auma®

Solutions for a world in motion

Bezpieczeństwo funkcjonalne - SIL

Zmniejszenie ryzyka dzięki zastosowaniu napędów elektrycznych

AUMA - ekspert w zakresie napędów ustawczych

AUMA jest jednym z wiodących światowych producentów napędów elektrycznych, sterowników do napędów oraz przekładni dla automatyzacji armatury przemysłowej. AUMA posiada 45-letnie doświadczenie w pracach badawczo-rozwojowych i produkcji elektrycznych napędów niepełno- i wieloobrotowych. AUMA produkuje swoje wyroby w dwóch niemieckich zakładach: w Muellheim i Ostfildern. Trzy centra serwisowe w Kolonii, Magdeburgu i Monachium świadczą usługi wsparcia technicznego. Grupa AUMA zatrudnia 2200 pracowników na całym świecie.

AUMA automatyzuje armaturę

Napędy AUMA muszą spełniać liczne złożone wymagania i funkcjonować w różnorodnych zastosowaniach - to nasza zawodowa codzienność. Nasza długoterminowa polityka produktowa opiera się na zasadzie konstrukcji modułowej, gwarantując wymaganą elastyczność w dostosowywaniu asortymentu napędów do wymogów klienta.

Globalna obecność

Aby była możliwa, konieczna jest dobra znajomość rynków. Myśleć globalnie, znaczy działać lokalnie. Dzięki rozbudowanej światowej sieci sprzedaży i usług każdy klient może liczyć na wsparcie kompetentnego lokalnego doradcy.

Dostawy z jednego źródła

Od projektu produktu do testów urządzenia i kontroli końcowej AUMA stosuje procedury ciągłego wytwarzania i zapewniania jakości, podlegające bieżącym inspekcjom.

Od 1964 roku AUMA zyskała wyjątkową renomę w branży napędów. Niezawodność i innowacyjność są pojęciami ściśle powiązanymi z AUMA. Jest tak dzięki zaangażowaniu naszych pracowników, którzy z poświęceniem pracują nad przyszłością napędów.

Spis treści

AUMA - ekspert w zakresie napędów ustawczych 2
O tym dokumencie 3
Zmniejszenie ryzyka dzięki bezpieczeństwu funkcjonalnemu 4
Normy PN EN IEC 61508 i PN EN IEC 61511 6
Jak osiągnąć bezpieczeństwo funkcjonalne? 7
Czym jest funkcja bezpieczeństwa? 8
Czym jest przyrządowy system bezpieczeństwa? 9
Najważniejsze parametry bezpieczeństwa 10
Określanie zdolności SIL 12
Zwiększanie zdolności SIL 13
Zdolność SIL produktów AUMA 14
SIL 2/SIL 3 dla zintegrowanych sterowników AC .2 w wersji SIL 16
Funkcje modułu SIL 18
Określenie wart. parametrów bezpieczeństwa produktów AUMA 20
Parametry bezpieczeństwa wybranych produktów AUMA 24
Dodatkowe informacje 26
Indeks 27

O tym dokumencie

Bezpieczeństwo funkcjonalne oraz SIL [poziom nienaruszalności bezpieczeństwa] są terminami dość często występującymi w połączeniu z bezpieczeństwem systemów technicznych - wspieranymi wydaniem nowych norm międzynarodowych.

Napędy AUMA są często wykorzystywane w zastosowaniach mających zasadnicze znaczenie dla bezpieczeństwa, a tym samym przyczyniają się do bezpiecznej eksploatacji systemów technicznych. Z tego powodu kwestia bezpieczeństwa funkcjonalnego jest dla nas tak istotna.

Niniejsza broszura dostarcza informacji na temat bezpieczeństwa funkcjonalnego napędów i sterowników napędów firmy AUMA. Oprócz podstawowego wprowadzenia do zagadnień bezpieczeństwa funkcjonalnego znajdą tu Państwo szczegółowe informacje dotyczące poziomu SIL produktów firmy AUMA.

Aktualne informacje o produktach AUMA są dostępne na stronie internetowej www.auma.com. Wszystkie dokumenty można pobrać ze strony.

2013.02.06

Zagadnienia bezpieczeństwa w nowoczesnych zakładach przemysłowych nabierają coraz większego znaczenia, w szczególności w instalacjach o wysokim poziomie zagrożeń w sektorze petrochemicznym, przemyśle chemicznym lub energetycznym.

Obecnie widoczna staje się wyraźna tendencja do wdrażania zaawansowanych systemów bezpieczeństwa aktywujących się w chwili awarii, w szczególności służących do monitorowania procesów stwarzających potencjalne zagrożenia zarówno dla ludzi, jak i dla środowiska naturalnego. Systemy te służą do wyłączania instalacji w sytuacji zagrożenia, odcinają dopływ niebezpiecznych substancji, chłodzą lub otwierają zawory nadmiarowe ciśnienia.

Aby ograniczyć zagrożenia stwarzane przez zakład, systemy te muszą skutecznie i niazawodnie realizować swoje funkcje w chwili uszkodzenia.

W jaki jednak sposób kierownictwo zakładów i producenci urządzeń mogą zagwarantować, że wdrożone systemy działają "bezpiecznie" i spełniają konieczne wymagania? W jaki sposób oszacować ryzyko uszkodzenia?

Odpowiedzi dostarczają normy dotyczące bezpieczeństwa funkcjonalnego: PN EN IEC 61508 i PN EN IEC 61511. Po raz pierwszy opisane w nich zostały metody oceny ryzyka uszkodzeń nowoczesnych systemów (często sterowanych oprogramowaniem) oraz określania działań zmierzających do zmniejszania ryzyka.

Bezpieczeństwo funkcjonalne. Co to oznacza?

Według PN EN IEC 61508, bezpieczeństwo funkcjonalne dotyczy systemów wykorzystywanych do realizacji funkcji bezpieczeństwa, których uszkodzenie wywiera znaczący wpływ na bezpieczeństwo zarówno osób, jak i środowiska naturalnego.

W celu zapewnienia bezpieczeństwa funkcjonalnego, funkcja zabezpieczenia w sytuacji awaryjnej musi gwarantować, że stan instalacji jest utrzymywany lub zostaje przywrócony do bezpiecznego poziomu.

Bezpieczeństwo funkcjonalne nie wiąże się z podstawowymi zagrożeniami stwarzanymi przez produkt lub instalację, na przykład przez części wirujące, ale z zagrożeniami, które mogą pojawić się w zakładzie na skutek awarii funkcji bezpieczeństwa.

Głównym celem bezpieczeństwa funkcjonalnego jest zmniejszenie prawdopodobieństwa wystąpienia niebezpiecznego uszkodzenia, a w konsekwencji - ograniczenie ryzyka dla ludzi i środowiska naturalnego do akceptowalnego poziomu.

Zmniejszenie ryzyka dzięki bezpieczeństwu funkcjonalnemu

Ogólnie mówiąc, bezpieczeństwo funkcjonalne - w połączeniu z dalszymi działaniami, takimi jak ochrona ppoż, bezpieczeństwo elektryczne lub zabezpieczenia przeciwwybuchowe - znacząco przyczyniają się do ogólnego bezpieczeństwa zakładu.

Czym jest SIL?

SIL jest terminem ściśle związanym z bezpieczeństwem funkcjonalnym. SIL to skrót od Safety Integrity Level [poziom nienaruszalności bezpieczeństwa] oraz jednostka, w jakiej mierzony jest stopień zmniejszenia ryzyka przez funkcje bezpieczeństwa.

Im większe są potencjalne zagrożenia stwarzane przez procesy lub instalacje, tym ostrzejsze są wymogi niezawodności funkcji bezpieczeństwa.

PN EN IEC 61508 określa cztery różne poziomy nienaruszalności bezpieczeństwa - od SIL 1 do SIL 4.

SIL 4 oznacza najwyższy, a SIL 1 - najniższy poziom nienaruszalności bezpieczeństwa. Dla każdego poziomu określono różne wartości docelowe prawdopodobieństwa awarii, które nie mogą zostać przekroczone przez funkcje zabezpieczające.

Do wyznaczenia wymaganego poziomu SIL stosuje się ocenę ryzyka.

Rola AUMY w tym kontekście

Produkty AUMA są podzespołami instalowanymi w układach pełniących funkcje zabezpieczające. Z tego powodu, oraz we współpracy z niezależnymi jednostkami badawczymi, takimi jak EXIDA i TÜV, sprawdziliśmy, który poziom SIL ma zastosowanie do naszych napędów, sterowników i przekładni.

W oparciu o ustalone parametry bezpieczeństwa projektanci zakładów mogą dobrać odpowiednie urządzenia, spełniające określone wymogi nienaruszalności bezpieczeństwa.

Początki

Tragiczne konsekwencje takich wypadków przemysłowych jak katastrofa w Seveso w 1976 roku (dioksyna) lub w Bhopalu w Indiach w 1984 roku (gaz) spowodowały konieczność dostosowania się światowego procesu standaryzacji w dziedzinie bezpieczeństwa do nowych okoliczności.

Na poziomie UE najpierw wydano dyrektywę Seveso I, a następnie Seveso II 96/82/WE w sprawie kontroli niebezpieczeństwa poważnych awarii związanych z substancjami niebezpiecznymi. Nadrzędnym celem tych dyrektyw jest ochrona osób, środowiska naturalnego oraz majątku. Ponadto zawierają one wyraźne instrukcje dla zakładów o wysokim potencjale zagrożeń.

W celu zharmonizowania tych dyrektyw po raz pierwszy opracowano normy krajowe w sprawie bezpieczeństwa funkcjonalnego. Pierwszą międzynarodową normę wydano w 1998 roku z numerem PN EN IEC 61508.

PN EN IEC 61508

IEC 61508 jest normą międzynarodową stosowaną do pełnego cyklu żywotności związanych z bezpieczeństwem systemów elektrycznych/elektronicznych/programowalnych systemów elektronicznych (E/E/PE). Tam, gdzie była taka możliwość, wymogi stawiane przez normy zostały przetransponowane na inne, na przykład mechaniczne podzespoły.

Norma jest stosowana przez projektantów instalacji i zakłady eksploatacyjne, a także przez producentów urządzeń.

Pełni ona funkcję niezależnego, podstawowego standardu i została uzupełniona kolejnymi normami, takimi jak PN EN IEC 61511 dla sektora technologicznego.

Koncepcja zmniejszania ryzyka

Celem jest zmniejszenie ryzyk, których źródłem są procesy technologiczne oraz instalacje, poprzez zastosowanie systemów związanych z bezpieczeństwem. Ogólnie mówiąc, norma ta zakłada, że wyłączenie wszystkich potencjalnych ryzyk jest niemożliwe. Proponuje ona przy tym metody służące do analizy ryzyka, jego zmniejszenia oraz oceny ryzyka szczątkowego.

Wymagania dla systemu związanego z bezpieczeństwem

Norma opisuje wymagania dla systemów związanych z bezpieczeństwem lub dla funkcji bezpieczeństwa i definiuje poziom nienaruszalności bezpieczeństwa (poziom SIL). Na tej podstawie ustalane są odpowiednie wymogi poziomu SIL dla zastosowanych w systemie podzespołów.

Uwzględnianie cyklu żywotności

Aby zminimalizować ryzyko uszkodzeń, należy wziąć pod uwagę pełny cykl żywotności komponentów, od specyfikacji przez wdrożenie aż do wycofania z eksploatacji.

PN EN IEC 61511

Norma ta obejmuje wdrożenie PN EN IEC 61508 zależnie od użytkownika, w szczególności w procesach przemysłowych. Definiuje ona wymogi dla systemów związanych z bezpieczeństwem stosowanych w procesach przemysłowych w celu zmniejszenia ryzyka.

Norma ta dotyczy głównie projektantów i użytkowników instalacji.

Zakres norm

Normy PN EN IEC 61508 i 61511 nie są jeszcze obowiązujące na obszarze Unii Europejskiej, ponieważ wciąż nie zostały zharmonizowane w formie dyrektywy UE. Jednakże spełnienie tych wymogów przynosi znaczące korzyści zarówno pracownikom zakładów, jak i producentom urządzeń:

- W przypadku zakładów i systemów, których uszkodzenie/usterka mogłoby mieć wpływ na bezpieczeństwo osób i środowiska naturalnego, metoda bezpieczeństwa funkcjonalnego uważana jest za najbardziej nowoczesną.
- Normy mogą zostać użyte do spełnienia podstawowych wymogów dyrektyw UE, jeśli zawierają odniesienia do zharmonizowanej normy europejskiej, lub - jeśli norma zharmonizowana nie jest dostępna do konkretnego zastosowania.
- Zapewnienia zgodności z normami PN EN IEC 61508 i 61511 coraz częściej domagają się przedstawiciele władz i firmy ubezpieczeniowe jako dowodu analizy ryzyka z odpowiednim jego zmniejszeniem.
- Wykorzystując wyroby sklasyfikowane według poziomu SIL, kierownictwo zakładów i producenci urządzeń mogą być pewni, że urządzenia zostały ocenione zgodnie z normami międzynarodowymi oraz że określony poziom nienaruszalności bezpieczeństwa został zagwarantowany.

Aby osiągnąć bezpieczeństwo funkcjonalne, trzeba przede wszystkim przeanalizować ryzyka stwarzane przez system lub proces technologiczny.

Normy PN EN IEC 61508 i 61511 dostarczają uznaną metodę oceny ryzyka. W celu identyfikacji procesów prowadzących do wystąpienia rzeczywistych, niebezpiecznych zdarzeń, stosowana jest zróżnicowana ocena automatyki zabezpieczeniowej. W rezultacie skoncentrować się można na podejmowaniu działań ograniczających ryzyko tylko wtedy, kiedy jest to rzeczywiście konieczne.

Ocena automatyki zabezpieczeniowej

Identyfikacja procesów stwarzających zagrożenie

Po pierwsze, konieczne jest zbadanie procesów, które prowadzą w zakładach do wystąpienia ewentualnych zagrożeń dla osób oraz środowiska naturalnego.

Zwykle chodzi tylko o kilka takich procesów. Na przykład podstawowe procedury sterowania procesami, które nie mają funkcji istotnych dla bezpieczeństwa, nie są brane pod uwagę.

Określenie wymaganego poziomu SIL

Każdy z potencjalnie niebezpiecznych procesów jest analizowany w celu określenia generowanego przez nie zagrożenia oraz konsekwencji uszkodzenia.

Ocenę ryzyka można sobie ułatwić, stosując system graficzny podobny do przedstawionego poniżej. Zależnie od zasięgu i prawdopodobieństwa wystąpienia ryzyka określone zostanie, czy proces musi zostać zabezpieczony funkcją bezpieczeństwa oraz jaki poziom nienaruszalności bezpieczeństwa SIL musi spełniać ta konkretna funkcja.

Dobór właściwych komponentów

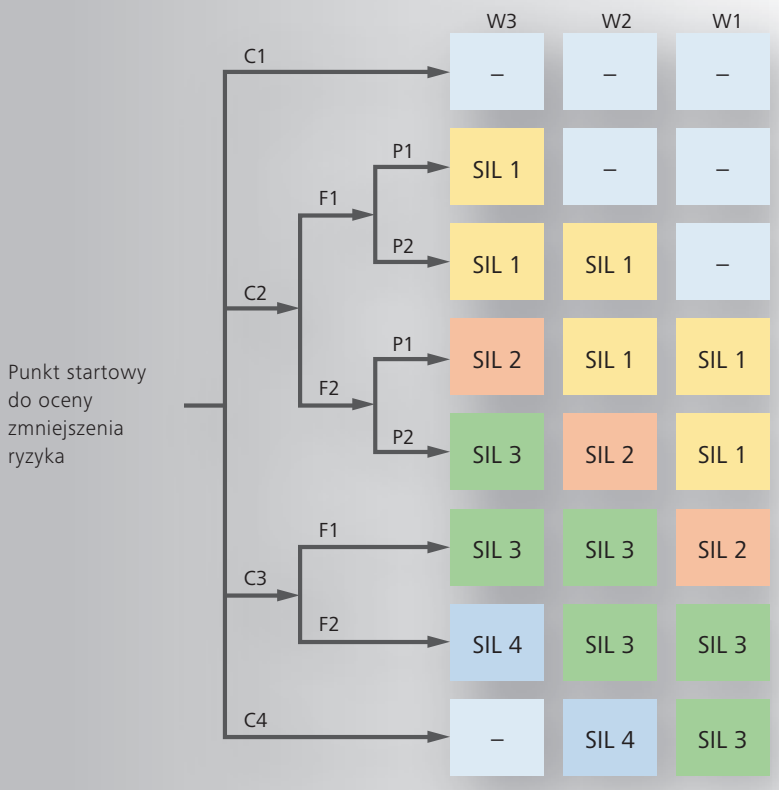
Podzespoły służące wdrożeniu funkcji bezpieczeństwa dobierane są w zależności od wymaganego poziomu SIL.

Aby uprościć tą procedurę producenci wyposażenia, tacy jak AUMA, wychodzą z inicjatywą testowania swoich urządzeń w celu ich sklasyfikowania według możliwych poziomów nienaruszalności bezpieczeństwa.

Weryfikacja wymaganego poziomu SIL

W oparciu o parametry bezpieczeństwa wdrożonych urządzeń sprawdza się, czy wymagany poziom SIL został osiągnięty w przypadku każdej z funkcji bezpieczeństwa. Jeśli tak nie jest, konieczne będzie podjęcie dodatkowych działań.

Wykres ryzyka dla oceny automatyki zabezpieczeniowej zgodnie z PN EN IEC 61508/61511



Konsekwencje

C1 Niewielkie uszkodzenia ciała lub niewielki niebezpieczny wpływ na środowisko naturalne
C2 Poważne trwałe uszkodzenia ciała lub 1 ofiara śmiertelna
C3 Kilka ofiar śmiertelnych
C4 Liczne ofiary śmiertelne

Uniknięcie zagrożenia

F1 Możliwe pod pewnymi warunkami
F2 Prawie niemożliwe

Czas narażenia osoby na niebezpieczeństwo w miejscu zagrożenia

P1 od przypadków rzadkich do częstych
P2 od przypadków częstych do stałego zagrożenia

Prawdopodobieństwo niepożądanego wystąpienia

W1 Bardzo nieznaczne
W2 Nieznaczne
W3 Względnie wysokie

Wymagany poziom nienaruszalności bezpieczeństwa

SIL 1 Wymóg najniższego poziomu bezpieczeństwa
SIL 4 Wymóg najwyższego poziomu bezpieczeństwa

Czym jest funkcja bezpieczeństwa?

Funkcje bezpieczeństwa to działania zabezpieczające inicjowane w przypadku awarii w celu uniknięcia obrażeń u osób, strat w środowisku naturalnym i majątku. Bezpieczeństwo funkcjonalne zapewnione jest wtedy, gdy funkcje bezpieczeństwa działają niezawodnie w razie awarii.

Typowe funkcje bezpieczeństwa to na przykład wyłączniki awaryjne zatrzymujące urządzenie lub monitorujące ciśnienie w zbiornikach.

W branży armatury przemysłowej zasadnicze znaczenie mają następujące funkcje:

- Bezpieczne otwarcie
- Bezpieczne zamknięcie
- Bezpieczne wyłączenie/zatrzymanie
- Sygnał zwrotny potwierdzenia bezpiecznego położenia krańcowego

Bezpieczne otwarcie na przykładzie zaworu bezpieczeństwa

W przypadku zbiorników, z którymi wiąże się potencjalne zagrożenie spowodowane nadmiernym ciśnieniem, otwarcie zaworu bezpieczeństwa traktowane jest jako funkcja bezpieczeństwa.

Czujnik stale monitoruje ciśnienie w zbiorniku. Z chwilą, gdy ciśnienie przekracza wartość nastawioną, sterownik PLC bezpieczeństwa traktuje to jako usterkę systemu i wysyła do napędu sygnał otwarcia, uwalniając ciśnienie w zbiorniku.

Bezpieczne zatrzymanie na przykładzie śluzy

IJeśli statek znajduje się pomiędzy otwartymi wrotami śluzy, funkcja bezpiecznego zatrzymania może polegać na niezawodnym zatrzymaniu procesu zamykania się wrót śluzy.

Funkcja bezpieczeństwa polegająca na bezpiecznym zatrzymaniu może również być wykorzystywana jako funkcja blokady. W takim przypadku blokada może zostać zamknięta tylko wtedy, kiedy sygnał "Bezpiecznego zatrzymania" nie jest podawany.

Podzespoły typowego przyrządowego systemu bezpieczeństwa

- Czujnik [1]
- Sterownik PLC bezpieczeństwa [2]
- Zespół [3]
  składający się z napędu i zaworu

Czym jest przyrządowy system bezpieczeństwa?

Funkcja bezpieczeństwa wdrażana jest przez zastosowanie podzespołów przyrządowego systemu bezpieczeństwa (SIS). W skład takiego systemu wchodzą zwykle: czujnik, główny sterownik PLC bezpieczeństwa i zespół wykonawczy. W branży armatury zespół wykonawczy obejmuje napęd i zawór.

Oceniając, czy pożądany poziom SIL został osiągnięty dla danej funkcji bezpieczeństwa, należy wziąć pod uwagę parametry bezpieczeństwa wszystkich poszczególnych komponentów wchodzących w skład przyrządowego systemu bezpieczeństwa (zob. również strona 12).

Podczas oceny potencjalnych zagrożeń generowanych przez proces analizowana jest każda funkcja bezpieczeństwa i określany jest wymagany poziom SIL. Niniejsze wytyczne mają pomóc w doborze odpowiednich urządzeń umożliwiających wdrożenie funkcji bezpieczeństwa.

Aby sklasyfikować urządzenie zgodnie z SIL, normy PN EN IEC 61508 i 61511 proponują zastosowanie rachunku prawdopodobieństwa.

Poniżej opisano najbardziej istotne parametry bezpieczeństwa.

Średnie prawdopodobieństwo uszkodzenia na przywołanie - (PFD)

Wartość PFD_{avg} (Średnie prawdopodobieństwo uszkodzenia na przywołanie) opisuje średnie prawdopodobieństwo niemożności zrealizowania funkcji bezpieczeństwa.

Zgodnie z PN EN IEC 61508 dozwolony zakres prawdopodobieństwa wystąpienia awarii został określony dla każdego z czterech poziomów nienaruszalności bezpieczeństwa.

SIL 1 stanowi najniższy poziom, SIL 4 – najwyższy. Im wyższy jest poziom bezpieczeństwa, tym niższe jest dopuszczalne prawdopodobieństwo awarii funkcji bezpieczeństwa w systemach pracujących na żądanie / inicjowanych/.

Poziom ryzyka nie jest jedynym decydującym czynnikiem dla systemu bezpieczeństwa w przypadku uszkodzenia/ usterki. Do istotnych czynników należy również częstotliwość spodziewanej awarii, a tym samym powiązane zapotrzebowanie na właściwe funkcje bezpieczeństwa.

PN EN IEC 61508 dzieli tryby operacyjne na wymagane/ inicjowane rzadko i często (lub dostosowane do pracy ciągłej.

Tryb pracy przy rzadkim przywołaniu

W trybie pracy przy rzadkim żądaniu /przy małej częstotliwości inicjowania/ zadziałanie funkcji bezpieczeństwa jest wymagane maksymalnie raz na rok. Zwykle taki tryb dotyczy funkcji bezpieczeństwa dla przemysłu wykorzystującego napędy.

Uwzględniane są tylko funkcje bezpieczeństwa. Napęd wykorzystywany do realizacji funkcji bezpieczeństwa, jak również do czynności "konwencjonalnego" otwierania i zamykania, może oczywiście otwierać lub zamykać zawór częściej w trakcie normalnej pracy. Przewidywany błąd/ usterka systemu wymagającego bezpiecznego zamknięcia zaworu nie może jednak występować częściej niż raz na rok.

Tryb pracy przy częstym (lub ciągłym) przywołaniu

W trybie pracy przy częstym (lub ciągłym) przywołaniu / przy dużej częstotliwości inicjowania/, funkcja bezpieczeństwa albo pracuje ciągle, albo na żądanie /jest inicjowana/ częściej niż raz do roku.

Podstawowym parametrem obliczeniowym bezpieczeństwa w tym trybie pracy jest prawdopodobieństwo wystąpienia awarii na godzinę, oznaczane jako wartość PFH.

Docelowe wartości PFD w trybie pracy przy rzadkim żądaniu

Poziom nienaruszalności bezpieczeństwa	Pomiar dopuszczalnego PFD_{avg} (rzadkie żądanie)	Teoretycznie dopuszczalne usterki dla funkcji bezpieczeństwa w trybie żądania
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	Jedno dopuszczalne niebezpieczne uszkodzenie na 10 lat
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	Jedno dopuszczalne niebezpieczne uszkodzenie na 100 lat
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	Jedno dopuszczalne niebezpieczne uszkodzenie na 1000 lat
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	Jedno dopuszczalne niebezpieczne uszkodzenie na 10 000 lat

W pierwszym etapie wartości PFD są obliczane dla każdego podzespołu systemu automatyki zabezpieczeniowej.

Poziom nienaruszalności bezpieczeństwa opisuje natomiast właściwości pełnej funkcji bezpieczeństwa, a nie jej pojedynczego elementu. Z tego powodu całkowita wartość PFD dla funkcji bezpieczeństwa musi zostać wyliczona na podstawie wartości PFD poszczególnych komponentów.

Intensywność uszkodzeń λ

Istotne znaczenie dla bezpieczeństwa systemu ma analiza możliwych źródeł uszkodzeń/usterek.

Mówiąc o intensywności uszkodzeń λ wprowadzamy rozróżnienie na uszkodzenia sklasyfikowane jako niebezpieczne, i jako bezpieczne, i w konsekwencji niewywierające wpływu na prawidłową realizację funkcji bezpieczeństwa. Ponadto, badane jest pokrycie diagnostyczne uszkodzenia.

Udział uszkodzeń bezpiecznych (SFF)

Wartość SFF (Safe Failure Fraction - udział uszkodzeń bezpiecznych) oznacza procentowy odsetek bezpiecznych uszkodzeń w ogólnej liczbie awarii. Uszkodzenia uważane są za bezpieczne, jeśli ich skutki nie są niebezpieczne dla systemu.

Im wyższa jest ta wartość, tym niższe jest prawdopodobieństwo niebezpiecznego uszkodzenia systemu. Wartość 62% oznacza, że 62 ze 100 uszkodzeń/usterek nie ma wpływu na bezpieczne funkcjonowanie systemu.

Odporność na defekty sprzętu (HFT)

HFT (Hardware Fault Tolerance - odporność na defekty sprzętu) to zdolność urządzenia funkcjonalnego do dalszego realizowania wymaganej funkcji bezpieczeństwa pomimo wystąpienia błędów lub odchyłek.

Tolerancja usterek sprzętu N oznacza, że wystąpienie usterki N + 1 może spowodować utratę funkcji bezpieczeństwa. Na przykład w przypadku odporności na defekty sprzętu wynoszącej 0, jeden błąd może spowodować uszkodzenie funkcji bezpieczeństwa.

W zasadzie HFT można zwiększyć, tworząc rezerwową architekturę systemu (zob. również strona 13).

Typ urządzenia

PN EN IEC 61508 wprowadza rozróżnienie pomiędzy prostymi i złożonymi urządzeniami.

Proste urządzenia typu A

Urządzenia typu A to "proste" jednostki, w przypadku których zachowanie awaryjne wszystkich komponentów jest w pełni znane. Obejmują one np. przekaźniki, rezystory i tranzystory, ale nie obejmują żadnych złożonych podzespołów elektronicznych, takich jak na przykład mikrokontrolery.

Złożone urządzenia typu B

Urządzenia typu B to "złożone" jednostki zawierające podzespoły elektroniczne, takie jak mikrokontroler, mikroprocesory i dedykowane układy scalone ASIC. W przypadku tych podzespołów, a w szczególności funkcji sterowanych oprogramowaniem, przewidywanie wszystkich usterek jest bardzo trudne.

Im bardziej skomplikowane urządzenie, tym wyższe wymagania

Poniższe tabele przedstawiają ostrzejsze wymagania mające zastosowanie do urządzeń typu B w stosunku do urządzeń typu A.

SFF i HFT dla urządzeń typu A

SFF (Udział uszkodzeń "bezpiecznych")	HFT (Odporność na defekty)		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % to < 90 %	SIL 2	SIL 3	SIL 4
90 % to < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

SFF i HFT dla urządzeń typu B

SFF (Udział uszkodzeń "bezpiecznych")	HFT (Odporność na defekty)		
	0	1	2
< 60 %	not allowed	SIL 1	SIL 2
60 % to < 90 %	SIL 1	SIL 2	SIL 3
90 % to < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Średni czas pomiędzy awariami (MTBF)

Średni czas eksploatacji pomiędzy awariami w latach oznacza teoretyczny czas eksploatacji pomiędzy dwoma następującymi po sobie uszkodzeniami i pozwala na wiarygodne ujęcie ilościowe. W żadnym wypadku nie należy mylić tego parametru z cyklem żywotności lub użytecznym cyklem żywotności systemu.

Poziom nienaruszalności bezpieczeństwa dotyczy zawsze kompletnej funkcji bezpieczeństwa. Tym samym traktowanie wartości PFD pod kątem pojedynczych podzespołów jest niewystarczające.

Zdolność SIL funkcji bezpieczeństwa

Aby określić zdolność SIL funkcji bezpieczeństwa, należy dodać wartości PFD poszczególnych układów. Otrzymana w ten sposób wartość PFD jest następnie porównywana z dozwolonym całkowitym prawdopodobieństwem wystąpienia niebezpiecznego uszkodzenia w systemach pracujących na żądanie dla wymaganego poziomu SIL.

Wartość mniejsza wskazuje, że nawet jeśli stosowane są tylko podzespoły sklasyfikowane jako SIL 2, nie gwarantuje to, że funkcja bezpieczeństwa jako całości również będzie na poziomie SIL 2. Poziom ten zostaje osiągnięty tylko wtedy, gdy całkowita wartość PFD wszystkich podzespołów mieści się w docelowym zakresie SIL 2.

Określanie zdolności SIL

Obliczanie całkowitej wartości SIL funkcji bezpieczeństwa - PFD

Wartość PFD czujnika PFD = 3.63 x 10^{-3} = SIL 2	+	**Wartość PFD sterownika PLC** PFD = 1.84 x 10^{-3} = SIL 2	+	**Wartość PFD napędu** PFD = 2.28 x 10^{-3} = SIL 2	+	**Wartość PFD armatury** PFD = 2.92 x 10^{-3} = SIL 2	=	**Całkowita wartość PFD funkcji bezp.** PFD = 1.07 x 10^{-2} = SIL 1

Jeśli obliczenia wykażą, że wybrane komponenty sprzętowe nie spełniają wymaganego poziomu SIL, to zdolność SIL można zwiększyć, podejmując dodatkowe działania, takie jak diagnozowanie i zapewnianie rezerw.

Test częściowego skoku zaworu (PVST)

Test częściowego skoku zaworu jest wykonywany w celu regularnej kontroli funkcji urządzenia. Napęd lub zawór pokonują wcześniej zdefiniowaną odległość - docelowo i z powrotem. W ten sposób sprawdza się, czy napęd rzeczywiście działa.

Test PVST jest uznaną metodą zwiększania dostępności poszczególnych komponentów funkcji bezpieczeństwa. Ten umożliwiający przewidywanie test pozwala wykluczyć błędy związane z bezpieczeństwem; prawdopodobieństwo wystąpienia niebezpiecznej awarii w systemach pracujących na żądanie zostaje zredukowane.

Test sprawdzający

Test ten służy do całościowej kontroli systemu. Jeśli czas pomiędzy wykonaniem dwóch takich testów zostaje skrócony na przykład z dwóch lat do jednego roku, zdolność SIL może zostać zwiększona, a ukryte uszkodzenia - wykryte.

Redundancja

W celu zwiększenia prawdopodobieństwa, że funkcja bezpieczeństwa zadziała w sytuacji awaryjnej, wykorzystywana jest redundantna architektura systemu. Dwa lub więcej urządzeń systemu związanego z bezpieczeństwem może pracować z uwzględnieniem trybu rezerwowego.

Zależnie od wymogu bezpieczeństwa, sprawdzają się różne konfiguracje MooN ("M z N"). Na przykład w przypadku konfiguracji 1oo2 ("jedno z dwóch"), jedno z dwóch urządzeń jest wystarczające do realizowania wymaganej funkcji bezpieczeństwa. Konfiguracja 2oo3 ("dwa z trzech") oznacza, że dwa z trzech urządzeń muszą funkcjonować prawidłowo. Rzeczywista architektura systemu zależy od wymaganej funkcji bezpieczeństwa. Bezpieczne otwarcie i bezpieczne zamknięcie zostały określone poniżej, w cyfrach.

Architektura systemu redundantnego może zwiększać tolerancję defektów sprzętu, a w konsekwencji - zdolność SIL.

W przypadku zastosowań na poziomie SIL 3, zgodnie z PN EN IEC 61511, redundancja stanowi wymóg konieczny.

Zwiększanie zdolności SIL

[1] **System redundantny dla bezpiecznego otwarcia**

[2] **System redundantny dla bezpiecznego zamknięcia**

Spodziewamy się reakcji ze strony naszych klientów. Dla projektantów i kierowników zakładów istotne znaczenie ma wdrożenie właściwych podzespołów dla danych wymogów bezpieczeństwa. Stosując złożoną procedurę, określiliśmy parametry bezpieczeństwa i - w rezultacie - zdolności SIL napędów, sterowników napędów i przekładni AUMA tak, aby w optymalnym zakresie wspierać naszych klientów w doborze podzespołów.

Alokowane funkcje bezpieczeństwa

Parametry bezpieczeństwa, a tym samym zdolność SIL, zależą od funkcji bezpieczeństwa realizowanej przez urządzenie w przypadku sytuacji awaryjnej w celu osiągnięcia bezpiecznego stanu systemu.

Funkcją kluczową napędów jest otwieranie i zamykanie zaworów. Wskutek tego AUMA kładzie największy nacisk na takie funkcje bezpieczeństwa napędów, jak bezpieczne otwarcie i bezpieczne zamknięcie.

Bezpieczne otwarcie/bezpieczne zamknięcie

Na żądanie funkcji bezpieczeństwa napęd porusza się w kierunku pozycji krańcowej OTWARCIA lub pozycji krańcowej ZAMKNIĘCIA.

Bezpieczne otwarcie/bezpieczne zamknięcie z testem częściowego skoku zaworu (PVST)

Test częściowego skoku zaworu przeprowadzany jest w regularnych odstępach czasu jako dodatkowa kontrola funkcji napędu, i tym samym zwiększa prawdopodobieństwo przewidzenia awarii. Prowadzi to do poprawy parametrów bezpieczeństwa.

Bezpieczne wyłączenie/ bezpieczne zatrzymanie

Na żądanie funkcji bezpieczeństwa silnik napędu zostaje zatrzymany. Zapobiega to niepożądanym uruchomieniom silnika.

Sygnał zwrotny potwierdzenia bezpiecznego położenia końcowego

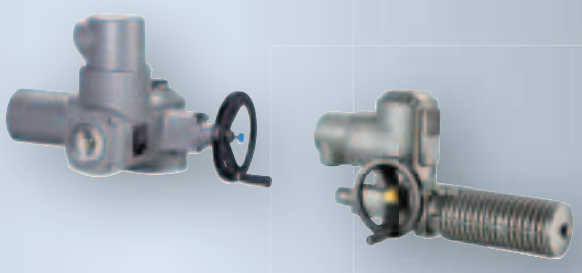
Elektromechaniczna jednostka sterująca wysyła sygnał bezpieczny w chwili, gdy pozycja krańcowa OTWARCIA lub ZAMKNIĘCIA lub moment obrotowy zostają osiągnięte. Zgodnie z normą nie jest to uważane za funkcję bezpieczeństwa. Jednakże w praktycznych zastosowaniach korzystne okazało się podanie parametrów bezpieczeństwa dla tej funkcji.

Przegląd wszystkich ocenionych wyrobów AUMA zamieściliśmy na stronie 23.
Szczegółowe dane dot. bezpieczeństwa wybranych napędów podajemy na stronie 25.

Napędy AUMA bez sterowników

W przypadku tych wersji funkcje kontrolne muszą być dostarczone przez klienta.

Przeprowadzono ocenę napędów SA. 1, SA. 2 i SG. 1, a także wersji do pracy regulacyjnej i ochrony przeciwwybuchowej. Napędy są sklasyfikowane jako urządzenia typu A. Zdolność SIL zależy od napędów i funkcji bezpieczeństwa. Na przykład napędy SA. 2 zostały sklasyfikowane na poziomie SIL 2 dla wszystkich funkcji bezpieczeństwa. Poziom SIL 3 można osiągnąć dzięki zastosowaniu architektury redundantnej.

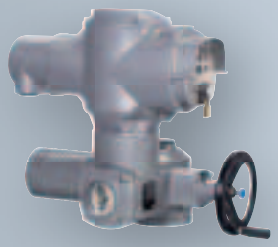


Napędy AUMA ze sterownikami AM

AM jako "proste" sterowniki z okablowaniem dyskretnym i bez złożonych podzespołów elektrycznych sklasyfikowane są jako urządzenia typu A. Przeprowadzono ocenę napędów SA. 1, SA. 2 i SG. 1. Zdolność SIL zależy od funkcji bezpieczeństwa i wersji schematu okablowania.

Badane wersje napędów SA .2 z wbudowanymi sterownikami AM zostały sklasyfikowane na poziomie SIL 2. Poziom SIL 3 można osiągnąć dzięki zastosowaniu architektury systemu redundantnego.

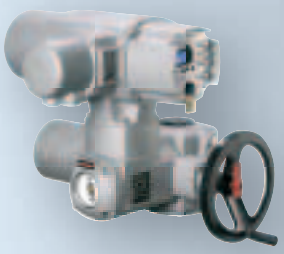
Funkcje bezpieczeństwa - bezpiecznego otwarcia/bezpiecznego zamknięcia - mogą być realizowane albo standardowymi wejściami dla otwierania i zamykania, albo przez odrębne wejście EMERGENCY.



Napędy AUMA ze sterownikami AC .1

Zintegrowane sterowniki AC .1 wraz z ich nowoczesną elektroniką oraz złożonymi podzespołami elektrycznymi zostały sklasyfikowane jako urządzenia typu B i podlegają ostrzejszym wymaganiom normy. Przeprowadzono ocenę napędów SA.1 i SG .1. Badane wersje napędów ze zintegrowanymi sterownikami AC .1 zostały sklasyfikowane na poziomie SIL 1.

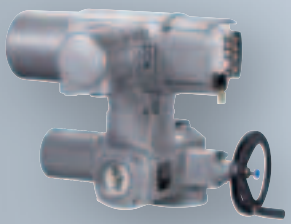
AC .1 również realizują funkcje bezp. otwarcia/ bezp. zamknięcia albo przez wejście standardowe, albo przez oddzielne wejście EMERGENCY. Np. kontrola normalnej pracy poprzez magistralę Field Bus może być realizowana standard. sygn. Field Bus, podczas gdy funkcja bezpieczeństwa jest realizowana bezpośrednio wejściem EMERGENCY.



Napędy AUMA ze sterownikami AC .2 w wersji SIL

Nowoczesne sterowniki do zastosowań SIL 2 zostały udostępnione ze zintegrowanymi sterownikami AC .2 w wersji SIL. Zabudowanie systemu redundantnego pozwala na zaklasyfikowanie na poziomie SIL 3.

Dalsze szczegóły dotyczące AC .2 w wersji SIL podajemy na kolejnych stronach.



Przekładnie AUMA

Wartości dot. bezpieczeństwa zostały określone również dla przekładni GS i GF AUMA. Przekładnie te zostały zaklasyfikowane na poziomie SIL 2.

Nasi klienci z pewnością docenią różnorodność funkcji oraz opcji nastaw zintegrowanych sterowników AC .2. Swobodnie konfigurowalne interfejsy równoległe i typu fieldbus umożliwiają ich wbudowanie w najbardziej wyrafinowane, rozproszone systemy sterowania. Sterowniki AC .2 są idealnym rozwiązaniem dla złożonych funkcji kontrolnych. Dodatkowe funkcje diagnostyczne gwarantują zwiększone bezpieczeństwo i niezawodność napędu. Obejmują one na przykład zapis danych operacyjnych w formie raportów zdarzeń z oznaczeniem czasu ich wystąpienia, ciągły rejestr temperatur i drgań wewnątrz napędu, a także monitorowanie parametrów cyklu życia.

AUMA opracowała specjalny moduł SIL do AC .2 w celu wykorzystania tych funkcji w zastosowaniach SIL 2 i SIL 3.

Moduł SIL

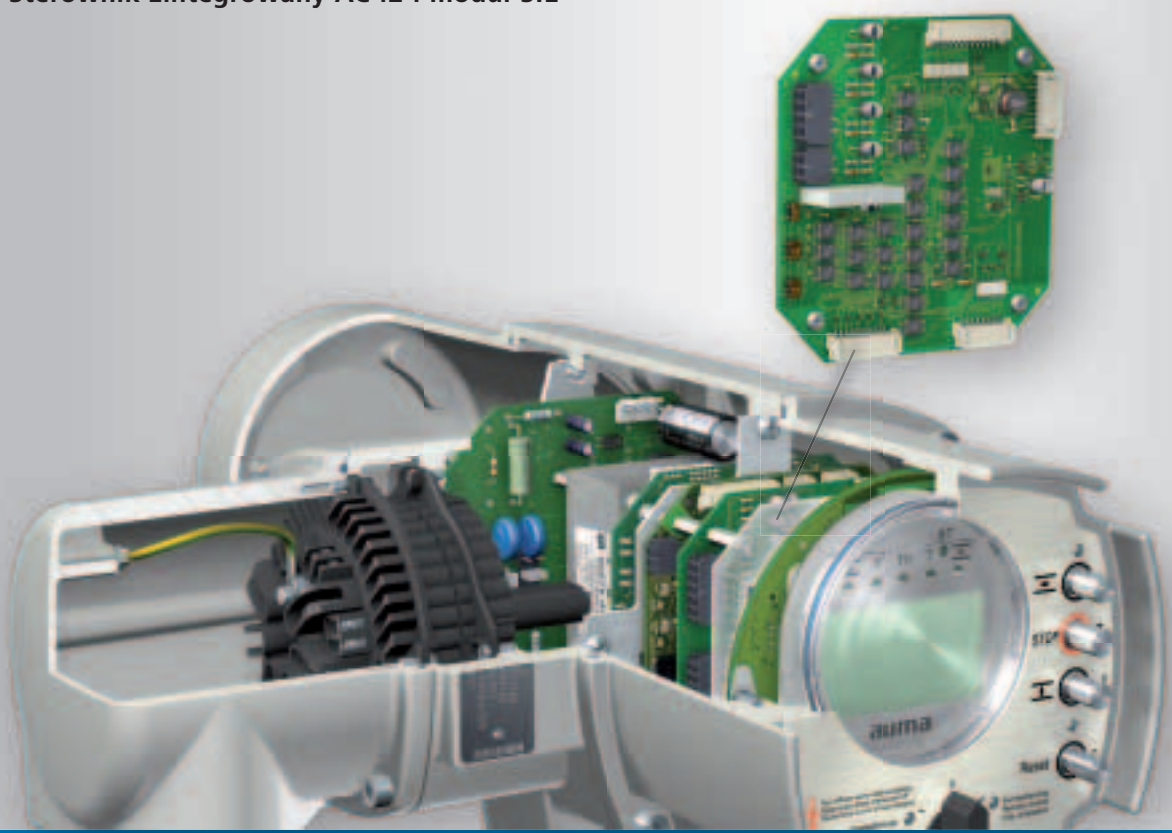
Moduł SIL składa się z dodatkowej płytki elektronicznej, odpowiedzialnej za realizację funkcji bezpieczeństwa. Płytka ta jest zabudowana w sterownikach AC .2 i ACEx .2.

Jeśli funkcja bezpieczeństwa zostaje wywołana w sytuacji awaryjnej, to standardowa logika AC .2 zostaje pominięta i funkcja bezpieczeństwa realizowana jest przez moduł SIL.

Moduły SIL skonstruowane są ze stosunkowo prostych podzespołów, takich jak tranzystory, oporniki i kondensatory, których wskaźniki awaryjności są w pełni znane. Tym samym AC .2 w wersji SIL jest klasyfikowany jako urządzenie typu A. Określone wartości bezpieczeństwa pozwalają na ich wdrożenie w zastosowaniach SIL 2 a nawet SIL 3 (pod warunkiem dostępności redundantnej architektury systemu - 1oo2).

SIL 2/SIL 3 dla zintegrowanych sterowników AC .2 w wersji SIL

Sterownik zintegrowany AC .2 i moduł SIL



Funkcja bezpieczeństwa priorytetem!

Układy wyposażone w AC .2 w wersji SIL łączą w sobie funkcje dwóch sterowników. Z jednej strony standardowe funkcje AC .2 mogą być wykorzystywane w "normalnej eksploatacji". Z drugiej strony wbudowany moduł SIL pełni funkcje bezpieczeństwa, zawsze nadrzędne w stosunku do zwykłej pracy. Jest to możliwe, ponieważ standardowa logika sterowania jest omijana z chwilą, gdy wywoływana jest funkcja bezpieczeństwa.

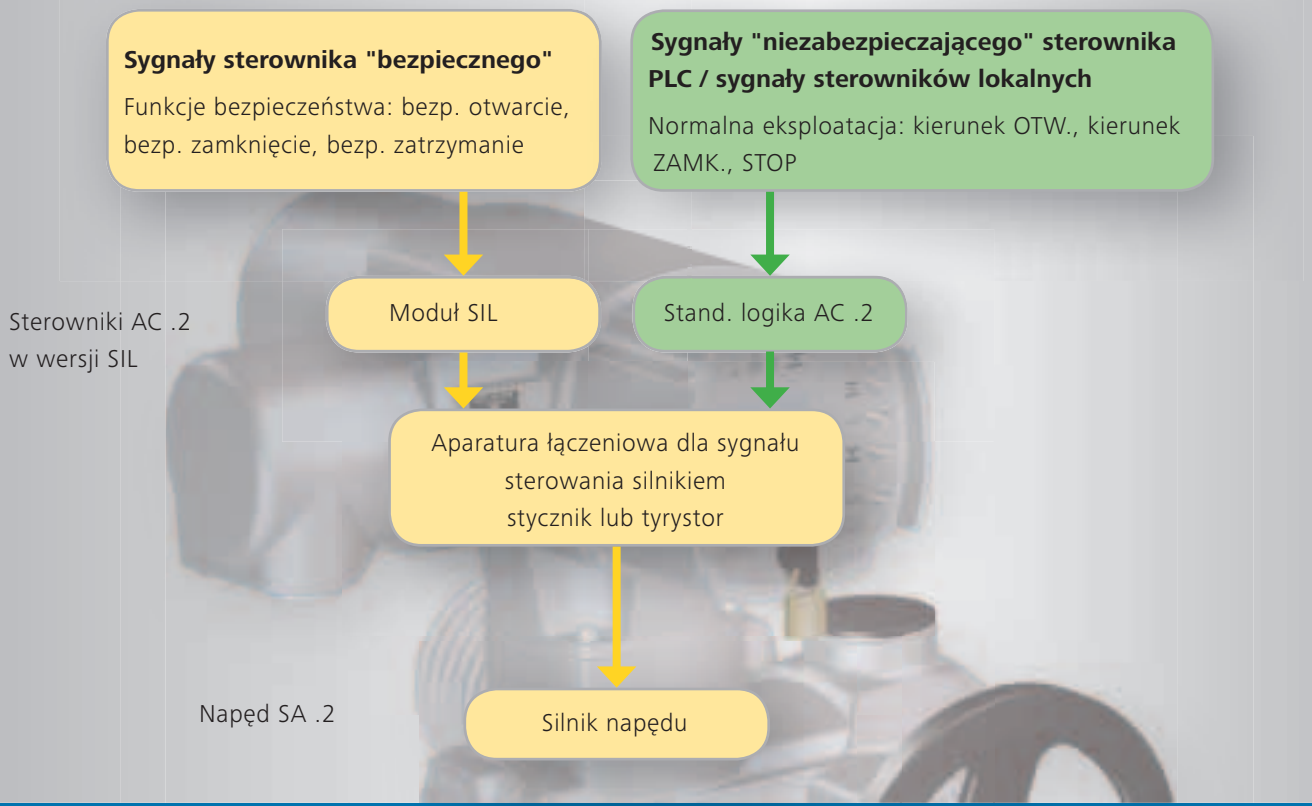
Poniższy rysunek przedstawia typową architekturę systemu z AC .2 w wersji SIL. AC .2 jest sterowany przez dwa główne sterowniki (PLC), "bezpieczny", sklasyfikowany wg SIL sterownik PLC oraz drugi, niezabezpieczający PLC.

Normalna praca realizowana jest poleceniami wydawanymi przez "niezabezpieczający" PLC, przetwarzanymi w standardowym układzie logicznym AC .2.

W sytuacji awaryjnej następuje przerwanie zwykłej pracy, a napędy sterowane są sygnałami przesyłanymi z bezpiecznego sterownika PLC przez wbudowany moduł SIL.

Jeśli napęd z AC .2 w wersji SIL wykorzystywany jest wyłącznie jako system bezpieczeństwa, to kontrola za pośrednictwem "niezabezpieczającego" PLC jest zbędna.

Przetwarzanie sygnałów dla zintegrowanego sterownika AC .2 w wersji SIL



Opcje konfiguracji

AC .2 w wersji SIL oferują wiele opcji konfiguracji. Wszystkie ustawienia dostosowane do potrzeb indywidualnego klienta przeprowadzone są u producenta: Jaka funkcja bezpieczeństwa musi być realizowana? W którym punkcie przerwać ruch? Ustawienia te są wprowadzane z przycisków DIP modułu SIL.

Funkcje bezpieczeństwa

Zastosowanie AC .2 w wersji SIL umożliwia realizację następujących funkcji bezpieczeństwa:

- Bezpieczne otwarcie/ zamknięcie
  (Bezpieczne ESD - awaryjne wyłączenie)
  Napęd działa w skonfigurowanych kierunkach OTWÓRZ lub ZAMKNIJ. Redundantne wejście sygnału zapewnia dodatkowe zabezpieczenie.

- Bezpieczne zatrzymanie
  W przypadku tej funkcji bezpieczeństwa polecenie pracy wysyłane przez niezabezpieczający PLC w kierunku OTWÓRZ lub ZAMKNIJ realizowane jest tylko wtedy, gdy wysyłany jest dodatkowy sygnał aktywujący z modułu SIL.
  Jeżeli tak nie jest, to praca w kierunku OTWÓRZ lub ZAMKNIJ jest zatrzymana, a nawet zawieszona.

- Bezpieczne otwarcie / bezpieczne zamknięcie w połączeniu z bezpiecznym zatrzymaniem.
  W takim przypadku funkcja bezpiecznego otwarcia / bezpiecznego zamknięcia ma pierwszeństwo.

Dodatkowo możliwe jest potwierdzenie osiągnięcia bezpiecznego położenia końcowego przez napęd.

Kryteria wyłączania napędu w pozycjach krańcowych

Podobnie jak w przypadku normalnej eksploatacji, dla funkcji bezpieczeństwa można zdefiniować kryteria wyłączania napędu. Podczas gdy kryteria wyłączania napędu służą ochronie zarówno zaworu, jak i napędu w normalnej eksploatacji, inicjowanie funkcji bezpieczeństwa może wymusić otwarcie lub zamknięcie zaworu niezależnie od uszkodzeń zaworu lub napędu.

Ogólnie mówiąc, dla funkcji bezpieczeństwa dostępne są następujące kryteria wyłączania:

- Wyłączenie przez wyłącznik krańcowy
  W chwili osiągnięcia wcześniej nastawionych punktów wyłączania w pozycjach końcowych OTWARCIA lub ZAMKNIĘCIA, sterownik automatycznie wyłącza napęd. Jeśli podczas przesterowania przyłożony zostaje zbyt duży moment obrotowy, np. z powodu zablokowania ciała obcego w zaworze, napęd jest wyłączany w celu ochrony zaworu, zanim osiągnie on położenie krańcowe.

- Wyłączenie w położeniu krańcowym
  Napęd zatrzymuje się tylko wtedy, gdy osiągnięte zostają krańcowe pozycje OTWARCIA lub ZAMKNIĘCIA, niezależnie od przyłożonego momentu obrotowego.

- Wyłączenie przez wyłącznik momentu obrotowego w położeniu krańcowym
  Napęd zatrzymuje się tylko wtedy, gdy osiągnięty zostaje wcześniej nastawiony moment dla pozycji krańcowej, niezależnie od pokonanej drogi.

- Brak wyłączenia napędu
  W tym przypadku wyłączniki momentu obrotowego i wyłączniki krańcowe są omijane, aby wymusić otwarcie lub zamknięcie zaworu. Aby uniknąć przepalenia silnika, zalecamy zastosowanie systemu AC .2 w wersji SIL z funkcją ochrony termicznej.

Monitorowanie pracy napędu

W celu zbadania niezawodności systemu prowadzony jest elektromechaniczny monitoring pracy napędu przez moduł SIL. Jeżeli napęd nie uruchamia się w zdefiniowanym pierwotnie czasie po wydaniu polecenia zadziałania, moduł SIL wysyła zbiorczy sygnał błędu SIL.

Ten bieżący monitoring działa również podczas zwykłej pracy.

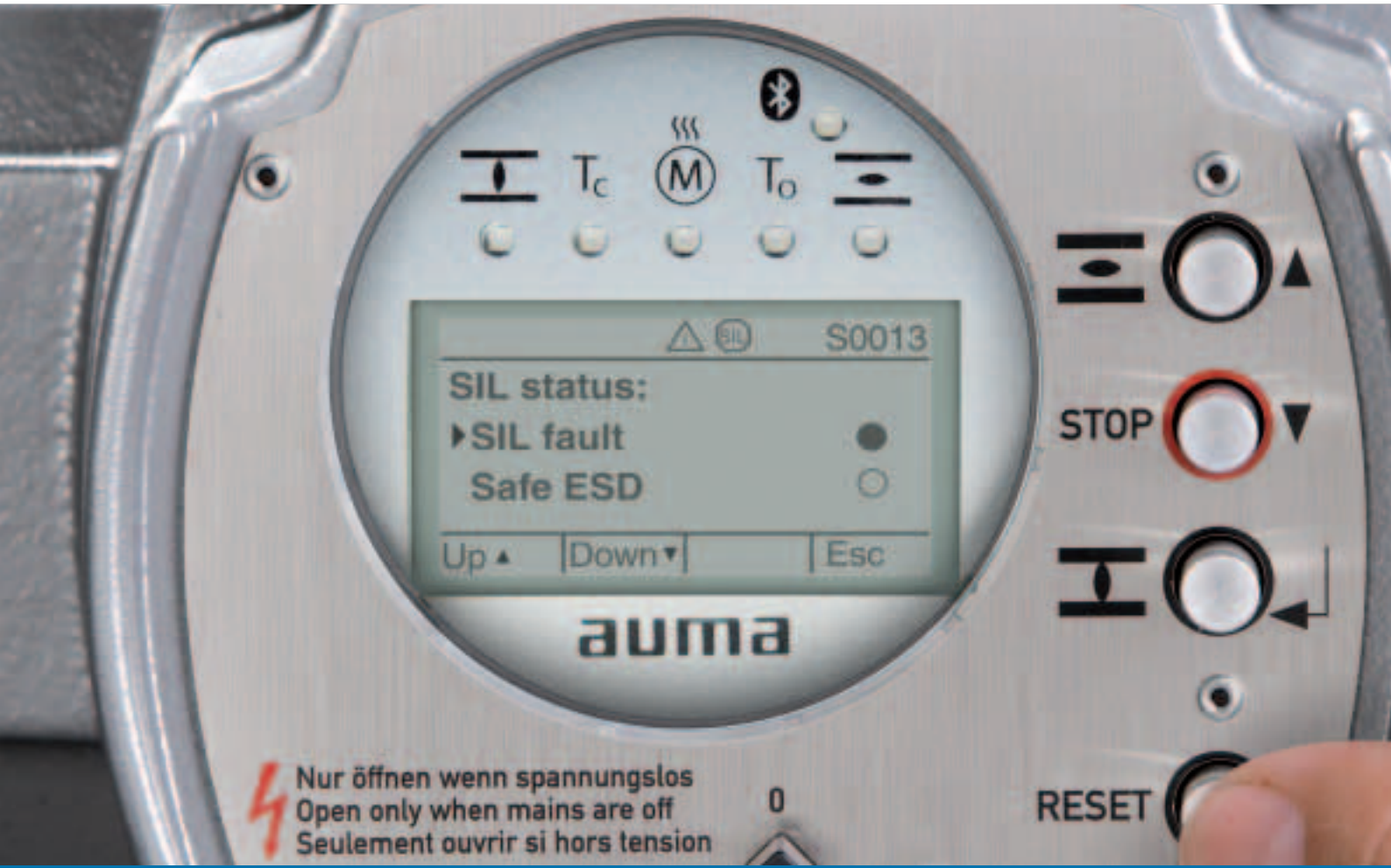
Bezpieczne wejścia i wyjścia

Moduł SIL posiada trzy bezpieczne wejścia i dwa bezpieczne wyjścia:

- 1 wejście redundantne bezpiecznego otwarcia/bezpiecznego zamknięcia
  (można je skonfigurować jako wejście otwarcia lub jako wejście zamknięcia)
- 1 wejście dla bezpiecznego zatrzymania lub zwolnienia w kierunku OTWARCIA
- 1 wejście dla bezpiecznego zatrzymania lub zwolnienia w kierunku ZAMKNIĘCIA
- 1 wyjście na zbiorczy sygnał błędu SIL
- 1 wyjście na sygnał "system gotowy"

Wyświetlacz

Wszelkie informacje o statusie modułu SIL, takie jak realizowanie funkcji bezpieczeństwa lub obecność zbiorczego sygnału błędu SIL, sygnalizowane są za pomocą symboli lub komunikatów na wyświetlaczu AC .2.



Określono parametry bezpieczeństwa, umożliwiając pewne i wiarygodne stwierdzenie zdolności SIL urządzeń produkowanych przez AUMA.

Normy PN EN IEC 61508 i 61511 sugerują dwie, częściowo różne procedury: Ocenę wyposażenia oraz ocenę całościową.

AUMA przystąpiła do oceny wyposażenia w oparciu o już wykonane urządzenia. Należą do nich napędy SA i SG, sterowniki AM i AC .1 oraz przekładnie GS i GF.

Natomiast zintegrowane sterowniki AC .2 w wersji SIL zostały ocenione całościowo. Ocena dotyczy nie tylko błędów przypadkowych, ale też błędów systematycznych na wszystkich etapach cyklu życia produktu, od specyfikacji produktu do momentu wycofania z eksploatacji.

Urządzenia już wprowadzone do obrotu

W celu przeprowadzenia oceny już wykonanych podzespołów normy PN EN IEC 61508 i 61511 przewidują deklaracje przydatności do użytku na podstawie oceny wyposażenia.

Parametry bezpieczeństwa określone są dla różnych składników wykorzystywanych do przeprowadzenia klasyfikacji SIL.

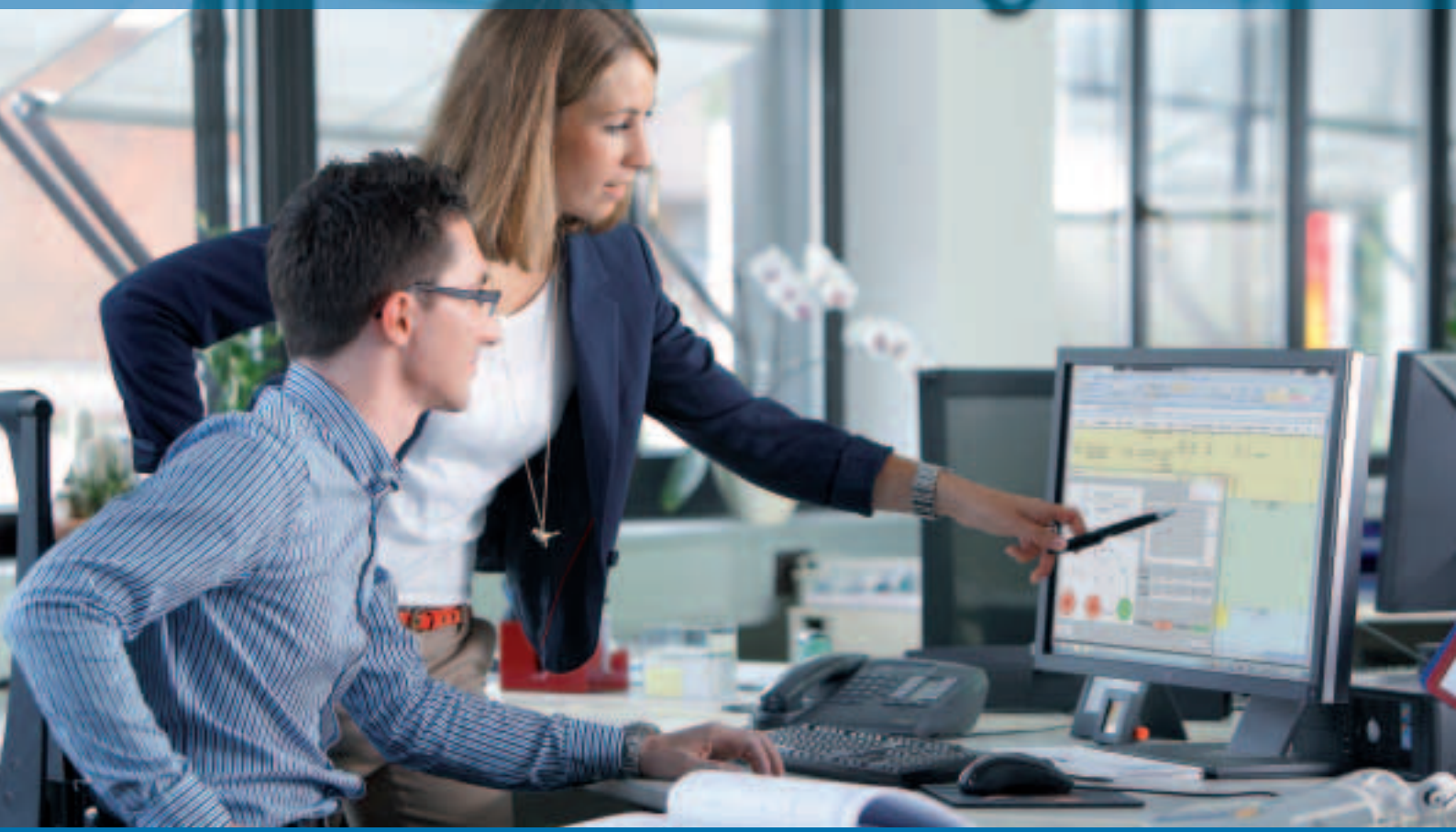
Podstawą do oceny wyposażenia sterowników AUMA są dane rodzajowe: do napędów AUMA wykorzystuje się dane zebrane drogą doświadczeń.

Dane ogólne dot. sterowników AUMA

Zbiory danych ogólnych są statystycznie określonymi wskaźnikami awaryjności poszczególnych podzespołów, wymienionymi w specjalnych bazach danych, zwanych "rejestrami danych niezawodności". Do przykładów należą standard SN 29500 SIEMENSA lub podręcznik EXIDA.

Parametry bezpieczeństwa podzespołów elektronicznych używanych w produktach AUMA zostały określone na podstawie podręcznika EXIDA.

Określenie wart. parametrów bezpieczeństwa produktów AUMA



Dane zebrane drogą doświadczeń dla napędów AUMA

W przypadku komponentów mechanicznych dostępnych jest niewiele danych ogólnych. Dane z doświadczenia, na przykład informacje dot. błędów, otrzymane w okresie gwarancyjnym oraz wyniki badań zostały wykorzystane przy wyciąganiu wniosków co do niezawodności przedmiotowych komponentów.

Do określenia parametrów bezpieczeństwa napędów AUMA wykorzystano dane zebrane w ciągu ostatnich 10-ciu lat.

FMEDA

Według normy PN EN IEC 61508, FMEDA (analiza przyczyn, skutków i diagnostyki usterki) jest uznaną metodą obliczania parametrów bezpieczeństwa.

Analiza ta prowadzona jest w ściśle określonych krokach, rejestrowanych i przejrzystych na każdym etapie.

Za pomocą FMEDA analizuje się scenariusze błędów i prawdopodobieństwo ich wystąpienia. Ponadto sprawdza się, czy potencjalne błędy są niebezpieczne dla funkcji bezpieczeństwa oraz czy mogą one zostać zdiagnozowane - a tym samym zidentyfikowane.

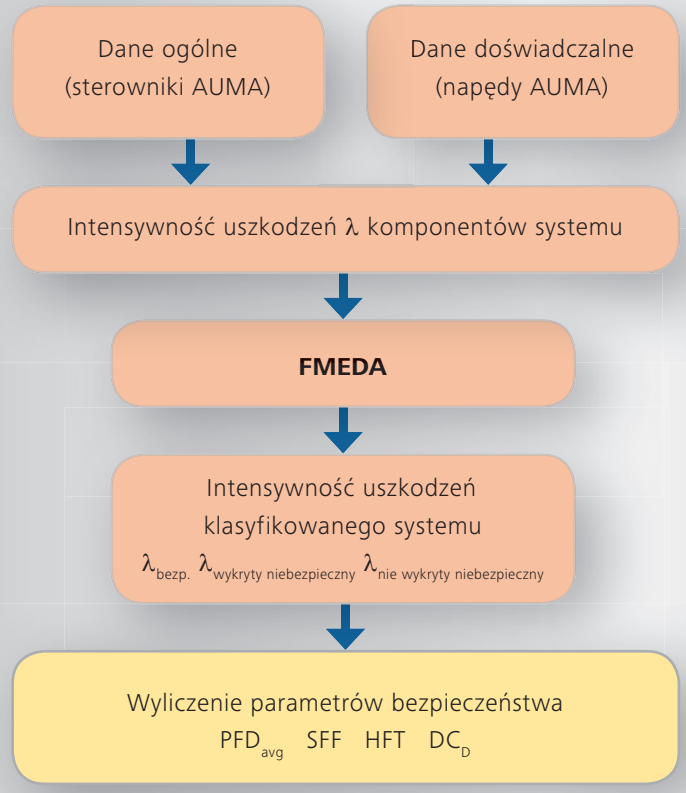
Otrzymane wskaźniki awaryjności wykorzystywane są do obliczania przeciętnego prawdopodobieństwa wystąpienia awarii w systemach pracujących na żądanie (PFD_{avg}), a także dalszych parametrów bezpieczeństwa, takich jak odsetek uszkodzeń bezpiecznych (SFF) oraz pokrycia diagnostycznego (DC_D).

Raporty i certyfikaty EXIDA

Parametry bezpieczeństwa wyrobów AUMA zostały określone we współpracy z EXIDA, najważniejszą międzynarodową jednostką certyfikującą w tym sektorze. Wyniki ocen zostały przedstawione w formie raportów EXIDA.

Tabela na stronie 23 zawiera wykaz wszystkich ocenionych pod kątem bezpieczeństwa oprzyrządowania produktów AUMA.

Procedura określania parametrów bezpieczeństwa



Ogólna ocena nowo zaprojektowanych produktów

Zintegrowany sterownik AC .2 w wersji SIL jest rozwiązaniem poddanym całościowej ocenie zgodności z PN EN IEC 61508. Oceniony został cały układ składający się z napędu SA .2 oraz sterowników AC .2 w wersji SIL. Procedurę certyfikacji przeprowadziło TÜV Nord [niemiecki organ certyfikacyjny].

Co przetestowano?

W porównaniu do oceny już wykonanych wyrobów, ogólna ocena obejmuje testy i certyfikację procedur projektowania i produkcji, których celem jest uniknięcie błędów systematycznych tam, gdzie jest to możliwe.

Wykres poniżej obrazuje podstawową zasadę przeprowadzania ogólnej oceny zgodnie z PN EN IEC 61508. Uwzględnione są zarówno systematyczne, jak i przypadkowe awarie/usterki produktu.

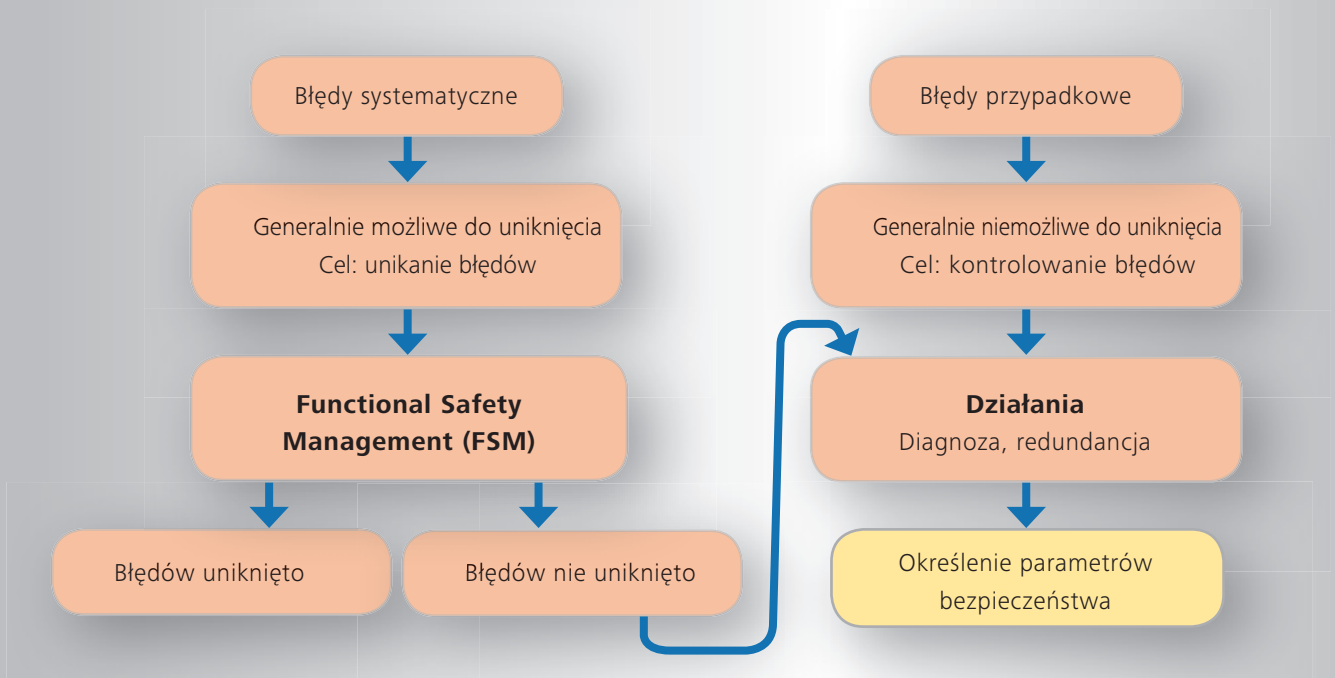
Błędy systematyczne

Zasadniczo, błędów systematycznych można uniknąć, ponieważ są to zwykle błędy powstałe na etapie projektowania lub produkcji. Dzięki systemowi zarządzania bezpieczeństwem funkcjonalnym wyszukiwane są możliwe źródła błędów i podejmowane są odpowiednie działania mające na celu uniknięcie błędów systematycznych.

System zarządzania bezpieczeństwem funkcjonalnym

System zarządzania bezpieczeństwem funkcjonalnym [Functional Safety Management - FSM] może być traktowany jako rozszerzenie systemu zarządzania jakością. Opisane w nim zasady i definicje pozwalają wyeliminować znaczną część źródeł błędów systematycznych.

Podstawowa zasada całościowej oceny



Błędy przypadkowe

Błędy przypadkowe są skutkiem na przykład zakłóceń zewnętrznych, i są uznawane zasadniczo jako niemożliwe do uniknięcia. Zatem zachodzi potrzeba wdrożenia metod kontrolowania tych błędów, na ile to możliwe.

Do działań dodatkowych zaliczyć możemy np. dodatkowe monitorowanie systemu oraz diagnostykę systemu, jak również architekturę redundantną.

Określenie parametrów bezpieczeństwa

Pomimo podjęcia wszelkich działań mających na celu zmniejszenie ryzyka, liczbę błędów szczątkowych należy rejestrować pod kątem oceny ryzyka szczątkowego. W tym celu określa się i przedstawia klientom takie parametry bezpieczeństwa produktów, jak prawdopodobieństwo wystąpienia awarii.

W AUMIE procedura ta jest taka sama, jak dla oceny wyposażenia (zob. strona 21).

Napędy i sterowniki AUMA z oceną SIL

Na żądanie, AUMA dostarcza raporty z testów wszystkich ocenionych napędów i sterowników wyposażonych w systemy automatyki zabezpieczeniowej. Ponadto dostępne są podsumowania dla różnych konfiguracji produktu.

Zob. przykładowe dane na str. 25.

Napęd	Sterownik	Funkcja bezpieczeństwa	Raport z testów
SA/SAR 07.1 – 16.1 SAExC/SARExC 07.1 – 16.1 SG 05.1 – 12.1 SGExC 05.1 – 12.1	bez zintegrowanego sterownika	Bezpieczne otwarcie/ zamknięcie Bezpieczne otwarcie/ zamknięcie PVST Bezpieczne wyłączenie/zatrzymanie	Raport EXIDA nr AUMA 0707-32 R003
		Potwierdzenie bezpiecznego położenia końcowego	Raport EXIDA nr AUMA 10-12-035 R005
SA/SAR 07.2 – 16.2 SAEx/SAREx 07.2 – 16.2	bez zintegrowanego sterownika	Bezpieczne otwarcie/ zamknięcie Bezpieczne otwarcie/ zamknięcie PVST Bezpieczne wyłączenie/zatrzymanie	Raport EXIDA nr AUMA 10-03-053 R006
		Potwierdzenie bezpiecznego położenia końcowego	Raport EXIDA nr AUMA 10-12-035 R005
SA/SAR 07.1 – 16.1 SAExC/SARExC 07.1 – 16.1 SG 05.1 – 12.1 SGExC 05.1 – 12.1 SA/SAR 07.2 – 16.2 SAEx/SAREx 07.2 – 16.2	AM 01.1/02.1 AMExC 01.1 AMExB 01.1	Bezpieczne otwarcie/ zamknięcie Bezpieczne otwarcie/ zamknięcie PVST Bezpieczne wyłączenie/zatrzymanie	Raport EXIDA nr AUMA 0707-32 R003
		Potwierdzenie bezpiecznego położenia końcowego	Raport EXIDA nr AUMA 10-12-035 R005
SA/SAR 07.1 – 16.1 SAExC/SARExC 07.1 – 16.1 SG 05.1 – 12.1 SGExC 05.1 – 12.1	AC 01.1 ACExC 01.1	Bezpieczne otwarcie/ zamknięcie Bezpieczne otwarcie/ zamknięcie PVST Bezpieczne wyłączenie/zatrzymanie	Raport EXIDA nr AUMA 07/07-32 R004
		Potwierdzenie bezpiecznego położenia krańcowego	Raport EXIDA nr AUMA 10-12-035 R005
SA/SAR 07.2 – 16.2 SAEx/SAREx 07.2 – 16.2	AC 01.2 w wersji SIL ACEx 01.2 w wersji SIL	Bezpieczne otwarcie/ zamknięcie Bezpieczne otwarcie/ zamknięcie PVST Bezpieczne zatrzymanie	
		Potwierdzenie bezpiecznego położenia krańcowego	Raport EXIDA nr AUMA 10-12-035 R005

Przekładnie AUMA z oceną SIL

Dostępne są również raporty z testów przekładni produkowanych przez firmę AUMA. Parametry bezpieczeństwa przekładni są niezależne od funkcji bezpieczeństwa.

Przekładnie	Raport z testów
GS 50.3 – 250.3, GS 315 – 500 GF 50.3 – GF 250.3	Raport EXIDA nr AUMA 12/02-079 R007

Parametry bezpieczeństwa wybranych produktów AUMA

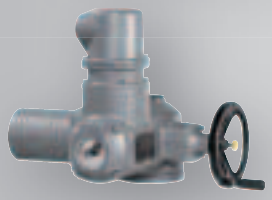
Poniżej podajemy podsumowanie parametrów bezpieczeństwa wybranych napędów i ich sterowników. Parametry te zależą od funkcji bezpieczeństwa, ponieważ definicje warunków bezpiecznych mogą się różnić, a tym samym wymagane jest rozważenie różnych środków bezpieczeństwa.

W przypadku napędów ze zintegrowanymi sterownikami parametry bezpieczeństwa zależą również od wersji schematu okablowania, z uwagi na fakt, że stosowane są w nich różne elementy o różniących się wskaźnikach awaryjności. Łącznie, określono parametry bezpieczeństwa dla około 150 różnych wersji.

Jeśli potrzebne są dalsze szczegóły, prosimy o kontakt.

Napędy wieloobrotowe SA/SAR 07.2 - SA/SAR 16.2 i SAEx/SAREx 07.2 - SAEx/SAREx 16.2 bez zintegrowanych sterowników

SA .2



SAEx .2

Raport Exida	AUMA 10-03-052 R006 wersja V1	AUMA 10-03-052 R006 wersja V2
Funkcja bezpieczeństwa	Bezpieczne otwarcie/bezpieczne zamknięcie	Bezpieczne otwarcie/bezpieczne zamknięcie z PVST[1)]
$\lambda_{bezpieczny}$	367 FIT	367 FIT
λ_{DD}	0 FIT	162 FIT
λ_{DU}	203 FIT	41 FIT
DC_D	0 %	80 %
MTBF	200 lat	200 lat
SFF	64 %	92 %
$T_{[proof]}$ = 1 rok	$PFD_{avg} = 1.05 \times 10^{-3}$	$PFD_{avg} = 4.96 \times 10^{-4}$
$T_{[proof]}$ = 2 lata	$PFD_{avg} = 1.92 \times 10^{-3}$	$PFD_{avg} = 6.55 \times 10^{-4}$
$T_{[proof]}$ = 5 lat	$PFD_{avg} = 4.53 \times 10^{-3}$	$PFD_{avg} = 1.13 \times 10^{-3}$
Zdolność SIL[2)]	SIL 2[3)]	SIL 2[3)]

Napędy wieloobrotowe SAEx/SAREx 07.2 - SAEx/SAREx 16.2 ze zintegrowanymi sterownikami AMExC 01.1

Przykładowe dane podano w oparciu o następujący schemat: MSP E310KC3–FF8EC TPA00R2AB-1E1-000. Ocena błędu realizowana jest przez styk K9 zbiorczego sygnału awarii.

SAEx .2 z AMExC .1

Raport Exida	AUMA 07/07-32 R003 wersja V53	AUMA 07/07-32 R003 wersja V54
Safety function	Bezpieczne otwarcie/bezpieczne zamknięcie	Bezpieczne otwarcie/bezpieczne zamknięcie z PVST[1)]
$\lambda_{bezpieczny}$	808 FIT	802 FIT
λ_{DD}	367 FIT	849 FIT
λ_{DU}	647 FIT	48 FIT
DC_D	36 %	95 %
MTBF	62 lata	66 lata
SFF	64 %	97 %
$T_{[proof]}$ = 1 rok	$PFD_{avg} = 2.82 \times 10^{-3}$	$PFD_{avg} = 3.65 \times 10^{-4}$
$T_{[proof]}$ = 2 lata	$PFD_{avg} = 5.64 \times 10^{-3}$	$PFD_{avg} = 6.27 \times 10^{-4}$
$T_{[proof]}$ = 5 lat	$PFD_{avg} = 1.40 \times 10^{-2}$	$PFD_{avg} = 1.31 \times 10^{-3}$
Zdolność SIL[2)]	SIL 2[3)]	SIL 2[3)]

1 Test częściowego skoku zaworu należy wykonać 10x częściej niż wynosi oczekiwane żądanie skoku.
2 Zdolność SIL oznacza, że obliczone wartości leżą w zakresie właściwym dla odnośnego SIL, co jednak nie oznacza, że są spełnione wszystkie stosowne wymagania normy PN EN IEC 61508.
3 Poziom SIL 3 można osiągnąć dzięki redundantnej architekturze systemu (1oo2).

Legenda

Wartość	Objaśnienie
$\lambda_{bezpieczny}$	**Lambda safe – intensywność wykrytych uszkodzeń bezpiecznych w jednostce czasu** λ określa awaryjność, tj. liczbę awarii układu w jednostce czasu. Awaryjność jest wymagana do obliczenia prawdopodobieństwa wystąpienia awarii w systemach pracujących na żądanie. Awaria jednostki w czasie [Failure In Time (FIT)] wskazuje liczbę awarii, do których doszło w ciągu 10^9 godzin: 1 FIT oznacza jedną awarię na 10^9 godzin lub jedną awarię na 114,000 lat. Awaria traktowana jest jako bezpieczna lub nie stanowiąca zagrożenia pod warunkiem, że jej wystąpienie nie powoduje niebezpiecznego stanu układu.
λ_{DD}	**Lambda Dangerous Detected – intensywność wykrytych uszkodzeń niebezpiecznych w jednostce czasu** Wskazuje liczbę wykrytych, niebezpiecznych awarii w ciągu 10^9 godzin na podstawie testów diagnostycznych. Uszkodzenie komponentu klasyfikowane jest jako niebezpieczne, jeśli uniemożliwia realizację funkcji bezpieczeństwa.
λ_{DU}	**Lambda Dangerous Undetected – intensywność wykrytych uszkodzeń niebezpiecznych w jednostce czasu** Wskazuje liczbę niewykrytych niebezpiecznych awarii w ciągu 10^9 godzin.
DC_D	**Pokrycie diagnostyczne niebezpiecznych awarii** Intensywność wykrytych uszkodzeń niebezpiecznych λ_{DD} wykrytych w testach diagnostycznych, związana z całkowitą liczbą wykrytych awarii niebezpiecznych, wyrażonych w procentach.
MTBF	**Średni czas pomiędzy awariami** Opisuje czas pracy pomiędzy dwoma następującymi po sobie awariami podzespołów. Samo wskazanie MTBF odnosi się do niezawodności urządzenia.

Wartość	Objaśnienie
SFF	Udział **uszkodzeń bezpiecznych SFF** Opisuje procentowy udział bezpiecznych uszkodzeń/usterek, które nie mogą spowodować awarii systemu. Im wyższa jest ta wartość, tym niższe jest prawdopodobieństwo niebezpiecznego uszkodzenia systemu. Wartość 62% oznacza, że 62 uszkodzenia/usterki ze 100 w ramach systemu są nie-krytyczne z perspektywy funkcji bezpieczeństwa.
T_{proof}	**Częstotliwość testów sprawdzających** Wartości parametrów bezpieczeństwa zachowują ważność przez określony czas pracy. Zatem w celu przywrócenia zaprojektowanej funkcjonalności urządzenia bezwzględnie konieczny jest test sprawdzający. Wartość PFD można zwiększyć skracając czas pomiędzy dwoma testami sprawdzającymi. Jednak odstęp czasowy nieprzekraczający jednego roku jest pozbawiony sensu.
PFD_{avg}	**Prawdopodobieństwo uszkodzenia na przywołanie.** Średnie prawdopodobieństwo wystąpienia awarii niebezpiecznej „w trybie pracy na żądanie" funkcji bezpieczeństwa.
Zdolność SIL	Alokacja odpowiedniego poziomu nienaruszalności bezpieczeństwa za pomocą dostępnej wartości PFD_{avg} danego komponentu. Podstawą jest przedział czasowy T_{proof} wynoszący jeden rok. W celu określenia poziomu SIL dla całego systemu automatyki zabezpieczeniowej SIS, należy dodać wszystkie wartości PFD wszystkich elementów składowych (patrz również strona 12).

Dodatkowe informacje

Celem tej broszury jest wprowadzenie do zagadnień bezpieczeństwa funkcjonalnego. Jeśli potrzebują Państwo dalszych informacji na ten temat, odsyłamy do następujących pozycji:

- Standard Norma PN EN IEC 61508 część 1 – 7
- Standard Norma PN EN IEC 61511 część 1 – 3
- Specialna publikacja "Funktionale Sicherheit" ["Bezpieczeństwo funkcjonalne"] autorstwa Josef Börcsök
- atp edition - wydanie 1-2/2011

Indeks

B

Bezpieczeństwo funkcjonalne
- Definicje 4
- Normy 6

Błąd systematyczny 22
Błędy
- przypadkowe 23
- systematyczne 22

C

Całkowita wartość PFD 12
Częstotliwość testów sprawdzających 25

D

Dane ogólne 20
Dane zebrane drogą doświadczenia 21

E

EXIDA 20, 21

F

Funkcja bezpieczeństwa 4, 8, 14, 18
FMEDA 21

H

HFT 11

M

Moduł SIL 16, 18
MTBF 11, 25

N

Napędy niepełnoobrotowe 14, 15, 23
Napędy wieloobrotowe 14, 15, 23
Normy
- PN EN IEC 61508 4, 6
- PN EN IEC 61511 4, 6

O

Ocena automatyki zabezpieczeniowej 7
Ocena ryzyka 7
Odporność na defekty sprzętu 11
Określenie 20, 21, 22

P

Parametry bezpieczeństwa
- Produkty AUMA 23, 24
- Definicje 10

Pokrycie diagnostyczne (DC) 25
Poziom nienaruszalności bezpieczeństwa 5
Prawdopodobieństwo wystąpienia awarii na godzinę 10
Prawdopodobieństwo uszkodzenia na przywołanie 10, 25
Przekładnie 15, 23
Przyrządowy system bezpieczeństwa 9
PVST 13

R

Redundancja 13
Rodzaje pracy 10

S

Safe Failure Fraction (SFF) 11, 25
Sterowniki zintegrowane 15, 23
SFF 11, 25
SIL 5, 10
System związany z bezpieczeństwem 6

Ś

Średni czas pomiędzy awariami 11, 25
Średnie prawdopodobieństwo uszkodzenia na przywołanie 10, 25

T

Test skoku częściowego zaworu 13
Test sprawdzający 13, 25
Tolerancja defektów sprzętu 11
Tryb ciągły 10
Tryb pracy na częste przywołanie 10
Tryb pracy na rzadkie przywołanie 10
Typ urządzenia 11

U

Udział uszkodzeń bezpiecznych (SFF) 11, 25
Urządzenie typu A 11
Urządzenie typu B 11
Uszkodzenia przypadkowe 23

W

Wartości lambda λ 25
Wartość PFD 10, 25
Wartość PFH 10
Wskaźniki awaryjności 11, 25
Wykres ryzyka 7

Z

Zdolność SIL
- Produkty AUMA 14, 15, 23, 25
- Określenie 12
- Doskonalenie 13

auma®

Solutions for a world in motion

[1] Napędy wieloobrotowe
SA 07.2 – SA 16.2
SA 25.1 – SA 40.1
Moment obrotowy od 10 do 32,000 Nm
Prędkość obrotowa od 4 do 180 min^{-1}

[2] Napędy wieloobrotowe SA/SAR
ze sterownikiem AUMATIC
Moment obrotowy od 10 do 1,000 Nm
Prędkość obrotowa od 4 do 180 min^{-1}

[3] Napędy liniowe SA/LE
Połączenie napędu wieloobrotowego SA i przekładni liniowej LE
Siła od
4 kN do 217 kN
Wysuw do 500 mm
Prędkość posuwu
od 20 do 360 mm/min

[4] Napędy niepełnoobrotowe
SG 05.1 – SG 12.1
Moment obrotowy od 100 do 1,200 Nm
Czas przesterowania dla 90° od 4 do 180 s

[5] Napędy niepełnoobrotowe SA/GS
Połączenie napędu wieloobrotowego SA i przekładni ślimakowej GS
Moment obrotowy do 675,000 Nm

[6] Przekładnie kątowe
GK 10.2 – GK 40.2
Moment obrotowy do 16,000 Nm

[7] Przekładnie walcowo-czołowe
GST 10.1 – GST 40.1
Moment obrotowy do 16,000 Nm

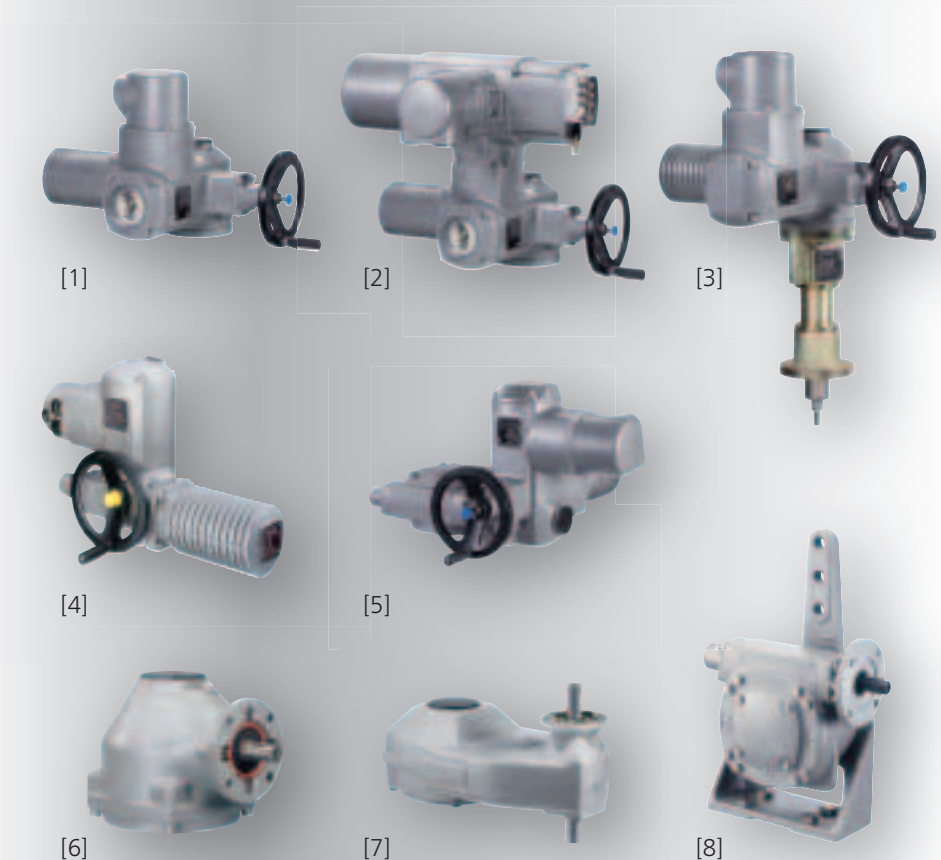
[8] Przekładnie ślimakowa z dźwignią
GF 50.3 – GF 250.3
Moment obrotowy do 45,000 Nm

AUMA Riester GmbH & Co. KG

Postfach 1362
D-79379 Muellheim/Germany
Tel +49 7631-809-0
Fax +49 7631-809-1250
riester@auma.com

AUMA Polska Sp. z o.o.

ul. Komuny Paryskiej 1 d
41-219 Sosnowiec/Polska
Tel +48 783-52-00
Fax +48 783-52-08
biuro@auma.com.pl



ISO 14001 TÜV SÜD ISO 9001
Nr rejestracyjny certyfikatu
12 100/104 4269

Y004.602/045/pl/1.12