PI INTERNATIONAL

PROFIsafe
Opis systemu

Otwarty standard dla automatyki przemysłowej

PROFI PROCESS FIELD BUS

PROFI INDUSTRIAL ETHERNET

PROFIBUS PNO

Szanowni Państwo,

PROFIBUS PNO jest międzynarodową organizacją, która zajmuje się rozwojem i standaryzacją sieci przemysłowych w automatyce. Pomagamy użytkownikom i producentom urządzeń pracujących w sieci PROFIBUS wykorzystać najnowsze i najlepsze rozwiązania i technologie. Naszym członkom zapewniamy stały dostęp do wiedzy i informacji technicznych.

Nasza organizacja powstała, aby realizować i chronić standard komunikacji i sterowania.

Wstęp

PROFIBUS jest jedynym standardem komunikacji przemysłowej dostarczającym całościowe rozwiązania zarówno dla automatyki procesowej jak i przemysłowej. PROFINET jest nowoczesnym standardem dla automatyki, opartym na przemysłowej sieci ETHERNET, dynamicznie rozwijającym się w przeciągu ostatnich kilku lat.. Obydwa protokoły są oparte na Grupie Profili Komunikacyjnych 3 (Communication Profile Family 3) zawartej w normach: IEC 61158 oraz IEC 61784-1/-2.

Jednym z najważniejszych wydarzeń związanych z działalnością organizacji PROFIBUS and PROFINET International (PI) była pierwsza specyfikacja dla komunikacji w aplikacjach związanych z bezpieczeństwem i zabezpieczeniami (Safety) w 1999 roku. Spowodowało to duży postęp w świecie automatyki.

Technologia ta jest określana jako **PROFIsafe** i jest oznaczona symbolem pokazanym poniżej.

Od tego wydarzenia profil PROFIsafe znacznie się rozwinął i stał się czołową technologią komunikacyjną w systemach bezpieczeństwa na świecie. Obecnie dąży się do tego aby PROFIsafe stał się standardem międzynarodowym w ramach **IEC 61784-3-3**.

Celem tego dokumentu jest dostarczenie niezbędnych informacji o technologii PROFIsafe i zagadnieniach pokrewnych bez wgłębiania się w detale związne z funkcjonowaniem. Nie jest intencją jakakolwiek zmiana norm lub oficjalnych specyfikacji i wytycznych wspomnianych poniżej. Są one ostateczne i prawomocne.

PROFIsafe został zatwierdzony przez BGIA i TÜV.

Systemy bezpieczeństwa są szczególną częścią automatyki. Dlatego rozpowszechnianie i wdrażanie technologii PROFIsafe musi być potraktowane bardzo poważnie. Zaangażowane przedsiębiorstwa i instytucje są zobowiązane do postępowania zgodnie z tzw. Polityką PROFIsafe (**PROFIsafe Policy**).

Ten krótki opis ma służyć jako dopełnienie i skromne podsumowanie oficjalnych dokumentów.

Skrót “F” w tym dokumencie oznacza “fail – safe”, “functional safety” lub “safety related”.

SPIS TREŚCI

1. Bezpieczeństwo w automatyce

Każdy aktywny proces przemysłowy jest w większym lub mniejszym stopniu powiązany z ryzykiem:

- okaleczenia lub śmierci ludzi,
- szkód w środowisku naturalnym,
- zniszczenia urządzeń.

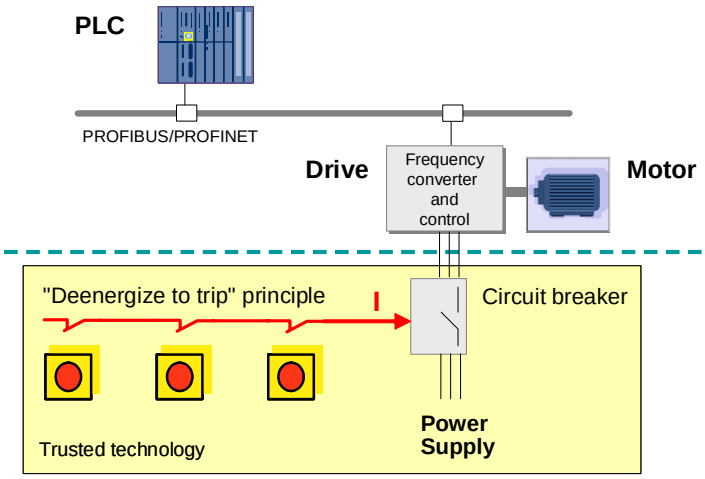
W większości procesów można wyeliminować ryzyko bez nakładania specjalnych wymagań na systemy automatyki. Jednakże istnieją aplikacje związane z wysokim ryzykiem n.p.: prasy, piły, roboty, systemy transportu i pakowania, procesy chemiczne, aplikacje w których występuje wysokie ciśnienie, systemy przeciwpożarowe, palniki, itd. Wspomniane aplikacje wymagają szczególnej ostrożności i zastosowania specjalnych technologii.

Obecnie na rynku są zauważalne tendencje do zachowania proporcji pomiędzy niezawodnością i dostępnością technologii w automatyce przy zachowaniu pewnego ustalonego poziomu kosztów. Oznacza to, że poziom zawodności lub usterkowości technologii jest akceptowalny w standardowych warunkach, ale nie wystarczający w aplikacjach o podwyższonym ryzyku.

Sytuacja ta może być porównana do systemu pocztowego. Przy dostarczeniu standardowej przesyłki oczekuje się możliwie najmniejszych kosztów przy zachowaniu pewnego ustalonego poziomu rzetelności usługi, natomiast do wysłania ważnej przesyłki każdy użyje opcji priorytetowej.

1.1 Tendencje

W przeszłości mikrokontrolery, oprogramowanie, komputery osobiste i sieci komunikacyjne w znaczny sposób wpływały na standardowe technologie w automatyce prowadząc przez to do redukcji kosztów, poprawy



Rysunek 1 Klasyczny układ bezpieczeństwa

elastyczności, wyższej dostępności. W aplikacjach o podwyższonych wymogach bezpieczeństwa, istniejące standardy i regulacje zabraniały stosowania tego rodzaju technologii. Systemy sterowania w tego rodzaju aplikacjach musiały być oparte wyłącznie na technologii przekaźnikowej. Patrz Rysunek 1.

Ta dwudzielność lub luka jest dosyć naturalna biorąc pod uwagę fakt, że bezpieczeństwo systemu jest oparte na sprawdzonej, niezawodnej technologii i materiałach. Niezawodność z kolei jest oparta na doświadczeniu. Jednak połączenie klasycznego „bezpieczeństwa” z nowoczesnymi rozwiązaniami stosowanymi w automatyce zawsze prowadzi do rozczarowań. Na przykład koszty dodatkowego okablowania i prac inżynieryjnych, mniejsza elastyczność i dostępność niż oczekiwano i inne wady jak nieokreślone pozycje zatrzymania maszyn i trudności z przywróceniem ich do pracy.

Sytuacja obecnie uległa diametralnej zmianie. Mikro kontrolery i oprogramowanie sprawdzają się przy zastosowaniu w milionach aplikacji. Od czasu opublikowania normy IEC 61508 są także podstawy do stosowania ich w systemach bezpieczeństwa.

Z powodzeniem zostały opracowane mechanizmy wykrywania błędów w wielu typach cyfrowych systemów komunikacji. Normy takie jak IEC 62280-1 utorowały drogę do tego.

1.2 Osiągnięcia PI

PI opracowała technologię PROFIsafe jako dodatkową warstwę nałożoną na istniejące protokoły PROFIBUS i PROFINET. Pozwala to na zmniejszenie prawdo-podobieństwa błędu w komunikacji pomiędzy stacją nadrzędną F–Host i urządzeniem F–Device do poziomu wymaganego przez obowiązujące normy lub niższego.

PROFIsafe jest realizowany wyłącznie na poziomie oprogramowania, co upraszcza jego implementację, zarówno dla systemów komunikacji opartych na standardzie PROFIBUS jak i PROFINET. Realizacja profilu PROFIsafe jest także możliwa poprzez bezprzewodowe kanały transmisji, takie jak **WLAN** i **Bluetooth**. Przy zastosowaniu odpowiednich systemów zabezpie- czających można wykorzystać otwartą sieć Industrial Ethernet.

Dzięki temu zrealizowane są wymagania dostępności i niskiego zużycia mocy w automatyce procesowej jak

również wymagania dotyczące krótkiego czasu reakcji, rzędu milisekund, w automatyce maszyn.

Nowoczesne urządzenia failsafe (z oznaczeniem F), takie jak ska- nery laserowe lub napędy failsafe mogą być konfigurowane zgodnie z potrzebami. Obsługa indywidualnych parametrów związanych z funkcjami bepzieczeństwa tych urządzeń (iParameters) została uproszczona dzięki zaawansowanemu systemowi wsparcia technicznego. Wspomniane wsparcie obejmuje interfejsy dla urządzeń failsafe, narzędzia inżynierskie (n.p. Tool Calling Interface) oraz funkcje zapisu i odzysku parametrów (**iPar-Server**). Warto podkreślić, że nakładki narzędziowe oraz funkcja iPar-Server mogą także być wykorzystane przez urządzenia nie pracujące w standardzie PROFIsafe.

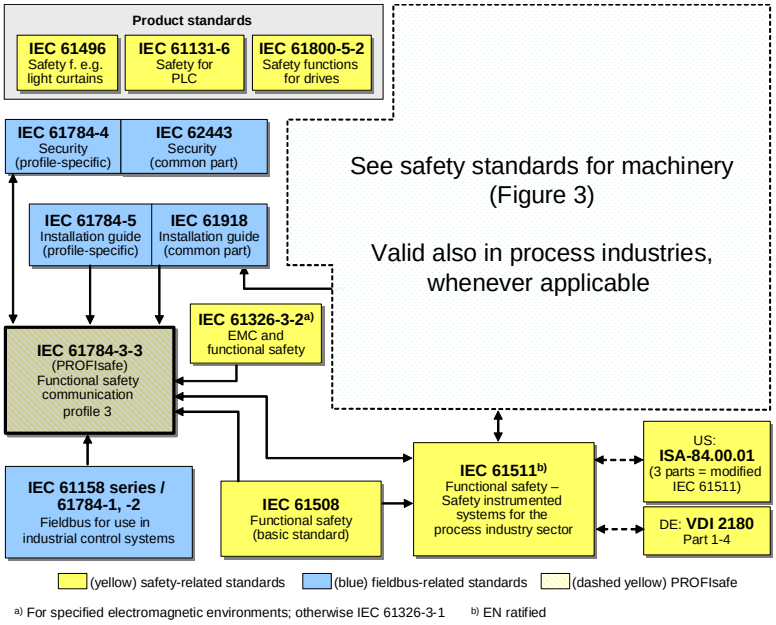
Norma IEC 61508 określa specjalne wymagania, takie jak zwiększona odporność na zakłócenia elektromagnetyczne bez wchodzenia w szczgóły techniczne. Uzupełnieniem tego, jest dokument "**PROFIsafe Environment**", który zawiera dodatkowe informacje, pomocne w implementacji układów o podwyższonym bezpieczeństwie.

Organizacja PI dopuszcza do użytku w systemach bezpieczeństwa opartych na standardach PROFIBUS i PROFINET tylko urządzenia certyfikowane zgodnie z normą IEC 61508. Zgodność z profilem PROFIsafe powinna być potwierdzona przez laboratorium testowe organizacji PI i zatwierdzona przez biuro PNO. Dodatkowy dokument "**PROFIsafe Test Specification**" określa rolę i zadania organizacji certyfikujących, jak TÜV oraz rolę i zadania laboratoriów testowych PI.

Na stronach www.profisafe.net oraz www.profibus.com można znaleźć więcej informacji na temat profilu PROFIsafe oraz ogólnych informacji o profilach PROFIBUS i PROFINET.

1.3 Standardy międzynarodowe

W większości krajów prawo określa sposób ochrony ludzi i środowiska. W Europie



Rysunek 2 Normy międzynarodowe dotyczące bezpieczeństwa i sieci polowych w automatyce procesowej

przykładami takich wytycznych są: “Low Voltage Directive”, “EMC Directive”, “Machinery Directive”. Przepisy poszczególnych krajów odnoszą się z kolei do standardów międzynarodowych.

Na Rysunku 3 pokazane zostały wybrane normy IEC oraz ISO dotyczące zagadnień bezpieczeństwa, sieci polowych i powiązania między nimi.

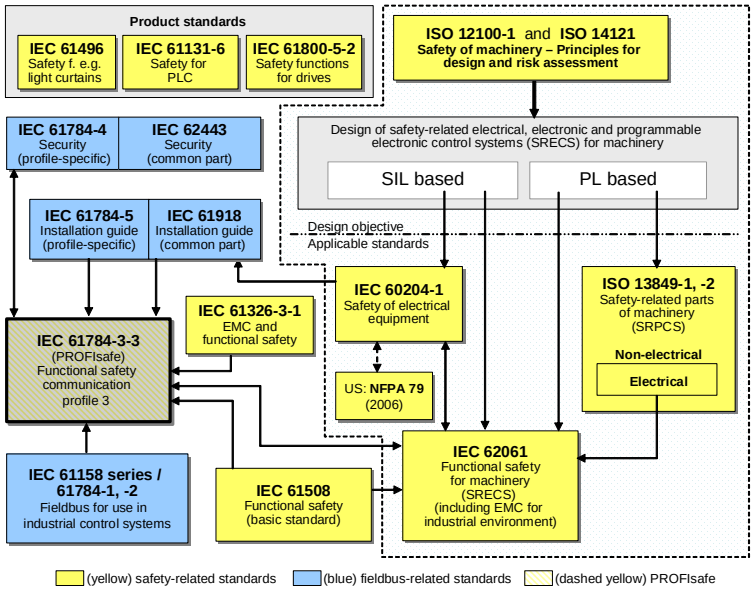
IEC 61508 jest główną normą dotyczącą zagadnień bezpieczeństwa funkcjolanego urządzeń elektrycznych, zastosowanych w aplikacjach o podwyższonym bezpieczeństwie. Dokument przedstawia ilościowe podejście do obliczeń poziomu nienaruszalności bezpieczeństwa (Safety Integrity Level - **SIL**). Jest to szczególnie użyteczne dla producentów urządzeń o podwyższonym bezpieczeństwie. Norma IEC 62061 opisuje specyficzne aspekty bezpieczeństwa maszyn oraz urządzeń i procesów przemysłowych. Standard ten dotyczy gotowych systemów, podsystemów i elementów oraz sposobów oceny funkcji bezpieczeństwa i ich kombinacji. Norma ISO 13849-1 jest następcą EN 954-1 i prezentuje podobny układ. Przedstawia jednak inny model obliczeniowy (Performance Levels - **PL**), który uwzględnia urządzenia, takie jak zawory hydrauliczne, itd. Norma ISO 12100-1 określa podstawową terminologię i metodologię z zakresu bezpieczeństwa maszyn. Norma ISO 14121 określa zasady szacowania ryzyka. Norma IEC 60204-1 określa ogólne wymagania i zalecenia dotyczące elektrycznego wyposażenia maszyn. Porusza zagadnienia takie jak zasilanie, ochrona przeciwporażeniowa, wyłączniki bezpieczeństwa, przewodniki i kable, itd. Normy produktowe takie jak IEC 61496, IEC 61800-5-2, i IEC 61131-6, opisują wymagania dla poszczególnych rodzin urządzeń.

Załącznik „Europejskiej dyrektywy maszynowej” (European Machinery Directive) wymienia urządzenia i części, które prawnie wymagają certyfikacji przez uprawniony organ (BIA, TÜV, FM (Factory Mutual), etc.). Jeśli istnieje odpowiednia, spójna norma (n.p. IEC 61496), oświadczenie producenta jest wystarczające.

Norma IEC 61326-3-1 określa wymagania podwyższonej odporności na zakłócenia elektromagnetyczne dla urządzeń F-Device oraz F-Host. Specjalne kryteria określające poziom bezpieczeństwa funkcjonalnego (functional safety - **FS**), pozwalają na niewłaściwe działanie urządzeń w warunkach zwiększonych zakłóceń elektromagnetycznych, przekraczających normalnie wyznaczone wartości. Jednakże, w takich przypadkach urządzenia (equipment under test - **EUT**) powinny przejść w stan bezpieczny.

Wytyczne dotyczące sieci polowych zostały określone w normach IEC 61158 oraz IEC 61784-1. Rozwiązania Realtime Ethernet takie jak PROFINET IO są określone w normie IEC 61784-2. Wspólne wytyczne dotyczące instalacji systemu (**installation guidelines**) zostały zebrane w normie IEC 61918, podczas gdy wymogi dotyczące poszczególnych profili znajdują się w normie IEC 61784-5. Wspólne wytyczne dotyczące bezpieczeństwa systemu (**safety guidelines)** zostały zebrane w normie IEC 62443, podczas gdy wymogi dotyczące poszczególnych profili znajdują się w IEC 61784-4.

Na Rysunku 2 pokazane zostały wybrane normy IEC oraz ISO zawierające wymogi dotyczące automatyki procesowej. Norma sektorowa IEC 61511 uwzględnia szczególną sytuację długofalowych doświadczeń (sprawdzonych w praktyce) z bardzo czułym oprzyrządowaniem procesowym i określonym środowiskiem elektromagnetycznym. Norma IEC 61326-3-2 bierze pod uwagę wspomniane wymagania EMC.



Rysunek 3 Normy międzynarodowe dotyczące bezpieczeństwa i sieci polowych w automatyce maszyn

2. Zadania

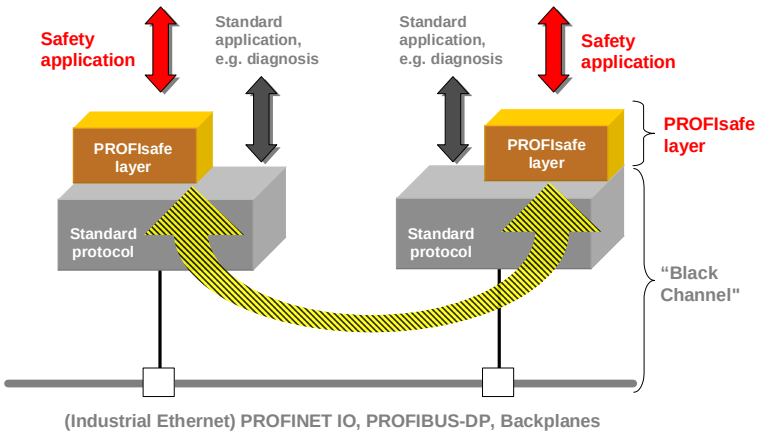
Od początku założeniem twórców profilu PROFIsafe było stworzenie wyczerpującego i wydajnego rozwiązania zarówno dla producentów jak i użytkowników urządzeń o podwyższonym bezpieczeństwie.

Protokół PROFIsafe powinien być kompatybilny z sieciami PROFIBUS i PROFINET bez wpływu na te istniejące już standardy sieci polowych. Możliwa powinna być transmisja danych systemu bezpieczeństwa – failsafe, za pomocą istniejących, standardowych kabli sieciowych razem ze „standardowymi" danymi. Rysunek 5.

"Jednokanałowe" ("Single Channel") rozwiązanie pozwala na komunikację ze standardowymi PLC posiadającymi zintegrowaną, ale logicznie odseparowaną funkcjonalność pozwalającą na przetwarzanie danych failsafe. Dzięki temu nie jest konieczne tworzenie równoległych połączeń. Redundancja medium może być realizowana opcjonalnie w celu osiągnięcia większej dostępności. Dla użytkowniów, którzy preferują fizyczną separację komunikacji standardowej i safety, zastosowanie profilu PROFIsafe nie będzie przeszkodą. Ponieważ można z powodzeniem wykorzystywać technologie PROFIBUS i PROFINET w oddzielnych sieciach.

Protokół PROFIsafe nie powinien w żaden sposób wpływać na standardowe protokoły sieciowe. Powinien także być możliwie niezależny od podstawowego medium transmisji, którym mogą być kable miedziane, światłowody, transmisja bezprzewodowa lub magistrala wewnętrzna. Takie czynniki jak prędkość czy wykrywanie błędów transmisji nie powinny mieć wpływu na działanie protokołu. Z punktu widzenia PROFIsafe są to warstwy transmisji „Black channel" (czarne kanały) Rysunek 4.

Wykorzystanie protokołu PROFIsafe powinno zwolnić użytkowników z konieczności oceny połączeń komunikacyjnych będących poza sieciami PROFIBUS i PROFINET, takich jak magistrala wewnętrzna. Funkcje zawarte w protokole powinny zatem zabezpieczać całą ścieżkę komunikacyjną od miejsca pochodzenia sygnału failsafe (n.p. moduł o podwyższonym bezpieczeństwie w oddalonym urządzeniu I/O), do miejsca, w którym zostanie on przetworzony (urządzenie nadrzędne F-Host) i vice versa. Rysunek 6

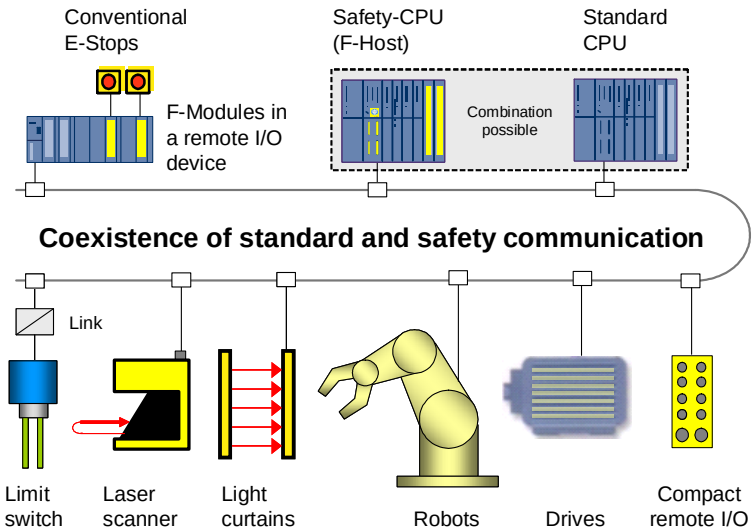


Rysunek 4 Założenie "Black Channel"

PROFIsafe pozwala na zachowanie poziomu bezpieczeństwa SIL3 zgodnie z normami IEC 61508 / IEC 62061, lub Kategorii 4 zgodnie z normą EN 954-1 lub PL "e" według normy ISO 13849-1.

Parametry protokołu PROFIsafe powinny być określane za pomocą standardowych mechanizmów sieci PROFIBUS i PROFINET, n.p. poprzez pliki GSD. Jednak parametry powinny być zabezpieczone podczas przechowywania, przypisywania wartości i przesyłu z narzędzia konfiguracyjnego do Kontrolera I/O lub Mastera DP i następnie do urządzenia podrzędnego F-Device. Wszystkie urządzenia F-Device i Moduły (F-Module) oddalonego urządzenia I/O powinny korzystać ze wspólnego zbioru parametrów w celu zapewnienia spójnej obsługi tych urządzeń.

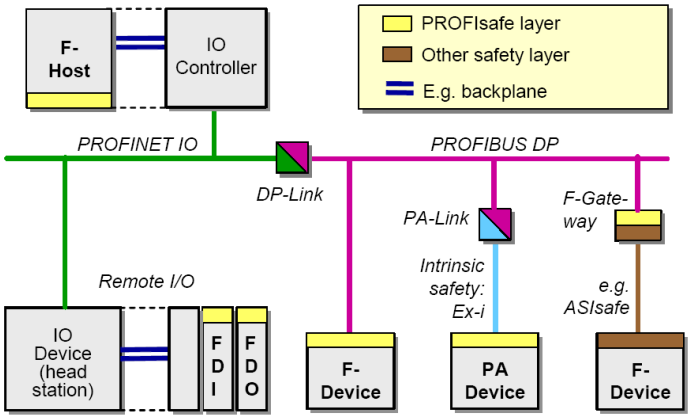
Indywidualne parametry urządzeń F-Device są specyficzne dla danej technologii, n.p. napędy ze obsługujące protokół PROFIsafe, skanery laserowe, itd. Obsługa tych parametrów



Rysunek 5 Założenie „wspólnego kanału" transmisji danych

poprzez pliki GSD pociąga za sobą ogromne nakłady pracy i zbędne zależności. Dlatego producenci urządzeń safety powinni mieć możliwość zintegrowania ich indywidualnych narzędzi do konfiguracji, parametryzacji i diagnostyki (narzędzia CPD) z narzędziami inżynierskimi poprzez odpowiednie interfejsy. Ułatwi to dostęp i komunikację z określonymi urządzeniami i modułami safety.

W celu umożliwienia szybkiej wymiany urządzenia F-Device w przypadku jego awarii, system powinien zapamiętać i przywrócić indywidualne parametry funkcji bezpieczeństwa (iPar-Server).



Rysunek 6 Elementy w sieci obsługiwane przez PROFIsafe

Urządzenie F-Host lub kontroler, który przeprowadza wstępną parametryzację, także powinien posiadać tę opcję.

Dodatkowa dokumentacja powinna określać wszystkie aspekty wykorzystania urządzeń o podwyższonym bezpieczeństwie, takie jak wymagania dla:

- Instalacji
- Bezpieczeństwa elektrycznego
- Zasilania
- Kompatybilności elektromagnetycznej
- Bezpieczeństwa danych

Producenci urządzeń o podwyższonym bezpieczeństwie wykorzystujących standard PROFIsafe powinni mieć dostęp do wsparcia technicznego w postaci centrów kompetencyjnych i laboratoriów testowych.

PROFIsafe w obecnej wersji spełania wszystkie wspomniane założenia.

Zanim dowiemy się czegoś więcej o protokole PROFIsafe przyjrzyjmy się niektórym wstępnym założeniom i ograniczeniom.

3. Ograniczenia warstwy "Black channel"

Mimo tego, że przy komunikacji w protokole PROFIsafe wykorzystywana jest koncepcja warstwy “Black channel”, są pewne elementy sieci PROFIBUS i PROFINET, które były brane pod uwagę w jego projektowaniu.

3.1 Podstawowe właściwości

Jedną z tych właściwości jest cykliczna wymiana danych pomiędzy kontrolerem i urządzeniami polowymi (wysłanie zapytania i oczekiwanie na odpowiedź). Zastosowanie mechanizmu odpytywania pozwala na natychmiastowe wykrycie uszkodzonego urządzenia. Mechanizm ten został zaadoptowany w standardzie PROFIsafe, dzięki czemu uniknięto konieczności odrębnego sprawadzania poprawności działania urządzeń.

Kolejną cechą komunikacji, zaadoptowaną w protokole PROFIsafe, jest relacja 1:1 pomiędzy kontrolerem sieci i urządzeniami polowymi, z którymi współpracuje. Dzięki temu, zapewniona jest autentyczność przesyłanych informacji. Powstaje jednak ograniczenie dostępności do modułu, będącego częścią urządzenia polowego, tylko przez jedno urządznie nadrzędne F-Host.

3.2 Komponenty sieci

Warstwa „Black channel” może składać się z kilku rodzajów komponentów sieciowych, takich jak switche, routery, łącza i bezprzewodowe kanały transmisyjne. W profilu PROFIsafe, istnieją pewne ograniczenia, mające na celu spełnienie wymagań klasy

Measure: / Error:	Consecutive Number (sign of life)	Time-out (with receipt)	Codename (for sender and receiver)	Data integrity (CRC)
Unintended repetition	X			
Loss	X	X		
Insertion	X	X	X	
Incorrect sequence	X			
Corruption				X
Unacceptable delay		X		
Adressing			X	
Masquerade (standard message mimics failsafe)		X	X	X
Revolving memory failures within switches	X			

Rysunek 7 Typy błędów transmisji i środki zapobiegawcze

bezpieczeństwa SIL3.

Dopuszcza się wykorzystanie wszelkiego rodzaju switchy, ale maksymalnie 100 można połączyć w szereg. Przestrzeń adresowa w obrębie wyspy PROFIsafe musi być niepowtarzalna. Połączone wyspy korzystające z tej samej przestrzeni adresowej muszą być odseparowane przez wykorzystanie routerów wieloportowych. Nie ma ograniczeń przy stosowaniu urządzeń służących do konwersji z sieci PROFINET do sieci PROFIBUS i dalej do wersji iskrobezpiecznej MBP-IS (Rysunek 6).

3.3 Bezpieczeństwo sieci bezprzewodowej

Bezprzewodowa transmisja danych jest dopuszczalna przy zagwarantowaniu odpowiedniego poziomu zabezpieczeń.

PROFIsafe określa pewne wymogi bepieczeństwa dla transmisji bezprzewodowej oraz dla sieci przewodowych połączonych z siecią Industrial Ethernet lub z otwartą siecią Internet.

3.4 Typy danych

Komunikacja polowa wykorzystuje wiele różnych typów danych do przesyłu informacji (patrz spis literatury str. 11). PROFIsafe wprowadza pewne uproszczenia poprzez zredukowanie ilości wykorzystywanych typów danych.

4. PROFIsafe – rozwiązanie

Zadaniem komunikacji w systemach bezpieczeństwa – safety, jest dostarczenie:

- Poprawnych danych
- Do odpowiedniego partnera
- Na czas

Przy transferze danych w sieciach o złożonej topologii mogą wystąpić różne błędy, spowodowane usterkami urządzeń, zakłóceniami transmisji lub innymi czynnikami. Dane mogą zostać utracone, powtarzać się, zostać pobrane z nieodpowiedniego miejsca, pojawić się z opóźnieniem lub w nieodpowiedniej kolejności, lub/i zawierać złe informacje. W przypadku komunikacji safety może także wystąpić nieodpowiednia adresacja: komunikaty standardowe omyłkowo pojawiają się na urządzeniu F-Device jako komunikaty safety. Błędy mogą powstawać także przy transmisji w sieciach o różnej prędkości. Poza licznymi rozwiązaniami znanymi z literatury, PROFIsafe koncentruje się na przedstawionych w tabeli, Rysunek 7.

4.1 Zabezpieczenia

Do kontroli transmisji w profilu PROFIsafe dodatkowo zastosowano:

- Seryjne numerowanie telegramów bezpieczeństwa
- Specyfikację czasową przychodzących telegramów ("watch-dog").
- Wprowadzenie haseł pomiędzy nadawcą i odbiorcą ("F-Address").
- Dodatkową sumę kontrolną dla zabezpieczenia danych (CRC = cyclic redundancy check)

Seryjne numerowanie (Consecutive Number) pozwala odbiorcy na sprawdzenie czy otrzymane dane są kompletne i dotarły w odpowiedniej kolejności. Odbiorca jako potwierdzenie wysyła do nadawcy także numerowane kolejno telegramy. Zasadniczo wędrujący bit (toggle bit) wystarcza. Ponieważ niektóre komponenty sieciowe mają funcje buforowe, n.p. switche, PROFIsafe wykorzystuje 32 – bitowy licznik.

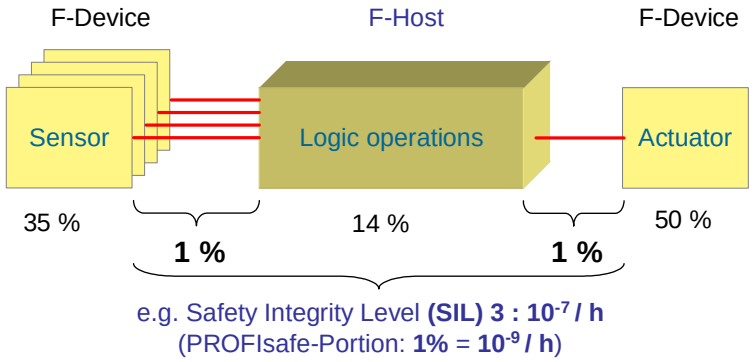
W systemach bezpieczeństwa ważne jest nie tylko, że otrzymane telegramy zawierają odpowiednie sygnały lub wartości, ale także, że dotrzą do odbiorcy w ściśle określonym czasie, umożliwia to automatyczną reakcję n.p. zatrzymanie urządzenia. W tym celu urządzenia safety wykorzystują timery (watchdog timers), które są resetowane za każdym razem kiedy do odbiorcy dociera nowy telegram PROFIsafe oznaczony kolejnym numerem.

Relacja 1:1 pomiędzy stacjami master i slave ułatwia wykrywanie błędnie skierowanych telegramów. Zarówno nadawca jak i odbiorca muszą posiadać oznaczenie (codename), które jest niepowtarzalne w obrębie sieci i może być wykorzystane do weryfikacji autentyczności telegramu PROFIsafe. PROFIsafe wykorzystuje do tego specjalny adres (F-Address), którym oznaczone jest każde urządzenie.

Suma kontrolna (Cyclic Redundancy Check CRC) odgrywa kluczową rolę w wykrywaniu uszkodzonych danych. PROFIsafe do podstawowej analizy propabilistycznej wykorzystuje zasady zawarte w normie IEC 61508, która określa prawdopodobieństwo wystąpienia niebezpiecznych błędów w funkcjach bezpieczeństwa, Rysunek 8.

Zgodnie z tymi założeniami obwód bezpieczeństwa zawiera wszystkie czujniki, urządzenia wykonawcze, elementy do przesyłu danych, procesy logiczne, które są umieszczone w funkcji bezpieczeństwa. IEC

PROFIsafe, leaving 99% of the budget for failures in sensors, actuators, or logic operations.



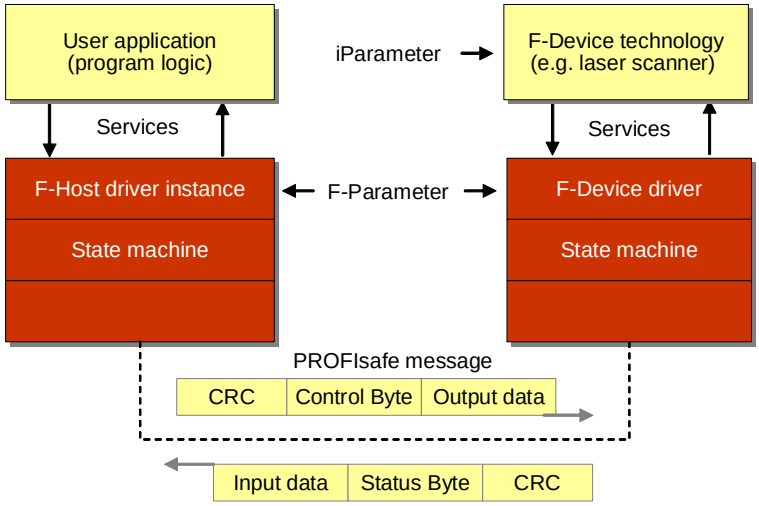
Rysunek 8 Funkcje bezpieczeństwa i poziom SIL

61508 definiuje ogólne prawdopodobieństwo wystąpienia błędu dla różnych poziomów zabezpieczeń SIL. Na przykład dla poziomu SIL3 jest to 10^{-7}/h. Przewidziano 1% udział dla błędów powstających przy transmisji danych w ogólnej wartości prawdopodobieństwa wystapienia błędu, co oznacza, że dopuszczalna wartość prawdopodobieństwa wystąpienia błędów transmisji wynosi 10^{-9}/h. Pozwala to na wyznaczenie odpowiednich wielomianów CRC dla poszczególnych długości telegramów PROFIsafe. PROFIsafe wykorzystuje 24 i 32 bitowe generatory wielomianów do wyliczenia 3 lub 4 bajtowych oznaczeń. Jakość wybranych wielomianów CRC oraz specjalna metoda obliczeń sprawia, że PROFIsafe jest całkowicie niezależny od mechanizmów wykrywania błędów warstwy „Black channel".

For example, for SIL3 this is 10^{-7}/h. PROFIsafe uses a carefully selected 32-bit CRC generator polynomial, which ensures a probability of dangerous failures per hour of less than 10^{-9}/h. This value is guaranteed, independent of the "Black Channel" in use. Thus, even in SIL3 applications, less than 1% of the overall budget of 10^{-7}/h per safety function is consumed by

4.2 Format ramki PROFIsafe

Wiadomość PROFIsafe wymieniana pomiędzy urządzeniem nadrzędnym F-Host i urządzeniem F-Device jest przesyłana jako nakładka standardowej ramki PROFIBUS lub PROFInet. W przypadku urządenia podrzędnego F-Device o budowie modułowej z kilkoma modułami safety cały pakiet przesyłanych danych składa się z kilku wiadomości PROFIsafe. Rysunek 9 prezentuje format ramki PROFIsafe.



Rysunek 10 Struktura warstwy PROFIsafe w urządzeniach F-Host i F-Device

Na początku ramki znajdują się dane wejściowe/wyjściowe. Struktury danych, dla poszczególnych urządzeń safety, w większości przypadków są określone przez odpowiednie pliki GSD (General Station Description). Zazwyczaj

F-Input/Output data	Status / Control Byte	CRC signature
		across F-Parameter, F-I/O data, Status/Control Byte, Monitoring Number
1 to 12/13 (max. 123) bytes	1 byte	4 bytes

Rysunek 9 Format ramki PROFIsafe

inne wymagania są stawiane przed systemem bezpieczeństwa przy wykorzystaniu go w automatyce maszyn a inne w automatyce procesowej. W pierwszym przypadku system oparty jest na bardzo szybkim przetwarzaniu krótkich zmiennych bitowych, w drugim przetwarzane są dłuższe (zmienno - przecinkowe) zmienne procesowe, co może zabierać trochę więcej czasu. Dlatego PROFIsafe oferuje struktury danych o dwóch różnych długościach. Krótsza, maksymalnie 12-bajtowa, wymagająca 3-bajtowego oznaczenia CRC. Dłuższa ograniczona do 123 bajtów, wymagająca 4-bajtowego oznaczenia CRC.

Dane systemu bezpieczeństwa - wejściowe/wyjściowe, spełniają funkcję bajtu kontrolnego jeśli wiadomość jest wysłana przez urządzenie nadrzędne F-Host lub bajtu statusowego w przypadku gdy nadawcą jest urządzenie podrzędne F-Device. Informacja ta jest potrzebna do synchronizacji wiadomości PROFIsafe nadawcy i odbiorcy.

Jak wspomniano powyżej dane PROFIsafe są zakończone sumą kontrolną (CRC) o danej długości w zależności od typu danych wejściowych/wyjściowych.

Przesyłane telegramy PROFIsafe nie zawierają informacji o ich kolejnych numerach. Zarówno nadawca jak i odbiorca wykorzystują do tego wewnętrzne liczniki, których praca jest synchronizowana poprzez bajt statusowy i kontrolny. Poprawność synchronizacji jest monitorowana poprzez wykorzystanie wartości liczników przy obliczaniu sumy kontrolnej.

Adres safety jest zabezpieczony także poprzez wykorzystanie go przy obliczaniu sumy kontrolnej.

4.3 Usługi PROFIsafe

Nadawcy i odbiorcy telegramów PROFIsafe działają w oparciu o warstwy znajdujące się powyżej warstw komunikacyjnych określanych jako "Black Channel" (Rysunek 4). Zazwyczaj warstwy PROFIsafe są realizowane programowo poprzez wykorzystanie specjalistycznych protokołów. Do ich głównych zadań należy kontrolowanie stanu urządzenia, cykliczne przetwarzanie telegramów PROFIsafe i wyjątków takich jak uruchomienie, włączenie/wyłączenie zasilania, obsługa błędów sumy kontrolnej itd. Rysunek 10 pokazuje jak wartswa PROFIsafe komunikuje się z częścią technologiczną urządzenia podrzędnego F-Device i programem użytkownika zawartym w urządzniu nadrzędnym F-Host.

4.3.1 Usługi F-Host

Do zadań wykonywanych przez urządzenie nadrzędne F-Host należy przetwarzanie danych wejściowych i wyjściowych związanych z funkcjami bezpieczeństwa. Podczas uruchomienia lub w wypadku wystąpienia błędów wartości bieżące poszczególnych zmiennych są automatycznie zastępowane poprzez domyślne wartości bezpieczne (fail-safe). Wszystkie zmienne powinny przyjąć wartość “0” w celu ustawienia odbiornika w stan bezpieczny (zdjęcie zasilania).

W przypadku urządzeń podrzędnych F-Device gdzie zdjęcie zasilania nie jest jedynym możliwym stanem bezpiecznym, ale warunki bezpieczeństwa są spełnione przy np. ustawieniu mniejszej prędkości, PROFIsafe umożliwia definiowanie tego typu stanów przez ustawienie flagi w bajcie kontrolnym (activate_FV). Jako odpowiedź, urządzenie podrzędne F-Device poprzez ustawienie odpowiedniej flagi w bajcie statusowym (FV_acivated), przesyła do programu użytkownika potwierdzenie przejścia w stan bezpieczny.

Błędy w komunikacji PROFIsafe powodują, że driver urządzenia nadrzędnego F-Host wymusza przejście w stan bezpieczny. Zazwyczaj funkcja bezpieczeństwa nie ma możliwości samoczynnego przejścia ze stanu bezpiecznego do stanu normalnej pracy bez świadomej ingerencji człowieka. W celu poinformowania programu użytkownika, że niezbędna jest interwencja operatora i potwierdzenie, PROFIsafe udostępnia dodatkową usługę „OA_Req”. PROFIsafe informuje urządzenie podrzędne F-Device o zgłoszeniu oczekującym. Dzięki temu urządzenie może to zasygnalizować poprzez diodę LED (opcjonalne). Potwierdzenie operatora może zostać przekazane z programu użytkownika do urządzenia nadrzędnego F-Host dzięki usłudze „OA_C”.

Parametry urządzenia F-Device specyficzne dla danej technologii są określane jako iParameters. Dodatkowe usługi umożliwiają zmianę parametrów urządzenia F-Device w trakcie jego pracy. Usługa „iPar_EN” pozwala na przełączenie urządznia podrzędnego w tryb gotowości do przyjęcia nowego zestawu parametrów iParameters. Usługa “iPar_OK” pozwala na zgłoszenie do programu użytkownika gotowości powrotu do normalnego trybu pracy.

4.3.2 Usługi F-Device

Usługi PROFIsafe dla urządzenia podrzędnego F-Device obejmują między innymi wymianę danych F-I/O, dodatkową możliwość generowania i zawiadamiania o wartościach fail-safe, wskaźniki obsługi parametrów iParameters oraz dla żądania operatora. Zastosowana technologia pozwala także na wysłanie do drivera urządzenia F-Host informacji o błędach w urządzeniu podrzędnym F-Device poprzez flagę "Device_Fault" w bajcie Status Byte.

Urządzenie F-Device powinno ponawiać żądanie reakcji na tyle długo, aby zostało one przesłane przez komunikację PROFIsafe (co najmniej przez czas dwóch inkrementacji kolejnego numeru telegramu). Jest to możliwe dzięki specjalnej usłudze przesyłającej do urządzenia F-Device informację o zmianie kolejnego numeru telegramu.

Informacje diagnostyczne mogą być przekazywane z warstwy PROFIsafe do warstwy technologicznej dzięki wykorzystaniu specjalnej usługi.

Istotny jest także fakt, że urządzenie F-Device jest w stanie przesłać parametry fail-safe (F-Parameters) do warstwy PROFIsafe. Urządzenie F-Device otrzymuje parametry fail-safe razem z wszystkimi innymi podczas uruchomienia. Znaczenie i funkcje parametrów fail-safe (F-Parameters) zostały opisane poniżej.

4.4 Parametry fail-safe (F-Parameters)

Parametry fail-safe (F-Parameters) zawierają informacje dla warstwy PROFIsafe potrzebne do dostosowania jej funkcji do konkretnych potrzeb klienta. Do najważniejszych parametrów fail-safe należą:

- F_S/D_Address (short F-Address)
- F_WD_Time
- F_SIL
- F_iPar_CRC
- F_Par_CRC

Parametr F_S/D_Address określa adres urządzenia safety, który jest unikalny w obrębie jednej wyspy PROFIsafe. Urządzenie F-Device porównuje przypisany F-Adres z lokalnie przpisaną mu wartością za pomocą przełączników zintegrowanych w urządzeniu lub z wprowadzoną wartością w celu zapewnienia poprawności połączenia.

Parametr F_WD_Time określa liczbę milisekund dla timera watchdog. Timer ten jest wykorzystywany do kontrolowania czasu nadejścia kolejnego telegramu PROFIsafe.

Parametr F_SIL zawiera informację na temat poziomu SIL, którego oczekuje użytkownik. Wartość tego parametru jest porównywana z lokalną wartością zdefiniowaną przez producenta urządzenia.

Parametr F_iPar_CRC pełni funkcję sygnatury dla całego zestawu parametrów iParameters dla urządzenia F-Device.

Parametr F_Par_CRC jest sygnaturą dla wszystkich parametrów fail-safe. Jego zadaniem jest zapewnienie poprawnego dostarczenia wszystkich parametrów fail-safe.

- PROFIsafe Policy V1.3; Order No. 2.282
- PROFIsafe - Profile for Safety Technology on PROFIBUS DP and PROFINET IO, V2.4; Order No. 3.192b
- PROFIsafe – Environmental Requirements, V2.5; Order No. 2.232
- PROFIsafe – Test Specification for F-Slaves, F-Devices, and F-Hosts, V2.1; Order No. 2.242
- PROFIsafe for PA-Devices, V1.0; Order No. 3.042
- PROFIdrive on PROFIsafe, V1.0; Order No. 3.272
- Rapid way to PROFIBUS DP; Order No. 4.072
- Industrial Communications with PROFINET; Order No. 4.182
- Specification for PROFIBUS Device Description and Device Integration, Volume 1: GSD, V5.04; Order No. 2.122
- GSDML Specification for PROFINET IO, V2.2; Order No. 2.352
- Profile Guideline, Part 1: Identification & Maintenance Functions, V1.1; Order No. 3.502
- Profile Guideline, Part 2: Data Types, Programming Languages, and Platforms, V1.0; Order No. 3.512
- Profile Guideline, Part 3: Diagnosis, Alarms and Time Stamping, V1.0; Order No. 3.522
- Communication Function Blocks on PROFIBUS DP and PROFINET IO, V2.0; Order No. 2.182

5. Jak wdrażać PROFIsafe?

W pierwszej kolejności należy się upewnić czy otrzymaliśmy całą, niezbędną literturę udostępnianą przez PI (patrz ramka poniżej). Należy korzystać z dokumentów w wersji przedstawionej poniżej lub nowszej. Poprzednia V1.30 specyfikacji PROFIsafe jest dostępna tylko jako dokument informacyjny i nie powinna być wykorzystywana przy projektowaniu nowych urządzeń.

Następnym krokiem powinno być zapozananie się przynajmniej z podstawowym standardem IEC61508 lub skonsultowanie potrzeb związanych z rozwojem w zakresie PROFIsafe, w celu osiągnięcia niezbędnego

poziomu bezpieczeństwa wykonywanych urządzeń. Jako regułę przyjęto, że nie jest możliwe stworzenie urządzenia safety tylko poprzez zaimplementowanie protokołu PROFIsafe. Zastosowany system bezpieczeństwa z protokołem i sposobem w jaki są one zaimplementowane określają ostateczny poziom SIL urządzenia.

5.1 Klasy safety

Nawet jeśli protokół PROFIsafe spełnia wymagania poziomu SIL3 nie zawsze jest potrzeba aby urządzenie safety także spełniało tak wysokie kryteria bezpieczeństwa. Ostateczny poziom zabezpieczeń zależy od wymagań konkrtenej aplikacji. Poprzez zastowanie mechanizmów takich jak redundancja, możliwe jest osiągnięcie wysokiego poziomu zabezpieczeń SIL, wykorzystując urządzenia podrzędne F-Device o niższym poziomie bezpieczeństwa.

5.2 Urządzenia F-Device

Istnieją dwa sposoby implementacji drivera PROFIsafe. Możliwe jest samodzielne stworzenie drivera od podstaw, opierając się na specyfikacji lub skorzystać z gotowych driverów dostępnych na rynku. Więcej informacji znajduje się w zakładce „Product quide" na stronie organizacji PI. Korzystanie z gotowych rozwiązań niesie za sobą udogodnienia, z których najważniejsze to fakt, że drivery posiadają niezbędne certyfikaty a także dostęp do cennych informacji i narzędzi oraz wsparcie techniczne.

W przypadku wykorzystywania standardów PROFIBUS i PROFInet możliwe jest wykorzystanie wszystkich dostępnych specjalizowanych układów scalonych (ASIC) jak i driverów PROFIsafe.

5.2.1 Zabezpieczenia plików GSD

Do działanie każdego urządzenia w sieciach PROFIBUS i PROFInet niezbędny jest plik GSD (General Station Description file). Po zdefiniowaniu części ogólnej pliku GSD dla urządzenia F-Device, konieczne jest zakodowanie parametrów fail-safe (F-Parameters). Część zawierająca parametry fail-safe musi być chroniona poprzez wykorzystanie specjalnej sygnatury CRC "F_ParamDescCRC" zapobiegającej powstawaniu błędów. Za pomocą odpowiedniego narzędzia konfiguracyjnego można sprawdzić poprawność danych zawierających opis parametrów fail-safe, wykorzystując do tego wspomnianą sygnaturę, która jest częścią pliku GSD.

5.2.2 Zabezpieczanie danych I/O

Plik GSD zawiera także informacje o formatach danych F-I/O (wejściowych i/lub wyjściowych). W celu zabezpieczenia tej części pliku GSD wykorzystana jest sygnatura "F_IO_StructureDescCRC".

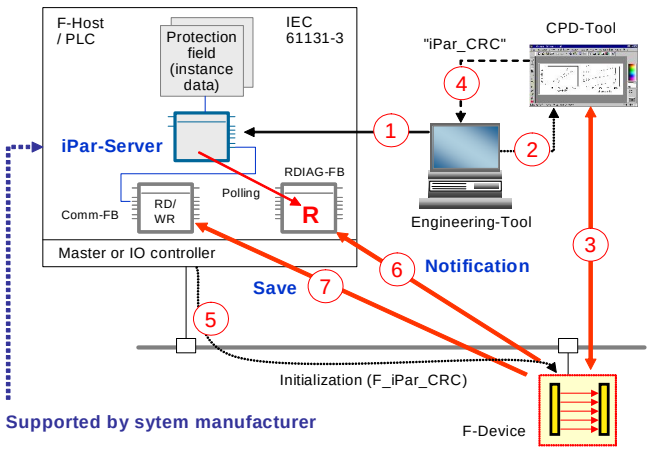
5.2.3 iParameter

Ze względu na dużą ilość urządzeń wykorzystywanych w aplikacjach związanych z bezpieczeństwem istnieje ogromna różnorodność parametrów (iParameter) dedykowanych dla poszczególnych urządzeń.

Ilość parametrów (iParameter) mieści się w zakresie od kilku bajtów w przypadku modułu safety (F-Module) do kilkudziesięciu kilobajtów dla skanera laserowego. Dla większości urządzeń safety istnieją specjalne programy narzędziowe służące do ich parametryzacji i diagnostyki (tzw. CPD-Tool). W przypadku takich urządzeń nie ma potrzeby zawierania danych potrzebnych do parametryzacji w pliku GSD.

W standardzie PROFIsafe zaleca się wykorzystanie nowego mechanizmu, określanego jako iPar-Server. Zaimplementowanie wspomnianego mechanizmu należy do producenta urządzenia nadrzędnego F-Host. Od poszczególnych producentów zależy także, czy jest on realizowany w części standardowej (nie safety) urządzenia F-Host, jako master nadający parametry, lub w obrębie sterowanego podsystemu w postaci standardowego sterownika PLC lub komputera pracującego w tej samej sieci.

Rysunek 11 za pomocą przykładu pokazuje zasady działania mechanizmu iPar-Server. Jednocześnie z konfiguracją sieci i nadaniem parametrów dla urządzenia podrzędnego inicjalizowana jest odpowiednia funkcja iPar-Server (1). Urządzenie F-Device może się przełączyć w tryb wymiany danych poprzez wykorzystanie stanu bezpiecznego (safe state)

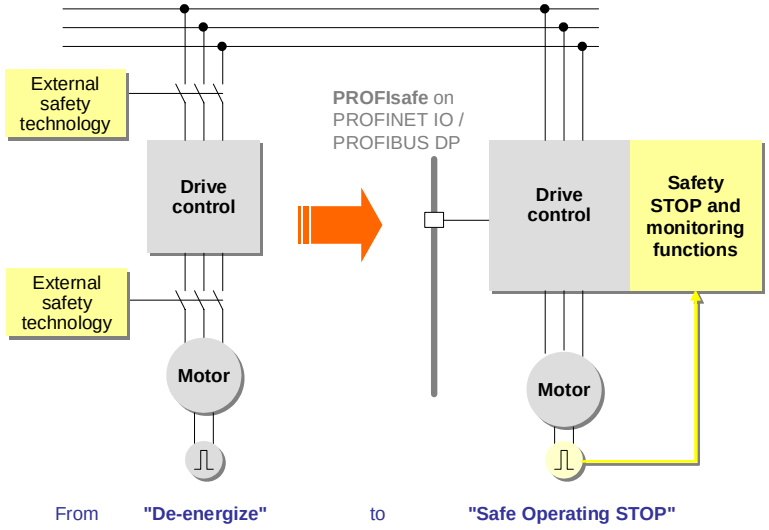


Rysunek 11 Koncepcja iPar-Server

(FV). Odpowiednie narzędzie CPD Tool może być wywołane poprzez wykorzystanie odpowiedniego interfejsu (2), takiego jak TCI (Tool Calling Interface) lub FDT (Field Device Tool) z narzedzia inżynierskiego, z którego pobierany jest adres konfigurowanego urządzenia. Narzędzie CPD Tool służy do parametryzacji, uruchomienia i testowania urządzenia (3). Po finalizacji obliczana jest sygnatura "iPar_CRC" i wyświetlana jako liczba heksadecymalna, po to żeby jej wartość mogła zostać skopiowana i wklejona w pole zmiennej "F_iPar_CRC" w części konfiguracyjnej narzędzia inżynierskiego (4). W celu przesłania parametru "F_iPar_CRC" do urządzenia podrzednego F-Device, niezbędny jest jego restart (5). Po ostatecznej weryfikacji urządzenie F-Device dostaje zezwolenie na przesłanie potwierdzenia do iPar-Server (6). Mechanizm ten pełni także podstawową funkcję diagnostyczną. iPar-Server wysyła informację diagnostyczną n.p. RDIAG FB w celu zinterpretowania żądania R i rozpoczęcia pobierania parametrów iParameter z urządzenia F-Device (7) za pomocą acyklicznej wymiany danych (Read Record).

Po wymianie uszkodzonego urządzenia F-Device, nowe urządzenie otrzymuje parametry fail-safe zawierające "F_iPar_CRC" przy uruchomieniu. W odróżnieniu od tradycyjnej parametryzacji urządzenia gdzie podczas wymiany lub braku podtrzymania pamięci, parametry są tracone, tutaj sprawdzana jest zgodność parametrów pomiędzy urządzniem a tymi zapisanymi w iPar-Server. Następnie inicjalizowany jest download parametrów (Write Record). Dzięki temu nowe urządzenie zachowuje pełną funkcjonalność poprzednika bez konieczności wykorzystania narzędzi inżynierskich lub CPD.

5.2.4 PROFIdrive



Rysunek 12 Napędy ze zintegrowanymi funkcjami safety, STOP i monitorującymi

Norma IEC 61800-5-2 określa pewne warunki bezpieczeństwa dla napędów posiadających zintegrowane funkcje safety. Obejmują one grupę funkcji zatrzymujących:

- Safe torque off (de-energize)
- Safe stop 1
- Safe stop 2
- Safe operating stop

Oraz grupę funkcji monitorujących:

- Safely limited acceleration
- Safely limited speed
- Safely limited torque / force
- Safely limited (absolute) position
- Safely limited increment
- Safe direction
- Safely limited motor temperature

Na Rysunku 12 pokazane jest w jaki sposób elektromechaniczne układy zatrzymujące są zastąpione poprzez elektroniczne wyłączniki safety i funkcje monitorujące. Głównym celem jest monitorowanie sterowania napędu i wyłączanie tylko na wypadek błędu. Grupa robocza PROFIdrive, należąca do PI określa wspomniane funkcje safety w ramach specjalnego dodatku do specyfikacji profilu PROFIdrive (patrz literatura powyżej).

5.2.5 Urządzenia PA

Urządzenia safety z zakresu automatyki procesowej są zgodne ze standardem IEC 61511, który bierze pod uwagę aspekty związane z użytkowaniem sprzętu "proven-in-use". Po spełnieniu szczególnych warunków urządzenie PA może osiągnąć wyższy stopień SIL jeśli jest odpowiednio przetestowane. Urządzenia PA zazwyczaj są zgodne z założeniami standardu IEC 61804. Integralną częścią standardu IEC 61804 jest specyfikacja EDD (Electronic Device Description). Grupa robocza "PA Devices" wchodząca w skład PI, określiła w dodatkowej specyfikacji jak implementować platformę PROFIsafe dla urządzeń PA (patrz literatura powyżej)

5.2.6 Funkcje I&M

Od 2005 roku tzw. funkcje I&M obowiązkowe są dla wszystkich urządzeń PROFIBUS i PROFInet realizujących usługi związane z komunikacją acykliczną. I&M oznacza "Identification and Maintenance" i pozwala w standaryzowany sposób pobierać informacje o

	PROFIsafe	Redundancy	PROFIsafe and Redundancy
Application	Factory and process automation: Presses, robots, level switches, shutdown valves, as well as burner control and cable cars	Process automation; Tranportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels	Process automation; Transportation infra-structure Chemical or pharma-ceutical productions, refineries, offshore; tunnels
High Availability	-	No downtimes at best (fault tolerance)	No downtimes at best (fault tolerance)
Safety	No dangerous failures (required by law or insurances)	Redundancy by itself does not provide safety	No dangerous failures (required by law or insurances)

kodzie producenta danego urządzenia, jego numerze seryjnym i katalogowym, wersji sprzętu i oprogramowania. Poprzez kod producenta i dodatkową informację na stronie internetowej PI, użytkownik może zostać przekierowany na stronę producenta zawierającą najaktualniejsze informacje o danym produkcie. Zobacz “Profile Guideline” (literatura powyżej).

5.2.7 Diagnostyka

Jedną z głównych zalet protokołów PROFIBUS i PROFINET, jest możliwość wysyłania przez urządzenia informacji diagnostycznych dla operatora w wyjątkowych sytuacjach takich jak usterka czy błąd. Dobra diagnostyka pozwala na skrócenie czasu postoju oraz redukcję kosztów. Oprócz kodowania informacji diagnostycznych, zadbano także o możliwość wyboru języka oraz dostarczenie funkcji HELP zawierającej wskazówki dotyczące poszczególnych sytuacji. Patrz dokument „Profile Guideline”.

5.3 Urządzenia F-Host

W zależności od producenta istnieją różne koncepcje urządzeń F-Host realizujących komunikację PROFIsafe: autonomiczne jednostki F-CPU lub zintegrowane w standardowym CPU, ale logicznie odseparowane funkcje safety.

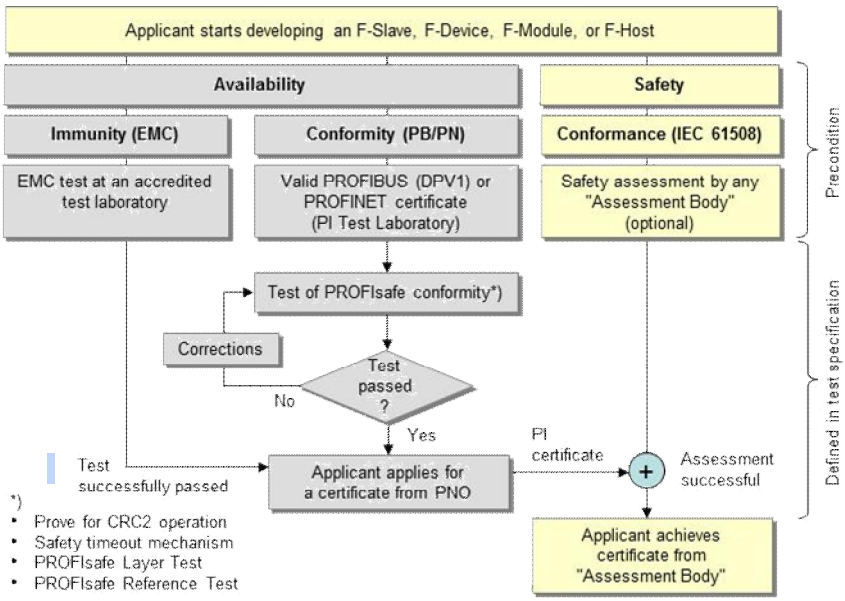
5.3.1 Możliwe struktury

Funkcje safety mogą być realizowane na wiele sposobów: poprzez redundancję sprzętową lub programową, wykorzystanie istniejących, różnych platform sprzętowych.

5.3.2 Klasy zgodności

W celu zapewnienia, że wszystkie dostępne na rynku urządzenia F-Device bedą obsługiwane przez wszystkie urządzenia F-Host wykorzystujące protokół PROFIsafe, określa on tzw. klasy zgodności dla urządzeń F-Host. Urządzenia F-Host obsługujące PROFIsafe powinny spełniać wymagania określone przez wspomniane klasy zgodności jako podstawę do certyfikacji PI. Rysunek 13.

Rysunek 13 Procedura testów i certyfikacji



6. Zgodność i certyfikacja

Zazwyczaj w obrębie jednej wyspy PROFIsafe kilka urządzeń różnych producentów komunikuje się między sobą. W celu zapewnienia poprawnej komunikacji, urządzenia muszą być zgodne ze specyfikacją PROFIsafe. Zazwyczaj wspomniana zgodność jest udokumentowana poprzez odpowiedni certyfikat wystawiony przez PI na podstawie raportu przygotowanego przez jedne z laboratoriów testowych PI.

6.1 Testy PROFIsafe

Mechanizmy protokołu PROFIsafe oparte są na skończonej liczbie stanów urządzenia. Dzięki temu przez odpowiednie obliczenia, możliwe było udowodnienie, że PROFIsafe może działać poprawnie w przypadku wystąpienia więcej niż dwóch niezależnych błędów lub usterek. Niezawodność ta została osiągnięta poprzez iwygenerowanie wszystkich możliwych przypadków “test-to-pass” i “test-to-fail”. Przypadki te zostały wykorzystane w urządzeniu automatyczenie testującym wartswę

PROFIsafe, które służy do sprawdzenia zgodności w urządzeniach F-Host i F-Device wykorzystujących PROFIsafe. Jest to część trzy etapowej procedury wchodzącej w skład czynności związanych z procesem certyfikacji urządzeń safety, zgodnie z IEC 61508. Rysunek 13.

6.2 Określanie stopnia niezawodności systemu Safety

Warto podkreślić, że laboratoria testowe PI przeprowadzają testy warstwy PROFIsafe w imieniu odpowiednich organów certyfikujących, takich jak:

- TÜV (worldwide)
- INRS (France)
- BGIA (Germany)
- SP (Sweden)
- SUVA (Switzerland)
- HSE (United Kingdom)
- FM, UL (USA)

Są to jedyne instytucje odpowiedzialne za określanie niezawodności systemów bezpieczeństwa według normy IEC 61508.

Dokumentacja każdego urządzenia F-Device obowiązkowo musi zawierać informację o parametrach SIL_{CL} (claim limit) i PFH_d (probability of dangerous failure per hour).

PROFIsafe dostarcza wytyczne dotyczące testów i certyfikacji. Obecnie dwa laboratoria testowe PI są akredytowane do testowania aplikacji wykorzystujących PROFIsafe.

7. Zastosowanie PROFIsafe

PROFIsafe nie byłby kompletny jeśli zawierałby tylko wytyczne dotyczącę protokołu komunikacyjnego safety. W przypadku urządzeń F-Device ważne są także inne aspekty związane z ich funkcjonowaniem:

- Ochrona urządzenia F-Device przed bardzo wysokimi napięciami powstającymi na kablach PROFIBUS / PROFINET pochodzącymi z nieznanego źródła
- Bezpieczeństwo przy wykorzystaniu wspólnego zasilanie 24V dla urządzeń F-Device oraz urządzeń standardowych pracujących w sieci?
- W jaki sposób testować moje urządzenie F-Device w zakresie „zwiększonej odporności", która wymagana jest w normie IEC 61508?
- Jakie reguły obowiązują przy instalacji?
- Jakie są wymogi bezpieczeństwa?

Dokument "PROFIsafe - Environmental Requirements" zawiera odpowiedzi na powyższe i inne pytania.

7.1 Bezpieczeństwo elektryczne

Standardy dotyczące sieci polowych IEC 61158 i IEC 61784-1, -2 wymagają aby wszystkie urządzenia w sieci były zgodne z prawnymi wymogami kraju, w którym są użytkowane. Wyznacznikiem wspomnianej zgodności może być na przykład znak CE. Przepisy związane z ochroną przeciwporażeniową w aplikacjach przemysłowych powinny opierać się na wytycznych zawartych w normach IEC 61010 lub IEC 61131-2, artykuł 10. Normy te dopuszczają tzw. układy PELV (Protected Extra Low Voltage), które ograniczają wartości napięć w przypadku jednej awarii, do zakresu nie stanowiącego zagrożenia dla człowieka.

7.2 Zasilanie

Jest możliwe wykorzystanie wspólnego zasilania 24V dla urządzeń standardowych jak również urządzeń F-Device/F-Host. W każdym przypadku obwód zasilania powinien być obwodem PELV.

7.3 Zwiększona odporność

Dla każdej aplikacji safety powinien zostać przygotowany dodatkowy dokument SRS (Safety Requirements Specification), który określa limity związane z odpornością na zakłócenia elektromagnetyczne (patrz IEC 61000-1-1), które są potrzebne do osiągnięcia kompatybilności elektromagnetycznej.
Wspomniane limity powinny być wyznaczone z uwzględnieniem zjawiska elektromagnetycznego (patrz IEC 61000-2-5) i wymaganego poziomu SIL.

Normy IEC 61326-3-1, IEC 61000-6-7 określają wymagania związane z odpornością dla urządzeń realizujących funkcje safety w aplikacjach przemysłowych.

Standardy produktowe takie jak IEC 61496-1 (n.p. skanery laserowe) mogą definiować zwiększone wymagania związane z odpornością na określone zjawiska.

Warunki otoczenia panujące w przemyśle procesowym mogą odbiegać od standardowych aplikacji. Dlatego w przypadku urządzeń PA można wykorzystać specjalne kryteria opisane w IEC 61326-3-2.

7.4 Wysoka niezawodność

Zadaniem systemów bezpieczeństwa (safety) jest maksymalna redukcja wypadków oraz zniszczeń spowodowanych przez błędy w maszynach oraz systemach sterowania. Głównym parametrem systemu safety jest tak zwany poziom nienaruszalności bezpieczeństwa SIL (Safety Integrity Level). Opisuje on prawdopodobieństwo wystąpienia błędu w funkcji safety w czasie godziny. Na przykład dla poziomu SIL3 jest to 10^{-7}/h.

Z kolei z punktu widzenia niezawodności systemu (fault tolerance) najważniejsza jest nieprzerwana praca funkcji sterujących nawet w sytuacji wystąpienia błędu. Parametrem pozwalającym określić

niezawodność systemu jest stosunek czasu pracy bez wystąpienia błędu do całkowitego czasu pracy (uptime to the total operation time), na przykład 99.99%. Redundancja jest jednym ze sposobów pozwalających na poprawienie niezawodności systemu.

PROFIsafe jest zaprojektowany w sposób pozwalający na jego działanie w układzie redundantnym (fault tolerant) lub bez redundancji. Na Rysunku 14 pokazane są możliwe kombinacje.

7.5 Wytyczne dotyczące instalacji

Założeniem twórców PROFIsafe było zintegrowanie komunikacji safety ze standardowymi sieciami PROFIBUS i PROFInet z możliwie minimalną ingerencją w istniejące wytyczne dotyczące instalacji sieci. W celu osiągnięcia dobrych rezultatów i spełanienia wszystkich wymaganych kryteriów zaleca się postępowanie zgodne ze specyfikacjami i wytycznymi PROFIsafe. Główne zagadnienia, które należy wziąść pod uwagę są przedstawione poniżej.

7.5.1 Warunki wstępne

Wszystkie urządzenia standardowe oraz safety (F-Devices) powinny spełniać warunki bezpieczeństwa elektrycznego, co było wspomniane w punkcie 7.1.

Wszystkie urządzenia F-Device powinny posiadać certyfikaty zgodne z IEC 61508, a w przypadku automatyki procesowej z IEC 61511. Urządzenia powinny być przetestowane pod kątem zgodności z PROFIsafe przez laboratoria testowe PI.

Wszystkie urzędzenia standardowe w sieci PROFIsafe muszą być zgodne ze standardem PROFIBUS lub PROFInet. Potwierdzeniem tego powinien być certyfikat PI lub inny równoważny dowód.

7.5.2 Założenia

W przyadku sieci PROFIBUS DP, odgałęzienia są niedozwolone.

Dla sieci PROFINET IO, obowiązują następujące założenia:

- Mniej niż 100 switchy w rzędzie
- Tylko jedno urządzenie F-Host na każdy moduł podrzędny
- Wszystkie komponenty sieci muszą być przystosowane do warunków przemysłowych (n.p. IEC 61131-2).
- Brak możliwości zastosowania routerów jednoportowych do separacji wysp PROFIsafe (oznaczonych przez niepowtarzalne F-Adresy)

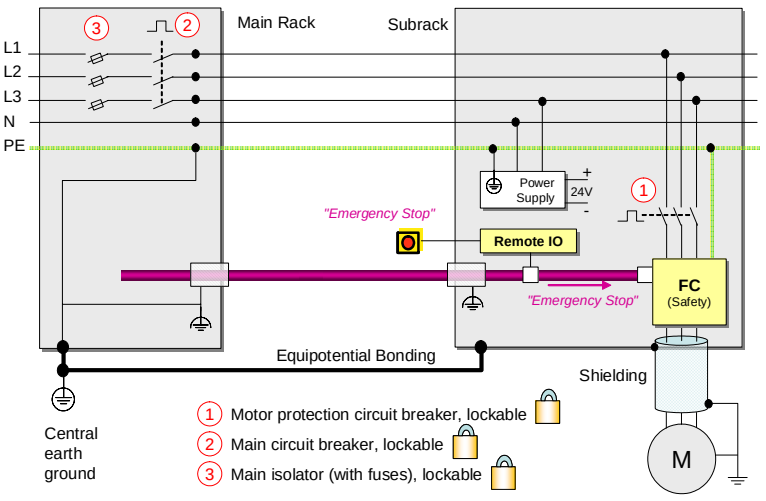
7.5.3 Okablowanie

Zarówno w przypadku sieci PROFIBUS jak i PROFINET zalecane jest stosowanie kabli ekranowanych z obustronnym połączenim ekranu do obudowy złącza, w celu uniknięcia wpływu zakłóceń elektromagnetycznych. W konsekwencji zazwyczaj wymagane jest wyrównanie potencjałów. Jeśli nie jest to możliwe można wykorzystać łącza światłowodowe.

7.5.4 Niezawodność

Nawet w przypadku stosowania kabli ekranowanych mogą wystąpić nieprzewidziane zakłócenia sygnału. Przyczyną takich zakłóceń może być na przykład niewsytarczające odfiltrowywanie zakłóceń na przyłączu DC przekształtnika częstotliwości. Innym źródłem niespodziewanego pogorszenia sygnału może być brak rezystorów terminujących itp. Nie jest to kwestia bezpieczeństwa (safety) systemu, ale jego niezawodności (availability). Jednak odpowiedni poziom niezawodności (availability) systemu jest warunkiem wstępnym do jedo bezpieczeństwa (safety). Funkcje safety pracujące na sprzęcie o niewystarczającej niezawodności mogą powodować nieuzasadnione przechodzenie urządzenia w stan bezpieczny.

Na rynku dostępnych jest wiele narzędzi i procedur dopuszczonych przez PI, służących do testowania jakości transmisji w sieciach.



Rysunek 15 Koncepcja wyłączania awaryjnego (IEC 60204-1)

Projektanci maszyn w przypadku określonej kompatybilności elektromagnetycznej, mogą na własne ryzyko wykorzystać przewody nieekranowane.

7.5.5 Safety - zalecenia

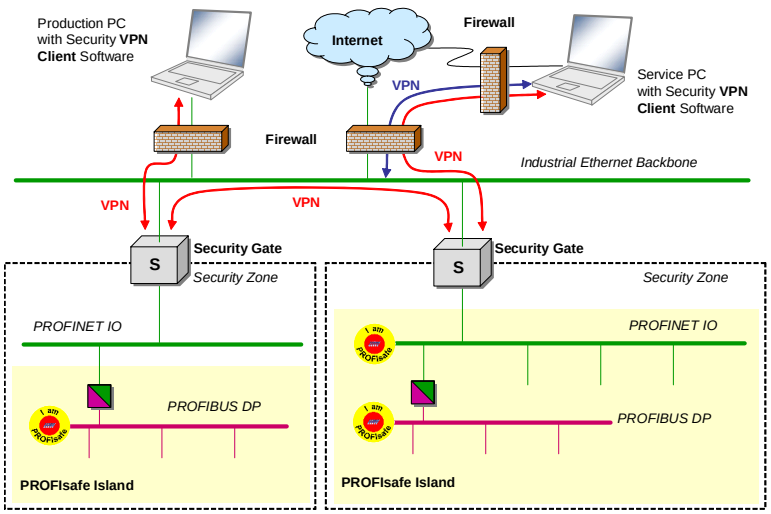
Opracowanie profilu PROFIsafe umożliwiło rozwój wielu urządzeń w zakresie bezpieczeństwa, w

szczególności napędów posiadających zintegrowane funkcje safety. Obecnie napędy mogą zapewnić przejście w stan bezpieczny bez odcinania zasilania silnika. Przykładem może być nowa funkcjonalność safety "SOS" (safe operating stop), która pozwala na utrzymanie silnika w ustalonej pozycji. Nowe możliwości wymagają zmiany podejścia użytkownika w pewnych kwestiach. Wcześniej naciśnięcie wyłącznika bezpieczeństwa powodowało fizyczne odcięcie zasilania silnika, przez co eliminowało się zagrożenie porażenia prądem.

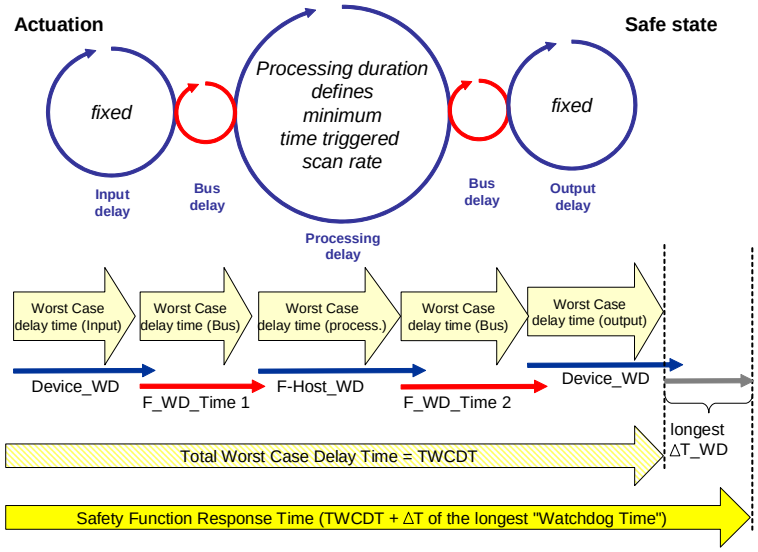
Norma IEC 60204-1 przedstawia koncepcję ochrony przeciwporażeniowej (wyłącznik awaryjny – wyłączony) wykorzystującą wyłączniki zabezpieczające silnik, wyłączniki główne oraz główne bezpieczniki i izolatory. Koncepcja ta została pokazana na Rysunku 15 Pokazuje on także zalecane 5 - żyłowe linie zasilające (TN-S) z rozdzielonymi przewodami N i PE oraz ekranowane przewody pomiędzy napędami i silnikami. Norma IEC 60204-1 jest cennym źródłem informacji dotyczących zagadnień bezpieczeństwa, które mogą stanowić dopełnienie technologi PROFIsafe. Standard NFPA 79 opisuje różnice obowiązujące na rynkach Ameryki Północnej, Rysunek3.

7.6 Transmisja bezprzewodowa

Coraz więcej aplikacji takich jak AGV (Automatem Guided Vehicles), maszyny obrotowe, roboty, panele dotykowe wykorzystuje transmisję bezprzewodową w sieciach PROFIBUS i PROFINET. PI opracowuje także specyfikacje dla standardów WLAN i Bluetooth. Mechanizm wykrywania błędów transmisji zastosowany w standardize PROFIsafe pozwala na jego implementację niezależnie od czarnego kanału (black channel) wykorzystywanego w transmisji. Jednak przy transmisji bezprzewodowej trzeba wziąć pod uwagę elementy przedstawione poniżej.



Rysunek 16 Bezpieczeństwo w sieciach "otwartych" i "zamkniętych"



Rysunek 17 Safety Function Response Time (SFRT)

7.7 Bezpieczeństwo

W przypadku sieci PROFINET, która jest oparta na otwartej sieci Industrial Ethernet oraz w kontekście transmisji bezprzewodowej zostały podniesione zagadnienia związane z bezpieczeństwem.

PI proponuje koncepcję tworzenia tzw. stref bezpieczeństwa (security zone), które można traktować jak sieci zamknięte, Rysunek 16. między strefami bepieczeństwa poprzez sieć otwartą n.p. Industrial Ethernet, jest wykorzystanie urządzeń określanych jako Security Gate (brama bezpieczeństwa). Urządzenia te wykorzystują powszechnie znane mechanizmy takie jak tunele VPN (Virtual Private Network) i Firewalle w celu zabezpieczenia przed włamaniem. Sieci PROFINET zawsze powinny działać w obrębie strefy bezpieczeństwa zabezpieczonej urządzeniem Securiy Gate, jeśli nie ma możliwości uniknięcia połączenia do otwartej sieci.

W przypadku transmisji bezprzewodowej standard IEE 802.11i określa wytyczne dotyczące bezpieczeństwa, wystarczające dla sieci PROFIsafe. Dopuszczalny jest tylko tryb Infrastructure Mode, tryb Adhoc Mode nie powinien być wykorzystywany. Więcej informacji na ten temat można znaleźć w specyfikacji PROFIsafe.

7.8 Czas odpowiedzi

Zazwyczaj czasy odpowiedzi standardowych funkcji sterujących są wystarczająco krótkie także dla funkcji safety. Jednakże pewne krytyczne czasowo aplikacje wymagają aby aspekt czasu odpowiedzi funckcji safety (SFRT – safety

function response times) został rozważony bardzo dokładnie. Prasy, które są chronione przez kurtyny świetlne są przykładem takich aplikacji. Projektant maszyny musi bardzo wcześnie znać odległość w jakiej ma zostać zamontowana kurtyna od niebezpiecznej prasy. Powszechnie zakłada się, że ludzka ręka porusza się maksymalnie z prędkością 2 m/s. Zgodnie z tym minimalny dystans s jaki trzeba wziąć pod uwagę wynosi s = 2 m/s x SFRT jeśli rozdzielczość kurtyny jest wystarczająca aby wykryć pojedynczy palec (EN 999). W innym wypadku trzeba uwzględnić parametry korygujące.

Jaka więc tajemnica kryje się za SFRT? Model na Rysunku 17 został wykorzystany do wyjaśnienia znaczenia tego parametru. Model zawiera wejściowe urządzenie F-Device, segment sieci z transmisją PROFIsafe, urządzenie F-Host przetwarzające sygnały, kolejny segment sieci z transmisją PROFIsafe oraz urządzenie wyjściowe F-Device. Maksymalny czas transmisji sygnału safety od urządzenia wejściowego do wyjściowego określany jest jako TWCDT (Total Worst Case Delay Time) biorąc pod uwagę, że wszystkie urządzenia biorące udział w transmisji wymagają określonego maksymalnego czasu cyklu. W przypadku aplikacji safety rozważania idą nieco dalej. Opóźnienie sygnału może być większe jeśli jeden z elementów biorących udział w transmisji ulega uszkodzeniu w pewnym punkcie czasu. W takiej sytuacji trzeba dodać Δt, które jest rónicą czasu potrzebnego do przesłania danych a wyznaczonym TWCDT (nie ma potrzeby brania pod uwagę więcej niż jednej usterki w danym punkcie czasu). Ostatecznie czas SFRT jest sumą czasu TWCDT oraz dodatkowego czasu opóźnienia Δt.

Zgodnie ze specyfikacją PROFIsafe, do każdego urządzenia F-Device powinna być załączona przez producenta informacja o jego czasie TWCDT aby na etapie projektu możliwe było oszacowanie czasu SFRT.

8. Dla integratorów

Jak dotąd dowiedzieliśmy się wiele o stosowaniu PROFIsafe. Czas aby powiedzieć kilka słów o aplikacjach i funkcjach zabezpieczających.

8.1 Dyrektywy i standardy

In many countries, the safety requirements for hazardous machineries are regulated by law. Within the EU this is the Machinery Directive 2006/42/ EC. This directive contains a list of so-called harmonized standards. For a machine builder, there is presumption of conformity to the directives if the relevant standards are fulfilled.

Relevant standards in the context of PROFIsafe are, for example, IEC 62061, ISO 13849, and ISO 12100 (see Chapter 1.3. and figure 2).

8.2 Strategia redukcji ryzyka

Dobrym rozwiązaniem jest projektowanie maszyn charakteryzujących się bezpieczeństwem wewnętrznym, co pozwala na wyeliminowanie zagrożeń. W pierwszej części normy ISO 12100 wymienione są wszystkie możliwe zagrożenia. W drugiej części przedstawiona jest strategia redukcji ryzyka związanego z użytkowaniem wszelkiego rodzaju zautomatyzowanych urządzeń poprzez oszacowanie ryzyka. Na oszacowanie ryzyka składa się analiza i wyznaczenie wartości ryzyka:

- Określenie ograniczeń oraz obszaru zastosowania maszyny
- Identyfikacja zagrożeń oraz niebezpiecznych sytuacji, które mogą powstać w całym cyklu życia maszyny
- Oszacowanie ryzyka dla każdego zidentyfikowanego zagrożenia i niebezpiecznej sytuacji
- Oszacowanie ryzyka i podjęcie decyzji o potrzebie jego redukcji

Wykorzystując metodę “3 – stopniową” (3-step method)

- projektowanie z uwzględnieniem wewnętrznych środków ochrony,
- zabezpieczenia oraz, jeśli to możliwe dodatkowe środki ochrony,
- informacja dla użytkownika o pozostałych zagrożeniach,

projektant maszyny może wyeliminować zagrożenia lub zredukować ryzyko związane z zagrożeniami poprzez wykorzystanie środków ochrony.

Zabezpieczenia i dodatkowe środki ochrony stanowią fundament dla funkcji zabezpieczających jak n.p. kurtyna świetlna, powiązane operacje logiczne oraz bezpiecznik wyłączający zasilanie silnika.

8.3 Zastosowanie IEC 62061

Normy IEC 62061 i ISO 13849 opisują metody postępowania z funkcjami zapezpieczającymi. Norma IEC 62061 jest skupiona na zagadnieniach związanych z technologią PROFIsafe i sterownikami programowalnymi z grupy failsafe (F-Host), natomiast norma ISO 13849 stanowi uzupełnienie jeśli chodzi o komponenty hydrauliczne, pneumatyczne, elektryczne i mechaniczne.

Norma IEC 62061 wymaga planu bezpieczeństwa obejmującego cały cykl życia maszyny, zawierającego project, role i zadania personelu, uruchomienie, wymiany, utrzymanie aż do demontażu.

ISO and IEC now are eager to harmonize and to improve the two

approaches of IEC 62061 and ISO 13849 via the project "ISO/IEC 17305" (figure 2).

8.4 Ocena ryzyka

Obydwa standardy proponują podobne koncepcje oceny ryzyka funkcji zabezpieczających, oparte na normie ISO 12100:

Ryzyko = stopień szkody/zranienia i prawdopodobieństwo wystąpienia tej szkody/zranienia

Prawdopodobieństwo wystąpienia szkody/zranienia składa się ze stopnia narażenia osób, częstotliwości zachodzenia zdarzeń niebezpiecznych i możliwości ich uniknięcia.

8.5 Wyznaczanie SIL

Obydwa standardy zawierają obliczone parametry. Jeden zawiera obliczenia dla parametru SIL drugi dla PL (Patrz 1.3). Możliwe jest przeliczenie jednego parametru na drugi. Jeśli czas pracy jest wystarczająco długi i ryzyko zostało oszacowane za pomocą odpowiednich narzędzi inżynierskich (n.p. kwestionariusz), można założyć, że różnica z punktu widzenia użytkownika będzie pomijalnie mała.

It is expected that the new ISO/IEC 17305 will be helpful in this respect.

8.6 Funkcje zabezpieczające

Norma IEC 62061 określa tzw. systemy sterowania safety (SRECS – safety-related control systems) z podsystemami pomiarowymi, przetwarzającymi i aktywacyjnymi. Podsystemy mogą zawierać elementy n.p. switche.

Najprostszą metodą na zaprojektowanie funkcji zabezpieczających jest wykorzystanie certyfikowanych urządzeń F-Device (czujniki, urządzenia załączające) i F-Host połączonych poprzez PROFIsafe.

8.7 Osiągnięty SIL

Dokumentacja każdego urządzenia F-Device zawiera informacje pozwalające na określenie poziomu SIL poszczególnych funkcji zabezpieczających. Najpierw wybierany jest najniższy SIL_{CL} (claim limit) spośród wszystkich urządzeń safety (F-Device, F-Host), który jednocześnie pozwala określić maksymalny SIL całej funkcji zabezpieczającej. W niektórych przypadkach producent może podnieść poziom SIL poprzez zastosowanie redundancji urządzeń F-Device i odpowiednich rozwiązań programowych.

W drugim etapie dodawane są wartości PFH_d i ponownie sprawdzany jest wynik pod kątem dopuszczalnego zakresu wartości dla poszczególnych poziomów SIL.

Najniższa wartość SIL z powyższych dwóch kroków jest przyjmowana jako osiągalny poziom SIL.

W poniższych sekcjach opisane są możliwości łączenia w obrębie oddalonych kart I/O, modułów safety (F-Module) z klasycznymi elektromechanicznymi urządzeniami zabezpieczającymi takimi jak wyłączniki bezpieczeństwa itd. Rysunek .

8.8 Elektromechanika

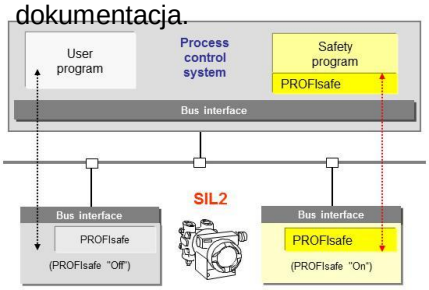
Norma IEC 62061 zawiera cztery ściśle określone architektury - A, B, C oraz D - podłączania klasycznych urządzeń zabezpieczających. Dla tych obwdów określone są także wzory pozwalające wyznaczyć prawdopodobieństwo awarii. Wykorzystując wartości B_{10} dla wyłączników, wyznaczoną liczbę cykli wyłącznika, informacje diagnostyczne oraz współczynnik CCF (common causa factor), można wyliczyć prawdopodobieństwo powstania niebezpiecznych awarii, co po dodaniu pozwala wyznaczyć ogólny poziom SIL.

8.9 Elementy nie - elektryczne

Norma ISO 13849-1 określa tzw. SRP/CS (Safety – Related Parts of Control Systems) także dla elementów hydraulicznych, pneumatycznych, elektrycznych i mechanicznych. Wartości współczynników PL oraz PFH_d mogą zostać wyznaczone dla takiego komponentu za pomocą wspomnianej normy a następnie przeliczone na poziom SIL dla funkcji bezpieczeństwa zgodnie z normą IEC 62061.

8.10 Walidacja

Norma IEC 62061 wymaga przeprowadzenia walidacji maszyny. Zgodnie z tym maszyna powinna zostać przetestowana oraz powinna zostać sporządzona dokumentacja.



9. Rodziny urządzeń F-Device

Wprowadzenie profilu PROFIsafe dało nowe możliwości dla urządzeń standardowych i safety. W tym rozdziale przedstawione są niektóre urządzenia F-Device i typowe aplikacje.

9.1 Oddalone I/O

Standardowe oddalone wyspy I/O dają możliwość dołączenia modułów o podwyższonym bezpieczeństwie (F-Modules),

bez konieczności zmiany stacji głównej. W tej kategorii dostępne są moduły (F-Modules) takie jak cyfrowe wejścia/wyjścia, analogowe wejścia/wyjścia, moduły zasilające, napędy silnikowe i przekształtniki częstotliwości ze zintegrowanymi funkcjami safety. Moduły mogą być pogrupowane i umożliwiać wyłączanie całej grupy modułów.

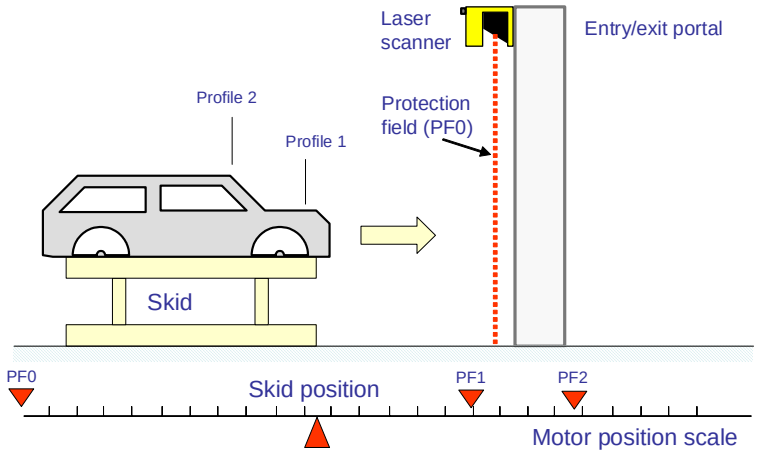
Wyłączniki bezpieczeństwa wymagają kosztownych, corocznych przeglądów, ponieważ każdy wyłącznik, bez wyjątku, musi być przetestowany. Nowa technologia pozwala na archiwizację wszystkich aktywacji wyłączników w ciągu roku. Dzięki temu sprawdzanie ogranicza się do pozostałych wyłączników, które nie były aktywowane, co z kolei niesie za sobą znaczne oszczędności.

9.2 Czujniki optyczne

Optyczne czujniki zabezpieczające takie jak kurtyny świetlne, skanery laserowe są ustandaryzowane w normie IEC 61496. Czujniki optyczne bardzo dobrze sprawdzają się przy ochronie portali wejściowych/wyjściowych, gdzie potrzebna jest pewna elastyczność ustawień. Przykład na Rysunku 18 pokazuje w jaki sposób PROFIsafe uzupełania możliwości skanerów laserowych i napędów, posiadających zintegrowane funkcje safety.

9.3 Napędy

Właściwości napędów związane z bezpieczeństwem zostały ustandaryzowane w normie IEC 61800-5-2. Funkcje bezpieczeństwa zazwyczaj wymagają wskaźnika położenia bezpiecznego. Wartość ta poprzez PROFIsafe jest dostępna dla użytkownika i może zastąpić fizyczne krańcówki lub czujniki sterfowe. Jak pokazuje Rysunek 18 pozycja silnika wpływa na sterfy



Rysunek 18 Programowe "czujniki" dla skanerów laserowych

ochrony skanera laserowego w zależności od bryły samochodu na portalu wejściowym/wyjściowym jednostki produkcyjnej.

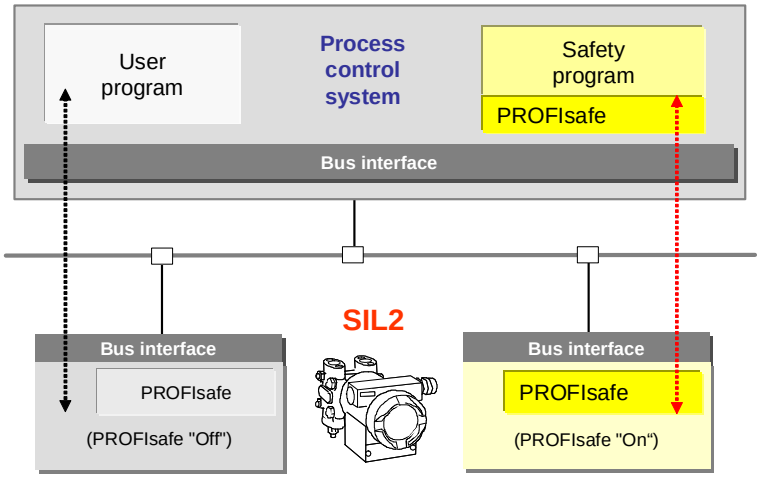
W rozdziale 5.2.4 wymienione są pewne właściwości urządzeń safety, które spowodują powstanie rewolucyjnych aplikacji w najbliższym czasie.

9.4 Roboty

Norma ISO 10218 określa wytyczne dotyczące układów bezpieczeństwa dla robotów. Nowe możliwości adaptacji układów bezpieczeństwa w napędach pozwalają także na przenieniesienie tych rozwiązań na roboty. Dzięki temu pojawiają się nowe możliwości w rozwoju takich technologii jak roboty kolaboracyjne, gdzie człowiek pracuje „ręka w ręke" z robotem.

9.5 F-Gateway

Dostępne są urządzenia F-Gateway spełniające wymogi aplikacji o podwyższonym bezpieczeństwie służące do konwersji pomiędzy siecią wykorzystującą PROFIsafe a siecią ASIsafe (AS-i Safety-at-work). Urządzenia te łączą w



Rysunek 19 PROFIsafe i NE97 dla urządzeń PA

sobie zalety tych dwóch środowisk komunikacyjnych. Podczas gdy w sieci ASIsafe można z łatwością zbierać sygnały z wielu wyłączników bezpieczeństwa połączonych w szereg, PROFIsafe z łatwością obsłuży znacznie bardziej skomplikowane urządzenia F-Device jak napędy ze zintegrowanymi funkcjami safety.

9.6 Urządzenia PA

Jak zostało wspomniane wcześniej zagadnienia związane

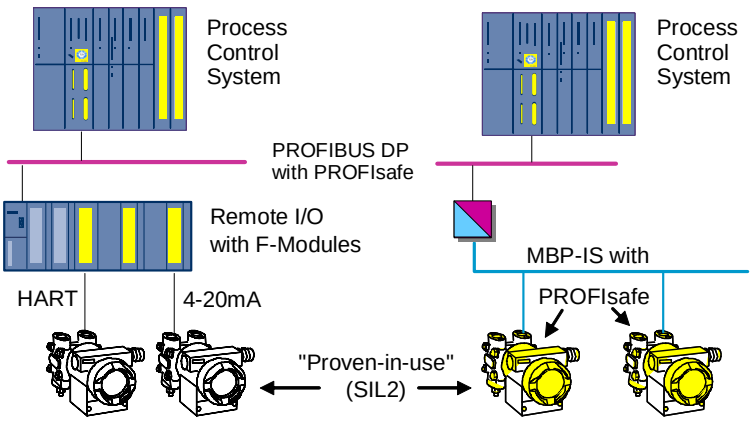
z bezpieczeństwem w automatyce procesowej zdefiniowane są w normie sektorowej IEC 61511. NAMUR jako organ normalizacyjny dla przemysłu chemicznego i farmaceutycznego publikuje branżowy standard NE97, który określa sposoby użytkowania komunikacji safety z urządzeniami polowymi safety. Urządzenia PA „proven-in-use”, obsługujące protokół PROFIBUS wykorzystujący MBP-IS jako warstwę fizyczną, posiadają driver obsługujący profil PROFIsafe, który może być “włączony” lub “wyłączony”. W jednym trybie urządznie pracuje jak standardowe urządzenie PA, natomiast w drugiej jak urządzenie o podwyższonym stopniu bezpieczeństwa F-Device, Rysunek 19.

NAMUR wprowadził inną pokrewną normę VDI 2180, która ułatwia rozwój urządzeń PA o podwyższonym stopniu bezpieczeństwa.

Obecnie większość aplikacji w automatyce procesowej wykorzystuje oddalone I/O z Modułami safety dla podłączenia urządzeń wykorzystujących standardy 4-20mA lub HART. Rysunek 20 pokazuje dwie możliwości wykorzystania profilu PROFIsafe do komunikacji z urządzeniami PA. Rozwiązanie to można uznać jako kompromis mimo tego, że nie pozwala na pełne wykorzystanie możliwości sieci polowej, takich jak szeroko-zakresowe pomiary, parametryzacja, zaawansowana diagnostyka.

9.6.1 Sygnalizatory poziomu

Zastosowanie PROFIsafe z sygnalizatorami poziomu wykorzystywanymi w zbiornikach daje wiele korzyści. PROFIBUS PA z iskrobezpiecznymi technologiami transmisji MBP-IS oraz RS485-IS bardzo dobrze spełnia wymagania tych urządzeń F-Device. PROFIsafe zapewnia bezpieczną transmisję sygnałów zamykających, podczas gdy warstwa „black channel” informuje użytkownika o statusie sygnalizatora.



Rysunek 20 Możliwości podłączania urządzeń PROFIsafe i PA

9.6.2 Zawory ESD

Podobne ulepszenia można uzyskać w przypadku zaworów ESD (Electronic Shut-Down). Głównym zadaniem w tym przypadku jest okresowe testowanie zaworu poprzez „częściowe uderzenia zaworu” oraz monitorowanie pozycji końcowej i czasu potrzebnego do jej osiągnięcia. Procedura ta może być przeprowadzana automatycznie przez urządzenie nadrzędne F-Host na żądanie użytkownika. Komunikacja RS485-IS wykorzystująca bariery pozwala na szybkie zamknięcie nawet w strefie Ex-i.

9.6.3 Przetwornik ciśnienia

Przetworniki ciśnienia posiadające zintegrowane funkcje bezpieczeństwa, łączą w sobie funkcje pomiaru poziomu w zbiorniku oraz funkcje zabezpieczające przed przepełnieniem zbiornika poprzez porównanie z wartością zadaną poziomu.

9.6.4 Czujniki gazu i ognia

Tego rodzaju czujniki wykorzystywane są n.p. na bezzałogowych platformach wiertniczych. Dodatkowa informacja o pozycji czujnika daje możliwość zamknięcia odpowiednich śluz.

10. Korzyści dla użytkownika

Obecnie zainstalowanych jest około 50 milionów urządzeń PROFIBUS i ponad 10 milionów urządzeń PROFINET. Dlatego głównym priorytetem przy rozwoju nowych technologi było i nadal jest zapewnienie pełnej kompatybilnośći z urządzeniami już działającymi w instalacjach.

Dzięki możliwościom jakie daje wykorzystanie protokołu PROFIsafe i koncepcji „Black channel", możliwe jest bezproblemowe przejście pomiędzy standardami PROFIBUS i PROFINET. Identyczne drivery PROFIsafe wykorzystuje się zarówno w urządzeniach PROFIBUS jak i PROFINET.

Wprowadzenie standardu PROFIsafe było trzy etapowym krokiem milowym:

- Od układów bezpieczeństwa opartych na przekaźnikach do programowalnych układów bezpieczeństwa
- Od połączeń wieloprzewodowych do komunikacji szeregowej spełniającej wymogi funkcji bezpieczeństwa
- Od autonomicznych do mogących pracować w grupach urządzeń ze zintegrowanymi funkcjami bezpieczeństwa

W poniższych rozdziałach znajduje się podsumowanie korzyści wynikające z zastosowania standardu PROFIsafe, przedstawione z różnych punktów widzenia.

10.1 Integratorzy i użytkownicy końcowi

- Takie same oszczędności jak w przypadku zastosowania sieci PROFIBUS: redukcja okablowania, elastyczna konfiguracja, parametryzacja oraz diagnostyka
- Prosta i ekonomiczna architektura systemu z możliwością wykorzystania urządzeń dostarczanych przez wielu producentów
- Ogólnie brak specjalnych restrykcji dotyczących instalacji
- Innowacyjne aplikacje safety dzięki możliwości komunikacji pomiędzy zaawansowanymi urządzniami F-Device
- Duża elastyczność w zamianie istniejącej technologii przekaźnikowej, jak również przy rozszeżaniu i modernizacji istniejących instalacji.
- Zintegrowana technologia dla automatyki maszyn i automatyki procesowej
- Szkolenie, dokumentacja i utrzymanie tylko jednej sieci
- Programowanie aplikacji standardowych i safety za pomocą jednego narzędzia i certyfikowanych bloków funkcyjnych
- Prosta dokumentowanie konfiguracji safety
- Ograniczone koszty związane z certyfikacją systemu dzięki wykorzystaniu certyfikowanych urządzeń
- Międzynarodowa akceptacja dzięki zgodności z IEC 61508
- Zatwierdzenie przez BGIA i TÜV

10.2 Producenci urządzeń

- Oprogramowanie zatwierdzone przez TÜV pozwala na proste zastosowanie i ekonomiczne powielanie rozwiązań PROFIsafe
- Komunikacja PROFIsafe może zostać zaadoptowana do sterowników ze zintegrowanymi funkcjami bezpieczeństwa o różnych architekturach
- POFIsafe daje możliwości implementacji nowych innowacyjnych rozwiązań w urządzeniach

10.3 Inwestycje

- Ogromna istniejąca baza zainstalowanych urządzeń obsługujących standardy PROFIBUS i PROFINET
- Organizacje PROFIBUS/PROFINET obecne na całym świecie
- Możliwość wykorzystania wszystkich istniejących i mających powstać w przyszłości standardów określanych przez PI do aplikacji o podwyższonym bezpieczeństwie
- PROFIsafe jest standardem miedzynarodowym określonym w normie IEC 61784-3-3
- Future software to assist the life-cycle of safety applications from design through assessment, validation, and documentation, thus further reducing efforts

11. PI

Aby zapewnić i zachować dominację systemu na rynku, rozwój technologii i niezależność od producentów utworzono w 1989r. organizację użytkowników sieci PROFIBUS – PROFIBUS User Organization (PNO) e.V w Niemczech. Jest to organizacja nonprofit reprezentująca producentów, użytkowników I uczelnie. PNO jest członkiem międzynarodowej PROFIBUS International (PI) założonej w roku 1995, reprezentującej obecnie 25 regionalnych ośrodków (Regional PROFIBUS Associations, RPA) oraz ponad 1,400 członków, którzy reprezentują jeden z największych rynków sieci polowych. Biura regionalne (RPA) organizują wystawy i seminaria dotyczące nowych technologii i kierunków rozwoju na rynku.

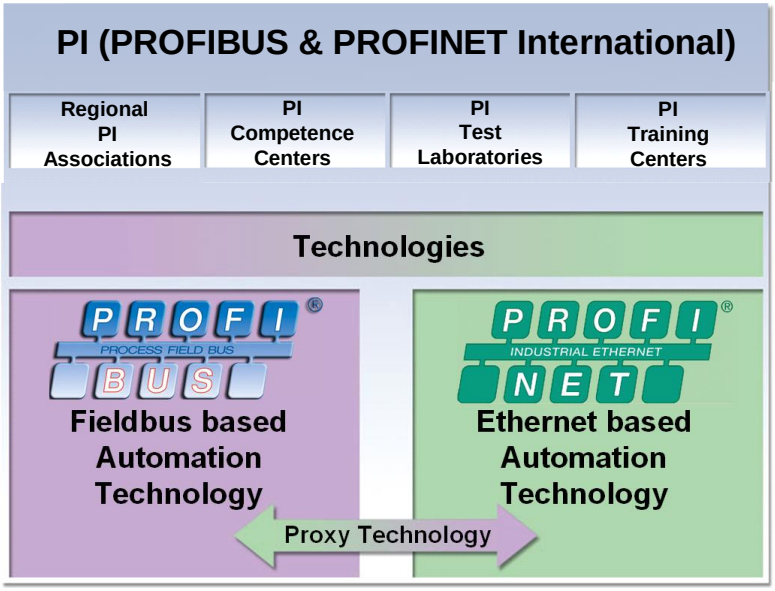
11.1 Zakres działań PI

Główne zadania PI stanowią:

- Obsługa i rozwój technologii PROFIBUS i PROFINET
- Wdrażanie i promocja sieci polowych opartych na baize standardów PROFIBUS i PROFINET
- Ochrona inwestycji dla użytkowników i producentów urządzeń przez standaryzację
- Reprezentacja interesów członków w komisjach i grupach standaryzujących
- Światowapomoc techniczna dla firm poprzez Centra Kompetencji (PICC)
- Zapewnienie stałej jakości I pewności działania poprzez certyfikację urządzeń
- Ogólnoświatowy standard szkoleń poprzez Centra Szkoleniowe (PITC)

11.2 Rozwój technologicznyg

PI przekazała rozwój PROFIBUS i PROFINET do PNO Niemcy, który określa rozwój I kierunki działań. Grupy rozwojowe dzielą się na



Rysunek 21 PROFIBUS & PROFINET International (PI)

Komitety Techniczne (Technical Committees – TC) z ponad 50 Grupami roboczymi (Working Groups – WG). Grupy robocze z ponad 500 ekspertami określaja nowe specyfikacje i profile, dbają o jakość i standaryzację, pracują w komisjach standaryzacyjnych i promują sieci PROFIBUS i PROFINET. Centra techniczne PI wyjaśniają wszystkie zgłaszane problemy techniczne.

11.3 Wsparcie techniczne

PI posiada ponad 50 akredytowanych Centrów kompetencyjnych na całym świecie. Dzięki temu użytkownicy mają dostęp do wszelkiego rodzaju informacji i wsparcia technicznego. Jako integralna część PI Centra kompetencyjne świadczą niezależne usługi serwisowe i stosują się do obustronnie uzgodnionych regulacji. Centra PICC są regularnie kontrolowane w ramach indywidualnie dopasowywanego procesu akredytacji. Adresy Centrów kompetencyjnych znajdują się na stronach PI.

11.4 Certyfikacja

PI posiada 10 akredytowanych Laboratoriów testowych PITL, które wspierają process certyfikacji produktów posiadających interfejs PROFIBUS/PROFINET. Główną częścią tego procesu są testy certyfikacyjne przeprowadzane we wspomnianych laboratoriach. Pomyślne przejście procedury testowej gwarantuje, że produkt spełnia wymagania standardu i jest wolny od jakichkolwiek błędów. Adresy Laboratoriów testowych dostępne są na stronach PI.

11.5 Szkolenia

Głównym założeniem przy tworzeniu Centrów szkoleniowych PI (PITC) było ustalenie jednego spójnego standardu szkoleń dla inżynierów i instalatorów. Centra szkoleniowe i związani z nimi eksperci muszą posiadać oficjalną akredytację. Pozwala to zapewnić jakość nie tylko dla szkoleń z zakresu PROFIBUS/PROFINET, ale także dla usług inżynierskich i instalacyjnych. Adresy Centrów szkoleniowych znajdują się na stronach PI.

11.6 Platforma informacyja – Internet

Na stronie internetowej www.profibus.com znajdują się aktualne informacje o organizacji PI oraz o technologiach PROFIBUS i PROFINET. Na powyższej stronie można znaleźć informacje produktowe, słownik,

interaktywne szkolenia. Strony PI zawierają także dużą bazę dokumentacji udostępnionych do pobrania.

Opracowanie i tłumaczenie

PROFIBUS PNO Polska
Tel.: +48 (0) 32 / 208 41 36
poland@profibus.com

www.profibus.org.pl

PROFIsafe – Safety Technology for PROFIBUS and PROFINET

System Description

Version 20 July 2007

Order Number 4.342

Publisher

PROFIBUS Nutzerorganisation e.V. PNO
Haid und Neu-Str. 7
76313 Karlsruhe
Deutschland
Tel.: +49 (0)721 / 96 58 590
Fax: +49 (0)721 / 96 58 589
germany@profibus.com

PROFIBUS Trade Organisation PTO
16101 N 82nd Street, Suite 38
AZ 85260 Scottsdale
USA
Tel.: +1 480 483 2456
Fax: +1 480 483 7202
usa@profibus.com

Liability Exclusion