DB_1".TagValue	W#16#C000
OUT0	TagOUT_0	FALSE
OUT1	TagOUT_1	FALSE
...		...
OUT13	TagOUT_13	FALSE
OUT14	TagOUT_14	TRUE
OUT15	TagOUT_15	TRUE

Wartość argumentu „"F_DB_1".TagValue" rodzaju danych WORD jest przekształcana na 16 wartości od „TagOUT_0" do „TagOUT_15" rodzaju BOOL.

13.9.4 SCALE: Skalowanie wartości(STEP 7 Safety V16)

Opis

Ta instrukcja skaluje wartość wejścia IN w jednostkach fizycznych pomiędzy wartością dolnego limitu na wejściu LO_LIM a wartością górnego limitu na wejściu HI_LIM. Przyjmuje się, że wartość na wejściu IN mieści się pomiędzy 0 a 27648. Wynik skalowania jest dostępny na wyjściu OUT.

Instrukcja wykorzystuje następujące równanie:

OUT = [IN × (HI_LIM – LO_LIM)] / 27648 + LO_LIM

Dopóki wartość na wejściu IN jest większa niż 27648, wyjście OUT jest połączone z HI_LIM, a OUT_HI jest ustawione na 1.

Dopóki wartość na wejściu IN jest mniejsza niż 0, wyjście OUT jest połączone z LO_LIM, a OUT_LO jest ustawione na 1.

Aby zapewnić odwrotne skalowanie, należy ustawić LO_LIM > HI_LIM. Przy odwrotnym skalowaniu wartość wyjścia OUT maleje gdy wartość wejściowa IN rośnie.

Każde wywołanie instrukcji „Scale value" (Skalowanie wartości) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. Ponadto, gdy instrukcja zostanie wstawiona do programu, automatycznie otwiera się okno „Call options" (Opcje wywołania), gdzie można utworzyć blok danych (pojedyncza instancja) (np. SCALE_DB_1) lub instancję wielokrotną (np. SCALE_Instance_1) dla instrukcji „Scale value" (Skalowanie wartości). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	INT	Wartość wejściowa do skalowania, w jednostkach
HI_LIM	Wejście	INT	Wartość górnego limitu zakresu wartości OUT
LO_LIM	Wejście	INT	Wartość dolnego limitu zakresu wartości OUT
OUT	Wyjście	INT	Wynik skalowania
OUT_HI	Wyjście	BOOL	1 = Wartość wejściowa > 27648: OUT = HI_LIM
OUT_LO	Wyjście	BOOL	1 = Wartość wejściowa < 0: OUT = LO_LIM

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	x	x	

o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Zachowanie w przypadku nadmiernej lub niedostatecznej wartości analogowej oraz wyjścia wartości fail-safe

Uwaga

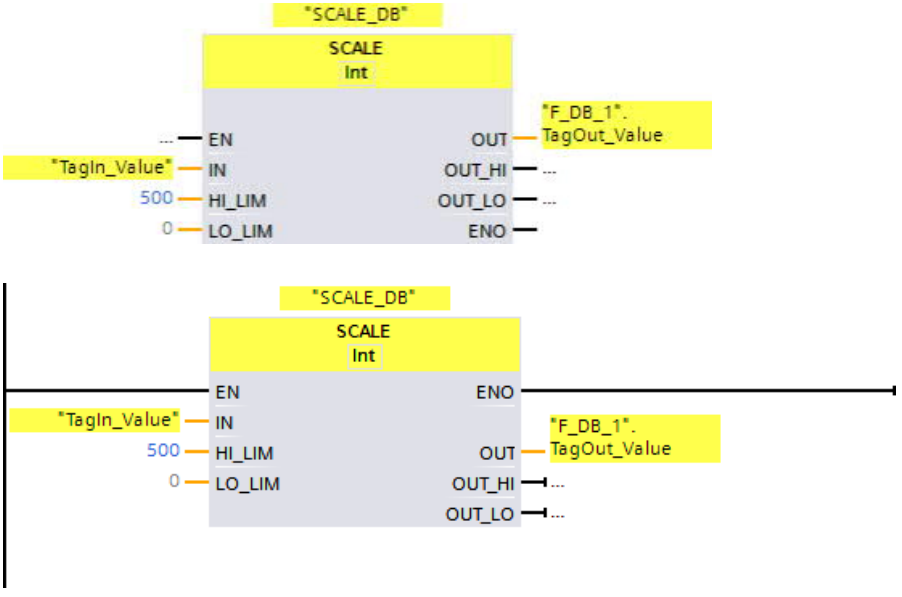
Jeśli wejścia z PII w SM 336; AI 6 x 13Bit or SM 336; F-AI 6 x 0/4 ... 20 mA HART są wykorzystywane jako wartości wejściowe, należy pamiętać, że system bezpieczeństwa wykrywa nadmierną lub niedostateczną wartość kanału tego F-SM jako usterkę F-I/O lub usterkę kanału. Wartość fail-safe 0 jest podawana zamiast $7FFF_H$ (przy nadmiernej wartości) lub 8000_H (przy niedostatecznej wartości) w PII do programu bezpieczeństwa.

Jeśli powinny być wyprowadzane inne wartości fail-safe, należy wykonać ocenę sygnału QBAD powiązanego F-I/O lub sygnału QBAD_I_xx / stanu wartości odnośnego kanału.

Jeśli wartość w PII F-SM wykracza poza zakres, lecz mieści się w > 27648 lub < 0, można podobnie wykonać odgałęzienie do wyjścia indywidualnej wartości fail-safe poprzez wykonanie oceny wyjść, kolejno OUT_HI oraz OUT_LO.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gdy argument „TagIn_Value" = 20000, wynik dla „"F_DB_1".TagOut_Value" to 361.

13.9.5 SCALE_D: Skalowanie wartości do rodzaju danych DINT (STEP 7 Safety V16) (S7-1200, S7-1500)

Opis

Ta instrukcja skaluje wartość wejścia IN w jednostkach fizycznych pomiędzy wartością dolnego limitu na wejściu LO_LIM a wartością górnego limitu na wejściu HI_LIM. Przyjmuje się, że wartość na wejściu IN mieści się pomiędzy 0 a 27648. Wynik skalowania jest dostępny na wyjściu OUT.

Instrukcja wykorzystuje następujące równanie:

OUT = [IN × (HI_LIM – LO_LIM)] / 27648 + LO_LIM

Dopóki wartość na wejściu IN jest większa niż 27648, wyjście OUT jest połączone z HI_LIM, a OUT_HI jest ustawione na 1.

Dopóki wartość na wejściu IN jest mniejsza niż 0, wyjście OUT jest połączone z LO_LIM, a OUT_LO jest ustawione na 1.

Aby zapewnić odwrotne skalowanie, należy ustawić LO_LIM > HI_LIM. Przy odwrotnym skalowaniu wartość wyjścia OUT maleje gdy wartość wejściowa IN rośnie.

Każde wywołanie instrukcji „Scale value to data type DINT" (Skalowanie wartości do rodzaju danych DINT) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. Ponadto, gdy instrukcja zostanie wstawiona do programu, automatycznie otwiera się okno „Call options" (Opcje wywołania), gdzie można utworzyć blok danych (pojedyncza instancja) (np. SCALE_D_DB_1) lub instancję wielokrotną (np. SCALE_D_Instance_1) dla instrukcji „Scale value to data type DINT" (Skalowanie wartości do rodzaju danych DINT). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Parametr

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	INT	Wartość wejściowa do skalowania, w jednostkach
HI_LIM	Wejście	DINT	Wartość górnego limitu zakresu wartości OUT
LO_LIM	Wejście	DINT	Wartość dolnego limitu zakresu wartości OUT
OUT	Wyjście	DINT	Wynik skalowania
OUT_HI	Wyjście	BOOL	1 = Wartość wejściowa > 27648: OUT = HI_LIM
OUT_LO	Wyjście	BOOL	1 = Wartość wejściowa < 0: OUT = LO_LIM

Wersje instrukcji

Dla tej instrukcji dostępna jest jedna wersja:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
2,0	—	x[1]	x[2]	

1 obsługiwane dla wersji oprogramowania V4.2 i wyższej

2 obsługiwane dla wersji oprogramowania V2.0 i wyższej

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Zachowanie w przypadku nadmiernej lub niedostatecznej wartości analogowej oraz wyjścia wartości fail-safe

Uwaga

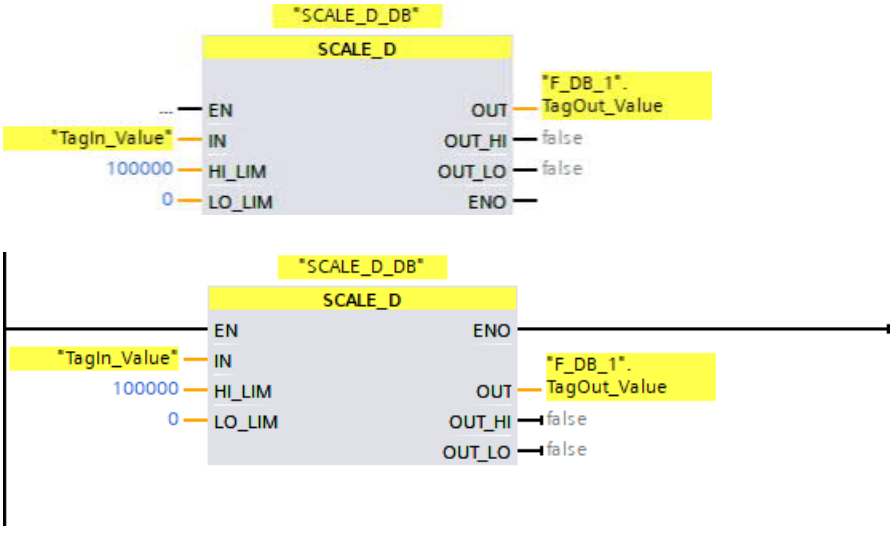
Jeśli wejścia z PII w SM 336; AI 6 x 13Bit or SM 336; F-AI 6 x 0/4 ... 20 mA HART są wykorzystywane jako wartości wejściowe, należy pamiętać, że system bezpieczeństwa wykrywa nadmierną lub niedostateczną wartość kanału tego F-SM jako usterkę F-I/O lub usterkę kanału. Wartość fail-safe 0 jest podawana zamiast $7FFF_H$ (przy nadmiernej wartości) lub 8000_H (przy niedostatecznej wartości) w PII do programu bezpieczeństwa.

Jeśli powinny być wyprowadzane inne wartości fail-safe, należy wykonać ocenę sygnału QBAD powiązanego F-I/O lub sygnału QBAD_I_xx / stanu wartości odnośnego kanału.

Jeśli wartość w PII F-SM wykracza poza zakres, lecz mieści się w > 27648 lub < 0, można podobnie wykonać odgałęzienie do wyjścia indywidualnej wartości fail-safe poprzez wykonanie oceny wyjść, kolejno OUT_HI oraz OUT_LO.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gdy argument „TagIn_Value" = 20000, wynik dla „"F_DB_1".TagOut_Value" to 72337.

13.10 Operacje sterowania programem

13.10.1 JMP: Skok, jeśli RLO = 1 (STEP 7 Safety V16)

Opis

Instrukcja „Jump if RLO = 1" (Skok, jeśli RLO = 1) pozwala na przerwanie liniowego wykonywania programu i wznowienie go w innej sieci. Sieć docelowa musi być zidentyfikowana przez etykietę skoku (strona 602) (LABEL). Opis etykiety skoku jest określany w symbolu zastępczym powyżej instrukcji.

Określona etykieta skoku musi znajdować się w tym samym bloku, w którym wykonywana jest instrukcja. Określona nazwa może wystąpić tylko raz na blok.

Jeśli wynik operacji logicznej (RLO) na wejściu instrukcji to „1" lub wejście nie jest podłączone, skok do sieci zidentyfikowanej przez etykietę skoku jest wykonywany. Kierunek skoku może być w stronę wyższych lub niższych numerów sieci.

Jeśli wynik operacji logicznej (RLO) na wejściu instrukcji to „0", program dalej jest wykonywany w następnej sieci.

Uwaga

(S7-1200, S7-1500)

Jeśli miejsce docelowe skoku (etykieta skoku) dla instrukcji „JMP" „JMPN" znajduje się powyżej instrukcji „JMP" lub „JMPN" (skok wstecz), nie można wstawić innych instrukcji do sterowania programem (JMP, JMPN, RET, etykieta skoku) pomiędzy nie.
Wyjątek: Możliwe jest wstawienie instrukcji „JMP" lub „JMPN" pomiędzy nie, jeśli znajdzie się pomiędzy nimi również powiązane miejsce docelowe skoku, a także poniżej powiązanej instrukcji „JMP" lub „JMPN" (skok naprzód).

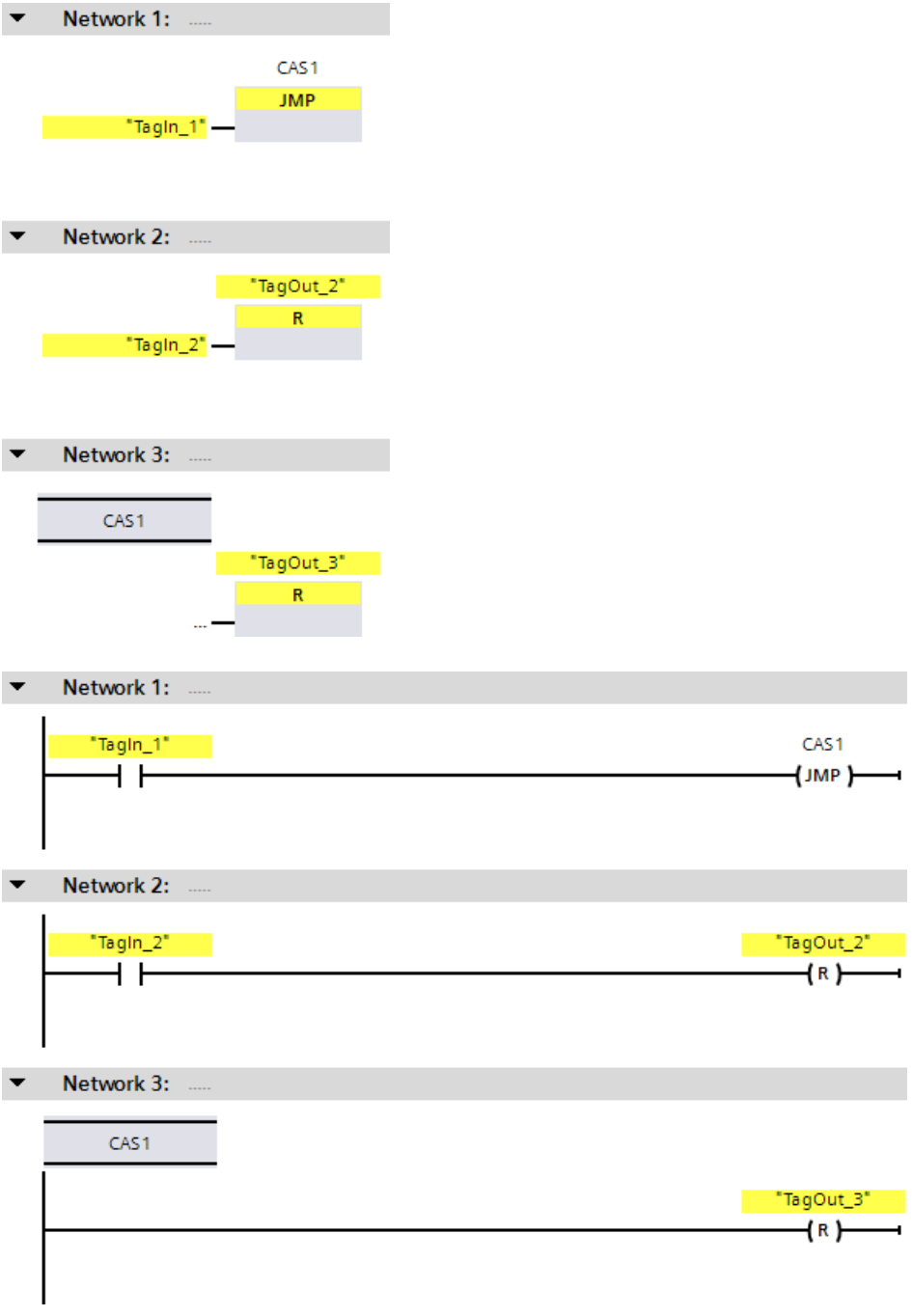
Niezgodność może prowadzić do błędów kompilacji lub przejścia F-CPU w tryb STOP.

Uwaga

Niedozwolone jest wstawianie instrukcji SENDDP lub SENDS7 pomiędzy instrukcję JMP lub JMPN oraz powiązane miejsce docelowe skoku (etykietę skoku).

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gd argument „TagIn_1" ma stan sygnału „1", instrukcja „Jump if RLO = 1" jest wykonywana. Wykonanie liniowe programu jest przerywane, a następnie kontynuowane w sieci 3, która została zidentyfikowana za pomocą etykiety skoku CAS1. Gdy wejście „TagIn_3" ma stan sygnału „1", wyjście „TagOut_3" jest resetowane.

13.10.2 JMPN: Skok, jeśli RLO = 0 (STEP 7 Safety V16)

Opis

Instrukcja „Jump if RLO = 0" (Skok, jeśli RLO = 0) pozwala na przerwanie liniowego wykonywania programu i wznowienie go w innej sieci, gdy wynik operacji logicznej na wejściu instrukcji to „0". Sieć docelowa musi być zidentyfikowana przez etykietę skoku (strona 602) (LABEL). Opis etykiety skoku jest określany w symbolu zastępczym powyżej instrukcji.

Określona etykieta skoku musi znajdować się w tym samym bloku, w którym wykonywana jest instrukcja. Określona nazwa może wystąpić tylko raz na blok.

Jeśli wynik operacji logicznej (RLO) na wejściu instrukcji to „0", skok do sieci zidentyfikowanej etykietą skoku jest wykonywany. Kierunek skoku może być w stronę wyższych lub niższych numerów sieci.

Jeśli wynik operacji logicznej (RLO) na wejściu instrukcji to „1", program dalej jest wykonywany w następnej sieci.

Uwaga

(S7-1200, S7-1500)

Jeśli miejsce docelowe skoku (etykieta skoku) dla instrukcji „JMP" „JMPN" znajduje się powyżej instrukcji „JMP" lub „JMPN" (skok wstecz), nie można wstawić innych instrukcji do sterowania programem (JMP, JMPN, RET, etykieta skoku) pomiędzy nie.
Wyjątek: Możliwe jest wstawienie instrukcji „JMP" lub „JMPN" pomiędzy nie, jeśli znajdzie się pomiędzy nimi również powiązane miejsce docelowe skoku, a także poniżej powiązanej instrukcji „JMP" lub „JMPN" (skok naprzód).

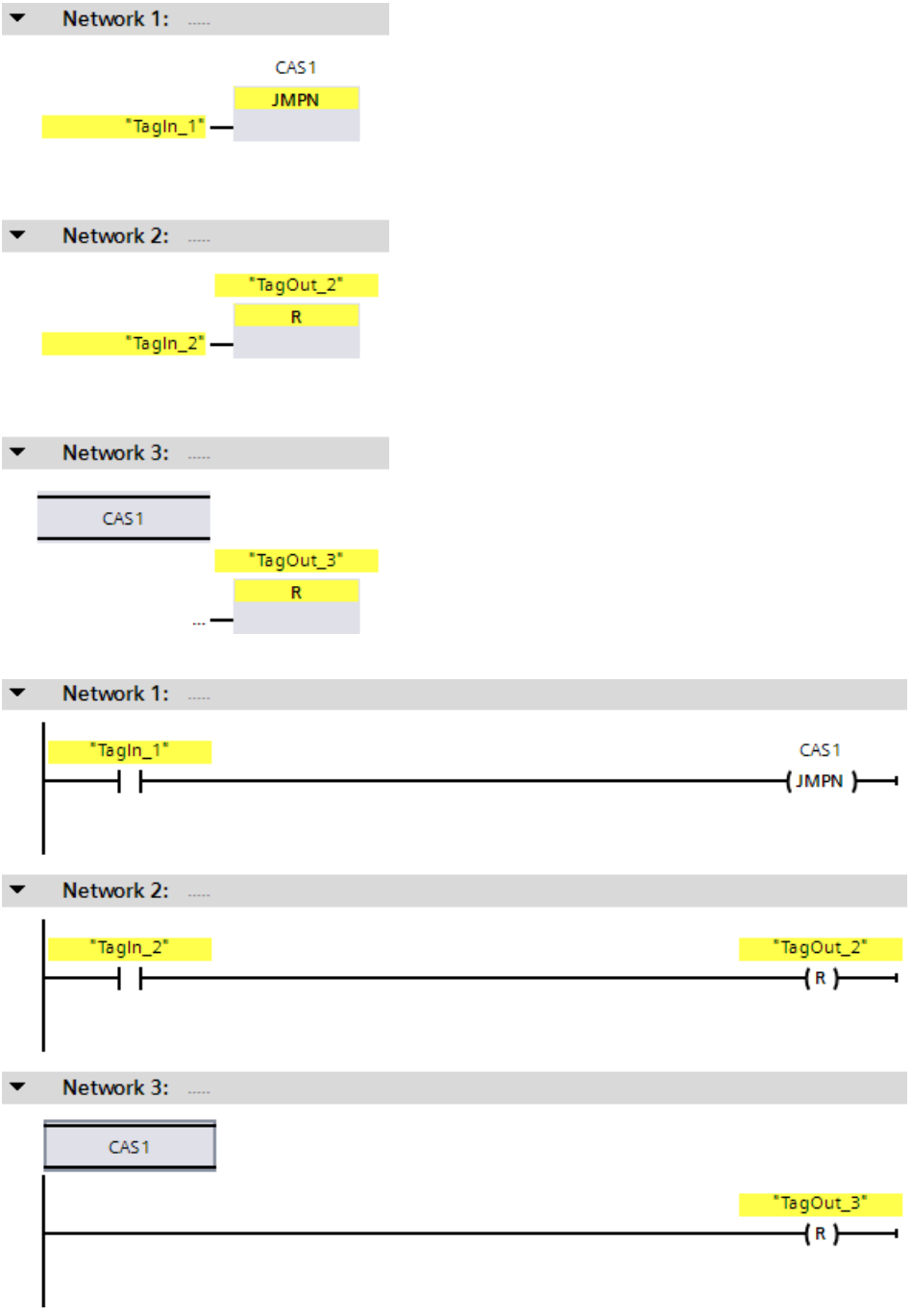
Niezgodność może prowadzić do błędów kompilacji lub przejścia F-CPU w tryb STOP.

Uwaga

Niedozwolone jest wstawianie instrukcji SENDDP lub SENDS7 pomiędzy instrukcję JMP lub JMPN oraz powiązane miejsce docelowe skoku (etykietę skoku).

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gd argument „TagIn_1" ma stan sygnału „0", instrukcja „Jump if RLO = 0" jest wykonywana. Wykonanie liniowe programu jest przerywane, a następnie kontynuowane w sieci 3, która została zidentyfikowana za pomocą etykiety skoku CAS1. Gdy wejście „TagIn_3" ma stan sygnału „1", wyjście „TagOut_3" jest resetowane.

13.10.3 LABEL: Etykieta skoku (STEP 7 Safety V16)

Opis

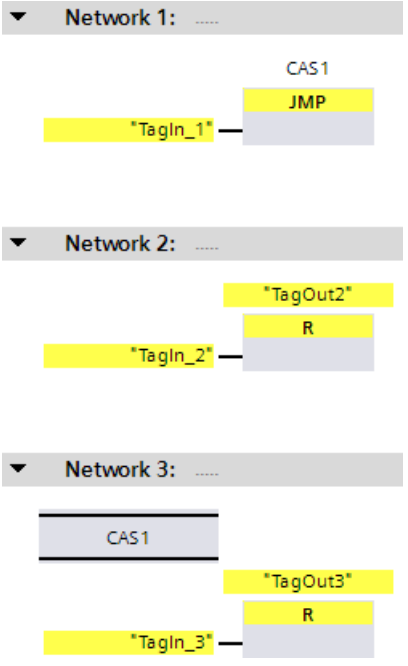
Za pomocą etykiety skoku można określić sieć docelową, w której ma być wznowione wykonywanie programu po skoku.

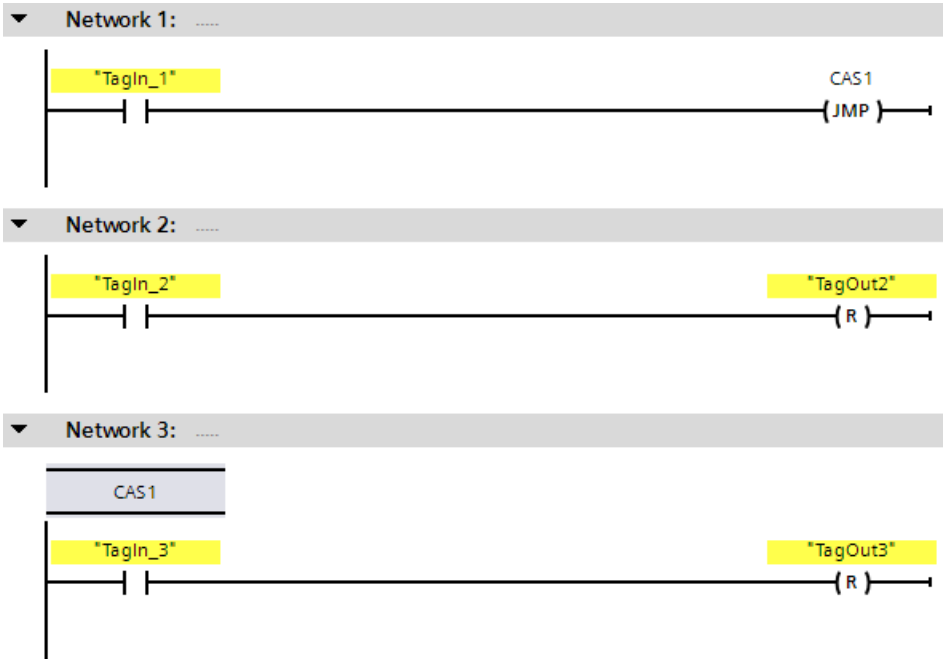
Etykieta skoku oraz instrukcja, w której należy określić etykietę, muszą znajdować się w tym samym bloku. Nazwa etykiety skoku może być przypisana tylko raz na blok.

W sieci można umieścić tylko jedną etykietę skoku. Do każdej etykiety można przeskoczyć z wielu miejsc.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:





Gd argument „TagIn_1" ma stan sygnału „1", instrukcja „Jump if RLO = 1" jest wykonywana. Wykonanie liniowe programu jest przerywane, a następnie kontynuowane w sieci 3, która została zidentyfikowana za pomocą etykiety skoku CAS1. Gdy wejście „TagIn_3" ma stan sygnału „1", wyjście „TagOut_3" jest resetowane.

Zobacz także

JMP:Skok, jeśli RLO = 1 (STEP 7 Safety V16) (strona 598)

JMPN:Skok, jeśli RLO = 0 (STEP 7 Safety V16) (strona 600)

RET: Powrót (STEP 7 Safety V16) (strona 604)

13.10.4 RET: Powrót (STEP 7 Safety V16)

Opis

Możliwe jest użycie instrukcji „Return" (Powrót) do zatrzymania przetwarzania bloku.

Jeśli wynik operacji logicznej (RLO) na wejściu instrukcji „Return" (Powrót) to „1" lub wejście pola F-CPU S7-1200/1500 nie zostało podłączone w FBD, wykonywanie programu jest kończone w bieżąco wywołanym bloku i kontynuowane w bloku wywołującym (przykładowo, w głównym bloku bezpieczeństwa) po funkcji wywołania. Jeśli RLO na wejściu instrukcji „Return" to „0", instrukcja nie jest wykonywana. Wykonywanie instrukcji jest kontynuowane w następnej sieci wywołanego bloku.

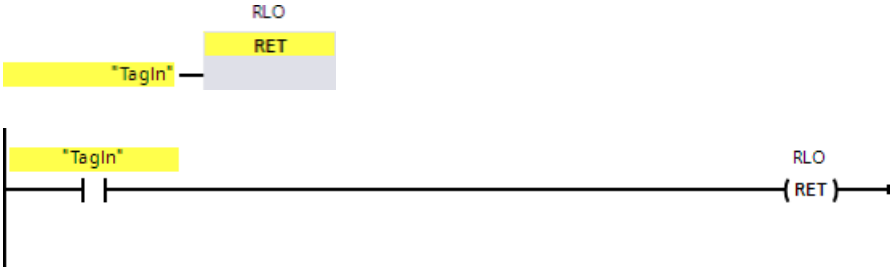
Wpływ na stan funkcji wywołania (ENO) nie ma znaczenia, ponieważ włączone wyjście „ENO" nie może być podłączone.

Uwaga

(S7-300, S7-400) Nie jest możliwe zaprogramowanie instrukcji RET w głównym bloku bezpieczeństwa.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Gdy argument „TagIn" zapewni stan sygnału „1", instrukcja „Return" (Powrót) jest wykonywana. Wykonywanie programu jest kończone w wywołanym bloku i jest kontynuowane w bloku wywołującym.

Zobacz także

JMP:Skok, jeśli RLO = 1 (STEP 7 Safety V16) (strona 598)

JMPN:Skok, jeśli RLO = 0 (STEP 7 Safety V16) (strona 600)

LABEL:Etykieta skoku (STEP 7 Safety V16) (strona 602)

13.10.5 OPN: Otwórz globalny blok danych (STEP 7 Safety Advanced V16) (S7-300, S7-400)

Opis

Za pomocą instrukcji „Open global data block" (Otwórz globalny blok danych) można otworzyć blok danych. Numer bloku danych jest przenoszony do rejestru DB. Kolejne polecenia DB uzyskują dostęp do odnośnych bloków zależnie od treści rejestru.

Uwaga

Podczas korzystania z instrukcji „Open global data block" (Otwórz globalny blok danych) należy pamiętać, że zawartość rejestru DB może ulec zmianie po wywołaniach F-FB/F-FC oraz „w pełni kwalifikowanym dostępie DB", więc nie ma gwarancji, że ostatni blok danych otwarty za pomocą tej instrukcji wciąż jest otwarty.

Należy zatem użyć następującej metody do adresowania danych, by uniknąć błędów podczas uzyskiwania dostępu do danych rejestru DB:

- Należy użyć adresowania symbolicznego.
- Korzystać jedynie z w pełni kwalifikowanego dostępu DB.

Aby wykonać operację „Open global data block" (Otwórz globalny blok danych), należy upewnić się, że rejestr DB został zapisany, powtarzając tę instrukcję po wywołaniach F- FB/F-FC oraz "w pełni kwalifikowanego dostępu DB". W przeciwnym razie może dojść do usterki.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
<Blok danych>	Wejście	BLOCK_DB	Otwarty blok danych

„W pełni kwalifikowany dostęp DB"

Początkowy dostęp do danych w bloku w F-FB/F-FC zawsze musi być „w pełni kwalifikowanym dostępem DB" lub musi być poprzedzony instrukcją „Open global data block" (Otwórz globalny blok danych). Dotyczy to również dostępu początkowego do danych bloku po etykiecie skoku.

Przykład „w pełni kwalifikowanego dostępu DB" oraz „nie w pełni kwalifikowanego dostępu DB" dostępny jest w dziale „Ograniczenia w językach programowania FBD/LAD" (strona 121).

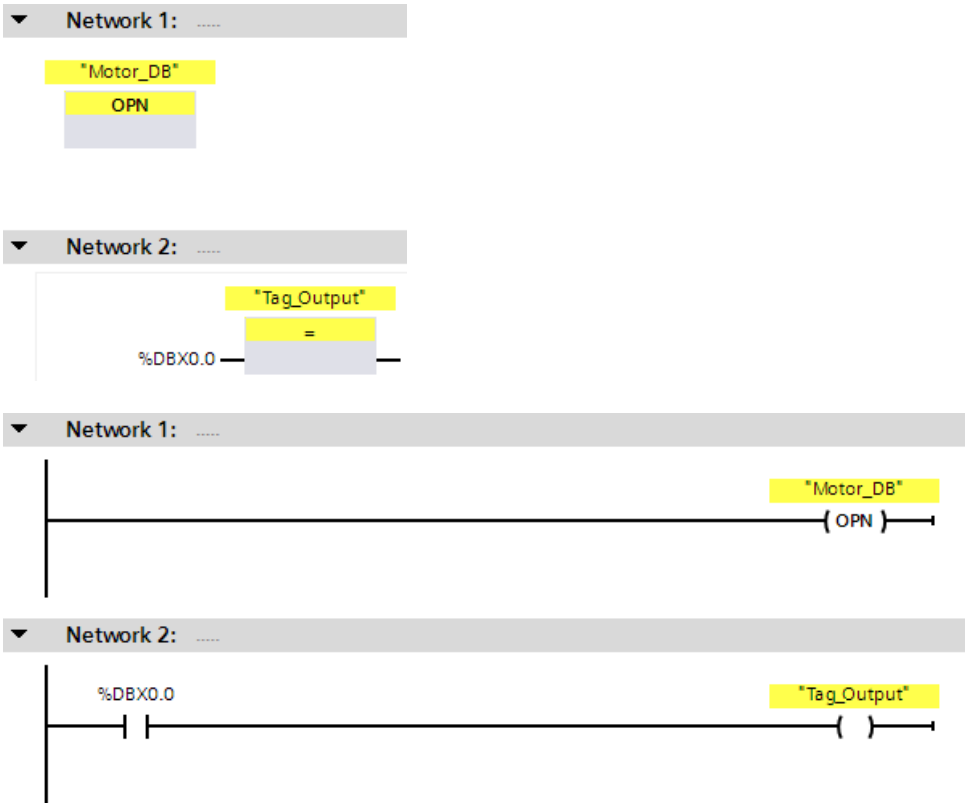
Dostęp do DB instancji

Możliwy jest również dostęp do instancji DB z F-FB z w pełni kwalifikowanym dostępem, np. do przenoszenia parametrów bloków. Nie jest możliwe uzyskanie dostępu do statycznych danych lokalnych w pojedynczej/wielu instancjach innych F-FB.

Należy pamiętać, że dostęp do instancji DB z F-FB, które nie zostały wywołane w programie bezpieczeństwa może spowodować przejście F-CPU do trybu STOP.

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Blok danych „Motor_DB" jest wywoływany w sieci 1. Numer bloku danych jest przenoszony do rejestru DB. Argument „DBX0.0" jest wyszukiwany w sieci 2. Stan sygnału argumentu „DBX0.0" jest przypisywany do argumentu „Tag_Output".

13.11 Operacje na słowach logicznych

13.11.1 AND: Operacja logiczna AND (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „AND logic operation" (Operacja logiczna AND) można połączyć wartość na wejściu IN1 z wartością na wejściu IN2, wykonując operację sumy logicznej i wyprowadzając wynik na wyjście OUT.

Po wykonaniu instrukcji bit 0 wartości na wejściu IN1 oraz bit 0 wartości na wejściu IN2 są sumowane logicznie. Wynik jest zapisywany w bicie 0 wyjścia OUT. Ta sama operacja logiczna jest wykonywana dla pozostałych bitów określonych wartości.

Bit wyniku ma stan wartości „1" jedynie, gdy oba bity z operacji również miały stan „1". Jeśli jeden z dwóch bitów operacji logicznej ma stan wartości „0", odnośny bit wyniku zostanie zresetowany.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

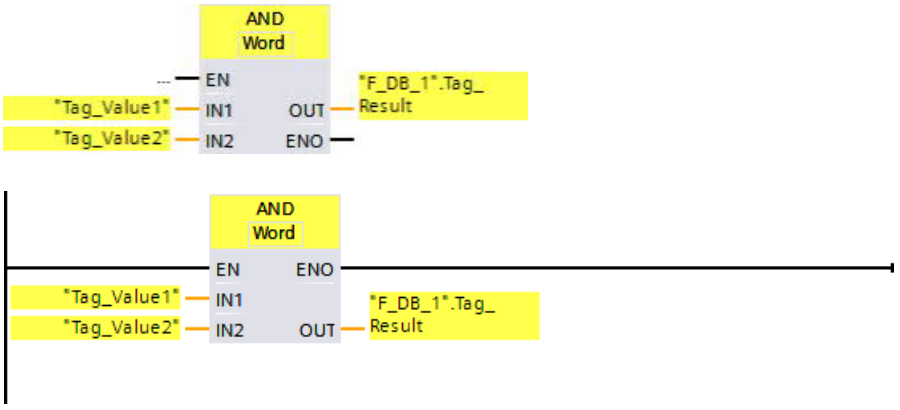
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN1	Wejście	WORD	Pierwsza wartość operacji logicznej
IN2	Wejście	WORD	Druga wartość operacji logicznej
OUT	Wyjście	WORD	Wynik instrukcji

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



IN1	"Tag_Value1" = 01010101 01010101
IN2	"Tag_Value2" = 00000000 00001111
OUT	"F_DB_1"."Tag_Result" = 00000000 00000101

Instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN". Wartość argumentu „Tag_Value1" jest sumowana logicznie z wartością argumentu „Tag_Value2". Wynik jest mapowany bit po bicie, po czym wyprowadzany w argumentzie „"F_DB_1".Tag_Result".

13.11.2 OR: Operacja logiczna OR (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „OR logic operation" (Operacja logiczna OR) można połączyć wartość na wejściu IN1 z wartością na wejściu IN2, wykonując operację iloczynu logicznego i wyprowadzając wynik na wyjście OR.

Po wykonaniu instrukcji bit 0 wartości na wejściu IN1 oraz bit 0 wartości na wejściu IN2 są mnożone logicznie. Wynik jest zapisywany w bicie 0 wyjścia OUT. Ta sama operacja logiczna jest wykonywana dla pozostałych bitów określonych tagów.

Bit wyniku ma stan wartości „1", gdy co najmniej jednej z dwóch bitów operacji również miał stan „1". Jeśli oba bity operacji logicznej mają stan wartości „0", odnośny bit wyniku zostanie zresetowany.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

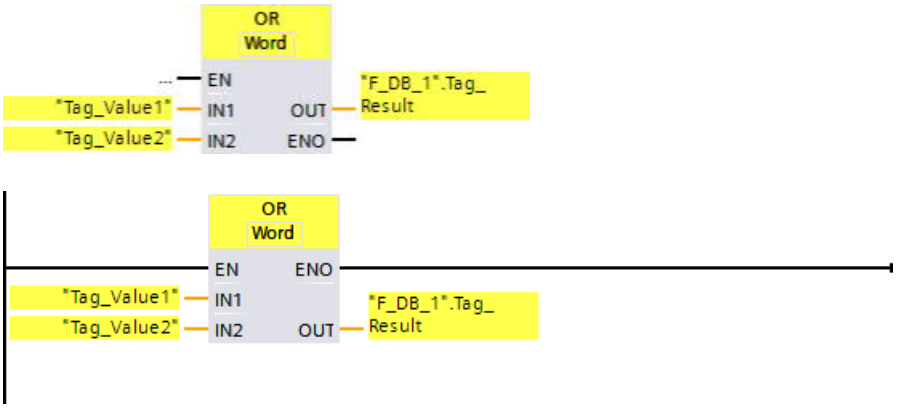
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN1	Wejście	WORD	Pierwsza wartość operacji logicznej
IN2	Wejście	WORD	Druga wartość operacji logicznej
OUT	Wyjście	WORD	Wynik instrukcji

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



IN1	"Tag_Value1" = 01010101 01010101
IN2	"Tag_Value2" = 00000000 00001111
OUT	"F_DB_1"."Tag_Result" = 01010101 01011111

Instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN". Wartość argumentu „Tag_Value1" jest mnożona logicznie z wartością argumentu „Tag_Value2". Wynik jest mapowany bit po bicie, po czym wyprowadzany w argumencie „"F_DB_1".Tag_Result".

13.11.3 XOR: Operacja logiczna EXCLUSIVE OR (STEP 7 Safety V16)

Opis

Za pomocą instrukcji „EXCLUSIVE OR logic operation" (Operacja logiczna EXCLUSIVE OR) można połączyć wartość na wejściu IN1 z wartością na wejściu IN2, wykonując operację alternatywy rozłącznej i wyprowadzając wynik na wyjście OUT.

Po wykonaniu instrukcji bit 0 wartości na wejściu IN1 oraz bit 0 wartości na wejściu IN2 są łączone logicznie w operacji alternatywy rozłącznej. Wynik jest zapisywany w bicie 0 wyjścia OUT. Ta sama operacja logiczna jest wykonywana dla pozostałych bitów określonych wartości.

Bit wyniku ma stan wartości „1", gdy jeden z dwóch bitów operacji ma stan „1". Jeśli oba bity operacji logicznej mają stan wartości „1" lub „0", odnośny bit wyniku zostanie zresetowany.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

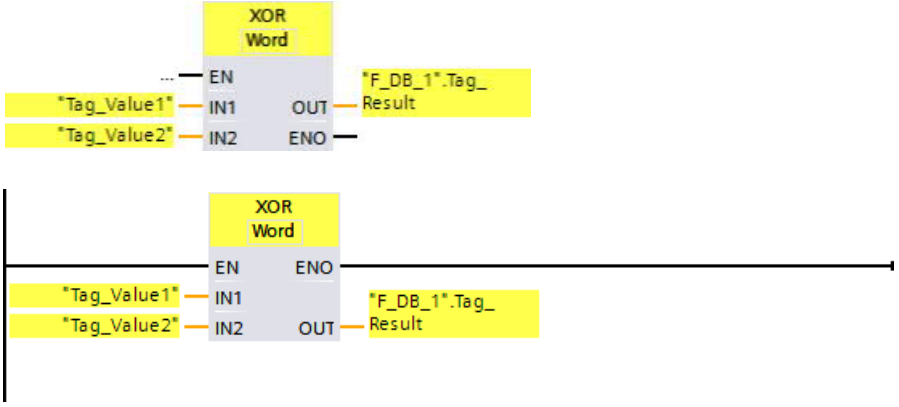
Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN1	Wejście	WORD	Pierwsza wartość operacji logicznej
IN2	Wejście	WORD	Druga wartość operacji logicznej
OUT	Wyjście	WORD	Wynik instrukcji

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



IN1	"Tag_Value1" = 01010101 01010101
IN2	"Tag_Value2" = 00000000 00001111
OUT	"F_DB_1"."Tag_Result" = 01010101 01011010

Instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN". Wartość argumentu „Tag_Value1" jest łączony logicznie operacją alternatywy rozłącznej z wartością argumentu „Tag_Value2". Wynik jest mapowany bit po bicie, po czym wyprowadzany w argumentzie „"F_DB_1".Tag_Result".

13.12 Przesunięcie i obrócenie

13.12.1 SHR: Przesunięcie w prawo (STEP 7 Safety V16)

Opis

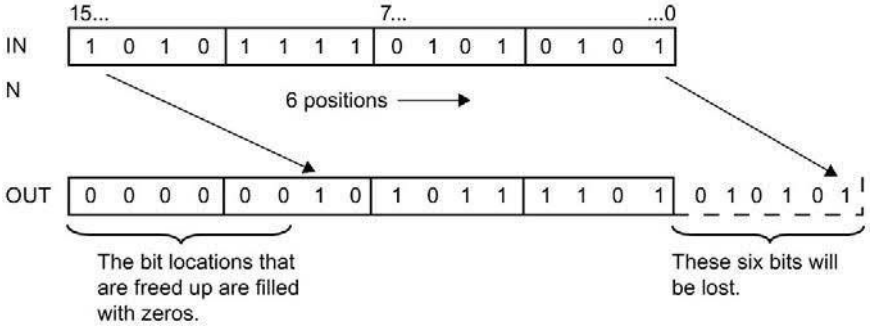
Za pomocą instrukcji „Shift right" (Przesunięcie w prawo) można przesunąć zawartość argumentu na wejściu IN bit po bicie w prawo i wyprowadzić wynik na wyjście OUT. Przy pomocy wejścia N można określić numer pozycji bitu, do którego należy przenieść określoną wartość.

Jeśli wartość na wejściu N to „0", wartość na wejściu IN jest kopiowana do argumentu na wyjściu OUT.

Jeśli wartość na wejściu N jest większa niż liczba dostępnych pozycji bitowych, wartość argumentu na wejściu IN jest przesuwana w prawo o dostępną liczbę pozycji.

Pozycje bitowe zwolnione po lewej stronie argumentu podczas operacji przesunięcia są zapełniane zerami.

Poniższa ilustracja przedstawia, jak argument rodzaju WORD jest przesuwany o 6 pozycji bitowych w prawo:



Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Uwaga

S7-300/400:

Ocenie podlega tylko niski bajt z wejścia N.

S7-1200/1500:

Jeśli wartość na wejściu N < 0, wyjście OUT jest ustawiane na 0.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	WORD	Przesuwana wartość
N	Wejście	INT	Liczba pozycji bitowych, o które przesuwana jest wartość
OUT	Wyjście	WORD	Wynik instrukcji

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	o	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	—	o	
1,3	x	o	o	
1,4	x	x	x	
2,0	x	x[1]	x[2]	

o Ta wersja nie jest już obsługiwana.

1 obsługiwane dla wersji oprogramowania V4.2 i wyższej

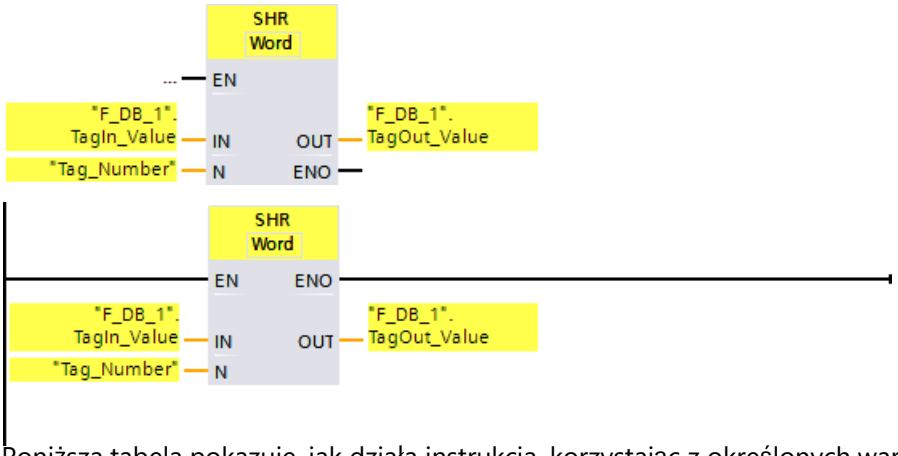
2 obsługiwane dla wersji oprogramowania V2.0 i wyższej

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Poniższa tabela pokazuje, jak działa instrukcja, korzystając z określonych wartości argumentów:

Parametr	Argument	Wartość
IN	"F_DB_1".TagIn_Value	0011 1111 1010 1111
N	Tag_Number	3
OUT	"F_DB_1".TagOut_Value	0000 0111 1111 0101

Instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN". Zawartość argumentu „"F_DB_1".TagIn_Value" jest przesuwana o trzy pozycje bitowe w prawo. Wynik jest wyprowadzany na wyjście „"F_DB_1".TagOut_Value".

13.12.2 SHL: Przesunięcie w lewo (STEP 7 Safety V16)

Opis

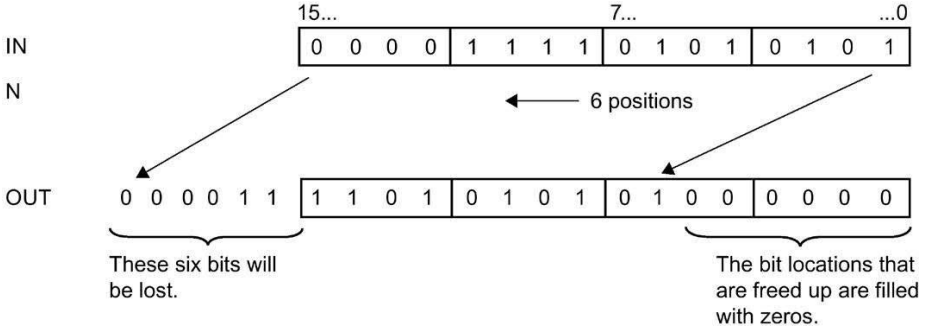
Za pomocą instrukcji „Shift left" (Przesunięcie w lewo) można przesunąć zawartość argumentu na wejściu IN bit po bicie w lewo i wyprowadzić wynik na wyjście OUT. Przy pomocy wejścia N można określić numer pozycji bitu, do którego należy przenieść określoną wartość.

Jeśli wartość na wejściu N to „0", wartość na wejściu IN jest kopiowana do argumentu na wyjściu OUT.

Jeśli wartość na wejściu N jest większa niż liczba dostępnych pozycji bitowych, wartość argumentu na wejściu IN jest przesuwana w lewo o dostępną liczbę pozycji.

Pozycje bitowe zwolnione po prawej stronie argumentu podczas operacji przesunięcia są zapełniane zerami.

Poniższa ilustracja przedstawia, jak argument rodzaju WORD jest przesuwany o 6 pozycji bitowych w lewo:



Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Uwaga

S7-300/400:

Ocenie podlega tylko niski bajt z wejścia N.

S7-1200/1500:

Jeśli wartość na wejściu N < 0, wyjście OUT jest ustawiane na 0.

Parametry

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	Wejście	WORD	Przesuwana wartość
N	Wejście	INT	Liczba pozycji bitowych, o które przesuwana jest wartość
OUT	Wyjście	WORD	Wynik instrukcji

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	o	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	—	o	
1,3	x	o	o	
1,4	x	x	x	
2,0	x	x[1]	x[2]	

o Ta wersja nie jest już obsługiwana.

1 obsługiwane dla wersji oprogramowania V4.2 i wyższej

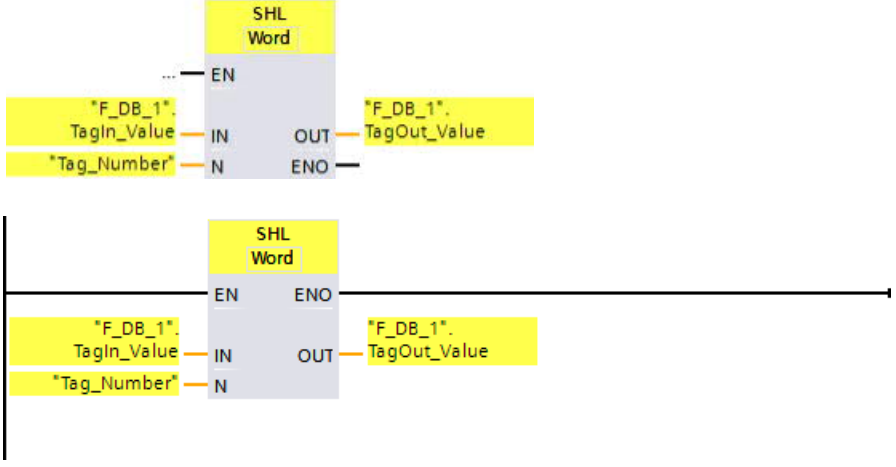
2 obsługiwane dla wersji oprogramowania V2.0 i wyższej

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Poniższa tabela pokazuje, jak działa instrukcja, korzystając z określonych wartości argumentów:

Parametr	Argument	Wartość
IN	"F_DB_1".TagIn_Value	0011 1111 1010 1111
N	Tag_Number	4
OUT	"F_DB_1".TagOut_Value	1111 1010 1111 0000

Instrukcja jest zawsze wykonywana, niezależnie od stanu sygnału na włączonym wejściu „EN". Zawartość argumentu „"F_DB_1".TagIn_Value" jest przesuwana o cztery pozycje bitowe w lewo. Wynik jest wyprowadzany na wyjście „"F_DB_1".TagOut_Value".

13.13 Instrukcje operatorskie

13.13.1 ACK_OP: Zatwierdzenie typu fail-safe (STEP 7 Safety V16)

Opis (S7-300, S7-400)

Ta instrukcja umożliwia zatwierdzenie fail-safe z poziomu systemu HMI. Pozwala, przykładowo, na sterowanie reintegracją F-I/O z systemu HMI. Zatwierdzenie odbywa się w dwóch krokach:

- Parametr wejściowy/wyjściowy IN zmienia się na wartość 6 przez dokładnie jeden cykl.
- Parametr wejściowy/wyjściowy IN zmienia się na wartość 9 w ciągu minuty na dokładnie jeden cykl.

Po tym, jak parametr wejściowy/wyjściowy IN zmieni się na wartość 6, instrukcja ocenia, czy parametr uległ zmianie na wartość 9, najwcześniej po 1 sekundzie, lub najpóźniej po jednej minucie. Wyjście OUT (wyjście do zatwierdzenia) jest wtedy ustawiane na 1 przez jeden cykl.

Jeśli została wprowadzona nieprawidłowa wartość lub jeśli parametr wejściowy/wyjściowy IN nie zmienił się na wartość 9 w ciągu jednej minuty bądź zmiana nastąpiła przed upłynięciem jednej sekundy, parametr wejściowy/wyjściowy IN jest resetowany do 0, a oba kroki podane powyżej należy powtórzyć.

Podczas czasu, w którym parametr wejściowy/wyjściowy IN musi zmienić się z 6 na wartość 9, wyjście Q jest ustawiane na 1. W przeciwnym razie na Q utrzymuje się wartość 0.

Każde wywołanie instrukcji „Fail-safe acknowledgment" (Zatwierdzenie fail-safe) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. ACK_OP_DB_1) lub wiele instancji (np. ACK_OP_Instance_1) dla instrukcji „Fail-safe acknowledgment" (Zatwierdzenie fail-safe). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Uwaga

Dla każdego wywołania AKC_OP należy zastosować odrębny obszar danych. Każde wywołanie może być przetwarzane tylko raz w cyklu grupy F-runtime.

F-CPU może przejść w stan STOP, jeśli nie zostanie to wykonane. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

OSTRZEŻENIE

Dwa kroki zatwierdzenia **nie mogą** być wyzwalane przez jedną operację, przykładowo, przez automatyczne zapisanie ich wraz z warunkami czasowymi w programie, a następnie uruchamiane przez pojedynczy przycisk.
Zapewnienie dwóch oddzielnych kroków zatwierdzenia zapobiega również błędnemu wyzwoleniu zatwierdzenia w systemie HMI nieodpornym na uszkodzenia. *(S013)*

OSTRZEŻENIE

W przypadku systemów HMI i F-CPU, które są wzajemnie połączone i użycia instrukcji ACK_OP do zatwierdzenia typu fail-safe, należy upewnić się, że zamierzony F-CPU zostanie zaadresowany **przed** wykonaniem dwóch kroków zatwierdzenia.

- W tym celu należy zapisać nazwę unikalną w całej sieci* dla F-CPU e DB standardowego programu użytkownika dla każdego F-CPU.
- W systemie HMI należy ustawić pole, z którego można odczytać nazwę F-CPU dla DB online przed wykonaniem dwóch kroków zatwierdzenia.
- Opcjonalnie:
  W systemie HMI należy ustawić pole do trwałego zapisu nazwy F-CPU. Następnie można określić, czy zamierzony F-CPU jest adresowany przez zwykłe porównanie odczytu online nazwy F-CPU z trwale zapisaną nazwą. *(S014)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci.

Uwaga

Odczyt wyjścia Q możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika.

Dla każdej instancji instrukcji ACK_OP można zapewnić parametr we/wy IN z oddzielnym słowem pamięci lub DBW z DB standardowego programu użytkownika.

Uwaga

Konfiguracja systemu kontroli operatorskiej i monitorowania nie ma wpływu na zbiorczy podpis bezpieczeństwa.

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Opis (S7-1200, S7-1500)

Ta instrukcja umożliwia zatwierdzenie fail-safe z poziomu systemu HMI. Pozwala, przykładowo, na sterowanie reintegracją F-I/O z systemu HMI. Zatwierdzenie odbywa się w dwóch krokach:

- Parametr wejściowy/wyjściowy IN zmienia się na wartość 6 przez dokładnie jeden cykl.
- Parametr wejściowy/wyjściowy IN zmienia się na wartość wejścia ACK_ID ciągu minuty na dokładnie jeden cykl.

Po tym, jak parametr wejściowy/wyjściowy IN zmieni się na wartość 6, instrukcja ocenia, czy parametr uległ zmianie na wartość wejścia ACK_ID najwcześniej po 1 sekundzie, lub najpóźniej po jednej minucie. Wyjście OUT (wyjście do zatwierdzenia) jest wtedy ustawiane na 1 przez jeden cykl.

Jeśli została wprowadzona nieprawidłowa wartość lub jeśli parametr wejściowy/wyjściowy IN nie zmienił się na wartość wejścia ACK_ID w ciągu jednej minuty bądź zmiana nastąpiła przed upłynięciem jednej sekundy, parametr wejściowy/wyjściowy IN jest resetowany do 0, a oba kroki podane powyżej należy powtórzyć.

Podczas czasu, w którym parametr wejściowy/wyjściowy IN musi zmienić się z 6 na wartość wejścia ACK_ID, wyjście Q jest ustawiane na 1. W przeciwnym razie na Q utrzymuje się wartość 0.

Każde wywołanie instrukcji „Fail-safe acknowledgment" (Zatwierdzenie fail-safe) musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. ACK_OP_DB_1) lub wiele instancji (np. ACK_OP_Instance_1) dla instrukcji „Fail-safe acknowledgment" (Zatwierdzenie fail-safe). Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Uwaga

Dla każdego wywołania AKC_OP należy zastosować odrębny obszar danych. Każde wywołanie może być przetwarzane tylko raz w cyklu grupy F-runtime.

F-CPU może przejść w stan STOP, jeśli nie zostanie to wykonane. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

OSTRZEŻENIE

Dwa kroki zatwierdzenia **nie mogą** być wyzwalane przez jedną operację, przykładowo, przez automatyczne zapisanie ich wraz z warunkami czasowymi w programie, a następnie uruchamiane przez pojedynczy przycisk.
Zapewnienie dwóch oddzielnych kroków zatwierdzenia zapobiega również błędnemu wyzwoleniu zatwierdzenia w systemie HMI nieodpornym na uszkodzenia. *(S013)*

OSTRZEŻENIE

W przypadku systemów HMI i F-CPU, które są wzajemnie połączone i użycia instrukcji ACK_OP do zatwierdzenia typu fail-safe, należy upewnić się, że zamierzony F-CPU zostanie zaadresowany **przed** wykonaniem dwóch kroków zatwierdzenia.

Alternatywa 1:

- Wartość dla każdego identyfikatora zatwierdzenia (wejście ACK_ID; rodzaj danych: INT) można wybrać dowolnie z zakresu od 9 do 30000, lecz musi być unikalna w całej sieci* dla wszystkich instancji instrukcji ACK_OP.
  Należy doprowadzić wartości stałe do wejścia ACK_ID podczas wywoływania instrukcji. Bezpośredni dostęp do odczytu lub zapisu w powiązanej instancji DB jest niedozwolony w programie bezpieczeństwa!

Alternatywa 2:

- Należy zapisać nazwę unikalną w całej sieci* dla F-CPU w DB standardowego programu użytkownika dla każdego F-CPU.
- W systemie HMI należy ustawić pole, z którego można odczytać nazwę F-CPU dla DB online przed wykonaniem dwóch kroków zatwierdzenia.
- Opcjonalnie:

  W systemie HMI należy ustawić pole do trwałego zapisu nazwy F-CPU. Następnie można określić, czy zamierzony F-CPU jest adresowany przez zwykłe porównanie odczytu online nazwy F-CPU z trwale zapisaną nazwą. *(S047)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci.

Uwaga

Odczyt wyjścia Q możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika.

Dla każdej instancji instrukcji ACK_OP należy zapewnić parametr we/wy IN z oddzielnym słowem pamięci lub DBW z DB standardowego programu użytkownika.

Uwaga

Zasilenie wejścia/wyjścia IN instrukcji ACK_OP, a także skonfigurowanie systemu kontroli operatorskiej i monitorowania nie ma wpływu na zbiorczy podpis bezpieczeństwa, zbiorczy podpis F-SW czy podpis bloku, który wywołuje instrukcję ACK_OP.

Zmiany w zasileniu wejścia/wyjścia IN lub konfiguracji systemu kontroli operatorskiej i monitorowania nie skutkują zatem zmianą zbiorczego podpisu bezpieczeństwa / zbiorczego podpisu F-SW / podpisu bloku wywołującego.

OSTRZEŻENIE

Podczas korzystania z instrukcji z przetwarzaniem czasu, należy uwzględnić poniższe źródła niedokładności taktowania podczas określania czasu odpowiedzi:

- Znana nieprecyzyjność taktowania (w oparciu o standardowe systemy) wynikająca z przetwarzania cyklicznego
- Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji (patrz ilustracja w dziale „Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji")
- Tolerancja wewnętrznego monitorowania czasu w F-CPU
  - Dla wartości czasowych do 200 ms, maksymalnie jest to 4 ms
  - Dla wartości czasowych większych lub równych 200 ms, maksymalnie jest to 2% (przypisanej) wartości czasu

Należy dobrać interwał pomiędzy dwoma czasami wywołania instrukcji z przetwarzaniem czasu w taki sposób, by osiągnąć wymagane czasy reakcji, uwzględniając możliwą nieprecyzyjność taktowania. *(S034)*

Parametry (S7-300, S7-400)

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
IN	InOut	INT	Zmienna wejściowa z systemu HMI
OUT	Wyjście	BOOL	Wyjście do zatwierdzenia
Q	Wyjście	BOOL	Status czasu

Parametry (S7-1200, S7-1500)

W poniższej tabeli znajdują się parametry instrukcji:

Parametr	Deklaracja	Rodzaj danych	Opis
ACK_ID	Wejście	INT	Identyfikator zatwierdzenia (9 do 30000)
IN	InOut	INT	Zmienna wejściowa z systemu HMI
OUT	Wyjście	BOOL	Wyjście do zatwierdzenia
Q	Wyjście	BOOL	Status czasu

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

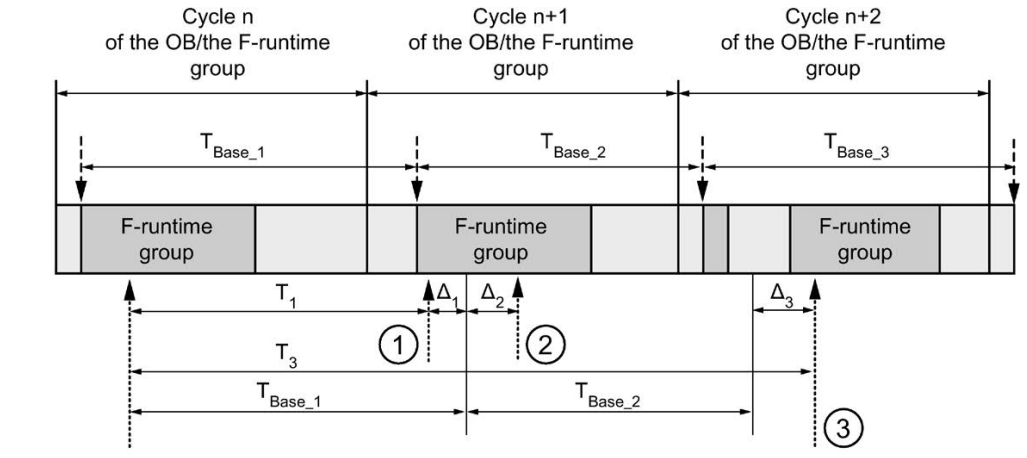
Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	x	—	o	Te wersje są funkcjonalnie identyczne z wersją V1.0 dla F-CPU S7-300/400. W przypadku F-CPU S7-1200/1500 należy również uwzględnić wejście ACK_ID.
1,2	x	o	o	
1,3	x	x	x	

o Ta wersja nie jest już obsługiwana.

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Nieprecyzyjność taktowania wynikająca z czasu aktualizacji podstawy czasowej używanej w instrukcji



----► = Time base update

·····► = Call time of an instruction with time processing

① Dla pierwszego wywołania w cyklu n+1, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się wcześniej niż w cyklu n o wielkość Δ_1, np. z powodu pominięcia części programu bezpieczeństwa grupy F-runtime przed czasem wywołania instrukcji w cyklu n+1. W przypadku czasu aktualizacji, instrukcja uwzględnia czas T_{Base_1} zamiast czasu T_1, który faktycznie upłynął w cyklu n od wywołania.

② Instrukcja jest wywoływana drugi raz w cyklu n+1. Nie obejmuje to kolejnego czasu aktualizacji (o Δ_2).

③ Dla wywołania w cyklu n+2, czas wywołania instrukcji względem uruchomienia grupy F-runtime pojawia się później niż w cyklu n o wielkość Δ_3, np. z powodu zakłócenia grupy F-runtime przez przerwanie wyższego priorytetu przed czasem wywołania instrukcji w cyklu n+2. Instrukcja uwzględniła czas $T_{Base_1} + T_{base_2}$ zamiast czasu T_3, który faktycznie upłynął w cyklu n od wywołania. Obowiązuje to również w przypadku, jeśli w cyklu n+1 nie wystąpiło wywołanie.

Przykład

Przykład zastosowania instrukcji dostępny jest w dziale „Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia nadrzędnego DP lub sterownika IO" (strona 196).

Zobacz także

Wdrażanie rozpoznawania użytkownika w programie bezpieczeństwa w F-CPU dla urządzenia I-slave lub I-device (strona 201)

13.14 Dodatkowe instrukcje

13.14.1 LAD

13.14.1.1 ---| |--- OV: Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400)

Opis

Instrukcja „Get status bit OV" (Pozyskanie bitu stanu) pozwala na wykrycie, czy wystąpiło przepełnienie zakresu numerycznego w ostatniej przetwarzanej instrukcji arytmetycznej.

Instrukcja „Get status bit OV" (Pozyskiwanie bitu stanu OV) działa jak styk normalnie otwarty. Jeśli zapytanie zostanie spełnione, instrukcja ma stan sygnału „1". Jeśli zapytanie nie zostanie spełnione, instrukcja ma stan sygnału „0".

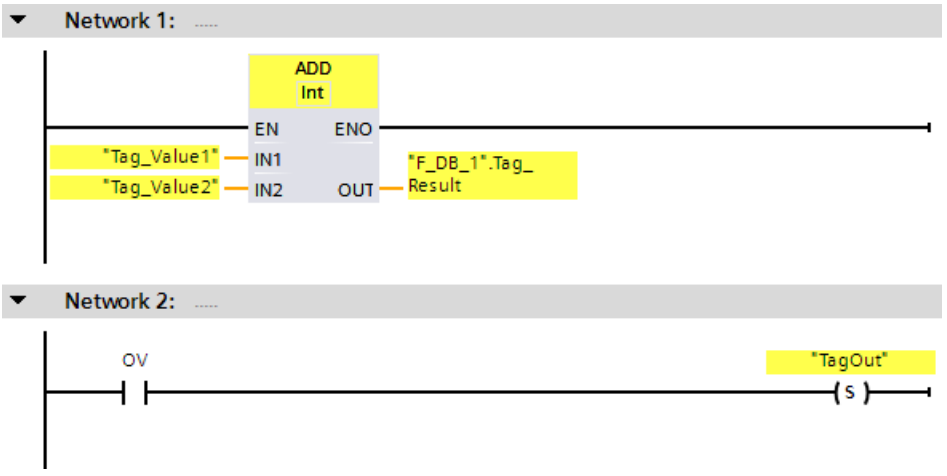
Ocena „Get status bit OV" (Pozyskiwanie bitu stanu OV) musi zostać wstawiona w sieci, która występuje po instrukcji wpływającej na OV. Ta sieć nie może zawierać żadnych etykiet skoku.

Uwaga

Czas wykonania instrukcji wpływającej na OV jest wydłużany, gdy stosowana jest instrukcja „Get status bit OV" (Pozyskanie bitu stanu) (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Add" jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu EN).

Wartość argumentu „Tag_Value1" jest dodawana do wartości argumentu „Tag_Value2". Wynik dodawania jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

W przypadku wykrycia przekroczenia wartości podczas wykonywania instrukcji „Add", bit stanu OV jest ustawiany na „1". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

13.14.1.2 ---| / |--- OV: Pozyskiwanie zanegowanego bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400)

Opis

Instrukcja „Get negated status bit OV" (Pozyskanie zanegowanego bitu stanu) pozwala na wykrycie, czy wystąpiło przepełnienie zakresu numerycznego w ostatniej przetwarzanej instrukcji arytmetycznej. Ta instrukcja jest dostępna jedynie w LAD.

Instrukcja „Get negated status bit OV" (Pozyskiwanie zanegowanego bitu stanu OV) działa jak styk normalnie zamknięty. Jeśli zapytanie zostanie spełnione, instrukcja ma stan sygnału „0". Jeśli zapytanie nie zostanie spełnione, instrukcja ma stan sygnału „1".

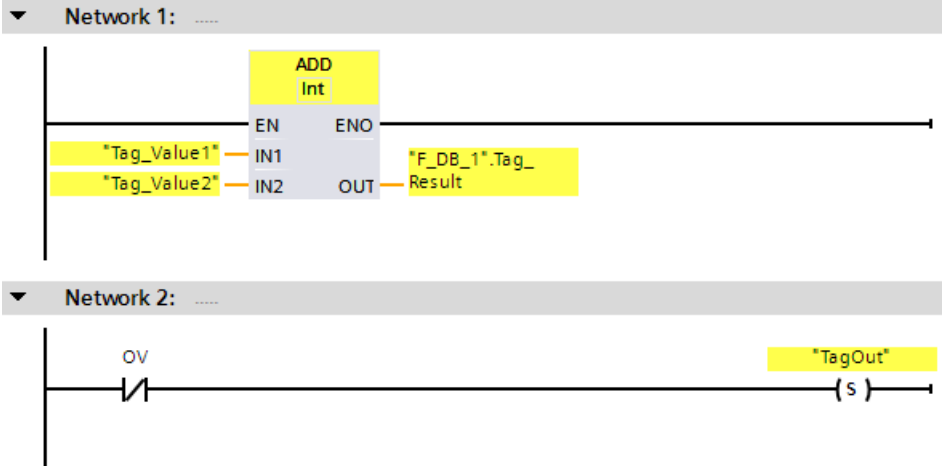
Ocena „Get negated status bit OV" (Pozyskiwanie zanegowanego bitu stanu OV) musi zostać wstawiona w sieci, która występuje po instrukcji wpływającej na OV. Ta sieć nie może zawierać żadnych etykiet skoku.

Uwaga

Czas wykonania instrukcji wpływającej na OV jest wydłużany, gdy stosowana jest instrukcja „Get negated status bit OV" (Pozyskanie zanegowanego bitu stanu) (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Instrukcja „Add" jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu EN).

Wartość argumentu „Tag_Value1" jest dodawana do wartości argumentu „Tag_Value2". Wynik dodawania jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

W przypadku *braku* wykrycia przekroczenia wartości podczas wykonywania instrukcji „Add", bit stanu OV jest ustawiany na „0". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

13.14.2 FBD

13.14.2.1 OV: Pozyskiwanie bitu stanu OV (STEP 7 Safety Advanced V16) (S7-300, S7-400)

Opis

Instrukcja „Get status bit OV" (Pozyskanie bitu stanu) pozwala na wykrycie, czy wystąpiło przepełnienie zakresu numerycznego w ostatniej przetwarzanej instrukcji arytmetycznej.

Ocena „Get status bit OV" (Pozyskiwanie bitu stanu OV) musi zostać wstawiona w sieci, która występuje po instrukcji wpływającej na OV. Ta sieć nie może zawierać żadnych etykiet skoku.

Jeśli zapytanie zostanie spełnione, instrukcja ma stan sygnału „1". Jeśli zapytanie nie zostanie spełnione, instrukcja ma stan sygnału „0".

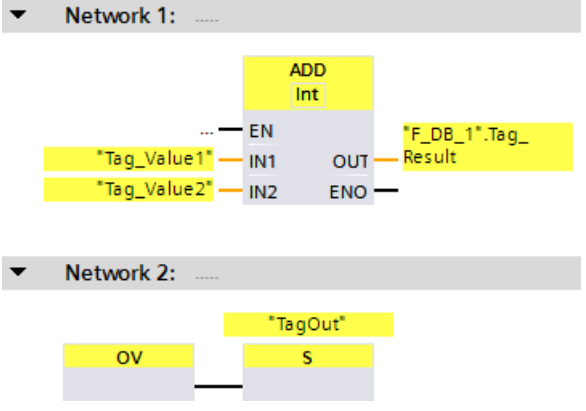
Możliwe jest zaprogramowanie zapytania bitu stanu OV dla „0" za pomocą instrukcji „Invert RLO" (Odwrócenie RLO).

Uwaga

Czas wykonania instrukcji wpływającej na OV jest wydłużany, gdy stosowana jest instrukcja „Get status bit OV" (Pozyskanie bitu stanu) (zobacz również arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100)).

Przykład

Poniższy przykład pokazuje sposób działania instrukcji:



Wartość argumentu „Tag_Value1" jest dodawana do wartości argumentu „Tag_Value2". Wynik dodawania jest przechowywany w argumentzie „"F_DB_1".Tag_Result".

W przypadku wykrycia przekroczenia wartości podczas wykonywania instrukcji „Add", bit stanu OV jest ustawiany na „1". W sieci 2, wykonywane jest następujące zapytanie bit stanu OV, instrukcja „Set output" (S) (Ustaw wyjście), po czym ustawiany jest argument „TagOut".

13.15 Komunikacja

13.15.1 PROFIBUS/PROFINET

13.15.1.1 SENDDP i RCVDP: Wysyłanie i odbiór danych poprzez PROFIBUS DP/PROFINET IO (STEP 7 Safety V16)

Wstęp

Instrukcje SENDDP i RCVDP służą do bezpiecznego wysyłania i odbierania danych wykorzystujących:

- Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie nadrzędne
- Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie nadrzędne do S7 Distributed Safety
- Komunikacja urządzenie nadrzędne bezpieczeństwa – urządzenie I-slave
- Komunikacja urządzenie I-slave bezpieczeństwa – urządzenie I-slave
- Komunikacja sterownik IO bezpieczeństwa – sterownik IO
- Komunikacja sterownik IO bezpieczeństwa – sterownik IO do S7 Distributed Safety
- Komunikacja sterownik IO bezpieczeństwa – I-device
- Komunikacja sterownik IO bezpieczeństwa – urządzenie I-slave

Opis

Instrukcja SENDDP wysyła 16 elementów danych rodzaju BOOL oraz 2 elementy danych rodzaju INT bądź jeden element danych rodzaju DINT (S7-1200, S7-1500) w sposób fail-safe do innego F-CPU poprzez PROFIBUS DP/PROFINET IO. Dane mogą zostać tam odebrane przez powiązaną instrukcję RCVDP.

Każde wywołanie tej instrukcji musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Można tam utworzyć blok danych (pojedynczą instancję) (np.
RCVDP_DB_1) dla tych instrukcji. Po utworzeniu nowego bloku, znajduje się on w folderze „STEP 7 Safety" w drzewku projektu pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe). Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO".
Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Za pomocą instrukcji SENDDP, dane do wysłania (przykładowo, wyjścia innych bloków bezpieczeństwa/instrukcji) są dostępne na wejściu SD_BO_xx, SD_I_xx lub SD_DI_00.

Za pomocą instrukcji RCVDP, odbierane dane są dostępne na wyjściach RD_BO_xx oraz RD_I_xx lub RD_DI_00 do dodatkowego przetwarzania przez inne bloki bezpieczeństwa/instrukcje.

(S7-1200, S7-1500) Na wejściu DINTMODE instrukcji SENDDP określa się, czy dane na wejściach SD_I_00 oraz SD_I_01 lub dane na wejściu SD_DI_00 są wysyłane.

Tryb roboczy F-CPU z instrukcją SENDDP jest zapewniany na wyjściu SENDMODE. Jeśli F-CPU z instrukcją SENDDP ma wyłączony tryb bezpieczeństwa, wyjście SENDMODE = 1.

Komunikacja między F-CPU odbywa się w tle za pomocą specjalnego protokołu bezpieczeństwa. Należy zdefiniować zależność komunikacji pomiędzy instrukcją SENDDP w jednym F-CPU a instrukcją RCVDP w innym F-CPU poprzez określenie identyfikatora komunikacji bezpieczeństwa na wejściach DP_DP_ID instrukcji SENDDP i RCVDP.
Do powiązanych instrukcji SENDDP i RCVDP przypisywane są te same wartości dla DP_DP_ID.

OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście DP_DP_ID; rodzaj danych: INT) można dobiera dowolnie**; jednakże, muszą być przez cały czas unikalne dla wszystkich połączeń komunika związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Unikalność należy sprawdzić w podsumowaniu bezpieczeństwa podczas odbioru programu bezpieczeństwa.

Należy doprowadzić stałe wartości*** do wejść DP_DP_ID oraz LADDR podczas wywoływania instrukcji. Bezpośredni dostęp do zapisu w powiązanej instancji DB do DP_DP_ID oraz LADDR nie jest dozwolony w programie bezpieczeństwa! *(S016)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

** S7-1200/1500: Od wersji V3.0 instrukcji SENDDP i RCVDP, nie jest nawiązywane połączenie na wejściu DP_DP_ID do identyfikatora komunikacji bezpieczeństwa „0".

*** S7-1200/1500: Od wersji V3.0 instrukcji the SENDDP i RCVDP, na wejście DP_DP_ID można również doprowadzać wartości zmienne z globalnego F-DB. W takim przypadku również należy skontrolować podczas odbioru programu bezpieczeństwa, czy zapewniona jest unikalność *przez cały czas*, sprawdzając algorytm do tworzenia wartości zmiennych. Jeśli nie można zagwarantować unikalnego identyfikatora komunikacji bezpieczeństwa podczas uruchomienia programu bezpieczeństwa, ponieważ jest on określany dopiero po uruchomieniu programu, należy upewnić się, że podczas tej fazy wartość na wejściu DP_DP_ID wynosi „0".

Uwaga

W obrębie programu bezpieczeństwa należy przypisać różne adresy początkowe (S7-300/400) lub identyfikatory sprzętowe (S7-1200/1500) dla każdego wywołania instrukcji SENDDP i RCVDP na wejściu LADDR.

Dla każdego wywołania instrukcji SENDDP i RCVDP należy użyć odrębnej instancji DB. Nie należy deklarować i wywoływać tych instrukcji jako instancji wielokrotnych.

(S7-300/400) Wejścia instrukcji RCVDP i RCVS7 nie mogą zawierać poprzedzających operacji logicznych (na przykład „operacji logicznej AND").

Wejścia instrukcji RCVDP nie mogą zostać zainicjowane przy użyciu w pełni kwalifikowanego dostępu DB z wyjściami instrukcji RCVDP lub RCVS7 wywoływanymi w sieci wyższego rzędu.

(S7-1200/1500) Wyjście RD_D_00 nie może być poddawane ocenie dla DINTMODE = 0; wyjścia RD_I_xx instrukcji RCVDP nie mogą być poddawane ocenie dla DINTMODE = 1.

(S7-1200/1500) Wyjścia instrukcji SENDDP i RCVDP nie mogą być zasilone tagami ze standardowego programu użytkownika. Wyjątek: Wyjścia RET_DPRD, RET_DPWR i DIAG.

W pełni kwalifikowany dostęp do DP_DP_ID i LADDR nie jest możliwy w programie

bezpieczeństwa.

Nie jest możliwe użycie rzeczywistego parametru dla wyjścia instrukcji RCVDP, jeśli jest on już używany dla wejścia tej samej lub innej instrukcji RCVDP bądź RCVS7.

F-CPU może przejść w stan STOP, jeśli nie zostanie to wykonane. Przyczyna zdarzenia diagnostycznego jest wprowadzana do bufora diagnostycznego F-CPU.

Uwaga

Niedozwolone jest wstawianie instrukcji SENDDP/RCVDP pomiędzy instrukcję JMP lub JMPN oraz powiązane miejsce docelowe skoku (etykietę skoku).

Nie można wstawić instrukcji RET przed instrukcją SENDDP.

Parametr SENDDP

W poniższej tabeli znajdują się parametry instrukcji SENDDP:

Parametr	Deklaracja	Rodzaj danych	Opis
SD_BO_00	Wejście	BOOL	Dane wysyłane BOOL 00
...			...
SD_BO_15	Wejście	BOOL	Dane wysyłane BOOL 15
SD_I_00	Wejście	INT	Dane wysyłane INT 00
SD_I_01	Wejście	INT	Dane wysyłane INT 01
SD_DI_00	Wejście	DINT	(S7-1200, S7-1500) (ukryte) Dane wysyłane DINT 00
DINTMODE	Wejście	DINT	(S7-1200, S7-1500) (ukryte) 0=SD_I_00 u. SD_I_01 są wysyłane 1=SD_DI_00 jest
DP_DP_ID	Wejście	INT	Identyfikator komunikacji bezp. pomiędzy SENDDP a RCVDP
TIMEOUT	Wejście	TIME	Czas monitorowania w ms dla komunikacji bezp. (zobacz również „Czasy monitorowania i odpowiedzi" (strona 649))
LADDR	Wejście	INT (S7-300, S7-400) HW_SUBMODULE (S7-1200, S7-1500)	Adres początkowy (S7-300, S7-400) lub identyfikator sprzętowy (S7-1200, S7-1500) obszaru adresowego/obszaru transferu: • Dla złącza DP/DP do kom. urz. nadrzędne bezp. – urz. nadrzędne • Do komunikacji urz. nadrzędne związane z bezp. – urz. I-slave • Do komunikacji urz. I-slave związane z bezp. – urz. I-slave • Dla złącza PN/PN komunikacji sterownik IO safety – sterownik IO • Do komunikacji sterownik IO safety – I-device • Do komunikacji sterownik IO safety – urządzenie I-slave
ERROR	Wyjście	BOOL	1=Błąd komunikacji
SUBS_ON	Wyjście	BOOL	1= RCVDP wyprowadza wartości fail-safe
RET_DPRD	Wyjście	WORD	W przypadku kodu błędu innego niż fail-safe RET_VAL dla instrukcji DPRD_DAT (opis kodów błędów, patrz pomoc do instrukcji DPRD_DAT („Extended instructions > Distributed I/O > Other") (Rozszerzone instrukcje > Rozproszone I/O > Inne)).
RET_DPWR	Wyjście	WORD	W przypadku kodu błędu innego niż fail-safe RET_VAL dla instrukcji DPWR_DAT (opis kodów błędów, patrz pomoc do instrukcji DPWR_DAT („Extended instructions > Distributed I/O > Other") (Rozszerzone instrukcje > Rozproszone I/O > Inne)).
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Parametr RCVDP:

W poniższej tabeli znajdują się parametry instrukcji RCVDP:

Parametr	Deklaracja	Rodzaj danych	Opis
ACK_REI	Wejście	BOOL	1=Zatwierdzenie do reintegracji danych wysyłanych po błędzie komunikacji
SUBBO_00	Wejście	BOOL	Wartość fail-safe dla danych odbieranych BOOL 00
...			...
SUBBO_15	Wejście	BOOL	Wartość fail-safe dla danych odbieranych BOOL 15
SUBI_00	Wejście	INT	Wartość fail-safe dla danych odbieranych INT 00
SUBI_01	Wejście	INT	Wartość fail-safe dla danych odbieranych INT 01
SUBDI_00	Wejście	DINT	(S7-1200, S7-1500) (ukryte) Wartość fail-safe dla danych odbieranych DINT 00
DP_DP_ID	Wejście	INT	Identyfikator komunikacji bezpieczeństwa pomiędzy SENDDP a
TIMEOUT	Wejście	TIME	Czas monitorowania w ms dla komunikacji związanej z bezp. (zobacz również „Czasy monitorowania i odpowiedzi" (strona 649))
LADDR	Wejście	INT (S7-300, S7-400) HW_SUBMODULE (S7-1200, S7-1500)	Adres początkowy (S7-300, S7-400) lub identyfikator sprzętowy (S7-1200, S7-1500) obszaru adresowego/obszaru transferu: • Dla złącza DP/DP do komunikacji urz. nadrzędne związane z bezp. – urządzenie nadrzędne • Do komunikacji urz. nadrzędne bezp. – urz. I-slave • Do komunikacji urz. I-slave bezp. – urz. I-slave • Dla złącza PN/PN komunikacji sterownik IO bezp. – sterownik IO • Do komunikacji sterownik IO związany z bezp. – I-device • Do komunikacji sterownik IO związany z bezp. – urządzenie I-slave
ERROR	Wyjście	BOOL	1=Błąd komunikacji
SUBS_ON	Wyjście	BOOL	1= Wartości fail-safe są wyprowadzane
ACK_REQ	Wyjście	BOOL	1 = Wymagane zatwierdzenie do reintegracji danych wysyłanych
SENDMODE	Wyjście	BOOL	1=F-CPU z instrukcją SENDDP w wyłączonym trybie
RD_BO_00	Wyjście	BOOL	Dane odbierane BOOL 00
...			...
RD_BO_15	Wyjście	BOOL	Dane odbierane BOOL 15
RD_I_00	Wyjście	INT	Dane odbierane INT 00
RD_I_01	Wyjście	INT	Dane odbierane INT 01
RD_DI_00	Wyjście	DINT	(S7-1200, S7-1500) (ukryte) Dane odbierane DINT 00
RET_DPRD	Wyjście	WORD	W przypadku kodu błędu innego niż fail-safe RET_VAL dla instrukcji DPRD_DAT (opis kodów błędów, patrz pomoc do instrukcji DPRD_DAT („Extended instructions > Distributed I/O > Other") (Rozszerzone instrukcje > Rozproszone I/O > Inne)).

Parametr	Deklaracja	Rodzaj danych	Opis
RET_DPWR	Wyjście	WORD	W przypadku kodu błędu innego niż fail-safe RET_VAL dla instrukcji DPWR_DAT (opis kodów błędów, patrz pomoc do instrukcji DPWR_DAT („Extended instructions > Distributed I/O > Other") (Rozszerzone instrukcje > Rozproszone I/O > Inne)).
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersja	S7-300/400	S7-1200	S7-1500	Funkcja
1,0	x	—	—	Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.0 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,1	o	—	o	Te wersje mają identyczne funkcje jak wersja V1.0.
1,2	x	—	o	
1,4	x	—	x	
1,3	x	—	o	S7-300/400: Te wersje mają identyczne funkcje jak wersja V1.0. S7-1200/1500: Zamiast 2 danych rodzaju INT, można wysłać/odebrać jedne dane rodzaju DINT. W przeciwnym razie funkcja identyczna z wersją V1.0.
1,5	x	x	x	
2,0	x	x[1]	x[2]	
3,0	x	x[1]	x[2]	S7-300/400: Ta wersja ma identyczne funkcje jak wersja V2.0. S7-1200/1500: • Na wejście DP_DP_ID można również doprowadzić tagi globalnego F- DB. W przypadku DP_DP_ID = 0, połączenie nie jest nawiązywane. • Obsługuje bajt stanu danych złącza PN/PN od V4.0 • Obsługuje symulację komunikacji w pracy S7-PLCISM W przeciwnym razie funkcjonalnie identyczna z wersją V2.0.

o Ta wersja nie jest już obsługiwana.

1 obsługiwane dla wersji oprogramowania V4.2 i wyższej

2 obsługiwane dla wersji oprogramowania V2.0 i wyższej

Po utworzeniu nowego F-CPU w *STEP 7 Safety*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Umieszczenie

Instrukcję RCVDP należy wstawić *albo* na początku głównego bloku bezpieczeństwa, *albo* (z F-CPU S7-1200/1500) w F-FB/F-FC wywoływanym bezpośrednio na początku głównego bloku bezpieczeństwa. Żadna inna instrukcja nie może zostać umieszczona wcześniej w głównym bloku bezpieczeństwa oraz żadna inna instrukcja nie może znaleźć się przed lub po w F-FB/F-FC.

Instrukcję SENDDP należy wstawić *albo* na końcu głównego bloku bezpieczeństwa, *albo* (z F-CPU S7-1200/1500) w F-FB/F-FC wywoływanym bezpośrednio na końcu głównego bloku bezpieczeństwa. Żadna inna instrukcja nie może zostać umieszczona później w głównym bloku bezpieczeństwa oraz żadna inna instrukcja nie może znaleźć się przed lub po w F-FB/F-FC.

Charakterystyka rozpoczęcia pracy

Po uruchomieniu systemów bezpieczeństwa do wysyłania i odbierania, należy po raz pierwszy nawiązać komunikację pomiędzy partnerami (instrukcje SENDDP i RCVDP). W tym czasie odbiorca (instrukcja RCVDP) wyprowadza wartości fail-safe obecne na jej wejściach SUBBO_xx oraz SUBI_xx lub alternatywnie SUBDI_00.

Instrukcje SENDDP i RCVDP sygnalizują to wartością 1 na wyjściu SUBS_ON. Wyjście SENDMODE ma ustawienie domyślne „0" i nie jest aktualizowane, dopóki wyjście SUBS_ON = 1.

Od wersji V3.0 instrukcji the SENDDP i RCVDP, komunikacja jest nawiązywana tylko, gdy DP_DP_ID <> 0.

Zachowanie w razie błędów komunikacji

Jeśli wystąpi błąd komunikacji, przykładowo, z powodu błędu podpisu (CRC) lub przekroczenia czasu monitorowania TIMEOUT bądź dla F-CPU S7-1200/1500 od wersji V3.0 ze względu na zmianę DP_DP_ID na 0 po nawiązaniu komunikacji, ustawiane są wyjścia ERROR i SUBS_ON = 1. Odbiorca (instrukcja RCVDP) wyprowadza wartości fail-safe obecne na jej wejściach SUBBO_xx oraz SUBI_xx lub alternatywnie SUBDI_00. Wyjście SENDMODE nie jest aktualizowane, gdy SUBS_ON = 1.

Dane wysyłane instrukcji SENDDP obecne na wejściach SD_BO_xx oraz SD_I_xx, alternatywnie SD_DI_00, są ponownie wyprowadzane jedynie, gdy błędy komunikacji nie są już wykrywane (ACK_REQ = 1) oraz po zatwierdzeniu (strona 196) instrukcji RCVDP za pomocą zbocza dodatniego na wejściu ACK_REI.

Błędy komunikacji występują również, jeśli wartości DP_DP_ID pomiędzy powiązanymi SENDDP i RCVDP tymczasowo się różnią podczas zmiany wartości zmiennej DP_DP_ID podczas nawiązywania komunikacji.

OSTRZEŻENIE

W przypadku zatwierdzenia użytkownika, należy połączyć wejście ACK_REI z sygnałem generowanym na wejściu operatora.

Wzajemne połączenie z automatycznie generowanym sygnałem nie jest dozwolone.*

(S040)

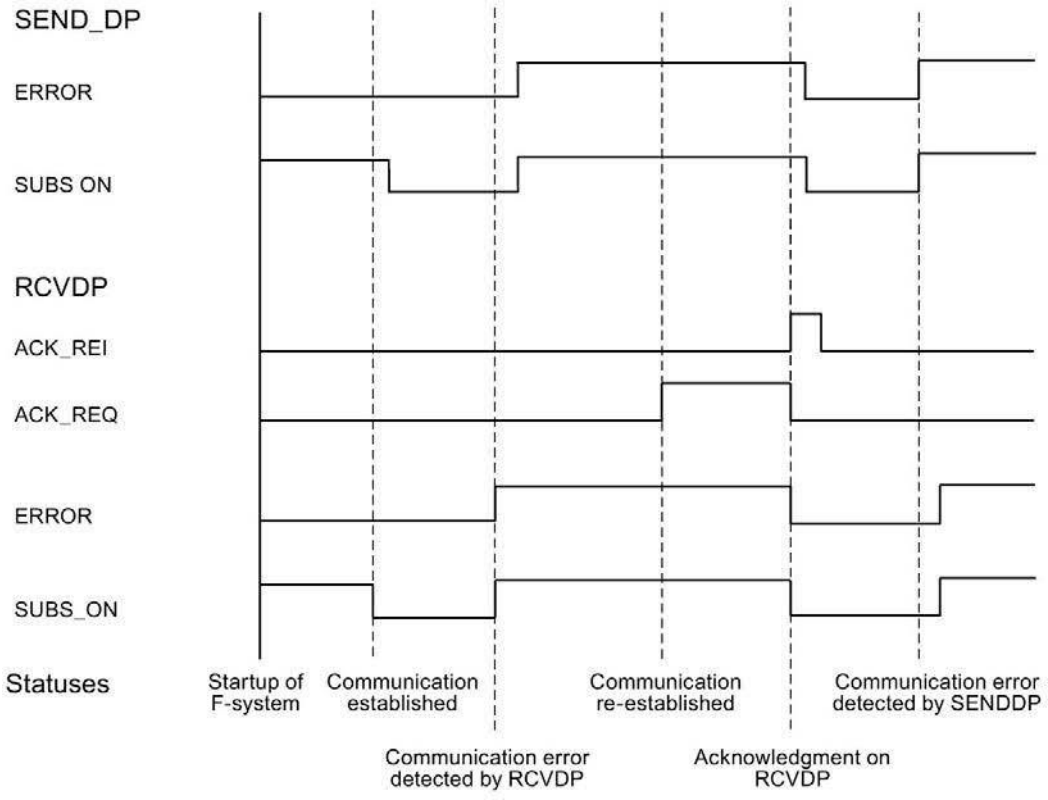
* Jeśli stosowane są zmienne identyfikatory komunikacji bezpieczeństwa, partner komunikacji instrukcji SENDDP lub RCVDP może zostać zmieniony podczas pracy. Wynikowe błędy komunikacji mogą zostać zatwierdzone jedynie przez automatycznie generowany sygnał na wejściu ACK_REI pod następującymi warunkami:

- Program bezpieczeństwa niezawodnie tworzy sygnał „Communication partner change is in progress" (Zmiana partnera komunikacji w toku) z instrukcją RCVDP na podstawie stanu procesowego.
- Sygnał „Communication partner change is in progress" (Zmiana partnera komunikacji w toku) jest dozwolony jedynie w stanie braku błędów komunikacji.
- Gdy sygnał „Communication partner change is in progress" (Zmiana partnera komunikacji w toku) jest aktywny, nie można przeprowadzić oceny otrzymanych wartości procesowych dla instrukcji RCVDP.
- Automatyczne zatwierdzenie może być wykonane jedynie, jeśli dostępny jest sygnał „Communication partner change is in progress" (Zmiana partnera komunikacji w toku).
- Pod względem bezpieczeństwa, automatyczna reintegracja jest dozwolona dla określonego procesu.

Należy pamiętać, że wyjście ERROR (1=błąd komunikacji) dla błędu komunikacji nie zostanie ustawione, o ile komunikacja pomiędzy partnerami (instrukcje SENDDP i RCVDP) nie została wcześniej nawiązana. Jeśli nie można nawiązać komunikacji po uruchomieniu systemów bezpieczeństwa wysyłania i odbierania, należy sprawdzić konfigurację komunikacji CPU safety – CPU, przypisanie parametrów instrukcji SENDDP i RCVDP oraz połączenie magistrali. Informacje o możliwych przyczynach błędu pozyskuje się również poprzez ocenę wyjść DIAG, RET_DPRD i RETDP_WR.

Zazwyczaj należy zawsze wykonywać ocenę RET_DPRD i RETDP_WR, ponieważ możliwe jest, iż tylko jedno z dwóch wyjść będzie zawierać informacje błędu.

Schematy taktowania SENDDP/RCVDP



Wyjście DIAG

Ponadto, informacje innego typu niż fail-safe, dotyczące rodzaju błędów komunikacji, jakie wystąpiły, są zapewniane na wyjściu DIAG instrukcji SENDDP i RCVDP do celów serwisowych.

Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG są zapisywane do czasu zatwierdzenia ich na wejściu ACK_REI instrukcji RCVDP.

Struktura DIAG w instrukcji SENDDP/RCVDP

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Zastrzeżony	—	—
Bit 1	Zastrzeżony	—	—
Bit 2	Zastrzeżony	—	—
Bit 3	Nieprawidłowy DP_DP_ID	DP_DP_ID ma wartość 0.	Sprawdzić DP_DP_ID z SENDDP lub RCVDP.
Bit 4	Wykryto przekroczenie czasu SENDDP/RCVDP	Standardowy program nadpisuje obszary transferu SENDDP i RCVDP.	Sprawdzić standardowy program pod kątem ochrony zapisu do obszarów transferu SENDDP i RCVDP. Uwzględnić również dostęp pośredni.
		DP_DP_ID z SENDDP oraz RCVDP są różne.	Sprawdzić DP_DP_ID z SENDDP oraz RCVDP.
		Dla identyfikatorów komunikacji bezpieczeństwa, wartości zostały zmienione na wejściu DP_DP_ID.	Gdy DP_DP_ID w SENDDP i RCVD znów są spójne, należy wykonać zatwierdzenie na wejściu ACK_REI.
		Zakłócenie w połączeniu magistrali do partnerskiego F-CPU.	Sprawdzić połączenie magistrali i upewnić się, że nie ma zewnętrznych źródeł zakłóceń.
		Nastawa czasu monitorowania dla F-CPU i partnerskiego F-CPU jest zbyt niska.	Sprawdzić przypisany czas monitorowania TIMEOUT dla SENDDP i RCVDP obu F-CPU. W razie potrzeby ustawić wyższą wartość. Ponownie skompilować program bezpieczeństwa.
		Konfiguracja złącza DP/DP lub złącza PN/PN jest nieprawidłowa.	Sprawdzić konfigurację złącza DP/DP lub złącza PN/PN.
		Wskaźnik ważności danych „DIA" na złączu DP/DP jest „ON" (wł).	Należy przełączyć wskaźnik ważności danych „DIA" na przełączniku DIL złącza DP/DP na „OFF" (wył).
		Parametr „Wskaźnik ważności danych DIA" na złączu PN/PN jest aktywny.	Należy wyłączyć parametr „Data validity display DIA" (Wyświetlacz ważności danych DIA) we właściwościach złącza PN/PN.
		Parametr „Aktywuj stan danych" złącza PN/PN (od wersji V4.0) jest aktywny.	Wyłączyć parametr „Aktywuj stan danych" we właściwościach złącza PN/PN (od wersji V4.0) lub S7-1200/1500: Zastosować instrukcje SENDDP i RCVDP w wersji V3.0.
		Usterka wewnętrzna złącza DP/DP lub złącza PN/PN.	Wymienić złącze DP/DP lub złącze PN/PN.
		CP jest w trybie STOP lub wewnętrzna usterka w CP	Przełączyć CP na tryb RUN. Sprawdzić bufor diagnostyczny CP. W razie potrzeby wymienić CP.
		F-CPU/partnerski F-CPU w trybie STOP lub usterka wewnętrzna w F-CPU/partnerskim F-CPU	Przełączyć F-CPU na tryb RUN. Sprawdzić bufor diagnostyczny F-CPU. W razie potrzeby wymienić F-CPU.
Bit 5	Wykryto błąd numeru sekwencji SENDDP/RCVDP	Patrz opis do bitu 4	Patrz opis do bitu 4

Nr bitu	Przypisanie	Możliwa przyczyna błędu	Rozwiązanie
Bit 6	Wykryto błąd CRC na SENDDP/RCVDP	Patrz opis do bitu 4	Patrz opis do bitu 4
		DP_DP_ID z SENDDP oraz RCVDP różne	Kontrola DP_DP_ID z SENDDP oraz RCVDP
Bit 7	Zastrzeżony	—	—

Zobacz także

Komunikacja z S7 Distributed Safety za pomocą połączenia PN/PN (komunikacja sterownik IO – sterownik IO) (strona 266)

Komunikacja z S7 Distributed Safety za pomocą połączenia DP/DP (komunikacja jednostka nadrzędna – jednostka nadrzędna) (strona 267)

Konfiguracja i programowanie komunikacji (S7-300, S7-400) (strona 209)

Komunikacja sterownik IO safety – sterownik IO (strona 212) Komunikacja urządzenie nadrzędne safety – urządzenie nadrzędne (strona 222)

Komunikacja sterownik IO safety – I-device (strona 232) Komunikacja urządzenie nadrzędne safety – urządzenie I-slave (strona 239)

Komunikacja sterownik IO safety – urządzenie I-slave (strona 257)

13.15.2 Komunikacja S7

13.15.2.1 SENDS7 i RCVS7: Komunikacja poprzez połączenia S7 (STEP 7 Safety Advanced V16) (S7-300, S7-400)

Wstęp

Instrukcje SENDS7 i RCVS7 służą do bezpiecznego wysyłania i odbierania danych poprzez połączenia S7.

Uwaga

W *STEP 7 Safety Advanced*, połączenia S7 są zazwyczaj dozwolone jedynie poprzez przemysłowy Ethernet.

Komunikacja safety poprzez połączenia S7 jest możliwa z oraz do F-CPU z interfejsem PROFINET lub F-CPU S7-400 z CP obsługującymi PROFINET. Zobacz również „Komunikacja safety poprzez połączenia S7" (strona 258).

Opis

Instrukcja SENDS7 wysyła dane zawarte w DB komunikacji bezpieczeństwa do DB komunikacji bezpieczeństwa powiązanej instrukcji RCVS7 innego F-CPU w sposób fail-safe, wykorzystując połączenie S7.

Każde wywołanie tej instrukcji musi mieć przypisany obszar danych, w którym zapisane są dane instrukcji. W tym celu otwiera się automatycznie okno „Call options" (Opcje wywołania) po wstawieniu instrukcji do programu. Tam można utworzyć blok danych (pojedynczą instancję) (np. SENDS7_DB_1) lub wiele instancji (np. SENDS7_Instance_1) dla tej instrukcji. Po utworzeniu nowego bloku danych, znajduje się on w drzewku projektu w folderze „STEP 7 Safety" pod hasłem „Program blocks > System blocks" (Bloki programowe > Bloki systemowe) lub, w przypadku instancji wielokrotnej, jako lokalny tag w dziale „Static" (Statyczny) interfejsu bloku. Więcej informacji dostępnych w pomocy do *STEP 7*.

Nie można połączyć włączonego wejścia „EN" oraz włączonego wyjścia „ENO". Dlatego też instrukcja jest zawsze wykonywana (niezależnie od stanu sygnału na włączonym wejściu „EN").

Informacje dotyczące DB komunikacji bezpieczeństwa znajdują się w dziale „ Programowanie komunikacji związanej z bezpieczeństwem poprzez połączenia S7" (strona 261).

DB komunikacji bezpieczeństwa to F-DB do komunikacja CPU safety – CPU ze specjalnymi właściwościami. Należy określić liczbę DB komunikacji bezpieczeństwa na wejściach SEND_DB oraz RCV_DB instrukcji SENDS7 i RCVS7.

Tryb roboczy F-CPU z instrukcją SENDS7 jest zapewniany na wyjściu SENDMODE instrukcji RCVS7. Jeśli F-CPU z instrukcją SENDS7 ma wyłączony tryb bezpieczeństwa, wyjście SENDMODE = 1.

Aby zmniejszyć obciążenie magistrali, można tymczasowo wyłączyć komunikację pomiędzy F-CPU na wejściu EN_SEND instrukcji SENDS7. W tym celu należy doprowadzić na wejście EN_SEND wartość „0" (domyślnie = „1"). W takim przypadku wysyłane dane nie są przesyłane do DB komunikacji bezpieczeństwa powiązanej instrukcji RCVS7, a odbiorca zapewnia wartości fail-safe przez ten okres (wartości początkowe DB komunikacji bezpieczeństwa). Jeśli pomiędzy partnerami nawiązana już była komunikacja, zostanie wykryty błąd komunikacji.

Należy określić lokalny identyfikator - z perspektywy F-CPU - dla połączenia S7 (z tabeli połączeń w widoku sieci) na wejściu ID instrukcji SENDS7 (zobacz również „Konfiguracja" (strona 41)).

Komunikacja między F-CPU odbywa się w tle za pomocą specjalnego protokołu bezpieczeństwa. Należy zdefiniować zależność komunikacji pomiędzy instrukcją SENDS7 w jednym F-CPU a instrukcją RCVS7 innym F-CPU poprzez określenie identyfikatora komunikacji parzystej liczby na wejściu R_ID (instrukcji SENDS7 i RCVS7). Powiązane instrukcje SENDS7 i RCVS7 odbierają tę samą wartość dla R_ID.

OSTRZEŻENIE

Wartości dla odnośnych identyfikatorów komunikacji bezpieczeństwa (wejście R_ID; rodzaj danych: DWORD) można dobierać dowolnie; jednakże, muszą być nieparzyste i unikalne dla wszystkich połączeń komunikacji związanej z bezpieczeństwem w całej sieci* oraz w obrębie CPU. Wartość R_ID + 1 jest przypisywana wewnętrznie i nie należy z niej korzystać.

Należy doprowadzić wartości stałe do wejść ID oraz R_ID podczas wywoływania instrukcji. Bezpośredni dostęp do odczytu lub zapisu w powiązanej instancji DB jest niedozwolony w programie bezpieczeństwa! *(S020)*

*Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/3 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

Uwaga

Dla każdego wywołania instrukcji SENDS7 i RCVS7 w programie bezpieczeństwa należy użyć odrębnej instancji DB. Nie należy deklarować i wywoływać tych instrukcji jako instancji wielokrotnych.

Wejścia instrukcji RCVS7 nie mogą zostać zainicjowane przy użyciu wyjść (przy pomocy w pełni kwalifikowanego dostępu DB) instrukcji RCVS7 lub RCVDP wywoływanymi w sieci wyższego rzędu.

Nie jest możliwe użycie rzeczywistego parametru dla wyjścia instrukcji RCVS7, jeśli jest on już używany dla wejścia tej samej lub innej instrukcji RCVS7 bądź RCVDP.

F-CPU może przejść w stan STOP, jeśli nie zostanie to wykonane. Zdarzenie diagnostyczne jest wprowadzane do bufora diagnostycznego F-CPU.

Uwaga

Nie jest możliwe zaprogramowanie instrukcji SENDS7/RCVS7 pomiędzy instrukcją JMP lub JMPN oraz powiązaną siecią docelową instrukcji JMP lub JMPN.

Nie można wstawić instrukcji RET przed instrukcją SENDS7.

Parametr SENDS7

W poniższej tabeli znajdują się parametry instrukcji SENDS7:

Parametr	Deklaracja	Rodzaj danych	Opis
SEND_DB	Wejście	BLOCK_DB	Liczba DB komunikacji bezpieczeństwa
TIMEOUT	Wejście	TIME	Czas monitorowania w ms dla komunikacji związanej z bezp. (zobacz również „Czasy monitorowania i odpowiedzi" (strona 649))
EN_SEND	Wejście	BOOL	1 = Wysyłanie aktywne
ID	Wejście	WORD	Identyfikator lokalny połączenia S7
R_ID	Wejście	DWORD	Wartość unikalna w całej sieci dla ID komunikacji bezpieczeństwa pomiędzy instrukcją SENDS7 a instrukcją RCVS7
ERROR	Wyjście	BOOL	1=Błąd komunikacji
SUBS_ON	Wyjście	BOOL	1= Blok odbiorczy wyprowadza wartości fail-safe
STAT_RCV	Wyjście	WORD	Parametr stanu innego niż fail-safe STATUS dla instrukcji URCV (opis kodów błędów znajduje się w pomocy do instrukcji URCV („Communication > S7 Communication" (Komunikacja > Komunikacja S7)))
STAT_SND	Wyjście	WORD	Parametr stanu innego niż fail-safe STATUS dla instrukcji USEND (opis kodów błędów znajduje się w pomocy do instrukcji USEND („Communication > S7 Communication" (Komunikacja > Komunikacja S7)))
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Parametr RCVS7

W poniższej tabeli znajdują się parametry instrukcji RCVS7:

Parametr	Deklaracja	Rodzaj danych	Opis
ACK_REI	Wejście	BOOL	Zatwierdzenie do reintegracji danych wysyłanych po błędzie komunikacji
RCV_DB	Wejście	BLOCK_DB	Liczba DB komunikacji bezpieczeństwa
TIMEOUT	Wejście	TIME	Czas monitorowania w ms dla komunikacji związanej z bezp. (zobacz również „Czasy monitorowania i odpowiedzi" (strona 649))
ID	Wejście	WORD	Identyfikator lokalny połączenia S7
R_ID	Wejście	DWORD	Wartość unikalna w całej sieci dla ID komunikacji bezpieczeństwa pomiędzy instrukcją SENDS7 a instrukcją RCVS7
ERROR	Wyjście	BOOL	1=Błąd komunikacji
SUBS_ON	Wyjście	BOOL	1= Wartości fail-safe są wyprowadzane
ACK_REQ	Wyjście	BOOL	1 = Wymagane zatwierdzenie do reintegracji danych
SENDMODE	Wyjście	BOOL	1=F-CPU z instrukcją SENDS7 w wyłączonym trybie bezpieczeństwa
STAT_RCV	Wyjście	WORD	Parametr stanu innego niż fail-safe STATUS dla instrukcji URCV (opis kodów błędów znajduje się w pomocy do instrukcji URCV („Communication > S7 Communication" (Komunikacja > Komunikacja S7)))

Parametr	Deklaracja	Rodzaj danych	Opis
STAT_SND	Wyjście	WORD	Parametr stanu innego niż fail-safe STATUS dla instrukcji USEND (opis kodów błędów znajduje się w pomocy do instrukcji USEND („Communication > S7 Communication" (Komunikacja > Komunikacja S7)))
DIAG	Wyjście	BYTE	Informacja o usłudze bez fail-safe

Wersje instrukcji

Dla tej instrukcji dostępnych jest kilka wersji:

Wersje	S7-300/400	S7-1500	Funkcja
1,0	x	—	
1,1	x	—	Ta wersja ma identyczne funkcje jak wersja V1.0. Obsługuje również starsze wersje wewnętrznie wywoływanych instrukcji. Gdy migrowane są projekty utworzone przy pomocy *S7 Distributed Safety V5.4 SP5*, automatycznie używana jest wersja 1.1 instrukcji. Aby skompilować po raz pierwszy migrowany program bezpieczeństwa przy użyciu *STEP 7 Safety Advanced*, zaleca się, by najpierw zaktualizować do najnowszej dostępnej wersji instrukcji.
1,2	x	—	Ta wersja ma identyczne funkcje jak wersja V1.0/1.1.. Obsługuje również starsze wersje wewnętrznie wywoływanych instrukcji.

Po utworzeniu nowego F-CPU w *STEP 7 Safety Advanced*, dla utworzonego F-CPU automatycznie ustawiana jest najnowsza dostępna wersja.

Więcej informacji odnośnie użycia wersji instrukcji można znaleźć w pomocy do *STEP 7* pod hasłem „Korzystanie z wersji instrukcji".

Umieszczenie

Instrukcja RCVS7 musi zostać wstawiona na początku głównego bloku bezpieczeństwa. Nie można przed nią wstawić żadnej innej instrukcji.

Instrukcja SENDS7 musi zostać wstawiona na końcu głównego bloku bezpieczeństwa. Nie można za nią wstawić żadnej innej instrukcji.

Charakterystyka rozpoczęcia pracy

Po uruchomieniu systemów bezpieczeństwa do wysyłania i odbierania, należy po raz pierwszy nawiązać komunikację pomiędzy partnerami (instrukcje SENDS7 i RCVS7). Odbiorca (instrukcja RCVS7) zapewnia wartości fail-safe przez ten okres (wartości początkowe w jego DB komunikacji bezpieczeństwa).

Instrukcje SENDS7 i RCVS7 sygnalizują to wartością 1 na wyjściu SUBS_ON. Wyjście SENDMODE (instrukcja RCVS7) ma ustawienie domyślne „0" i nie jest aktualizowane, dopóki wyjście SUBS_ON = 1.

Zachowanie w razie błędów komunikacji

W razie wystąpienia błędu komunikacji, przykładowo, ze względu na błąd podpisu (CRC) lub przekroczenia czasu monitorowania TIMEOUT, ustawiane są wyjścia ERROR oraz nd SUBS_ON = 1. Odbiorca (instrukcja RCVS7) zapewnia wtedy wartości fail-safe (wartości początkowe w jego DB komunikacji bezpieczeństwa). Wyjście SENDMODE nie jest aktualizowane, gdy SUBS_ON = 1.

Dane wysyłane obecne w DB komunikacji bezpieczeństwa (instrukcja SENDS7) nie są wyprowadzane, dopóki nie będzie wykrywanych błędów komunikacji (ACK_REQ = 1) i zostanie wykonane zatwierdzenie (strona 196) dodatnim zboczem na wejściu ACK_REI instrukcji RCVS7.

⚠ OSTRZEŻENIE

W przypadku zatwierdzenia użytkownika, należy połączyć wejście ACK_REI z sygnałem generowanym na wejściu operatora.

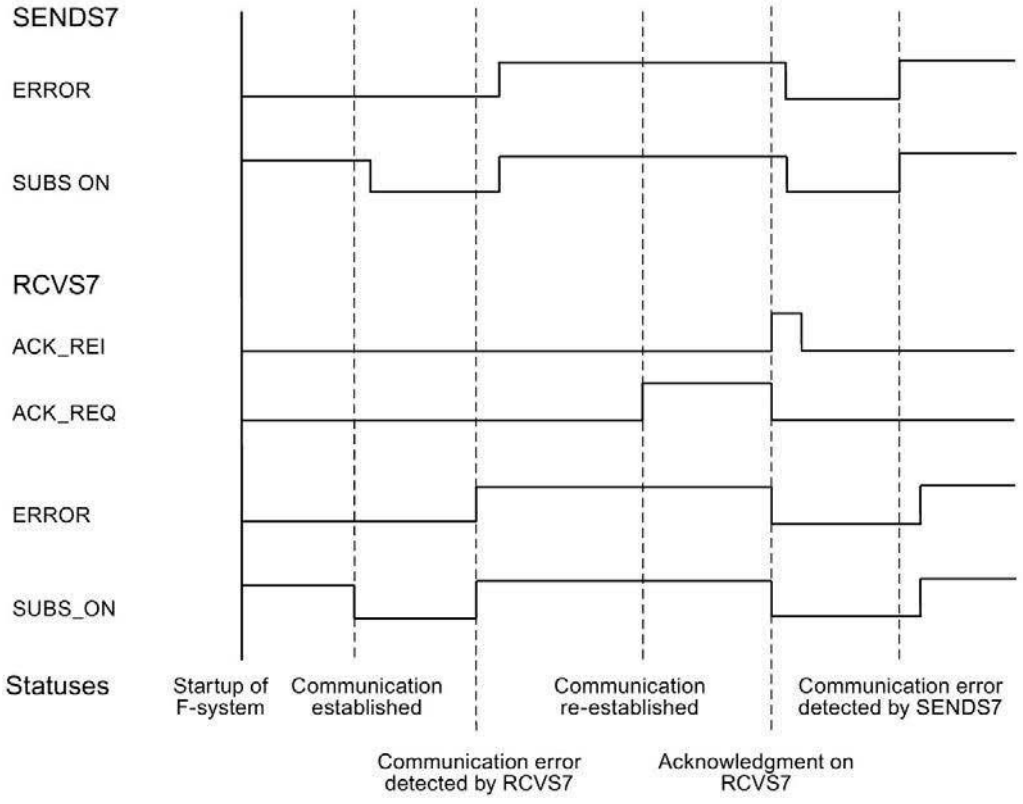
Wzajemne połączenie z automatycznie generowanym sygnałem nie jest dozwolone. *(S040)*

Należy pamiętać, że wyjście ERROR (1=błąd komunikacji) zostanie ustawione po raz pierwszy na błąd komunikacji, jeśli komunikacja została już nawiązana pomiędzy partnerami (instrukcje SENDS7 i RCVS7). Jeśli nie można nawiązać komunikacji po uruchomieniu systemów bezpieczeństwa wysyłania i odbierania, należy sprawdzić konfigurację komunikacji CPU safety – CPU, przypisanie parametrów instrukcji SENDS7 i RCVS7 oraz połączenie magistrali. Możliwe jest również uzyskanie informacji o możliwych przyczynach błędu poprzez wykonanie oceny wyjść STAT_RCV i STAT_SND.

Zazwyczaj należy zawsze wykonywać ocenę STAT_RCV i STAT_SND, ponieważ możliwe jest, iż tylko jedno z dwóch wyjść będzie zawierać informacje błędu.

Jeśli jeden z bitów DIAG jest ustawiony na wyjściu DIAG, należy również sprawdzić, czy długość i struktura powiązanego DB komunikacji bezpieczeństwa po obu stronach komunikacji są zgodne.

Schematy taktowania SENDS7 i RCVS7



Wyjście DIAG

Informacje inne niż fail-safe dotyczące rodzaju błędów komunikacji, które wystąpiły, są dostępne na wyjściu DIAG do celów serwisowych. Odczyt tych informacji możliwy jest poprzez system kontroli operatorskiej i monitorowania, lub, jeśli to możliwe, można ocenić je w standardowym programie użytkownika. Bity DIAG są zapisywane do czasu zatwierdzenia ich na wejściu ACK_REI powiązanej instrukcji RCVS7.

Struktura DIAG

Nr bitu	Przypisanie SENDS7 i RCVS7	Możliwa przyczyna błędu	Rozwiązanie
Bit 0	Zastrzeżony	—	—
Bit 1	Zastrzeżony	—	—
Bit 2	Zastrzeżony	—	—
Bit 3	Zastrzeżony	—	—
Bit 4	Wykryto przekroczenie czasu przez SENDS7 i RCVS7	Usterka w połączeniu magistrali do partnerskiego F-CPU	Sprawdzić połączenie magistrali i upewnić się, że nie ma zewnętrznych
		Nastawa czasu monitorowania dla F-CPU i partnerskiego F-CPU jest zbyt niska	Sprawdzić przypisany czas monitorowania TIMEOUT dla SENDS7 i RCVS7 obu F-CPU. Jeśli to możliwe, ustawić większą wartość. Ponownie skompilować program bezpieczeństwa
		CP jest w trybie STOP lub wewnętrzna usterka w CP	• Przełączyć CP w tryb RUN • Sprawdzić bufor diagnostyczny CP • W razie konieczności wymienić CP
		F-CPU/partnerski F-CPU w trybie STOP lub usterka wewnętrzna w F-CPU/partnerskim F-CPU	• Przełączyć F-CPU w tryb RUN • Sprawdzić bufor diagnostyczny F-CPU • W razie konieczności wymienić F-CPU
		Komunikacja została wyłączona z EN_SEND = 0.	Ponownie włączyć komunikację na powiązanej SENDS7 za pomocą EN_SEND = 1.
		Połączenie S7 uległo zmianie, przykładowo, adres IP CP uległ zmianie	Skompilować ponownie program bezpieczeństwa i pobrać go do F-CPU
Bit 5	Wykryto błąd numeru sekwencji dla SENDS7 i RCVS7	Patrz opis do bitu 4	Patrz opis do bitu 4
Bit 6	Wykryto błąd CRC dla SENDS7 i RCVS7	Patrz opis do bitu 4	Patrz opis do bitu 4
Bit 7	RCVS7: Nie można nawiązać komunikacji	Konfiguracja komunikacji CPU safety – CPU jest nieprawidłowa, przypisanie parametrów instrukcji SENDS7 i RCVS7 jest nieprawidłowe Zobacz również opis do bitu 4	Sprawdzić konfigurację komunikacji CPU safety – CPU, przypisanie parametrów instrukcji SENDS7 i RCVS7 jest nieprawidłowe Zobacz również opis do bitu 4
	SENDS7: Zastrzeżony	—	—

Czasy monitorowania i

A

Wstęp

W tym dziale można poznać:

- Które określone czasy monitorowania bezpieczeństwa wymagają konfiguracji
- Jakie zasady należy przestrzegać podczas określania czasów
- monitorowania Gdzie wprowadzić określone czasy monitorowania
- bezpieczeństwa

  Jakie zasady należy przestrzegać w przypadku maksymalnego czasu odpowiedzi

Wsparcie obliczeń

Na stronie internetowej dostępny jest arkusz kalkulacyjny (http://support.automation.siemens.com/WW/view/en/49368678/133100) pomagający w obliczaniu przybliżonych czasów pracy grup F-runtime, minimalnego czasu monitorowania bezpieczeństwa oraz maksymalnych czasów odpowiedzi systemu bezpieczeństwa.

Informacje dodatkowe

Czasy monitorowania i odpowiedzi dla części standardowej są obliczane w SIMATIC Safety identycznie jak w przypadku standardowych systemów automatyzacji S7-300, S7-400, S7-1200 i S7-1500 i nie zostały tu opisane. Opis tego obliczania można znaleźć w *instrukcji sprzętowej do CPU*.

A.1 Konfigurowanie czasów

Czasy monitorowania do skonfigurowania

Należy skonfigurować następujące czasy

Monitorowanie...	Nastawy...	Parametry	Zobacz
Czas cyklu bezpieczeństwa lub limit ostrzeżenie czasu cyklu grup F-runtime zawierających program bezpieczeństwa	w *Safety Administration Editor*: • Okno do definiowania grupy F-runtime	Maksymalny czas cyklu grupy F-runtime	• Procedura definiowania grupy F-runtime (S7-300, S7-400) (strona 141) • Procedura definiowania grupy F-runtime (S7-1200, S7-1500) (strona 145)
komunikacji związanej z bezpieczeństwem pomiędzy F-CPU a F-I/O poprzez PROFIsafe (czas monitorowania PROFIsafe)	w *edytorze sieci i sprzętu*: • Centralnie, podczas konfiguracji F-CPU; właściwości F- CPU; • lub podczas konfiguracji F-I/O; właściwości F-I/O	Czas monitorowania bezpieczeństwa F_WD_TIME	• Konfiguracja F-CPU (strona 46) • Konfiguracja F-I/O (strona 51) • Specjalne przypadki konfiguracji urządzeń podrzędnych DP opartych na GSD fail-safe oraz urządzeń I/O fail-safe opartych na GSD (strona 76)
komunikacji CPU safety – CPU	Na wejściu TIMEOUT instrukcji: • SENDDP; RCVDP; SENDS7; RCVS7	TIMEOUT	• Komunikacja (strona 631)
(S7-1200, S7-1500) Komunikacja z użyciem Flexible F-Link	w Safety Administration Editor: • obszar „Flexible F-Link"	Czas monitorowania bezpieczeństwa komunikacji bezpieczeństwa	• Obszar „Flexible F-Link" (S7-1200, S7-1500) (strona 98) • Komunikacja grupy F-runtime (S7-1200, S7-1500) (strona 154) • Konfiguracja i programowanie komunikacji z użyciem Flexible F-Link (S7-1200, S7-1500) (strona 312)

(S7-300, S7-400) Nie jest konieczne konfigurowanie czasu monitorowania komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime.

Zasady konfigurowania czasów monitorowania

Podczas konfigurowania czasów monitorowania należy uwzględnić dostępność, a także bezpieczeństwo systemu:

- Dostępność: Aby zapewnić, że monitorowanie czasu nie zostanie wyzwolone w przypadku braku błędu, czasy monitorowania muszą być wystarczająco długie.
- Bezpieczeństwo: Aby zapewnić, że czas bezpieczeństwa procesu nie zostanie przekroczony, wybrane czasy monitorowania muszą być wystarczająco krótkie.

OSTRZEŻENIE

Zagwarantowanie (z perspektywy fail-safe), że stan przekazywanego sygnału zostanie uzyskany po stronie nadawcze i przeniesiony do odbiorcy jest możliwe jedynie, jeśli poziom sygnału utrzymuje się co najmniej tak długo jak przypisany czas monitorowania. *(S018)*

Ogólna procedura konfigurowania czasów monitorowania

Do konfigurowania czasów monitorowania należy użyć poniższej procedury:

1. Skonfigurować standardowy system.
   Należy odnieść się do odpowiednich *instrukcji sprzętowych* oraz *pomocy do STEP 7*, by uzyskać niezbędne informacje.
2. Skonfigurować określone czasy monitorowania systemu bezpieczeństwa z uwzględnieniem dostępności. Przy pomocy arkusza kalkulacyjnego (http://support.automation.siemens.com/WW/view/en/49368678/133100) można obliczyć przybliżony minimalny czas monitorowania.
   Przy pomocy arkusza można obliczyć maksymalny czas odpowiedzi i skontrolować, czy
3. czas bezpieczeństwa procesu nie został przekroczony. W razie potrzeby należy skrócić określone czasy monitorowania systemu bezpieczeństwa.

A.1.1 Minimalny czas monitorowania dla czasu cyklu grupy F-runtime

Parametr „Maximum cycle time of the F-runtime group" (Maksymalny czas cyklu grupy F-runtime)

Czas monitorowania dla czasu cyku grupy F-runtime konfiguruje się w *Safety Administration Editor,* w obszarze roboczym do definiowania grupy F-runtime (strona 139).

Aby nie dopuścić do aktywowania monitorowania cyklu grupy F-runtime, gdy nie ma aktywnych usterek i tym samym dopuścić do zatrzymania F-CPU, należy ustawić odpowiednio wysoki maksymalny czas cyklu grupy F-runtime.

Przy pomocy arkusza kalkulacyjnego (http://support.automation.siemens.com/WW/view/en/49368678/133100) można określić minimalny czas monitorowania dla czasu cyklu grupy F-runtime. Należy zwrócić uwagę na komentarze w pliku arkusza.

W przypadku F-CPU S7-1200/1500, można również użyć „Limitu ostrzeżenia czasu cyklu grupy F-runtime" (strona 145), „Maksymalnego czasu cyklu grupy F-runtime" (strona 145) oraz tagów TCYC_CURR (strona 158) i TCYC_LONG (strona 158) do odpowiedniego ustawienia parametrów.

A.1.2 Minimalny czas monitorowania dla komunikacja związanej z bezpieczeństwem pomiędzy F-CPU a F-I/O

Parametr „F-monitoring time" (Czas monitorowania bezpieczeństwa)

Dostępne są dwie opcje konfiguracji czasu monitorowania komunikacji związanej z bezpieczeństwem pomiędzy F-CPU a F-I/O:

- Centralnie, w *edytorze sprzętu i sieci* podczas przypisywania parametrów F-CPU (strona 46); we właściwościach F-CPU, lub
- podczas przypisywania parametrów F-I/O (strona 51) w *edytorze sprzętu i sieci*; we właściwościach F-I/O

„Czas monitorowania bezpieczeństwa" = Czas monitorowania PROFIsafe T_{PSTO}

Określony czas monitorowania PROFIsafe T_{PSTO} musi być odpowiednio wysoki, by nie powodować wyzwalania monitorowania czasu cyklu bezpieczeństwa, gdy nie wystąpiły żadne usterki.

Przy pomocy arkusza kalkulacyjnego (http://support.automation.siemens.com/WW/view/en/49368678/133100) można obliczyć czas odpowiedzi dostępny dla SIMATIC Safety w celu ustalenia minimalnego czasu monitorowania komunikacji związanej z bezpieczeństwem pomiędzy F-CPU a F-I/O.

Należy zwrócić uwagę na komentarze w pliku arkusza.

Kontrola określająca, czy czas monitorowania PROFIsafe jest zbyt krótki

Uwaga

Podczas odbioru systemu bezpieczeństwa można wykonać kontrolę przy aktywnym trybie bezpieczeństwa, by określić, czy skonfigurowany czas monitorowania PROFIsafe nie jest za krótki.

Kontrola tego czasu pozwala na upewnienie się, iż skonfigurowany czas monitorowania wystarczająco przekracza minimalny czas monitorowani. W ten sposób można uniknąć wystąpienia sporadycznych błędów czasu monitorowania.

Procedura:

1. Wstawić F-I/O (taki, który nie będzie później potrzeby do pracy systemu).
2. Przypisać krótszy czas monitorowania dla tego F-I/O niż dla F-I/O w systemie.
3. Jeśli dodatkowy F-I/O wskaże usterkę i zostanie wydany komunikat diagnostyczny „Monitoring time for safety message frame exceeded" (Czas monitorowania dla ramki komunikatu bezpieczeństwa przekroczony), oznacza to ustawienie poniżej minimalnego
4. możliwego czasu monitorowania PROFIsafe.
   Należy zwiększać czas monitorowania dodanego F-I/O do chwili, gdy nie będzie wskazywać usterki. Ten czas monitorowania odpowiada w przybliżeniu minimalnemu możliwemu czasowi monitorowania.

Warunki:

Wstawiany dodatkowo F-I/O oraz F-I/O, dla którego sprawdza się czas monitorowania PROFIsafe, muszą mieć wspólne następujące właściwości:

- Muszą być wstawione na tym samym regale
- Muszą być węzłami w tej samej podsieci

Wskazówka:

Rozsądnym działaniem może być pozostawienie dodatkowego F-I/O dla systemów, które będą modyfikowane lub rozbudowywane podczas eksploatacji po odbiorze technicznym. Ten F-I/O zapewni wczesne ostrzeżenie w przypadku zmian w zachowaniu czasowym, pozwalając na uniknięcie przestoju procesu wskutek awarii F-I/O systemowego.

A.1.3 Minimalny czas monitorowania komunikacji CPU safety – CPU

Wejście TIMEOUT na SENDDP oraz RCVDP lub SENDS7 i RCVS7/czas monitorowania bezpieczeństwa dla komunikacji poprzez Flexible F-Link

Monitorowanie czasu odbywa się w instrukcjach SENDDP oraz RCVDP (strona 631) lub SENDS7 oraz RCVS7 (strona 642) partnera komunikacyjnego. Należy przypisać monitorowanie identycznego czasu dla obu instrukcji na wejściu TIMEOUT.

Czas monitorowania TIMEOUT należy ustawić wystarczająco duży, by nie doszło do uruchomienia monitorowania, gdy nie doszło do usterki.

Dla komunikacji poprzez Flexible F-Link ustala się czas monitorowania bezpieczeństwa dla komunikacji podczas jej tworzenia (strona 98).

Przy pomocy arkusza kalkulacyjnego (http://support.automation.siemens.com/WW/view/en/49368678/133100) można obliczyć czas odpowiedzi dostępny dla SIMATIC Safety w celu ustalenia minimalnej wartości dla parametru TIMEOUT czasu monitorowania bezpieczeństwa.

Należy zwrócić uwagę na komentarze w pliku arkusza.

A.1.4 Czas monitorowania dla komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime

Czas monitorowania dla komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime (S7-300, S7-400)

Czas monitorowania dla komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime jest określany automatycznie z wartości dla „Maksymalny czas cyklu grupy F-runtime" (obszar roboczy definiowania grupy F-runtime (strona 139) w *Safety Administration Editor*).

Czas monitorowania = (maksymalny czas cyklu dla 1. grupy F-runtime) + (maksymalny czas cyklu dla 2. grupy F-runtime)

Czas monitorowania dla komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime (S7-1200, S7-1500)

Obliczenie czasu monitorowania komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime możliwe jest z wartości „Maksymalny czas cyklu grupy F-runtime" (obszar roboczy definiowania grupy F-runtime (strona 139) w Safety Administration Editor)m jeśli umieści się domyślny program użytkownika dla komunikacji grupy F-runtime w przetwarzaniu wstępnym/końcowym (strona 86).

Czas monitorowania = (maksymalny czas cyklu dla 1. grupy F-runtime) + (maksymalny czas cyklu dla 2. grupy F-runtime)

A.2 Czasy odpowiedzi funkcji

Definicja czasu odpowiedzi

Czas odpowiedzi to okres od wykrycia sygnału wejściowego do zmiany powiązanego sygnału wyjściowego.

Zakres fluktuacji

Rzeczywisty czas odpowiedzi mieści się pomiędzy minimalnym a maksymalnym czasem odpowiedzi. W konfiguracji systemu zawsze należy uwzględniać maksymalny czas.

Zasady maksymalnego czasu odpowiedzi funkcji bezpieczeństwa

Maksymalny czas odpowiedzi funkcji bezpieczeństwa musi być krótszy niż czas bezpieczeństwa procesu.

Definicja czasu bezpieczeństwa procesu

Czas bezpieczeństwa procesu to okres pomiędzy wystąpieniem błędu, podczas którego proces może pozostać aktywny bez spowodowania urazu personelu lub uszkodzenia środowiska, a chwilą ukończenia odpowiedzi.

Sterowanie systemu bezpieczeństwa może wykonać dowolną kontrolę podczas czasu bezpieczeństwa procesu, co obejmuje jego nieprawidłowość lub całkowity brak. Czas bezpieczeństwa procesu zależy od rodzaju procesu i wymaga określenia zależnie od przypadku.

Procedura obliczania czasu odpowiedzi

Arkusz kalkulacyjny do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100) pozwala na określenie maksymalnego czasu odpowiedzi funkcji bezpieczeństwa.

Przy pomocy arkusza można obliczyć maksymalny czas odpowiedzi funkcji bezpieczeństwa, a następnie sprawdzić, czy czas bezpieczeństwa procesu nie został przekroczony.

W razie potrzeby należy zmniejszyć określone czasy monitorowania systemu bezpieczeństwa (patrz Minimalny czas monitorowania komunikacji związanej z bezpieczeństwem pomiędzy F-CPU a F-I/O (strona 652)).

OSTRZEŻENIE

Możliwe jest skorzystanie z arkusza kalkulacyjnego do obliczenia czasu odpowiedzi lub przekroczenia czasu oczekiwania podczas korzystania z komunikacji Flexible F-Link, jeśli zastosowano poniższe wskazówki dotyczące standardowych instrukcji spójnej transmisji danych:

Komunikacja CPU-CPU (strona 312)

Należy wywołać standardową instrukcję dla spójnego wysyłania danych oraz zatwierdzenia przetwarzania końcowego grupy F-runtime (strona 86). Korzystając ze standardowej instrukcji do odbierania danych i zatwierdzania w spójny sposób, należy rozróżnić, czy standardowe połączenie komunikacji jest jednoznaczne. W przypadku jednoznaczny połączeń (takich jak DPRD_DAT / DPWR_DAT), konieczne jest wywołanie standardowej instrukcji w przetwarzaniu wstępnym grupy F-runtime (strona 86). Jeśli połączenie nie jest jednoznaczne (np. połączenie S7, połączenia TCP), należy wywołać standardową instrukcję w cyklicznym przerwaniu OB. Musi być ono wywoływane w interwałach krótszych niż grupa F-runtime. Zalecany jest do tego współczynnik 1:5.

Komunikacja grupy F-runtime (strona 154)

Do wysłania danych w przetwarzaniu końcowym nadawczej grupy F-runtime, należy wywołać standardową instrukcję UMOVE_BLK. Do wysłania zatwierdzenia w przetwarzaniu końcowym odbiorczej grupy F-runtime, należy wywołać standardową instrukcję UMOVE_BLK. *(S089)*

OSTRZEŻENIE

Czas odpowiedzi funkcji bezpieczeństwa zależy, między innymi, od czasu cyklu F-OB, czasu pracy grupy F-runtime, oraz, w przypadku stosowania rozproszonego F-I/O, przypisania parametrów PROFINET/PROFIBUS.

Dlatego też przypisanie parametrów/konfiguracja standardowego systemu wpływa na czas odpowiedzi funkcji bezpieczeństwa.

Przykłady:

- Zwiększenie pierwszeństwa standardowego OB w porównaniu do F-OB może wydłużyć czas cyklu dla F-BO lub czas pracy grupy F-runtime ze względu na przetwarzanie priorytetowe standardowego OB. Należy pamiętać, że podczas tworzenia obiektów technologicznych, mogą zostać automatycznie utworzone OB o bardzo wysokim priorytecie.
- Zmiana w cyklu zegara wysyłania PROFINET zmienia czas cyklu F-OB z klasą zdarzenia „Cykl synchroniczny".

Należy pamiętać, że konfiguracja / przypisanie parametrów standardowego systemu nie podlega ochronie dostępu do programu bezpieczeństwa i nie prowadzi do modyfikacji zbiorczego podpisu bezpieczeństwa.

Jeśli nie zastosowano środków organizacyjnych mających na celu uniemożliwienie zmian w konfiguracji / przypisaniu parametrów standardowego systemu z wpływem na czas odpowiedzi, należy zawsze korzystać z czasów monitorowania do obliczania maksymalnego czasu odpowiedzi funkcji bezpieczeństwa (patrz „Konfigurowanie czasów monitorowania" (strona 650)).

Czasy monitorowania są chronione przed zmianą za pomocą ochrony dostępu programu bezpieczeństwa i są rejestrowane przez zbiorczy podpis bezpieczeństwa, a także przez zbiorczy podpis F-SW,

W przypadku korzystania z arkusza kalkulacyjnego do obliczania czasu odpowiedzi (http://support.automation.siemens.com/WW/view/en/49368678/133100), należy uwzględnić wartość, która została określona dla „Any standard system runtimes" (Dowolne czasy pracy standardowego systemu) jako wartość maksymalnego czasu odpowiedzi. *(S085)*

Lista kontrolna

B

Cykl użytkowania systemów automatyki typu fail-safe

Poniższa tabela zawiera listę kontrolną podsumowującą wszystkie czynności w cyklu użytkowania systemu fail-safe SIMATIC Safety, w tym wymogi i zasady, jakie należy przestrzegać przy danej czynności.

Lista

Legend

- Samodzielne działy odnoszą się do niniejszej dokumentacji.
- *„Podręcznik F-SM"* odnosi się do podręcznika „System automatyzacji S7-300, system I/O rozproszonych ET 200M, moduły sygnałowe fail-safe" (http://support.automation.siemens.com/WW/view/en/19026151).
- *„Podręcznik moduły bezpieczeństwa"* odnosi się do podręcznika „System I/O rozproszonych ET 200S, moduły fail-safe" (http://support.automation.siemens.com/WW/view/en/27235629).
- *„Podręcznik ET 200eco"* odnosi się do podręcznika „Stacja I/O rozproszonych ET 200eco, moduły I/O fail-safe" (
- http://support.automation.siemens.com/WW/view/en/19033850).

  „Podręcznik ET 200eco PN" odnosi się do podręcznika „ET 200eco PN F-DI 8 x 24 VDC, 4xM12 / F-DQ 3 x 24 VDC/2.0A PM, 3xM12."
- (https://support.industry.siemens.com/cs/search?search=6ES7146-6FF00-0AB0&type=Manual&lc=en-US).
- *„Podręcznik ET 200pro"* odnosi się do podręcznika „System I/O rozproszonych ET 200pro, moduł I/O fail-safe" (
- http://support.automation.siemens.com/WW/view/en/22098524).

  „Podręcznik ET 200iSP" odnosi się do podręcznika „Urządzenie I/O rozproszonych ET
- 200iSP, moduły fail-safe" (http://support.automation.siemens.com/WW/view/en/47357221).
- *„Podręcznik ET 200SP"* odnosi się do podręcznika „System ET 200SP" (http://support.automation.siemens.com/WW/view/en/58649293).
- *„Podręcznik ET 200MP"* odnosi się do podręcznika „System I/O rozproszonych S7-1500/ET 200MP" (http://support.automation.siemens.com/WW/view/en/59191792).

  „Podręcznik moduły ET 200SP" odnosi się do instrukcji obsługi urządzeń modułów bezpieczeństwa do systemu I/O rozproszonych ET 200SP (https://support.industry.siemens.com/cs/ww/en/ps/14059/man)

Faza	Należy mieć na uwadze co następuje	Odniesienia	Kontrola
Planowanie			
Wymogi: „Specyfikacja wymogów bezpieczeństwa" dostępna dla zamierzonej aplikacji	Zależne od procesu	—	
Specyfikacja architektury systemu	Zależne od procesu	—	
Przypisanie funkcji i podfunkcji do elementów systemu	Zależne od procesu	pod „Opis produktu" (strona 21)	
Dobór czujników i elementów wykonawczych	Wymogi dla elementów wykonawczych	*Podręcznik F-SM*, dział 6,5; *Podręcznik moduły bezpieczeństwa*, dział 4.5; *Podręcznik ET 200eco*, dział 5.5; *Podręcznik ET 200eco PN*, dział 5.2; *Podręcznik ET 200pro,* dział 4.4 *Podręcznik ET 200S*, dział 4.5 *Podręcznik ET 200SP*,	
Specyfikacja wymaganych właściwości bezpieczeństwa dla poszczególnych elementów	IEC 61508:2010	—	
Konfiguracja			
Instalacja licencji	Wymogi dla instalacji	pod „Instalacja/deinstalacja licencji STEP 7 Safety Basic V16" (strona 28) lub „Instalacja/deinstalacja licencji STEP 7 Safety Advanced V16" (strona 29)	
Dobór elementów S7	Opisy konfiguracji	pod „Opis produktu" (strona 21); *Podręcznik F-SM*, dział 3; *Podręcznik moduły bezp.*, dział 3; *Podręcznik ET 200eco*, dział 3; *Podręcznik ET 200eco PN*, dział 4; *Podręcznik ET 200pro*, dział 2; *Podręcznik ET 200iSP*, dział 3; *Podręcznik moduły ET 200SP*, dział 3; *Podręcznik moduły ET 200MP*, dział 3;	
Konfigurowanie sprzętu	• Opis systemów bezpieczeństwa • Weryfikacja stosowanych elementów sprzętowych w oparciu o Załącznik 1 raportu certyfikacji	pod „Konfiguracja" (strona 41); Załącznik 1 raportu certyfikacji	

Faza	Należy mieć na uwadze następuje	Odniesienia	Kontrola
Konfiguracja F-CPU	• Poziom ochrony, „Ochrona zapisu do bloków bezpieczeństwa" (S7-300, S7-400) • Poziom ochrony, co najmniej „Pełny dostęp" (S7-1200, S7-1500) • Hasło • Włączona kompatybilność bezp. • Definiowanie/ustawianie parametrów zależnych bezpieczeństwa • Czas cyklu dla grupy F-runtime, w której program bezpieczeństwa będzie wykonywany, zdefiniowany zgodnie z wymogami i przepisami bezpieczeństwa – tak jak w standardowych systemach.	pod „Konfiguracja F-CPU" (strona 46) *Standardowy S7-300; Standardowy S7-400; S7-1200 standard; S7-1500 standard;* pod „Czasy monitorowania i odpowiedzi" (strona 649)	
Konfiguracja F-I/O	• Ustawienia trybu bezpieczeństwa • Ustawianie rodzaju pasywacji • Konfigurowanie czasów monitorowania • Definiowanie oceny czujnika • Definiowanie zachowania diagnostyki • Specjalne parametry bezpieczeństwa • Przypisywanie nazw • Unikalne adresy PROFIsafe	pod „Konfiguracja F-I/O" (strona 51) lub „Specjalne przypadki konfiguracji urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O typu fail-safe opartych na GSD" (strona 76) pod „Czasy monitorowania i odpowiedzi" (strona 649) *Podręcznik F-SM*, działy 3, 9, 10; *Podręcznik moduły bezpieczeństwa*, działy 2.4, 7; *Podręcznik ET 200eco,* działy 3, 8, *Podręcznik ET 200eco PN*, dział 6; *Podręcznik ET 200pro*, działy 2.4, 8;	
Programowanie			
Definiowanie projektu i struktury programu	• Należy przestrzegać ostrzeżeń i uwag dotyczących programowania	pod „Omówienie programowania" (Page 114), „Struktura programu bezpieczeństwa (S7-300, S7-400)" (strona 115), Struktura programu bezpieczeństwa (S7-1200, S7-1500)" (strona 117); „Programowanie zabezpieczenia rozruchu" (strona 165);	

Faza	Należy mieć na uwadze następuje	Odniesienia	Kontrol
Tworzenie grup F-runtime	• Przypisanie F-FB lub F-FC jako głównego bloku bezpieczeństwa do bloku wywołania (S7-300, S7-400) lub F-OB (S7-1200, S7- 1500) • Ustawienia maksymalnego czasu cyklu dla grupy F-runtime zgodnie z wymogami (zależnie od procesów i przepisów bezpieczeństwa) • Tworzenie DB do komunikacji grupy F-runtime • (S7-300, S7-400) Wywołanie głównych bloków bezpieczeństwa bezpośrednio z OB (np. OB 35), FB lub FC • (S7-1200, S7-1500) Wywołanie głównego bloku bezpieczeństwa z F-OB	pod „Definiowanie grup F-runtime" (strona 139) pod „Czasy monitorowania i odpowiedzi" (strona 649)	
Tworzenie/wstawianie bloków bezpieczeństwa	• Generowanie, edytowanie i zapisywanie F-FB, F-FC oraz F-DB zgodnie z wymogami struktury programu • Opis: – Dostęp F-I/O – Pasywacja i ponowna integracja F-I/O – Wstawianie bloków bezpieczeństwa z bibliotek globalnych – Komunikacja CPU safety – CPU – Komunikacja ze standardowym programem użytkownika	pod „Tworzenie bloków bezpieczeństwa w FBD / LAD" (strona 160) pod „Adresowanie F-I/O" (strona 166) pod „Wdrażanie zatwierdzenia użytkownika" (strona 196) pod „Ponowne użycie bloków bezpieczeństwa" (strona 163) pod „Konfiguracja i programowanie komunikacji (S7-300, S7-400)" (strona 209) oraz „Konfiguracja i programowanie komunikacji (S7-1200, S7- 1500) (strona 273) pod „Wymiana danych pomiędzy standardowym programem użytkownika a programem bezpieczeństwa"	
Kompilowanie programu bezpieczeństwa	—	pod „Kompilowanie programu bezpieczeństwa" (strona 323)	
Wdrażanie wywołania programu bezpieczeństwa (S7-300, S7- 400)	Kontrola, czy główny blok bezpieczeństwa jest wywoływany bezpośrednio w OB (np. OB 35), FB lub FC.	pod „Definiowanie grup F-runtime" (strona 139)	
Instalacja			
Konfiguracja sprzętowa	Opis • Instalacja • Okablowanie	pod „Omówienie konfiguracji" (strona 41) „Szczegóły konfiguracji systemu bezpieczeństwa" (strona 45); *Podręcznik F-SM*, działy 5, 6; *Podręcznik moduły bezp.*, działy 3, 4; *Podręcznik ET 200eco*, działy 3, 4; *Podręcznik ET 200eco PN*, działy 4, 5; *Podręcznik ET 200pro*, działy 2, 3; *Podręcznik ET 200iSP,* działy 3 i 4; *Podręcznik ET 200SP*, działy 4 i 5; *Podręcznik ET 200MP*, działy 4 i 5	

Faza	Należy mieć na uwadze następuje	Odniesienia	Kontrol
Odbiór techniczny, testowanie			
Włączenie	Opis odbioru technicznego – identycznie jak w standardowym	Standardowy S7-300; S7-400 standard; S7-1200 standard; S7-1500 standard; Standardowy sterownik programowy S7-1500; WinAC RTX F	
Pobieranie programu bezpieczeństwa i standardowego programu użytkownika	Opis • Pobieranie • Identyfikacja programu • Porównywanie programów	pod „Pobieranie danych projektu do F-CPU" (strona 325) pod „Porównywanie programów bezpieczeństwa" (strona 354)	
Testowanie programu bezpieczeństwa	• Opis wyłączania trybu bezpieczeństwa • Procedura zmiany danych programu bezpieczeństwa	pod „Pobieranie danych projektu" (strona 325); „Testowanie programu bezpieczeństwa" (strona 363); „Wyłączanie trybu bezpieczeństwa" (strona 360)	
Zmiana programu bezpieczeństwa	Opis • Wyłączanie trybu bezpieczeństwa • Zmiana programu bezpieczeństwa	pod „Zmiana programu bezpieczeństwa w trybie RUN (S7-300, S7-400)" (strona 371); „Wyłączan trybu bezpieczeństwa" (strona 360); „Usuwanie programu bezpieczeństwa" (strona 137);	
Testowanie parametrów związanych z bezpieczeństwem	Opis konfiguracji	pod „Drukowanie danych projektu" (strona 357); *Podręcznik F-SM*, działy 4, 9, 10; *Podręcznik moduły bezpieczeństwa*, działy 2.4, 7; *Podręcznik ET 200eco*, działy 3, 8; *Podręcznik ET 200eco*, dział 6; *Podręcznik ET 200pro*, działy 2.4, 8; *Podręcznik ET 200iSP,* działy 2.4, 7, 8 *Podręcznik moduły ET 200SP*, dział 4 *Podręcznik moduły ET 200MP*, dział 4	
Zatwierdzenie systemu			
Zatwierdzenie	• Opis i uwagi dotyczące zatwierdzenia • Wydruki	pod „Zatwierdzenie systemu" (strona 376)	
Obsługa, konserwacja			
Ogólna obsługa	Uwagi dotyczące obsługi	pod „Uwagi dotyczące trybu bezpieczeństwa programu bezpieczeństwa" (strona 401)	
Ochrona dostępu	—	pod „Ochrona dostępu" (strona 103)	
Diagnostyka	Odpowiedzi na usterki i zdarzenia	pod „Przewodnik po diagnostyce (S7-300, S7-400)" (strona 407); „Przewodnik po diagnostyce (S7-1200)" (strona 409); Przewodnik po diagnostyce (S7-1500)" (strona 408);	

Faza	Należy mieć na uwadze następuje	Odniesienia	Kontrol
Wymiana elementów oprogramowania i sprzętu	Opis • Wymiana modułu • Aktualizacja systemów operacyjnych w F-CPU – identycznie jak w standardowym • Aktualizacja elementów SW Uwagi • Aktualizacja systemu operacyjnego w IM	pod „Wymiana elementów programowych i sprzętowych" (strona 404); „Adresowanie F-I/O" (strona 166); Pomoc do *STEP 7*	
Deinstalacja licencji, demontaż	• Uwagi dotyczące deinstalacji licencji • Uwagi dotyczące demontażu modułów	pod „Instalacja/deinstalacja licencji STEP 7 Safety Basic V16" (strona 28); „Instalacja/deinstalacja licencji STEP 7 Safety Advanced V16" (strona 29); „Wymiana elementów programowych i sprzętowych" (strona 404);	

Glosariusz

Ochrona dostępu

Systemy typu fail-safe muszą być chronione przed niebezpiecznym, nieupoważnionym dostępem. Ochrona dostępu do systemów bezpieczeństwa jest wykonywana przy użyciu dwóch haseł (jedno do F-CPU, drugie do programu bezpieczeństwa).

Automatycznie generowane bloki bezpieczeństwa

Bloki bezpieczeństwa, które są automatycznie generowane oraz, w razie potrzeby, wywoływane, gdy program bezpieczeństwa jest kompilowany, aby wygenerować wykonalny program z programu bezpieczeństwa utworzonego przez użytkownika.

Kategoria

Kategoria zgodnie z ISO 13849-1:2015 lub EN ISO 13849-1:2015

Za pomocą SIMATIC Safety, można używać trybu bezpieczeństwa do kategorii 4.

Awaria kanału

Awaria związana z kanałem, taka jak przerwanie przewodu

W obrębie CPU

W kontekście F-I/O, „w obrębie CPU" oznacza wszystkie F-I/O przypisane do F-CPU: Centralny F-I/O tego F-CPU, a także F-I/O, dla których F-CPU to urządzenie nadrzędne DP/sterownik IO oraz przypisane F-I/O we współdzielonym urządzeniu. F-I/O adresowany przy pomocy komunikacji urządzenie I-slave – urządzenie podrzędne jest przypisywany do F-CPU urządzenia I-slave, a nie do F-CPU urządzenia nadrzędnego DP / sterownika IO.

W kontekście komunikacji CPU safety – CPU, „w obrębie CPU" obejmuje wszystkie połączenia komunikacji związanej z bezpieczeństwem, które zostały skonfigurowane w F-CPU.

CRC Cykliczna kontrola redundancji sygnatura CRC

Podpis CRC

Ważność danych procesu w ramce komunikatu bezpieczeństwa, poprawność przypisanych zależności adresowych oraz parametry safety są potwierdzane za pomocą sygnatury CRC, ujętego w ramce komunikatu bezpieczeństwa.

DB do komunikacji grupy F-runtime

F-DB dla komunikacji związanej z bezpieczeństwem pomiędzy grupami F-runtime

Depasywacja

Reintegracja

Wyłączony tryb bezpieczeństwa

Tymczasowa dezaktywacja trybu bezpieczeństwa do celów testowania, odbioru technicznego itp. Przy wyłączonym trybie bezpieczeństwa możliwe są tylko następujące czynności:

- Pobieranie zmian programu bezpieczeństwa do F-CPU podczas trwającej operacji (w trybie RUN)
- Funkcje testowe, takie jak „Modify" (Modyfikuj) lub inne sposoby dostępu do zapisy danych programu bezpieczeństwa (z ograniczeniami)

Gdy tryb bezpieczeństwa jest wyłączony, bezpieczeństwo systemu należy zagwarantować innymi środkami organizacyjnymi, takimi jak monitorowana praca czy ręczne wyłączenie bezpieczeństwa.

Analiza rozbieżności

Analiza rozbieżności dla równoważności lub nierównoważności jest wykorzystywana do wejść fail-safe w celu wykrywania błędów spowodowanych przez charakterystykę czasową dwóch sygnałów w tej samej funkcjonalności. Analiza rozbieżności jest wykonywana, gdy na dwóch powiązanych sygnałach wejściowych zostaną wykryte różne poziomy (podczas testowania nierównoważności: ten sam poziom). Po upłynięciu wyznaczonego okresu (czas rozbieżności), wykonywana jest kontrola, sprawdzająca, czy różnica w poziomach (podczas testowania nierównoważności: ten sam poziom) zniknęły. Jeśli nie, następuje błąd rozbieżności. Analiza rozbieżności jest wykonywana pomiędzy dwoma sygnałami wejściowymi oceny 1oo2 czujników (ocena czujnika) w wejściu fail-safe.

Czas rozbieżności

Możliwy do przypisania czas dla analizy rozbieżności. Jeśli czas rozbieżności zostanie ustawiony zbyt wysoko, czas detekcji awarii oraz czas reakcji na awarię są zbędnie wydłużane. Jeśli czas rozbieżności zostanie ustawiony zbyt nisko, zmniejsza się dostępność, ponieważ błąd rozbieżności jest wykrywany gdy tak naprawdę nie występuje.

Złącze DP/DP

Urządzenie do łączenia dwóch podsieci PROFIBUS DP, wymagane do komunikacji urządzenie nadrzędne - urządzenie nadrzędne pomiędzy programami bezpieczeństwa w różnych F-CPU w SIMATIC Safety oraz S7 Distributed Safety.

Ekspert

Zatwierdzenie systemu, tj. test akceptacji parametrów związanych z bezpieczeństwem systemu, jest zazwyczaj wykonywane przez niezależnego eksperta (przykładowo, z TÜV).

Urządzenia podrzędne DP oparte na GSD typu fail-safe

Urządzenia podrzędne DP oparte na GSD typu fail-safe to standardowe urządzenia podrzędne działające na PROFIBUS z protokołem DP. Muszą działać zgodnie z normą IEC 61784-1:2010 (profile Fieldbus) oraz profilem magistrali PROFIsafe. Plik GSD jest wykorzystywany w ich konfiguracji.

Urządzenia I/O oparte na GSD typu fail-safe

Urządzenia I/O oparte na GSD typu fail-safe to standardowe urządzenia działające na PROFINET z protokołem I/O. Muszą działać zgodnie z normą IEC 61784-1:2010 (profile Fieldbus) oraz profilem magistrali PROFIsafe w V2-MODE. Plik GSD jest wykorzystywany w ich konfiguracji.

Moduły I/O fail-safe

Moduły ET 200eco oraz ET 200eco PN, które można wykorzystać do pracy związanej z bezpieczeństwem (tryb bezpieczeństwa). Moduły te są wyposażone w zintegrowane funkcje bezpieczeństwa. Działają zgodnie z normą IEC 61784-1:2010 (profile Fieldbus) oraz profilem magistrali PROFIsafe.

Moduły fail-safe

Moduły fail-safe ET 200SP, ET 200S, ET 200pro, ET 200iSP, które można wykorzystać w rozproszonych systemach I/O ET 200SP, ET 200S, ET 200pro lub ET 200iSP.

Moduły fail-safe S7-1500/ET 200MP, które można zastosować centralnie w S7-1500 lub w rozproszonym systemie I/O ET 200MP.

Moduł fail-safe S7-1200, który można zastosować centralnie w systemie S7-1200.

Moduły te są wyposażone w zintegrowane funkcje bezpieczeństwa (tryb bezpieczeństwa) do obsługi fail-safe. Działają zgodnie z profilem magistrali PROFIsafe.

Systemy typu fail-safe

Systemy typu fail-safe (systemy bezpieczeństwa) to systemu pozostające w bezpiecznym stanie lub przełączające się do niego niezwłocznie po wystąpieniu określonej usterki.

Funkcja reakcji na awarię

Funkcja bezpieczeństwa użytkownika

Czas reakcji na awarię

Maksymalny czas reakcji na awarię dla systemu bezpieczeństwa określa czas pomiędzy wystąpieniem błędu a bezpieczną reakcją dotkniętego nim wyjścia fail-safe.

Bloki bezpieczeństwa

Poniższe bloki fail-safe są wykonane jako bloki bezpieczeństwa:

- te utworzone przez użytkownika w LAD lub FBD
- te utworzone przez użytkownika jako F-DB
- te wybrane przez użytkownika z biblioteki globalnej
- te dodane automatycznie w programie bezpieczeństwa (F-DB, automatycznie generowane bloki bezpieczeństwa, współdzielone F-FB, DB F-I/O; instancja DB w F-FB)

Wszystkie bloki bezpieczeństwa są przedstawione na żółto w drzewku projektu.

F-CALL

„Bloki wywołania bezpieczeństwa"

Zbiorczy podpis bezpieczeństwa

Zbiorczy podpis bezpieczeństwa unikalnie identyfikuje konkretny stan danych projektu związanych z bezpieczeństwem. Jest ważny do identyfikacji projektu, a także do zatwierdzenia na miejscu instalacji programu bezpieczeństwa, na przykład przez eksperta.

Podpis adresu komunikacji bezpieczeństwa

Podpis adresu komunikacji bezpieczeństwa jest tworzony z nazw i UUID komunikacji bezpieczeństwa dla połączeń komunikacyjnych przy pomocy Flexible F-Link, wykorzystywanych w programie bezpieczeństwa.

DB komunikacji bezpieczeństwa

Bloki danych fail-safe do

- komunikacji CPU safety – CPU poprzez połączenia S7
- Komunikacja z użyciem Flexible F-Link

Rodzaj danych PLC zgodnych z bezpieczeństwem (UDT)

Rodzaj danych PLC zgodnych z bezpieczeństwem (UDT) to rodzaj danych, w których można wykorzystać wszystkie rodzaje danych, jakie można zastosować w programach bezpieczeństwa.

F-CPU

F-CPU to centralna jednostka obliczeniowa z funkcjonalnością fail-safe, zatwierdzona do użycia w SIMATIC Safety, w której program bezpieczeństwa może działać wraz ze standardowym programem użytkownika.

F-DB

Opcjonalne bloki danych typu fail-safe, które można zabezpieczyć przed odczytem i zapisem w obrębie całego programu bezpieczeństwa (wyjątek: DB do komunikacji grupy F-runtime).

Adres docelowy bezpieczeństwa

adres PROFIsafe

F-FB

Bloki funkcyjne typu fail-safe (z instancją DB), w których użytkownik programuje program bezpieczeństwa w FBD lub LAD.

F-FC

FC fail-safe, w których użytkownik programuje program bezpieczeństwa

Zbiorczy podpis F-HW

Zbiorczy podpis bezpieczeństwa unikalnie identyfikuje konkretny stan konfiguracji sprzętowej związanej z bezpieczeństwem. Zbiorczy podpis F-HW jest ważny do dokumentowania zmian/braku zmian w konfiguracji sprzętowej związanej z bezpieczeństwem, np. w kontekście zatwierdzenia zmian.

F-I/O

Zbiorcza nazwa wejść i wyjść fail-safe dostępnych w *SIMATIC S7* do integracji, między innymi, w SIMATIC Safety. Dostępne są następujące moduły:

- moduł I/O typu fail-safe ET 200eco
- moduł I/O typu fail-safe ET 200eco PN
- moduły sygnałowe fail-safe S7-300
- moduły fail-safe do S7-1200
- moduły fail-safe do ET 200MP
- moduły fail-safe do ET 200SP
- moduły fail-safe do ET 200S
- moduły fail-safe do ET 200pro
- moduły fail-safe do ET 200iSP
- Urządzenia podrzędne DP oparte na GSD typu fail-safe
- Urządzenia I/O oparte na GSD typu fail-safe

DB F-I/O

Blok danych typu fail-safe dla F-CPU do F-I/O w *STEP 7 Safety*. DB F-I/O jest automatycznie generowany dla każdego F-I/O, gdy F-I/O jest konfigurowany w *edytorze sprzętu i sieci*. DB F-I/O zawiera tagi, dla których użytkownik może lub musi przeprowadzić ocenę lub zapis w programie bezpieczeństwa.

- Do reintegracji F-I/O po błędach komunikacji
- Do reintegracji F-I/O po awarii F-I/O lub kanału
- Jeśli F-I/O musi być pasywowany wskutek szczególnych stanów programu bezpieczeństwa (przykładowo, pasywacji grupy)
- Do ponownego przypisania parametrów urządzeń podrzędnych DP opartych na GSD typu fail-safe/urządzeń I/O opartych na GSD lub aktywacji komunikacji HART dla F-I/O z odnośną funkcjonalnością
- Do wykonania oceny, czy wyprowadzane są wartości fail-safe czy dane procesowe

Usterki F-I/O

Usterka F-I/O związana z modułem, taka jak błąd komunikacji lub błędne przypisanie parametru

F-I/O adresu PROFIsafe typu 1

F-I/O zapewniające unikalność adresu PROFIsafe wyłącznie na podstawie adresu docelowego bezpieczeństwa, przykładowo, moduły bezpieczeństwa ET 200S. Adres PROFIsafe jest zazwyczaj przypisywany za pomocą przełączników DIP.

F-I/O adresu PROFIsafe typu 2

F-I/O mogące zapewnić unikalność adresu PROFIsafe na podstawie kombinacji adresu źródłowego bezpieczeństwa oraz adresu docelowego bezpieczeństwa, przykładowo, moduły bezpieczeństwa S7-1500/ET 200MP. Adres PROFIsafe jest zazwyczaj przypisywany za pomocą *STEP 7 Safety*.

Moduły bezpieczeństwa

Moduły fail-safe

F-OB

F-OB wywołuje główny blok bezpieczeństwa grupy F-runtime w F-CPU S7-

Grupa F-runtime

Program bezpieczeństwa składa się z jednej lub dwóch grup F-runtime. Grupa F-runtime to konstrukcja logiczna kilku powiązanych bloków bezpieczeństwa. Jest generowana wewnętrznie przez system bezpieczeństwa. Grupa F-runtime składa się z następujących bloków:

Główny blok bezpieczeństwa, F-OB (S7-1200, S7-1500), jeśli ma zastosowanie F-FB/ F-FC, jeśli ma zastosowanie F-DB, DB F-I/O, bloki bezpieczeństwa bibliotek globalnych, instancja DB, F-DB oraz automatycznie generowane bloki bezpieczeństwa.

DB informacji o grupie F-runtime

DB informacji o grupie F-runtime zapewnia kluczowe informacje o odnośnej grupie F-runtime oraz całym programie bezpieczeństwa.

DB współdzielone typu F

(S7-300, S7-400) Blok danych typu fail-safe, zawierający wszystkie współdzielone dane programu bezpieczeństwa oraz dodatkowe informacje wymagane przez system bezpieczeństwa. DB współdzielone typu F jest automatycznie wstawiane i rozszerzane podczas kompilowania konfiguracji sprzętowej. Przy pomocy jego nazwy F_GLOBDB, użytkownik może wykonać ocenę określonych danych w programie bezpieczeństwa.

F-SM

moduły sygnałowe fail-safe S7-300

Adres źródłowy bezpieczeństwa

adres PROFIsafe

Zbiorczy podpis F-SW

Zbiorczy podpis bezpieczeństwa unikalnie identyfikuje konkretny stan programu bezpieczeństwa. Zbiorczy podpis F-SW jest ważny do dokumentowania zmian/braku zmian w programie bezpieczeństwa, np. w kontekście zatwierdzenia zmian.

Bloki systemu bezpieczeństwa

Bloki bezpieczeństwa typu fail-safe, które są automatycznie wstawiane i wywoływane, gdy program bezpieczeństwa jest kompilowany, aby wygenerować wykonalny program z programu bezpieczeństwa utworzonego przez użytkownika.

Systemy bezpieczeństwa

Systemy typu fail-safe

Konfiguracja sprzętowa

Konfiguracja sprzętowa obejmuje konfigurację standardowych parametrów dla CPU i standardowych I/O, a także konfigurację parametrów związanych z bezpieczeństwem dla F-CPU i I/O.

I-device

Funkcjonalność „I-device" (inteligentnego urządzenia I/O) w CPU pozwala na wymianę danych ze sterownikiem I/O i wykorzystanie go , np. jako inteligentnego procesora wstępnego dla podprocesu. W takim przypadku I-device jest łączone jako urządzenie I/O z głównym sterownikiem I/O.

Połączenie IE/PB

Urządzenie do łączenia systemów PROFINET IO i PROFIBUS DP wymagane, między innymi, do komunikacji sterownik IO – urządzenie I-slave pomiędzy programami bezpieczeństwa w różnych F-CPU w SIMATIC Safety.

Parametr i

Poszczególne parametry urządzeń podrzędnych DP opartych na GSD typu fail-safe oraz urządzeń I/O opartych na GSD typu fail-safe

Urządzenie podrzędne

Funkcjonalność „urządzenia I-slave" (inteligentnego urządzenia podrzędnego DP) w CPU pozwala na wymianę danych z urządzeniem nadrzędnym DP i wykorzystanie go, np. jako inteligentnego procesora wstępnego dla podprocesu. W takim przypadku urządzenie I-slave jest łączone jako urządzenie podrzędne DP z nadrzędnym urządzeniem DP.

Główny blok bezpieczeństwa

„Wstępny blok bezpieczeństwa" do programowania fail-safe programu bezpieczeństwa w *STEP 7 Safety*. Główny blok bezpieczeństwa to F-FB lub F-FC, które użytkownik przypisuje do wywołań F-OB (S7- 1200, S7-1500) lub bloku (OB, FC, FB) (S7-300, S7-400) z grupy F-runtime.

Główny blok bezpieczeństwa zawiera program bezpieczeństwa i wszelkie wywołania innych F-FB/F-FC do tworzenia programu.

W całej sieci

Sieć składa się z jednej lub kilku podsieci. „W całej sieci" oznacza poza ograniczeniami podsieci. W PROFIBUS, sieć obejmuje wszystkie węzły dostępne poprzez PROFIBUS DP. W PROFINET IO, sieć obejmuje wszystkie węzły dostępne poprzez RT_Class_1/2/32 (Ethernet/WLAN/Bluetooth, warstwa 2), oraz, jeśli ma zastosowanie, RT_Class_UDP (IP, warstwa 3).

Pasywacja

Gdy występuje pasywacja dla F-I/O z wejściami, system bezpieczeństwa zapewnia program bezpieczeństwa z wartościami fail-safe (0) zamiast danych procesowych obecnych na wejściach fail-safe w PII.

Gdy pasywacja występuje w F-I/O z wyjściami, system bezpieczeństwa wyprowadza wartości fail-safe (0) na wyjściach fail-safe zamiast wartości wyjściowych zapewnianych przez program w PIQ.

PL

Poziom niezawodności (PL) zgodnie z normą ISO 13849-1:2015 lub EN ISO 13849-1:2015

Przy użyciu SIMATIC Safety można osiągnąć maksymalny PL e w trybie bezpieczeństwa.

Złącze PN/PN

Urządzenie do łączenia dwóch systemów PROFIBUS IO, wymagane do komunikacji sterownik IO – sterownik IO pomiędzy programami bezpieczeństwa w różnych F-CPU w SIMATIC Safety oraz S7 Distributed Safety.

PROFIsafe

Profil magistrali safety PROFIBUS DP i PROFINET IO do komunikacji pomiędzy programem bezpieczeństwa a F-I/O w systemie bezpieczeństwa. Patrz IEC 61784-3-3:2010 lub PROFIsafe – Profil do technologii bezpieczeństwa na PROFIBUS DP i PROFINET IO; nr zamówieniowy: 3.192 (V2.6.1).

Adresy PROFIsafe

Adres PROFIsafe (nazwa kodowa zg. z IEC 61784-3-3:2010) służy do ochrony standardowych mechanizmów adresowania, takich jak adresy IP. Adres PROFIsafe składa się z adresu źródłowego bezpieczeństwa i adresu docelowego bezpieczeństwa. Każdy F-I/O ma zatem dwie części adresu, adres źródłowy bezpieczeństwa i adres docelowy bezpieczeństwa.

Adres źródłowy bezpieczeństwa jest przypisywany automatycznie i wyświetlany dla urządzeń podrzędnych DP opartych na GDS typu fail-safe/urządzeń I/O opartych na GSD typu fail-safe oraz modułów bezpieczeństwa ET 200SP, ET 200MP, ET 200eco PN oraz S7-1200. Adres źródłowy bezpieczeństwa dla modułów bezpieczeństwa ET 200S, ET 200eco, ET 200pro, ET 200iSP oraz F-SM S7-300 to zawsze 1. W przypadku modułów bezpieczeństwa ET 200SP/ET 200MP, adres źródłowy bezpieczeństwa odpowiada „centralnemu adresowi źródłowemu bezpieczeństwa" przypisanego F-CPU.

Należy skonfigurować adres docelowy bezpieczeństwa w *edytorze sprzętu i sieci*. Adres docelowy bezpieczeństwa dla modułów bezpieczeństwa ET 200S, ET 200eco, ET 200pro, ET 200iSP oraz F-SM S7-300 przypisuje się przy pomocy przełącznika. W przypadku modułów bezpieczeństwa ET 200SP i ET 200MP, ET 200eco PN należy przypisać adres PROFIsafe w *edytorze sprzętu i sieci*. W przypadku modułów bezpieczeństwa S7-1200, adres docelowy bezpieczeństwa jest przypisywany automatycznie przez system bezpieczeństwa.

Podpis programu

zbiorczy podpis bezpieczeństwa

Dane projektu

Dane projektu obejmują konfigurację sprzętową i program użytkownika.

Reintegracja

Przełączenie z wartości fail-safe (0) na dane procesowe (reintegracja F-I/O) odbywa się automatycznie lub po zatwierdzeniu użytkownika w DB F-I/O. Metoda reintegracji zależy od następujących czynników:

- Powód pasywacji F-I/O lub kanałów F-I/O
- Przypisanie parametrów w DB F-I/O DB lub w samej konfiguracji (przykładowo, moduły typu fail-safe ET 200MP na F-CPU S7-1500 oraz moduły typu fail-safe S7-1200 na F-CPU S7-1200)

Po reintegracji modułu F-I/O z wejściami, dane procesu oczekujące na wejściach w PII są ponownie zapewniane do programu bezpieczeństwa. W przypadku F-I/O z wyjściami, system bezpieczeństwa ponownie przenosi wartości wyjściowe dostępne w PIQ w programie bezpieczeństwa na wyjścia fail-safe.

RIOforFA Safety

Zdalne IO do automatyzacji fabryki w PROFIsafe; profil do F-I/O

Moduły sygnałowe typu fail-safe S7-300

Moduły sygnałowe typu fail-safe serii modułów S7-300, które można wykorzystać do pracy związanej z bezpieczeństwem (tryb bezpieczeństwa) jako scentralizowane moduły w S7- 300 lub jako rozproszone moduły w systemie I/O ET 200M. Moduły sygnałowe typu fail-safe są wyposażone w zintegrowane funkcje bezpieczeństwa. Działają zgodnie z profilem magistrali PROFIsafe.

S7-PLCSIM

Aplikacja *S7-PLCSIM* pozwala na wykonanie i przetestowanie programu na symulowanym systemie automatyzacji na urządzeniu programistycznym lub PC. Jako że symulacja w pełni odbywa się na urządzeniu programistycznym lub PC, nie jest potrzebny żaden sprzęt (CPU, I/O).

Stan bezpieczny

Podstawową zasadą pojęcia bezpieczeństwa w systemach typu fail-safe jest istnienie bezpiecznego stanu dla wszystkich zmiennych procesowych. W przypadku cyfrowego F-I/O zgodnego z normą IEC 61508:2010, zawsze jest to wartość „0”.

Safety Administration Editor

Safety Administration Editor pomaga w wykonywaniu głównych zadań programu

Funkcja bezpieczeństwa

Mechanizm zintegrowany z F-CPU oraz F-I/O pozwalający na stosowanie ich w -> systemach fail-safe.

Zgodnie z IEC 61508:2010, funkcja wdrożona przez urządzenie bezpieczeństwa w celu uzyskania systemu w bezpiecznym stanie lub sprowadzenia go do bezpiecznego stanu w razie określonej awarii. (funkcja reakcji na awarię -> funkcje bezpieczeństwa użytkownika)

Ramka komunikatu bezpieczeństwa

W trybie bezpieczeństwa, dane są przekazywane w ramkach komunikatów pomiędzy F- CPU a F-I/O, lub pomiędzy F-CPU w komunikacji CPU safety – CPU.

Tryb bezpieczeństwa

1. Tryb roboczy F-I/O, w którym komunikacja safety może odbywać się przy użyciu ramek komunikatu bezpieczeństwa.
2. Tryb roboczy programu bezpieczeństwa. W trybie bezpieczeństwa programu bezpieczeństwa, wszystkie mechanizmy bezpieczeństwa do wykrywania błędów i reakcji na usterki są włączone. W trybie bezpieczeństwa, program bezpieczeństwa nie może być modyfikowany podczas działania. Tryb bezpieczeństwa może być wyłączony przez użytkownika (wyłączony tryb bezpieczeństwa).

Program bezpieczeństwa

Program użytkownika safety

Protokół bezpieczeństwa

Ramka komunikatu bezpieczeństwa

Podsumowanie bezpieczeństwa

Podsumowanie bezpieczeństwa zapewnia dokumentację danych projektu związanych z bezpieczeństwem, pomagającą wykonać zatwierdzenie systemu.

Komunikacja safety

Komunikacja safety jest wykorzystywana do wymiany danych typu fail- safe.

Konfiguracja sprzętowa safety

Konfiguracja sprzętowa safety obejmuje konfigurację parametrów związanych z bezpieczeństwem dla F-CPU, a także konfigurację urządzeń F-I/O.

Dane projektu safety

Dane projektu safety obejmują konfigurację sprzętową, a także program bezpieczeństwa.

Ocena czujnika

Dostępne są dwa rodzaje oceny czujnika:

- Ocena 1oo1 – sygnał czujnika jest odczytywany raz
- Ocena 1oo2 - sygnał czujnika jest odczytywany dwa razy przez ten sam F-I/O, a następnie wewnętrzne porównywany

Współdzielone urządzenie

Funkcjonalność „urządzenie współdzielone" pozwala na dystrybucję submodułów urządzenia IO pomiędzy różnymi sterownikami IO.

Podpis

zbiorczy podpis bezpieczeństwa

SIL

Poziom nienaruszalności bezpieczeństwa SIL zgodnie z normą IEC 61508:2010. Im wyższy poziom SIL, tym bardziej wytrzymałe środki zapobiegania awariom systematycznym oraz do zarządzania awariami systematycznymi i losowymi usterkami sprzętu.

Przy użyciu SIMATIC Safety można osiągnąć maksymalny poziom SIL3 w trybie bezpieczeństwa.

Komunikacja standardowa

Komunikacja wykorzystywana do wymiany danych niezwiązanych z bezpieczeństwem.

Tryb standardowy

Tryb roboczy F-I/O, w którym komunikacja safety pomiędzy F- CPU a F-I/O za pomocą ramek komunikacji bezpieczeństwa nie jest możliwa; jedynie komunikacja standardowa jest możliwa w tym trybie.

Standardowy program użytkownika

Program użytkownika nie-safety

Rozruch systemu bezpieczeństwa

Przy pomocy F-CPU, standardowy program użytkownika uruchamia się w normalny sposób. Po uruchomieniu programu bezpieczeństwa wszystkie F-DB są inicjalizowane z wartościami z pamięci "load memory" – jak w przypadku zimnego restartu. Oznacza to, że zapisane informacje o błędach są kasowane.

System bezpieczeństwa wykonuje automatyzację reintegrację F-I/O.

Program użytkownika

Program użytkownika obejmuje standardowy program użytkownika oraz program bezpieczeństwa.

Funkcje bezpieczeństwa użytkownika

funkcje bezpieczeństwa do procesu mogą mieć postać funkcji użytkownika lub funkcji reakcji na usterkę. Użytkownik musi jedynie zaprogramować własne funkcje bezpieczeństwa. W przypadku wystąpienia błędu, jeśli system bezpieczeństwa nie może dłużej wykonywać swojej faktycznej funkcji, wykonuje funkcję reakcji na usterkę; przykładowo, powiązane wyjścia są wyłączane, a F-CPU, jeśli to konieczne, przełącza się w tryb STOP.

Stan wartości

Stan wartości to dodatkowe informacje binarne dla wartości kanału. Stan wartości jest wprowadzany do wejścia obrazu procesui zapewnić informacje o ważności wartości kanału.

1: Ważne dane procesowe są wyprowadzane na wartość kanału.

0: Wartość fail-safe jest wyprowadzana na wartość kanału.

Stosowana instrukcja

Instrukcja, której wersja jest wyświetlona w kolumnie „Version" (Wersja) karty zadań „Instructions" (Instrukcje):