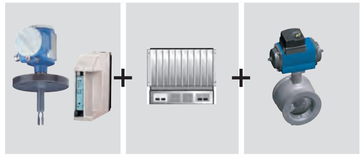
Korzyści z normalizacji wg PN-EN 61508 oraz PN-EN 61511

- Międzynarodowe ujednolicenie metod oceny oprzyrządowania związanego z bezpieczeństwem
- Ocena systemów sterowania używanych do zwiększania bezpieczeństwa w zakresie usterek systematycznych oraz statystycznie potwierdzonych uszkodzeń losowych
- Umożliwienie zarządzania „cyklem życia bezpieczeństwa", w tym m.in. przejrzyste dokumentowanie każdego kroku podczas projektowania obwodów realizujących funkcję bezpieczeństwa
- Pełna ocena pętli zabezpieczeniowej według jednolitych reguł (czujnik/przetwornik, układ logiczny, urządzenie wykonawcze)
- Wymagane bezpieczeństwo można uzyskać przez zastosowanie przebadanego oprzyrządowania z atestem SIL bez ponoszenia wysokich kosztów związanych z daleko idącymi zmianami w technologii procesu

Tor realizacji funkcji bezpieczeństwa w pętli zabezpieczeniowej

Czujnik/przetwornik	Układ logiczny	Urządzenie wykonawcze



People for Process Automation

Endress+Hauser jest wiodącym dostawcą przyrządów pomiarowych i rozwiązań automatyki procesów dla wszystkich gałęzi inżynierii przemysłowej.
Wspieramy logistykę przedsiębiorstw, dostarczając systemy telemetryczne do gromadzenia oraz przetwarzania danych o procesach i stanach magazynowych. Nasza oferta to połączenie najwyższej jakości produktów, atrakcyjnych cen i kompleksowego wsparcia serwisowego.

Gwarancja niezawodności i efektywności naszych rozwiązań daje przewagę konkurencyjną naszych Klientów. Globalna sieć zakładów produkcyjnych oraz przedstawicielstw lokalnych utwierdza pozycję Endress+Hauser jako lidera rynkowego. Oddziały regionalne w całej Polsce służą Państwu pomocą i wsparciem w doborze i eksploatacji systemów kontrolno-pomiarowych Endress+Hauser.

Fundamentem marki Endress+Hauser od ponad 55 lat jej istnienia jest doświadczenie i wiedza o procesach technologicznych we wszystkich branżach przemysłu oraz kreatywność i zaangażowanie naszych pracowników.

Polska

Endress+Hauser Polska spółka z o.o.
ul. Wołowska 11
51-116 Wrocław
tel. 71 773 00 00
fax 71 773 00 60
info@pl.endress.com
http://www.pl.endress.com

Endress+Hauser
People for Process Automation

Poziom · Ciśnienie · Przepływ · Temperatura · Analiza Cieczy · Rejestracja · Komponenty Systemów · Usługi · Rozwiązania

PN-EN 61508/PN-EN 61511

Bezpieczeństwo funkcjonalne w inżynierii procesowej – ograniczanie ryzyka awarii przy użyciu przyrządowych systemów bezpieczeństwa

Endress+Hauser
People for Process Automation

Poziom nienaruszalności bezpieczeństwa

Przyrządowe systemy bezpieczeństwa

Urządzenia stosowane w inżynierii przemysłowej, sklasyfikowane i poddane ocenie odnośnie niezawodności, są ważnymi elementami podnoszenia bezpieczeństwa ludzi, ochrony majątku przed zniszczeniem i środowiska naturalnego przed zanieczyszczeniem lub skażeniem.

W większości krajów uprzemysłowionych wymagania odnośnie bezpieczeństwa ludzi, środków trwałych na instalacjach technologicznych i środowiska naturalnego podążają za najnowszą techniką, która pozwala wytwarzać i dostarczać urządzenia pomiarowe i wykonawcze oraz układy sterowania o bardzo wysokiej niezawodności. Dlatego wymagania te opisano w formie obowiązującej normy, jako podstawę przyjmując powszechnie akceptowane zalecenia IEC 61508* (Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/elektronicznych programowalnych systemów związanych z bezpieczeństwem).

* w Polsce znane jako PN-EN 61508

Czym jest SIL?
Przyrządowe systemy bezpieczeństwa (SIS, Safety Instrumented Systems) są projektowane i używane, aby zapobiegać lub łagodzić skutki niebezpiecznych zdarzeń. W szczególności zostały pomyślane, aby chronić zdrowie i życie ludzi, czystość środowiska naturalnego a także minimalizować straty materialne na instalacji przemysłowej, które pojawiają się wskutek awarii. Poziom nienaruszalności bezpieczeństwa (SIL, Safety Integrity Level) definiuje ilościowo ograniczenie ryzyka takiej awarii do wartości akceptowalnej. Zalecenia IEC 61508 określają poziomy ryzyka (tzw. graf ryzyka) oraz dają wytyczne do projektowania funkcji bezpieczeństwa, jakie powinien realizować przyrządowy system bezpieczeństwa złożony z urządzenia pomiarowego, układu logicznego i urządzenia wykonawczego. W zaleceniach IEC 61508 znaleźć można m.in. metodologię "unikania usterek" (uszkodzenia systematyczne) i "kontroli usterek" (uszkodzenia systematyczne i losowe). Wymagania dla elementów przyrządowego systemu bezpieczeństwa (np. pętli zabezpieczeniowej), którego zadaniem jest realizowanie funkcji bezpieczeństwa, są dzięki wspomnianym zaleceniom dokładnie opisane.

Zalecenia IEC 61508 umożliwiły sformułowanie tzw. norm sektorowych, w tym IEC 61511* („Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa dla sektora inżynierii przemysłowej"). I tak, zalecenia IEC 61511 określają m.in. kryteria klasyfikacji elementów przyrządowego systemu bezpieczeństwa, jak np. „sprawdzony w użyciu".

Kiedy korzysta się z wytycznych zawartych w IEC 61508?
Wytyczne z IEC 61508 odnoszą się do wszelkich przypadków, w których używa się systemów elektrycznych, elektronicznych lub programowalnych elektronicznych, realizujących funkcję bezpieczeństwa (np. funkcja odcięcia dopływu pary przegrzanej po przekroczeniu granicznej wartości ciśnienia w rurociągu w celu jego zabezpieczenia przed rozszczelnieniem i wybuchem). IEC 61508 odnosi się do wszystkich aplikacji inżynierskich, w których usterki pracującego systemu (np. obiegu wodno-parowego wytwarzającego parę przegrzaną) mają decydujący wpływ na bezpieczeństwo ludzi pracujących na instalacji, czystość środowiska naturalnego i sprawność infrastruktury obiektu przemysłowego.

* w Polsce znane jako PN-EN 61511

PN-EN 61508 / PN-EN 61511

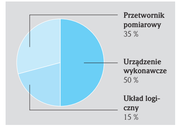
Ocena bezpieczeństwa i wymagania odnośnie bezpieczeństwa

Różnica między PN-EN 61508 i wcześniejszymi wytycznymi
Po raz pierwszy norma wymaga dowodu ilościowego wystąpienia uszkodzeń niebezpiecznych, opartego na obliczeniach statystycznych. Celem jest opisanie liczbowo ryzyka awarii, które pozostało po wyeliminowaniu wszystkich potencjalnych źródeł jej wystąpienia. Obliczenia są realizowane dla całej pętli zabezpieczeniowej, składającej się z urządzenia pomiarowego, układu logicznego (np. sterownika PLC) i urządzenia wykonawczego (np. zaworu). Prawdopodobieństwa uszkodzenia niebezpiecznego każdego z tych elementów są sumowane (PFD) i analizowane dla całego obwodu zabezpieczeniowego. Obwód taki najczęściej przyjmuje postać 1oo1 (wybór jednego kanału spośród jednego dostępnego, czyli tzw. głosowanie „jeden z jednego") lub 2oo3 (wybór dwóch kanałów z trzech dostępnych, czyli tzw. głosowanie „dwa z trzech"). Prawidłowe stosowanie normy PN-EN 61508 polega na jej kwvrzględnianiu w całym cyklu życia elementu pętli zabezpieczeniowej, a więc podczas jego projektowania, rozwoju, wytwarzania oraz eksploatacji.

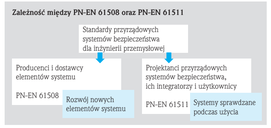
SIL	PFD_{avg}
4[1]	$\geq 10^{-5}$ ... $< 10^{-4}$
3	$\geq 10^{-4}$ ... $< 10^{-3}$
2	$\geq 10^{-3}$ ... $< 10^{-2}$
1	$\geq 10^{-2}$ ... $< 10^{-1}$

Zależność poziomów nienaruszalności bezpieczeństwa SIL od średniego prawdopodobieństwa niezadziałania funkcji bezpieczeństwa pętli zabezpieczeniowej, która pracuje w trybie na żądanie przywołanie.

Parametr PFD_{avg} określa odpowiedzialność każdego elementu pętli zabezpieczeniowej za prawidłowe zadziałanie jej funkcji bezpieczeństwa (np. blokady dalszego wzrostu ciśnienia w zbiorniku z gazem skroplonym LPG).

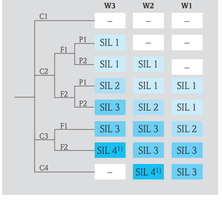


Zależność między PN-EN 61508 oraz PN-EN 61511



W celu obniżania ryzyka, obie normy PN-EN 61508 i PN-EN 61511 definiują następujące kroki postępowania:
- Definicja i oszacowanie ryzyka zgodnie z obliczonymi prawdopodobieństwami wystąpienia uszkodzenia niebezpiecznego urządzenia pomiarowego, układu logicznego i urządzenia wykonawczego w ciągu całego okresu ich eksploatacji
- Wskazanie i zastosowanie metod ograniczenia ryzyka
- Zastosowanie właściwych elementów w przyrządowym systemie bezpieczeństwa (sklasyfikowanych statystycznie lub przebadanych w trakcie rozwoju)
- Okresowe testy prawidłowego działania funkcji bezpieczeństwa

Graf ryzyka według PN-EN 61508/61511



Konsekwencje awarii
C1 niewielkie obrażenia ludzi
C2 poważne obrażenia jednej lub kilku osób; możliwy zgon jednej osoby
C3 zgony kilku osób
C4 duża liczba ofiar śmiertelnych

Narażenie na skutki awarii
F1 rzadkie lub okresowe
F2 częste lub ciągłe

Ograniczanie ryzyka awarii
P1 możliwe pod określonymi warunkami
P2 prawie niemożliwe

Prawdopodobieństwo zajścia zdarzenia
W1 bardzo małe
W2 niewielkie
W3 względnie duże

[1] SIL 4 nie może być osiągnięty przy wyłącznym stosowaniu elementów przyrządowego systemu bezpieczeństwa

SFF, HFT, SIL

Zależności między parametrami związanymi z bezpieczeństwem

Udział uszkodzeń bezpiecznych (SFF, Safe Failure Fraction)
Odsetek uszkodzeń, które nie wprowadzają oprzyrządowania związanego z bezpieczeństwem w stan braku zdolności do realizowania funkcji bezpieczeństwa.

Tolerancja defektów sprzętu (HFT, Hardware Fault Tolerance)
Zdolność oprzyrządowania do realizowania funkcji bezpieczeństwa w obecności błędów lub usterek. Parametr HFT równy N oznacza, że N+1 usterek może spowodować utratę zdolności oprzyrządowania do realizowania funkcji bezpieczeństwa. Poza utrzymywanymi na maksymalnym poziomie prawdopodobieństwami uszkodzeń niebezpiecznych (PFD), **poziom nienaruszalności bezpieczeństwa (SIL, Safety Integrity Level)** nadany funkcji bezpieczeństwa realizowanej przez oprzyrządowanie przeznaczone do tego celu, zgodnie z PN-EN 61508 zależy od kombinacji parametrów SFF oraz HFT.

Różnica między urządzeniami "prostymi" i "złożonymi"
Zachowanie się urządzenia „prostego" (typu A), gdy pojawi się jego usterka, jest w pełni przewidywalne.
Rodzaje uszkodzeń wszystkich jego elementów są dobrze opisane. Są nimi m.in. rezystory, tranzystory, przekaźniki itp.

Zachowanie się urządzenia "złożonego" (typu B), gdy pojawi się jego usterka, nie jest w pełni przewidywalne.
Przynajmniej jeden z jego elementów nie posiada dobrze opisanych wszystkich rodzajów uszkodzeń. Takimi elementami są m.in. mikroprocesory, układy ASIC itp.

Typ A: urządzenia „proste" (wszelkie usterki znane i opisane)

SFF Udział uszkodzeń bezpiecznych	HFT Tolerancja defektów sprzętu		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 – < 90 %	SIL 2	SIL 3	SIL 4
90 – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Typ B: urządzenia „złożone" (nie wszystkie usterki znane i opisane)

SFF Udział uszkodzeń bezpiecznych	HFT Tolerancja defektów sprzętu		
	0	1	2
< 60 %	nie dopuszcza się	SIL 1	SIL 2
60 – < 90 %	SIL 1	SIL 2	SIL 3
90 – < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Dla urządzeń „sprawdzonych w użyciu" parametr HFT może być pomniejszony o 1 (dotyczy wyłącznie SIL < 3) pod określonymi warunkami, zdefiniowanymi w PN-EN 61511.

Parametry

niezbędne do prawidłowego projektowania oprzyrządowania związanego z bezpieczeństwem

Istnieje kilka metod oceny elementów przyrządowego systemu bezpieczeństwa, w tym czujników i urządzeń wykonawczych:
- **Pełna ocena według normy PN-EN 61508**
  Kompletna ocena urządzenia i oprogramowania, zwykle prowadzona dla nowo powstających urządzeń. Analizie poddawane są m.in. metody unikania i kontroli usterek podczas projektowania, wytwarzania i eksploatacji urządzenia (cykl życia bezpieczeństwa).
- **"Sprawdzony w użyciu" według norm PN-EN 61508 oraz PN-EN 61511**
  Na potrzeby właściwej oceny istniejącego już na rynku urządzenia, norma PN-EN 61511 określa jego przydatność jako składnika przyrządowego systemu bezpieczeństwa. Ocena jest prowadzona na podstawie analizy statystycznej partii egzemplarzy sprawdzonych w użyciu. Analizie poddawane jest również oprogramowanie oraz procedury wytwórcy urządzenia, mające na celu ciągłą poprawę jego niezawodności.

Informacje wymagane przez projektanta lub użytkownika końcowego
Aby przeprowadzić ocenę przydatności oprzyrządowania związanego z bezpieczeństwem w określonym zadaniu ograniczania ryzyka, muszą zostać spełnione wymagania wybranego poziomu nienaruszalności bezpieczeństwa (SIL). Wynikają one wprost z analizy grafu ryzyka. W zależności od żądanego poziomu nienaruszalności bezpieczeństwa (SIL1, 2, 3 lub 4) należy określić wszystkie parametry ważne dla wdrożenia aplikacji związanej z bezpieczeństwem.

Bezpieczeństwo	Stan, w którym ryzyko ograniczono do akceptowalnego poziomu
E/E/PE	System elektryczny/elektroniczny/programowalny elektroniczny System sterowania, zabezpieczający lub monitorowania oparty na jednym lub więcej E/E/PE
Bezpieczeństwo funkcjonalne	Zdolność systemu do podejmowania niezależnych działań w celu osiągnięcia i utrzymania zdefiniowanego urządzeniu stanu bezpiecznego
Funkcja bezpieczeństwa	Funkcja realizowana przez przyrządowy systemu bezpieczeństwa E/E/PE, inny techniczny system bezpieczeństwa lub zewnętrzne ośrodki ograniczania ryzyka. Jej zadaniem jest doprowadzenie do osiągnięcia stanu bezpiecznego przez instalację zautomatyzowaną. W szczególności, zadziałanie funkcji bezpieczeństwa ma kluczowe znaczenie, gdy zachodzi realne ryzyko utraty kontroli nad instalacją zautomatyzowaną oraz narażenia zdrowia lub życia ludzi, czystości środowiska lub zniszczenia majątku trwałego.
SIL (poziom nienaruszalności bezpieczeństwa)	Norma PN-EN 61508 definiuje cztery dyskretne poziomy nienaruszalności bezpieczeństwa (SIL1 do SIL4). Każdy poziom odpowiada przedziałowi prawdopodobieństwa niezadziałania funkcji bezpieczeństwa. Im wyższy jest ten poziom, tym mniejsze jest prawdopodobieństwo niezadziałania tej funkcji.
SFF (udział uszkodzeń bezpiecznych)	Odsetek uszkodzeń, które nie wprowadzają oprzyrządowania związanego z bezpieczeństwem w stan braku zdolności do realizowania funkcji bezpieczeństwa.
PFD_{avg}	Średnie prawdopodobieństwo nie zadziałania funkcji bezpieczeństwa
λ_{SD}	Współczynnik występowania błędów bezpiecznych wykrywanych przez testy sprawdzające
λ_{SU}	Współczynnik występowania błędów bezpiecznych nie wykrywanych przez testy sprawdzające
λ_{DD}	Współczynnik występowania błędów niebezpiecznych wykrywanych przez testy sprawdzające
λ_{DU}	Współczynnik występowania błędów niebezpiecznych nie wykrywanych przez testy sprawdz.
HFT (tolerancja defektów sprzętu)	Zdolność oprzyrządowania do realizowania funkcji bezpieczeństwa w obecności błędów lub usterek. Parametr HFT równy N oznacza, że N+1 usterek może spowodować utratę zdolności oprzyrządowania do realizowania funkcji bezpieczeństwa.
T_1 [w latach]	Interwał testu sprawdzającego. Okresowy test przeprowadzany w celu wykrycia usterek w oprzyrządowaniu związanym z bezpieczeństwem.
MTBF	Średni czas bezawaryjnej pracy oprzyrządowania
MTTR	Średni czas przywracania zdatności oprzyrządowania do użycia
Głosowanie "MooN"	Architektura „M kanałów z N dostępnych": klasyfikacja i opis przyrządowego systemu bezpieczeństwa z uwagi na nadmiarowość i zastosowaną metodę wyboru kanału. "N" oznacza liczbę wszystkich dostępnych kanałów systemu (nadmiarowość), "M" oznacza liczbę sprawnych kanałów niezbędnych do zadziałania funkcji bezpieczeństwa. Przykład: pomiar ciśnienia z głosowaniem typu 1oo2. Przyrządowy system bezpieczeństwa decyduje, że ciśnienie przekroczyło uprzednio określoną wartość, gdy jeden z dwóch czujników ciśnienia ją zmierzy i wykaże. Dla architektury typu 1oo1 dostępny będzie tylko jeden czujnik ciśnienia.
MooND	Głosowanie typu „M kanałów z N dostępnych" wraz z diagnostyką
Rodzaj pracy na rzadkie przywołanie	Rodzaj pracy, w którym częstość przywołań funkcji przyrządowego systemu bezpieczeństwa jest nie większa niż raz na rok i nie większa niż podwójna częstość testu sprawdzającego
Rodzaj pracy – ciągła lub na częste przywołanie	Rodzaj pracy, w którym częstość przywołań funkcji przyrządowego systemu bezpieczeństwa jest większa niż raz na rok i większa niż podwójna częstość testu sprawdzającego
PN-EN 61508 (część 1 do 7)	Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych przyrządowych systemów bezpieczeństwa (Dotyczy: producentów i dostawców oprzyrządowania związanego z bezpieczeństwem)
PN-EN 61511 (część 1 do 3)	Bezpieczeństwo funkcjonalne: przyrządowe systemy bezpieczeństwa dla inżynierii procesowej (Dotyczy: projektantów systemów, integratorów i użytkowników końcowych)

Endress+Hauser

Twój partner w podnoszeniu bezpieczeństwa człowieka, instalacji technologicznej i środowiska naturalnego

Aparatura kontrolno-pomiarowa Endress+Hauser
- Najwyższej jakości przetworniki poziomu, ciśnienia, temperatury, przepływomierze i komponenty systemów automatyki przystosowane do pracy w przyrządowych systemach bezpieczeństwa (SIS)
- Wszystkie parametry aparatury kontrolno-pomiarowej związane z bezpieczeństwem dostępne u jednego źródła
- Nieodpłatna, pełna dokumentacja AKP związana z bezpieczeństwem w jednolitym formacie: certyfikaty, instrukcje dotyczące bezpieczeństwa, deklaracje producenta itd. dla ułatwienia projektowania, uruchomień, eksploatacji i prowadzenia okresowych testów sprawdzających obwodów regulacji, zabezpieczeń i odcięć krytycznych
- Ocena aktualizacji oprogramowania urządzeń pod kątem bezpieczeństwa według normy PN-EN 61508

Doświadczenie i wiedza inżynierów Endress+Hauser z zakresu bezpieczeństwa funkcjonalnego
- Wsparcie dla projektantów i użytkowników końcowych oprzyrządowania związanego z bezpieczeństwem w zakresie właściwego stosowania norm PN-EN 61508 oraz PN-EN 61511
- Szkolenia z zakresu eksploatacji aparatury kontrolno-pomiarowej w przyrządowych systemach bezpieczeństwa (SIS)

Aparatura kontrolno-pomiarowa Endress+Hauser dla wszystkich gałęzi inżynierii procesowej jest rozwijana zgodnie z wytycznymi normy PN-EN 61508.

Pełna lista urządzeń Endress+Hauser przystosowanych do pracy w przyrządowych systemach bezpieczeństwa wraz z kompletną dokumentacją jest dostępna w Internecie pod adresem **http://www.pl.endress.com/sil**