Bezpieczeństwo Funkcjonalne Poziom Nienaruszalności Bezpieczeństwa

Dr Thomas Reus
Matthias Garbsch

Bezpieczeństwo Funkcjonalne SIL Poziom Nienaruszalności Bezpieczeństwa

Dr Thomas Reus
Matthias Garbsch

Przedmowa

Przedmowa
Kto powinien przeczytać niniejszą publikację?
Niniejsza publikacja ma służyć jako pomoc wprowadzająca w tematykę bezpieczeństwa funkcjonalnego (rozdział 4 "Słowniczek", strona 15). Jest ona skierowana do klientów i pracowników JUMO, a jej treść ogranicza się do obszarów i zastosowań, w których wykorzystywane są produkty JUMO.

Dlaczego JUMO oferuje produkty SIL
JUMO opracowuje i produkuje m.in. produkty zgodne z dyrektywą dotyczącą urządzeń ciśnieniowych, dyrektywą maszynową, dyrektywą ATEX i specjalnymi normami dla produktów inżynierii bezpieczeństwa, takimi jak DIN 3440.

Norma DIN EN 61508 jest obecnie niezbędna dla produktów przeznaczonych do zastosowań bezpieczeństwa, ponieważ definiuje ona "stan techniki" w zakresie bezpieczeństwa funkcjonalnego.

Zestawienie produktów z funkcją SIL
Aktualny przegląd i szczegółowe informacje na temat naszych produktów z certyfikatem SIL można znaleźć na stronie:
www.jumo.de Products Approvals SIL.

Terminologia
Niniejsza broszura często odwołuje się do normy (DIN) EN 61508. Pełny tytuł tej normy to "Bezpieczeństwo funkcjonalne systemów E/E/PE związanych z bezpieczeństwem". Jej treść jest identyczna z międzynarodową normą IEC 61508.

Dr. Thomas ReusMatthias Garbsch

JUMO GmbH & Co. KG
Moritz-Juchheim-Straße 1
36039 Fulda, Germany
Phone: +49 661 6003-0
Fax: +49 661 6003-607
Email: thomas.reus@jumo.net
matthias.garbsch@jumo.net
Internet: www.jumo.net

Part No.: 00476107
Book No.: FAS630
Edition: April 2016
ISBN: 978-3-935742-18-4

Spis treści

Spis treści

1 Podstawy prawne, znaczenie norm

1.1 Motywacja do wprowadzenia norm

Naszym codziennym życiem rządzą maszyny i urządzenia, którym bezwiednie powierzamy nasze życie, np. samochody, sygnalizacja świetlna, sprzęt medyczny, instalacje energetyczne.

Z tego powodu ustawodawca wydał ustawy i inne przepisy prawne, które określają konkretne wymagania w zakresie bezpieczeństwa.

Na przykład w Niemczech ustawowe branżowe stowarzyszenia ubezpieczeniowe ("Berufsgenossenschaften") ustanawiają przepisy dotyczące zapobiegania wypadkom i nadzorują ich realizację. W całej Unii Europejskiej dyrektywy UE określają wymagania dla systemów i ich operatorów, w celu ochrony i zapewnienia zdrowia oraz jakości środowiska. Określają one specyficzne cechy produktów dla ochrony zdrowia i bezpieczeństwa konsumentów.

W Niemczech przestrzeganie norm i wymaganych standardów bezpieczeństwa jest egzekwowane poprzez ustawę o bezpieczeństwie urządzeń i produktów, w połączeniu z prawem do odszkodowania określonym przez § 823 niemieckiego kodeksu cywilnego ("Bürgerliches Gesetzbuch"). Dlatego nie tylko producenci urządzeń, jak JUMO, lecz także użytkownicy instalacji i urządzeń są zobowiązani do realizacji odpowiednich wymogów bezpieczeństwa.

Podobne regulacje obowiązują również w innych krajach.

W tym miejscu należy rozróżnić pomiędzy produktami bezpiecznymi w ogólnym znaczeniu, a produktami, które są specjalnie zaprojektowane do zastosowań związanych z bezpieczeństwem. W przypadku tych ostatnich, norma (DIN) EN 61508 stała się obecnie niezbędna, ponieważ definiuje ona "aktualny stan techniki" w zakresie bezpieczeństwa funkcjonalnego.

1.2 Normy bezpieczeństwa funkcjonalnego - rozwój (DIN) EN 61508

Kluczowym wydarzeniem była awaria spowodowana zatruciem gazem w północnowłoskim mieście Seveso w lipcu 1976 roku. Od tego czasu dyrektywa Unii Europejskiej 96/82/UE określiła warunki prawne dla zakładów o wysokim potencjale zagrożenia.

Niemiecka realizacja dyrektywy 96/82/UE jest zawarta w przepisach dotyczących niebezpiecznych zdarzeń w Federalnej Ustawie o Bezpieczeństwie Emisji (12. BImSchV).

Do dnia 31 lipca 2004 r. przepisy dotyczące niebezpiecznych wypadków odnosiły się do norm DIN V 19250 i DIN V 19251, w których wymagania były określone dla klas AK 1 do 8.

Od 2002 roku norma (DIN) EN 61508 wprowadza nową metodę oceny ryzyka i wymagane potwierdzenie skuteczności systemów bezpieczeństwa, aby w dalszym ciągu spełniać cele przepisów dotyczących niebezpiecznych zdarzeń. Definiuje ona cztery poziomy bezpieczeństwa: SIL1 do SIL4.

Tym samym norma (DIN) EN 61508 zastąpiła niemieckie normy DIN V 19250 i DIN V 19251.

Ratyfikacja serii norm miała miejsce w lipcu 2001 roku. Norma została następnie zaakceptowana przez europejską organizację normalizacyjną CENELEC. W dniu 1 sierpnia 2002 została włączona do niemieckiego zbioru norm jako (DIN) EN 61508 (VDE 0803) i tym samym definiuje stan techniki dla E/E/PE (elektrycznych, elektronicznych i programowalnych systemów elektronicznych), które są zaangażowane w funkcje bezpieczeństwa dla zastosowań istotnych dla bezpieczeństwa.

(DIN) EN 61508 jest normą ogólną, tzn. niezależną od zastosowania. Jest to podstawowa norma i dlatego ogólnie obowiązuje dla wszystkich systemów E/E/PE.

(DIN) EN 61508 jest oparta na międzynarodowej normie IEC 61508 i dlatego jest ważna na całym świecie. Jest to pierwszy międzynarodowy zharmonizowany zestaw przepisów, który jest niezależny od zastosowania dla wszystkich systemów E/E/PE.

Na tej podstawie powstają obecnie, jeden po drugim, standardy specyficzne dla danego zastosowania, takie jak:

- (DIN) EN 61511 dla bezpieczeństwa funkcjonalnego w inżynierii procesowej,
- (DIN) EN 62061 dla bezpieczeństwa funkcjonalnego w układach sterowania maszyn.

1 Podstawy prawne, znaczenie norm

Dalszy rozwój metodologii standaryzacji został wymuszony przez stale rosnącą złożoność nowoczesnych systemów o kluczowym znaczeniu dla bezpieczeństwa. Do połowy lat 90-tych można było powiedzieć: zastosowanie mikroelektroniki lub mikrokomputerów w inżynierii bezpieczeństwa było niewyobrażalne lub możliwe tylko przy użyciu bardzo zaangażowanego sprzętu testowego. W tym czasie wiele norm i przepisów nadal wyraźnie wymagało konwencjonalnych rozwiązań z blokadami realizowanymi przez przekaźniki lub styczniki. Stosowanie urządzeń nowocześniejszych, bardziej ekonomicznych, a często nawet lepszych z punktu widzenia inżynierii bezpieczeństwa, nie było dozwolone. Wymagania, jakie musi spełniać system, stają się jednak coraz bardziej złożone i z reguły mogą być ekonomicznie spełnione tylko przez rozwiązania elektroniczne. Dotyczy to w szczególności sektora komputerów cyfrowych i automatyki, gdzie w jednostce centralnej stosowane są złożone układy cyfrowe.

1.3 Pozycja prawna normy (DIN) EN 61508 w rozumieniu dyrektywy UE

(DIN) EN 61508 opisuje aktualny stan techniki w zakresie bezpieczeństwa funkcjonalnego.
Nie jest ona jednak zharmonizowana jako część dyrektywy UE, tzn. nie istnieje automatyczne założenie spełnienia celów ochronnych dyrektywy związanej z tą normą.
W chwili obecnej zgodność jest więc dobrowolna i nie jest wiążąca w rozumieniu dyrektyw UE.
Niemniej jednak producent wyrobu inżynierii bezpieczeństwa może zastosować normę (DIN) EN 61508 w celu spełnienia wymagań podstawowych zgodnie z dyrektywami europejskimi.
Wynika to z nowej koncepcji normy, np. w następujących przypadkach:

Zharmonizowana norma europejska (taka jak (DIN) EN 954 i (DIN) EN 60204-1, które ujednolicają Dyrektywę Maszynową) zawiera odniesienie do (DIN) EN 61508. Gwarantuje to, że odpowiednie wymagania normy są spełnione ("wspólnie stosowana norma").
Jeżeli producent stosuje normę (DIN) EN 61508 w myśl tego przepisu, w sposób fachowy i odpowiedzialny, to korzysta z założenia o spełnieniu wymagań normy odniesienia.

Nie ma zharmonizowanej normy (jak np. DIN 3440, DIN EN 14597) dla danego zastosowania. W takim przypadku producent może zastosować normę (DIN) EN 61508 (stan techniki). Nie można jednak założyć, że spełnione są wymagania.

Wyjaśnienie:
Dla przemysłu przetwórczego norma (DIN) EN 61511 została już wyprowadzona z normy (DIN) EN 61508 jako norma podstawowa. Podobnie dla dyrektywy maszynowej dostępna jest norma (DIN) EN 62061. Dla inżynierii spalinowej standardowo dostępna jest norma (DIN) EN 50156.W zakresie techniki spalania jako norma dostępna jest norma (DIN) EN 50156.

2 Podstawowa zasada normy (DIN) EN 61508

2.1 Zmiany w stosunku do poprzednich norm bezpieczeństwa

W normie (DIN) EN 61508 dotyczącej bezpieczeństwa funkcjonalnego, wymagania dla systemów bezpieczeństwa są podzielone na poziomy nienaruszalności bezpieczeństwa (SIL) (patrz Słowniczek). Przyrządy, czujniki i sterowniki muszą zatem posiadać klasyfikację SIL zgodnie z normą. Pojawia się również nowe rozumienie bezpieczeństwa. Podczas gdy poprzednie normy dotyczące inżynierii bezpieczeństwa obejmowały zazwyczaj analizę czysto jakościową, nowa norma wymaga po raz pierwszy ilościowego zbadania całego systemu i udowodnienia, że ryzyko szczątkowe jest wystarczająco małe.

Ponadto, po raz pierwszy uregulowany został również cały cykl życia systemu bezpieczeństwa, patrz rozdział 2.4 *"Cykl życia", strona 10*.

2.2 Zmniejszenie ryzyka

Każde zastosowanie technologii wiąże się z jednoczesnym ryzykiem związanym z inżynierią bezpieczeństwa. Im bardziej zagrożeni są ludzie, mienie lub środowisko, tym więcej środków należy podjąć w celu zmniejszenia tego ryzyka. Ryzyko powinno być przynajmniej tak zredukowane, aby prawdopodobieństwo utraty życia przez osobę w wyniku awarii urządzenia technicznego było mniejsze niż 4-10 wypadków śmiertelnych / na osobę i rok.

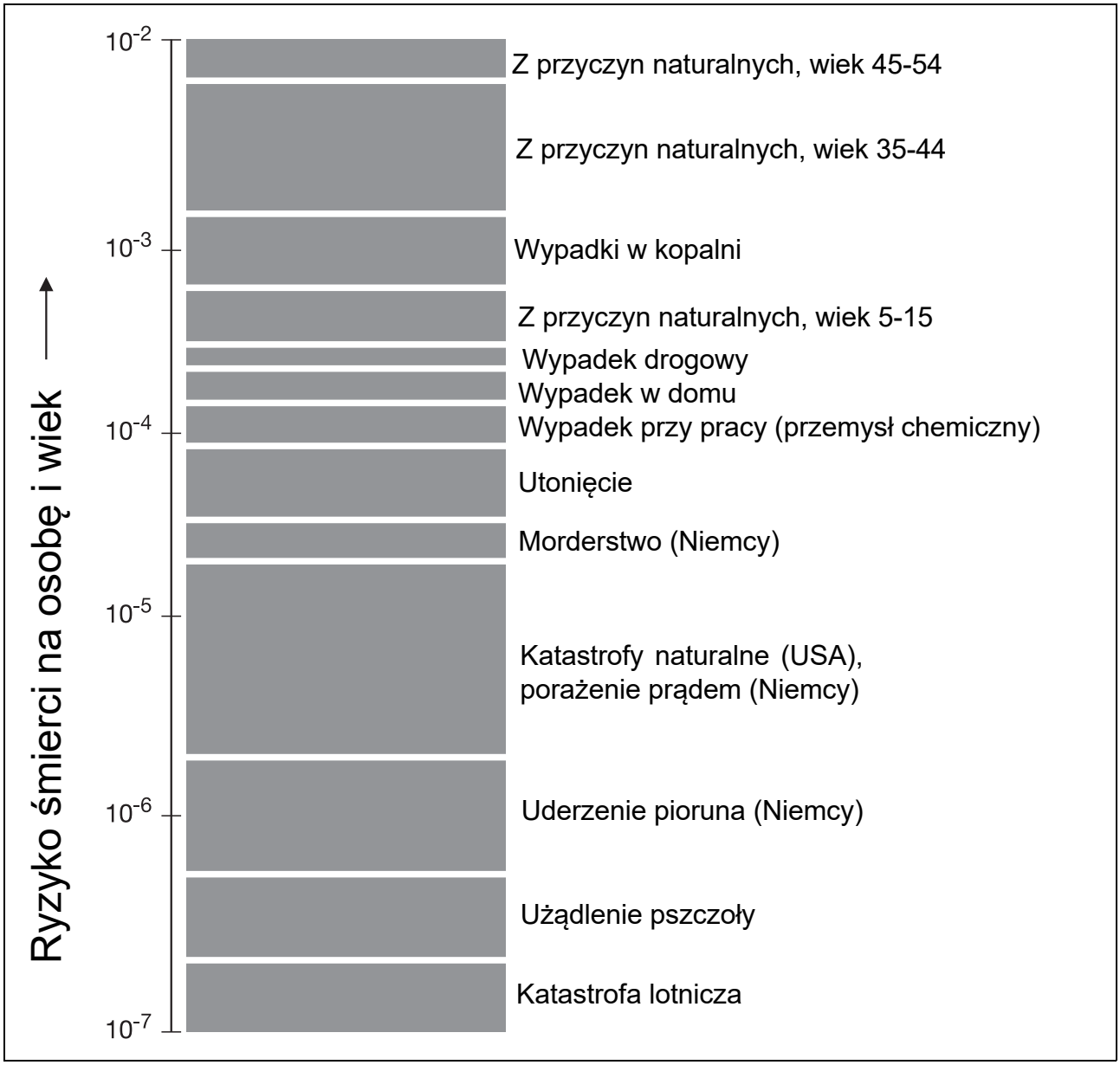
Jest to w przybliżeniu równoważne ryzyku utraty życia przez jedną osobę z przyczyn naturalnych w ciągu roku. Ryzyko to zmienia się w zależności od wieku danej osoby i mieści się w przedziale od 2-10 do 4-10.

Zestawienie podstawowych zagrożeń życia codziennego przedstawiono na rys. 1 na stronie 8.

W celu osiągnięcia bezpieczeństwa funkcjonalnego maszyny lub instalacji należy zapewnić, aby istotne dla bezpieczeństwa części urządzeń sterujących i zabezpieczających funkcjonowały prawidłowo, a w przypadku awarii reagowały w taki sposób, że system pozostanie bezpieczny lub zostanie wprowadzony w stan bezpieczny.

Celem normy (DIN) EN 61508 jest unikanie błędów w systemach bezpieczeństwa lub kontrolowanie błędów i ograniczanie prawdopodobieństwa wystąpienia niebezpiecznych awarii (ryzyka) w określony sposób. Dla pozostałego ryzyka szczątkowego wymagany jest dowód ilościowy.

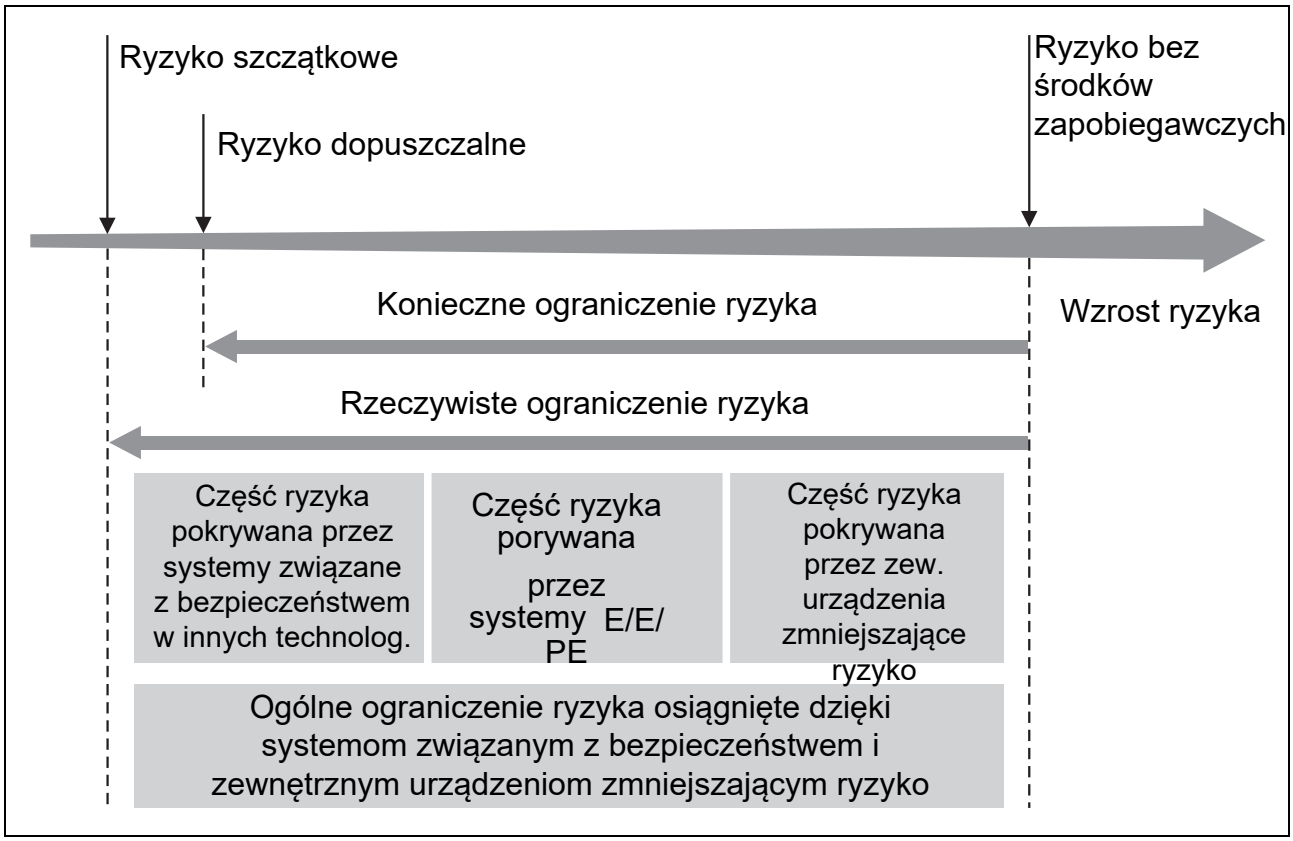
2 Podstawowa zasada normy (DIN) EN 61508



Rysunek 1: Podsumowanie podstawowych zagrożeń

2.3 Ryzyko dopuszczalne

Dopuszczalne ryzyko dla danej technologii nie zawsze jest jasno zdefiniowane, ale zasadniczo jest określane przez środowisko, przy uwzględnieniu czynników społecznych i politycznych.
Jeżeli ryzyko związane z instalacją techniczną jest postrzegane jako zbyt wysokie, należy wdrożyć specjalne środki w celu jego zmniejszenia.
Niezbędne zmniejszenie ryzyka uzyskuje się poprzez połączenie wszystkich środków ochronnych mających wpływ na bezpieczeństwo. Ryzyko szczątkowe powinno być co najwyżej nie większe niż ryzyko tolerowane.
W ostatecznym rozrachunku operator zakładu musi zaakceptować i ponieść ryzyko szczątkowe.



Rysunek 2: Zmniejszenie ryzyka: założenia ogólne

2 Podstawowa zasada normy (DIN) EN 61508

2.4 Cykl życia

Operator systemu bezpieczeństwa musi podjąć odpowiednie kroki w celu oceny i redukcji ryzyka podczas całego cyklu życia systemu. W tym celu norma (DIN) EN 61508 zaleca następujące kroki:

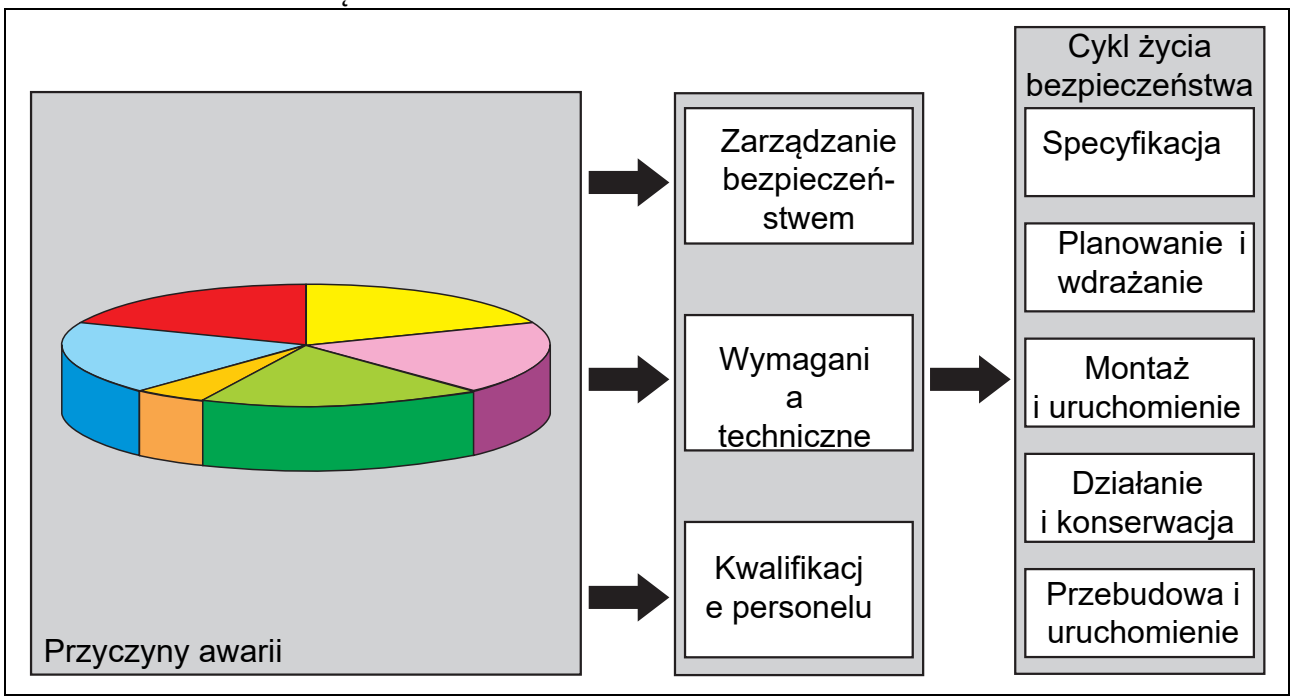
Definicja i ocena ryzyka na podstawie szczegółowych prawdopodobieństw awarii - dla całego obwodu bezpieczeństwa (pętli) od punktu pomiarowego przez system sterowania do napędu, jak również podczas całego cyklu życia (Overall Safety Life Cycle) danego zastosowania.
Można to zrobić na przykład poprzez FMEDA (Failure Mode, Effect and Diagnostics Analysis) lub Hazard Analysis.

Określenie i wdrożenie środków (Zarządzanie Bezpieczeństwem Funkcjonalnym) w celu zmniejszenia ryzyka szczątkowego.

Użycie odpowiedniego (certyfikowanego) sprzętu.

Okresowe sprawdzanie, czy przepisy są prawidłowo przestrzegane.

Ogólny zarys procedury postępowania systematycznego przedstawiono na rysunku 3. Pierwszym krokiem jest przeprowadzenie analizy awarii. Następnie wybiera się środki do utrzymania kontroli nad usterkami i wdraża się te środki.



Rysunek 3: Procedura wdrażania (DIN) EN 61508

2.5 Zadanie JUMO w cyklu życia bezpieczeństwa

Operator systemu bezpieczeństwa potrzebuje pewnej ilości danych technicznych i informacji o wszystkich stosowanych urządzeniach, aby móc przeprowadzić ocenę ryzyka dla całej pętli bezpieczeństwa i dla całego okresu eksploatacji systemu.

Dla użytkownika instalacji korzystne jest, aby mógł korzystać z urządzeń posiadających certyfikat SIL. W tym przypadku producent, np. JUMO, poprzez szczegółową analizę zagrożeń i ryzyka ustalił już niezbędne dane dla danego urządzenia. Wszystkie istotne dane i informacje dla klienta są następnie przedstawiane w instrukcji bezpieczeństwa. Stosowane tam pojęcia wyjaśnione są w następnym rozdziale.

3 Terminy stosowane w normie (DIN) EN 61508

3.1 Nienaruszalność bezpieczeństwa i jej pomiar - Poziom Nienaruszalności Bezpieczeństwa (SIL)

Poziom nienaruszalności bezpieczeństwa (niezawodność związana z bezpieczeństwem) systemu to "Prawdopodobieństwo, że system bezpieczeństwa wykona wymaganą funkcję bezpieczeństwa we wszystkich określonych warunkach w określonym czasie zgodnie ze specyfikacją."

Poziom nienaruszalności bezpieczeństwa (Safety Integrity Level - SIL) jest miarą nienaruszalności bezpieczeństwa. Jest on podzielony na cztery odrębne poziomy, przy czym poziom nienaruszalności bezpieczeństwa 4 reprezentuje najwyższy poziom nienaruszalności bezpieczeństwa, a poziom nienaruszalności bezpieczeństwa 1 reprezentuje poziom najniższy.

Osiągalny SIL jest określany przez następujące parametry:

- prawdopodobieństwo niebezpiecznego uszkodzenia funkcji bezpieczeństwa (PFD lub PFH),
- sprzętowa odporność na awarie (HFT),
- wskaźnik uszkodzeń bezpiecznych (SFF),
- typ części składowych (typ A lub typ B),
- czas życia, oraz
- dowód - test.

3.2 PFD, PFH: tryby pracy i prawdopodobieństwo awarii

W klasyfikacji SIL rozróżnia się dwa tryby pracy: Low Demand Mode (tryb niskiego zapotrzebowania) i High Demand Mode (tryb wysokiego zapotrzebowania).

Tryb niskiego zapotrzebowania
W przypadku pracy w trybie niskiego zapotrzebowania zakłada się, że funkcja bezpieczeństwa musi reagować średnio tylko raz w roku. W tym przypadku wartość SIL jest określana na podstawie PFD (Probability of Failure on Demand - prawdopodobieństwo awarii na żądanie).

PFD jest miarą prawdopodobieństwa awarii funkcji bezpieczeństwa na żądanie, w systemie działającym przy niskim poziomie zapotrzebowania.

Tryb niskiego zapotrzebowania jest zwykle spotykany w instalacjach i zakładach przemysłu przetwórczego. Występują tu na przykład systemy awaryjnego wyłączenia, które uaktywniają się tylko wtedy, gdy normalny proces wymyka się spod kontroli.

Tryb dużego zapotrzebowania
W przypadku pracy w trybie wysokiego zapotrzebowania zakłada się, że funkcja bezpieczeństwa musi reagować stale lub średnio raz na godzinę.

W przypadku wysokiego lub ciągłego tempa zapotrzebowania stosuje się miarę PFH (Probability of Failure per Hour), która wyraża prawdopodobieństwo wystąpienia awarii funkcji bezpieczeństwa w ciągu jednej godziny.

Tryb wysokiego zapotrzebowania jest zwykle spotykany w instalacjach produkcyjnych, gdzie konieczne jest ciągłe monitorowanie operacji produkcyjnych.

3 Terminy stosowane w normie (DIN) EN 61508

Tryb pracy z niskim poziomem zapotrzebowania (Low Demand Mode)	
Poziom nienaruszalności bezpieczeństwa	**PFD** (średnie prawdopodobieństwo awarii funkcji bezpieczeństwa na żądanie usługi)
SIL 4	10^{-5} do $<10^{-4}$
SIL 3	10^{-4} do $<10^{-3}$
SIL 2	10^{-3} do $<10^{-2}$
SIL 1	10^{-2} do $<10^{-1}$

Tabela 1: Poziom nienaruszalności bezpieczeństwa: wartości graniczne wskaźnika awaryjności dla funkcji bezpieczeństwa działającej przy niskim poziomie zapotrzebowania

Tryb pracy z wysokim poziomem zapotrzebowania (High Demand Mode)	
Poziom nienaruszal-ności bezpieczeństwa	**PFH** (prawdopodobieństwo wystąpienia niebezpiecznej awarii na godzinę)
SIL 4	10^{-9} do $<10^{-8}$
SIL 3	10^{-8} do $<10^{-7}$
SIL 2	10^{-7} do $<10^{-6}$
SIL 1	10^{-6} do $<10^{-5}$

Tabela 2: Poziom nienaruszalności bezpieczeństwa: wartości graniczne wskaźnika awaryjności dla funkcji bezpieczeństwa działającej przy wysokim poziomie zapotrzebowania, lub przy ciągłym zapotrzebowaniu

3.3 HFT, SFF: Nienaruszalność bezpieczeństwa sprzętu

Następujące parametry są również wykorzystywane do określania klasyfikacji SIL:

- sprzętowa odporność na awarie (HFT) i
- udział uszkodzeń bezpiecznych (SFF, Safe Failure Fraction)

W tabelach 3 i 4 przedstawiono tę zależność.
Zgodnie z normą (DIN) EN 61508 należy rozróżniać pomiędzy systemami typu A i typu B.

Systemy typu A
System częściowy może być postrzegany jako system typu A, jeżeli w odniesieniu do elementów, które są niezbędne do realizacji funkcji bezpieczeństwa,

a) sposoby uszkodzenia wszystkich wykorzystywanych komponentów są odpowiednio określone, oraz

b) odpowiedź systemu częściowego w warunkach uszkodzenia może być całkowicie określona, oraz

c) dla systemu częściowego dostępne są wiarygodne dane dotyczące awarii, oparte na doświadczeniu praktycznym, w celu wykazania, że zakładane wskaźniki awaryjności dla rozpoznanych i nierozpoznanych awarii niebezpiecznych mogą zostać osiągnięte.

Systemy typu B
Wszystkie pozostałe systemy mogą być postrzegane jako systemy typu B, tzn. system częściowy może być postrzegany jako system typu B, jeżeli w odniesieniu do elementów, które są niezbędne do realizacji funkcji bezpieczeństwa,

a) sposoby uszkodzenia co najmniej jednego z zastosowanych komponentów nie są odpowiednio określone, lub

b) nie można w pełni określić reakcji układu częściowego w warunkach uszkodzenia, lub

c) dla systemu częściowego nie są dostępne żadne odpowiednio wiarygodne dane dotyczące awarii, oparte na doświadczeniu praktycznym, które potwierdzałyby założone wskaźniki awaryjności dla rozpoznanych i nierozpoznanych niebezpiecznych awarii.

HFT (Hardware Fault Tolerance)
Odporność na błędy N dla sprzętu oznacza, że N+1 błędów może spowodować awarię funkcji bezpieczeństwa.
Odporność na błędy sprzętowe definiowana jest również przez zastosowaną architekturę "MooN".
Wyrażenie MooN (dla architektury z M z N kanałów) opisuje architekturę urządzenia SIL.
Przykładowo, 1oo2 oznacza architekturę z 2 kanałami, przy czym każdy z kanałów może realizować funkcję bezpieczeństwa.
Dla systemu 1oo2, HFT = 1
Dla systemu 1oo1, HFT = 0

SFF (Safe Failure Fraction)

SFF to odsetek awarii nie stanowiących zagrożenia, tzn. wyższy SIL wymaga wyższego SFF.
Współczynnik SFF systemu jest obliczany na podstawie indywidualnych współczynników awaryjności (wartości) dla poszczególnych komponentów, patrz rozdział 3.5*"Współczynnik* awaryjności*",strona 14.*

Systemy typu A			
Wskaźnik uszkodzeń bezpiecznych (SFF)	**Sprzętowa odporność na awarie**		
	HFT = 0	HFT = 1	HFT = 2
<60%	SIL1	SIL2	SIL3
60 do <90%.	SIL2	SIL3	SIL4
90 do <99%.	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

Tabela 3: Nienaruszalność bezpieczeństwa sprzętu: ograniczenia wynikające z architektury, dla systemów częściowych typu A związanych z bezpieczeństwem

Systemy typu B			
Wskaźnik uszkodzeń bezpiecznych (SFF)	**Sprzętowa odporność na awarie**		
	HFT = 0	HFT = 1	HFT = 2
<60%	niedozwolony	SIL1	SIL2
60 do <90%.	SIL1	SIL2	SIL3
90 do <99%.	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

Tabela 4: Nienaruszalność bezpieczeństwa sprzętu: ograniczenia wynikające z architektury, dla systemów częściowych typu B związanych z bezpieczeństwem

3 Terminy stosowane w normie (DIN) EN 61508

3.4 Okres użytkowania i odstęp testu sprawdzającego

Okres użytkowania
Po upływie okresu użytkowania urządzenia należy je wymienić, ponieważ nie spełnia ono już wymogów certyfikatu SIL.

Odstęp testu sprawdzającego
Odstęp czasu między testami kontrolnymi definiuje powtarzany test mający na celu wykrycie usterek w systemie SIL, tak aby w razie potrzeby można było przywrócić system do stanu "jak nowego". Jeżeli okres próbny jest taki sam jak okres eksploatacji, wówczas nie jest wymagany żaden test próbny.

3.5 Wskaźnik usterek

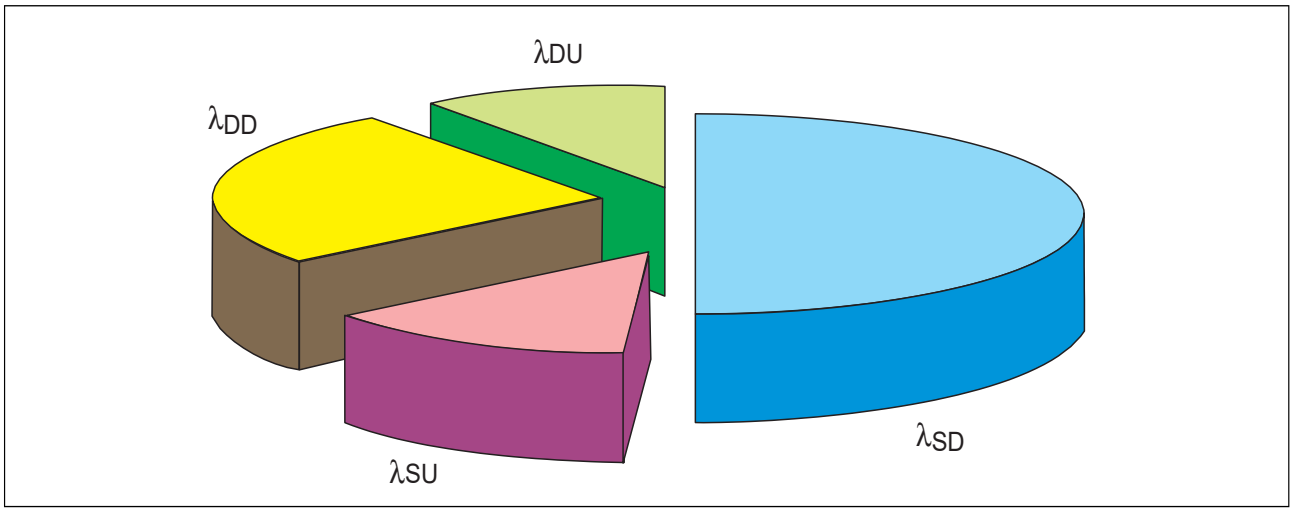
Po pomyślnie zakończonej analizie zagrożeń i ryzyka, konieczne jest wdrożenie jej wyników do systemu. Ważną rolę odgrywa zdolność systemu do wykrywania usterek i odpowiedniego reagowania. Należy więc rozróżnić usterki niebezpieczne i niegroźne oraz możliwość ich wykrycia lub nie.

Wskaźnik awaryjności jest określany przez współczynnik λ , i jest ogólnie podzielony na cztery grupy (patrz Rysunek 4):

- λ_{SD} = bezpieczny wykryty wskaźnik awaryjności (usterki, które zostały wykryte i nie stanowią zagrożenia),
- λ_{SU} = bezpieczny niewykryty wskaźnik awaryjności (usterki niewykryte i nie stanowiące zagrożenia),
- λ_{DD} = niebezpieczna wykryta awaryjność (usterki, które są wykryte i niebezpieczne),
- λ_{DU} = niebezpieczna niewykryta awaryjność (usterki, które nie są wykryte i stanowią zagrożenie),

Zazwyczaj usterki wykryte i niegroźne stanowią największą część. Niewykryte, niebezpieczne usterki λ_{DU} stanowią z kolei niewielką część wszystkich możliwych usterek. Ten rodzaj usterek jest jednak najbardziej niebezpieczny, dlatego też należy podjąć odpowiednie środki, aby jego udział był jak najmniejszy.

Wymiar dla tych wartości λ to FIT (Failures In Time, w 1 x 10^{-9} na godzinę).



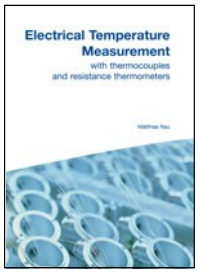
Rysunek 4: Usterki w szczegółach

Wskaźnik usterki λ	= Wskaźnik awaryjności systemu (λ) jest ogólnie podzielony na cztery grupy: • λ_{SD} = bezpieczny wykryty wskaźnik awaryjności (usterki, które zostały wykryte i nie stanowią zagrożenia), • λ_{SU} = bezpieczny niewykryty wskaźnik awaryjności (usterki niewykryte i nie stanowiące zagrożenia), • λ_{DD} = niebezpieczna wykryta awaryjność (usterki, które są wykryte i niebezpieczne), • λ_{DU} = niebezpieczna niewykryta awaryjność (usterki, które nie są wykryte i stanowią zagrożenie),
systemy E/E/PE FIT	= Systemy elektryczne, elektroniczne i programowalne elektroniczne (E/E/EP)
(Awarie w czasie)	= Awarie w czasie (1×10^{-9} na godzinę)
Bezpieczeństwo Funkcjonalne	= Zdolność systemu do wykonywania niezbędnych działań w celu osiągnięcia lub utrzymania określonego stanu bezpieczeństwa dla instalacji znajdujących się pod kontrolą tego systemu.
HFT (Sprzętowa odporność na awarie)	= Odporność na błędy N dla sprzętu oznacza, że N+1 błędów może może spowodować awarię funkcji bezpieczeństwa.
Okres użytkowania	= Po upływie okresu użytkowania urządzenia, należy je wymienić, ponieważ nie spełnia już wymagań certyfikatu SIL.
MooN (M out of N)	= Architektura bezpieczeństwa dla M z N kanałów. Na przykład 1oo2 oznacza architekturę z 2 kanałami, przy czym każdy z kanałów może realizować funkcję bezpieczeństwa.
PFD (Prawdopodobieństwo awarii na żądanie)	= PFD jest miarą prawdopodobieństwa awarii funkcji bezpieczeństwa na żądanie, w systemie działającym przy niskim poziomie zapotrzebowania (prawdopodobieństwo niebezpiecznej awarii systemu na żądanie).
PFH (Prawdopodobieństwo awarii na godzinę)	W przypadku wysokiego lub ciągłego zapotrzebowania stosuje się miarę PFH, która wyraża prawdopodobieństwo wystąpienia awarii funkcji bezpieczeństwa w ciągu jednej godziny (prawdopodobieństwo niebezpiecznej awarii).
Proof-check interval	= Przedział kontroli poprawności definiuje powtarzany test mający na celu wykrycie usterek w systemie SIL, tak aby w razie potrzeby można było przywrócić system do stanu "jak nowy".
SFF (Wskaźnik uszkodzeń bezpiecznych)	= Odsetek awarii innych niż niebezpieczne
SIL (Poziom nienaruszalności bezpieczeństwa)	= Poziom nienaruszalności bezpieczeństwa (SIL) jest miarą nienaruszalności bezpieczeństwa systemu. Nienaruszalność bezpieczeństwa systemu to prawdopodobieństwo, że system wykona wymaganą funkcję bezpieczeństwa we wszystkich zdefiniowanych warunkach w określonym czasie. SIL dzieli się na cztery odrębne poziomy, przy czym poziom nienaruszalności bezpieczeństwa 4 reprezentuje najwyższy poziom nienaruszalności bezpieczeństwa, a poziom integralności bezpieczeństwa 1 reprezentuje poziom najniższy.

4 Słowniczek

Materiał informacyjny od JUMO - dla początkujących i tych z pewnym doświadczeniem praktycznym

Wiedza jest potrzebna nie tylko do tworzenia produktów JUMO, lecz także do ich późniejszego zastosowania. Dlatego też oferujemy naszym użytkownikom szereg publikacji dotyczących aspektów techniki pomiarowej i sterowania.
Publikacje te mają na celu zapoznanie krok po kroku z szerokim zakresem zastosowań, zarówno dla początkujących, jak i dla tych, którzy mają już pewne doświadczenie praktyczne. Ilustrują one przede wszystkim tematy ogólne z pewnymi zastosowaniami specyficznymi dla JUMO.
Oprócz literatury technicznej JUMO i naszych nowych programów do pobrania oferujemy również możliwość zamówienia online naszych broszur i katalogów CD-ROM.

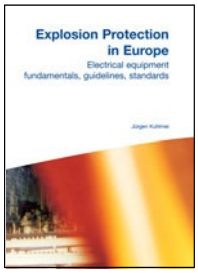


Elektryczny pomiar temperatury z termoparami i termometry oporowe
Matthias Nau

FAS 146
Nr katalogowy: 00085081
ISBN: 978-3-935742-07-X
Bezpłatnie

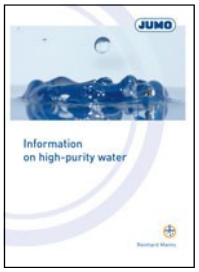
Inżynieria sterowania
Podstawowe zasady i wskazówki dla praktyków
Manfred Schleicher

FAS 525
Nr sprzedaży: 00323761
ISBN: 978-935742-01-6
Bezpłatnie



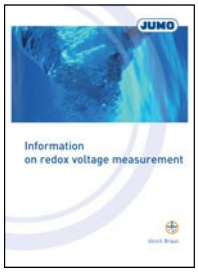
Ochrona przeciwwybuchowa w Europie
Urządzenia elektryczne podstawy, wytyczne, normy
Jürgen Kuhlmei

FAS 547
Nr katalogowy: 000414312 ISBN: 978-3-935742-10-X
Bezpłatnie



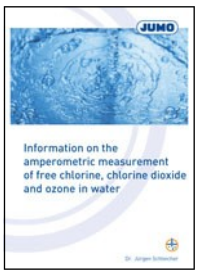
Informacje na wodzie o wysokiej czystości
Reinhard Manns

FAS 614
Nr sprzedaży: 00403834
Bezpłatnie



Informacje w sprawie pomiaru napięcia redox
Ulrich Braun

FAS 615
Nr sprzedaży: 00398237
Bezpłatnie

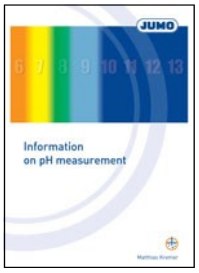


Informacje na temat amperometrycznych pomiarów wolnego chloru, dwutlenku chloru i ozonu w wodzie
Dr. Jürgen Schleicher

FAS 619
Nr sprzedaży: 00398147
Bezpłatnie

Sterowniki mocy SCR
Podstawowe zasady i wskazówki dla profesjonalistów
Manfred Schleicher, Winfried Schneider

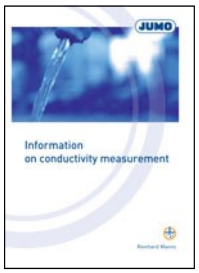
FAS 620
Nr sprzedaży: 00400481
ISBN: 978-3-935742-05-4
Bezpłatnie



Informacje w sprawie pomiaru pH
Matthias Kremer

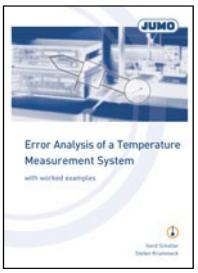
FAS 622
Nr sprzedaży: 00403233
Bezpłatnie

Materiał informacyjny od JUMO - dla początkujących i tych z pewnym doświadczeniem praktycznym



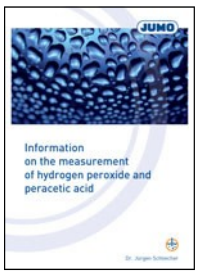
Informacje
w sprawie pomiaru
przewodności
Reinhard Manns

FAS 624
Nr sprzedaży:
00411341
Bezpłatnie



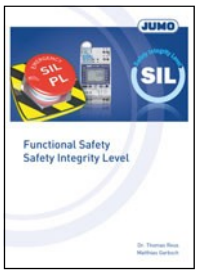
Analiza błędów
System Pomiaru Temperatury
z przykładami praktycznymi
Gerd Scheller, Stefan Krummeck

FAS 625
Nr sprzedaży: 00415704
ISBN-13: 978-3-935742-13-4
Bezpłatnie



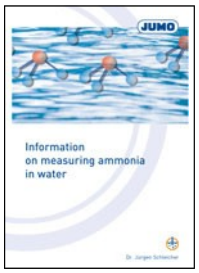
Informacje na temat pomiaru
nadtlenku wodoru
i kwas nadoctowy
Dr. Jürgen Schleicher

FAS 628
Nr sprzedaży:
00420697
Bezpłatnie



Bezpieczeństwo
funkcjonalne Poziom
integralności
bezpieczeństwa
Dr. Thomas Reus, Matthias Garbsch

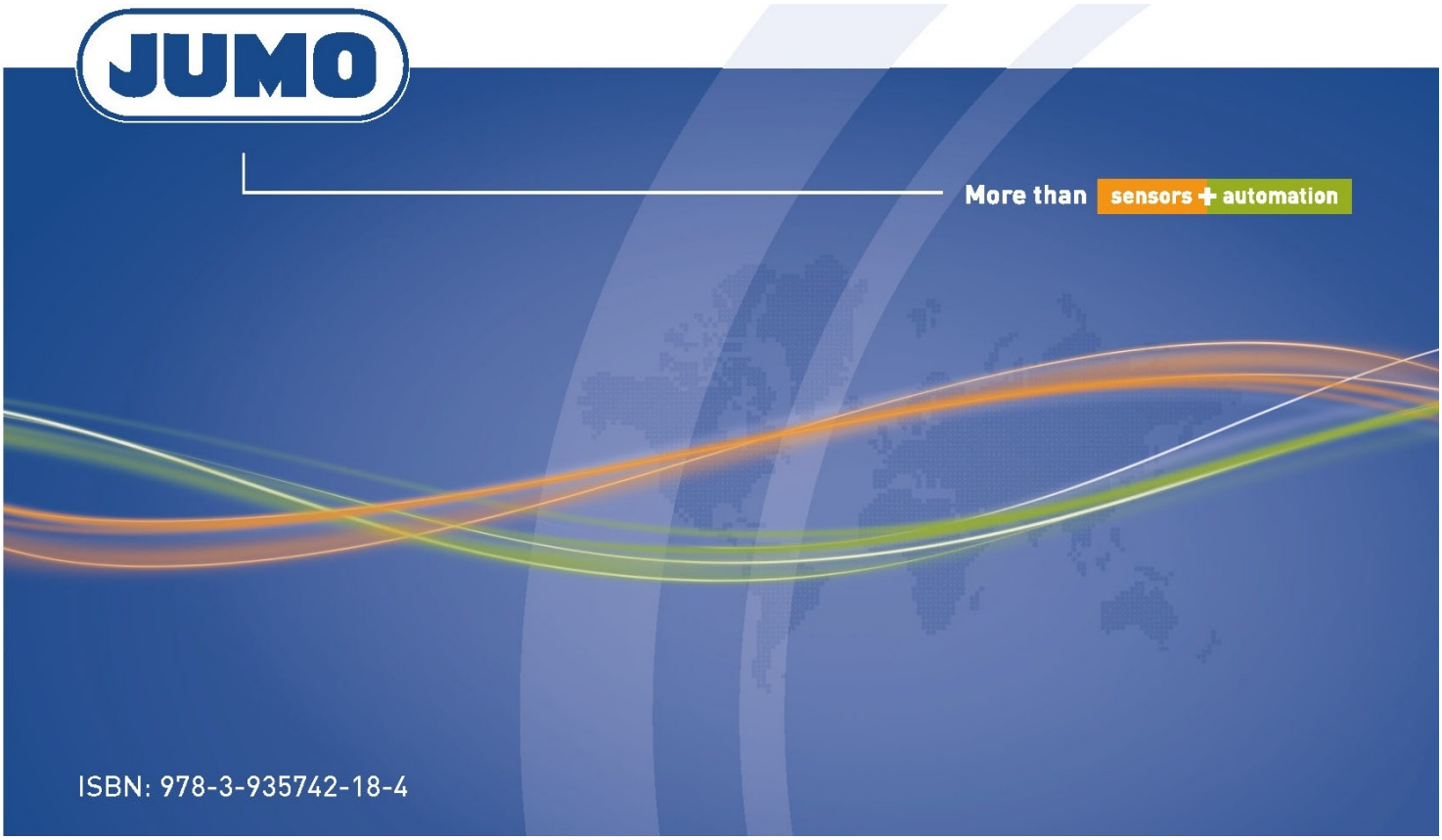
FAS 630
Nr sprzedaży:
00476107
Bezpłatnie



Informacje
w sprawie pomiaru amoniaku w wodzie
Dr. Jürgen Schleicher

FAS 631
Nr sprzedaży:
00485097
Bezpłatnie

Zapraszamy do odwiedzenia naszej strony internetowej www.jumo.net i zapoznania się z szeroką gamą produktów JUMO dla różnych obszarów zastosowań. Na naszej stronie internetowej znajdą Państwo więcej szczegółów i informacji o osobach kontaktowych w przypadku wymagań, pytań i zamówień.



ISBN: 978-3-935742-18-4

www.jumo.net