INTEX

CENTRUM SZKOLENIOWE SYSTEMÓW AUTOMATYKI

PROFIBUS to jedyny system komunikacyjny, który stosowany jest zarówno w systemach automatyzacji maszyn czy linii produkcyjnych jak również w aplikacjach procesowych. Jego „młodszy brat" PROFINET pozwala na wykorzystanie zalet sieci Ethernet.

Porównanie najistotniejszych cech tych systemów zostało przedstawione w artykule „PROFINET IO vs. PROFIBUS DP" dostępnym na www.intex.com.pl

Opublikowana w 1999 roku specyfikacja PROFIsafe definiuje dodatkowe mechanizmy pozwalające na detekcję błędów w kanale komunikacyjnym. Dzięki niej systemy PROFIBUS, a od 2005 (specyfikacja PROFIsafe 2.0) również PROFINET mogą być stosowane w systemach bezpieczeństwa.

W 2010 roku zainstalowanych zostało 300.000 urządzeń obsługujących PROFIsafe, co w porównaniu do roku poprzedniego stanowi znaczny wzrost (w 2009 roku – 220.000). Liczba zainstalowanych urządzeń wykorzystujących PROFIsafe na koniec 2010 osiągnęła poziom 1,15Mln. PROFIsafe aktualnie jest niepodważalnym liderem w zakresie zintegrowanych systemów bezpieczeństwa.

Poniższa publikacja przedstawia najistotniejsze cechy technologii PROFIsafe, ze szczególnym uwzględnieniem korzyści wynikających z jej zastosowania.

PROFIsafe – rozwiązanie dla zintegrowanych systemów bezpieczeństwa

PROFIsafe

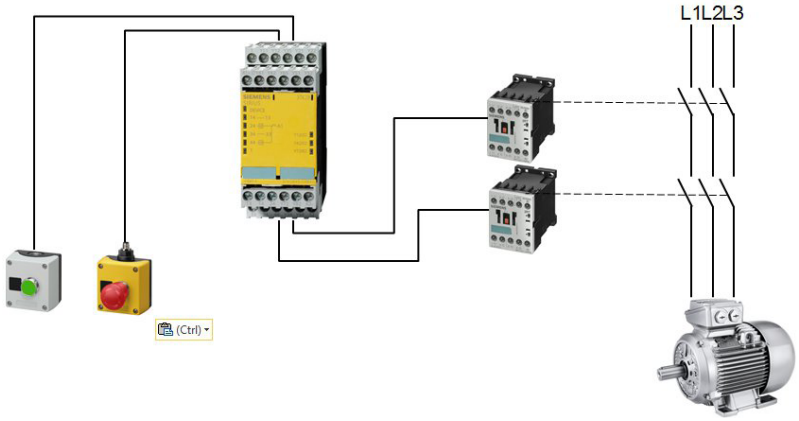
Wprowadzenie

Większość procesów produkcyjnych w mniejszym lub większym stopniu związanych jest z niebezpieczeństwem zranienia lub śmierci personelu obsługi, zagrożeniem dla środowiska ewentualnie systemu produkcyjnego (maszyny, linii produkcyjnej).

Typowymi przykładami aplikacji gdzie zagrożenie personelu obsługi lub użytkowników jest bardzo wysokie są prasy, piły, maszyny wykorzystujące roboty, maszyny pakujące, systemy transportu.

Inną grupą są procesy chemiczne, aplikacje wykorzystujące wysokie ciśnienia lub temperatury. We wszystkich tych aplikacjach wymagane jest stosowanie środków minimalizujących zagrożenie dla ludzi, środowiska czy też środków trwałych.

Klasyczne podejście do zabezpieczeń wykorzystuje dedykowane urządzenia peryferyjne współpracujące z odpowiednimi układami logicznymi odpowiedzialnymi za nadzorowanie stanu obiektu i wyzwalanie funkcji bezpieczeństwa w razie wykrycia błędu lub jakiegokolwiek zagrożenia. Układy te najczęściej są w pełni niezależne od systemu sterowania nadzorującego proces produkcyjny. Takie podejście wymaga stosowania niezależnego okablowania, ale być może również programowania dedykowanych sterowników bezpieczeństwa, a tym samym wpływa na elastyczność oraz koszt systemu.



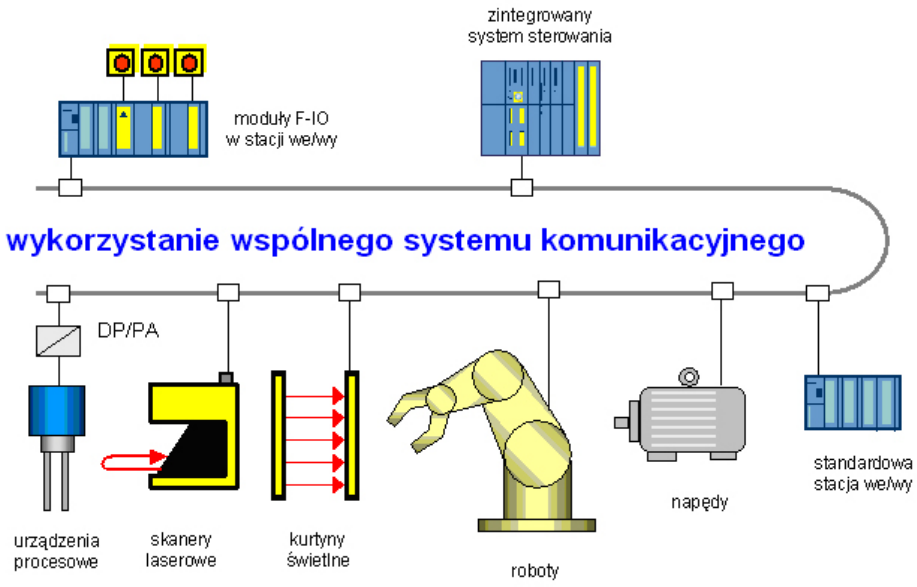
Ilustracja 1: Uproszczony przykład klasycznego układu sterowania silnikiem z realizacją funkcji bezpieczeństwa

Aktualnie dostępne są rozwiązania integrujące obsługę funkcji bezpieczeństwa w ramach systemu sterowania maszyną/procesem. Sytuacja taka stała się możliwa, ponieważ lata doświadczeń oraz miliony aplikacji pozwoliły na określenie warunków, jakie należy spełnić, aby programowane urządzenie mikroprocesorowe można było uznać za niezawodne i określić jego zachowanie w sytuacjach awaryjnych jako przewidywalne.

Aby umożliwić integrację systemu bezpieczeństwa w ramach systemu sterowania należy zdefiniować dodatkowe mechanizmy zwiększające pewność przekazywania danych procesowych oraz możliwości detekcji błędów tak, aby prawdopodobieństwo wystąpienia błędu, który nie zostanie wykryty, nie przekraczało poziomu definiowanego przez zadaną kategorię SIL (Safety Integrity Level, dokładna definicja w IEC 61508).

Dzięki integracji systemu sterowania oraz bezpieczeństwa możliwa jest rezygnacja z dedykowanych przekaźników bezpieczeństwa, jednocześnie okablowanie dedykowane dla tych systemów zostanie zastąpione przez system magistralowy bądź urządzenia bezpieczeństwa zostaną dołączone do już istniejącego systemu komunikacyjnego. (Ilustracja 1, 2)

W systemie zintegrowanym poza elementami związanymi ze sterowaniem obiektem np. systemy rozproszonych we/wy, napędy, enkodery, wyświetlacze, pojawiają się elementy obwodów zabezpieczających np. wyłączniki bezpieczeństwa, kurtyny świetlne, skanery laserowe.



Ilustracja 2: Zintegrowany system sterowania (urządzenia bezpieczeństwa i standardowe dołączone do tej samej sieci, obsługiwane przez ten sam sterownik)

Elementy te mogą być dołączane do dedykowanych modułów sygnałowych (F-IO) zainstalowanych w systemie rozproszonych we/wy (obok kart standardowych) lub bezpośrednio do sieci dzięki wbudowanemu interfejsowi komunikacyjnemu.

W przypadku rozwiązań bazujących na protokołach PROFIBUS lub PROFINET zadania związane ze zwiększeniem pewności przekazywania informacji oraz detekcji błędów są realizowane przez warstwę PROFIsafe.

PROFIsafe w urządzeniach

PROFIsafe otwiera przed producentami urządzeń nowe możliwości oraz zakresy aplikacji dla oferowanych produktów.

Systemy rozproszonych wejść/wyjść umożliwiają jednoczesną obsługę standardowych torów sygnałowych, jak również torów związanych z obwodami bezpieczeństwa. Aktualnie dostępne rozwiązania pozwalają na obsługę sygnałów cyfrowych w zakresie wejść jak i wyjść oraz wejść analogowych. Dodatkowo możliwe jest bezpośrednie sterowanie silnikiem poprzez moduł zintegrowany w ramach stacji rozproszonych we/wy.

W zakresie urządzeń optycznych oferowane są kurtyny oraz skanery laserowe wyposażone w interfejs sieciowy. Urządzenia te pozwalają na monitorowanie dostępu do strefy gdzie występuje zagrożenie dla personelu obsługi. Dzięki nim możliwa jest częściowa rezygnacja z zabezpieczeń mechanicznych (osłony, furtki), a tym samym możliwe jest również skrócenie czasu potrzebnego na wejście do strefy zagrożenia np. w celu wymiany detalu, który podlega obróbce. Wykorzystanie tych elementów w miejsce zabezpieczeń mechanicznych pozwala na zwiększenie wydajności maszyny.

W systemach napędowych jednym ze sposobów realizacji funkcji bezpieczeństwa jest wykorzystanie zewnętrznych elementów typu przekaźniki bezpieczeństwa, opcjonalne moduły dla przekształtników pozwalające na realizację blokady sterowania impulsami czy też styczniki pozbawiające układ napędowy zasilania.

Wykorzystanie PROFIsafe umożliwia zastąpienie zewnętrznych elementów elektromechanicznych przez elektroniczne układy wyłączania

i monitorowania prędkości lub pozycji wbudowane w przekształtnik.

Możliwości udostępniane przez system napędowy zgodny z PROFIsafe zdefiniowane są w rozszerzeniach profilu PROFIdrive (PROFIdrive on PROFIsafe – Interface for functional safety).

Funkcjonalność PROFIsafe w napędach umożliwia znaczne uproszczenie okablowania i jednocześnie realizację funkcji, które w rozwiązaniu konwencjonalnym wymagały wykorzystania wielu dodatkowych elementów, bądź ich realizacja nie była możliwa.

Systemy napędowe zgodne z PROFIsafe mogą realizować dwa rodzaje funkcji: funkcje bezpieczeństwa związane z zatrzymaniem napędu oraz funkcje bezpieczeństwa związane z monitorowaniem bezpiecznego zachowania napędu. (Ilustracja 3)

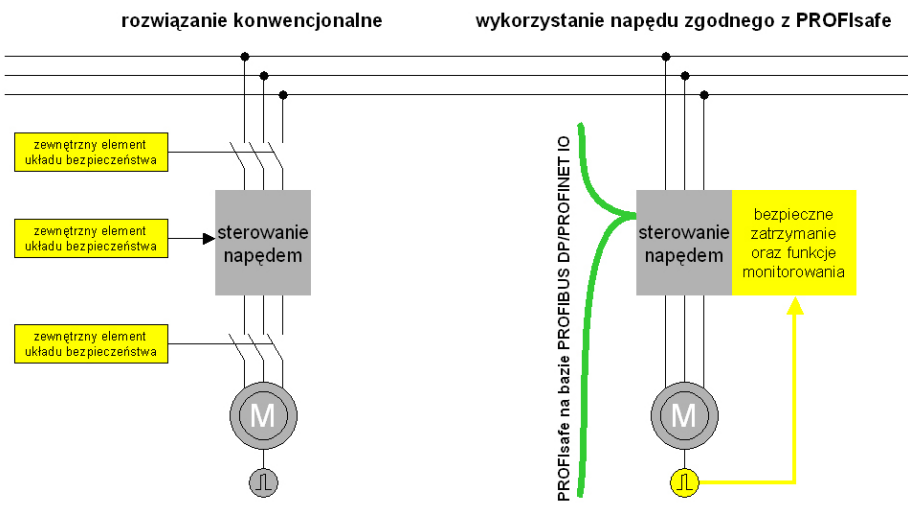
Do funkcji bezpiecznego zatrzymania napędu należą (ilustracja 4):

- STO *(Safe Torque Off)* – funkcja odpowiedzialna za pozbawienie napędu zasilania i jego niekontrolowane zatrzymanie,
- SS1 *(Safe STOP 1)* – zapewnia kontrolowane zatrzymanie napędu ze zdefiniowanymi limitami (rampa, czas), a następnie przejście w tryb STO,
- SS2 *(Safe STOP 2)* – zapewnia kontrolowane zatrzymanie napędu ze zdefiniowanymi limitami (rampa, czas), a następnie przejście w tryb SOS,
- SOS *(Safe Operational STOP)* – monitoruje pozycję napędu po zatrzymaniu, jej zadaniem jest zabezpieczenie układu przed rozpędzeniem się w wyniku działania sił zewnętrznych.

W zakresie funkcji monitorujących, napędy mogą udostępniać funkcje:

- SLS *(Safe Limited Speed)* – zabezpiecza napęd przed przekroczeniem zadanej prędkości maksymalnej,
- SLP *(Safe Limited Position)* – odpowiada za kontrolę czy ruchy napędu mieszczą się w zadanych granicach,
- SDI *(Safe DIrection)* – pozwala na określenie bezpiecznego kierunku rotacji dla napędu,
- SLT *(Safe Limited Torque)* – chroni napęd przed przekroczeniem zdefiniowanego momentu.

Przekroczenie zdefiniowanych dla funkcji SLS, SLP, SDI warunków skutkuje wyzwoleniem funkcji bezpieczeństwa związanych z zatrzymaniem napędu (rodzaj funkcji zależy od aplikacji), zaś w przypadku przekroczenia zadanego momentu w trybie SLT wyzwala funkcję STO.



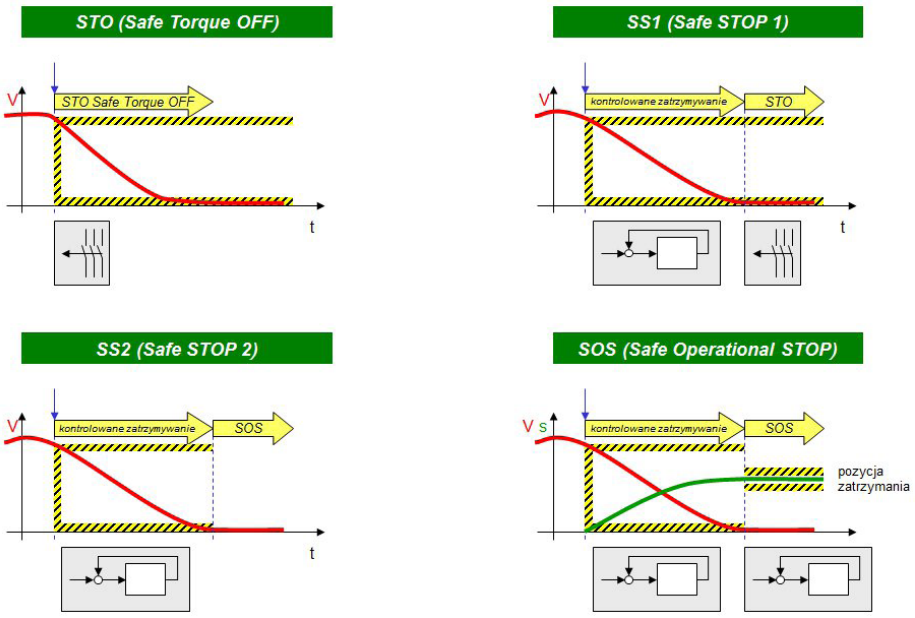
Ilustracja 3: System napędowy ze zintegrowanymi funkcjami awaryjnego zatrzymania oraz monitorowania

Połączenie systemów napędowych oraz urządzeń optycznych zgodnych z PROFIsafe pozwala na znaczne uproszczenie układu sterowania.

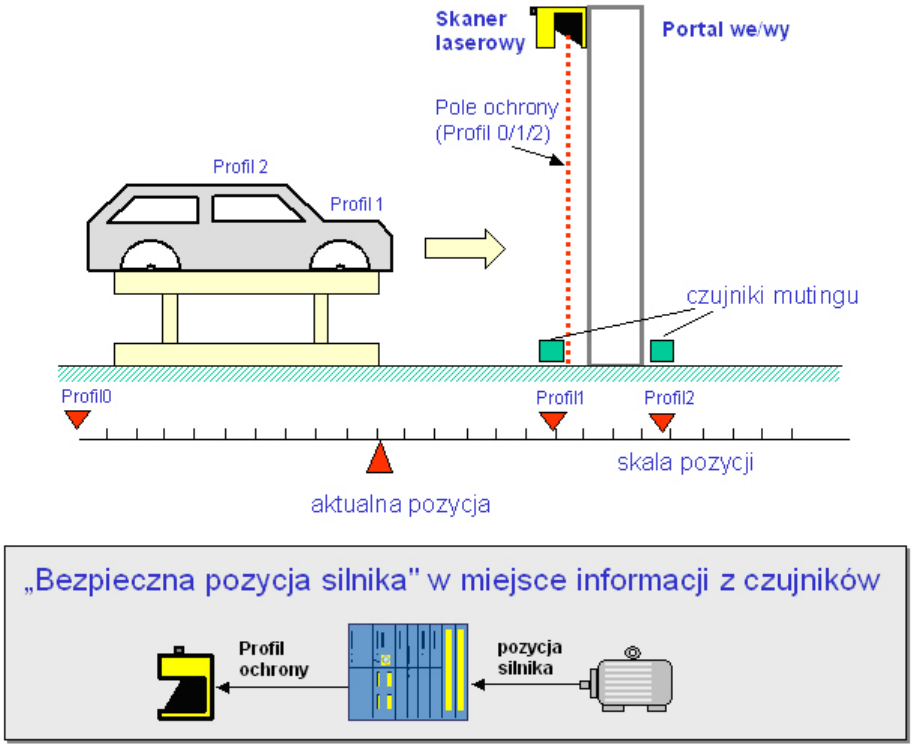
Jednym z przykładów może być brama wjazdowa/wyjazdowa ze strefy, w której występuje zagrożenie dla personelu obsługi. Bazując na urządzeniach zgodnych z PROFIsafe możliwa jest rezygnacja z elementów ochrony mechanicznej jak np. odpowiednio profilowanych furtek oraz czujników sprawdzających pozycję wjeżdżającego/wyjeżdżającego elementu (czujniki mutingu).

Przykład takiej aplikacji prezentuje kolejna ilustracja.

Zadaniem skanera laserowego jest monitorowanie prześwitu bramy i detekcja próby wejścia do strefy niebezpiecznej przez bramę. W skanerze zdefiniowano 3 profile (strefy ochrony) prześwitu bramy. Profile te odpowiadają: detekcji w pełnym zakresie (profil0) oraz detekcji w ograniczonym zakresie (profil1/proifl2). Detekcja w ograniczonym zakresie wykorzystywana jest, np. w trakcie wprowadzania karoserii do strefy. W zależności od pozycji karoserii wykorzystywany powi-



Ilustracja 4: Porównanie funkcji bezpieczeństwa w zakresie bezpiecznego zatrzymania napędu

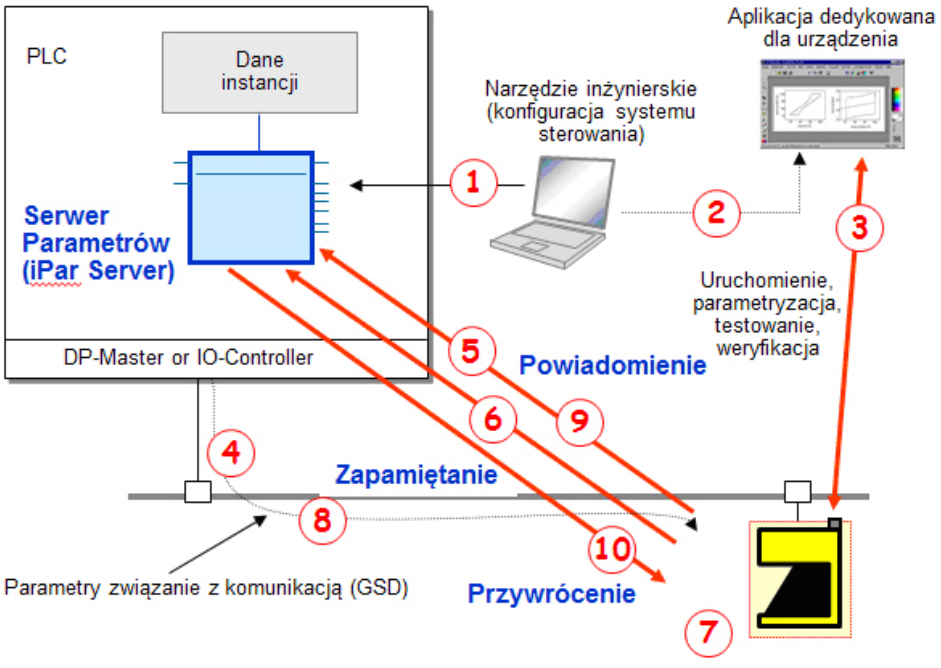


Ilustracja 5: Przykład aplikacji dla urządzeń zgodnych z PROFIsafe

nien być profil1 lub profil2. Informacja o pozycji może być pobierana z czujników zbliżeniowych (czujniki mutingu), ale również może pochodzić z napędu lub enkodera zgodnego z PROFIsafe. W przypadku wykorzystania informacji z napędu lub enkodera czujniki zbliżeniowe stają się zbędne.

Inną grupą aplikacji, gdzie korzyści z zastosowania napędów zgodnych z PROFIsafe mogą być duże są aplikacje, w których w sytuacjach awaryjnych, bądź w strefach zagrożenia dla personelu zatrzymanie napędu zastąpione zostanie przez znaczne ograniczenie i monitorowanie prędkości.

Sytuacja taka pozwala na kontynuowanie procesu, a tym samym zwiększenie wydajności (np. w przypadku montażu elementów w trakcie ich przesuwania) lub ograniczenie strat w wyniku przerwania procesu (np. rozprowadzanie kleju przez robota).



Ilustracja 6: Wykorzystanie uniwersalnego serwera parametrów

Serwer parametrów – iPar Server

Niektóre z urządzeń wykorzystywanych w systemach bezpieczeństwa (ale nie tylko) wymagają parametryzacji specyficznej dla aplikacji, w której pracują. Jednym z przykładów może być skaner laserowy, dla którego konieczne jest określenie obszarów chronionych oraz obszarów, których naruszenie będzie generowało ostrzeżenie. Producenci tego typu urządzeń dostarczają własne oprogramowanie pozwalające na definicję parametrów spełniających wymagania konkretnej aplikacji.

Oprogramowanie to wymagane jest przede wszystkim ze względu na prosty interfejs użytkownika, ale również pozwalają na ominięcie ograniczeń, jakimi obarczone są metody opisu/definicji parametrów w plikach GSD dla urządzeń z interfejsem PROFIBUS DP czy GSDML dla urządzeń z interfejsem PROFINET IO.

Cechą tych aplikacji jest również to, że komunikują się z urządzeniem wykorzystując dedykowany interfejs (np. RS-232) oraz kabel połączeniowy. Sytuacja taka powoduje, że w czasie awarii, kiedy należy wymienić uszkodzone urządzenie konieczna jest parametryzacja zamiennika, a to z kolei wymaga dedykowanego oprogramowania, kabla połączeniowego, komputera no i najważniejsze … czasu.

Aby uniknąć tych niedogodności na potrzeby profilu PROFIsafe opracowana została koncepcja serwera parametrów iPar Server (individual Parameter Server). Koncepcja ta przedstawiona jest na ilustracji 6.

W trakcie konfiguracji urządzenia w ramach systemu sieciowego (PROFIBUS DP lub PROFINET IO) w programie sterowania PLC stworzona powinna zostać także instancja skojarzonego serwera parametrów (krok1). W czasie uruchomienia systemu do parametryzacji urządzenia obiektowego wykorzystywana jest dedykowana aplikacja dostarczona przez producenta.

Aplikacja ta może zostać wywołana bezpośrednio z narzędzia inżynierskiego wykorzystywanego do konfiguracji systemu sterowania poprzez interfejsy FDT (Field Device Tool) lub TCI (Tool Calling Interface) (krok 2).

Po finalnej weryfikacji zdefiniowanej konfiguracji (krok 3) w konfigurato-

rze systemu sterowania definiowane są ostateczne parametry urządzenia, które następnie są ładowane do PLC, a to z kolei przekazuje je do urządzenia obiektowego (krok 4).

Po uruchomieniu komunikacji urządzenie zgłasza się do skojarzonego serwera parametrów (iPar Server) (krok 5) z prośbą o przechowanie kopii bieżących parametrów. Dane te są pobierane z wykorzystaniem komunikacji acyklicznej (krok 6). Na tym etapie proces uruchomienia systemu został zakończony.

Po wymianie urządzenia obiektowego na nowe (np. po jego uszkodzeniu) (krok 7) jest ono ponownie parametryzowane przez jednostkę nadrzędną wykorzystując parametry zdefiniowane w konfiguracji (krok 8 identyczny jak krok 4). Na podstawie otrzymanych parametrów urządzenie „orientuje się", że jego bieżące parametry aplikacyjne nie są zgodne z oczekiwanymi, co skutkuje wygenerowaniem powiadomienia dla systemu nadrzędnego (krok 9) z prośbą o załadowanie dodatkowych parametrów specyficznych dla urządzenia (krok 10). Po przywróceniu parametrów urządzenie jest gotowe do pracy, bez konieczności wykorzystywania dodatkowego narzędzia w celu jego parametryzacji.

Wykorzystanie funkcjonalności iPar Server pozwala na znaczne skrócenie czasu przestoju spowodowanego awarią urządzenia obiektowego i jednocześnie znacznie upraszcza procedurę jego wymiany.

W tym miejscu warto dodać, że aktualnie specyfikacja iPar Server została wyłączona z profilu PROFIsafe tak, aby tę funkcjonalność można było wykorzystać nie tylko dla urządzeń związanych z systemami bezpieczeństwa.

Korzyści wynikające z integracji funkcji bezpieczeństwa w systemie sterowania

Integracja funkcji bezpieczeństwa w ramach kontrolera odpowiedzialnego za sterowanie maszyną lub procesem otwiera nowe możliwości dla aplikacji, ale również oferuje wiele korzyści w przypadku standardowych aplikacji.

Najważniejsze zalety tej integracji to:

- **prosta rozbudowa** systemu sterowania o funkcje bezpieczeństwa dzięki możliwości instalacji modułów we/wy obsługujących obwody bezpieczeństwa w ramach stacji rozproszonych we/wy. W tym przypadku nie ma potrzeby wykorzystywania dedykowanego systemu komunikacyjnego, najczęściej również nie są wymagane żadne zmiany w samej stacji rozproszonych we/wy,
- **znaczna redukcja okablowania** związanego z obwodami bezpieczeństwa (jako konsekwencja integracji w ramach systemów rozproszonych we/wy) dzięki możliwości dopasowania topologii sieci do aktualnych potrzeb,
- wykorzystanie **wspólnego zestawu narzędzi** (oprogramowanie, interfejsy komunikacyjne) do obsługi aplikacji standardowej oraz związanej z zabezpieczeniami,
- **prosta implementacja, modyfikacja i rozszerzenie** funkcji bezpieczeństwa ze względu na jej implementację w postaci programu, a nie na bazie dedykowanego sprzętu z własnym okablowaniem,
- **uproszczenie diagnostyki** systemu sterowania dzięki skupieniu informacji związanych ze sterowaniem jak i zabezpieczeniami w jednym kontrolerze,
- **prosty zapis i modyfikację funkcji bezpieczeństwa** dzięki wykorzystaniu standardowych edytorów programu dla PLC (LAD/FBD),
- **łatwe przekazywanie informacji** pomiędzy aplikacją odpowiedzialna za sterowanie, a funkcjami bezpieczeństwa.

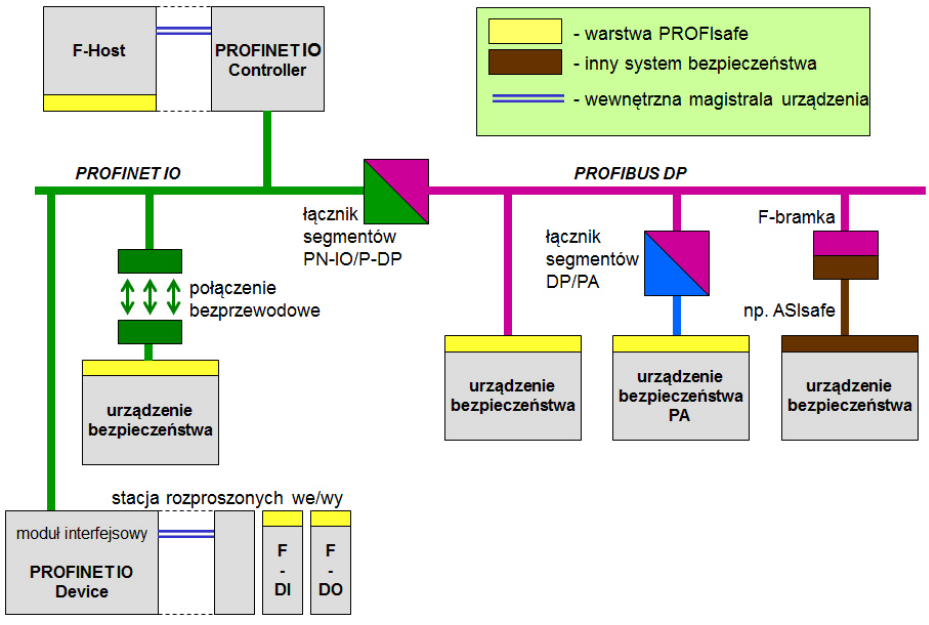
Implementacja PROFIsafe

Jednym z istotnych założeń, jakie przyjęto na etapie specyfikacji profilu PROFIsafe było uniezależnienie od kanału komunikacyjnego przekazującego informacje pomiędzy sterownikiem bezpieczeństwa, a urządzeniami obiektowymi.

Podejście to nazwano z angielskiego „Black channel". Traktuje ono kanał komunikacyjny jak „czarną skrzynkę", która dla użytkownika jest elementem nierozpoznanym. Aby zabezpieczyć się przed przekłamaniami, jakie mogą powstać w nieznanym kanale komunikacyjnym należało zdefiniować dodatkowe mechanizmy zabezpieczające przekazywane informacje, ale również pozwalające na detekcję przekłamań, jakie może wprowadzić kanał komunikacyjny.

W aktualnie projektowanych systemach automatyki informacja pomiędzy jednostką realizującą algorytm sterowania, a urządzeniami peryferyjnymi może być przekazywana z wykorzystaniem kilku kanałów. Na ilustracji 7 prezentowany jest typowy przykład.

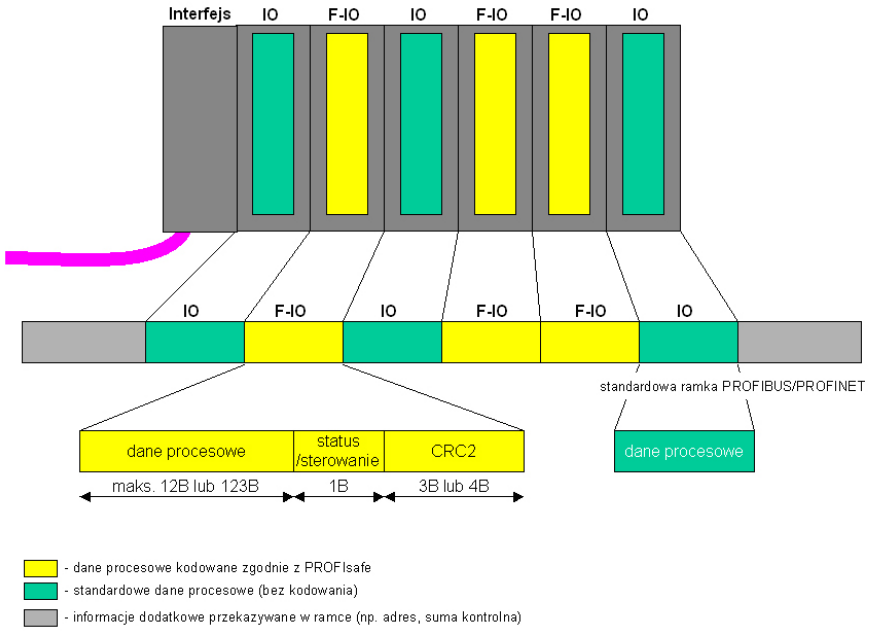
Jak widać na ilustracji 9 dane procesowe są przekazywane przez magistrale wewnętrzne systemu sterowania, być może również urządzenia peryferyjnego. Dodatkowo pojawia się magistrala integrująca system rozproszony (np. PROFIBUS DP lub PROFINET IO), a czasami również moduł sprzęgający różne sieci (np. bramka pomiędzy siecią PROFINET IO, a PROFIBUS DP).



Ilustracja 7: Kanały komunikacyjne wykorzystywane w procesie przekazywania danych pomiędzy systemem sterowania, a urządzeniami obiektowymi

Co więcej dany protokół komunikacyjny może być przesyłany przez różne media przykładowo dla protokołu PROFINET IO użytkownik ma do dyspozycji warstwę fizyczną zgodną z IEEE 802.3 (Ethernet), ale również IEEE802.11 (WLAN). W przypadku PROFIBUS zgodnie ze standardem może to być RS-485, światłowód, ale również MBP.

W celu zwiększenia możliwości detekcji błędów powstających w kanale transmisyjnym profil PROFIsafe definiuje format pakietu dla danych wymienianych pomiędzy kontrolerem oraz stacją lub modułem zgodnym z PROFIsafe. Format ten przedstawiony jest poniżej.



Ilustracja 9: Wymiana danych pomiędzy stacją rozproszonych we/wy zawierającą moduły zgodne z PROFIsafe, a kontrolerem

Pakiet PROFIsafe zawiera (ilustracja 8):

- dane procesowe: maksymalnie 12 lub 123 bajty,
- bajt statusowy/kontrolny (w zależności od kierunku przekazywania informacji),
- cykliczny kod nadmiarowy (CRC) o długości 3 lub 4 bajtów w zależności od długości pola danych.

dane procesowe	status lub sterowanie	kod nadmiarowy **CRC2**
informacje z urządzenia peryferyjnego lub dla elementu wykonawczego	przekazuje informacje diagnostyczne lub sterujące pomiędzy stacjami (kontrolerem, a urządzeniem peryferyjnym)	generowany dla danych, bajtu sterującego/statusowego z uwzględnieniem wirtualnego licznika pakietów oraz F-parametrów
maksymalnie 12 lub 123 bajty	**1 bajt**	**3 lub 4 bajty**

Ilustracja 8: Format pakietu zgodnego z PROFIsafe *(PROFIsafe Process Data Unit)*

Powyższy format dotyczy tylko i wyłącznie przekazywania danych procesowych pomiędzy elementami układu bezpieczeństwa.

Przykładowo, jeżeli stacja rozproszonych we/wy zawiera moduły standardowe (IO) oraz zgodne z PROFIsafe (F-IO), wtedy dla każdego z modułów F-IO generowany jest odrębny pakiet zgodny z powyższym formatem, zaś informacje z modułów standardowych przekazywane są bezpośrednio. Dane z wielu modułów są przekazywane w jednej ramce, zgodnie z konfiguracją stacji.

Obsługa PROFIsafe w urządzeniach jest zwykle realizowana na poziomie wewnętrznego oprogramowania w postaci sterownika PROFIsafe (PROFIsafe driver- PSD). Część kodu odpowiedzialna za realizację funkcjonalności PROFIsafe korzysta z danych udostępnianych przez standardowy kod obsługujący kanał komunikacyjny (np. sterownik PROFIBUS DP lub PROFINET).

Warstwa PROFIsafe związana jest z przekazywaniem informacji pomiędzy elementami układu bezpieczeństwa, zaś pozostałe funkcje jak np. diagnostyka, parametryzacja są obsługiwane przez standardowe oprogramowanie komunikacyjne. (Ilustracja 10)

Podstawowym zadaniem warstwy PROFIsafe jest przekazywanie danych procesowych (w formacie PROFIsafe). Ponadto w trakcie rozruchu lub detekcji błędów dane procesowe są zastępowane domyślnymi wartościami bezpiecznymi.

Najczęściej będą to wartości nakazujące wyłączenie obwodu wykonawczego, jednak dozwolone są także inne wartości (zależne od aplikacji) np. zmień prędkość napędu na bezpieczną.

Wyzwolenie bezpiecznych wartości oraz sprawdzanie ich obecności odbywa się poprzez bajt sterujący/statusowy w pakiecie PROFIsafe.

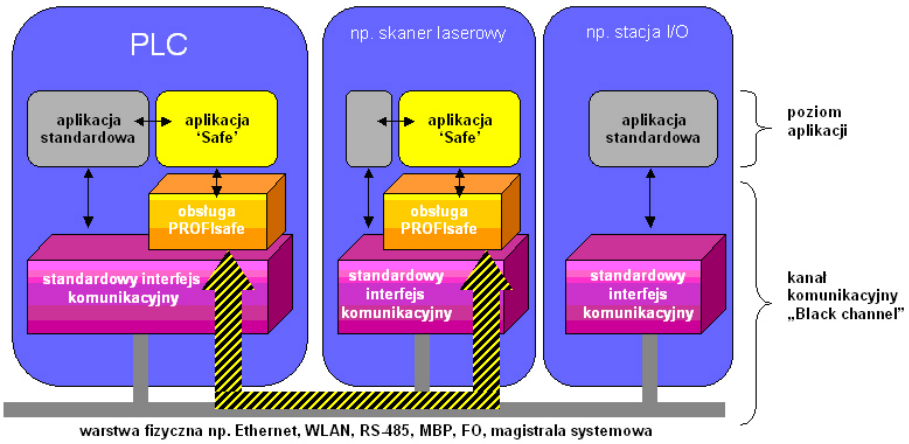
Ponieważ przejście ze stanu bezpiecznego do normalnego nie może odbywać się automatycznie, a wymaga interwencji użytkownika, dlatego też funkcja bezpieczeństwa może zażądać potwierdzenia (ustawiając jeden z bitów w bajcie sterującym, co może być sygnalizowane na module poprzez np. diodę LED).

Dodatkowo warstwa PROFIsafe odpowiedzialna jest za przekazywanie aplikacji bezpieczeństwa specyficznych dla niej danych określanych jako iParameters (individual Parameters – patrz iPar Server).

Aby zwiększyć pewność przekazywania danych procesowych pomiędzy urządzeniami tworzącymi układ bezpieczeństwa i jednoczenie umożliwić detekcję błędów niewykrywanych przez standardowy mechanizm transmisji, dane procesowe należy uzupełnić o dodatkowe informacje. (Ilustracja 11)

Błędy transmisji, jakie mogą wystąpić w kanale komunikacyjnym (ilustracja 12), to:

- niezamierzone powtórzenie pakietu,
- utrata pakietu,
- wstawienie dodatkowego pakietu,
- zakłócenie sekwencji pakietów,
- przekłamanie pakietu,



Ilustracja 10: Umiejscowienie warstwy PROFIsafe w systemie operacyjnym urządzeń.

- nadmierne opóźnienie,
- błąd adresacji,
- maskarada (pakiet standardowy zostanie tak zmodyfikowany, że jego struktura będzie zgodna z formatem pakietu PROFIsafe),
- błędy buforowania - w przypadku kanału, który może buforować pakiety (np. przełączniki, routery dla sieci Ethernet) może wystąpić błąd zapełniania/opróżniania bufora.

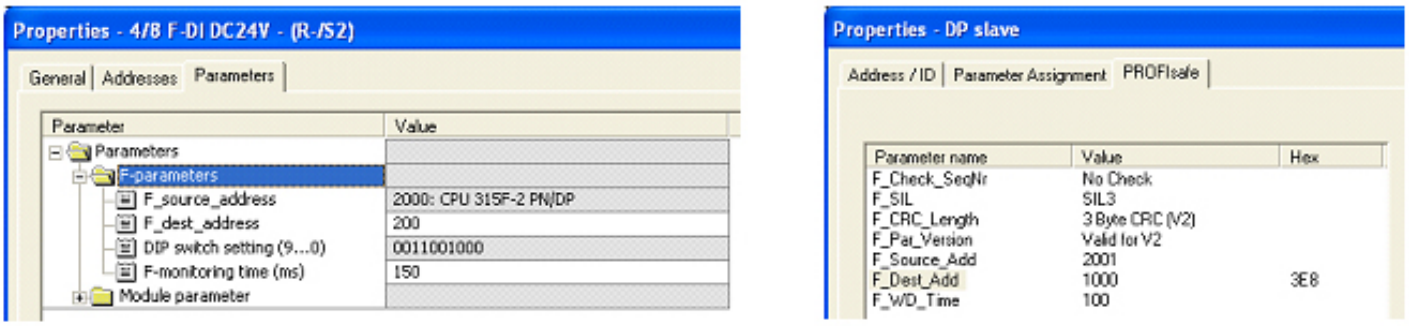
W celu detekcji wystąpienia tego typu błędów, dane procesowe przesyłane pomiędzy urządzeniami wykorzystującymi PROFIsafe dodatkowo zabezpieczane są poprzez:

- numer przekazywanego pakietu (licznik),
- dodatkowy adres dla nadawcy i odbiorcy pakietu (niezależny od adresu sieciowego). W przypadku modułów sygnałowych każdy z modułów otrzyma własny adres, który powinien być unikalny w ramach systemu,
- układ czasowy sprawdzający czy odpowiedź została otrzymana w zadanym czasie,
- własny mechanizm sprawdzania spójności pakietu niezależny od mechanizmu sprawdzania spójności dla całego pakietu.

Dodatkowy adres instancji PROFIsafe (z języka ang. określany jako F_Dest_Addr/F_Source_Addr) oraz czas, w jakim powinien zostać odebrany pakiet od partnera (F-monitoring time lub F_WD_time) definiowany jest we właściwościach modułu wykorzystującego profil PROFIsafe.

Licznik pakietów aktualnie jest licznikiem wirtualnym, ponieważ nie jest on przesyłany przez sieć (był przesyłany przez sieć w wersji 1.x profiu PROFIsafe). Jest on generowany na podstawie informacji zawartych w bajcie statusowym pakietu PROFIsafe.

Dodatkowo w przypadku PROFIsafe założono, że komunikacja pomiędzy stacjami odbywa się w sposób cykliczny i dlatego brak odpowiedzi (utrata pakietu) zostanie natychmiast wykryta i zasygnalizowana przez partnera. Innym założeniem jest komunikacja 1:1 pomiędzy urządzeniem peryferyjnym,



Ilustracja 11: Przykład definicji dodatkowych parametrów dla modułu wykorzystującego PROFIsafe

Poniższa tabela prezentuje zależność pomiędzy błędem, jaki może wprowadzić kanał komunikacyjny, a zabezpieczeniem pozwalającym na jego detekcję.

błąd \ zabezpieczenie	numer pakietu	nadzorowanie czasu wymiany pakietów	dodatkowy adres nadawcy/odbiorcy	spójność danych CRC2
niezamierzone powtórzenie pakietu	X			
utrata pakietu	X	X		
wstawienie dodatkowego pakietu	X	X	X	
zakłócenie sekwencji pakietów	X			
przekłamane pakietu				X
nadmierne opóźnienie		X		
błąd adresacji			X	
maskarada		X	X	X
błędy buforowania	X			

Ilustracja 12: : Mechanizmy zabezpieczające wprowadzone w PROFIsafe oraz błędy, jakie przy ich pomocy można wykryć

a kontrolerem (dane urządzenie/slot wymienia cyklicznie informacje tylko z jednym kontrolerem). Obydwa założenia są spełnione przez protokoły z rodziny PROFIBUS/PROFINET.

Należy podkreślić, że przedstawione mechanizmy dotyczą tylko komunikacji pomiędzy źródłem danych, a ich odbiorcą np. pomiędzy modułem sygnałowym, a kontrolerem i nie dotyczą elementów niezgodnych z PROFIsafe (np. standardowe moduły sygnałowe w stacji rozproszonych we/wy – patrz ilustracja 7).

Podsumowanie

Zintegrowane systemy bezpieczeństwa oparte na PROFIsafe to sprawdzona i bezpieczna technologia.

Integracja funkcji bezpieczeństwa w ramach jednego systemu sterowania może pociągać za sobą redukcję kosztów i oferuje dodatkowe możliwości funkcjonalne.

Jak każda nowa technologia jednocześnie jednak wymaga nabycia nowych kwalifikacji, zmiany przyzwyczajeń i podejścia do systemu sterowania, zarówno ze strony projektanta jak użytkownika końcowego.

mgr inż. Artur Szymiczek
Certified PROFIsafe Designer

INTEX Sp. z o.o.
PROFIBUS&PROFINET
Competence & Training Center

Mgr inż. Artur Szymiczek
CERTIFIED PROFIBUS&PROFINET ENGINEER
CERTIFIED PROFIsafe DESIGNER

Dyrektor Techniczny w firmie INTEX Centrum Szkoleniowe Systemów Automatyki, akredytowanej jednostce PROFIBUS&PROFINET INTERNATIONAL COMPETENCE&TRAINING CENTER.

Uznany w branży za wybitnego specjalistę w zakresie technologii PROFIBUS&PROFINET w Polsce, z piętnastoletnim doświadczeniem praktycznym.

Autor licznych publikacji i dokumentacji szkoleniowych z zakresu systemów sterowania opartych na rozwiązaniach firmy SIEMENS oraz systemów komunikacji przemysłowej.

W prowadzonych przez niego różnorodnych szkoleniach uczestniczyło już kilka tysięcy specjalistów w Polsce.

INTEX

Szkolenia otwarte z zakresu:

SIEMENS SIMATIC S7-300/400
SIEMENS SIMATIC S7-1200
SIEMENS SIMATIC S7-200
SIEMENS SIMATIC S5
SIEMENS SIMATIC HMI
SIEMENS SIMATIC PCS7
SIEMENS NAPĘDY

Szkolenia niezależne od zastosowanego sprzętu:

PROFIBUS & PROFINET
OPC
INDUSTRIAL ETHERNET
AS-INTERFACE

Ponad 20.000 uczestników

Szkolenia dla urzędów pracy i w ramach projektów EFS

Szkolenia zamknięte, wyjazdowe, doradztwo i konsultacje

Audyty i wykrywanie błędów sieci PROFIBUS

Narzędzia diagnostyczne i komponenty infrastruktury dla sieci PROFIBUS i PROFINET

Approved Partner firmy SIEMENS

Akredytowana jednostka PI Competence Center oraz PI Training Center

INTEX Sp. z o.o.
ul. Portowa 4
44-102 Gliwice

Tel. 32 230 75 16

Fax 32 230 75 17
intex@intex.com.pl
www.intex.com.pl