PODRĘCZNIK BEZPIECZEŃSTWA MASZYN 5

Allen-Bradley

Guardmaster®

Systemy sterowania związane z bezpieczeństwem maszyn

Zasady, normy i wdrożenie

(Podręcznik bezpieczeństwa – wersja 5)

LISTEN. THINK. SOLVE.℠

Rockwell Automation

Systemy sterowania związane z bezpieczeństwem maszyn

Spis treści

Rozdział 1 **Przepisy** **2**
Dyrektywy i prawodawstwo Unii Europejskiej, dyrektywa maszynowa, dyrektywa narzędziowa, przepisy USA, Urząd ds. Bezpieczeństwa i Zdrowia w Pracy, przepisy kanadyjskie

Rozdział 2 **Normy** **18**
ISO (International Organisation for Standardisation), IEC (International Electrotechnical Commission), zharmonizowane normy europejskie EN, normy USA, normy OSHA, normy ANSI, normy kanadyjskie, normy australijskie

Rozdział 3 **Strategia bezpieczeństwa** **22**
Ocena ryzyka, określanie limitów maszyny, identyfikacja zadań i zagrożeń, szacowanie i ograniczanie ryzyka, projektowanie maszyn wewnętrznie bezpiecznych, systemy i środki ochronne, weryfikacja, szkolenie, sprzęt ochrony osobistej, normy

Rozdział 4 **Realizacja środków ochronnych** **34**
Zabezpieczenie przed nieoczekiwanym uruchomieniem, blokowanie i oznakowanie (LOTO), ochronne systemy odłączające, uniemożliwienie dostępu, stałe osłony zamykające, wykrywanie dostępu oraz technologie i systemy bezpieczeństwa

Rozdział 5 **Obliczanie bezpiecznej odległości** **56**
Wzory, wytyczne i aplikacje rozwiązań bezpieczeństwa wykorzystujące obliczanie bezpiecznej odległości do bezpiecznego sterowania elementami ruchomymi stwarzającymi zagrożenie.

Rozdział 6 **Systemy sterowania związane z bezpieczeństwem i bezpieczeństwo funkcjonalne** **60**
Informacje ogólne co to jest bezpieczeństwo funkcjonalne? Normy IEC/EN 62061 i EN ISO 13849-1:2008, SIL i IEC/EN 62061, PL i EN ISO 13849-1:2008, porównanie PL i SIL

Rozdział 7 **Projektowanie systemu wg EN ISO 13849** **66**
Narzędzie SISTEMA, architektury (struktury) systemów bezpieczeństwa, czas misji, średni czas do defektu niebezpiecznego ($MTTF_D$), pokrycie diagnostyki (DC), wspólna przyczyna defektów (CCF), błędy systematyczne, poziom zapewnienia bezpieczeństwa (PL), rodzaje podsystemów i ich łączenie, walidacja, oddawanie maszyny do użytkowania, wykluczanie defektów

Rozdział 8 **Projektowanie systemu wg IEC/EN 62061** **87**
Projektowanie podsystemów wg IEC/EN 62061, wpływ interwału testów sprawdzających, wpływ analizy defektów wywołanych wspólną przyczyną, metodologia porównania z kategoriami, ograniczenia architektury, współczynniki B10 i B10d, defekty wywołane wspólną przyczyną (CCF), pokrycie diagnostyki (DC), tolerancja defektów sprzętowych, zarządzanie bezpieczeństwem funkcjonalnym, prawdopodobieństwo defektu niebezpiecznego (PFH_D), interwał testów sprawdzających, udział defektów bezpiecznych (SFF), błędy systematyczne

Rozdział 9 **Systemy sterowania związane z bezpieczeństwem, uwagi dodatkowe** **98**
Przegląd, kategorie systemów sterowania, niewykryte błędy, parametry elementów i systemów, analiza przyczyn defektu, wykluczenia defektów, kategorie zatrzymania zgodnie z normami IEC/EN 60204-1 i NFPA 79, wymagania systemów sterowania bezpieczeństwem, normy dot. robotów: USA i Kanada

Rozdział 10 **Przykłady rozwiązań** **110**
Przykład zastosowania kalkulatora poziomu zapewnienia bezpieczeństwa SISTEMA z biblioteką produktów SISTEMA firmy Rockwell Automation.

Rozdział 11 **Produkty, narzędzia i usługi** **138**
Produkty, technologie, narzędzia i usługi dostarczane przez firmę Rockwell Automation.

Allen-Bradley

Rozdział 1: Przepisy

Dyrektywy i prawodawstwo Unii Europejskiej

Rozdział zawiera zbiór wskazówek dla osób zainteresowanych bezpieczeństwem maszyn, zwłaszcza systemami ochronnymi i zabezpieczającymi obowiązującymi w Unii Europejskiej. Jest przeznaczony dla projektantów i użytkowników urządzeń przemysłowych.

W celu propagowania koncepcji otwartego rynku w Europejskim Obszarze Gospodarczym (EOG) – w którego skład wchodzą wszystkie kraje członkowskie Unii Europejskiej oraz trzy inne państwa – wszystkie kraje członkowskie są zobowiązane do wprowadzenia przepisów prawnych określających zasadnicze wymagania bezpieczeństwa dla maszyn oraz ich użytkowania.

Maszyny, które nie spełniają tych wymagań, nie mogą być sprzedawane na terenie EOG.

Jest kilka dyrektyw europejskich dotyczących bezpieczeństwa maszyn i urządzeń przemysłowych, ale dwie mające najbardziej bezpośredni związek z tym zagadnieniem to:

1 Dyrektywa maszynowa

2 Dyrektywa dotycząca stosowania sprzętu roboczego

Te dwie dyrektywy są ze sobą bezpośrednio związane, ponieważ zasadnicze wymagania bezpieczeństwa i ochrony zdrowia z dyrektywy maszynowej, mogą być zastosowane do weryfikacji bezpieczeństwa wyposażenia roboczego z dyrektywy narzędziowej.

W tym rozdziale omówiono aspekty obu dyrektyw. Zaleca się, aby z zawartymi tutaj wymaganiami zapoznała się każda osoba związana z projektowaniem, dostawą, zakupem lub użytkowaniem sprzętu przemysłowego na obszarze lub poza obszarem EOG, a także w innych krajach europejskich. Jeśli dostawcy lub użytkownicy maszyn nie będą postępować zgodnie z postanowieniami omawianych dyrektyw, większość z nich po prostu nie uzyska zezwolenia na dostarczanie lub obsługę maszyn.

Istnieją również inne dyrektywy europejskie, które mogą dotyczyć maszyn. Większość z nich skupia się wyłącznie na swoich własnych obszarach zastosowań, dlatego też znajdują się poza naszą tematyką. Warto jednak zauważyć, że tam gdzie to konieczne, należy postępować również zgodnie ze ich wymaganiami. Przykłady to: Dyrektywa o kompatybilności elektromagnetycznej (EMC) 2014/30/WE i dyrektywa ATEX 2014/34/UE.

Dyrektywa maszynowa

Dyrektywa maszynowa dotyczy dostarczania nowych maszyn oraz innego sprzętu, takiego jak elementy systemów bezpieczeństwa. Dostarczanie maszyn niezgodnych z postanowieniami i wymogami dyrektywy na terenie UE jest przestępstwem.

Najszersza definicja „maszyny" stosowana w ramach dyrektywy ma brzmienie: zespół części lub podzespołów, wyposażony w mechanizm napędowy inny niż bezpośrednio wykorzystujący siłę mięśni ludzkich lub zwierzęcych, którego przynajmniej jedna część jest ruchoma, połączonych w całość mającą konkretne zastosowanie.

Oznakowanie CE umieszczone na maszynie

Aktualna dyrektywa maszynowa (2006/42/EC) zastąpiła poprzednią wersję (98/37/EC) pod koniec 2009 roku. Precyzuje ją i uzupełnia, ale nie wprowadza żadnych radykalnych zmian w zasadniczych wymaganiach BHP. Wprowadza pewne zmiany, uwzględniający rozwój technologii i metodologii. Rozszerza swój zakres o dodatkowe typy sprzętu (np. dźwigi budowlane). Istnieje obecnie wyraźny wymóg oceny ryzyka w celu ustalenia, które wymagania ochrony zdrowia i bezpieczeństwa są odpowiednie i zostały również wprowadzone zmiany w procedurach oceny zgodności sprzętu z załącznika IV.
Szczegółowe informacje i wskazówki dotyczące definicji i wszystkich innych aspektów dyrektywy maszynowej można znaleźć na oficjalnej stronie internetowej UE:

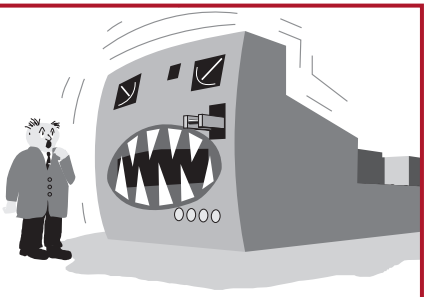
http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm

Podstawowe postanowienia poprzedniej dyrektywy (98/37/EC) w zakresie maszyn zostały wprowadzone 1 stycznia 1995 roku, a dla elementów bezpieczeństwa – 1 stycznia 1997 roku.

Postanowienia obecnej dyrektywy (2006/42/EC) zaczęły obowiązywać 29 grudnia 2009 roku. Producent lub jego autoryzowany przedstawiciel odpowiadają za to, aby dostarczany sprzęt spełniał wymagania dyrektywy. Obejmuje to:

- Zapewnienie zastosowania odpowiednich środków ochrony zdrowia i bezpieczeństwa wyszczególnionych w załączniku I dyrektywy
- Przygotowanie dokumentacji technicznej
- Przeprowadzenie odpowiedniej oceny zgodności
- Udostępnienie „Deklaracji zgodności EC"
- Dołączenie oznaczenia CE, tam gdzie jest ono wymagane
- Zapewnienie instrukcji umożliwiających bezpieczne użytkowanie

Zasadnicze wymagania ochrony zdrowia i bezpieczeństwa (BHP)



Maszyna musi spełniać wymagania BHP

Załącznik 1 dyrektywy zawiera listę zasadniczych wymagań BHP, z którymi – tam gdzie to konieczne – muszą być zgodne maszyny. Wymagania te opracowano z myślą o projektowaniu i konstruowaniu bezpiecznych maszyn. Postępowanie zgodne z wymaganiami pozwala na użytkowanie, regulację i konserwację maszyn przez cały cykl życia, bez narażania bezpieczeństwa i zdrowia osób. Następujący tekst zawiera krótki przegląd niektórych typowych wymagań, ale ważne jest, aby stosować się do wszystkich wymagań BHP podanych w Załączniku 1. W celu ustalenia, które wymagania BHP obowiązują w przypadku określonego urządzenia, należy przeprowadzić ocenę ryzyka.

Wymogi BHP w załączniku 1 podają w sposób hierarchiczny środki służące eliminacji ryzyka:

(1) Projektowanie maszyn wewnętrznie bezpiecznych. Tam gdzie jest to możliwe, sam projekt zapobiegnie pewnym zagrożeniom. Tam gdzie nie jest to możliwe, należy wykorzystać **(2) dodatkowe urządzenia ochronne**, np. osłony z punktami dostępu wyposażonymi w blokady, osłony niematerialne takie jak kurtyny świetlne, maty czułe na nacisk itp. Wszelkie ryzyka resztkowe, wobec których nie można stosować powyższych metod, należy ograniczać, stosując **(3) sprzęt ochrony osobistej i/lub szkolenia**. Odpowiednie środki powinny zostać określone przez dostawcę maszyny.

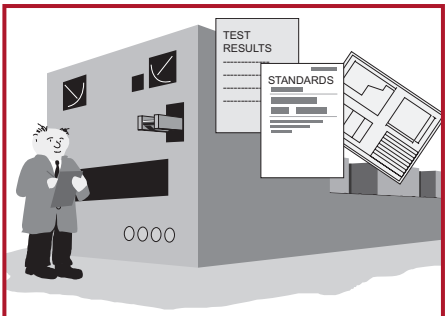
Do konstrukcji i obsługi maszyny należy wykorzystywać odpowiednie materiały. Należy zapewnić prawidłowe oświetlenie oraz metody przenoszenia. Elementy i systemy sterowania powinny być bezpieczne i niezawodne. Maszyny nie mogą uruchamiać się nieoczekiwanie i powinny być wyposażone w co najmniej jedno urządzenie zatrzymywania awaryjnego. Należy również wziąć pod uwagę złożone instalacje, w których na bezpieczeństwo mogą wpływać procesy znajdujące się przed i za maszyną. Defekt zasilania lub obwodu sterowania nie może prowadzić do sytuacji niebezpiecznej. Maszyny muszą pracować stabilnie i być zdolne do wytrzymania możliwych do przewidzenia obciążeń. Maszyny nie mogą mieć wystających krawędzi oraz powierzchni mogących spowodować obrażenia ciała.

Do uniknięcia zagrożeń ze strony części ruchomych należy stosować osłony lub urządzenia ochronne. Muszą one mieć trwałą konstrukcję oraz być odporne na próby obejścia. Osłony stałe powinny być montowane w sposób pozwalający na demontaż wyłącznie przy użyciu narzędzi, a mocowania osłon muszą być blokowane. Osłony ruchome powinny blokować sterowanie. Osłony nastawne powinny być łatwo regulowane bez stosowania narzędzi.

Należy zapobiegać zagrożeniom wynikającym z korzystania z energii elektrycznej lub innej, w tym także energii zmagazynowanej. Ryzyko obrażeń spowodowanych temperaturą, wybuchem, hałasem, drganiami, zapyleniem, gazami lub radiacją powinno być minimalne. Powinny istnieć zalecenia dotyczące konserwacji i obsługi technicznej. Należy stosować wystarczające urządzenia sygnalizacyjne i ostrzegawcze. Maszyny powinny być dostarczane z instrukcjami bezpiecznej instalacji, użytkowania, regulacji itd.

Ocena zgodności

Projektant lub inny podmiot odpowiedzialny powinien móc przedstawić dowód potwierdzający zgodność z wymaganiami zasadniczymi. Plik ten powinien zawierać wszystkie istotne informacje, takie jak wyniki testów, rysunki, specyfikacje itp.



Maszyna musi spełniać wymagania BHP

Zharmonizowana norma europejska (EN), wymieniona w Dzienniku Urzędowym Unii Europejskiej dla dyrektywy maszynowej, której data ustania domniemania zgodności nie minęła, pozwala założyć zgodność z określonymi wymogami zasadniczymi. (Wiele najnowszych norm wymienionych w Dzienniku Urzędowym UE obejmuje odwołania do wymagań zasadniczych, które są objęte normą). W związku z powyższym, tam gdzie sprzęt jest zgodny ze zharmonizowanymi normami europejskimi, zadanie przedstawienia deklaracji zgodności z wymaganiami zasadniczymi jest znacznie uproszczone, a producent czerpie również korzyści z większej pewności prawnej. Stosowanie tych norm nie jest wymagane przez prawo, jednak silnie zaleca się ich zastosowanie, ponieważ udowodnienie zgodności przy zastosowaniu innych metod może okazać się zadaniem niezwykle złożonym. Omawiane normy wspierają dyrektywę maszynową i są opracowywane przez Europejski Komitet Normalizacyjny (CEN) we współpracy z ISO oraz przez Europejski Komitet Normalizacyjny Elektrotechniki (CENELEC) we współpracy z IEC.

Musi być przeprowadzone gruntowne, udokumentowane oszacowanie ryzyka, aby zapewnić, że zostały zdefiniowane wszystkie potencjalne zagrożenia maszynowe. Również w tym przypadku, odpowiedzialność za spełnienie wymagań zasadniczych, nawet tych niewymienionych w zharmonizowanych normach EN, spoczywa na producencie maszyny.

Dokumentacja techniczna

Producent lub jego autoryzowany przedstawiciel muszą przygotować dokumentację techniczną w celu uwiarygodnienia zgodności z wymaganiami zasadniczymi. Plik ten powinien zawierać wszystkie istotne informacje, takie jak wyniki testów, rysunki, specyfikacje itp.

Nie jest wymagane, aby wszystkie informacje były stale dostępne w formie drukowanej, ale konieczne jest udostępnienie całej dokumentacji technicznej w celu umożliwienia inspekcji na żądanie kompetentnych władz (organu wyznaczonego przez kraj UE do monitorowania zgodności maszyn).

Minimalny zakres, który powinna obejmować dokumentacja techniczna:

1. Ogólne rysunki sprzętu zawierające schematy obwodów sterowania.
2. Szczegółowe rysunki, obliczenia itp. wymagane do określenia zgodności maszyny z zasadniczymi wymaganiami.
3. Dokumentacja oceny ryzyka, obejmująca zasadnicze wymagania mające zastosowanie w przypadku maszyny oraz opis zastosowanych środków zabezpieczających.
4. Lista norm oraz innych zastosowanych specyfikacji technicznych wskazujących na dostosowanie się do zasadniczych wymagań.
5. Opis metod zastosowanych w celu wyeliminowania zagrożeń związanych z maszynami.
6. Tam gdzie to ma zastosowanie, wszelkie raporty techniczne lub zaświadczenia uzyskane od organu kontrolnego lub innej instytucji.
7. Raporty techniczne wyników testów, jeśli deklarowana jest zgodność ze zharmonizowaną normą europejską.
8. Egzemplarz instrukcji maszyny.
9. Tam gdzie ma to zastosowanie, deklaracja włączenia dotycząca nieukończonej maszyny oraz odpowiednie instrukcje montażu dla takiej maszyny.
10. Jeśli ma zastosowanie, kopie deklaracji zgodności WE maszyny lub innych produktów wchodzących w skład maszyny.
11. Kopia deklaracji zgodności z WE

Przy produkcji seryjnej należy podać szczegółowe informacje na temat zastosowanych środków wewnętrznych (np. systemów jakości) zapewniających, że wszystkie wyprodukowane maszyny zachowują zgodność z wymaganiami:

- Producent musi wykonać niezbędne badania lub testy elementów, mocowań lub ukończonej maszyny w celu określenia, czy opracowany projekt i konstrukcja pozwalają na jej bezpieczny montaż i obsługę.

- Dokumentacja techniczna nie musi występować w formie pojedynczego dokumentu, ale powinna być możliwość składania jej i udostępniania w rozsądnym czasie. Musi być także dostępna przez dziesięć lat od momentu wyprodukowania ostatniego egzemplarza maszyny.

Opis techniczny nie musi zawierać szczegółowych planów lub innych konkretnych informacji dotyczących podzespołów użytych w procesie produkcji maszyny, o ile nie są one potrzebne do poświadczenia zgodności z wymaganiami zasadniczymi BHP.

Ocena zgodności maszyn z załącznika IV

Ocena zgodności

Pewne typy sprzętu wymagają zastosowania środków specjalnych. Sprzęt taki wymieniono w załączniku IV do dyrektywy. Są to maszyny niebezpieczne, takie jak niektóre maszyny do obróbki drewna, prasy, wtryskarki, sprzęt kopalniany, podnośniki samochodowe, itp.

Załącznik IV zawiera również niektóre elementy bezpieczeństwa, takie jak urządzenia ochronne przeznaczone do wykrywania obecności osób (np. kurtyny świetlne) i moduły logiki przeznaczone do zapewnienia bezpieczeństwa.

W przypadku maszyn z załącznika IV, które nie są w pełni zgodne ze stosownymi zharmonizowanymi normami europejskimi, producent lub jego autoryzowany przedstawiciel muszą zastosować jedną z następujących procedur:

1. Badanie typu WE. Należy przygotować dokumentację techniczną i dostarczyć próbną maszynę do jednostki notyfikowanej (ośrodka badań) w celu przeprowadzenia badania typu WE. W przypadku pomyślnych wyników maszyna uzyska certyfikat badania typu WE. Ważność certyfikatu należy weryfikować co pięć lat w jednostce notyfikowanej.

2. Całkowite zapewnienie jakości. Musi zostać przygotowana dokumentacja techniczna, a producent powinien działać w ramach zatwierdzonego systemu kontroli jakości w zakresie projektowania, produkcji, kontroli końcowej oraz testów. System jakości musi zapewniać zgodność maszyny z postanowieniami dyrektywy. System jakości musi być okresowo weryfikowany przez jednostkę notyfikowaną.

Sprawdzanie przez jednostkę notyfikowaną

W przypadku maszyn, które nie zostały ujęte w Załączniku IV lub maszyn, które zostały ujęte w Załączniku IV, ale które są w pełni zgodne ze stosownymi zharmonizowanymi normami europejskimi, producent lub jego autoryzowany przedstawiciel mają możliwość przygotowania dokumentacji technicznej oraz poddania własnej ocenie i zadeklarowania zgodności urządzenia. Muszą być przygotowane kontrole wewnętrzne, których celem jest zapewnienie, że wyprodukowany sprzęt nadal pozostaje zgodny.

Jednostki notyfikowane

Na terenie UE istnieje sieć jednostek notyfikowanych, które komunikują się ze sobą i pracują zgodnie ze wspólnymi kryteriami. Jednostki notyfikowane są wyznaczane przez organy rządowe (nie przez przemysł), a informacje na ich temat można pobrać ze strony:

http://ec.europa.eu/growth/tools-databases/nando/

Procedura wystawiania deklaracji zgodności WE

Wszystkie dostarczane maszyny muszą posiadać oznaczenie CE. Maszyny powinny być również dostarczane z deklaracją zgodności WE.

Oznakowanie CE informuje o zgodności maszyny z wszelkimi odnośnymi dyrektywami europejskimi oraz o wykonaniu odpowiednich procedur oceny zgodności. Stosowanie znaku CE dyrektywy maszynowej w przypadku maszyn niespełniających odpowiednich wymogów ochrony zdrowia i bezpieczeństwa jest niezgodne z prawem.

Deklaracja zgodności WE musi zawierać następujące informacje:

- Nazwę firmy i pełny adres producenta oraz jego autoryzowanego przedstawiciela, jeśli dotyczy;
- Nazwę i adres osoby upoważnionej do przygotowywania dokumentacji technicznej, która musi być mieszkańcem Wspólnoty (w przypadku producenta spoza UE może to być „autoryzowany przedstawiciel”);
- Opis i identyfikacja maszyny, w tym nazwę ogólną, funkcję, model, typ, numer seryjny oraz nazwę handlową;
- Jednoznaczną deklarację potwierdzającą, że maszyna spełnia wszystkie wymagane postanowienia dyrektywy, a tam, gdzie ma to zastosowanie, podobną deklarację potwierdzająca zgodność z innymi dyrektywami i/lub odpowiednimi postanowieniami, z którymi maszyna jest zgodna;
- Odniesienie do zastosowanych zharmonizowanych norm, jeśli dotyczy;
- Odniesienie do zastosowanych innych norm technicznych i specyfikacji, jeśli dotyczy;
- (w przypadku maszyn z załącznika IV) – jeśli dotyczy – nazwa, adres i numer identyfikacyjny jednostki notyfikowanej, która przeprowadziła badanie typu WE określone w załączniku IX oraz numer świadectwa badania typu WE;
- (w przypadku maszyn z załącznika IV) – jeśli dotyczy – nazwa, adres i numer identyfikacyjny jednostki notyfikowanej, która zatwierdziła pełny system zapewniania jakości określony w załączniku X;
- Miejscowość i data deklaracji;
- Nazwisko i podpis osoby upoważnionej do wystawiania deklaracji w imieniu producenta lub autoryzowanego przedstawiciela.

Deklaracja włączenia WE maszyny nieukończonej

DEKLARACJA WŁĄCZENIA powinna być wydawana w przypadku sprzętu dostarczanego z innymi elementami, które razem, w późniejszym czasie utworzą kompletną maszynę. Nie należy stosować znaku CE. Deklaracja powinna określać, że sprzęt nie może zostać oddany do użytku, jeśli deklaracji zgodności nie uzyskała maszyna, której ten sprzęt jest podzespołem. Musi zostać przygotowana dokumentacja techniczna, a maszyna nieukończona musi być dostarczona wraz z informacjami zawierającymi opis warunków, które należy spełnić w celu zapewnienia prawidłowego włączenia do finalnej maszyny, aby zapewnić bezpieczeństwo.

Opcja ta nie jest dostępna w przypadku sprzętu, który może działać samodzielnie lub którego działanie powoduje zmianę funkcji maszyny.

Deklaracja włączenia musi zawierać następujące informacje:

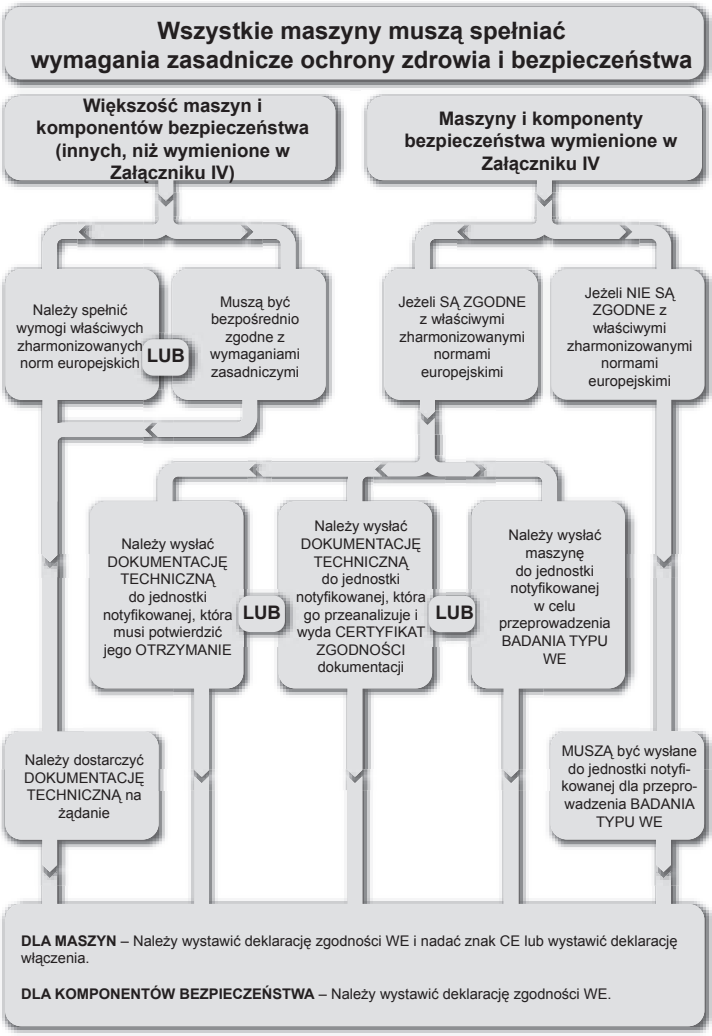
- Nazwę firmy i pełny adres producenta maszyny nieukończonej oraz autoryzowanego przedstawiciela, jeśli dotyczy;
- Nazwę i adres osoby upoważnionej do przygotowywania odpowiedniej dokumentacji technicznej, która musi być mieszkańcem Wspólnoty (w przypadku producenta spoza UE może to być „autoryzowany przedstawiciel");
- Opis i identyfikacja maszyny nieukończonej, w tym nazwę ogólną, funkcję, model, typ, numer seryjny oraz nazwę handlową;
- Zdanie deklarujące, które zasadnicze wymagania dyrektywy zostały zastosowane i spełnione oraz, że odpowiednia dokumentacja techniczna została przygotowana zgodnie z częścią B załącznika VII, oraz – jeśli dotyczy – zdanie deklarujące zgodność maszyny nieukończonej z innymi odpowiednimi dyrektywami;
- Zobowiązanie przekazania, w odpowiedzi na uzasadnione żądanie władz krajowych, odpowiednich informacji dotyczących maszyny nieukończonej. Zobowiązanie powinno obejmować metodę przekazania informacji i nie powinno naruszać praw własności intelektualnej producenta maszyny nieukończonej;
- Oświadczenie stanowiące, że maszyna nieukończona nie może być włączona do eksploatacji dopóki finalna maszyna, w skład której została ona włączona, nie uzyska deklaracji zgodności z odpowiednią dyrektywą, jeśli dotyczy;
- Miejscowość i data deklaracji;
- Nazwisko i podpis osoby upoważnionej do wystawiania deklaracji w imieniu producenta lub autoryzowanego przedstawiciela.

Maszyny dostarczane spoza UE – autoryzowani przedstawiciele

Jeśli producent z siedzibą poza UE (lub EOG) eksportuje maszyny do UE, musi on wyznaczyć autoryzowanego przedstawiciela.

Autoryzowany przedstawiciel oznacza osobę fizyczną lub prawną zamieszkałą we Wspólnocie Europejskiej, która uzyskała pisemne upoważnienie od producenta do wykonywania wszelkich czynności i obowiązków związanych z dyrektywą maszynową.

Dyrektywa UE dotycząca sprzętu roboczego (dyrektywa narzędziowa)



Dyrektywa maszynowa dotyczy dostawców, natomiast dyrektywa narzędziowa (2009/104/EC) obejmuje użytkowników maszyn. Jej treść obejmuje wszystkie sektory przemysłu i zawiera informacje na temat ogólnych obowiązków pracodawców oraz minimalnych wymagań dotyczących bezpieczeństwa związanego ze sprzętem roboczym. Wdrażając postanowienia tej dyrektywy, wszystkie kraje członkowskie UE ustanawiają swoje własne akty prawne.

Na przykład na obszarze Wielkiej Brytanii dyrektywa obowiązuje jako „The Provision and Use of Work Equipment Regulations" (określana często akronimem P.U.W.E.R.). Metoda wdrożenia może się różnić w zależności od kraju, ale postanowienia dyrektywy są zachowane w każdym przypadku.

Artykuły dyrektywy zawierają szczegółowe informacje na temat rodzajów sprzętu i miejsc pracy objętych dyrektywą.

Nakładają one także ogólne obowiązki na pracodawcę, np. konieczność wdrożenia bezpiecznych systemów pracy oraz dostarczania odpowiedniego i bezpiecznego sprzętu, który należy prawidłowo konserwować. Operatorzy maszyn powinni zostać przeszkoleni i zaznajomieni z zasadami bezpiecznego użytkowania.

Nowe maszyny (oraz maszyny używane sprowadzone spoza obszaru UE) dostarczone po 1 stycznia 1993 roku (w Polsce po 1 maja 2004 roku) powinny być zgodne z wszelkimi odnośnymi dyrektywami dot. produktów, np. z dyrektywą maszynową (mają również zastosowanie środki przejściowe). Używany sprzęt pochodzący z UE dostarczony po raz pierwszy na stanowisko pracy musi od razu spełniać minimalne wymagania, wyszczególnione w załączniku dyrektywy narzędziowej.

Uwaga: Istniejące lub używane maszyny, które przeszły gruntowny remont lub modernizację, są sklasyfikowane jako nowy sprzęt, dlatego sposób ich użytkowania musi być zgodny z postanowieniami dyrektywy maszynowej (nawet jeśli maszyna jest przeznaczona do użytku wewnętrznego firmy).

Zgodność sprzętu roboczego jest ważnym wymogiem dyrektywy. Podkreśla ona odpowiedzialność pracodawcy za przeprowadzenie odpowiednich procesów oceny ryzyka.

Wymogiem jest prawidłowa konserwacja maszyny. Zazwyczaj wiąże się to z koniecznością opracowania harmonogramu planowej konserwacji zapobiegawczej. Zaleca się, aby prowadzony był dziennik zawierający aktualne informacje. Jest to szczególnie ważne w przypadku, gdy konserwacja i kontrola sprzętu przyczynia się do podtrzymywania nienaruszalności systemów i urządzeń bezpieczeństwa.

Załącznik do dyrektywy narzędziowej zawiera minimalne wymagania dotyczące sprzętu roboczego.

Jeśli sprzęt odpowiada stosownym dyrektywom dot. produktu, np. dyrektywie maszynowej, będzie on automatycznie odpowiadać odpowiednim wymogom projektowym wyszczególnionym w minimalnych wymaganiach w załączniku.

Kraje członkowskie są upoważnione do wydawania ustaw dotyczących stosowania sprzętu roboczego, które wykraczają poza minimalne wymagania dyrektywy narzędziowej.

Szczegółowe informacje na temat dyrektywy dotyczącej stosowania sprzętu roboczego można znaleźć na oficjalnej stronie UE:

https://osha.europa.eu/en/legislation/directives/3

Przepisy USA

Ta sekcja przedstawia niektóre wymagania bezpieczeństwa obowiązujące w USA dotyczące zabezpieczania maszyn. Stanowią one jedynie punkt wyjścia. Czytelnik powinien samodzielnie znaleźć więcej informacji na temat wymagań dotyczących konkretnych zastosowań i podjąć działania zapewniające, że opracowane projekty, obszary zastosowań, stosowane procedury konserwacji oraz praktyki są zgodne z potrzebami własnymi oraz przepisami lokalnymi i krajowymi.

W Stanach Zjednoczonych istnieje wiele organizacji promujących bezpieczeństwo przemysłowe. Można wśród nich wymienić:

1. Korporacje stosujące się do obowiązujących wymogów oraz opracowujące swoje własne wymagania wewnętrzne;

2. Urząd ds. Bezpieczeństwa i Zdrowia w Pracy (OSHA, Occupational Safety and Health Administration);

3. Organizacje przemysłowe, takie jak Krajowe Stowarzyszenie ds. Ochrony Przeciwpożarowej (NFPA, National Fire Protection Association), Stowarzyszenie Robotyki Przemysłowej (RIA, Robotics Industries Association), Stowarzyszenie Technologii Produkcyjnych (AMT, The Association of Manufacturing Technology) oraz dostawcy produktów i rozwiązań związanych z bezpieczeństwem, np. Rockwell Automation.

Urząd ds. Bezpieczeństwa i Zdrowia w Pracy

W Stanach Zjednoczonych jednym z głównych organów wpływających na bezpieczeństwo przemysłowe jest Urząd ds. Bezpieczeństwa i Zdrowia w Pracy (OSHA, Occupational Safety and Health Administration). Urząd OSHA został założony w 1971 roku na mocy ustawy Kongresu USA. Celem ustawy jest zapewnianie bezpiecznych i zdrowych warunków pracy oraz ochrona zasobów ludzkich. Ustawa upoważnia Sekretarza ds. Pracy do określania obowiązkowych norm bezpieczeństwa i zdrowia dotyczących działalności związanej z handlem międzystanowym. Ustawa dotyczy zatrudnienia w Stanach Zjednoczonych, Dystrykcie Kolumbii, Wspólnocie Portoryko, na Wyspach Dziewiczych, Samoa Amerykańskim, Guamie, Powierniczych Wyspach Pacyfiku, wyspie Wake, Dalekich Wyspach Mniejszych określonych w dokumencie „Outer Continental Shelf Lands Act", Wyspie Johnstona oraz w Strefie Kanału Panamskiego.

Podstawowe wymagania znajdują się w artykule 5. Każdy pracodawca powinien zapewnić swoim pracownikom miejsce pracy wolne od rozpoznanych zagrożeń, mogących spowodować śmierć lub poważne obrażenia ciała. Powinien także postępować zgodnie z normami bezpieczeństwa i zdrowia ogłoszonymi w Ustawie.

Artykuł 5 mówi również, że wszyscy pracownicy powinni postępować zgodnie z normami bezpieczeństwa i zdrowia w pracy, a także zgodnie z wszelkimi obowiązującymi przepisami, regulacjami oraz nakazami zgodnymi z Ustawą, które dotyczą ich czynności i zachowania.

Zgodnie z Ustawą OSHA odpowiedzialność spoczywa na pracowniku i pracodawcy. Jest to różnica w stosunku do dyrektywy maszynowej, w której odpowiedzialność za dostarczanie na rynek maszyn wolnych od zagrożeń dotyczy dostawcy. W Stanach Zjednoczonych dostawca może sprzedawać maszyny bez żadnych środków zabezpieczających. Aby maszyna była bezpieczna, środki te muszą zostać dodane przez użytkownika. Praktyka taka była wprawdzie powszechna w czasie przyjmowania Ustawy, jednak obecnie istnieje tendencja, by dostarczać maszyny wyposażone w środki ochronne. Wiąże się to z faktem, że projektowanie bezpiecznych rozwiązań zintegrowanych z maszyną jest znacznie bardziej opłacalne niż dodawanie środków ochronnych po zaprojektowaniu i zmontowaniu maszyny. Normy starają się teraz określać, aby dostawca i użytkownik wspólnie definiowali wymagania dotyczące środków ochronnych. Dzięki temu produkowane maszyny będą nie tylko bezpieczne, ale również bardziej wydajne.

Sekretarz ds. Pracy może upowszechniać wszelkie normy ogólnokrajowe oraz obowiązujące normy federalne, jako normę dotyczącą bezpieczeństwa i zdrowia w pracy, jeśli publikacja takich norm będzie oznaczać poprawę bezpieczeństwa i zdrowia odnośnie do konkretnie określonych zadań pracowników.

OSHA realizuje to zadanie, publikując przepisy w Temacie 29 Kodeksu Przepisów Federalnych (29 CFR – Code of Federal Regulation). Normy dotyczące maszyn przemysłowych opublikowała OSHA w części 1910 w 29 CFR. Teksty te są ogólnie dostępne na stronie Administracji Bezpieczeństwa i Higieny Pracy (OSHA): www.osha.gov. W przeciwieństwie do wielu norm, które są dobrowolne, normy OSHA stanowią przepisy prawa.

Niektóre ważne elementy odnoszące się do bezpieczeństwa maszyn:

A – Informacje ogólne
B – Przyjęcie i rozszerzenie obowiązujących norm federalnych
C – Ogólne zasady dotyczące bezpieczeństwa i zdrowia
H – Materiały niebezpieczne
I – Sprzęt ochrony osobistej
J – Ogólne środowisko sterowania (wraz z procedurą Lockout/Tagout)
O – Maszyny i zabezpieczenia maszyn
R – Przemysły specjalne
S – Wymagania elektryczne

Niektóre normy OSHA odnoszą się do norm dobrowolnych. Prawnymi następstwami włączenia przez odniesienie jest traktowanie materiału w taki sposób, jakby został w całości opublikowany w Rejestrze Federalnym. Gdy norma ogólnokrajowa jest włączana przez odniesienie w jednej z podczęści, jest ona traktowana jak przepis prawa.
Na przykład dobrowolna norma NFPA 70, znana jako Narodowy Kodeks Elektryczny USA, włączona jest przez odniesienie do podczęści S. Zabieg ten sprawia, że wymogi normy NFPA 70 stają się obowiązujące.

Podczęść J regulacji 29 CFR 1910.147 obejmuje sterowanie niebezpieczną energią. Norma ta jest powszechnie znana pod nazwą Lockout/Tagout. Odpowiednią normą dobrowolną jest ANSI Z244.1. Podstawowe wymagania normy dotyczą odłączania zasilania maszyn, przy których prowadzone są prace serwisowe lub konserwacyjne. Jej celem jest zapobieganie nieoczekiwanemu załączeniu lub uruchomieniu maszyny, które mogłoby skutkować obrażeniami pracowników.

Aby zapobiec obrażeniom ciała u pracowników, pracodawcy muszą opracować program blokowania i oznakowania (LOTO) oraz zastosować procedury montażu odpowiednich elementów blokujących i oznakowań w urządzeniach odłączających energię, a także wdrożyć inne środki unieruchamiania maszyn i urządzeń, tak aby wyeliminować możliwości niespodziewanego włączenia zasilania, uruchomienia maszyny lub uwolnienia zmagazynowanej energii.

Drobne modyfikacje i regulacja narzędzi oraz wykonywanie innych mniej istotnych czynności serwisowych podczas normalnej eksploatacji sprzętu w procesie produkcji zostały omówione w normie ANSI Z244 „Alternative measures" (Środki alternatywne) pod warunkiem, że są one rutynowe, powtarzalne i zintegrowane z pracą urządzeń produkcyjnych, a praca jest wykonywana przy użyciu alternatywnych środków zapewniających należytą ochronę. Ma to bezpośrednie oparcie w dokumencie OSHA pt. „OSHA Minor Servicing Exception" (Drobne prace serwisowe w drodze wyjątku). Środki alternatywne to urządzenia ochronne, takie jak kurtyny świetlne, maty bezpieczeństwa, osłony ryglowane oraz inne podobne urządzenia podłączone do systemu bezpieczeństwa. Zadaniem projektanta i użytkownika maszyny jest określenie, które czynności są „drobne", a które „rutynowe", „powtarzalne" i „nieodłączne". Może to być zdefiniowane podczas oceny ryzyka.

Podczęść O obejmuje „Maszyny i zabezpieczenia maszyn". Zawiera ogólne wymagania związane ze wszystkimi maszynami, a także wymagania dotyczące pewnych konkretnych maszyn. Podczas powoływania OSHA w 1971 roku przyjęto wiele ówczesnych norm ANSI. Normę B11.1 – dotyczącą pras mechanicznych – przyjęto na przykład jako normę 1910.217.

Norma 1910.212 to ogólna norma OSHA dotycząca maszyn. Podaje ona, że należy zastosować co najmniej jedną metodę zabezpieczenia maszyny, w celu ochrony operatora i innych pracowników znajdujących się w obszarze roboczym, przed takimi zagrożeniami, jak strefy pochwycenia, wciągania, elementy obracające się, wyrzucane odłamki i iskry. Tam gdzie to możliwe, osłony powinny być przymocowane do maszyny lub, jeśli to niemożliwe, należy je zabezpieczyć w inny sposób. Osłony nie powinny stwarzać dodatkowego zagrożenia. Jeżeli konieczne jest zdemontowanie osłon, musi to być możliwe tylko za pomocą narzędzia.

„Stanowisko robocze" to obszar maszyny, w którym jest wykonywana faktyczna obróbka przetwarzanego materiału. Stanowisko robocze maszyny, której działanie stanowi zagrożenie dla pracownika, powinno być osłonięte. Urządzenie ochronne powinno być zgodne z wszelkimi odpowiednimi normami, a przypadku ich braku, powinno być zaprojektowane i zmontowane w taki sposób, aby podczas cyklu pracy żadna część ciała operatora nie znajdowała się w strefie niebezpiecznej.

Podczęść S (1910.399) zawiera wymagania elektryczne OSHA. Instalacja lub sprzęt mogą zostać zaakceptowane przez Zastępcę Sekretarza ds. Pracy i zatwierdzone w rozumieniu niniejszej podczęści S, jeśli zostały zaakceptowane, certyfikowane, zarejestrowane, oznakowane lub w inny sposób określone jako bezpieczne przez akredytowane krajowe laboratorium testowe (NRTL – Nationally Recognized Testing Laboratory).

Co to jest „sprzęt"? Jest to ogólne pojęcie odnoszące się do materiałów, mocowań, urządzeń, przyrządów, osprzętu, aparatów oraz podobnych elementów, używanych jako część lub w połączeniu z instalacją elektryczną.

Co to oznacza „zarejestrowany"? Sprzęt jest uznawany za „zarejestrowany", jeśli został umieszczony na liście, która (a) jest publikowana przez akredytowane krajowe laboratorium testowe (NRTL), przeprowadzające okresowe kontrole procesu produkcyjnego tego typu sprzętu, oraz (b) określa, że sprzęt jest zgodny z normami ogólnokrajowymi lub został przetestowany i określony jako bezpieczny w konkretnym zastosowaniu.

Od sierpnia 2009 roku następujące firmy są uznawane przez OSHA jako laboratoria NRTL:

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

Ostateczną decyzję dotyczącą tego, co jest wymagane, wydaje organ posiadający jurysdykcję (AHJ – Authority Having Jurisdiction). Przykładowo w takich stanach jak Nowy Jork, Kalifornia i Illinois obowiązują dodatkowe wymagania.

Niektóre stany przyjęły swoje własne przepisy BHP, w których mogą znajdować się kryteria dodatkowe w stosunku do przepisów krajowych/federalnych. W dwudziestu czterech stanach, w Portoryko i na Wyspach Dziewiczych obowiązują plany stanowe zgodne z OSHA. Przyjęto tam także lokalne normy oraz polityki egzekwowania. W większości stany te przyjmują normy identyczne z federalnym przepisami OSHA. W niektórych stanach przyjęto jednak inne normy dotyczące omawianego tematu lub obowiązują tam inne polityki egzekwowania. Pracodawcy muszą dostarczać historię wypadków do OSHA. Tam opracowywane są informacje dotyczące wypadkowości, które następnie są przesyłane do biur lokalnych i wykorzystywane do ustalania kolejności kontroli. Podstawowe kierunki kontroli to:

- Zagrożenie bezpośrednie
- Katastrofy i ofiary w ludziach
- Skargi pracownicze
- Branże wysokiego ryzyka
- Lokalne kontrole zaplanowane
- Kontrole sprawdzające
- Krajowe i lokalne programy tematyczne

Naruszenie norm OSHA może skutkować nałożeniem grzywny. Wysokości grzywien są następujące:

- Poważne: do 7000 USD za jedno naruszenie,
- Inne niż poważne: uznaniowo, ale nie więcej niż 7000 USD,
- Powtórne: do 70 000 USD za jedno naruszenie,
- Zamierzone: do 70 000 USD za jedno naruszenie,
- Naruszenia powodujące śmierć: dodatkowe sankcje karne,
- Brak wyeliminowania naruszenia: 7000 USD dziennie.

Przepisy kanadyjskie

W Kanadzie bezpieczeństwo przemysłowe jest zarządzane na poziomie regionalnym. Każda prowincja ma swoje własne przepisy, które tam obowiązują i są egzekwowane. Na przykład w Ontario przyjęto ustawę Ochrony Zdrowia i Bezpieczeństwa, w której określono uprawnienia i obowiązki wszystkich osób w miejscu pracy. Jej głównym założeniem jest ochrona pracowników przed zagrożeniami podczas wykonywania pracy. W akcie ustanowiono procedury postępowania z zagrożeniami w miejscu pracy oraz określono sposób egzekwowania prawa w przypadku, gdy zgodność z wymogami nie została uzyskana w sposób dobrowolny.

W rozdziale 7 ustawy znajduje się przepis 851 określający konieczność przeprowadzenia wstępnego przeglądu bezpieczeństwa i zdrowia. Przegląd ten jest wymagany w Ontario w odniesieniu do wszystkich nowych, wyremontowanych lub zmodernizowanych maszyn. Wynikiem przeglądu jest obowiązkowy raport sporządzany przez wykwalifikowanego inżyniera.

Rozdział 2: Normy

W tym rozdziale przedstawiono niektóre typowe normy międzynarodowe i krajowe odnoszące się do bezpieczeństwa maszyn. Przedstawione informacje nie stanowią wyczerpującego zestawienia, lecz raczej ogólne spojrzenie na te aspekty bezpieczeństwa maszyn, które są tematem normalizacji. Niniejszy rozdział należy przeczytać w połączeniu z rozdziałem Przepisy.

Kraje całego świata starają się wspólnie opracowywać globalne normy zharmonizowane. Jest to widoczne zwłaszcza w kontekście bezpieczeństwa maszyn. Globalne normy bezpieczeństwa maszyn są nadzorowane przez dwie organizacje: ISO oraz IEC. Zastosowanie mają nadal normy regionalne i krajowe, które często wspierają wymagania lokalne, ale wiele państw skłania się ku stosowaniu norm międzynarodowych opracowanych właśnie przez ISO i IEC.

Przykładem są normy EN stosowane w krajach EOG. Wszystkie nowe normy EN są zgodne – a w większości przypadków identyczne pod względem treści – z normami ISO i IEC. Obecnie również w USA robi się często odniesienia do norm IEC i ISO.

Normy IEC obejmują zagadnienia elektrotechniczne, natomiast ISO dotyczą wszystkich pozostałych. Organizacje te zrzeszają jako członków większość krajów uprzemysłowionych. Normy dotyczące bezpieczeństwa maszyn są opracowywane przez grupy robocze składające się z ekspertów pochodzących z wielu obszarów przemysłowych świata.

W większości krajów normy można uznawać za dobrowolne, natomiast przepisy są prawnie obowiązujące. Normy są jednak zazwyczaj traktowane jako praktyczna interpretacja przepisów. Oznacza to, że normy i przepisy są ze sobą blisko związane.

ISO (International Organization for Standardization)

ISO to pozarządowa organizacja, w której skład wchodzą organy opracowujące normy krajowe, działające na terenie większości państw świata (157 krajów w momencie druku dokumentu). System jest koordynowany przez Centralny Sekretariat znajdujący się w Genewie w Szwajcarii. ISO opracowuje normy dotyczące bardziej wydajnego, bezpieczniejszego i czystszego projektowania, produkowania oraz użytkowania maszyn. Normy sprawiają też, że handel międzynarodowy staje się łatwiejszy i uczciwszy. Normy ISO są oznaczane trzema literami ISO.

Normy ISO dla maszyn są, podobnie jak normy EN, podzielone na trzy poziomy: typ A, B i C (opis europejskich norm zharmonizowanych znajduje się w dalszej części rozdziału).

Aby uzyskać więcej informacji, odwiedź witrynę ISO:*www.iso.org.*

IEC (International Electrotechnical Commission)

IEC opracowuje i publikuje międzynarodowe normy dotyczące technologii elektrycznych, elektronicznych oraz podobnych. IEC, za pośrednictwem swoich członków, promuje międzynarodową współpracę we wszystkich aspektach norm elektrotechnicznych oraz działań powiązanych, takich jak na przykład ocena zgodności z normami elektrotechnicznymi.

Aby uzyskać więcej informacji, odwiedź witrynę IEC:*www.iec.ch*

Europejskie normy zharmonizowane EN

Normy te są wspólne dla wszystkich krajów EOG. Ich opracowywaniem zajmują się organizacje CEN oraz CENELEC. Stosowanie norm jest nieobligatoryjne, jednak projektowanie i produkcja sprzętu zgodnie z tymi normami stanowią najlepszy sposób zapewnienia zgodności z wymogami zasadniczymi dyrektywy maszynowej.

Europejskie normy zharmonizowane podzielono na trzy typy: A, B i C.

NORMY typu A: dotyczą aspektów związanych ze wszystkimi typami maszyn.

NORMY typu B: są podzielone na 2 podgrupy.
NORMY typu B1: dotyczą konkretnych aspektów bezpieczeństwa i ergonomii maszyn.
NORMY typu B2: dotyczą komponentów bezpieczeństwa i urządzeń ochronnych.

NORMY typu C: dotyczą konkretnych typów lub grup maszyn.

Należy zauważyć, że zgodność z normą typu C oznacza automatycznie domniemaną zgodność z wymaganiami zasadniczymi, na których norma się opiera. Jeśli odpowiednia norma C nie istnieje, jako częściowy lub pełny dowód spełnienia wymagań zasadniczych mogą być wykorzystywane normy typu A i B, przez wskazanie zgodności o odpowiednimi rozdziałami.

Współpraca między organizacjami CEN/CENELEC oraz ISO i IEC została uregulowana odpowiednimi umowami. Oznacza to, że już niedługo opracowane zostaną wspólne normy ogólnoświatowe. W większości przypadków normy EN mają swoje odpowiedniki wśród norm IEC lub ISO. W ogólnym zamierzeniu ich treści będą takie same, a różnice dotyczące aspektów regionalnych zostaną opublikowane we wstępie do normy.

Kompletna lista norm EN związanych z bezpieczeństwem maszyn znajduje się pod adresem:

http://ec.europa.eu/growth/single-market/european-standards/

Normy USA

Normy OSHA

Tam gdzie to możliwe, OSHA publikuje jako normy bezpieczeństwa normy ogólnokrajowe lub obowiązujące normy federalne. Obligatoryjne zapisy norm (słowo „powinien" w języku norm oznacza obowiązkowość) włączane są jako odniesienie i mają ten sam skutek oraz moc prawną, jak normy wyszczególnione w części 1910. Jako przykład może posłużyć ogólnokrajowa norma NFPA 70 wymieniona jako dokument referencyjny w Dodatku A, podczęści S, Wymagania elektryczne Części 1910 w 29 CFR. NFPA 70 to norma dobrowolna opracowana przez Narodowe Stowarzyszenie Ochrony Przeciwpożarowej (NFPA: National Fire Protection Association). Jest ona również znana jako Krajowy Kodeks Elektryczny (NEC: National Electric Code). Przez włączenie wszystkie obligatoryjne wymagania kodeksu NEC są również obligatoryjne według norm OSHA.

Normy ANSI

Prywatny sektor nieobligatoryjnych systemów normalizacyjnych jest na obszarze Stanów Zjednoczonych zarządzany i koordynowany przez Amerykański Krajowy Instytut Normalizacyjny (ANSI, American National Standards Institute). Jest to prywatna organizacja członkowska typu non-profit, wspierana przez różnorodne organizacje sektora prywatnego i publicznego.

ANSI nie opracowuje samodzielnie nowych norm. Wspomaga proces opracowywania, pomagając w uzgadnianiu stanowisk różnych grup specjalistów. ANSI zapewnia także, że grupy specjalistów przestrzegają uzgodnionych wytycznych oraz postępują otwarcie i zgodnie z ustalonymi procedurami.
Normy te podzielono na kategorie takie jak normy aplikacyjne lub konstrukcyjne. Normy aplikacyjne określają w jaki sposób realizowane są zabezpieczenia maszyn. Jednym z przykładów jest norma ANSI B11.1, zawierająca informacje na temat użytkowania osłon na prasach mechanicznych, oraz norma ANSI/RIA R15.06, omawiająca zabezpieczenia wykorzystywane do wygrodzenia cel robotów.

Narodowe Stowarzyszenie Ochrony Przeciwpożarowej

Narodowe Stowarzyszenie Ochrony Przeciwpożarowej (NFPA, National Fire Protection Association) powstało w 1896 roku. Jego zadaniem jest ograniczanie wpływu pożarów na jakość życia. Cel ten jest realizowany przez wspieranie uzgodnionych naukowo kodeksów i norm, przeprowadzanie badań i szkoleń dotyczących ochrony przeciwpożarowej oraz szkoleń z zakresu bezpieczeństwa. NFPA wspiera wiele norm, których postanowienia pomagają zrealizować powyższe zadanie. Dwie ważne normy dotyczące bezpieczeństwa przemysłowego oraz środków ochronnych to Krajowy Kodeks Elektryczny (NEC, National Electric Code) oraz Norma Elektryczna dla Maszyn Przemysłowych (Electrical Standard for Industrial Machinery).

Narodowe Stowarzyszenie Ochrony Przeciwpożarowej wspiera NEC od 1911 roku. Oryginalny dokument kodeksu opracowano w 1897 roku w wyniku połączonych wysiłków

różnych zainteresowanych stron, działających w branży ubezpieczeniowej, elektrycznej, budowlanej oraz pokrewnych. Od tej pory kodeks NEC był wielokrotnie aktualizowany. Aktualizacje mają miejsce raz na trzy lata.
Artykuł 670 kodeksu NEC zawiera szczegółowe informacje na temat maszyn przemysłowych i odsyła czytelnika do Normy Elektrycznej dla Maszyn Przemysłowych (NFPA 79).

Norma NFPA 79 dotyczy wyposażenia i urządzeń elektrycznych i elektronicznych, a także systemów maszyn przemysłowych. Celem NFPA 79 jest dostarczanie szczegółowych informacji z zakresu promowania bezpieczeństwa życia i mienia, związanych z zastosowaniem sprzętu, przyrządów lub systemów elektrycznych/elektronicznych jako elementów maszyn przemysłowych. Treść normy NFPA 79, oficjalnie przyjętej przez ANSI w roku 1962, jest bardzo podobna do treści normy IEC 60204-1.

Maszyny, które nie są uwzględnione w konkretnych normach OSHA, muszą być wolne od rozpoznanych zagrożeń mogących powodować śmierć lub poważne obrażenia. Maszyny te należy projektować i obsługiwać co najmniej zgodnie z wymaganiami obowiązujących norm przemysłowych. Normę NFPA 79 można stosować do maszyn, które nie są wyraźnie uwzględnione w normach OSHA.

Normy kanadyjskie

Normy CSA (Canadian Standards Association) stanowią odzwierciedlenie ogólnokrajowych uzgodnień producentów i użytkowników, klientów, sprzedawców, związków i organizacji specjalistycznych, a także agencji rządowych. Są stosowane w szerokim zakresie w przemyśle i handlu, a ich zapisy są często włączane do przepisów obowiązujących w miastach, prowincjach i okręgach. Dotyczy to zwłaszcza przepisów związanych ze zdrowiem, bezpieczeństwem, budownictwem i konstruowaniem oraz środowiskiem.

Osoby prywatne, firmy i stowarzyszenia z całej Kanady wyrażają swoje poparcie dla opracowywania norm CSA poprzez poświęcenie dobrowolnie swojego czasu i umiejętności w pracach Stowarzyszenia oraz wspierają je swoim stałym członkostwem. Stowarzyszenie CSA liczy łącznie ponad 7000 działaczy dobrowolnych oraz 2000 członków wspierających.

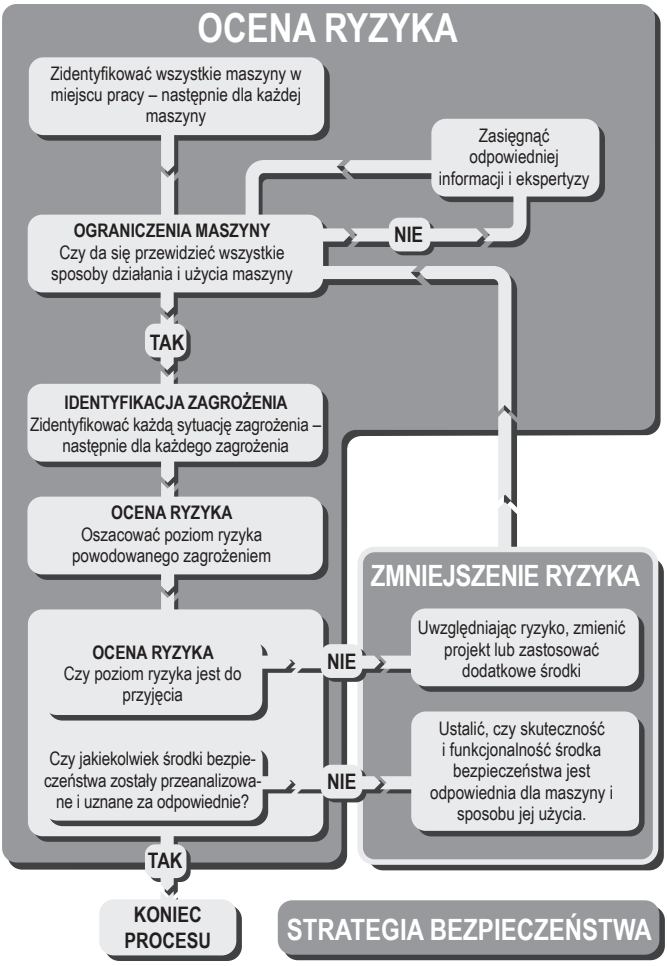
Organem nadzorującym krajowy system normalizacyjny jest Kanadyjski Instytut Normalizacyjny. Jest to federacja niezależnych i samodzielnych organizacji, pracujących w interesie narodowym nad dalszym rozwojem i udoskonalaniem nieobligatoryjnych norm.

Normy australijskie

Większość tych norm jest blisko związana z odpowiednimi normami ISO/IEC/EN
Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Telefon: +61 2 8206 6000
E-mail:mail@standards.org.au – Strona internetowa: *www.standards.org.au*

Rozdział 3: Strategia bezpieczeństwa

Z czysto funkcjonalnego punktu widzenia maszyna jest tym lepsza, im bardziej efektywnie przetwarza materiał. Aby jednak maszyna mogła wykonywać swoją pracę, musi być również bezpieczna. Faktycznie bezpieczeństwo powinno być traktowane jako podstawowy aspekt pracy maszyny.
Aby opracować prawidłową strategię bezpieczeństwa, należy zrealizować dwie główne czynności, które są od siebie wzajemnie zależne. Zależność pokazano na poniższej ilustracji.



Na wstępnie wykonywana jest **OCENA RYZYKA**, oparta na dokładnym zrozumieniu ograniczeń i funkcji maszyny oraz zadań, które mogą być wymagane do wykonania podczas jej cyklu życia.

Następnie, jeśli to konieczne, wykonywane jest **OGRANICZENIE RYZYKA**. Na podstawie informacji uzyskanych podczas etapu oceny ryzyka wybierane są odpowiednie środki bezpieczeństwa. Sposób realizacji wymienionych czynności stanowi podstawę STRATEGII BEZPIECZEŃSTWA maszyny.

Zastosowanie tego systematycznego podejścia daje pewność, że wszystkie aspekty są brane pod uwagę, a zasada nadrzędna nie ulega zagubieniu w szczegółach. Cały proces powinien być udokumentowany. Zapewni to nie tylko bardziej dogłębną analizę, ale też wyniki analizy będą dostępne do sprawdzenia przez inne firmy.

Niniejszy rozdział dotyczy zarówno producentów, jak i użytkowników maszyn. Producent musi upewnić się, że maszyna może bezpiecznie działać. Ocena ryzyka powinna zaczynać się już w fazie projektowania maszyny i brać pod uwagę wszystkie możliwe do przewidzenia zadania wykonywane przez maszynę. Taki typ podejścia zadaniowego w pierwszych iteracjach oceny ryzyka okazuje się niezwykle ważny. Na przykład może regularnie występować potrzeba regulacji ruchomych elementów maszyny. Środki pozwalające bezpiecznie wykonać tę czynność powinny zostać opracowane w fazie projektowania maszyny. Jeśli nie zostanie to wykonane na początkowym etapie, wdrożenie zabezpieczenia w późniejszym czasie może być trudne lub wręcz niemożliwe. W wyniku tego może się okazać, że regulacja ruchomych elementów jest wciąż wymagana, ale nie da się jej przeprowadzić w sposób bezpieczny ani wydajny. Maszyna, w przypadku której w trakcie oceny ryzyka wzięto pod uwagę wszystkie zadania robocze, będzie maszyną bezpieczniejszą i bardziej wydajną.

Zadaniem użytkownika (lub pracodawcy) jest zapewnienie, by maszyny w środowisku pracy były bezpieczne. Nawet jeśli maszyna została określona przez producenta jako bezpieczna, na użytkowniku nadal spoczywa obowiązek przeprowadzenia oceny ryzyka w celu sprawdzenia, czy jest ona bezpieczna w jego środowisku pracy. Maszyny bywają często używane w okolicznościach, które nie zostały przewidziane przez producenta. Gdy na przykład frezarka jest użytkowana na terenie warsztatów szkolnych, należy wziąć pod uwagę dodatkowe aspekty, których nie ma potrzeby rozważać, gdy jest użytkowana w hali przemysłowej. Istnieje także możliwość, że poszczególne bezpieczne maszyny mogą być połączone ze sobą w sposób, który czyni ich użytkowanie niebezpiecznym.

Należy także pamiętać, że w przypadku gdy firma użytkownika nabywa dwie lub więcej niezależnych maszyn i integruje je w jednym procesie sterowania, staje się producentem zespołu maszyn.

Przyjrzyjmy się zatem podstawowym czynnościom, wymaganym do opracowania prawidłowej strategii bezpieczeństwa. Przedstawione dalej etapy można zastosować do istniejącej instalacji fabrycznej lub pojedynczej nowej maszyny.

Ocena ryzyka

Błędem jest uznawanie oceny ryzyka za obciążenie. Jest to przydatny proces dostarczający ważnych informacji oraz pozwalający użytkownikowi lub projektantowi podejmować logiczne decyzje dotyczące metod zapewniania bezpieczeństwa.

Zagadnienie to zostało uwzględnione w różnych normach. Najszerzej wykorzystywane na świecie wytyczne zawiera norma EN ISO 12100 Bezpieczeństwo maszyn – ogólne zasady projektowania – ocena ryzyka i zmniejszanie ryzyka. Raport techniczny ISO: Dostępny jest również raport ISO/TR 14121-2. Zawiera on praktyczne wskazówki i przykładowe metody oceny ryzyka.

Bez względu na technikę stosowaną do oceny ryzyka, rezultaty o szerszym zakresie i jednocześnie lepiej wyważone można uzyskać w przypadku, gdy jest ona realizowana przez wielofunkcyjny zespół, a nie przez jednego pracownika.

Ocena ryzyka to proces iteracyjny przeprowadzany dla różnych etapów cyklu życia maszyny. Dostępne informacje będą się różniły zależnie od etapu cyklu życia. Na przykład, jeśli ocena ryzyka jest wykonywana przez konstruktora maszyny, ma on dostęp do wszystkich szczegółowych informacji o mechanizmach maszyny i użytych materiałach. Może jednak jedynie w przybliżeniu zakładać, w jakim środowisku pracy będzie ona pracowała. Ocena ryzyka wykonywana przez użytkownika maszyny wiąże się z kolei z brakiem dostępu do szczegółów technicznych, lecz jednocześnie daje pełną możliwość sprawdzenia zachowania maszyny w środowisku pracy. Najlepiej jeśli wynik jednej iteracji stanowi jednocześnie dane wejściowe dla kolejnej.

Określanie limitów maszyny

Zadanie to polega na zgromadzeniu i przeanalizowaniu danych dotyczących części, mechanizmów i funkcji maszyny. Konieczne będzie również uwzględnienie wszystkich typów kontaktu użytkownika z maszyną oraz środowiskiem, w którym będzie pracować. Celem tego etapu jest dokładne zrozumienie maszyny oraz sposobu jej użytkowania.

Jeśli osobne maszyny są ze sobą połączone, mechanicznie lub przy użyciu systemów sterowania, powinny być traktowane jako jedna maszyna, dopóki nie zostaną podzielone na strefy przez odpowiednie środki ochronne.

Należy wziąć pod uwagę wszystkie ograniczenia i etapy cyklu życia maszyny, uwzględniając jej instalację, oddanie do eksploatacji, utrzymanie, likwidację, prawidłową pracę i użytkowanie, a także następstwa możliwych do przewidzenia przypadków niewłaściwego użytkowania i uszkodzeń.

Identyfikacja zadań i zagrożeń

Wszystkie zagrożenia związane z maszyną należy zidentyfikować i skatalogować z uwzględnieniem ich typu oraz miejsca występowania. Typy zagrożeń to m.in. zmiażdżenie, odcięcie, zaplątanie, wyrzut części, spaliny, promieniowanie, substancje toksyczne, ciepło, hałas itp.

Wyniki analizy zadania powinny być porównane z wynikami identyfikacji ryzyka. Wskaże to potencjalny punkt styczności pracownika z zagrożeniem, czyli sytuację niebezpieczną. Wszystkie sytuacje niebezpieczne muszą być wyszczególnione. Istnieje możliwość, że jedno zagrożenie może powodować wystąpienie różnych typów sytuacji niebezpiecznych, w zależności od osoby lub wykonywanego zadania. Na przykład obecność przeszkolonego i mającego wysokie kwalifikacje konserwatora może mieć inne następstwa niż obecność nieprzeszkolonej sprzątaczki, która nie ma żadnej wiedzy na temat maszyny. Jeżeli w takiej sytuacji każdy przypadek jest opisany i oddzielnie rozpatrzony można będzie uzasadnić zastosowanie innych środków ochronnych dla konserwatora, a innych dla sprzątaczki. Jeśli przypadki te nie będą opisane i oddzielnie rozpatrzone, będzie trzeba założyć wystąpienie najgorszego możliwego scenariusza i zastosować te same środki ochronne zarówno dla służb konserwacyjnych, jak i sprzątających.

Czasem konieczne jest przeprowadzenie ogólnej oceny ryzyka dotyczącej istniejącej maszyny, w której zamontowano już środki ochronne (np. maszyny zawierającej niebezpieczne elementy ruchome, zabezpieczone przez osłonę blokującą). Niebezpieczne elementy ruchome stanowią potencjalne zagrożenie, które może stać się zagrożeniem rzeczywistym w przypadku uszkodzenia systemu blokującego. O ile system blokujący nie został wcześniej zatwierdzony (np. przez ocenę ryzyka lub projekt zgodny z odpowiednią normą), jego obecność nie powinna być brana pod uwagę.

Szacowanie ryzyka

Jest to jeden z najważniejszych aspektów oceny ryzyka. Do tego zagadnienia można podejść na wiele sposobów. Podstawowe zasady przedstawiono na kolejnych stronach.

Ze wszystkimi maszynami stwarzającymi sytuacje niebezpieczne wiąże się ryzyko wypadku (np. odniesienia obrażeń). Im większe ryzyko, tym ważniejsze staje się podjęcie odpowiednich działań. Dla niektórych zagrożeń ryzyko może być niewielkie i możliwe do zaakceptowania, ale w innych przypadkach ryzyko może być tak duże, że w celu ochrony konieczne będzie zastosowanie nadzwyczajnych środków. W związku z tym, aby odpowiedzieć na pytanie „czy i co zrobić z ryzykiem”, należy je oszacować.

Ryzyko jest często postrzegane wyłącznie w kontekście dotkliwości obrażeń na skutek wypadku. W celu oszacowania poziomu występującego ryzyka należy uwzględnić stopień potencjalnych obrażeń ORAZ prawdopodobieństwo ich wystąpienia.

Raport ISO TR 14121-2 „Ocena ryzyka – Praktyczny przewodnik i przykłady metod" przedstawia różne metody oceny ilościowej ryzyka. Istnieją różnice w terminologii i systemach punktacji, ale wszystkie metody odwołują się do zasad zawartych w normie EN ISO 12100. Następujący tekst określa podstawowe zasady oceny ilościowej ryzyka, a jego przeznaczeniem jest zapewnienie wsparcia niezależnie od tego, która metodologia została zastosowana. Generalnie opiera się on na parametrach podanych w punkcie 6.5 raportu ISO TR 14121-2 – Hybrid Tool.

Pod uwagę brane są następujące czynniki:
- STOPIEŃ POTENCJALNYCH OBRAŻEŃ.
- PRAWDOPODOBIEŃSTWO ICH WYSTĄPIENIA.

Prawdopodobieństwo wystąpienia uwzględnia co najmniej dwa czynniki:
- CZĘSTOTLIWOŚĆ NARAŻENIA.
- PRAWDOPODOBIEŃSTWO ODNIESIENIA OBRAŻEŃ.

Współczynnik prawdopodobieństwa jest często dzielony na dwa inne współczynniki:
- PRAWDOPODOBIEŃSTWO WYSTĄPIENIA.
- PRAWDOPODOBIEŃSTWO UNIKNIĘCIA.

Należy uwzględnić wszelkie dostępne dane i ekspertyzy. Uwzględnia się wszystkie etapy cyklu życia maszyny, dlatego w celu uniknięcia nadmiernego skomplikowania należy opierać się na najgorszych przypadkach dotyczących poszczególnych czynników. Ważne jest również, by zachować zdrowy rozsądek. Podejmowane decyzje powinny uwzględniać to, co jest wykonalne, realne i akceptowalne. Właśnie w takich sytuacjach sprawdza się koncepcja zespołów wielofunkcyjnych.

Na tym etapie nie powinno się zwykle uwzględniać żadnego istniejącego systemu zabezpieczeń. Jeśli oszacowanie ryzyka wykaże konieczność zastosowania systemu ochronnego, wymagane charakterystyki będzie można określić na podstawie metodologii przedstawionych w dalszej części.

Stopień ciężkości potencjalnego urazu

W poniższych rozważaniach przyjmuje się, że wypadek czy incydent rzeczywiście się wydarzył. Na podstawie dokładnej analizy zagrożenia można określić najbardziej dotkliwe obrażenie.

Pamiętaj: w tym przypadku zakłada się, że obrażenia są nieuniknione, a pod uwagę brana jest jedynie ich dotkliwość. Należy przyjąć, że operator jest narażony na niebezpieczny ruch lub proces. Stopień ciężkości urazu powinien być oszacowany w zgodności z czynnikami właściwymi dla przyjętej metodologii.

Na przykład w następujący sposób:
- Śmierć, utrata oka lub ramienia
- Skutek nieodwracalny, np. utrata palców
- Skutek odwracalny wymagający pomocy lekarskiej
- Skutek odwracalny wymagający udzielenia pierwszej pomocy

Częstotliwość narażenia

Częstotliwość narażenia określa, jak często operator lub konserwator jest narażony na zagrożenie. Częstotliwość narażenia na zagrożenie może zostać sklasyfikowana zgodnie z czynnikami właściwymi dla wybranej metodologii.

Na przykład w następujący sposób:
- Częściej niż 1 raz na godzinę
- Od 1 razu na godzinę do 1 razu dziennie
- Od 1 razu dziennie do 1 razu na 2 tygodnie
- Od 1 razu na 2 tygodnie do 1 razu w roku
- Rzadziej niż 1 raz w roku

Prawdopodobieństwo wystąpienia obrażeń

Należy przyjąć, że operator jest narażony na niebezpieczny ruch lub proces. Prawdopodobieństwo wystąpienia zdarzenia niebezpiecznego może zostać sklasyfikowane zgodnie z czynnikami właściwymi dla wybranej metodologii. W celu sklasyfikowania tego prawdopodobieństwa należy uwzględnić charakterystykę maszyny, oczekiwane zachowanie człowieka i inne czynniki.

Na przykład w następujący sposób:
- Do pominięcia
- Rzadkie
- Możliwe
- Prawdopodobne
- Bardzo wysokie

Prawdopodobieństwo uniknięcia obrażeń

Przy uwzględnieniu sposobu współpracy ludzi z maszyną i innych parametrów, takich jak prędkość ruchu przy uruchomieniu, prawdopodobieństwo uniknięcia obrażeń może zostać sklasyfikowane zgodnie z czynnikami właściwymi dla wybranej metodologii.

Na przykład w następujący sposób:
- Prawdopodobne
- Możliwe
- Niemożliwe

Po rozpatrzeniu wszystkich punktów wyniki zostają przedstawione w formie wykresu lub tabeli, w zależności od sposobu zastosowanej oceny ilościowej ryzyka. Powyższa procedura jest jedną z form ilościowego oszacowania ryzyka w przypadku różnych rodzajów zagrożeń stwarzanych przez maszynę. Informacja ta może zostać wykorzystana przy podejmowaniu decyzji, które z zagrożeń należy zredukować, aby uzyskać możliwy do przyjęcia poziom bezpieczeństwa.

Ograniczenie ryzyka

Teraz należy rozważyć każdą maszynę i po kolei poszczególne zagrożenia, jakie ona powoduje i podjąć środki ukierunkowane na rozpatrzenie tych zagrożeń.

Hierarchia środków ograniczania ryzyka
Pod uwagę należy wziąć trzy podstawowe metody i stosować je w następującej kolejności:

1. Eliminacja lub możliwie największe ograniczenie ryzyka (projektowanie maszyn wewnętrznie bezpiecznych).
2. Instalacja zabezpieczeń i uzupełniających środków zabezpieczających w przypadku zagrożeń, których nie da się wyeliminować na etapie projektu.
3. Dostarczenie informacji dotyczących bezpiecznego użytkowania, z włączeniem znaków ostrzegawczych i sygnalizacji. Niezbędne są również informacje o jakimkolwiek ryzyku szczątkowym, a także o tym, czy konieczne jest przeprowadzenie odpowiedniego szkolenia lub zapewnienie środków ochrony osobistej.

Należy rozważyć zastosowanie każdego ze środków w kolejności od góry do dołu (jeśli jest to możliwe). W rezultacie wdrożeniu podlegać będzie kombinacja środków ochronnych.

Eliminacja ryzyka (projektowanie wewnętrznie bezpieczne)

W fazie projektowania maszyny można uniknąć wielu możliwych zagrożeń. Wystarczy wziąć pod uwagę czynniki takie jak zastosowane materiały, wymagania dostępu, gorące powierzchnie, metody przeniesienia napędu, miejsca uwięzienia, poziomy napięcia itp.

Jeśli na przykład dostęp do strefy niebezpiecznej nie jest wymagany, rozwiązaniem jest zamknięcie ruchu w korpusie maszyny lub wygrodzenie jej osłoną stałą.

Systemy i środki zabezpieczające

Jeśli jest wymagany dostęp do strefy niebezpiecznej, sprawy nieco się komplikują. Konieczne będzie zapewnienie, by dostęp był możliwy wyłącznie wtedy, gdy maszyna jest bezpieczna. Wymagane może być zastosowanie środków ochronnych, takich jak osłony blokujące i/lub systemy wyzwalające. Wybór urządzeń i systemów ochronnych powinien w dużym stopniu zależeć od charakterystyki pracy maszyny. Jest to niezwykle ważne, ponieważ system ograniczający wydajność maszyny stwarza zagrożenie nieautoryzowanego usunięcia lub obejścia.

Jedna z najbliższych i najbardziej kompletnych interakcji między człowiekiem a maszyną pojawia się podczas prac konserwacyjnych, wykrywania i usuwania usterek oraz napraw. Dla zapewnienia bezpieczeństwa w przypadku działań rutynowych i drobnych ingerencji może być możliwe wykorzystanie środków zabezpieczających opartych na systemie związanym z bezpieczeństwem (patrz opis w dalszej części). Jednak ze wszystkich przepisów wynika całkowicie jasno, że – dla wszelkich ingerencji w rodzaju poważnych prac konserwacyjnych, napraw, demontażu lub prac na obwodach zasilania – powinny być stosowane zarówno przepisy, jak i urządzenia zapewniające odseparowanie i rozproszenie energii maszyny (niekiedy z włączeniem siły grawitacji). W ten sposób można usunąć ryzyko nieoczekiwanego uruchomienia i kontaktu ze źródłami energii. Jest to przedmiotem wielu różnych przepisów i norm. Przykładowo, poprzedni tekst w sekcji „Przepisy USA" zawiera przepisy i normy dla „blokad zabezpieczających i oznakowania ostrzegawczego" (LOTO). Odnośne wymagania zawarte są również w normach EN 1037 i ISO 14118 „Zapobieganie niespodziewanemu uruchomieniu". Wskazówki i wymagania w zakresie technologii elektrycznych podane są także w normach IEC/EN 60204-1 i NFPA 79.
Oczywiście sprawą nadrzędną jest zastosowanie właściwego systemu pracy, zapewniającego wdrożenie wszystkich poprawnych procedur.

Kolejny podrozdział opisuje niektóre typowe realizacje.

Zapobieganie niespodziewanym załączeniom

Zapobieganie niespodziewanym załączeniom jest omówione w wielu normach. Przykłady obejmują normy ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 i AS 4024.1603. We wszystkich występuje wspólna zasada: podstawową metodą zapobiegania niespodziewanym załączeniom jest usunięcie energii z systemu i zablokowanie go w stanie bezpiecznym. Celem jest umożliwienie bezpiecznego wejścia osób do niebezpiecznych stref maszyny.

Lockout/Tagout

Nowe maszyny muszą być wyposażone w blokowane urządzenie odcinające dopływ energii. Dotyczy to wszystkich typów energii, w tym elektrycznej, hydraulicznej, pneumatycznej, grawitacyjnej i laserowej. Lockout oznacza zablokowanie urządzenia odłączającego energię. Zdjęcie blokady może być dozwolone tylko tej osobie, która ją założyła lub kierownika w kontrolowanych warunkach. Jeśli na maszynie pracuje kilka osób, urządzenie odłączające energię musi zostać zablokowane przez każdą z nich. Każda blokada musi być identyfikowalna przez jej właściciela.

W USA, w starszych maszynach, w których nigdy nie było urządzeń odłączających, alternatywą jest oznakowanie (tagout). W takiej sytuacji maszyna jest wyłączana i oznaczana ostrzeżeniem, że nie wolno jej uruchamiać, ponieważ właściciel oznaczenia pracuje na maszynie. Od początku 1990 roku także maszyny modernizowane muszą mieć zainstalowane blokowane urządzenia odłączające energię.

Urządzenie odłączające energię to urządzenie mechaniczne, które fizycznie zapobiega przesyłaniu lub uwalnianiu energii. Mogą to być wyłączniki, odłączniki, rozłączniki ręczne, zestawy gniazdo/wtyczka lub zawory przestawiane ręczne. Urządzenia odłączające energię elektryczną muszą odłączać wszystkie nieuziemione przewody czynne, a bieguny nie mogą działać niezależnie.

Odłączanie energii i oznakowanie służy do zapobiegania niespodziewanemu uruchomieniu maszyny. Niespodziewane uruchomienie może mieć różne przyczyny: uszkodzenie systemu sterowania; nieprawidłowe zadziałanie przycisku start, czujnika, stycznika lub zaworu; przywrócenie zasilania po zaniku; inne czynniki wewnętrzne i zewnętrzne. Po zakończeniu procesu odłączania lub oznakowania należy sprawdzić, czy energia uległa rozproszeniu.

Bezpieczne systemy odłączające

Bezpieczne systemy odłączające wykonują prawidłowe wyłączanie i pozwalają na łatwe blokowanie zasilania maszyny. Rozwiązanie to sprawdza się dobrze w przypadku dużych maszyn i systemów produkcyjnych, zwłaszcza gdy wiele źródeł energii jest zlokalizowanych na antresolach lub w odległych miejscach.

Rozłączniki

Do lokalnego odłączania urządzeń elektrycznych można zainstalować rozłącznik tuż przed urządzeniem, które będzie odłączane i blokowane. Przykładem urządzeń zdolnych realizować obie wymienione funkcje są rozłączniki serii 194E.

Systemy kluczy sekwencyjnych

Kolejną metodą wdrożenia systemu blokowania są systemy kluczy sekwencyjnych. Większość takich systemów zaczyna się od urządzenia odłączającego energię. Po wyłączeniu łącznika za pomocą głównego przełącznika, energia elektryczna jest odłączana jednocześnie od wszystkich nieuziemionych przewodów czynnych. Następnie można wyjąć klucz główny i przenieść w miejsce, gdzie wymagany jest dostęp do maszyny. Bardziej złożone konfiguracje blokowania można uzyskać, dodając do systemu różne dodatkowe elementy.

Inne metody blokowania

Odłączanie i oznakowanie musi być realizowane podczas serwisowania lub konserwacji urządzeń. Uniemożliwienie ingerencji we wnętrze maszyny podczas normalnej pracy produkcyjnej realizowane jest za pomocą środków ochronnych takich, jak systemy osłon blokujących. Różnica między serwisowaniem/konserwacją a normalnymi czynnościami produkcyjnymi nie zawsze jest oczywista.

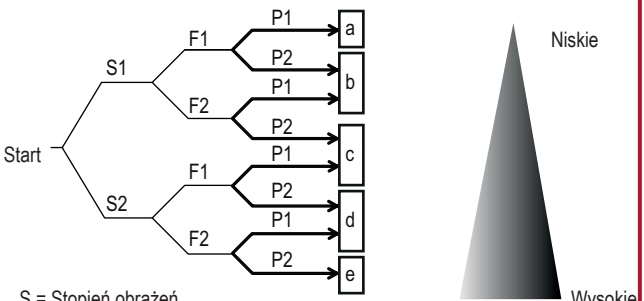
Pewne drobne regulacje i zadania serwisowe, które odbywają się podczas normalnych operacji produkcji, nie wymagają zablokowania maszyny. Można tutaj wymienić czynności takie jak ładowanie i rozładowywanie materiałów, wymiana i regulacja mniejszego oprzyrządowania, serwisowe smarowanie oraz usuwanie odpadów materiału. Czynności te muszą być rutynowe, powtarzalne i związane z wykorzystaniem sprzętu produkcyjnego, a praca jest wykonywana z zastosowaniem innych środków, takich jak środki ochronne, które zapewniają należytą ochronę. Środki ochronne to urządzenia takie jak osłony blokujące, kurtyny świetlne i maty bezpieczeństwa. Po zastosowaniu odpowiedniej logiki i napędów z certyfikacją bezpieczeństwa operatorzy są w stanie uzyskać bezpieczny dostęp do niebezpiecznych stref maszyny podczas normalnych zadań produkcyjnych i drobnych czynności serwisowych.

W tym przypadku bezpieczeństwo maszyny zależy od odpowiedniego zastosowania prawidłowego działania systemu ochronnego, nawet w przypadku defektu. Należy teraz wziąć pod uwagę aspekt prawidłowej pracy systemu. W ramach każdego typu, możliwy jest wybór technologii o różnym stopniu wydajności nadzorowania defektów, ich wykrywania lub zapobiegania im.

Idealnie by było, gdyby każdy system ochronny był doskonały, absolutnie bez żadnej możliwości doprowadzenia do sytuacji niebezpiecznej. W praktyce jesteśmy jednak ograniczeni zakresem wiedzy oraz materiałów. Kolejnym bardzo realnym ograniczeniem są koszty. Biorąc pod uwagę te czynniki staje się oczywiste, że potrzebne są sposoby na dopasowanie zakresu środków zabezpieczających do poziomu ryzyka ustalonego na etapie oszacowania ryzyka.

Bez względu na typ wybranego urządzenia ochronnego należy pamiętać, że „system związany z bezpieczeństwem” może zawierać wiele elementów, takich jak urządzenia ochronne, okablowanie, urządzenia odłączające zasilanie, a czasem także elementy systemu sterowania maszyny. Wszystkie elementy systemu (wraz z osłonami, mocowaniami, okablowaniem itd.) powinny mieć odpowiednie charakterystyki zapewnienia bezpieczeństwa odpowiednie do projektu i technologi. Normy IEC/EN 62061 i EN ISO 13849-1 klasyfikują poziomy hierarchiczne zapewnienia bezpieczeństwa dla układów sterowania związanych z bezpieczeństwem i zawierają w załącznikach metody oceny ryzyka, które umożliwiają określenie wymogów nienaruszalności systemu bezpieczeństwa.

Norma EN ISO 13849-1:2015 zawiera rozszerzony graf ryzyka, przedstawiony w załączniku A.



S = Stopień obrażeń
F = Częstotliwość lub czas trwania narażenia
P = Prawdopodobieństwo uniknięcia

Muszą być określone dla każdej funkcji bezpieczeństwa!

IEC 62061 w załączniku A także zawiera metodę oceny ryzyka, do której formularz przedstawiono poniżej.

Ocenie ryzyka i środki bezpieczeństwa

Produkt: _____
Wydane poprzez: _____
Data: _____

Czarny obszar = Wymagane środki bezpieczeństwa
Szary obszar = Zalecane środki bezpieczeństwa

Dokument nr:
Stanowi część:
☐ Wstępna ocena ryzyka
☐ Pośrednia ocena ryzyka
☐ Kontrolna ocena ryzyka

Konsekwencje	Wskaźnik ciężkości Se	Klasa Cl					Częstotliwość i czas trwania Fr		Prawdopodobieństwo wystąpienia Pr		Wskaźnik uniknięcia Av	
		3–4	5–7	8–10	11–13	14–15						
Śmierć, utrata oka lub ramienia		SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<=1 godz.	5	Częste	5		
Trwałe, utrata palców			OM	SIL 1	SIL 2	SIL 3	>1 godz. do <=1 dzień	5	Prawdopodobne	4		
Odwracalne, pomoc medyczna				OM	SIL 1	SIL 2	>1 dzień do <=2 tygodnie	4	Możliwe	3	Niemożliwe	5
Odwracalne, pierwsza pomoc					OM	SIL 1	>2 tygodnie do <=1 rok	3	Rzadkie	2	Możliwe	3
							>1 rok	2	Pomijalne	1	Prawdopodobne	1

Nr ser.	Ryz. Nr	Ryzyko	Se	Fr	Pr	Av	Cl	Środek bezpieczeństwa	Bezpieczne

Uwagi

Użycie którejkolwiek z powyższych metod powinno dostarczyć równoważnych wyników. Każdą metodę należy stosować w połączeniu ze szczegółowymi informacjami znajdującymi się w odnośnej normie.

Niezwykle ważne jest, aby postępować zgodnie z treścią wytycznych przedstawionych w użytej normie. Grafu lub tabeli ryzyka nie można stosować bez uwzględnienia dodatkowych czynników lub w nadmiernie uproszczony sposób.

Weryfikacja

Po wybraniu środków ochronnych, przed ich wdrożeniem należy powtórzyć etap szacowania ryzyka. Jest to procedura, o której często się zapomina. Zdarza się, że zainstalowanie środka ochronnego wywoła u operatora maszyny poczucie całkowitego i kompletnego bezpieczeństwa w stosunku do pierwotnie przewidzianego zagrożenia.
Ponieważ jednak nie ma on już takiego poczucia zagrożenia, jak na początku, może postępować z maszyną w inny sposób. Może on znacznie częściej narażać się na zagrożenia, np. może wchodzić do dalszych stref maszyny niż zazwyczaj. Oznacza to, że w przypadku defektu środków ochronnych osoby te będą narażone na większe ryzyko niż określone początkowo. Jest to ryzyko rzeczywiste i należy je oszacować. Jak widać, ocena ryzyka to proces, który musi być powtarzany z uwzględnieniem wszystkich możliwych do przewidzenia zmian sposobu obsługi maszyny. Wynik omawianego etapu jest używany do sprawdzenia, czy proponowane środki ochronne są faktycznie odpowiednie. Dodatkowe informacje można znaleźć w załączniku A normy IEC/EN 62061.

Szkolenia, sprzęt ochrony osobistej itd.

Ważne jest, aby operatorzy odbyli niezbędne szkolenie dotyczące bezpiecznych metod pracy z maszyną. Nie oznacza to jednak, że nie powinny być stosowane również inne środki. Niedopuszczalne jest, by zamiast wprowadzenia osłon po prostu powiedzieć operatorowi, aby nie zbliżał się do stref niebezpiecznych.

Konieczne może być również korzystanie przez operatora ze sprzętu, takiego jak specjalne rękawice, okulary ochronne, maski tlenowe itp. Projektant maszyny musi określić typ wymaganego sprzętu. Zastosowanie sprzętu ochrony osobistej nie powinno stanowić podstawowej metody zabezpieczenia, lecz uzupełniać środki ochronne wymienione wcześniej. Zazwyczaj będzie również potrzebne użycie znaków i oznaczeń zwiększających świadomość obecności ryzyka szczątkowego.

Rozdział 4: Realizacja środków ochronnych

Jeśli wyniki oceny ryzyka pokażą, że maszyna lub proces wiąże się z ryzykiem odniesienia obrażeń, zagrożenie to należy wyeliminować lub ograniczyć. Sposób realizacji tego zamierzenia zależy od typu maszyny oraz zagrożenia. Środki ochronne systemu sterowania bezpieczeństwa w połączeniu z osłonami uniemożliwiają dostęp do strefy niebezpiecznej lub – jeśli dostęp jest możliwy – zapobiegają wystąpieniu w niej niebezpiecznego ruchu. Typowe przykłady takich środków ochronnych, omówione w dalszej części, to osłony blokujące, kurtyny świetlne, maty bezpieczeństwa, sterowanie oburęczne oraz urządzenia zezwalające.

Urządzenia i systemy zatrzymania awaryjnego są powiązane z systemami sterowania bezpieczeństwa, ale nie są to bezpośrednie systemy ochronne. Należy je traktować wyłącznie jako dodatkowe środki ochronne.

Zapobieganie dostępowi za pomocą osłon stałych

Jeśli zagrożenie dotyczy części maszyny niewymagającej dostępu, do maszyny należy przymocować osłonę stałą. Demontaż takich osłon musi wymagać zastosowania narzędzi. Osłony stałe muszą 1) być odporne na środowisko pracy, 2) tam, gdzie to konieczne, chronić przed wyrzucanymi odłamkami oraz 3) nie stwarzać zagrożenia z powodu np. ostrych krawędzi. Osłony stałe mogą mieć otwory w miejscu styku z maszyną oraz otwory wynikające z zastosowania wygrodzenia z siatki.

Okna umożliwiają wygodne monitorowanie pracy maszyny. Jednak przy wyborze materiału na szybę należy wziąć pod uwagę, że reakcje chemiczne z płynami obróbkowymi, promieniowanie UV, jak również proces naturalnego starzenia się materiału może z czasem spowodować jego degradację.

Rozmiar otworów powinien uniemożliwiać operatorowi kontakt z zagrożeniem. Tabela O-10 w U.S. OHSA 1910.217 (f) (4), ISO 13854, tabela D-1 w ANSI B11.19, tabela 3 w CSA Z432 i AS4024.1 zawierają wytyczne dotyczące odpowiedniej odległości określonego otworu od zagrożenia.

Wykrywanie dostępu

Środki bezpieczeństwa mogą służyć do wykrywania dostępu do zagrożenia. Jeśli jako sposób ograniczania ryzyka wybrano metodę wykrywania, projektant musi rozumieć, że należy zastosować kompletny system bezpieczeństwa. Samodzielne urządzenie zabezpieczające nie zapewni wymaganej redukcji ryzyka. Wspomniany system bezpieczeństwa zawiera zazwyczaj trzy bloki: 1) urządzenie wejściowe wykrywające dostęp do zagrożenia, 2) urządzenie logiczne przetwarzające sygnały od urządzeń wykrywających, sprawdza stan systemu bezpieczeństwa oraz wyłącza lub załącza urządzenia wyjściowe, 3) urządzenie wyjściowe sterujące elementem wykonawczym (np. silnikiem).

Urządzenia wykrywające

Obecność osób wchodzących do strefy zagrożenia lub znajdujących się w niej można wykrywać przy użyciu wielu różnych urządzeń. Wybór rozwiązania najbardziej odpowiedniego do konkretnego zastosowania zależy od wielu czynników.

- Czynniki środowiskowe, które mogą wpływać na niezawodność detektora
- Częstotliwość dostępu,
- Czas zatrzymania zagrożenia,
- Ważność zakończenia cyklu maszyny, oraz
- Zapobieganie rozrzutowi odłamków i wydostawaniu się płynów, aerozoli,oparów itp.

Przed odłamkami, płynami, parami oraz innymi typami zagrożeń można zabezpieczyć się, stosując odpowiednio dobrane blokujące osłony ruchome, które są często stosowane, gdy dostęp do zagrożenia jest rzadki. Osłony blokujące można również zaryglować, by uniemożliwić dostęp do maszyny, która znajduje się w środku cyklu pracy lub jej zatrzymanie wymaga długiego czasu.

Jeśli wymagany jest częsty i szybki dostęp operatora do strefy zagrożenia, stosuje się zwykle urządzenia wykrywające obecność, takie jak kurtyny świetlne, maty lub skanery laserowe. Urządzenia tego typu nie zapewniają jednak ochrony przed odłamkami, parami, płynami oraz innymi typami zagrożeń.

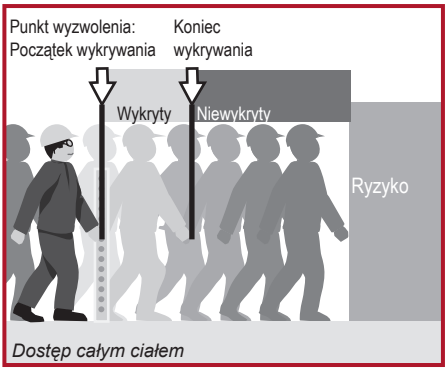
Najlepszym środkiem ochronnym jest urządzenie lub system zapewniający maksymalną ochronę, przy minimalnym utrudnieniu normalnej pracy maszyny. Należy wziąć pod uwagę wszystkie aspekty maszyny, ponieważ doświadczenie uczy, że systemy trudne w obsłudze są bardziej narażone na demontaż lub ominięcie.

Urządzenia wykrywające obecność

Specyfikacja techniczna IEC TS 62046 dostarcza użytecznych wskazówek w zakresie urządzeń wykrywających obecność. Jej stosowanie jest zalecane.Decydując się na ochronę strefy lub obszaru, należy mieć pełną wiedzę na temat wymaganych funkcji bezpieczeństwa. Zazwyczaj występować będą co najmniej dwie funkcje.

- Wyłączenie lub odcięcie zasilania, gdy osoba wejdzie do strefy zagrożenia.
- Uniemożliwienie załączenia lub zezwolenia na zasilanie, gdy osoba znajduje się w strefie zagrożenia.

Na pierwszy rzut oka może się wydawać, że czynności te są identyczne, jednakże pomimo ich oczywistego wzajemnego związku i realizacji za pomocą tych samych urządzeń, stanowią one dwie osobne funkcje zabezpieczające. Do uzyskania pierwszej z nich potrzebne jest urządzenie wyzwalające. Jest to urządzenie, które wykrywa przekroczenie określonego punktu przez część ciała osoby, a następnie wysyła sygnał do wyłączenia zasilania. Jeśli osoba całkowicie przekroczy punkt wyzwalający i jej obecność nie jest już wykrywana, to druga funkcja (zapobieganie załączeniu) może nie zostać zrealizowana.



Na rysunku zilustrowano przykład pełnego dostępu, gdy urządzeniem wyzwalającym jest zamontowana pionowo kurtyna świetlna. Osłony blokujące są również jedynie urządzeniami wyzwalającymi, jeśli nie ma żadnego zabezpieczenia przed zamknięciem osłony po wejściu.

Jeśli pełny dostęp nie jest możliwy i osoba nie może przekroczyć całkowicie punktu wyzwalającego, jej obecność będzie zawsze wykryta i druga funkcja (zapobieganie załączeniu) będzie zrealizowana. W przypadku dostępu częściowego wyzwalanie i wykrywanie obecności jest realizowane przez ten sam typ urządzeń. Jedyną różnicą jest rodzaj aplikacji.

Urządzenia wykrywające obecność służą do wykrywania obecności osób. Do rodziny tych urządzeń należą kurtyny świetlne, jednowiązkowe bariery świetlne, skanery laserowe i maty bezpieczeństwa. Dla wszystkich urządzeń wykrywających obecność wielkość strefy wykrywania i miejsce instalacji urządzenia muszą uwzględniać wymaganą odległość bezpieczną.

Kurtyny świetlne bezpieczeństwa

Kurtyny świetlne bezpieczeństwa są to po prostu fotoelektryczne czujniki obecności, zaprojektowane do ochrony personelu przed obrażeniami związanymi z niebezpiecznym ruchem maszyny. Znane również jako aktywne optoelektroniczne urządzenia ochronne (AOPD) lub wyposażenie elektroczułe (ESPE), kurtyny świetlne zapewniają optymalny poziom bezpieczeństwa i umożliwiają zwiększenie wydajności. Kurtyny świetlne są idealnie do zastosowań, w których wymagany jest częsty i łatwy dostęp personelu do stanowiska roboczego z zagrożeniem.
Kurtyny świetlne są projektowane i testowane zgodnie z IEC 61496-1 i IEC 61496-2.

Laserowe skanery bezpieczeństwa

Laserowe skanery bezpieczeństwa używają zwierciadła wirującego do odchylania impulsów świetlnych, co tworzy płaszczyznę wykrywania. Położenie obiektu jest określane na podstawie kąta obrotu zwierciadła. Korzystając z techniki „czasu przelotu”

(time-of-flight) odchylonego niewidzialnego promienia światła, skaner może również określić w jakiej odległości znajduje się wykryty obiekt. Znając odległość oraz położenie obiektu, skaner laserowy może wyznaczyć jego dokładne położenie w strefie.

Maty bezpieczeństwa czułe na nacisk

Urządzenia te są używane do ochrony obszaru podłoża wokół maszyny. Sieć wzajemnie połączonych mat układana wokół strefy zagrożenia. Jeśli mata zostanie naciśnięta (np. wejdzie na nią operator), moduł sterowania wyłączy zasilanie strefy niebezpiecznej. Maty czułe na nacisk są często stosowane w strefach zamkniętych z wieloma maszynami, w elastycznych systemach wytwarzania lub gniazdach robotów. Jeśli wymagany jest dostęp do gniazda (np. w celu zmiany ustawień lub „uczenia" robota), eliminują one niebezpieczny ruch w przypadku, gdy operator opuści strefę bezpieczną. Bardzo istotne jest unieruchomienie mat(y) za pomocą właściwych i bezpiecznych mocowań.

Listwy czułe na nacisk

Urządzenia tego typu to elastyczne listwy, które można montować na krawędziach ruchomych części, takich jak stoły maszynowe lub drzwi mechaniczne, które stwarzają ryzyko zmiażdżenia lub obcięcia.

Jeśli ruchoma część uderzy operatora (lub odwrotnie), jednocześnie zostanie wciśnięta listwa elastyczna, a to spowoduje aktywację polecenia wyłączenia zasilania zagrożenia. Listwy czułe na nacisk można także stosować do zabezpieczenia maszyn, w których występuje ryzyko uwięzienia. Jeśli operator zostanie pochwycony przez maszynę, dotknięcie listwy spowoduje wyłączenie zasilania maszyny.

Kurtyny świetlne, skanery, maty podłogowe i listwy czułe na nacisk są określane mianem „urządzeń wyzwalających". Nie ograniczają one dostępu, lecz jedynie go „wykrywają". Bezpieczeństwo ich działania polega na możliwości zarówno wykrywania, jak i wyłączania. Nadają się zasadniczo wyłącznie do zastosowania na maszynach, których mogą być szybko zatrzymanie po wyłączeniu zasilania. Ponieważ operator może bezpośrednio wejść lub sięgnąć do strefy zagrożenia, oczywiste jest, że czas niezbędny do zatrzymania maszyny musi być krótszy od czasu, w którym operator może wejść w kontakt z zagrożeniem po aktywacji urządzenia wyzwalającego.

Wyłączniki bezpieczeństwa

Jeśli dostęp do maszyny potrzebny jest rzadko lub w przypadku, gdy zachodzi możliwość wyrzucenia części, często preferowane są osłony ruchome (robocze). Osłona blokuje źródło zasilania zagrożenia, aby w sytuacji pozostawienia otwartych drzwi zasilanie to zostało wyłączone.

Podejście to wymaga zastosowania wyłącznika blokującego na osłonie. Sygnał sterowania źródła zasilania zagrożenia przechodzi przez wyjścia wyłącznika. Źródło zasilania jest zazwyczaj elektryczne, jednak występują również źródła pneumatyczne lub hydrauliczne. W przypadku wykrycia ruchu (otwarcia) osłony wyłącznik blokujący

aktywuje polecenie wyłączenia zasilania strefy zagrożenia, bezpośrednio lub przez stycznik mocy (lub zawór).

Niektóre wyłączniki blokujące mają wbudowane urządzenie ryglujące osłonę w położeniu zamkniętym, pozwalające na otwarcie osłony wyłącznie wtedy, gdy maszyna jest w trybie bezpiecznym.

W przypadku większości zastosowań kombinacja osłony ruchomej i wyłącznika blokującego z ryglowaniem lub bez ryglowania jest najbardziej niezawodnym i oszczędnym rozwiązaniem. Norma EN ISO 14119 dostarcza użytecznych wskazówek odnośnie do wyboru wszystkich typów urządzeń blokujących osłon. Jej stosowanie jest zalecane.

Dostępnych jest wiele różnych wyłączników bezpieczeństwa obejmujących:

- **Wyłączniki blokujące językowe** – urządzenia te wymagają elementu wykonawczego w kształcie języka, który jest wsuwany i wyjmowany z wyłącznika

- **Wyłączniki blokujące zawiasowe** – urządzenia te są umieszczane na zawiasach osłon i do aktywacji wykorzystują otwarcie osłony.

- **Wyłączniki ryglujące** – niekiedy wymagane jest ryglowanie osłony w położeniu zamkniętym lub opóźnianie możliwości otwarcia osłony. Stosowane są wtedy urządzenia nazywane wyłącznikami blokującymi z ryglowaniem. Są one odpowiednie dla maszyn o długim czasie wybiegu, ale mogą także znacząco poprawić poziom bezpieczeństwa większości rodzajów maszyn.

- **Wyłączniki blokujące bezkontaktowe** – do aktywacji tych urządzeń nie jest wymagany kontakt fizyczny. Niektóre typy mają wbudowaną funkcję kodowania zapewniającą większą odporność na próby ominięcia zabezpieczenia.

- **Wyłączniki pozycyjne (krańcowe)** – wyzwalane są zazwyczaj za pomocą krzywki liniowej lub obrotowej popychającej wyłącznik krańcowy w trybie wymuszonym. Zazwyczaj stosuje się je na osłonach przesuwnych.

- **Blokady z zamkami sekwencyjnymi** – zamki takie realizują blokowanie sterowania jak i blokowanie zasilania. W przypadku „blokowania sterowania” urządzenie wysyła polecenie zatrzymania do urządzenia pośredniczącego, a te wyłącza urządzenie końcowe, odłączając zasilanie od urządzenia wykonawczego. „Blokowanie zasilania” polega na tym, że polecenie zatrzymania bezpośrednio wyłącza zasilanie urządzeń wykonawczych maszyny.

Urządzenia interfejsu operatora

Funkcja zatrzymania – opisy kategorii zatrzymywania maszyn i systemów produkcyjnych zostały uwzględnione w normach zharmonizowanych, obowiązujących w USA, Kanadzie, Europie oraz na poziomie międzynarodowym.

UWAGA: Kategorie te różnią się od kategorii określonych w normie ISO 13849-1. Szczegółowe informacje można znaleźć w normach NFPA 79 i IEC/EN 60204-1. Typy zatrzymania podzielono na trzy kategorie:

Kategoria 0 oznacza zatrzymanie przez natychmiastowe odłączenie zasilania od napędów maszyny. Jest to równoznaczne z zatrzymaniem niekontrolowanym. Po odłączeniu zasilania hamowanie wymagające zasilania nie będzie działać. Oznacza to, że silniki będą w wybiegu i zatrzymają się po dłuższym czasie. Innymi słowy, materiał może zostać upuszczony przez uchwyty maszyny, które wymagają zasilania do jego utrzymania. Mechaniczne środki zatrzymania (hamulce) niewymagające zasilania mogą być także zastosowane do zatrzymania kategorii 0. Zatrzymanie kategorii 0 ma pierwszeństwo przed zatrzymaniem kategorii 1 i 2.

Kategoria 1 to zatrzymanie kontrolowane, w którym do momentu zatrzymania napędy maszyny muszą pozostać zasilone. Zasilanie napędów zostaje odłączone dopiero po zatrzymaniu. Ta kategoria zatrzymywania pozwala na hamowanie w celu szybkiego zatrzymania ruchu niebezpiecznego, a następnie odłączenie zasilania od napędów. Ten rodzaj zatrzymania umożliwia szybsze i bardziej kontrolowane zatrzymanie, z którego ponowne uruchomienie może nastąpić w krótszym czasie. UWAGA: W wydaniu normy IEC 60204-1 z 2016 roku liczba rodzajów zatrzymania kategorii 1 zostaje zwiększona.

Kategoria 2 to zatrzymanie kontrolowane przy pozostawieniu zasilania napędów maszyny. Kategoria 2 to normalne zatrzymanie produkcyjne.

Każde zatrzymywanie powinno być jedną z wymienionych wyżej kategorii. Funkcja zatrzymywania to czynność wykonywana przez elementy systemu sterowania związane z bezpieczeństwem w odpowiedzi na sygnał wejściowy. Należy stosować zatrzymania kategorii 0 lub 1. Funkcje zatrzymywania muszą mieć pierwszeństwo przed funkcjami uruchamiania. Wybór kategorii dla każdej funkcji zatrzymania powinien być określony na podstawie oceny ryzyka.

Funkcja zatrzymywania awaryjnego

Funkcja zatrzymywania awaryjnego musi działać jako kategoria zatrzymywania 0 lub 1 i być określona przez ocenę ryzyka. Załączenie funkcji musi być wywołane działaniem człowieka. Uaktywniona funkcja powinna mieć pierwszeństwo przed innymi funkcjami i działaniami we wszystkich trybach pracy maszyny. Jej celem jest możliwie najszybsze odłączenie zasilania, bez spowodowania dodatkowego zagrożenia. Wszędzie tam, gdzie występuje zagrożenie dla operatora, należy zapewnić łatwy dostęp do urządzenia zatrzymywania awaryjnego. Musi ono być zawsze gotowe do działania i łatwo dostępne. Pulpity sterownicze operatorów powinny zawierać co najmniej jedno urządzenie zatrzymania awaryjnego. W razie potrzeby dodatkowe urządzenia zatrzymywania awaryjnego można również umieszczać w innych miejscach. Istnieją różne rodzaje urządzeń zatrzymywania awaryjnego. Przykładem najczęściej spotykanych są przyciski i wyłączniki linkowe.

Do niedawna w obwodach zatrzymywania awaryjnego wymagane było stosowanie elementów elektromechanicznych. Z najnowszych zmian w normach takich jak IEC 60204-1 i NFPA 79 wynika, że w obwodach zatrzymywania awaryjnego można wykorzystywać sterowniki PLC oraz inne typy elektronicznych elementów logicznych, spełniające wymagania norm takich jak IEC 61508.

Urządzenia zatrzymania awaryjnego są uzupełniającym sprzętem ochronnym. Nie mogą być traktowane jak podstawowe urządzenia ochronne, ponieważ nie zapobiegają dostępowi do zagrożenia, ani nie wykrywają dostępu do zagrożenia. Są one zależne od interakcji z człowiekiem.

Dalsze informacje na temat wyłączników awaryjnych można znaleźć w normach ISO/EN 13850, IEC 60947-5-5, NFPA 79 i IEC 60204-1 oraz AS4024.1 i Z432-94.

Przyciski zatrzymania awaryjnego

Przycisk używany jako urządzenie stopu awaryjnego musi mieć kształt grzybka, kolor czerwony i żółte tło. Gdy urządzenie stopu awaryjnego zostanie naciśnięte, musi zatrzasnąć się w tej pozycji. Polecenie zatrzymania nie może być generowane bez zatrzaśnięcia. Zresetowanie urządzenia stopu awaryjnego nie może wywołać sytuacji niebezpiecznej. Restart maszyny powinien wymagać zastosowania oddzielnych i zamierzonych czynności.

Jedną z najnowszych technik stosowanych w przypadku urządzeń zatrzymania awaryjnego jest samonadzorowanie. Do przycisku montowany jest dodatkowy zestyk, który nadzoruje, czy elementy z tyłu panelu nadal znajdują się na swoich miejscach. Funkcja jest znana jako blok zestyków z samonadzorowaniem. Zawiera zestyk, który zamyka się po zatrzaśnięcia bloku zestyków na panelu.

Wyłączniki linkowe

W przypadku maszyn takich jak przenośniki często znacznie wygodniejsze i bardziej efektywne jest zastosowanie wyłącznika linkowego wzdłuż strefy zagrożenia jako urządzenia zatrzymywania awaryjnego. Urządzenia tego typu używają stalowej linki dołączonej do zatrzaskowego wyłącznika. Chwycenie linki w dowolnym miejscu i pociągnięcie w dowolnym kierunku powoduje aktywację wyłącznika i odłączenie zasilania od maszyny.

Wyłączniki linkowe muszą wykrywać zarówno pociągnięcie linki, jak również jej poluzowanie. Wykrywanie luzu linki daje pewność, że nie została ona przerwana i nadal jest gotowa do użycia.

Długość linki wpływa na działanie wyłącznika. Dla małych odległości wyłącznik montowany jest tylko na jednym końcu linki. Z drugiej strony montuje się sprężynę napinającą. Jeśli odległości są duże, wyłącznik musi być montowany na obu końcach. Dzięki temu do aktywacji polecenia zatrzymania wystarczy jedno działanie. Bardzo ważne jest użycie właściwie umiejscowionych śrub oczkowych do podwieszenia i

prowadzenia linki. Wymagana wartość siły rozciągającej linki nie powinna przekraczać 200 N na dystansie 400 mm w punkcie środkowym pomiędzy dwiema śrubami oczkowymi. W celu zapewnienia prawidłowego działania należy stosować się do zaleceń producenta.

Urządzenia sterowania oburęcznego

Zastosowanie urządzeń sterowania oburęcznego to popularna metoda zapobiegania dostępu do maszyny, która pracuje w niebezpiecznych warunkach. Do uruchomienia maszyny wymagane jest jednoczesne (w odstępie do 0,5 s) naciśnięcie dwóch elementów. To zapewnia, że obie dłonie operatora znajdują się w bezpiecznym miejscu (tj. na elementach sterowania), z dala od strefy zagrożenia. W warunkach niebezpiecznych elementy sterowania muszą być ciągle naciskane. Jeśli którykolwiek element zostanie zwolniony, maszyna musi zatrzymać pracę, a przed ponownym uruchomieniem maszyny należy również zwolnić drugi element. Powoduje to wymuszenie zabezpieczenia i zapobiega samowolnemu zastąpieniu czynności wykonywanej dwoma rękami przez czynność wykonywaną jedną ręką.

Efektywność oburęcznego systemu sterowania zależy mocno od niezawodności jego elementów oraz nadzorowania defektów. Warto zatem dopilnować, aby te aspekty zostały zaprojektowane zgodnie z odpowiednimi wymaganiami. Działanie oburęcznego systemu bezpieczeństwa jest podzielone w ISO 13851 (EN 574) na typy powiązane z kategoriami normy ISO 13849-1. Najczęściej wykorzystywane są typy IIIB oraz IIIC. Związek typów z kategoriami bezpieczeństwa przedstawiono w poniższej tabeli.

Wymagania	**Typy**				
	I	**II**	**III**		
			A	**B**	**C**
Aktywacja jednoczesna			X	X	X
Zastosowanie kategorii 1 (wg normy ISO 13849-1)	X		X		
Zastosowanie kategorii 3 (wg normy ISO 13849-1)		X		X	
Zastosowanie kategorii 4 (wg normy ISO 13849-1)					X

Tabela wymogów z normy ISO 13851

Wymiary fizyczne należy zaprojektować w sposób zapobiegający nieprawidłowej obsłudze (np. ręką i łokciem). Cel ten można osiągnąć przez odsunięcie lub osłony. Maszyna nie powinna przechodzić z jednego cyklu do kolejnego bez uprzedniego zwolnienia i naciśnięcia obu przycisków. Rozwiązanie takie przerywa powtarzalność cyklu i zapobiega możliwości zablokowania obu przycisków i w rezultacie przestawieniu maszyny na tryb pracy ciągłej. Zwolnienie dowolnego przycisku musi powodować zatrzymanie maszyny.

Zastosowanie urządzenia sterowania oburęcznego należy dokładnie przemyśleć, ponieważ zazwyczaj wiąże się z nimi pewien poziom ryzyka. Sterowanie oburęczne chroni tylko osobę, która z niego korzysta. Chroniony operator musi obserwować każdą próbę dostępu do zagrożenia, ponieważ pozostali pracownicy mogą nie być objęci ochroną.

Dodatkowe wytyczne odnoszące się do urządzeń sterowania oburęcznego znajdują się w normie ISO 13851 (EN 574).

Urządzenia zezwalające

Urządzenia zezwalające to elementy sterowania będące częścią strategii umożliwiającej operatorowi wejście do strefy zagrożenia w czasie pracy maszyny tylko w przypadku, gdy napędy pracują z bezpieczną prędkością, a operator trzyma w ręku aktywne urządzenie zezwalające. Urządzenia zezwalające to zwykle łączniki dwu- lub trójpozycyjne. Łącznik dwupozycyjny jest wyłączony, gdy nie jest wciśnięty, a załącza się po naciśnięciu. Łączniki trójpozycyjne są wyłączone, gdy nie są naciśnięte (pozycja 1), załączone po naciśnięciu do położenia środkowego (pozycja 2) oraz wyłączone po naciśnięciu poza położenie środkowe (pozycja 3). Oprócz tego, w przypadku powrotu z pozycji 3 do 1, obwód wyjściowy nie może zostać zamknięty przy przejściu przez pozycję 2.

Urządzenia zezwalające należy stosować w połączeniu z innymi funkcjami związanymi z bezpieczeństwem. Typowym przykładem jest ustawienie ruchu w nadzorowanym trybie pracy powolnej. Podczas korzystania z urządzenia zezwalającego musi być nadawany sygnał, informujący o aktywności urządzenia.

Urządzenia logiki

Urządzenia logiki są kluczowym elementem systemu sterowania związanego z bezpieczeństwem. Realizują one funkcje sprawdzania i monitorowania systemu bezpieczeństwa, zezwalając na uruchomienie maszyny lub wykonując polecenia jej zatrzymania.

Różne urządzenia logiki są wykorzystywane do tworzenia bezpiecznych architektur, spełniających wymogi złożoności i funkcjonalności maszyny. Małe oprzewodowane na stałe przekaźniki bezpieczeństwa są najbardziej ekonomicznym rozwiązaniem dla małych maszyn, dla których dedykowane urządzenie logiczne jest wystarczające do zapewnienia funkcji bezpieczeństwa. Modułowe i konfigurowalne przekaźniki bezpieczeństwa są preferowane w zastosowaniach, w których wymagana jest duża liczba różnych urządzeń ochronnych oraz minimalne sterowanie strefowe. W maszynach średnich, dużych i o znacznym stopniu komplikacji najlepszym rozwiązaniem mogą się okazać programowalne systemy bezpieczeństwa z układami rozproszonych wejść/wyjść.

Przekaźniki bezpieczeństwa MSR

Moduły przekaźników bezpieczeństwa MSR (Monitoring Safety Relay) stanowią ważny element wielu systemów bezpieczeństwa. Zawierają one zazwyczaj co najmniej dwa lub więcej przekaźniki o przełączaniu wymuszonym oraz dodatkowe obwody zapewniające działanie funkcji bezpieczeństwa.

Konstrukcja przekaźników o wymuszonym przełączaniu zapobiega jednoczesnemu zamknięciu zestyków zwiernych i zestyków rozwiernych. Niektóre przekaźniki MSR są wyposażone w półprzewodnikowe wyjścia bezpieczeństwa.

Przekaźniki bezpieczeństwa realizują w systemie bezpieczeństwa wiele funkcji sprawdzających. Po załączeniu zasilania wykonują test elementów wewnętrznych. Po aktywacji urządzeń wejściowych, porównują stan wejść redundantnych. Jeżeli jest to dopuszczalne, przekaźnik bezpieczeństwa MSR sprawdza elementy wykonawcze podłączone do jego wyjść. Jeśli wynik jest prawidłowy, przekaźnik oczekuje na sygnał resetowania, aby aktywować wyjścia. Dlatego też prawidłowo wybrany i skonfigurowany przekaźnik MSR może wykrywać błędy systemu, sprawdzając podłączone do niego urządzenia wejścia i wyjścia. Może również stanowić element blokujący uruchomienie lub restart

Wybór odpowiedniego przekaźnika bezpieczeństwa zależy od czynników takich jak: typ monitorowanego urządzenia, typ resetowania, liczba i typ wyjść itp.

Typy wejść w przekaźnikach bezpieczeństwa MSR

Różne typy urządzeń ochronych wymagają odmiennych sygnałów wejściowych dla przekaźników bezpieczeństwa MSR, dlatego też bardzo ważne jest sprawdzenie kompatybilności. Poniżej przedstawiono krótkie podsumowanie możliwych rodzajów urządzeń wejściowych wraz z wymaganiami wykrywania zwarć międzykanałowych.

Wyłączniki blokujące elektromechaniczne, niektóre wyłączniki blokujące bezkontaktowe, urządzenia stopu awaryjnego: zestyki mechaniczne, jednokanałowe, z jednym zestykiem rozwiernym lub dwukanałowe, z dwoma zestykami rozwiernymi. Przekaźnik bezpieczeństwa MSR powinien obsługiwać jeden lub dwa kanały i zapewniać wykrywanie zwarć międzykanałowych w konfiguracjach dwukanałowych.

Niektóre wyłączniki blokujące bezkontaktowe i urządzenia stopu awaryjnego: zestyki mechaniczne, dwukanałowe z jednym zestykiem zwiernym i jednym zestykiem rozwiernym. Przekaźnik musi zapewniać przetwarzanie wejść różnicowych.

Urządzenia z wyjściami półprzewodnikowymi: kurtyny świetlne, skanery laserowe i niektóre bezkontaktowe wyłączniki blokujące posiadają dwa wyjścia dostarczające prąd i same wykrywają zwarcia międzykanałowe. Przekaźnik MSR musi mieć możliwość ignorowania zwarć międzykanałowych.

Maty czułe na nacisk: maty stanowią obwód zwierający dwa kanały. Przekaźnik bezpieczeństwa MSR musi być specjalnie zaprojektowany i skonfigurowany dla tego zastosowania.

Listwy czułe na nacisk: niektóre listwy są zaprojektowane jak maty 4-przewodowe. Inne to urządzenia dwuprzewodowe o zmiennej rezystancji. Przekaźnik MSR musi wykrywać zwarcie obwodu lub zmianę rezystancji.

Wykrywanie ruchu silnika: wykorzystuje pomiar siły przeciwelektromotorycznej silnika podczas wybiegu. Przekaźnik musi być odporny na wysokie napięcia oraz wykrywać niskie napięcia indukowane podczas wybiegu.

Wykrywanie zatrzymywania: przekaźnik musi wykrywać impulsy z różnych redundantnych czujników.

Sterowanie oburęczne: przekaźnik musi wykrywać różnicowe wejścia normalnie otwarte i normalnie zamknięte, a także zapewnić kontrolę jednoczesności do 0,5 s oraz obsługę sekwencji logiki.

Przekaźniki bezpieczeństwa MSR mogą być zaprojektowane indywidualnie lub skonfigurowane do pracy z każdym z wymienionych typów urządzenia. Wynika to z faktu, że każdy z nich ma inną charakterystykę elektryczną. Niektóre z przekaźników MSR można całkowicie przekonfigurować na inne typy działania. Do niektórych przekaźników MSR można podłączać różne typy urządzeń wejściowych, ale gdy tylko urządzenie zostanie wybrane, MSR może współdziałać tylko z nim. Projektant powinien zatem wybrać lub skonfigurować przekaźnik zgodny z urządzeniem wejściowym.

Impedancja wejściowa

Impedancja wejściowa przekaźników bezpieczeństwa określa liczbę urządzeń wejściowych, które można podłączyć do przekaźnika oraz odległość montażu tych urządzeń. Na przykład, przekaźnik bezpieczeństwa może mieć maksymalną dopuszczalną impedancję wejściową równą 500 omów. Jeśli impedancja będzie większa niż 500 omów, wyjścia przekaźnika nie zostaną załączone. W związku z tym użytkownik powinien upewnić się, że wartość impedancji wejściowej jest mniejsza od maksymalnej określonej w danych technicznych. Impedancja wejściowa zależy od długości, rozmiaru i typu użytego przewodu.

Liczba urządzeń wejściowych

Do określenia liczby urządzeń wejściowych podłączonych do przekaźnika MSR oraz częstotliwości ich sprawdzania powinna być zastosowana procedura oceny ryzyka. Aby mieć pewność, że urządzenia zatrzymania awaryjnego i osłony blokujące są sprawne, ich działanie powinno być sprawdzane w regularnych odstępach czasu, określonych przez ocenę ryzyka. Np. osłona blokująca podłączona do dwukanałowego wejścia przekaźnika MSR, która otwierana jest w każdym cyklu pracy maszyny (np. wiele razy dziennie), w ogóle nie musi być sprawdzana. Wynika to z faktu, że otwieranie osłony powoduje wykonanie przez przekaźnik MSR sprawdzenia wejść i wyjść (zależnie od konfiguracji), wykrywające pojedyncze defekty. Im częściej osłona jest otwierana, tym lepsza nienaruszalność procesu sprawdzania.

Innym przykładem są przyciski stopu awaryjnego. Ponieważ zaprojektowano je z myślą o sytuacjach awaryjnych, nie są one używane zbyt często. Dlatego też należy opracować i wdrożyć program okresowego sprawdzania przycisków stopu awaryjnego w celu potwierdzania ich sprawności. Taka operacja wykonana na systemie bezpieczeństwa jest określana jako przeprowadzenie testu funkcjonalnego. Trzecim przykładem są drzwi dostępu do układu regulacji maszyny, które – podobnie jak przyciski stopu awaryjnego – mogą być rzadko uży-

wane. Również w tym przypadku powinien zostać opracowany program przeprowadzania testów funkcjonalnych zgodnie z harmonogramem.

Konieczność sprawdzania urządzeń wejściowych oraz częstotliwość wykonywania testów określana jest przez ocenę ryzyka. Im większy poziom ryzyka, tym większa wymagana nienaruszalność procesu sprawdzania. Im rzadziej wykonywane jest sprawdzanie „automatyczne", tym częściej należy wykonywać sprawdzanie „ręczne".

Wykrywanie zwarcia międzykanałowego na wejściu

W układach dwukanałowych zwarcia międzykanałowe w urządzeniach wejściowych muszą być wykrywane przez system bezpieczeństwa. Realizowane jest to przez urządzenie wejściowe lub przekaźnik bezpieczeństwa.

Mikroprocesorowe przekaźniki bezpieczeństwa, a także kurtyny świetlne, skanery laserowe czy zaawansowane czujniki bezkontaktowe, wykrywają wymienione wyżej zwarcia na różne sposoby. Typowym sposobem wykrywania zwarć międzykanałowych jest testowanie impulsowe. Sygnały wejściowe przekaźnika MSR są impulsami o wysokiej częstotliwości. Impulsy kanału 1 jest przesunięte względem impulsów kanału 2. W przypadku zwarcia, impulsy pojawią się jednocześnie i są wykrywane przez urządzenie.

W elektromechanicznych przekaźnikach bezpieczeństwa wykorzystuje się inną technikę: jedno wejście ma przeciwną polaryzację niż wejście drugie, a drugie wejście jest obniżające. Zwarcie kanału 1 do kanału 2 powoduje zadziałanie zabezpieczenia nadprądowego i wyłączenie systemu bezpieczeństwa.

Wyjścia

Przekaźniki MSR mogą mieć różną liczbę wyjść. Typ wyjść pomaga określić jaki typ przekaźnika MSR, należy zastosować w konkretnej aplikacji.

Przekaźniki MSR mają co najmniej 2 bezzwłoczne wyjścia bezpieczeństwa. Wyjścia bezpieczeństwa są typu normalnie otwartego. Spełniają one wymogi bezpieczeństwa dzięki redundancji i testowaniu wewnętrznemu. Drugi typ wyjść to wyjścia zwłoczne. Są one zazwyczaj wykorzystywane do zatrzymania kategorii 1, gdy maszyna wymaga czasu na wykonanie procedury zatrzymania, zanim udzielone zostanie zezwolenie na wejście do strefy zagrożenia. W przekaźniki MSR mają także wyjścia pomocnicze. Zazwyczaj są one typu normalnie zamkniętego.

Parametry wyjścia

Parametry wyjścia określają zdolność urządzenia ochronnego do łączenia obciążeń. Dla urządzeń przemysłowych podawane są wartości dla obciążeń rezystancyjnych lub elektromagnetycznych. Obciążeniem rezystancyjnym może być element typu grzejnik. Obciążenia elektromagnetyczne to elementy charakteryzujące się dużą indukcyjnością, takie jak przekaźniki, styczniki lub elektrozawory. Parametry znamionowe dla obciążeń przedstawiono w załączniku A normy IEC 60947-5-1.

Oznaczenie literowe: po literze występuje liczba, na przykład A300. Litera określa wartość umownego prądu termicznego w obudowie oraz jego rodzaj – stały lub przemienny. Np. litera A oznacza prąd przemienny 10 A. Liczba odnosi się do znamionowego napięcia izolacji. Np. liczba 300 oznacza 300 V.

Kategoria użytkowania: kategoria użytkowania określa typ obciążeń, do których łączenia jest przeznaczone urządzenie. W poniższej tabeli przedstawiono kategorie użytkowania wg IEC 60947-5.

Kategoria użytkowania	Opis typu obciążenia
AC-12	Sterowanie obciążeniami rezystancyjnymi i półprzewodnikowymi z izolacją za pomocą łączników optycznych
AC-13	Sterowanie obciążeniami półprzewodnikowymi z izolacją transformatorową
AC-14	Sterowanie małymi obciążeniami elektromagnetycznymi (poniżej 72 VA)
AC-15	Obciążenia elektromagnetyczne większe niż 72 VA
DC-12	Sterowanie obciążeniami rezystancyjnymi i półprzewodnikowymi z izolacją za pomocą łączników optycznych
DC-13	Sterowanie obciążeniami elektromagnetycznymi
DC-14	Sterowanie obciążeniami elektromagnetycznymi z rezystorami ekonomicznymi

Prąd termiczny, Ith: umowny prąd termiczny w obudowie, to wartość prądu, który wykorzystywany jest do testów przyrostu temperatury wyposażenia zamontowanego w określonej obudowie.

Znamionowe napięcie łączeniowe Ue i znamionowy prąd łączeniowy Ie: Znamionowy łączeniowy prąd i znamionowe łączeniowe napięcie określają zdolność załączania i wyłączania w normalnych warunkach pracy. Typowe napięcia znamionowe produktów z rodziny Allen-Bradley Guardmaster wynoszą 125 V AC, 250 V AC i 24 V DC.

VA: wartości VA (Volt x Amper) określają możliwości elementów łączeniowych do załączania i wyłączania obciążeń.

Przykład 1: Oznaczenie A150, AC-15 wskazuje, że zestyki mogą załączyć obwody o mocy 7200 VA. Przy napięciu 120 V AC zestyki mogą załączyć obwód z prądem rozruchowym 60 A. Ponieważ AC-15 dotyczy obciążeń elektromagnetycznych, prąd rozruchowy obciążenia elektromagnetycznego będzie miał wartość 60 A tylko przez krótki czas. Zdolność wyłączenia obwodu to tylko 720 VA, ponieważ prąd ustalony obciążenia elektromagnetycznego wynosi 6 A i jest równy znamionowemu prądowi łączeniowemu.

Przykład 2: Oznaczenie N150, DC-13 wskazuje, że zestyki mogą załączać obwody o mocy 275 VA. Przy napięciu 125 V AC zestyki mogą załączyć z prądem 2,2 A. Obciążenia elektromagnetyczne prądu stałego nie mają prądu rozruchowego w przeciwieństwie do obciążeń elektromagnetycznych prądu zmiennego. Zdolność wyłączenia obwodu to również 275 VA, ponieważ prąd ustalony obciążenia elektromagnetycznego wynosi 2,2 A i jest równy znamionowemu prądowi łączeniowemu.

Ponowne uruchomienie maszyny

Jeśli w działającej maszynie zostanie otwarta osłona blokująca, wyłącznik blokujący bezpieczeństwa zatrzyma maszynę. W większości przypadków koniecznym jest, aby zamknięcie osłony nie powodowało natychmiastowego restartu maszyny. Najpopularniejszym sposobem realizacji tego jest zastosowanie układu podtrzymania stycznika.

Naciśnięcie i zwolnienie przycisku start powoduje natychmiastowe wzbudzenie cewki stycznika, który zamyka zestyki główne. Prąd będzie płynął przez zestyki główne, gdy cewka będzie zasilania (podtrzymana elektrycznie) przez zestyk pomocniczy stycznika, który jest mechanicznie połączony z zestykami głównymi. Zanik zasilania głównego lub sterowania powoduje wyłączenie cewki i otwarcie głównego obwodu zasilającego oraz zestyków pomocniczych. Osłona blokująca jest podłączona do obwodu sterowania stycznika. Oznacza to, że w celu ponownego uruchomienia maszyny należy najpierw zamknąć osłonę, a następnie nacisnąć przycisk startu normalnego w położenie „ON” (ZAŁ.), co spowoduje zresetowanie stycznika i uruchomienie maszyny.

Warunki dotyczące funkcji blokującej zostały omówione w normie ISO 12100 (wyciąg):

„Gdy osłona jest zamknięta, niebezpieczne funkcje maszyny chronione przez osłonę mogą działać, ale zamknięcie osłony nie może samo w sobie inicjować tego działania”.

W wielu maszynach opisane wyżej funkcje są realizowane przez zastosowanie styczników pojedynczych lub podwójnych (albo systemów zapewniających takie samo działanie). Podczas montażu blokady w istniejącej maszynie należy określić, czy układ sterowania napięciem spełnia te wymagania. W razie potrzeby trzeba zastosować dodatkowe środki.

Funkcje resetowania

W przekaźnikach bezpieczeństwa Allen-Bradley Guardmaster stosowane są funkcje nadzorowanego resetu ręcznego lub resetu automatycznego/ręcznego.

Nadzorowany reset ręczny

W przypadku nadzorowanego resetu ręcznego wymagana jest zmiana stanu obwodu resetującego po zamknięciu osłony lub odblokowaniu przycisku stopu awaryjnego. Połączone mechanicznie rozwierne zestyki pomocnicze styczników mocy są podłączone szeregowo z przyciskiem impulsowym. Po otwarciu i ponownym zamknięciu osłony

przekaźnik bezpieczeństwa nie zezwala na ponowne uruchomienie maszyny, dopóki nie zostanie wciśnięty i zwolniony przycisk resetu. Jest to zgodne z dodatkowym wymaganiem dla resetu ręcznego wg normy EN ISO 13849-1, zgodnie z którymi funkcja resetowania zapewnia, że oba styczniki są WYŁĄCZONE oraz oba obwody blokujące (a w związku z tym także osłony) są zamknięte, jak również (ponieważ wymagana jest zmiana stanu) przycisk resetu nie został w żaden sposób ominięty ani zablokowany (na stałe). W przypadku pomyślnych wyników sprawdzeń maszyna może być uruchomiona ponownie za pomocą normalnych elementów sterowania. Norma EN ISO 13849-1 wymienia zmianę stanu przycisku z naciśniętego na nienaciśnięty (zbocze opadające).

Przycisk resetu powinien znajdować się w miejscu zapewniającym dobrą widoczność strefy zagrożenia. Dzięki temu operator będzie mógł sprawdzić obszar przed rozpoczęciem pracy.

Reset automatyczny/ręczny

Niektóre przekaźniki bezpieczeństwa mają reset automatyczny/ręczny. Tryb resetu ręcznego nie jest monitorowany, co oznacza, że reset następuje przez naciśnięcie przycisku. Zwarcie obwodu lub zacięcie się przycisku nie zostaną wykryte. Przy tym podejściu spełnienie dodatkowego wymagania dla resetu ręcznego wg normy EN ISO 13849-1 może okazać się niemożliwe, jeśli nie zostaną zastosowane dodatkowe środki.

Obwód resetu może być zwarty zworą pozwalając na reset automatyczny. Użytkownik musi zapewnić inny mechanizm zapobiegający uruchamianiu maszyny po zamknięciu osłony.

Urządzenie z resetem automatycznym nie wymaga ręcznego przełączania, ale po dezaktywacji, zawsze przeprowadzane jest sprawdzenie nienaruszalności systemu przed wykonaniem resetu. System z resetem automatycznym nie powinien być mylony z urządzeniem, które nie ma funkcji resetu. W przypadku tych drugich system bezpieczeństwa jest załączany natychmiast po dezaktywacji, ale sprawdzenie nienaruszalności systemu nie jest przeprowadzane.

Przycisk resetu powinien znajdować się w miejscu zapewniającym dobrą widoczność strefy zagrożenia. Dzięki temu operator będzie mógł sprawdzić obszar przed rozpoczęciem pracy.

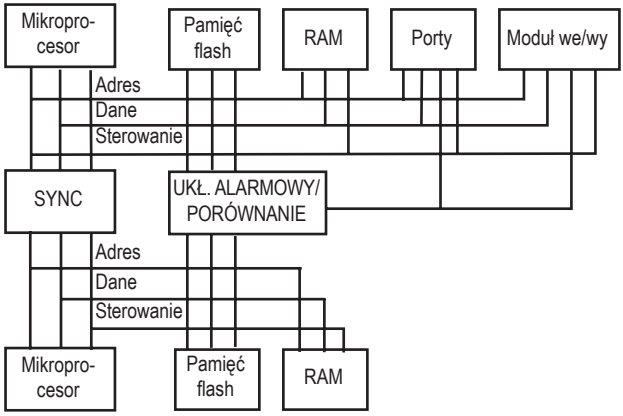
Osłony sterujące

Osłona sterująca zatrzymuje maszynę po otwarciu osłony i natychmiast uruchamia maszynę po zamknięciu osłony. Zastosowanie osłon sterujących jest dozwolone pod rygorystycznymi warunkami, ponieważ każde nieoczekiwane uruchomienie lub defekt w układzie zatrzymania mogą mieć bardzo niebezpieczne następstwa. System blokujący musi mieć najwyższą możliwą niezawodność (często zaleca się stosowanie ryglowania osłon). Zastosowanie osłon sterujących można brać pod uwagę wyłącznie w przypadku maszyn, w których po zamknięciu osłony operator lub jakakolwiek część jego ciała nie ma możliwości pozostania w strefie zagrożenia lub dostania się do niej. Osłona sterująca powinna być jedyną drogą dostępu do strefy zagrożenia.

Programowalne sterowniki bezpieczeństwa

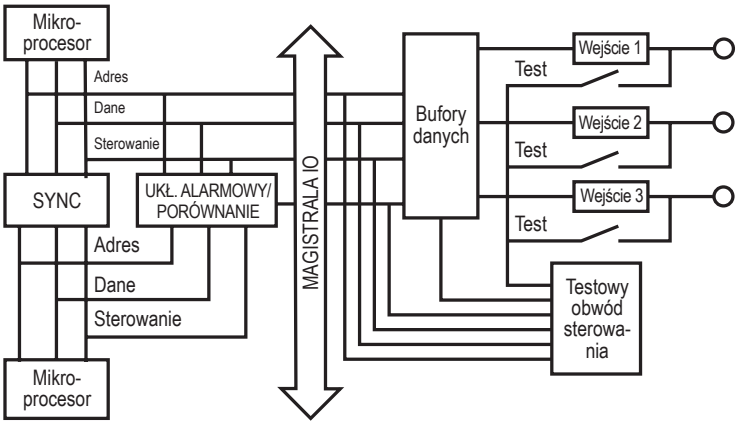
Opracowanie programowalnych sterowników logicznych bezpieczeństwa zostało podyktowane potrzebą zapewnienia elastycznych i skalowalnych rozwiązań bezpieczeństwa. Programowalne sterowniki bezpieczeństwa oferują użytkownikom taką samą swobodę sterowania bezpieczeństwem, do jakiej przywykli oni w standardowych sterownikach programowanych. Między sterownikami standardowymi i sterownikami bezpieczeństwa są jednak duże różnice. Sterowniki bezpieczeństwa są wykorzystywane w wielu platformach, gdzie zapewniają zgodność z wymaganiami dotyczącymi skalowalności, funkcjonalności oraz zintegrowania najbardziej złożonych systemów bezpieczeństwa.

Do obsługi wejść/wyjść, pamięci oraz bezpiecznej komunikacji używanych jest wiele mikroprocesorów. Analiza diagnostyczna jest wykonywana przez obwody nadzorujące. Ten typ architektury jest znany jako 1oo2D, ponieważ funkcje bezpieczeństwa mogą być realizowane przez każdy z dwóch mikroprocesorów, a ich synchroniczne działanie jest zapewniane przez funkcje diagnostyczne.



Architektura 1oo2D

Także każdy obwód wejściowy jest wewnętrznie testowany wiele razy na sekundę, aby upewnić się, że działa prawidłowo. Nawet jeśli przycisk zatrzymania awaryjnego jest naciskany raz w miesiącu, obwód wewnętrzny jest testowany w sposób ciągły.



Schemat blokowy wejściowego modułu bezpieczeństwa

Wyjścia sterowników bezpieczeństwa są elektromechaniczne lub półprzewodnikowe. Obwody wyjściowe, podobnie jak wejściowe, są testowane wiele razy na sekundę, aby upewnić się, że mogą być bezpiecznie wyłączone. Jeśli uszkodzeniu ulegnie jeden z trzech obwodów, wyjście zostanie wyłączone przez pozostałe dwa, a do wewnętrznego obwodu monitorowania wysyłana będzie informacja o błędzie.
Jeśli stosuje się urządzenia bezpieczeństwa z zestykami mechanicznymi (wyłączniki awaryjne, wyłączniki osłon itp.), można zastosować impulsowe sygnały testujące do wykrywania zwarć międzykanałowych.

Oprogramowanie

Sterowniki bezpieczeństwa programuje się bardzo podobnie, jak standardowe sterowniki programowalne. Cała dodatkowa diagnostyka i sprawdzanie błędów są realizowane przez system operacyjny, zatem programista wcale nie wie, że te czynności są wykonywane. Większość sterowników bezpieczeństwa ma specjalne instrukcje do pisania programów dla systemów bezpieczeństwa. Funkcje realizowane przez instrukcje mają naśladować zadania wykonywane przez odpowiadające im przekaźniki bezpieczeństwa. Np. działanie instrukcji Emergency Stop jest bardzo podobne do działania przekaźnika MSR. Chociaż logika leżąca u podstaw każdej z tych instrukcji jest złożona, programy bezpieczeństwa są stosunkowo proste, ponieważ programiści po prostu łączą te bloki ze sobą. Instrukcje te, a także inne instrukcje logiczne, matematyczne, do obsługi danych itd., są certyfikowane przez niezależne firmy, które zapewniają, że ich działanie jest zgodne z odnośnymi normami.

Funkcje bezpieczeństwa są najczęściej programowane przy użyciu bloków funkcyjnych. Poza blokami funkcyjnymi i logiką drabinkową sterowniki bezpieczeństwa oferują certyfikowane instrukcje aplikacyjne. Certyfikowane instrukcje bezpieczeństwa zapewniają działanie zgodne z konkretnym typem aplikacji.

Certyfikowane bloki funkcyjne można wykorzystywać z niemal wszystkimi urządzeniami bezpieczeństwa. Jednym wyjątkiem są czułe na nacisk listwy bezpieczeństwa, w których stosowana jest technologia rezystancyjna.

Sterowniki bezpieczeństwa generują „sygnaturę", umożliwiającą śledzenie wprowadzanych zmian. Sygnatura jest tworzona na podstawie kombinacji programu, konfiguracji wejść/wyjść oraz znacznika czasu. Kiedy programowanie i walidacja zostaną zakończone, użytkownik powinien zapisać sygnaturę jako część wyników walidacji, w celu jej przyszłego wykorzystania. Jeśli program wymaga wprowadzenia zmian, należy przeprowadzić jego ponowną walidację oraz zapisać nową sygnaturę. Aby zapobiec nieautoryzowanym zmianom, program można również zabezpieczyć hasłem.

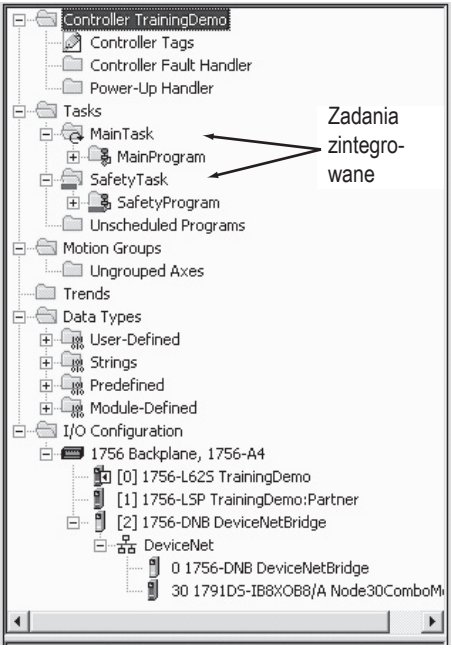
W porównaniu z przekaźnikami bezpieczeństwa okablowanie programowalnych systemów logicznych jest uproszczone. Zamiast podłączania do konkretnych zacisków przekaźnika bezpieczeństwa, urządzenia wejściowe są podłączane do dowolnych zacisków wejściowych, a urządzenia wyjściowe do dowolnych zacisków wyjściowych. Zaciski są następnie przypisywane do konkretnych urządzeń za pomocą oprogramowania.

Zintegrowane sterowniki bezpieczeństwa

Rozwiązania sterowania bezpieczeństwem są obecnie dostępne jako całkowicie zintegrowane w pojedynczą architekturę sterowania, gdzie działają jednocześnie funkcje bezpieczeństwa oraz standardowe funkcje sterowania. Zdolność sterowania ruchem, napędami, procesami, szarżami, szybkimi sekwencjami oraz bezpieczeństwem na poziomie SIL 3 przez jeden sterownik daje duże korzyści. Integracja sterowania standardowego i bezpieczeństwa pozwala na wykorzystanie wspólnych narzędzi i technologii, które ograniczą koszty projektowania, instalacji, uruchamiania i utrzymania. Możliwość zastosowania zwykłego sprzętu sterującego, rozproszonych wejść/wyjść bezpieczeństwa lub urządzeń bezpieczeństwa w sieci bezpieczeństwa, a także paneli HMI prowadzi do ograniczenia kosztów związanych z zakupem i utrzymaniem, przy jednoczesnym skracaniu czasu trwania prac rozwojowych. Wszystko to zwiększa wydajność, szybkość rozwiązywania problemów oraz zmniejsza koszty szkoleń.

Przykład integracji sterowania z bezpieczeństwem przedstawiono na rysunku. Standardowe funkcje niezwiązane z bezpieczeństwem znajdują się w zadaniu głównym (Main Task). Funkcje związane z bezpieczeństwem znajdują się w zadaniu bezpieczeństwa (Safety Task).

Wszystkie funkcje standardowe oraz związane z bezpieczeństwem są od siebie oddzielone. Przykładem są zmienne bezpieczeństwa, które mogą być odczytywane bezpośrednio przez logikę standardową. Zmienne te mogą być wymieniane między sterownikami GuardLogix w sieciach EtherNet/IP, ControlNet lub DeviceNet. Zmienne bezpieczeństwa mogą być także czytane bezpośrednio przez urządzenia zewnętrzne, panele operatorskie, komputery lub inne sterowniki.



1. Logika i zmienne standardowe zachowują się podobnie jak ControlLogix.

2. Zmienne standardowe, z zakresu programu lub sterownika oraz urządzeń zewnętrznych, interfejsy HMI, komputery, inne sterowniki itp.

3. Jako sterownik zintegrowany, GuardLogix umożliwia mapowanie zmiennych standardowych na zmienne bezpieczeństwa i wykorzystanie ich w zadaniu bezpieczeństwa. Dzięki temu można odczytać informację stanu ze standardowej części sterownika GuardLogix. Dane te nie mogą być użyte do bezpośredniego sterowania wyjściem bezpieczeństwa.

4. Zmienne bezpieczeństwa mogą być odczytywane bezpośrednio przez logikę standardową.

5. Zmienne bezpieczeństwa mogą być odczytywane lub zapisywane przez logikę bezpieczeństwa.

6. Zmienne bezpieczeństwa mogą być wymieniane między sterownikami GuardLogix za pośrednictwem protokołu EtherNet/IP.

7. Zmienne bezpieczeństwa z zakresu programu lub sterownika mogą być odczytywane przez urządzenia zewnętrzne, interfejsy HMI, komputery, inne sterowniki itp. Uwaga: gdy te dane zostaną odczytane, są one traktowane jako dane standardowe, a nie dane bezpieczeństwa.

Sieci bezpieczeństwa

Sieci komunikacyjne, występujące na poziomie produkcyjnym, od zawsze pozwalały producentom na poprawę elastyczności, zwiększenie diagnostyki, zwiększenie odległości, ograniczenie kosztów instalacji i okablowania, ułatwienie utrzymania oraz ogólną poprawę wydajności produkcji. Te same korzyści można uzyskać, wdrażając przemysłowe sieci bezpieczeństwa. Umożliwiają one producentom rozmieszczanie wejść/wyjść bezpieczeństwa i innych urządzeń bezpieczeństwa wokół maszyny przy zastosowaniu pojedynczego kabla sieciowego dla łączności standardowej i bezpieczeństwa. Ogranicza to koszty instalacji, poprawia diagnostykę oraz umożliwia zwiększenie złożoności systemów bezpieczeństwa. Sieci bezpieczeństwa zapewniają także bezpieczną komunikację między programowanymi sterownikami bezpieczeństwa, pozwalając użytkownikowi rozmieszczać elementy sterujące związane z bezpieczeństwem w wielu inteligentnych systemach.

Sieci bezpieczeństwa mają zaprojektowane mechanizmy do wykrywania błędów transmisji i uruchamiania właściwych funkcji reagujących na błąd. Wykrywane błędy komunikacji to: wstawienie komunikatu, utrata komunikatu, uszkodzenie komunikatu, opóźnienie komunikatu, powtórzenie komunikatu oraz nieprawidłowa sekwencja komunikatu.

W przypadku większości zastosowań wykrycie błędu powoduje przejście urządzenia w zdefiniowany stan wyłączenia, określany zwykle „stanem bezpiecznym". Wejściowy lub wyjściowy moduł komunikacyjny bezpieczeństwa odpowiada za wykrywanie tych błędów komunikacji, a następnie za przejście w stan bezpieczny, jeśli jest to wymagane.

Pierwsze sieci bezpieczeństwa były przeznaczone do zastosowania z konkretnymi typami mediów lub schematów dostępu, więc producenci byli zmuszeni do korzystania ze specjalnego okablowania, kart sieciowych, routerów, mostów itd., które stały się tym samym częścią funkcji bezpieczeństwa. W sieciach tego typu występowały ograniczenia polegające na tym, że komunikacja obsługiwała tylko urządzenia bezpieczeństwa. Oznaczało to konieczność wykorzystywania dwóch lub większej liczby sieci w strategii sterowania maszyną (jedna sieć do sterowania standardowego, a druga do sterowania związanego z bezpieczeństwem), co wiązało się ze zwiększonymi kosztami instalacji, szkoleń i części zamiennych.

W nowoczesnych sieciach bezpieczeństwa komunikacja z urządzeniami bezpieczeństwa i standardowymi może się odbywać przy użyciu jednego kabla sieciowego. Protokół CIP (Common Industrial Protocol) to protokół o standardzie otwartym opracowany przez ODVA (Open DeviceNet Vendors Association). Umożliwia on bezpieczną komunikację między urządzeniami bezpieczeństwa w sieciach DeviceNet, ControlNet oraz EtherNet/IP. Ponieważ protokół CIP Safety to rozszerzenie standardowego protokołu CIP, urządzenia bezpieczeństwa i standardowe mogą znajdować się w tej samej sieci. Sieci zawierające urządzenia bezpieczeństwa można również łączyć, wykorzystując mosty sieciowe. Dzięki temu możliwe jest dzielenie urządzeń bezpieczeństwa na mniejsze grupy w celu dopasowania czasów odpowiedzi oraz uproszczenia rozmieszczania urządzeń w sieci. Ponieważ protokół bezpieczeństwa jest związany ściśle z urządzeniami końcowymi (sterownikami bezpieczeństwa, modułami we/wy bezpieczeństwa, komponentami bezpieczeństwa), używane są standardowe kable, karty sieciowe, mosty i routery, eliminując tym samym stosowanie specjalnego sprzętu sieciowego oraz usuwając te urządzenia z funkcji bezpieczeństwa.

Urządzenia wyjściowe

Przekaźniki i styczniki bezpieczeństwa

Przekaźniki i styczniki służą do odłączania zasilania od elementów wykonawczych. Użycie przekaźników i styczników sterujących do celów bezpieczeństwa jest uzyskiwane przez wprowadzenie do nich funkcji specjalnych.

Informacja o stanie przekaźników sterujących i styczników jest przekazywana do monitorujących urządzeń logicznych za pomocą połączonych mechanicznie zestyków pomocniczych. Dzięki zastosowaniu takich zestyków możliwe jest zapewnienie funkcji bezpieczeństwa. Aby spełnić wymagania mechanicznego połączenia zestyków, zestyki rozwierne i zwierne nie mogą być jednocześnie zamknięte. Wymagania dotyczące zestyków połączonych mechanicznie przedstawiono w normie IEC 60947-4-1. Po sklejeniu się zestyków zwiernych zestyki rozwierne pozostaną otwarte na co najmniej 0,5 mm. Analogicznie, jeśli zestyki rozwierne ulegną sklejeniu, zestyki zwierne pozostaną otwarte.

Systemy bezpieczeństwa mogą być uruchamianie tylko z określonych miejsc. W przypadku standardowych przekaźników i styczników zamknięcie zestyków zwiernych jest możliwe przez naciśnięcie zwory. W urządzeniach bezpieczeństwa zwora jest zabezpieczona przed ręcznym przesterowaniem, aby uniknąć niespodziewanego uruchomienia.

W stycznikach zestyk rozwierny jest napędzany przez zworę główną. Styczniki bezpieczeństwa mają dodatkowy blok z zestykami połączonymi mechanicznie. Jeśli taki blok odpadnie od postawy, zestyki połączone mechanicznie pozostaną zamknięte. Dlatego też zestyki te muszą być zamontowane trwale do pomocniczego lub głównego stycznika bezpieczeństwa. W przypadku dużych styczników blok dodatkowy nie wystarczy do prawidłowego odwzorowania stanu zwory głównej. Stosuje się wówczas zestyki lustrzane, umieszczane po obu stronach stycznika.

Czas zwolnienia stycznika ma znaczącą rolę dla obliczania odległości bezpiecznej. Często stosuje się tłumiki przepięć podłączone do cewek w celu wydłużenia żywotności zestyków sterujących cewkami. W przypadku cewek zasilanych prądem przemiennym czas zwolnienia pozostaje niezmieniony. Czas zwolnienia dla cewek zasilanych prądem stałym wydłuża się. Wielkość ta zależy od typu wybranego tłumika.

Przekaźniki sterujące i styczniki są przeznaczone do przełączania dużych obciążeń, od 0,5 A do ponad 100 A. W systemach bezpieczeństwa prądy są jednak małe. Sygnał zwrotny generowany przez urządzenie logiczne systemu bezpieczeństwa może mieć natężenie od kilku do kilkudziesięciu miliamperów, zazwyczaj przy napięciu 24 V DC. Aby tak małe prądy mogły być skutecznie przełączane, w stycznikach bezpieczeństwa stosowane są pozłacane zestyki rozwidlone.

Zabezpieczenie przeciążeniowe

Normy elektryczne wymagają, aby silniki były zabezpieczone przed przeciążeniem. Diagnostyka zapewniana przez zabezpieczenia przeciążeniowe poprawia nie tylko ochronę sprzętu, lecz także bezpieczeństwo operatora. Współczesne technologie pozwalają wykrywać defekty takie jak przeciążenie, zanik fazy, zwarcie doziemne, utknięcie, zatarcie, niedociążenie, asymetria i przegrzanie. Odpowiednio wczesne wykrywanie i powiadamianie o nieprawidłowych warunkach pracy wydłuża czas produkcji ciągłej oraz chroni operatorów i pracowników obsługi technicznej przed nieprzewidzianymi niebezpiecznymi sytuacjami.

Napędy i serwonapędy

Napędy i serwonapędy bezpieczeństwa mogą być wykorzystane do powstrzymania energii obrotowej w trakcie zatrzymania bezpiecznego i awaryjnego.

Napędy prądu zmiennego są uznawane za bezpieczne, jeśli zastosowano w nich redundantne kanały odłączające zasilanie od obwodu sterowania bramkami. Kanały nadmiarowe są monitorowane przez logikę zewnętrzną lub zintegrowaną, w zależności od rodzaju napędu. Dzięki takiej redundancji można stosować napędy bezpieczeństwa w obwodach zatrzymania awaryjnego, bez konieczności używania styczników.

W serwonapędach funkcje bezpieczeństwa są realizowane podobnie jak w przemiennikach częstotliwości, z wykorzystaniem redundantnych sygnałów bezpieczeństwa do aktywacji funkcji „bezpiecznego wyłączenia momentu”.

Systemy połączeniowe

Systemy połączeniowe zapewniają zmniejszenie kosztów instalacji i utrzymania systemu bezpieczeństwa. Przy projektowaniu należy uwzględnić urządzenia jednokanałowe, dwukanałowe, dwukanałowe z sygnalizacją oraz inne typy urządzeń.

Jeśli wymagane jest szeregowe połączenie blokad dwukanałowych, instalację można uprościć, stosując moduły rozdzielcze. Moduły mają stopień ochrony IP67 co oznacza, że można je montować na maszynach w odległych lokalizacjach. Jeśli wymagana jest obsługa różnorodnych urządzeń, można zastosować moduł ArmorBlock Guard I/O. W celu dostosowania różnych typów urządzeń wejścia są konfigurowane programowo.

Rozdział 5: Obliczanie odległości bezpiecznej

Nim operator wejdzie w kontakt z zagrożeniem, musi ono znaleźć się w stanie bezpiecznym. Do obliczania bezpiecznej odległości wykorzystywane są dwie grupy norm. W niniejszym rozdziale podzielono je na:

ISO EN: (EN ISO 13855)

US CAN: (ANSI B11.19, ANSI RIA R15.06 oraz CAN/CSA Z434-03)

Wzór

Minimalna odległość bezpieczna zależy od czasu wymaganego do przetworzenia polecenia zatrzymania oraz od odległości, na jaką operator może wejść do strefy zagrożenia nim zostanie wykryty. Na całym świecie jest używany taki sam wzór oraz obowiązują te same wymagania. Jedyne różnice występują w nazwach zmiennych oraz używanych jednostkach miar.

Wzory są następujące:

ISO EN: $S = K \times T + C$

US CAN: $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

gdzie: Ds i S są minimalną odległością bezpieczną strefy zagrożenia od najbliższego punktu wykrywania

Kierunek zbliżania

W przypadku obliczania odległości bezpiecznej w obszarach, gdzie zastosowano kurtyny świetlne lub skanery, należy uwzględnić kierunek zbliżania się do urządzenia wykrywającego. Możliwe kierunki zbliżania są następujące:

normalny – kierunek zbliżania jest prostopadły do płaszczyzny wykrywania,

poziomy – kierunek zbliżania jest równoległy do płaszczyzny wykrywania,

ukośny – kierunek zbliżania jest skośny w stosunku do płaszczyzny wykrywania.

Stała prędkości

K to stała prędkości. Wartość stałej prędkości zależy od ruchliwości operatora (tj. od szybkości ruchów jego ręki, szybkości chodzenia oraz długości kroków). Ten parametr jest określony na podstawie badań, zgodnie z którymi można przyjąć założenie, że szybkość ruchów ręki jest równa 1600 mm/s, gdy ciało operatora jest nieruchome. Należy wziąć pod uwagę warunki występujące w rzeczywistej sytuacji. Zgodnie z ogólnymi wytycznymi prędkość zbliżania może zmieniać się w zakresie od 1600 mm/s do 2500 mm/s. Prawidłową wartość stałej prędkości należy określić podczas oceny ryzyka.

Czas zatrzymania

T to całkowity czas zatrzymania systemu. Czas ten jest wyrażony w sekundach i jest liczony od momentu aktywacji sygnału zatrzymywania do momentu ustania zagrożenia. Aby ułatwić analizę można go podzielić na mniejsze części (Ts, Tc, Tr oraz Tbm). Ts – najdłuższy możliwy czas zatrzymania maszyny/urządzenia. Tc – najdłuższy możliwy czas zatrzymania systemu sterowania. Tr – czas odpowiedzi urządzenia ochronnego, z uwzględnieniem jego interfejsu. Tbm to dodatkowy czas zatrzymania, pozwalający układowi nadzoru hamulca wykrycie przekroczenia czasu zatrzymania, określonego wstępnie przez użytkownika. Czas Tbm jest używany w przypadku obrotowych elementów pras mechanicznych. Jeśli wartości Ts + Tc + Tr nie są znane, zwykle określane są przez urządzenie odmierzające czas zatrzymania.

Współczynniki głębokości wnikania

Współczynniki głębokości wnikania są reprezentowane przez wielkości C i Dpf. Określają maksymalną drogę w kierunku zagrożenia przed wykryciem obecności przez urządzenie ochronne. Współczynniki głębokości wnikania różnią się w zależności od typu urządzenia i aplikacji. Najkorzystniejszy współczynnik głębokości wnikania należy określić według właściwej normy. W przypadku normalnego kierunku zbliżania do kurtyny świetlnej lub skanera obszaru, których czułość jest mniejsza niż 64 mm, normy ANSI i Kanady podają wartość:

Dpf = 3,4 x (czułość wykrywania – 6,875 mm) ale nie mniej niż zero.

Dla normalnego kierunku zbliżania do kurtyny świetlnej lub skanera, których czułość jest mniejsza niż 40 mm, normy ISO i EN podają wartość:

C = 8 x (czułość wykrywania – 14 mm), ale nie mniej niż zero

Wyniki obu wzorów spotykają się dla czułości 19,3 mm. Jeśli czułość jest mniejsza niż 19 mm, bardziej restrykcyjne są normy US CAN, ponieważ kurtyny świetlne i skanery muszą być bardziej oddalone od zagrożenia. W przypadku czułości większych od 19,3 mm, bardziej restrykcyjne są normy ISO i EN. Producenci maszyn przeznaczonych do stosowania na całym świecie, muszą wybrać z obu wzorów najgorsze warunki wynikające z obydwu równań.

Sięganie przez barierę

W przypadku gorszych czułości, współczynniki głębokości wnikania oraz czułości nieznacznie się różnią w normach US CAN i ISO EN. Wartość w normach ISO EN to 850 mm, natomiast w normach US CAN wynosi ona 900 mm. Normy różnią się również co do czułości.

Sięganie nad barierą

Obie normy są zgodne co do minimalnej wysokości najniższej wiązki, która powinna wynosić 300 mm nad podłożem, różnią się jednak ze względu na minimalną wysokość najwyższej wiązki. Norma ISO EN podaje wartość 900 mm, natomiast normy US CAN podaje 1200 mm. Wartości te wydają się być dyskusyjne. Biorąc pod uwagę sięganie nad barierą, wysokość najwyższej wiązki wykrywającej powinna być znacznie wyższa i dopasowana do operatora stojącego. Jeśli operator może sięgnąć ponad płaszczyzną wykrywania, należy zastosować powyższe kryteria.

Bariery jedno lub wielowiązkowe

Wymagania dla barier jedno i wielowiązkowych omówiono szczegółowo w normach ISO EN. Poniższe rysunki przedstawiają „praktyczne" wysokości wielu wiązek nad podłogą. Głębokość wnikania jest w większości przypadków równa 850 mm, a w sytuacji zastosowania pojedynczej wiązki wynosi 1200 mm. Dla porównania, zagadnienie to zostało w normach US CAN uwzględnione przez wymagania związane z sięganiem przez barierę. Pod uwagę należy zawsze brać sytuacje sięgania nad, pod oraz poza barierą jedno i wielowiązkową.

# Wiązki	Wysokość nad podłogą – mm (cale)	C – mm (cale)
1	750 (29.5)	1200 (47.2)
2	400 (5.7), 900 (35.4)	850 (33.4)
3	300 (11.8), 700 (27.5), 1100 (43.3)	850 (33.4)
4	300 (11.8), 600 (23.6), 900 (35.4), 1200 (47.2)	850 (33.4)

Obliczanie odległości

Dla normalnego kierunku zbliżania do kurtyn świetlnych sposób obliczania odległości bezpiecznej w normach ISO EN oraz US CAN jest bardzo podobny, jednak występują pewne różnice. W przypadku normalnego kierunku zbliżania do pionowych kurtyn świetlnych, dla których czułość wykrywania wynosi maksymalnie 40 mm, ISO EN wymaga wykonania dwóch kroków. Najpierw należy obliczyć S, używając wartość 2000 jako stałą prędkości.

S = 2000 x T + 8 x (d -1 4)

Minimalna możliwa odległość S to 100 mm.

Drugi krok jest stosowany, gdy odległość jest większa niż 500 mm. Wtedy wartość K można zmniejszyć do 1600. Jeśli K = 1600, minimalna wartość S wynosi 500 mm.

W normach US CAN zaprezentowano podejście jednoetapowe: Ds = 1600 x T * Dpf

W wyniku tego, przy czasach odpowiedzi mniejszych od 560 ms, różnice między wartościami obliczonymi przy użyciu różnych norm są większe niż 5%.

Ukośny kierunek zbliżania

W większości przypadków kurtyny świetlne i skanery są montowane w pozycji pionowej (normalny kierunek zbliżania) lub poziomej (równoległy kierunek zbliżania). Taki montaż nie jest uważany za ukośny, jeśli kąt odchylenia jest mniejszy niż ±5°. Gdy kąt przekracza ±5°, należy wziąć pod uwagę potencjalne ryzyko (np. mniejszą odległość) związane z możliwymi do przewidzenia kierunkami zbliżania się. Generalnie kierunki zbliżania pod kątem większym niż 30° względem płaszczyzny odniesienia (np. podłogi) powinny być traktowane jako normalne, natomiast kierunki, dla których kąty te są mniejsze niż 30°, powinny być traktowane jako równoległe.

Maty bezpieczeństwa

W przypadku mat bezpieczeństwa obliczając odległość bezpieczną, należy wziąć pod uwagę szybkość operatora oraz długość kroków. Przyjmuje się, że operator idzie, a mata jest przymocowana do podłogi. Współczynnik głębokości wnikania dla pierwszego kroku operatora na macie wynosi 1200 mm. Jeżeli operator musi wejść na podwyższenie, współczynnik ten może zostać zmniejszony o 40% w odniesieniu do wysokości stopnia. Ważne jest zamocowanie mat(y) w sposób uniemożliwiający jakiekolwiek przemieszczenie.

Przykład

Przykład: Operator zbliża się prostopadle do kurtyny świetlnej o czułości 14 mm, podłączonej do przekaźnika bezpieczeństwa MSR, który z kolei połączony jest ze stycznikiem zasilanym prądem stałym i wyposażonym w tłumik diodowy. Czas Tr odpowiedzi systemu bezpieczeństwa jest równy 20 + 15 + 95 = 130 ms. Czas zatrzymania maszyny to Ts + Tc = 170 ms. Nadzorowanie hamulca nie jest stosowane. Wartość Dpf to 25,4 mm, natomiast wartość C jest równa zero. Obliczenia przedstawiają się następująco:

Dpf = 3,4 (14 – 6,875) = 24,2 mm

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0,17 + 0,13 + 0) + 1
Ds = 63 x (0,3) + 1
Ds = 18,9 + 1
Ds = 505 mm

C = 8 (14 – 14) = 0

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm

Zgodnie z obliczeniami minimalny bezpieczny odstęp kurtyny świetlnej bezpieczeństwa od zagrożenia wynosi 508 mm i można go stosować na całym świecie.

Rozdział 6: Systemy sterowania związane z bezpieczeństwem

Informacje ogólne

Co to jest system sterowania związany z bezpieczeństwem (SRCS – Safety Related Control System)? Jest to część systemu sterowania maszyny, którego zadaniem jest zapobieganie sytuacjom zagrożenia. Może to być osobny system dedykowany lub zintegrowany ze standardowym systemem sterowania.

Złożoność jego może być różna, począwszy od prostych, takich jak wyłączniki blokujące osłon i wyłączniki stopu awaryjnego połączone szeregowo z cewkami styczników mocy, a kończąc na złożonych systemach zawierających zarówno proste, jak i zaawansowane urządzenia, komunikujące się przez oprogramowanie i sprzęt komputerowy.

Systemy sterowania związane z bezpieczeństwem odpowiadają za wykonywanie funkcji bezpieczeństwa. SRCS musi działać prawidłowo we wszystkich możliwych do przewidzenia warunkach. Czym więc jest funkcja bezpieczeństwa, jak zaprojektować realizujący ją system oraz czy zrobiliśmy to, co jest wymagane?

Funkcja bezpieczeństwa

Funkcja bezpieczeństwa jest realizowana przez elementy układu sterowania maszyny związane z bezpieczeństwem i ma na celu zapewnienie lub utrzymanie bezpiecznej kontroli nad urządzeniem w obliczu określonego zagrożenia lub wielu zagrożeń. Niezadziałanie funkcji bezpieczeństwa może skutkować natychmiastowym zwiększeniem ryzyka korzystania ze sprzętu, czyli wystąpieniem zagrożenia.

„Sytuacja niebezpieczna” powstaje w przypadku, w którym osoba może zostać narażona na zagrożenie. Zaistnienie takiej sytuacji nie oznacza automatycznie, że operator odniesie obrażenia. Narażona osoba może rozpoznać zagrożenie i uniknąć obrażeń. Osoba ta może jednak również nie rozpoznać zagrożenia albo zagrożenie może być spowodowane niezamierzonym uruchomieniem. Głównym zadaniem projektanta systemu bezpieczeństwa jest zapobieganie występowaniu sytuacjom niebezpiecznym oraz niezamierzonym uruchomieniom.

Przed funkcją bezpieczeństwa można postawić kilka wymagań. W przypadku funkcji bezpieczeństwa aktywowanej przez osłonę blokującą wymagania są trzy:

1. Elementy stwarzające zagrożenie nie mogą uruchomić się, dopóki nie zostaną zamknięte osłony;

2. Otwarcie osłony musi powodować natychmiastowe zatrzymanie elementu stwarzającego zagrożenie, jeśli maszyna pracowała w chwili jej otwarcia;

3. Zamknięcie osłony nie może powodować ponownego uruchomienia elementu stwarzającego zagrożenie.

Definiując funkcję bezpieczeństwa dla określonej aplikacji, słowo „zagrożenie" należy zmienić na konkretne zagrożenie. Źródła zagrożenia nie można mylić z następstwami jego wystąpienia. Zmiażdżenie, odcięcie i poparzenie to następstwa zagrożenia. Przykładami źródeł zagrożeń są silnik, młot, nóż, palnik, pompa, laser, robot, manipulator, elektromagnes, zawór, inny typ elementu wykonawczego lub zagrożenie mechaniczne związane z przyciąganiem ziemskim.

Mówiąc o systemach bezpieczeństwa używa się zwrotu „przed lub w momencie przywołania funkcji bezpieczeństwa". Co to jest przywołanie funkcji bezpieczeństwa? Przykładami przywołania funkcji bezpieczeństwa są: otwarcie osłony blokującej, przejście przez kurtynę świetlną, wejście na matę bezpieczeństwa lub naciśnięcie przycisku stopu awaryjnego. Operator żąda zatrzymania zagrożenia lub pozostawienia go w stanie wyłączenia, jeśli urządzenie jest już zatrzymane.

Funkcje bezpieczeństwa są realizowane przez elementy systemu sterowania związane z bezpieczeństwem. Funkcja bezpieczeństwa nie jest wykonywana przez pojedyncze urządzenie, tylko np. przez osłonę. Z osłony blokującej wysyłane jest polecenie do urządzenia logicznego, które następnie wyłącza napęd. Funkcja bezpieczeństwa rozpoczyna działanie w momencie wysłania polecenia i kończy w chwili zrealizowania określonego celu.

System bezpieczeństwa należy projektować tak, aby uzyskiwany poziom nienaruszalności odpowiadał poziomowi ryzyka na maszynie. Wyższe ryzyko wymaga wyższych poziomów nienaruszalności, umożliwiających wykonanie funkcji bezpieczeństwa. Systemy zabezpieczeń maszyny mogą być klasyfikowane według poziomów skuteczności działania ich funkcji bezpieczeństwa lub, innymi słowy, poziomu nienaruszalności bezpieczeństwa funkcjonalnego.

Bezpieczeństwo funkcjonalne systemów sterowania

Co to jest bezpieczeństwo funkcjonalne?

Bezpieczeństwo funkcjonalne stanowi część bezpieczeństwa ogólnego, które z kolei zależy od prawidłowego zadziałania procesu lub sprzętu w odpowiedzi na sygnały wejściowe. Raport techniczny IEC TR 61508-0 przedstawia następujący przykład, który pomaga zrozumieć znaczenie bezpieczeństwa funkcjonalnego. „Przykładem bezpieczeństwa funkcjonalnego może być zabezpieczenie termiczne, wykorzystujące czujnik termiczny w uzwojeniu silnika elektrycznego w celu odłączenia zasilania silnika zanim ulegnie on przegrzaniu. Natomiast zapewnienie specjalistycznej izolacji wytrzymującej wysokie temperatury nie jest przykładem bezpieczeństwa funkcjonalnego (chociaż nadal jest to przykład zabezpieczenia i może on chronić przed dokładnie tym samym zagrożeniem)".

W ramach kolejnego przykładu porównajmy osłonę stałą z osłoną blokującą. Osłony stałe nie są formą bezpieczeństwa funkcjonalnego, choć mogą zapobiegać dostępowi do takiego samego zagrożenia jak osłony blokujące. Osłony blokujące są przykładem bezpieczeństwa funkcjonalnego. Po otwarciu osłony wyłącznik blokujący pełni funkcję „wejścia" do systemu, który następnie przechodzi w stan bezpieczny. Bezpieczeństwo

obsługi można również zwiększyć, stosując środki ochronne takie jak sprzęt ochrony osobistej (PPE). Sprzęt ochrony osobistej nie jest jednak uznawany jako bezpieczeństwo funkcjonalne.

Bezpieczeństwo funkcjonalne to pojęcie wprowadzone w normie IEC 61508:1998. Od tego czasu termin ten był niekiedy kojarzony tylko z programowalnymi systemami bezpieczeństwa. Takie rozumienie jest błędne. Bezpieczeństwo funkcjonalne dotyczy bowiem szerokiej gamy urządzeń używanych do budowy systemów bezpieczeństwa. Urządzenia takie jak wyłączniki blokujące, kurtyny świetlne, przekaźniki bezpieczeństwa, sterowniki bezpieczeństwa, styczniki bezpieczeństwa i napędy bezpieczeństwa można połączyć w formę systemu bezpieczeństwa, który realizuje specyficzne funkcje związane z bezpieczeństwem. To jest właśnie bezpieczeństwo funkcjonalne.

W związku z tym bezpieczeństwo funkcjonalne elektrycznych systemów sterowania jest bardzo ważne w kontekście kontrolowania zagrożeń od ruchomych części maszyn.

Z zapewnieniem bezpieczeństwa funkcjonalnego wiążą się dwa wymagania:

- funkcja bezpieczeństwa oraz
- nienaruszalność bezpieczeństwa.

W określaniu wymagań dla bezpieczeństwa funkcjonalnego kluczową rolę odgrywa proces oceny ryzyka. Analiza zadania i ryzyka pozwala na określenie wymagań funkcjonalnych w zakresie bezpieczeństwa (tj. funkcji bezpieczeństwa). Szacowanie ryzyka skutkuje ustaleniem wymogów w zakresie nienaruszalności bezpieczeństwa (tj. nienaruszalności bezpieczeństwa lub poziomu zapewnienia bezpieczeństwa).

Cztery najważniejsze normy dotyczące bezpieczeństwa funkcjonalnego systemów sterowania dla maszyn to:

1. IEC/EN 61508 „Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów sterowania związanych z bezpieczeństwem”

   Norma zawiera wymagania i zasady dotyczące projektowania złożonych, elektronicznych i programowalnych systemów oraz podsystemów. Norma ma charakter ogólny i nie jest ograniczona wyłącznie do sektora maszyn.

2. IEC/EN 62061: Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem

   Jest to wersja normy IEC/EN 61508 dotycząca maszyn. Zawiera ona wymagania odnoszące się do projektowania wszystkich typów elektrycznych systemów sterowania związanych z bezpieczeństwem maszyn, a także projektowania niezłożonych podsystemów i urządzeń. Wszystkie podsystemy złożone i programowalne muszą spełniać wymagania IEC/EN 61508

3. EN ISO 13849-1: Bezpieczeństwo maszyn – Elementy systemów sterowania związane z bezpieczeństwem

   Celem tej normy jest zapewnienie bezpośredniej ścieżki przejścia z kategorii poprzedniej normy EN 954-1.

4. IEC 61511: Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora procesów przemysłowych

   Ta norma stanowi implementację normy IEC/EN 61508 nakierowaną na sektor procesowy.

Normy dotyczące bezpieczeństwa funkcjonalnego stanowią znaczący krok do przodu, wykraczający poza istniejące wymagania, takie jak niezawodność sterowania i kategorie, wyszczególnione w poprzedniej normie ISO 13849-1:1999 (EN 954-1:1996).

Powyższe kategorie nie zostały jednak całkowicie wycofane, są one nadal używane w aktualnej wersji normy EN ISO 13849-1.

Normy IEC/EN 62061 i EN ISO 13849-1

Normy IEC/EN 62061 i EN ISO 13849-1 dotyczą elektrycznych systemów sterowania związanych z bezpieczeństwem. Istnieje możliwość, że zostaną one ostatecznie połączone w pojedynczą normę wykorzystującą wspólną terminologię. Obie normy zapewniają uzyskanie takich samych wyników, ale przy użyciu innych metod. Oferują użytkownikom możliwość wyboru opcji, która pasuje najlepiej do konkretnej sytuacji. Użytkownik może wybrać jedną z norm do stosowania i są one obie zharmonizowanie w ramach europejskiej dyrektywy maszynowej.
W wyniku zastosowania obu norm otrzymuje się porównywalne poziomy zapewnienia i nienaruszalności bezpieczeństwa. Metodologie obu norm różnią się, dzięki czemu użytkownicy mogą je wykorzystywać w różnych zastosowaniach.
Metodologia normy IEC/EN 62061 pozwala wdrażać złożone funkcje bezpieczeństwa z zastosowaniem architektur systemów, uważanych wcześniej za niekonwencjonalne. Metodologia normy EN ISO 13849-1 pozwala na bardziej bezpośrednie i mniej skomplikowane ścieżki dla bardziej konwencjonalnych funkcji bezpieczeństwa, wdrażanych za pomocą konwencjonalnych architektur systemowych.

Ważnym elementem odróżniającym obie normy jest przydatność dla różnych technologii. Norma IEC/EN 62061 jest bardziej odpowiednia do systemów elektrycznych. Natomiast norma EN ISO 13849-1 może być stosowana do systemów pneumatycznych, hydraulicznych, mechanicznych, a także elektrycznych.

Wspólny raport techniczny dla IEC/EN 62061 i EN ISO 13849-1

Połączony raport został przygotowany w ramach IEC i ISO w celu zapewnienia pomocy użytkownikom obu norm.

Omawia on relacje między tymi dwiema normami oraz wyjaśnia, w jaki sposób można uzyskać równoważność między PL (poziomem zapewnienia bezpieczeństwa) wg normy EN ISO 13849-1 a SIL (poziomem nienaruszalności bezpieczeństwa) wg normy IEC/EN 62061, zarówno na poziomie systemu, jak i podsystemu.

Aby wykazać, że obie normy zapewniają równoważne wyniki, raport przedstawia przykładowy system bezpieczeństwa obliczony zgodnie z metodologiami obu norm. Raport również przedstawia pewne problemy, które zostały poddane różnym interpretacjom. Prawdopodobnie jednym z istotniejszych zagadnień jest kwestia wykluczeń defektów.

W zasadzie, jeśli funkcja bezpieczeństwa, która ma być wdrożona do systemu sterowania związanego z bezpieczeństwem, wymaga najwyższego poziomu zapewnienia bezpieczeństwa PLe, poleganie na samych wykluczeniach defektów w celu osiągnięcia tego poziomu nie może być traktowane jako norma. Jest to uzależnione od zastosowanej technologii oraz docelowego środowiska pracy. W związku z tym ważne jest, aby projektant podjął dodatkowe środki w zakresie stosowania wykluczania defektów, wraz ze wzrostem wymogów w zakresie poziomu działania.

Generalnie stosowanie metodologii wykluczeń defektów w przypadku mechanicznych aspektów elektromechanicznych wyłączników nie może być brane pod uwagę przy wyznaczania poziomu PLe w projekcie układu sterowania powiązanego z bezpieczeństwem. Wykluczenia, które mogą być zastosowane do specyficznych defektów mechanicznych (np. zużycie, korozja, pęknięcia) są opisane w tabeli A.4 normy ISO 13849-2.

Na przykład system osłony blokującej, który powinien uzyskać poziom PLe będzie musiał wykazywać odporność na co najmniej jeden defekt (np. dwa konwencjonalne mechaniczne wyłączniki krańcowe), aby osiągnąć ten poziom, ponieważ wykluczenie defektów takich jak uszkodzenie głowicy wyłącznika nie jest normalnie uzasadnione. Może być jednak dopuszczalne wykluczenie innych defektów, jak zwarcie obwodu w szafie sterowniczej zaprojektowanej zgodnie z odpowiednimi normami.

SIL i IEC/EN 62061

IEC/EN 62061 opisuje zarówno wartość ryzyka jak i zdolność systemu sterowania do ograniczenia ryzyka za pomocą SIL (Safety Integrity Level – poziom nienaruszalności bezpieczeństwa). W sektorze maszynowym używane są trzy poziomy nienaruszalności bezpieczeństwa (SIL). Najniższy to SIL 1, a najwyższy to SIL 3.

W związku z tym, że termin SIL jest stosowany w taki sam sposób w innych sektorach przemysłowych, takich jak petrochemiczny, energetyczny i kolejowy,

norma IEC/EN 62061 jest bardzo przydatna, gdy maszyny są używane w tych sektorach. Jednak ponieważ poziom ryzyka w sektorach takich jak przemysł procesowy, może być wyższy, w normie IEC 61508 oraz w normie IEC 61511 dla sektora procesowego włączono poziom SIL 4.

Poziom nienaruszalności bezpieczeństwa (SIL) ma zastosowanie do funkcji bezpieczeństwa. Podsystemy wchodzące w skład systemu realizującego funkcję bezpieczeństwa muszą mieć odpowiedni poziom SIL. Poziom ten jest określany jako SIL Claim Limit (SIL CL). Aby zastosować go w prawidłowy sposób, należy wcześniej dokładnie przeczytać i zrozumieć normę IEC/EN 62061.

PL i EN ISO 13849-1

W normie EN ISO 13849-1 nie jest używany termin SIL; zamiast niego zastosowano określenie PL (Performance Level – poziom zapewnienia bezpieczeństwa Pod wieloma względami poziomy PL oraz SIL są ze sobą związane. Jest pięć poziomów działania. Najniższy to PLa, najwyższy to PLe.

Porównanie PL i SIL

Ta tabela przedstawia przybliżoną relację pomiędzy poziomem zapewnienia bezpieczeństwa (PL) a poziomem nienaruszalności bezpieczeństwa (SIL) w przypadku zastosowania w strukturach typowych obwodów.

PL (poziom zapewnienia bezpieczeństwa)	PFH_D (prawdopodobieństwo defektu niebezpiecznego na godzinę)	SIL (poziom nienaruszalności bezpieczeństwa)
a	$\geq 10^{-5}$ do $<10^{-4}$	Brak
b	$\geq 3 \times 10^{-6}$ do $<10^{-5}$	1
c	$\geq 10^{-6}$ do $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ do $<10^{-6}$	2
e	$\geq 10^{-8}$ do $<10^{-7}$	3

Przybliżony związek między PL i SIL

WAŻNE: Powyższa tabela to jedynie ogólna porównanie i NIE MOŻNA jej wykorzystywać do konwersji z jednego typu poziomu na drugi. Należy wziąć pod uwagę pełne wymagania określone w normach. Więcej szczegółowych informacji przedstawiono w tabelach w Załączniku K.

Rozdział 7: Projektowanie systemu według normy EN ISO 13849

Prawidłowe stosowanie normy EN ISO 13849-1 będzie możliwe dopiero po pełnym i szczegółowym zapoznaniu się z jej treścią. Poniżej przedstawiono jedynie krótkie omówienie.

Norma określa wymagania do projektowania i integracji elementów systemu sterowania związanych z bezpieczeństwem, wraz pewnymi aspektami oprogramowania. Norma dotyczy systemu związanego z bezpieczeństwem, ale może być także stosowana do komponentów składowych systemów.

Oprogramowanie SISTEMA do obliczania poziomu zapewnienia bezpieczeństwa

SISTEMA to narzędzie programowe umożliwiające wdrożenie normy EN ISO 13849-1. Jego użycie znacznie upraszcza aspekty ilościowe i obliczeniowe związane ze stosowaniem normy.

SISTEMA oznacza „Safety Integrity Software Tool for the Evaluation of Machine Applications" i jest regularnie przeglądane i aktualizowane przez instytut IFA. Wymaga on wprowadzenia różnych typów danych bezpieczeństwa funkcjonalnego, zgodnie z informacjami przedstawionymi w dalszej części tego rozdziału. Dane mogą być wprowadzane ręcznie lub automatycznie, przy użyciu biblioteki danych producenta programu SISTEMA.

Biblioteka danych do programu SISTEMA firmy Rockwell Automation jest dostępna do pobrania wraz z łączem do strony programu SISTEMA pod adresem:
www.rockwellautomation.com, under Solutions & Services > Safety Solutions.

Przegląd normy EN ISO 13849-1

Przedstawiony poniżej ogólny przegląd ma za zadanie prezentację podstawowych zapisów normy EN ISO 13849-1. Zawiera on również wzmiankę na temat wersji opublikowanej na początku roku 2016. Jest bardzo ważne, aby sama norma została szczegółowo przeanalizowana.
Norma ta ma szerokie zastosowanie i uwzględnia wszystkie technologie, w tym elektryczne, hydrauliczne, pneumatyczne i mechaniczne. Mimo że norma ISO 13849-1 jest odpowiednia dla systemów złożonych, w przypadku złożonych komponentów z wbudowanym oprogramowaniem odsyła ona czytelnika również do normy IEC 61508.

Końcowym produktem normy ISO 13849-1 są poziomy zapewnienia bezpieczeństwa (Performance Levels: PL a, b, c, d lub e). Oryginalna koncepcja kategorii zostaje zachowana, ale występują dodatkowe wymagania konieczne do spełnienia, aby poziom zapewnienia bezpieczeństwa (PL) w systemie został osiągnięty.

Wymagania mogą być wyszczególnione w podstawowej formie, jako:

- Architektura systemu. W zasadzie obejmuje ona zakres, który dotychczas był kojarzony z kategoriami

- Dane o niezawodności wymagane dla części składowych systemu.
- Pokrycie diagnostyczne. Przedstawia efektywność monitorowania błędów w układzie
- Ochrona przed defektami wywołanymi wspólną przyczyną
- Ochrona przed błędami systematycznymi
- Specyficzne wymagania dotyczące oprogramowania, jeśli mają zastosowanie

W dalszej części dokładniej przyjrzymy się tym czynnikom, ale wcześniej warto rozpatrzyć podstawowy cel i ogólną zasadę tej normy. Na tym etapie jest oczywiste, że występują dodatkowe względy, z którymi trzeba się zapoznać, ale szczegóły staną się bardziej zrozumiałe, gdy zrozumiemy, co norma ma na celu i dlaczego.

Po pierwsze, dlaczego potrzebujemy tej normy? Doskonale wiemy, że technologia wykorzystywana w systemach bezpieczeństwa maszyn mocno rozwinęła się i w znacznym stopniu uległa zmianie w przeciągu ostatnich dziesięciu lat. Jeszcze stosunkowo niedawno systemy bezpieczeństwa polegały na „prostym" sprzęcie z bardzo przewidywalnymi trybami błędów. Ostatnio da się zauważyć coraz szersze wykorzystywanie bardziej skomplikowanych urządzeń programowalnych i elektronicznych w systemach bezpieczeństwa. Zapewniło nam to korzyści w zakresie kosztów, elastyczności i kompatybilności, ale jednocześnie oznacza to, że wcześniejsze normy straciły rację bytu. Aby określić, czy dany system bezpieczeństwa jest odpowiednio dobry, musimy dobrze go poznać. Jest to powodem, dla którego normy bezpieczeństwa funkcjonalnego wymagają więcej informacji. Ponieważ systemy bezpieczeństwa wykorzystują podejście „czarnej skrzynki" przez integrację wstępnie zakwalifikowanych podsystemów, znacznie istotniejsza staje się ich zgodność z normami. W związku z tym normy muszą być w stanie odpowiednio przeegzaminować daną technologię. Aby zapewnić tę funkcję, muszą odwołać się do podstawowych czynników: niezawodności, wykrywania błędów oraz nienaruszalności strukturalnej i systemowej. Jest to właśnie zadaniem normy EN ISO 13849-1.

Aby sporządzić logiczny plan w zgodzie z normą, należy uwzględnić dwa podstawowe różne typy użytkowników: projektanci podsystemów związanych z bezpieczeństwem oraz projektanci systemów związanych z bezpieczeństwem. Ogólnie rzecz biorąc, projektant podsystemu (najczęściej producent elementu związanego z bezpieczeństwem) będzie podlegał większej dyscyplinie. Będzie on musiał zapewnić wymagane dane, tak aby projektant systemu był pewny, że podsystem ma odpowiednią nienaruszalność dla systemu. Z reguły wymaga to testowania, analiz i obliczeń. Wyniki będą przedstawiane w formie danych wymaganych przez normę.

Projektant systemu (z reguły integrator lub projektant maszyny) wykorzysta dane o podsystemie w celu przeprowadzenia względnie prostych obliczeń umożliwiających ustalenie całościowego poziomu zapewnienia bezpieczeństwa (PL) systemu.

Określenie funkcji bezpieczeństwa

Musimy określić funkcję bezpieczeństwa. Oczywiście funkcja bezpieczeństwa musi być adekwatna do wymaganego zadania. W jaki sposób pomaga nam w tym norma? Ważne jest, aby zdać sobie sprawę, że wymaganą funkcjonalność można ustalić przez rozpatrzenie dominujących charakterystyk w rzeczywistej aplikacji. Może to być traktowane jako etap projektowania koncepcji bezpieczeństwa. Nie może to być całkowicie objęte normą, ponieważ norma nie uwzględnia wszystkich charakterystyk określonej aplikacji. Często również dotyczy to konstruktora maszyny, który buduje maszynę, ale niekoniecznie musi znać dokładne warunki, w których będzie ona używana.

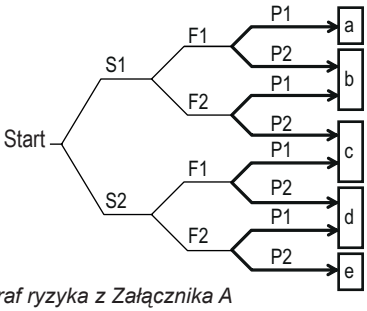
Norma zapewnia pewną pomoc w formie zestawienia wielu powszechnie stosowanych funkcji bezpieczeństwa (np. funkcja bezpiecznego zatrzymania aktywowana przez środek ochronny, funkcja automatycznego zawieszania działania, funkcja start/restart) oraz przez określenie pewnych typowo powiązanych wymagań. Analiza normy EN ISO 12100: Na tym etapie zalecane jest zastosowanie „Podstawowych zasad projektowania i oceny ryzyka". Raport ISO TR 22100-2 zawiera użyteczne wskazówki dotyczące związków między przeprowadzeniem oceny ryzyka dla maszyny zgodnie z normą ISO 12100 a procedurą przydzielenia poziomu PL według normy EN ISO 13849-1. Istnieje szeroka gama norm dotyczących maszyn, które określają wymagania funkcji bezpieczeństwa dla określonych maszyn. W ramach norm europejskich EN są one normami typu C, a niektóre z nich mają dokładne odpowiedniki w normach ISO. Raport ISO TR 22100-1 zawiera również dodatkowe informacje na temat związku między normami ISO 12100 i C.

To oczywiste, że etap projektowania koncepcji bezpieczeństwa zależy od typu maszyny oraz od charakterystyk aplikacji i środowiska, w którym jest ona używana. Konstruktor maszyny musi przewidzieć te czynniki, aby móc zaprojektować bezpieczne rozwiązanie. Zamierzone warunki (tj. oczekiwane) sposoby użycia powinny być podane w instrukcji dla użytkownika. Użytkownik maszyny musi sprawdzić, czy są one zgodne z rzeczywistymi warunkami użytkowania.

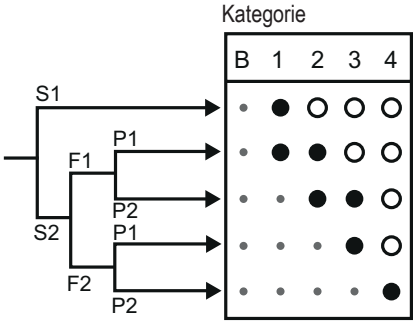
Poziom PLr służy do określenia, jaki poziom zapewnienia bezpieczeństwa jest wymagany przez funkcję bezpieczeństwa. Jest on wyznaczany podczas oceny ryzyka. Aby ustalić PLr norma udostępnia graf ryzyka, na którym wprowadzane są aplikacyjne współczynniki stopnia obrażeń, częstotliwości narażenia oraz możliwości uniknięcia wypadku.

Wartością wyjściową jest PLr. Użytkownicy starej normy EN 954-1 będą znać to podejście, ale należy zwrócić uwagę, że w normie EN ISO 13849-1 linia S1 rozdziela się, podczas gdy na starym wykresie nie. Wersja z roku 2015 zapewnia możliwość zmniejszenia PLr o jeden poziom w określonych okolicznościach, w zależności od przewidywanego prawdopodobieństwa wystąpienia.

Projektowanie systemu według normy EN ISO 13849



Graf ryzyka z Załącznika A normy EN ISO 13849-1



Graf ryzyka z załącznika B normy EN 954-1

Tak więc mamy już opis funkcji bezpieczeństwa i wymagany poziom zapewnienia bezpieczeństwa PLr dla elementów układu sterowania związanych z bezpieczeństwem (SRP/CS), które zostaną użyte w tej funkcji. Teraz trzeba zaprojektować system i zapewnić, aby był zgodny z wymaganym poziomem zapewnienia bezpieczeństwa PLr.

Jednym z istotnych czynników związanych z decyzją dotyczącą wyboru normy (EN 13849-1 lub EN/IEC 62061) jest stopień złożoności funkcji bezpieczeństwa. W większości przypadków funkcja bezpieczeństwa dla maszyn będzie względnie prosta i norma EN ISO 13849-1 będzie najodpowiedniejsza. Do oceny PL wykorzystywane są dane o niezawodności, pokrycie diagnostyczne [DC], architektura systemu [kategoria], odporność na defekty wywołane wspólną przyczyną oraz wymagania dotyczące oprogramowania (jeśli jest to potrzebne).

Jest to uproszczony opis, którego celem jest jedynie przedstawienie ogólnego zarysu. Ważne jest zrozumienie, że muszą być zastosowane wszystkie postanowienia zawarte w treści normy. Jednak pomoc znajduje się w zasięgu ręki. Dostępne jest oprogramowanie SISTEMA, które pomaga w zakresie dokumentacji i obliczeń. Umożliwia ono również utworzenie dokumentacji technicznej.

Narzędzie programowe SISTEMA jest dostępne w wielu językach, m.in. niemieckim i angielskim. IFA, twórca narzędzia SISTEMA, jest uznaną w Niemczech instytucją badawczą i testującą. Jest ona szczególnie zaangażowana w rozwiązywanie problemów naukowych i technicznych związanych z bezpieczeństwem w kontekście ustawowych ubezpieczeń wypadkowych i zapobiegania wypadkom w Niemczech. Organizacja współpracuje z agencjami BHP z ponad 20 krajów.

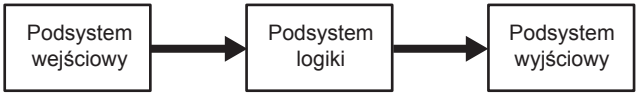
Eksperci z IFA wraz z pracownikami BG mają znaczny udział w procesie przygotowania norm EN ISO 13849-1 oraz IEC/EN 62061.

„Biblioteka" danych komponentów bezpieczeństwa firmy Rockwell Automation przeznaczonych do użytku z oprogramowaniem SISTEMA jest dostępna pod adresem: *www.rockwellautomation.com, under Solutions & Services > Safety Solutions.*

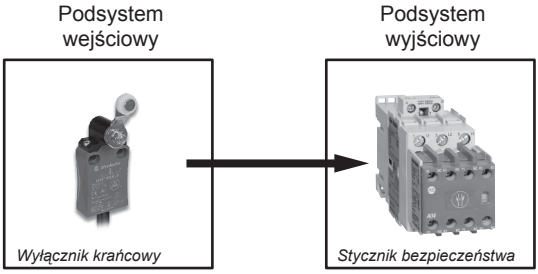
Niezależnie od sposobu obliczania poziomu zapewnienia bezpieczeństwa PL ważne jest, aby rozpocząć od właściwych podstaw. Musimy postrzegać nasz system w taki sam sposób, jak norma, więc zacznijmy od tego.

Struktura systemu

Każdy system może być podzielony na podstawowe komponentu lub „podsystemy". Każdy podsystem pełni określoną funkcję dyskretną. W działaniu większości systemów można wyodrębnić trzy podstawowe funkcje: wejście, logiczne i napędowe (niektóre proste układy mogą nie mieć fazy logiki).



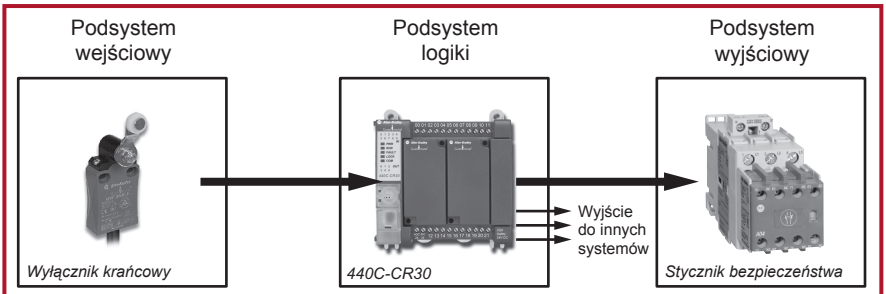
Grupy elementów, które wdrażają te funkcje to podsystemy.



Wyłącznik blokujący i stycznik bezpieczeństwa

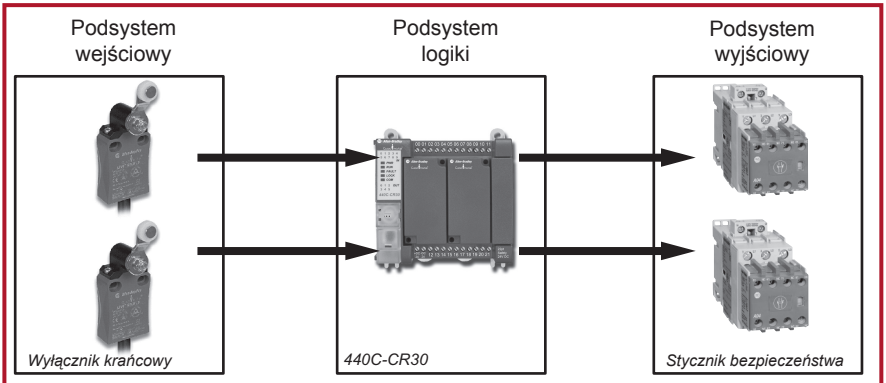
Powyżej został przedstawiony prosty przykład jednokanałowego układu elektrycznego. Składa się on jedynie z podsystemów wejścia i wyjścia.

Projektowanie systemu według normy EN ISO 13849



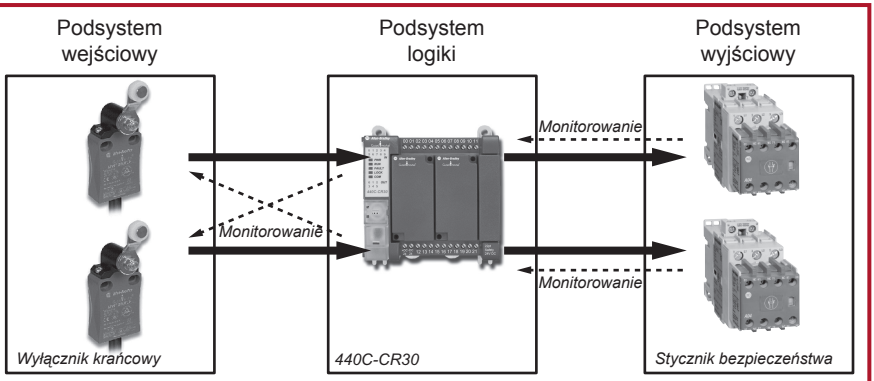
Wyłącznik blokujący, sterownik bezpieczeństwa i stycznik bezpieczeństwa

System pokazany powyżej jest nieco bardziej skomplikowany, ponieważ wymagany jest również pewien układ logiczny. Sam sterownik bezpieczeństwa będzie wewnętrznie odporny na błędy (np. dzięki strukturze dwukanałowej), ale system jako całość jest nadal ograniczony do statusu jednokanałowego z powodu pojedynczego wyłącznika krańcowego oraz pojedynczego stycznika. System jednokanałowy zawiedzie, jeżeli wystąpi defekt jednego z jego podsystemów; nie jest on „odporny na błędy”.



Dwukanałowy system bezpieczeństwa

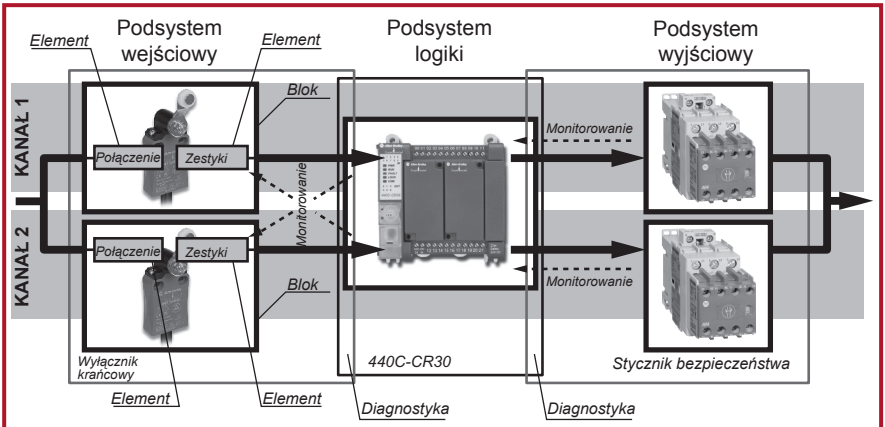
System dwukanałowy (zwany również redundantnym lub „odpornym na błędy”) został pokazany powyżej. Każdy z jego podsystemów dysponuje dwoma kanałami i nawet w przypadku pojedynczego błędu jego funkcja bezpieczeństwa pozostaje aktywna. Dopiero dwa błędy – jeden w każdym z kanałów – spowodują, że zawiedzie funkcja bezpieczeństwa i cały system bezpieczeństwa. Wyraźnie widać, że system dwukanałowy jest mniej podatny na defekty i wystąpienie stanu niebezpiecznego, niż system jednokanałowy. Ale możemy jeszcze zwiększyć poziom niezawodności [w zakresie funkcji bezpieczeństwa], jeśli uwzględnimy środki diagnostyczne do wykrywania defektów. Oczywiście w przypadku wykrycia defektu musimy również zareagować i zapewnić, aby system przeszedł do stanu bezpiecznego. Poniższy schemat przedstawia zastosowanie środków diagnostycznych uzyskanych za pomocą technik monitorowania.



Diagnostyka z dwukanałowym systemem bezpieczeństwa

Najczęściej (lecz nie zawsze) jest tak, że system ma dwa kanały we wszystkich swoich podsystemach. W związku z tym możemy zauważyć, że w tym przypadku każdy podsystem posiada dwa „podkanały". Norma określa je jako „bloki". Podsystem dwukanałowy będzie miał minimum dwa bloki, a system jednokanałowy będzie miał minimum jeden blok. Możliwe, że niektóre systemy będą miały kombinację bloków dwukanałowych i jednokanałowych.

Aby dokładniej zbadać system, musimy przyjrzeć się częściom składowym bloków. Oprogramowanie SISTEMA do określania tych części składowych stosuje termin „elementy".



Podzielony system z diagnostyką z dwukanałowym systemem bezpieczeństwa

Podsystem wyłączników krańcowych jest przedstawiony z uwzględnieniem podziału na elementy składowe. Podsystem styczników wyjściowych został podzielony na poziomie bloków na dwa. Podsystem logiki nie jest podzielony, ponieważ stanowi element certyfikowany i zatwierdzony przez producenta do umieszczenia na danym poziomie PL. Funkcja monitorowania wyłączników krańcowych oraz styczników jest zadaniem sterownika. W związku z tym pola reprezentujące podsystemy wyłącznika krańcowego i stycznika lekko nachodzą na pole podsystemu logiki.

Zasada dzielenia systemu na mniejsze elementy ma odzwierciedlenie w metodologii przedstawionej w normie EN ISO 13849-1 oraz w zasadach dotyczących podstawowej struktury systemu zawartych w narzędziu SISTEMA. Warto jednak zauważyć, że występują pewne nieznaczne różnice. Norma nie wymaga bezwzględnego stosowania powyższej metodologii, dopuszczając uproszczoną metodę oszacowania poziomu PL, której pierwszym krokiem jest podzielenie całego systemu na kanały, a następnie na bloki w ramach każdego z kanałów. Przy zastosowaniu narzędzia SISTEMA zwykle wygodniejsze jest podzielenie systemu na podsystemy, a następnie każdego podsystemu na bloki. W normie nie opisano w sposób wyraźny koncepcji podsystemów, ale jej zastosowanie w narzędziu SISTEMA stanowi podejście bardziej zrozumiałe i intuicyjne. Oczywiście opisane różnice nie mają wpływu na końcowe obliczenia. Zarówno narzędzie SISTEMA, jak i zapisy normy, korzystają z tych samych zasad i formuł. Warto nadmienić, że podejście podsystemowe jest również wykorzystywane w normie EN/IEC 62061.

System, którego użyliśmy jako przykład jest tylko jednym z pięciu podstawowych typów architektury systemu wyznaczonych przez normę. Osoba znająca pojęcie kategorii rozpozna nasz przykład jako reprezentatywny dla kategorii 3 lub 4.

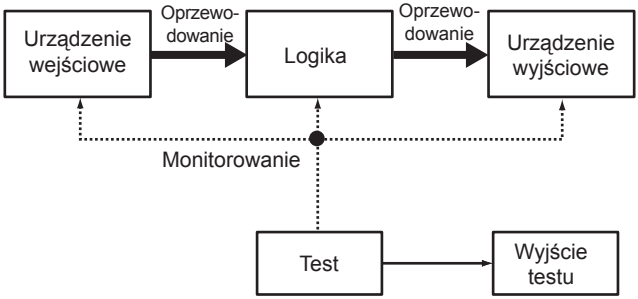
Norma stosuje pięć oryginalnych kategorii z poprzedniej normy EN 954. Są one nazywane kategoriami wskazanej architektury (Designated Architecture Categories). Wymagania dla kategorii są niemal (ale nie zupełnie) identyczne, jak w przypadku normy EN 954-1. Wskazane kategorie architektury są przedstawione na następnych rysunkach. Należy zwrócić uwagę na to, że mogą one być zastosowane w pełnym systemie lub podsystemie. Nie należy rozumieć schematów w kategoriach dosłownej struktury fizycznej. Stanowią one raczej graficzne przedstawienie wymogów koncepcyjnych.

Wskazana architektura kategorii B

Wskazana architektura kategorii B musi wykorzystywać podstawowe zasady bezpieczeństwa (patrz załącznik normy EN ISO 13849-2). System lub podsystem może zawieść w przypadku pojedynczego defektu.
Pełne wymagania można znaleźć w normie EN ISO 13849-1.

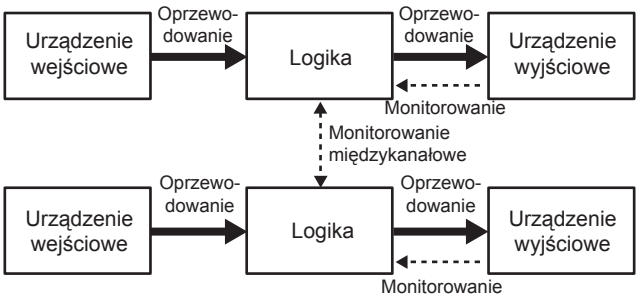
Wskazana architektura kategorii 1

Wskazana architektura kategorii 1 posiada taką samą strukturę jak kategoria B i nadal zawieść w przypadku pojedynczego defektu. Ale w związku z tym, że musi być ona oparta o sprawdzone zasady bezpieczeństwa (patrz załącznik do normy EN ISO 13849-2), staje się to mniej prawdopodobne, niż w przypadku kategorii B. Pełne wymagania można znaleźć w normie EN ISO 13849-1.



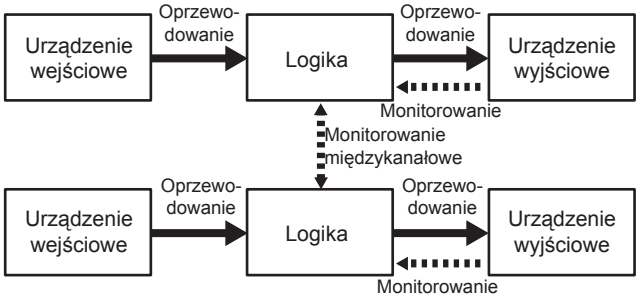
Wskazana architektura kategorii 2

Wskazana architektura kategorii 2 musi wykorzystywać podstawowe zasady bezpieczeństwa (patrz załącznik do normy EN ISO 13849-2). Musi również być zastosowane monitorowanie diagnostyczne za pomocą testu funkcjonalnego systemu lub podsystemu. Musi on nastąpić przy uruchomieniu, a następnie okresowo, z częstotliwością równą stu testom na każde żądanie przywołania funkcji bezpieczeństwa. Poprawka z 2015 roku dopuszcza alternatywny wymóg w stosunku do funkcji bezpieczeństwa, pozwalający jej przejść w stan bezpieczny przed upływem bezpiecznego czasu procesu. System lub podsystem może wciąż zawieść w przypadku wystąpienia pojedynczego błędu między testami funkcjonalnymi, jest to jednak zazwyczaj mniej prawdopodobne niż dla kategorii 1. Należy zauważyć, że dla kategorii 2 użytej do uzyskania poziomu PLd muszą istnieć dwa urządzenia generujące sygnał wyjściowy, ponieważ w przypadku wykrycia błędu testowy sygnał wyjściowy powinien zainicjować stan bezpieczny. Pełne wymagania można znaleźć w normie EN ISO 13849-1.



Wskazana architektura kategorii 3

Wskazana architektura kategorii 3 musi wykorzystywać podstawowe zasady bezpieczeństwa (patrz załącznik do normy EN ISO 13849-2). Występuje również wymóg określający, że w przypadku wystąpienia pojedynczego defektu system/podsystem powinien nadal działać poprawnie. Oznacza to, że system musi być odporny na jeden defekt w funkcji bezpieczeństwa. Najbardziej typowym sposobem spełnienia tego wymogu jest zastosowanie architektury dwukanałowej, która została przedstawiona powyżej. Kolejny wymóg dotyczy konieczności wykrywania pojedynczych defektów tam, gdzie to możliwe. Jest to taki sam wymóg, jak oryginalny wymóg dotyczący kategorii 3 w normie EN 954-1. W tamtym kontekście znaczenie frazy „tam, gdzie to możliwe" wydaje się nieco problematyczne. Oznaczałoby to bowiem, że kategoria 3 obejmuje wszystkie systemy redundantne bez wykrywania defektów (często określane dosadnie jako „głupia redundancja"), jak również systemy redundantne z wykrywaniem wszystkich pojedynczych defektów. Problem ten został rozwiązany w EN ISO 13849-1 przez określenie jakości pokrycia diagnostycznego (DC, Diagnostic Coverage). Da się zauważyć, że im większa niezawodność ($MTTF_D$) systemu, tym mniejsze jest wymagane pokrycie diagnostyczne. Jednak w każdym wypadku pokrycie dla architektury kategorii 3 nie może być mniejsze niż 60%.



Wskazana architektura kategorii 4

Wskazana architektura kategorii 4 musi wykorzystywać podstawowe zasady bezpieczeństwa (patrz załącznik do normy EN ISO 13849-2). Ma ona podobny schemat

jak kategoria 3, ale wymaga ona lepszego monitorowania, tj. wyższego pokrycia diagnostycznego. Przedstawiają to grubsze kropkowane linie oznaczające funkcje monitorowania. Zasadnicza różnica między kategorią 3 a 4 jest taka, że w przypadku kategorii 3 musi być wykryta większość defektów, a w przypadku kategorii 4 muszą być wykryte wszystkie pojedyncze niebezpieczne defekty i ich kombinacje. W praktyce jest to zazwyczaj osiągane dzięki wysokiemu poziomowi diagnostyki, która daje pewność, że wszystkie istotne błędy zostaną wykryte zanim dojdzie do ich kumulacji. Pokrycie diagnostyczne musi wynosić przynajmniej 99%.

Dane o niezawodności

Norma EN ISO 13849-1 wykorzystuje ilościowe dane o niezawodności do obliczeń poziomu PL osiąganego przez elementy systemu sterowania związane z bezpieczeństwem. Pierwsze pytanie, które się z tym wiąże, brzmi „skąd brać te dane?" Można używać danych z uznawanych podręczników niezawodności, ale norma wyraźnie określa, że preferowanym źródłem jest producent. Dlatego też firma Rockwell Automation udostępnia istotne informacje w formie biblioteki danych dla narzędzia SISTEMA.
Zanim zagłębimy się w szczegóły, musimy ustalić jakiego typu dane są wymagane oraz dowiedzieć się, jak są one opracowywane.

Najważniejszym typem danych wymaganych jako część ustalania poziomu działania PL w normie (i programie SISTEMA) jest PFH (prawdopodobieństwo defektu niebezpiecznego na godzinę). Są to te same dane, co w normie IEC 61508, określane skrótem PFH_D stosowanym w normie IEC/EN 62061.

PL (poziom zapewnienia bezpieczeństwa)	PFH_D (prawdopodobieństwo defektu niebezpiecznego na godzinę)	SIL (poziom nienaruszalności bezpieczeństwa)
a	$\geq 10^{-5}$ do $<10^{-4}$	Brak
b	$\geq 3 \times 10^{-6}$ do $<10^{-5}$	1
c	$\geq 10^{-6}$ do $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ do $<10^{-6}$	2
e	$\geq 10^{-8}$ do $<10^{-7}$	3

Powyższa tabela przedstawia relację między PFH_D a PL i SIL. W przypadku niektórych podsystemów, PFH_D można uzyskać od producenta. Ułatwia to obliczenia. Producent zazwyczaj będzie musiał przeprowadzić względnie skomplikowane obliczenia i/lub testy podsystemów, aby uzyskać dane. W przypadku, gdy są one niedostępne, norma EN ISO 13849-1 zezwala na alternatywne uproszczone podejście, bazujące na współczynniku $MTTF_D$ (średni czas do defektu niebezpiecznego) dla jednego kanału. Poziom PL (a co za tym idzie PFH_D) systemu lub podsystemu może być następnie obliczony za pomocą metodologii i wzorów podanych w normie. Można to zrobić jeszcze wygodniej, korzystając z narzędzia SISTEMA.

UWAGA: Trzeba mieć świadomość, że w przypadku systemu dwukanałowego (z diagnostyką lub bez) zastosowanie formuły $1/PFH_D$ do określenia $MTTF_D$ nie jest prawidłową metodą w rozumieniu normy EN ISO 13849-1. Norma ta wymaga ustalenia $MTTF_D$ dla pojedynczego kanału. Wartość ta znacznie różni się od wartości $MTTF_D$ dla kombinacji dwóch kanałów lub podsystemu dwukanałowego. Jeśli znane jest PFH_D podsystemu dwukanałowego, można wprowadzić tę wielkość bezpośrednio do narzędzia SISTEMA.

$MTTF_D$ pojedynczego kanału

Oznacza średni czas przed wystąpieniem uszkodzenia, które mogłoby prowadzić do utraty funkcji bezpieczeństwa. Jest wyrażony w latach. Jest to uśredniona wartość $MTTF_D$ dla „bloków" każdego kanału i może być zastosowana w systemie lub podsystemie. Norma podaje następujący wzór, który jest używany do obliczania średniej ze wszystkich $MTTF_D$ każdego elementu użytego w pojedynczym kanale lub podsystemie.

Na tym etapie wartość narzędzia SISTEMA staje się widoczna. Użytkownicy nie muszą tracić czasu na żmudne analizy tabeli i obliczenia wzorów, ponieważ te działania są wykonywane przez oprogramowanie. Końcowe wyniki można wydrukować w formie wielostronicowego raportu.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$

Wzór D1 z normy EN ISO 13849-1

W większości systemów dwukanałowych oba kanały są identyczne, w związku z czym wynik otrzymany przy zastosowania wzoru reprezentuje dowolny z kanałów.

Jeśli kanały systemu/podsystemu są inne, norma proponuje wzór, który uwzględnia te różnice.

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

Ten wzór w rezultacie uśrednia dwie wartości średnie. W ramach uproszczenia, dopuszczalne jest również użycie wartości dla najgorszego kanału.

Norma grupuje $MTTF_D$ w trzech zakresach:

Oznaczenie $MTTF_D$ każdego kanału	**Zakres $MTTF_D$ każdego kanału**
Niskie	3 lata <= $MTTF_D$ < 10 lat
Średnie	10 lat <= $MTTF_D$ < 30 lat
Wysokie	30 lat <= $MTTF_D$ < 100 lat

Poziomy $MTTF_D$

Należy zwrócić uwagę, że norma EN ISO 13849-1 ogranicza przydatną wartość $MTTF_D$ pojedynczego kanału podsystemu do maks. 100 lat, nawet jeśli uzyskane wartości rzeczywiste są znacznie wyższe.

Jak przekonamy się później, uzyskany zakres średniego $MTTF_D$ jest następnie zestawiany z kategorią wskazanej architektury oraz pokryciem diagnostycznym (DC) w celu uzyskania wstępnej oceny PL. Został tutaj użyty termin „wstępnej", ponieważ nadal muszą być spełnione inne wymogi, w tym nienaruszalność systemowa oraz środki przeciwko defektom wywołanym wspólną przyczyną.

Metody wyznaczania danych

Należy teraz sięgnąć o jeden poziom głębiej w zagadnienie w jaki sposób producent uzyskuje dane w formie PFH_D lub $MTTF_D$. Zrozumienie tego zagadnienia jest kwestią zasadniczą w przypadku pracy z danymi producenta. Komponenty można pogrupować na trzy podstawowe typy:

- Mechaniczne (elektromechaniczne, mechaniczne, pneumatyczne, hydrauliczne itp.)
- Elektroniczne (tj. półprzewodnikowe)
- Oprogramowanie

Występuje zasadnicza różnica pomiędzy typowymi mechanizmami uszkodzeń dla tych trzech typów technologii. Zasadniczo można to podsumować następująco:

Technologia mechaniczna:

Prawdopodobieństwo wystąpienia uszkodzenia jest proporcjonalne do niezawodności i kategorii użytkowania. Im większa intensywność użytkowania, tym bardziej możliwe jest, że jedna z części składowych systemu ulegnie uszkodzeniu i przestanie działać. Należy zauważyć, że intensywne korzystanie z maszyny nie jest jedyną przyczyną awarii. Jeśli jednak nie ograniczymy czasu lub liczby cykli działania, będzie to przyczyna najczęstsza. Stycznik o cyklu przełączania raz na dziesięć sekund będzie bez wątpienia działał niezawodnie znacznie krócej niż identyczny stycznik wykonujący jedno przełączenie dziennie.

Urządzenia mechaniczne zawierają zazwyczaj elementy projektowane indywidualnie z myślą o konkretnym zastosowaniu. Elementy te są kształtowane, formowane, odlewane,

poddawane obróbce itd., a następnie łączone za pomocą cięgien, sprężyn, magnesów, uzwojeń elektrycznych itd. w celu utworzenia określonego mechanizmu. Ponieważ części składowe zazwyczaj nie mają żadnej historii zastosowania w innych aplikacjach, nie da się odnaleźć żadnych istniejących danych dotyczących niezawodności. Oszacowanie wartości współczynników PFH_D oraz $MTTF_D$ mechanizmu jest zazwyczaj oparte na testach. Obie normy EN/IEC 62061 i EN ISO 13849-1 zalecają procedurę testową znaną jako test $B10_D$.

W ramach testu $B10_D$ grupa badanych urządzeń (zazwyczaj co najmniej 10) jest testowana w środowisku odzwierciedlającym warunki robocze. Średnia liczba cykli roboczych osiągniętych do czasu, gdy 10% badanych urządzeń ulegnie defektowi prowadzącemu do uszkodzenia niebezpiecznego, nazywana jest wartością B10d. W praktyce często zdarza się, że wszystkie urządzenia przechodzą do stanu bezpiecznego. W takiej sytuacji norma określa, że wartość B10d (niebezpieczna) przyjmuje podwojoną wartość B10.

Technologia elektroniczna:

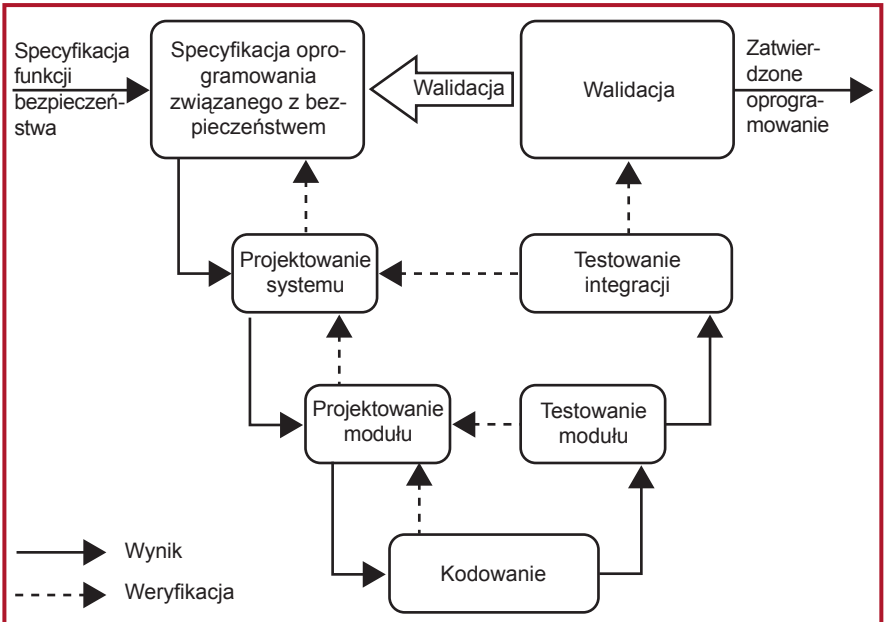
W tym przypadku nie występuje mechaniczne zużycie ruchomych części. Jeśli środowisko robocze zapewnia warunki zgodne z charakterystyką elektryczną i temperaturową, większość defektów obwodu elektronicznego jest proporcjonalna do niezawodności (lub jej braku) jego elementów składowych. Defekt pojedynczego elementu może mieć wiele przyczyn, np. niedokładne wykonanie, nadmierne przepięcia zasilania, problemy z połączeniami mechanicznymi itd. Defekty elementów elektronicznych są zasadniczo wywoływane przez obciążenie, czas i temperaturę, ale trudno je przewidzieć na drodze analizy, a ich natura jest przypadkowa. W związku z tym przeprowadzenie testów urządzenia elektronicznego w warunkach laboratoryjnych niekoniecznie pozwala opracować długoterminowe wzorce awarii.

W celu określenia niezawodności urządzeń elektronicznych korzysta się zwykle z analizy i obliczeń. Wiarygodne dane dotyczące poszczególnych elementów można odnaleźć w podręcznikach dotyczących niezawodności. Analiza danych pozwala wyznaczyć elementy, których defekt może być niebezpieczny. Przyjmuje się za dopuszczalne uśrednianie rodzajów uszkodzeń elementów jako w 50% bezpieczne, a w 50% niebezpieczne. Przyjęcie takiego założenia to jednak bardzo ostrożny szacunek.

W normie IEC 61508 podano wzory służące do obliczania ogólnego prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego (PFH lub PFD) urządzenia, tj. podsystemu. Są one dość skomplikowane i uwzględniają (tam, gdzie to możliwe) dane dotyczące niezawodności elementów, ryzyka wystąpienia defektów wywołanych wspólną przyczyną (współczynnik beta), pokrycia diagnostycznego (DC), interwału testu funkcjonalnego oraz testu sprawdzającego. Jest jednak dobra wiadomość. Złożone obliczenia są zazwyczaj wykonywane przez producenta urządzenia. Normy EN/IEC 62061 i EN ISO 13849-1 dopuszczają wykonywanie obliczeń dla podsystemu w ten sposób zgodnie z normą IEC 61508. Uzyskany PFH_D może być wykorzystany bezpośrednio w załączniku K normy EN ISO 13849-1 lub w narzędziu obliczeniowym SISTEMA.

Oprogramowanie:

Błędy oprogramowania są w swojej naturze zawsze systematyczne. Wynikają one ze sposobu opracowania, napisania lub kompilowania programu. W związku z tym wszystkie są spowodowane przez sam system projektowania, a nie przez działanie programu. Kontrolowanie błędów oprogramowania oznacza zatem konieczność kontrolowania tego systemu. Wymagania oraz metodologie dotyczące tego zadania znajdują się w normach IEC 61508 i EN ISO 13849-1. W niniejszej publikacji nie będziemy ich szczegółowo omawiać. Wystarczy powiedzieć, że wykorzystano w nich klasyczny model V. Dodatkowe utrudnienie dla projektanta stanowi oprogramowanie wbudowane. Najbardziej typowym podejściem jest zaprojektowanie oprogramowania wbudowanego zgodnie z metodami formalnymi opisanymi w IEC 61508-3. W przypadku kodu aplikacji używanego przez programistę, w większości programowalnych urządzeń bezpieczeństwa wykorzystuje się „certyfikowane" bloki funkcyjne i procedury. Upraszcza to walidację poprawności kodu aplikacji. Należy jednak pamiętać, że walidacji poprawności trzeba także poddać gotowy program. Sposób łączenia i parametryzacji bloków musi zostać zatwierdzony jako prawidłowy i właściwy w odniesieniu do przeznaczenia. Wytyczne dotyczące tego procesu znajdują się w normach EN ISO 13849-1 i IEC/EN 62061.



Model V projektowania oprogramowania

Pokrycie diagnostyczne

Temat ten został już poruszony przy okazji omawiania wskazanych architektur kategorii 2, 3 i 4. Kategorie te wymagają przeprowadzenia pewnych testów diagnostycznych, których zadaniem jest sprawdzenie, czy funkcje bezpieczeństwa nadal działają. Do opisania efektywności testowania używane jest pojęcie „pokrycia diagnostycznego" (często używany jest skrót DC). Należy zauważyć, że współczynnik DC opiera się nie tylko na liczbie elementów, które mogą ulec niebezpiecznemu uszkodzeniu. Bierze pod uwagę całkowitą częstość występowania uszkodzeń niebezpiecznych. Wielkość ta jest oznaczana symbolem λ i określana mianem „wskaźnika awaryjności". Współczynnik DC wyraża związek częstości występowania uszkodzeń z dwoma poniższymi typami uszkodzeń niebezpiecznych.

Wykryte uszkodzenie niebezpieczne (λdd): defekty powodujące lub mogące spowodować utratę funkcji bezpieczeństwa, lecz dające się wykryć. Po wykryciu defektu funkcja reagująca na defekt powoduje przejście systemu do stanu bezpiecznego.

Uszkodzenie niebezpieczne (λd): wszystkie defekty powodujące lub mogące spowodować utratę funkcji bezpieczeństwa. Do grupy tej zaliczane są zarówno uszkodzenia wykryte, jak i niewykryte. Oczywiście najbardziej niebezpiecznymi uszkodzeniami są te, które pozostają niewykryte (oznaczone symbolem λdu).

Pokrycie diagnostyczne DC jest wyrażone wzorem;
DC = λdd/λd wyrażone w procentach.

Znaczenie pojęcia DC w normach EN ISO 13849-1 i EN/IEC 62061 jest identyczne, różne są jednak metody obliczania tego współczynnika. W drugiej normie zaproponowano użycie obliczeń opartych na analizie trybu uszkodzenia, jednak dopuszczalna jest również metoda uproszczona, wykorzystująca tabele zawarte normie EN ISO 13849-1. W tabelach tych przedstawione są typowe techniki diagnostyczne wraz z odpowiadającymi im procentowymi współczynnikami DC. W pewnych przypadkach nadal należy jednak ufać zdrowemu rozsądkowi. W niektórych technikach współczynnik DC jest na przykład proporcjonalny do częstości wykonywania testów. Czasem powstają dyskusje, w których pada stwierdzenie, że powyższe podejście jest zbyt ogólne. Obliczanie współczynnika DC może jednak zależeć od wielu różnych zmiennych. Bez względu na zastosowaną technikę, uzyskane wyniki mogą traktowane tylko jako dane szacunkowe.

Należy również pamiętać, że tabele EN ISO 13849-1 oparto na wynikach intensywnych badań przeprowadzonych przez instytut IFA, które uzyskano, stosując sprawdzone, rzeczywiste techniki diagnostyczne używane w rzeczywistych aplikacjach. Uproszczając, norma dzieli współczynnik DC na cztery podstawowe zakresy:

<60% = brak
60% to <90% = niskie
90% to <99% = średnie
≥99% = wysokie

Podejście polegające na pracy z zakresami, a nie dokładnymi wartościami procentowymi również można potraktować jako bardziej realistyczne, gdy uwzględnimy realny poziom dokładności. Narzędzie SISTEMA wykorzystuje te same tabele wyszukiwania co norma. W związku z tym, że zastosowanie złożonej elektroniki wzrasta w urządzaniach związanych z bezpieczeństwem, zakres DC staje się ważniejszym wskaźnikiem. Prawdopodobnie dalsze prace związane z normami będą w dalszym ciągu zajmować się wyjaśnianiem tych kwestii. Tymczasem korzystanie z intuicji inżynierskiej i zdrowego rozsądku powinno wystarczyć w wyborze odpowiedniego zakresu DC.

Defekty wywołane wspólną przyczyną

W większości systemów lub podsystemów dwukanałowych (tj. odpornych na jeden błąd) zasada diagnostyczna opiera się na przesłance, że nie wystąpią jednocześnie uszkodzenia niebezpieczne obu kanałów. Termin „jednocześnie" można sprecyzować jako „w przedziale czasowym testu diagnostycznego". Jeśli przedział czasowy testu diagnostycznego jest w miarę krótki (np. krótszy niż osiem godzin) można w uzasadniony sposób założyć, że jest bardzo mało prawdopodobne, aby wystąpiły w tym czasie dwa oddzielne i niezależne uszkodzenia. Jednak norma wyjaśnia, że należy dobrze zastanowić się nad tym, czy możliwości wystąpienia uszkodzeń naprawdę są oddzielne i niezależne. Na przykład, jeśli uszkodzenie jednego elementu może zgodnie z logicznym rozumowaniem prowadzić do uszkodzenia innych elementów, wtedy wszystkie zaistniałe uszkodzenia są uważane za defekt pojedynczy.

Możliwe jest również, że zdarzenie, które wywołuje uszkodzenie jednego elementu, może również wywoływać uszkodzenie innych elementów. Nazywa się to „defektem wywołanym wspólną przyczyną" i termin ten najczęściej występuje jako skrót CCF. Gęstość występowania CCF jest z reguły określana jako współczynnik beta (β). Bardzo ważne jest, aby projektanci podsystemów i systemów brali pod uwagę możliwość wystąpienia CCF. Istnieje wiele różnych typów CCF i odpowiadających im metod zapobiegania. W normie EN ISO 13849-1 zaproponowano racjonalny kompromis między nadmierną złożonością a zbytnim uproszczeniem. Podobnie jak w EN/IEC 62061 zdecydowano się na rozwiązanie typowo jakościowe. Zostało to zrealizowane przez zestawienie środków, których efektywność w zapobieganiu występowania CCF została potwierdzona.

Nr	Środek przeciw CCF	Punkty
1	Separacja/oddzielenie	15
2	Zróżnicowanie	20
3	Projekt/aplikacja/doświadczenie	20
4	Szacowanie/analiza	5
5	Umiejętności/szkolenie	5
6	Środowisko	35

Punktowanie środków przeciw defektom wywołanym wspólną przyczyną

Odpowiednia liczba tych środków musi być zaimplementowana w projekcie systemu lub podsystemu. Można stwierdzić przy pewnym uzasadnieniu, że stosowanie samej tej listy może nie być adekwatne w zakresie zapobiegania wszystkim możliwym defektom CCF. Jednak jeśli rozważy się prawidłowo intencję tej listy, stanie się oczywiste, że sensem jej wymogu jest sprawienie, aby projektant przeanalizował możliwości dotyczące CCF oraz wdrożył odpowiednie środki zaradcze na podstawie typu technologii i właściwości aplikacji. Użycie listy narzuca uwzględnienie pewnych najbardziej fundamentalnych i skutecznych technik, takich jak zróżnicowanie trybów uszkadzania i kompetencje projektowania. Narzędzie SISTEMA instytutu IFA wymaga również użycia tabeli środków zapobiegających wystąpieniu CCF i udostępnia je w wygodnej formie.

Błędy systematyczne

We wcześniejszych rozdziałach omówiono jakościowe dane bezpieczeństwa dotyczące niezawodności. Za przykład posłużyły współczynnik $MTTF_D$ i prawdopodobieństwo wystąpienia defektu niebezpiecznego. Temat nie został jednak jeszcze całkowicie wyczerpany. Omawiając powyższe pojęcia, tak naprawdę braliśmy pod uwagę defekty o charakterze przypadkowym. Nawet norma IEC/EN 62061 wyraźnie określa skrót PFH_D jako prawdopodobieństwo wystąpienia przypadkowego defektu sprzętu. Są jednak pewne typy defektów, znane jako „błędy systematyczne”. Można je przypisać błędom wynikającym z projektu lub procesu wytwarzania. Klasycznym przykładem może posłużyć błąd występujący w kodzie programu. Sposoby unikania tego typu błędów (a zarazem defektów) opisano w Aneksie G normy. Opisane tam środki zapobiegania dotyczą stosowania odpowiednich materiałów i technik produkcyjnych, przeglądów, analiz i symulacji komputerowych. W każdym środowisku roboczym występują możliwe do przewidzenia zdarzenia oraz zjawiska. Jeśli następstwa ich wystąpienia nie są kontrolowane, mogą doprowadzić do wystąpienia uszkodzenia. Aneks G opisuje również środki przydatne w takich sytuacjach. Na przykład łatwo jest przewidzieć, że w systemie mogą występować zaniki zasilania. W związku z tym brak zasilania elementu musi skutkować stanem bezpiecznym systemu. Stosowane środki zapobiegawcze często wynikają ze zdrowego rozsądku, ale są zawsze konieczne. Jeśli błędy systematyczne nie będą kontrolowane i unikane, wszystkie pozostałe wymagania normy mogą okazać się pozbawione znaczenia. W niektórych przypadkach będzie również konieczne zastosowanie środków zapobiegawczych identycznych jak dla nadzorowania przypadkowych defektów sprzętowych (w celu uzyskania wymaganego współczynnika PFH_D), takich jak automatyczne testy diagnostyczne lub stosowanie urządzeń redundantnych.

Wykluczanie defektów

Jednym z podstawowych narzędzi służących do analizy systemów bezpieczeństwa jest analiza uszkodzeń. Projektant i użytkownik muszą zrozumieć, jak system bezpieczeństwa będzie zachowywać się w przypadku wystąpienia defektu. Analizę można wykonać, wykorzystując różne techniki. takie jak analiza drzewa defektów, analiza rodzajów, skutków i krytyczności uszkodzeń, analiza drzewa zdarzeń oraz przeglądy intensywności obciążenia.

Podczas wykonywania analizy może okazać się, że niektóre defekty nie mogą być wykryte przez automatyczne testy diagnostyczne bez poniesienia nadmiernych kosztów. Ponadto prawdopodobieństwo ich wystąpienia może być bardzo małe dzięki projektowi, konstrukcji i metodom testowania ukierunkowanym na maksymalną redukcję defektów. W takiej sytuacji defekty można wykluczyć z dalszych rozważań. Wykluczenie defektu polega na odrzuceniu możliwości jego wystąpienia, gdy prawdopodobieństwo zaistnienia tego zdarzenia w systemie SRCS jest pomijalne.

Norma EN ISO 13849-1 umożliwia wykluczenie defektu na podstawie technicznego nieprawdopodobieństwa jego wystąpienia, powszechnie akceptowanego doświadczenia technicznego i wymagań technicznych związanych z aplikacją. Norma EN ISO 13849-2 podaje przykłady i uzasadnienie wykluczenia niektórych defektów w przypadku systemów elektrycznych, pneumatycznych, hydraulicznych i mechanicznych. Każde wykluczenie defektu należy szczegółowo uzasadnić w prowadzonej dokumentacji technicznej.

Ocena systemu sterowania związanego z bezpieczeństwem (SRCS), w którym nie przyjęto założenia, że niektóre defekty można wykluczyć, nie zawsze jest możliwa. Szczegółowe informacje na temat wykluczania defektów znajdują się w normie ISO 13849-2.

Gdy poziom ryzyka zwiększa się, uzasadnienie wykluczenia defektu staje się bardziej surowe. Ogólnie rzecz biorąc, jeśli poziom zapewnienia PLe jest wymagany dla funkcji bezpieczeństwa, która ma być wdrożona przez system sterowania związany z bezpieczeństwem, osiągnięcie tego poziomu nie może być oparte wyłącznie na wykluczeniu defektów. Jest to uzależnione od zastosowanej technologii oraz docelowego środowiska pracy. W związku z tym niezbędne jest, aby projektant podjął dodatkowe środki w zakresie stosowania wykluczania defektów, wraz ze wzrostem wymogów w zakresie poziomu PL.

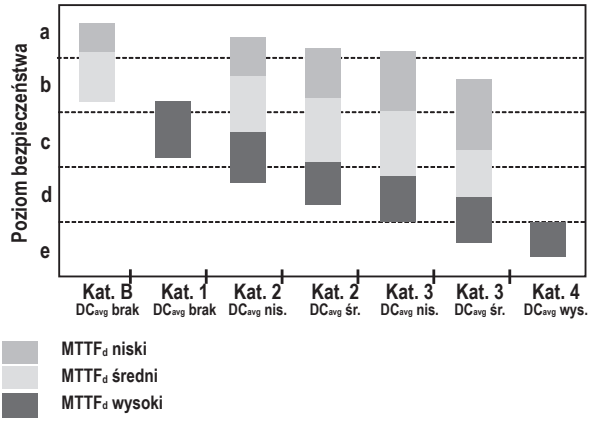
Poziom zapewnienia bezpieczeństwa (PL)

Poziom działania to poziom dyskretny, określający zdolność elementów systemu sterowania związanych z bezpieczeństwem do wykonania funkcji bezpieczeństwa.

Aby oszacować PL uzyskany przez wdrożenie jednej z pięciu architektur wskazanych, potrzebne są następujące dane systemu (lub podsystemu):

- $MTTF_D$ (średni czas do defektu niebezpiecznego w każdym kanale)
- DC (pokrycie diagnostyczne)
- Architektura (kategoria)

Na poniższym schemacie przedstawiono graficzną metodę określania PL na podstawie wymienionych wyżej współczynników. Tabela w załączniku K zawiera rezultaty z modeli Markowa w formie tabelarycznej, na których opiera się ten schemat. Z tabeli tej należy korzystać, jeśli wymagane jest dokładniejsze określenie poziomu.



Graficzne wyznaczanie PL

Aby uzyskać zgodność z wymaganym PL, należy wziąć pod uwagę pozostałe czynniki. Dotyczą one wymagań dla defektów o wspólnej przyczynie, błędów systematycznych, warunków środowiskowych i czasu misji. Jeżeli parametr PFH_D systemu lub podsystemu jest znany, tabele w załączniku K mogą posłużyć do obliczenia poziomu PL.

Projektowanie i łączenie podsystemów

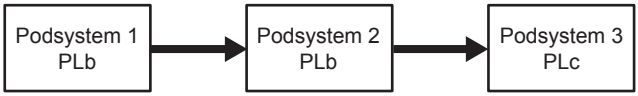
Podsystemy o określonym poziomie PL mogą być łączone w system przy użyciu poniższej tabeli.

PL_{low}	**N_{low}**	**PL**
a	>3	niedozwolone
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Obliczanie PL dla podsystemów połączonych szeregowo

Użycie niniejszej tabeli nie jest konieczne; może to być jedynie bardzo prosta alternatywna metoda określenia najbardziej niekorzystnych wartości PFHd, jeśli nie są one znane. Poziom wydajności PL można obliczyć za pomocą innych metod, w tym narzędzia SISTEMA. Powody, dla których można skorzystać z tabeli są oczywiste. Po pierwsze, system może być tylko tak dobry, jak jego najsłabszy podsystem. Po drugie, im więcej podsystemów, tym większe prawdopodobieństwo wystąpienia defektu.

W systemie przedstawionym na poniższym schemacie najniższy poziom działania mają podsystemy 1 i 2. Oba mają PLb. Oznacza to, że korzystając z tabeli, należy czytać wiersz b (w kolumnie PLlow), następnie wiersz 2 (w kolumnie Nlow), aby w końcu odczytać uzyskany poziom PL jako b (w kolumnie PL). Gdyby wszystkie trzy podsystemy były zgodne z PLb, uzyskany poziom PL całego systemu byłby PLa.



Połączenie szeregowe podsystemów tworzących system PLb

Walidacja

Walidacja funkcji bezpieczeństwa obejmuje i przekracza zakres weryfikacji uzyskanych poziomów zapewnienia bezpieczeństwa. Celem walidacji jest uwierzytelnienie wdrożonej funkcji bezpieczeństwa pod względem spełnienia przez nią wszystkich ogólnych wymagań bezpieczeństwa dla maszyny. Walidacja odgrywa ważną rolę w procesie projektowania systemów bezpieczeństwa i oddawania ich do użytku. Wymagania dla walidacji zostały określone w normie ISO/EN 13849-2:2012. Wymaga ona planu walidacji i opiera się na technikach testowania i analizowania, takich jak analiza drzewa defektu oraz analiza rodzajów, skutków i krytyczności uszkodzeń (FMEA). Większość przedstawionych wymagań będzie dotyczyć producenta, a nie użytkownika podsystemu.

Oddanie maszyny do użytku

Na etapie oddawania maszyny do użytku należy przeprowadzić walidację funkcji bezpieczeństwa we wszystkich trybach pracy, uwzględniając wszystkie normalne i przewidywalne sytuacje nietypowe. Konieczne jest także wzięcie pod uwagę różnych kombinacji wejść oraz kolejności wykonywanych operacji. Procedura ta jest ważna, ponieważ należy zawsze sprawdzić, czy system nadaje się do zastosowania w rzeczywistym środowisku roboczym. Charakterystyki mogą czasem różnić się od tych, których oczekiwano na etapie projektowania.

Rozdział 8: Projektowanie systemu wg IEC/EN 62061

IEC/EN 62061 – „Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i programowalnych elektronicznych systemów sterowania związanych z bezpieczeństwem" – to wersja normy IEC/EN 61508 mająca zastosowanie do maszyn. Przedstawia wymagania do projektowania, na poziomie systemu, maszynowych elektrycznych systemów sterowania związanych z bezpieczeństwem, a także projektowania niezłożonych podsystemów i urządzeń.

Wyniki oceny ryzyka służą do opracowania strategii ograniczania ryzyka, która z kolei identyfikuje funkcje sterowania związane z bezpieczeństwem. Funkcje te należy udokumentować, uwzględniając:

- specyfikację wymagań funkcjonalnych oraz
- specyfikację wymagań nienaruszalności bezpieczeństwa.

Wymagania funkcjonalne zawierają szczegóły dotyczące częstości działania, wymaganego czasu odpowiedzi, trybów pracy, cykli obciążenia, środowiska roboczego oraz funkcji reagowania na defekty. Wymagania nienaruszalności bezpieczeństwa są wyrażone za pomocą poziomów nienaruszalności bezpieczeństwa (SIL). W zależności od złożoności systemu, aby określić czy projekt systemu spełnia wymagany SIL, należy brać pod uwagę niektóre lub wszystkie elementy przedstawione w poniższej tabeli.

Elementy do określania SIL	**Symbol**
Prawdopodobieństwo defektu niebezpiecznego na godzinę	PFH_D
Tolerancja defektów sprzętu	HFT
Udział uszkodzeń bezpiecznych	SFF
Odstęp między testami kontrolnymi	T_1
Interwał między testami diagnostycznymi	T_2
Podatność na defekty wywołane wspólną przyczyną	β
Pokrycie diagnostyczne	DC

Wielkości związane z poziomami SIL

Podsystemy

Termin „podsystem" ma w IEC/EN 62061 specjalne znaczenie. Jest to pierwszy poziom podziału systemu na części, które jeśli zawiodą, mogą spowodować utratę funkcji bezpieczeństwa. Oznacza to, że jeśli w systemie zastosowano dwa wyłączniki redundantne, żaden z nich nie jest podsystemem. Na podsystem składają się oba wyłączniki oraz powiązana z nimi funkcja wykrywania defektów.

Prawdopodobieństwo defektu niebezpiecznego na godzinę (*PFH*$_D$)

W celu określenia wskaźnika awaryjności na poziomie elementu norma IEC/EN 62061 wykorzystuje te same podstawowe metody, jak omówione w części dotyczącej normy EN ISO 13849-1. Te same środki i metody mają zastosowanie w przypadku elementów „mechanicznych" i elektronicznych. W normie IEC/EN 62061 nie został uwzględniony czas MTTF$_D$ w latach. Wskaźnik defektów na godzinę (λ) jest obliczany bezpośrednio lub uzyskiwany z wartości B10 na podstawie poniższego wzoru:

λ = 0,1 x C/B10 (gdzie C = liczba cykli roboczych na godzinę)

Występuje znaczna różnica między normami, dotycząca metodologii ustalania całkowitego *PFH*$_D$ dla podsystemu lub systemu. W celu określenia prawdopodobieństwa defektu podsystemu należy przeprowadzić analizę elementów. Podane są wzory, które umożliwiają obliczenia dla typowej architektury podsystemu (opisanej w dalszej części opracowania). Tam gdzie te wzory nie mają zastosowania, konieczne będzie użycie bardziej złożonych metod obliczania, np. modeli Markowa. Prawdopodobieństwo defektu niebezpiecznego na godzinę (*PFH*$_D$) dla każdego podsystemu jest następnie dodawane w celu ustalenia łącznego prawdopodobieństwa *PFH*$_D$ dla systemu. Następnie można użyć tabeli 3 z normy dla określenia, jaki poziom nienaruszalności bezpieczeństwa (SIL) jest właściwy dla tego zakresu parametru *PFH*$_D$.

SIL (poziom nienaruszalności bezpieczeństwa)	***PFH*$_D$ (prawdopodobieństwo defektu niebezpiecznego na godzinę)**
3	≥10^{-8} do <10^{-7}
2	≥10^{-7} do <10^{-6}
1	≥10^{-6} do <10^{-5}

Prawdopodobieństwo defektu niebezpiecznego dla poziomów SIL

Dane dotyczące *PFH*$_D$ dla podsystemu są zazwyczaj podawane przez producenta. Dane dotyczące komponentów i systemów bezpieczeństwa firmy Rockwell Automation można pobrać ze strony:

www.rockwellautomation.com, under Solutions & Services > Safety Solutions

IEC/EN 62061 podaje jasno, że możliwe do użycia są również dane umieszczone w poradnikach o niezawodności, jeżeli są odpowiednie.

Dla urządzeń elektromechanicznych o małej złożoności mechanizm uszkodzeń jest zwykle związany z liczbą i częstością operacji, a nie z czasem. Dlatego też w przypadku tych elementów dane będą pochodzić z pewnych typów testów (np. testy B10 przedstawione w rozdziale dotyczącym normy EN ISO 13849-1). Aby skonwertować B10d lub podobne dane na *PFH*$_D$, wymagane są informacje związane z daną aplikacją, takie jak przewidywana liczba operacji na rok.

UWAGA: w zasadzie poniższe równanie jest prawdziwe (uwzględniając współczynnik zmiany lat na godziny):

$PFH_D = 1/MTTF_D$

Trzeba jednak mieć świadomość, że w przypadku systemu dwukanałowego (z diagnostyką lub bez) zastosowanie formuły $1/PFH_D$ do określenia $MTTF_D$ nie jest prawidłową metodą w rozumieniu normy EN ISO 13849-1. Ta norma wymaga zastosowania parametru $MTTF_D$ dla pojedynczego kanału. Wartość ta znacznie różni się od wartości $MTTF_D$ dla kombinacji dwóch kanałów lub podsystemu dwukanałowego z włączeniem pokrycia diagnostycznego.

Ograniczenia architektury

Cechą zasadniczą normy IEC/EN 62061 jest to, że system bezpieczeństwa jest podzielony na podsystemy. Poziom nienaruszalności bezpieczeństwa, który może być przypisany podsystemowi, jest ograniczony nie tylko przez PFH_D, ale również przez tolerancję defektów sprzętowych i udział uszkodzeń bezpiecznych. Tolerancja defektów sprzętu to zdolność systemu do wykonywania swoich funkcji w obecności defektów. Zerowa tolerancja defektów oznacza, że funkcja nie będzie wykonana po pojawieniu się pojedynczego defektu. Tolerancja jednego defektu oznacza, że podsystem wykona swoje funkcje po pojawieniu się pojedynczego defektu. Udział uszkodzeń bezpiecznych to część całkowitej ilości uszkodzeń, które nie prowadzą do defektów niebezpiecznych. Kombinacja tych dwóch elementów jest znana jako ograniczenia architektury, a jej wartością wyjściową jest SIL CL (SIL Claim Limit – granica żądanego SIL) Związek ograniczeń architektury z poziomami SIL CL przedstawiono w poniższej tabeli. Podsystem (i w związku z tym obejmujący go system) musi spełniać wymagania PFH_D oraz ograniczeń architektury wraz z innymi stosownymi postanowieniami normy.

Udział uszkodzeń bezpiecznych (SFF)	Tolerancja defektów sprzętu		
	0	1	2
<60%	Niedozwolony, oprócz określonych wyjątkowych przypadków	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

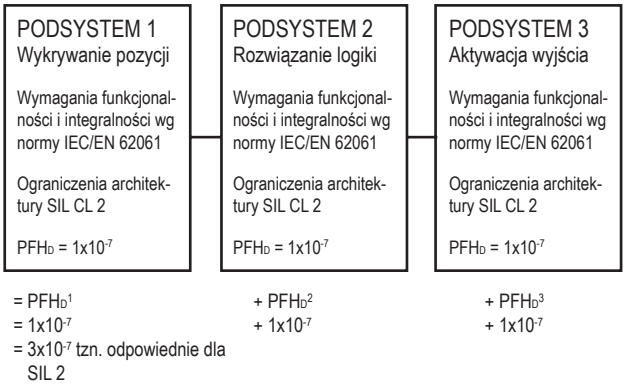
Ograniczenia architektury dla SIL

Na przykład architektura podsystemu, która ma odporność na jeden błąd i udział uszkodzeń bezpiecznych 75%, jest ograniczona maksymalnie do poziomu SIL 2, niezależnie od prawdopodobieństwa wystąpienia defektu niebezpiecznego. W przypadku

łączenia podsystemów, SIL uzyskiwany przez SRCS będzie mniejszy lub równy najniższemu SIL CL dla dowolnego podsystemu, który realizuje funkcje sterowania bezpieczeństwem.

Realizacja systemu

Aby obliczyć prawdopodobieństwo defektu niebezpiecznego, każdą funkcję bezpieczeństwa należy rozbić na bloki funkcyjne, które następnie traktuje się jako podsystemy. Implementacja systemu typowej funkcji bezpieczeństwa zawiera urządzenie wykrywające podłączone do urządzenia logiki, które jest podłączone do napędu. Tworzy to szeregowe połączenie podsystemów. Jak już się przekonaliśmy, jeśli można określić prawdopodobieństwo defektu niebezpiecznego dla każdego podsystemu i znany jest ich SIL CL, wtedy prawdopodobieństwo defektu systemu można łatwo obliczyć, dodając prawdopodobieństwa defektów podsystemów. Koncepcję tą przedstawiono poniżej.



$= PFH_D^1$
$= 1x10^{-7}$
$= 3x10^{-7}$ tzn. odpowiednie dla SIL 2

$+ PFH_D^2$
$+ 1x10^{-7}$

$+ PFH_D^3$
$+ 1x10^{-7}$

Jeżeli jest na przykład wymagane uzyskanie poziomu SIL 2, każdy z podsystemów musi mieć granicę żądanego SIL CL (Claim Limit) na poziomie co najmniej SIL 2, a suma PFH_D dla systemu nie może przekroczyć limitu dozwolonego przez tabelę zestawiającą prawdopodobieństwo defektów niebezpiecznych dla klasyfikacji SIL.

Projektowanie podsystemów – IEC/EN 62061

Jeśli projektant systemu korzysta z elementów, które są „spakowane" w gotowe podsystemy zgodne z IEC/EN 62061, zadanie jest łatwiejsze, ponieważ wtedy nie mają zastosowania żadne specyficzne wymagania projektowania podsystemów. Te wymagania są zasadniczo spełnione przez producenta urządzenia (podsystemu) i są znacznie bardziej złożone niż te wymagane do projektowania na poziomie systemu.

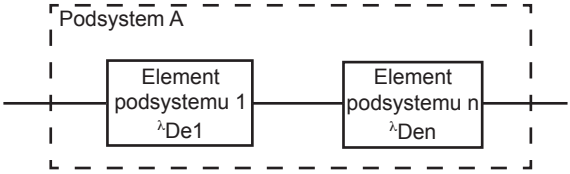
Norma IEC/EN 62061 wymaga, aby złożone podsystemy, takie jak sterowniki bezpieczeństwa były zgodne z normą IEC 61508 lub innymi odpowiednimi normami. Oznacza to, że do urządzeń używających złożone elementy elektroniczne lub programowalne, stosowane są pełne rygory normy IEC 61508. Może to być bardzo

trudnym i wymagającym procesem. Na przykład oszacowanie PFH_D uzyskanego przez złożony podsystem może być bardzo skomplikowanym procesem, wykorzystującym takie techniki, jak modelowanie Markowa, schematy blokowe niezawodności oraz analiza drzewa defektów.

IEC/EN 62061 podaje wymagania do projektowania podsystemów o mniejszej złożoności. Dotyczą one względnie prostych elementów elektrycznych, takich jak wyłączniki blokujące oraz elektromechaniczne przekaźniki bezpieczeństwa. Wymagania nie są tak złożone, jak te w IEC 61508, ale nadal są raczej skomplikowane.

W normie IEC/EN 62061 wyszczególniono cztery architektury logiczne podsystemów oraz podano odpowiadające im wzory do obliczania PFH_D uzyskiwanego przez podsystemy o małej złożoności. Architektury stanowią odwzorowanie wyłącznie logiczne i nie powinny być traktowane jak architektury fizyczne. Cztery architektury logiczne podsystemów wraz z odpowiednimi wzorami przedstawiono na poniższych czterech schematach.

Dla poniższej podstawowej architektury podsystemu, prawdopodobieństwa defektu niebezpiecznego są po prostu dodawane.

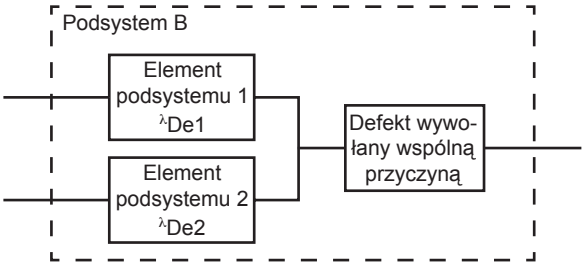


Architektura logiczna podsystemu A

$\lambda DssA = \lambda De1 + \ldots + \lambda Den$
$PFHDssA = \lambda DssA$

Lambda (λ) służy do określenia wskaźnika defektów wyrażonego za pomocą liczby defektów na godzinę. Jednostką wskaźnika defektów jest liczba defektów na godzinę. Lambda D (λD) to wskaźnik defektów niebezpiecznych. Lambda DssA ($\lambda DssA$) to wskaźnik defektów niebezpiecznych podsystemu A. Powstaje przez dodanie wskaźników defektów poszczególnych elementów: e1, e2, e3 itd. aż do en. Aby prawdopodobieństwo wyrażało możliwość wystąpienia uszkodzenia na godzinę, jest ono mnożone przez 1 godzinę.

Na kolejnym schemacie przedstawiono system o tolerancji jednego defektu, bez funkcji diagnostycznych. Jeśli architektura pozwala na tolerancję jednego defektu, należy wziąć pod uwagę możliwość wystąpienia defektów wywołanych wspólną przyczyną. Wyznaczenie współczynnika awarii wywołanej wspólną przyczyną przedstawiono w dalszej części rozdziału.



Architektura logiczna podsystemu B

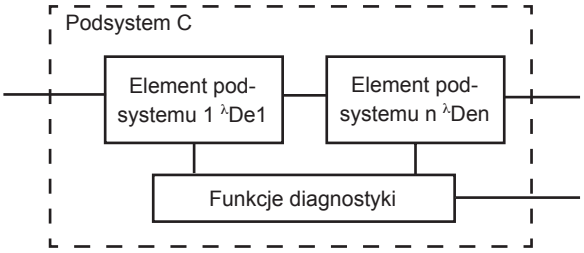
$DssB = (1-\beta)^2 \times \lambda De1 \times \lambda De2 \times T1 + \beta \times (\lambda De1 + \lambda De2)/2$
PFHDssB = λDssB

Wzór dotyczący tej architektury uwzględnia równoległe rozmieszczenie elementów podsystemu oraz wprowadza następujące dwa elementy z poprzedniej tabeli „Wielkości związane z poziomami SIL".

β (beta) – podatność na defekty wywołane wspólną przyczyną

T1 – odstęp między testami kontrolnymi albo czas życia, zależnie od tego, który okres jest krótszy. Test sprawdzający ma na celu wykrycie defektów i degradacji podsystemu bezpieczeństwa, aby mógł powrócić do warunków pracy. W praktyce często oznacza to wymianę (podobnie, jak równoważny termin „czas misji" w normie EN ISO 13849-1).

Na kolejnym schemacie przedstawiono funkcjonalną reprezentację systemu o zerowej tolerancji defektów z funkcją diagnostyczną. W celu zmniejszenia prawdopodobieństwa defektów niebezpiecznych sprzętu używane jest pokrycie diagnostyczne. Testy diagnostyczne są wykonywane automatycznie. Definicja pokrycia diagnostycznego jest taka sama jak podano w normie EN ISO 13849-1, czyli stosunek liczby wykrytych defektów niebezpiecznych do wszystkich defektów niebezpiecznych.

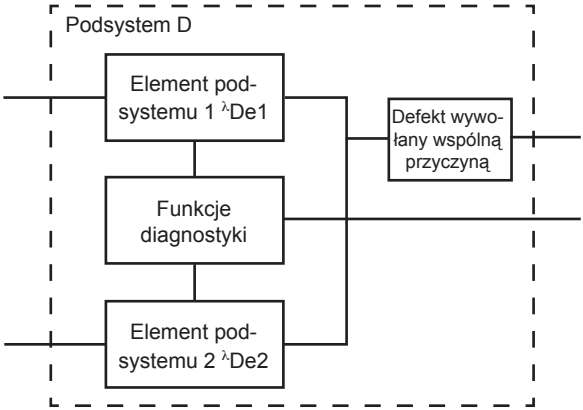


Architektura logiczna podsystemu C

$\lambda_{DssC} = \lambda_{De1} (1 - DC_1) + \ldots + \lambda_{Den} (1 - DC_n)$
PFHDssC = λDssC

W powyższych wzorach uwzględniono pokrycie diagnostyczne (DC) poszczególnych elementów podsystemu. W tej sytuacji wskaźniki defektów każdego podsystemu są redukowane przez odpowiadające im pokrycie diagnostyczne.

Poniżej pokazano czwarty przykład architektury podsystemu. Jest to system odporny na pojedyncze defekty i realizujący funkcje diagnostyczne. W przypadku tolerancji jednego defektu należy także wziąć pod uwagę możliwość defektu wywołanego wspólną przyczyną.



Architektura logiczna podsystemu D

Jeśli elementy podsystemu są różne, zastosowanie mają następujące wzory:

λDssD = (1 – β)2 {[λDe1 x λDe2 x (DC1+ DC2)] x T2/2 + [λDe1 x λDe2 x (2- DC1 – DC2)] x T1/2 } + β x (λDe1 + λDe2)/2
PFHDssD = λDssD

Jeśli elementy podsystemu są identyczne, można zastosować poniższe wzory:

$A_{DssD} = (1 - \beta)^2 \{[\lambda_{De}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}^2 \times (1 - DC)] \times T_1 \} + \beta \times \lambda_{De}$
PFHDssD = λDssD

Należy zauważyć, że w obu wzorach zastosowano jeden dodatkowy parametr T2, czyli interwał diagnostyki. Określa on okresowe testowanie funkcji. Jest to mniej wszechstronny test, niż test sprawdzający.

Przyjmijmy np. następujące wartości w przykładzie, w którym elementy podsystemu są identyczne:

β = 0,05
λDe = 1 x 10^{-6} defektów na godzinę
T1 = 87 600 godzin (10 lat)
T2 = 2 godziny
DC = 90%

PFH_{DssD} = 5,790E-8 defektów niebezpiecznych na godzinę. Mieści się to w zakresie wymaganym dla SIL 3

Wpływ odstępu między testami kontrolnymi

Norma IEC/EN 62061 stanowi, że preferowany (ale nie obligatoryjny) odstęp między testami kontrolnymi (PTI) wynosi 20 lat. Zobaczmy, jaki jest wpływ odstępu między testami kontrolnymi na system. Jeśli przeliczymy wzór z T1 o wartości 20 lat, uzyskamy wynik PFHDssD = 6,58E-8. Mieści się to w dalszym ciągu w zakresie wymaganym dla SIL 3. Projektant musi wziąć pod uwagę, że aby uzyskać w wyniku całkowity wskaźnik defektów niebezpiecznych, dany podsystem musi być połączony z innymi podsystemami.

Analiza wpływu defektu wywołanego wspólną przyczyną

Przeanalizujmy wpływ, jaki defekty wywołane wspólną przyczyną mają na system. Załóżmy, że dzięki dodatkowym środkom poprawiono współczynnik β (beta) do wartości równej 1% (0,01), natomiast odstęp między testami kontrolnymi cały czas wynosi 20 lat. Wskaźnik defektów niebezpiecznych poprawi się, osiągając wartość 2,71E-8, co oznacza, że podsystem jest teraz bardziej odpowiedni do użycia w systemie kategorii SIL 3.

Defekty wywołane wspólną przyczyną (CCF)

Defekt wywołany wspólną przyczyną występuje wtedy, gdy wiele defektów spowodowanych tą samą przyczyną powoduje powstanie uszkodzenia niebezpiecznego. Informacje o CCF są zazwyczaj przydatne tylko dla projektanta podsystemu, którym zwykle jest producent. Używane są one jako składnik wzorów do oszacowania PFH_D podsystemu. CCF nie jest zwykle wymagany przy projektowaniu na poziomie systemu.

Prosta metoda oszacowania CCF została przedstawiona w załączniku F normy IEC/EN 62061. W poniższej tabeli przedstawiono podsumowanie procesu punktowania.

Nr	Środek przeciw CCF	Punkty
1	Separacja/oddzielenie	25
2	Zróżnicowanie	38
3	Projekt/aplikacja/doświadczenie	2
4	Szacowanie/analiza	18
5	Umiejętności/szkolenie	4
6	Środowisko	18

Punktowanie środków przeciwko defektom wywołanym wspólną przyczyną

Środkom zastosowanym przeciwko CCF przyznawana jest punktacja. Przedstawiony w poniższej tabeli współczynnik wspólnej przyczyny defektów oblicza się dodając punkty. Współczynnik beta jest używany w modelowaniu podsystemów do „dostrojenia" wskaźnika defektów.

Łączna liczba punktów	Współczynnik defektu wywołanego wspólną przyczyną (Beta)
<35	10% (0,1)
35 – 65	5% (0,05)
65 – 85	2% (0,02)
85 – 100	1% (0,01)

Współczynnik beta dla awarii wywołanej wspólną przyczyną

Pokrycie diagnostyczne (DC)

W celu zmniejszenia prawdopodobieństwa defektów niebezpiecznych sprzętu wykonuje się automatyczne testy diagnostyczne. Możliwość wykrycia wszystkich defektów niebezpiecznych sprzętu byłaby ideałem, ale w praktyce wartość maksymalna osiąga 99% (można to również wyrazić jako 0,99).

Pokrycie diagnostyczne to stosunek liczby wykrytych defektów niebezpiecznych do liczby wszystkich defektów niebezpiecznych.

$$DC = \frac{\text{Wskaźnik wykrytych niebezpiecznych defektów, } \lambda_{DD}}{\text{Wskaźnik wszystkich niebezpiecznych defektów, } \lambda_{Dtotal}}$$

Zakres wartości pokrycia diagnostycznego wynosi od zera do 99%.

Tolerancja defektów sprzętu

Tolerancja defektów sprzętu odzwierciedla liczbę defektów, które mogą wystąpić w podsystemie, przed wystąpieniem defektu niebezpiecznego. Np. tolerancja jednego defektu oznacza, że dwa defekty mogą spowodować utratę funkcji bezpieczeństwa, a jeden nie.

Zarządzanie bezpieczeństwem funkcjonalnym

Norma podaje wymagania do kontroli zarządzania i działań, które są konieczne do uzyskania elektrycznego systemu sterowania związanego z bezpieczeństwem.

Odstęp między testami kontrolnymi

Odstęp między testami kontrolnymi to czas, po którym podsystem musi zostać gruntowanie sprawdzony lub zastąpiony, aby zapewnić, że stan jest „jak nowy". W sektorze maszynowym jest to w praktyce realizowane przez wymianę podsystemu. Oznacza to, że odstęp między testami kontrolnymi jest zazwyczaj równy czasowi życia. W normie EN ISO 13849-1 czas ten jest nazywany „czasem misji".

Test kontrolny może wykryć defekty i degradację w systemie SRCS, dzięki czemu system można przywrócić do stanu najbardziej zbliżonego do stanu nowości. Test kontrolny musi być w stanie wykryć 100% wszystkich defektów niebezpiecznych z uwzględnieniem funkcji diagnostycznej (jeśli jest stosowana). Poszczególne kanały należy testować osobno.

W przeciwieństwie do testów diagnostycznych, które są wykonywane automatycznie, testy kontrolne są zazwyczaj wykonywane ręcznie przy odłączonej energii. Automatyczne testy diagnostyczne są wykonywane znacznie częściej niż przeprowadzane rzadko testy kontrolne. Testy diagnostyczne (np. impulsowe) mogą być wykorzystywane do automatycznego wykrywania zwarć i przerwań obwodu wyłącznika blokującego.

Odstęp między testami kontrolnymi musi być określony przez producenta. Czasami producent podaje zakres różnych częstotliwości testowania. Zamiast przeprowadzania testu kontrolnego bardziej powszechnie stosowana jest po prostu wymiana podsystemu na nowy.

Udział uszkodzeń bezpiecznych (SFF)

Udział uszkodzeń bezpiecznych jest podobny do pokrycia diagnostycznego, ale uwzględnia dodatkowo wewnętrzną tendencję elementu do niepowodzenia przejścia w stan bezpieczny. Np. przepalenie się bezpiecznika jest uszkodzeniem, ale jest wysokie prawdopodobieństwo, że uszkodzeniem tym jest otwarcie obwodu, co w większości przypadków będzie uszkodzeniem bezpiecznym. SFF to (suma

wszystkich uszkodzeń „bezpiecznych" plus wykrytych uszkodzeń niebezpiecznych) podzielona przez (sumę uszkodzeń „bezpiecznych" plus wykrytych i niewykrytych uszkodzeń niebezpiecznych). Należy zdać sobie sprawę, że jedynymi uwzględnianymi typami uszkodzeń są te, które mogą mieć wpływ na działanie funkcji bezpieczeństwa.

Wartość SFF (jeżeli ma ona znaczenie) jest zazwyczaj podawana przez producenta.

Udział uszkodzeń bezpiecznych (SFF) można obliczyć za pomocą następującego równania:

$$SFF = (\sum\lambda_S + (\sum\lambda_{DD})/((\sum\lambda_S + (\sum\lambda_D)$$

gdzie:

$\sum\lambda_S$ = wskaźnik uszkodzeń bezpiecznych,
$\sum\lambda_S + \sum\lambda_D$ = wskaźnik wszystkich uszkodzeń,
λ_{DD} = wskaźnik wykrytych uszkodzeń niebezpiecznych,
λ_D = wskaźnik wszystkich uszkodzeń niebezpiecznych.

Błędy systematyczne

Norma zawiera wymagania związane z kontrolowaniem i unikaniem błędów systematycznych. Błędy systematyczne różnią się od przypadkowych defektów sprzętu, pojawiających się w przypadkowych momentach i wynikających zwykle ze zużycia elementów składowych urządzeń. Typowe rodzaje możliwych do wystąpienia błędów systematycznych to błędy związane z projektowaniem oprogramowania, błędy projektowania sprzętu, błędy specyfikacji wymagań oraz błędy procedur roboczych. Poniżej wyszczególniono przykładowe etapy, których realizacja jest niezbędna do uniknięcia błędów systematycznych:

- prawidłowy dobór, łączenie, rozmieszczenie, montaż i instalacja elementów;
- stosowanie dobrych praktyk technicznych;
- przestrzeganie specyfikacji producenta oraz instrukcji instalacji;
- zapewnianie kompatybilności między elementami;
- odporność na warunki środowiskowe;
- stosowanie odpowiednich materiałów.

Rozdział 9: Systemy sterowania związane z bezpieczeństwem – uwagi dodatkowe

Przegląd

Ten rozdział dotyczy ogólnych uwarunkowań i zasad dotyczących struktur, które należy wziąć pod uwagę podczas projektowania systemu sterowania związanego z bezpieczeństwem.

Kategorie układów sterowania

„Kategorie" systemów sterowania pochodzą z poprzedniej normy EN 954-1:1996 (ISO 13849-1:1999). Są one jednak nadal często stosowane do opisów konstrukcji systemów sterowania związanych z bezpieczeństwem i pozostają integralnym elementem normy EN ISO 13849-1 jako architektury wskazane. Opis i wymagania poszczególnych kategorii zostały przedyskutowane uprzednio w części „Przegląd normy EN ISO 13849-1" niniejszej publikacji. Zadaniem tego podrozdziału jest przedstawienie uproszczonych, ale praktycznych wskazówek dotyczących sposobów wdrażania struktur kategorii.

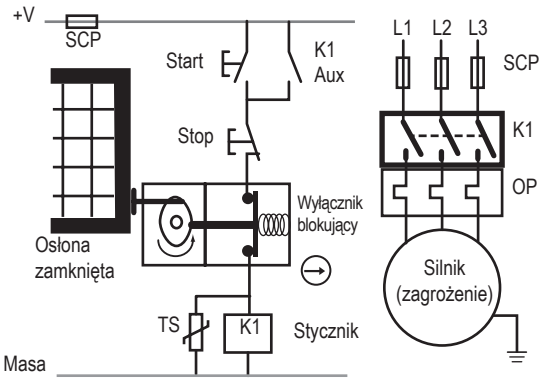
Kategoria B

Kategoria B powinna być brana pod uwagę jako podstawowy „fundament" dla tworzenia wszystkich pozostałych kategorii. Nie zawiera ona żadnych specjalnych warunków ani struktur poza podstawowymi zasadami bezpieczeństwa przedstawionymi w załącznikach A do D normy EN ISO 13849-2. Zasady te reprezentują ogólną dobrą praktykę w projektowaniu i doborze materiałów.

Kategoria 1

Kategoria 1 wymaga zastosowania wypróbowanych komponentów i sprawdzonych zasad bezpieczeństwa.

Przedstawiono tutaj typowy układ, dla którego oczekiwane jest uzyskanie kategorii 1. Blokada i stycznik odgrywają kluczowe role w procesie odłączenia energii z silnika w przypadku, gdy konieczny jest dostęp do strefy niebezpiecznej. Wyłącznik blokujący spełnia wymagania normy IEC 60947-5-1 dla zestyków z bezpośrednim otwarciem, co pokazuje symbol strzałki wewnątrz koła. Przy zastosowaniu sprawdzonych komponentów prawdopodobieństwo odłączenia energii jest wyższe dla kategorii 1 niż dla kategorii B. Zastosowanie wypróbowanych komponentów ma na celu zminimalizowanie możliwości utraty funkcji bezpieczeństwa, ale należy zauważyć, że w dalszym ciągu pojedynczy defekt może prowadzić do jej utraty.

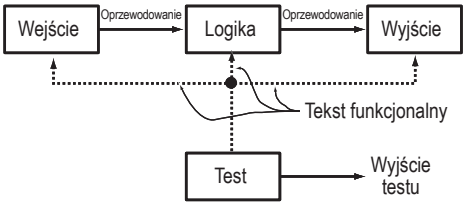


Prosty system bezpieczeństwa kategorii 1

Kategoria 1 zapobiega defektom funkcji bezpieczeństwa za pomocą prostego projektu opartego o komponenty o wysokiej niezawodności. Jeśli ten sposób zapobiegania nie zapewnia wystarczającego ograniczenia ryzyka, należy zastosować funkcję wykrywania defektów. Wykrywanie błędów i defektów stanowi podstawę systemów kategorii 2, 3 i 4, w których coraz bardziej surowe wymagania umożliwiają osiągnięcie wyższych poziomów redukcji zagrożenia.

Kategoria 2

Aby system był zgodny z kategorią 2, oprócz spełnienia wymagań kategorii B i wykorzystywania wypróbowanych zasad bezpieczeństwa, musi on również realizować funkcje testujące. Testy muszą być przeznaczone do wykrywania defektów w elementach systemu sterowania związanych z bezpieczeństwem. Jeśli nie zostaną wykryte żadne defekty, maszyna może działać dalej. W przypadku wykrycia defektu funkcja odpowiedzi na defekt musi zapewnić pozostanie maszyny w stanie bezpiecznym.



Sprzęt testujący może być zintegrowany z systemem bezpieczeństwa lub funkcjonować jako niezależne urządzenie.

Testowanie należy wykonywać:

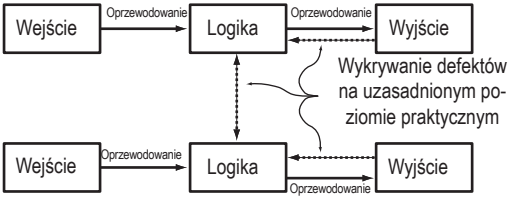
- po pierwszym załączeniu zasilania maszyny,
- przed zainicjowaniem zagrożenia, oraz
- okresowo, jeśli wymaga tego ocena ryzyka.

Uwaga: Norma EN ISO 138491-1 zakłada stosunek 100:1 między częstością testowania a częstością przywołania funkcji bezpieczeństwa lub test na przywołanie funkcji bezpieczeństwa z możliwością wykrycia defektu i zatrzymania maszyny w czasie krótszym, niż jest potrzebny do osiągnięcia strefy niebezpiecznej.

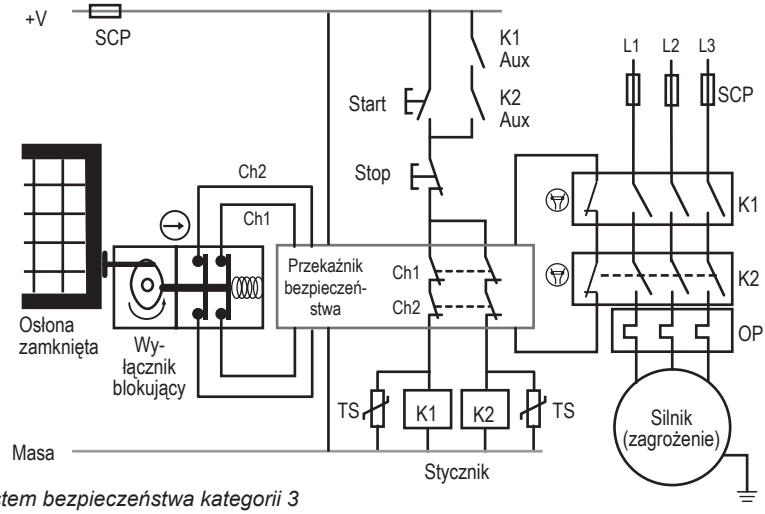
Zasadniczo system lub podsystem bezpieczeństwa musi być testowany w celu sprawdzenia, czy funkcja bezpieczeństwa ciągle pracuje prawidłowo Oznacza to, że w przypadku technologii mechanicznej może to być trudne lub niemożliwe do spełnienia. Podejście oparte na kategorii 2 jest bardziej odpowiednie dla technologii elektronicznej. Dla uzyskania poziomu PLd konieczny jest sygnał wyjścia testu zdolny do zainicjowania stanu bezpiecznego w przypadku wystąpienia defektu.

Kategoria 3

Oprócz konieczności spełnienia wymagań dla kategorii B oraz stosowania wypróbowanych zasad bezpieczeństwa, kategoria 3 wymaga prawidłowego działania funkcji bezpieczeństwa po pojawieniu się pojedynczego defektu. Gdy jest to rozsądnie praktyczne, defekt musi być wykryty w momencie kolejnego przywołania funkcji bezpieczeństwa lub przed nim.
Niektóre defekty, takie jak zwarcia międzykanałowe nie powodujące natychmiastowej utraty funkcji bezpieczeństwa, mogą pozostać niewykryte. Oznacza to, że dla kategorii 3 nagromadzenie niewykrytych defektów może prowadzić do utraty funkcji bezpieczeństwa.



Obok przedstawiono schemat blokowy wyjaśniający zasadę systemu kategorii 3. Działanie funkcji bezpieczeństwa jest zapewnione przez redundancję połączoną z nadzorowaniem wzajemnym i nadzorowaniem wyjść.



System bezpieczeństwa kategorii 3

Przykład systemu kategorii 3 przedstawiono na rysunku powyżej. Wyłącznik blokujący jest wyposażony w redundantny zestaw zestyków. Przekaźnik bezpieczeństwa (MSR) ma obwody wewnętrznie zredundowane, które nadzorują się wzajemnie. Do odłączania zasilania silnika służy redundantny zestaw styczników. Styczniki są monitorowane przez przekaźnik MSR za pośrednictwem zestyków połączonych mechanicznie.

Wykrywanie defektów należy uwzględnić dla każdej części systemu bezpieczeństwa. Jakie są tryby defektów dwukanałowego wyłącznika blokującego? Jakie są tryby defektów przekaźnika MSR? Jakie są tryby defektów styczników K1 i K2? Jakie są tryby defektów okablowania?

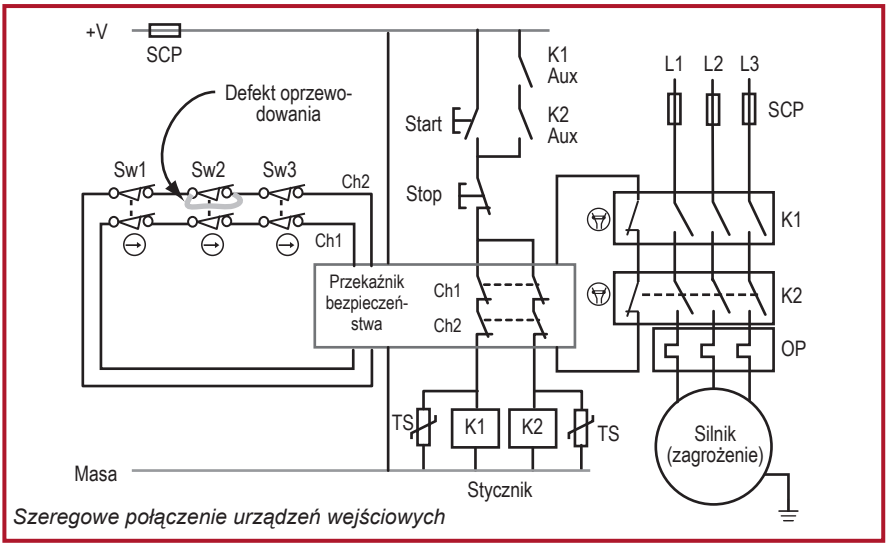
Dla obwodów kategorii 3 powszechnie przyjęte jest użycie pojedynczego wyłącznika blokującego z redundantnym zestawem zestyków elektrycznych. Oznacza to, że możliwość defektu pojedynczego komponentu w połączeniu aktywatora musi zostać wykluczona. Jeżeli nie da się wykluczyć tego defektu, oznacza to, że pojedynczy defekt może spowodować utratę funkcji bezpieczeństwa. Jest bardzo ważne, aby każde wykluczenie defektu zostało w pełni uzasadnione.

Przekaźnik bezpieczeństwa MSR zapewnia diagnostykę defektów dla wyłączników blokujących i styczników. Przekaźnik MSR może również wykonywać inne funkcje, jak na przykład ręczne resetowanie. W odniesieniu do ich architektury wewnętrznej przekaźniki bezpieczeństwa MSR mają zazwyczaj poziom PLe lub SIL 3.

Dwa styczniki powinny mieć zabezpieczenie przed przeciążeniem i zwarciem. Prawdopodobieństwo defektu stycznika spowodowanego zgrzaniem zestyków jest małe, lecz nie zerowe. Stycznik może także zawieść, jeśli bieguny mocy pozostaną zamknięte z powodu zaklinowania mechanizmu. Jeśli jeden stycznik przejdzie w stan uszkodzenia niebezpiecznego, drugi stycznik będzie wciąż działał, wyłączając zasilanie silnika. Uszkodzenie pierwszego stycznika zostanie wykryte przez przekaźnik MSR podczas kolejnego cyklu pracy maszyny. Gdy osłona zostanie zamknięta, a przycisk uruchomienia naciśnięty, połączone mechanicznie zestyki uszkodzonego stycznika pozostaną otwarte i przekaźnik MSR nie będzie w stanie zamknąć wyjść bezpieczeństwa, ujawniając defekt.

Defekty niewykryte

W przypadku struktury systemu kategorii 3 mogą występować pewne defekty, których nie można wykryć, ale same z siebie nie mogą prowadzić do utraty funkcji bezpieczeństwa. W przypadku systemów, w których defekty są wykrywalne musimy wiedzieć, czy w pewnych okolicznościach nie mogą one zostać zamaskowane lub przypadkowo zresetowane przez działanie innych urządzeń w strukturze systemu.



Szeregowe połączenie urządzeń wejściowych

Pokazano tu używane powszechnie podłączanie wielu urządzeń do nadzorującego przekaźnika bezpieczeństwa. Każde urządzenie ma dwa zestyki normalnie zamknięte z działaniem bezpośrednim. Takie rozwiązanie ogranicza koszty okablowania, ponieważ urządzenia wejściowe są łączone szeregowo. Załóżmy, że wystąpi zwarcie na jednym z zestyków w Sw2, jak pokazano na rysunku. Czy ten defekt można wykryć?

Jeśli wyłącznik Sw1 (lub Sw3) zostanie otwarty, otwarte zostaną również kanały Ch1 i Ch2, a przekaźnik MSR odłączy zasilanie od zagrożenia. Jeśli następnie wyłącznik Sw2 zostanie otwarty i ponownie zamknięty, defekt na jego zestykach nie zostanie wykryty,

ponieważ na wejściach przekaźnika MSR nie będzie zmiany stanu: oba kanały Ch1 i Ch2 pozostaną otwarte. Gdy wyłącznik Sw1 (lub Sw3) zostanie zamknięty, można wykonać restart zagrożenia, naciskając przycisk Start. W tych okolicznościach defekt nie spowodował utraty funkcji bezpieczeństwa, ale nie został wykryty. Pozostaje w systemie i kolejny defekt (zwarcie na drugim zestyku wyłącznika Sw2) może doprowadzić do utraty funkcji bezpieczeństwa.

Jeśli tylko wyłącznik Sw2 zostanie otwarty i zamknięty, a inne wyłączniki nie wykonały żadnej czynności, kanał Ch1 zostanie otwarty, a kanał Ch2 pozostanie zamknięty. Przekaźnik MSR wyłączy zagrożenie, ponieważ kanał Ch1 został otwarty. Po zamknięciu wyłącznika Sw2, naciśnięcie przycisku Start nie uruchomi silnika, gdyż kanał Ch2 nie był otwarty. Defekt został wykryty. Jeśli jednak z jakiegoś powodu wyłącznik Sw1 (lub Sw3) zostanie otwarty, a następnie zamknięty, oba kanały Ch1 i Ch2 zostaną otwarte, a następnie obwód zostanie zamknięty. Ta sekwencja stanowi symulację resetowania defektu i spowoduje niezamierzone zresetowanie przekaźnika MSR.

Powstaje pytanie, jakie pokrycie diagnostyczne może być zapewnione przez poszczególne wyłączniki tej strukturze zgodnie z normami EN ISO 13849-1 lub IEC 62061? Do czasu publikacji raportu ISO TR 24119 (listopad 2015: Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts) nie istniały jednoznaczne szczegółowe wytyczne w tym względzie, jednak normalną praktykę stanowiło założenie wskaźnika DC równego 60%, pod warunkiem, że wyłączniki były testowane indywidualnie w odcinkach czasu umożliwiających wykrycie defektu. Jeśli istniało prawdopodobieństwo, że co najmniej jeden wyłącznik nie zostanie nigdy indywidualnie przetestowany, uzasadniona była argumentacja, że pokrycie diagnostyczne DC powinno wynosić zero. Raport ISO TR 24119 zawiera szczegółowe wytyczne dotyczące ustalania wskaźnika DC dla urządzeń blokujących przy użyciu połączonych szeregowo zestyków bezpotencjałowych. Poniższa tabela zawiera podstawowe informacje. Jest bardzo ważne, aby w celu ustalenia aktualnego największego dopuszczalnego wskaźnika DC dla dowolnej architektury i aplikacji przestudiować dokument w całości.

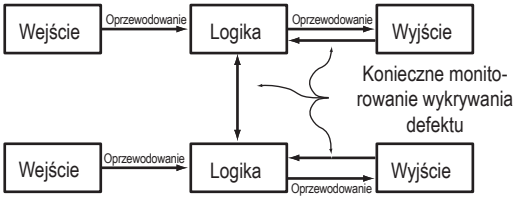
Liczba często używanych osłon ruchomych[1]	Liczba dodatkowych osłon ruchomych	Prawdopodobieństwo maskowania	Pokrycie diagnostyczne	Maks. osiągalny poziom
0	2 do 4	Niskie	Średnie	PL d
	5 do 30	Średnie	Niskie	PL d
	>30	Wysokie	Brak	PL c
1	1	Niskie	Średnie	PL d
	2 do 4	Średnie	Niskie	PL d
	≥5	Wysokie	Brak	PL c
>1	--	Wysokie	Brak	PL c

[1] Częstotliwość otwierania wyższa niż raz na godz.

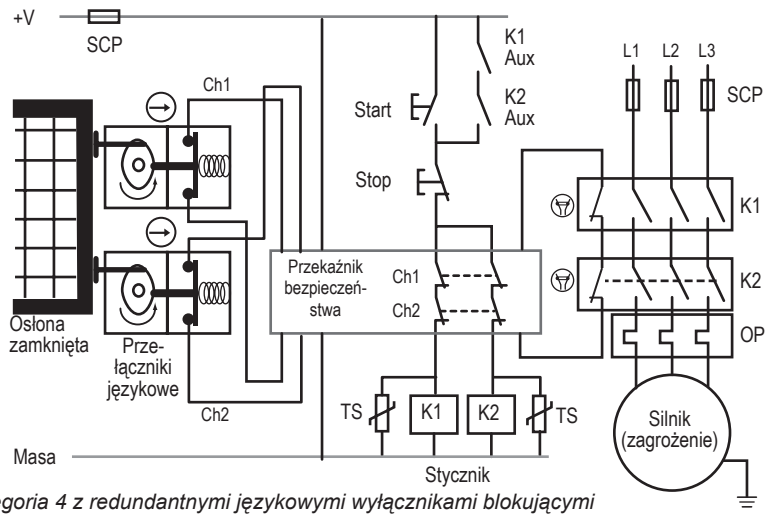
Połączenie szeregowe zestyków elektromechanicznych jest ograniczone do poziomu PLd (maks.), a w niektórych przypadkach może być ograniczone do PLc. Należy wziąć pod uwagę, że w każdym przypadku przewidywanego wystąpienia maskowania defektu (np. kilka ruchomych osłon zostanie otwartych w tym samym czasie w ramach normalnej eksploatacji lub obsługi), wynik DC zostanie ograniczony do zera.
Warto też zauważyć, że te wymagania kategorii 3 zawsze należało uwzględnić, ale stały się pierwszoplanowe dopiero po wprowadzeniu nowszych norm bezpieczeństwa funkcjonalnego.

Kategoria 4

Podobnie jak kategoria 3, również kategoria 4 wymaga, aby system bezpieczeństwa spełniał wymagania kategorii B, opierał się na sprawdzonych zasadach bezpieczeństwa i uruchamiał funkcję bezpieczeństwa w przypadku pojedynczego defektu. W przeciwieństwie do kategorii 3, gdzie kumulacja defektów może prowadzić do utraty funkcji bezpieczeństwa, kategoria 4 wymaga wykonania funkcji bezpieczeństwa także przy kumulacji defektów. W praktyce jest to zazwyczaj osiągane dzięki wysokiemu poziomowi diagnostyki, która daje pewność, że wszystkie istotne błędy zostaną wykryte zanim dojdzie do ich kumulacji. Kumulacja defektów dotyczy teoretycznie wystąpienia 2 defektów, ale w niektórych systemach należy uwzględniać 3 defekty.

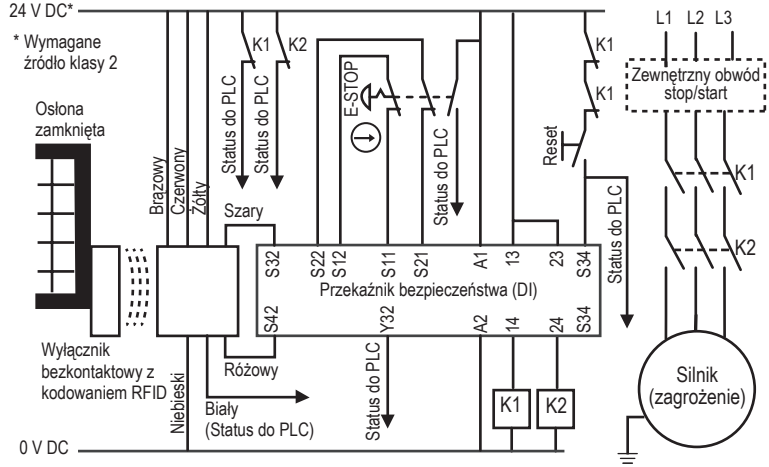


Poniżej pokazano schemat blokowy dla kategorii 4. Wymagane jest monitorowanie międzykanałowe oraz obu urządzeń wyjściowych. Kategoria 4 ma wyższe pokrycie diagnostyczne niż kategoria 3.



Kategoria 4 z redundantnymi językowymi wyłącznikami blokującymi

Jeszcze do stosunkowo niedawna wyłączniki blokujące z pojedynczym językiem i dwoma kanałami elektrycznymi były stosowane w obwodach kategorii 4. Aby było możliwe użycie wyłącznika blokującego z pojedynczym językiem w obwodzie dwukanałowym, konieczne jest wykluczenie możliwych defektów wywołanych uszkodzeniem mechanicznego połączenia języka z zestykami wyłącznika. Jednak zgodnie z raportem technicznym ISO TR 23849 tego rodzaju wykluczenie defektu nie powinno być stosowane w systemach poziomu PLe lub SIL 3. Jeżeli projektant systemu bezpieczeństwa preferuje użycie językowych wyłączników blokujących, powinien w celu spełnienia wymagań kategorii 4 zastosować dwa niezależne wyłączniki.



Kategoria 4 z elektronicznym wyłącznikiem blokującym z kodowaniem RFID

Nowoczesna technologia wykorzystuje inne podejście do kwestii uzyskania architektury kategorii 4 (oraz poziomów PLe/SIL 3). Zastosowanie złożonej elektroniki umożliwiło ekonomiczną integrację odporności na defekty i wysokiego poziomu pokrycia diagnostycznego w pojedynczym urządzeniu. Pokazane urządzenie blokujące nie tylko uzyskało kategorię 4, ale też cechuje się bardzo wysoką odpornością na manipulację (obejście) dzięki zastosowaniu kodowania RFID. Może być ono również połączone szeregowo z innymi podobnymi urządzeniami bez obniżenia kategorii lub pokrycia diagnostycznego.

PL (poziom zapewnienia bezpieczeństwa) dla komponentów i systemów

Wskazane architektury (kategorie) wg normy EN ISO 13849 mogą być użyte zarówno jako składnik do wyznaczenia poziomu PL dla komponentu (urządzenia) bezpieczeństwa, jak i wyznaczenia PL całego systemu. Wprowadza to nieco zamieszania, które można uporządkować poprzez zrozumienie możliwości komponentów. Jednak z podanych powyżej przykładów wynika jasno, że podsystem taki jak wyłącznik blokujący z kategorią 1 może być użyty samodzielnie w systemie kategorii 1.
Może on również stanowić część systemu kategorii 3 lub 4, jeśli dwa wyłączniki są używane razem z funkcją diagnostyczną realizowaną przez przekaźnik bezpieczeństwa.

Niektóre elementy, takie jak przekaźniki bezpieczeństwa i programowalne sterowniki bezpieczeństwa mają swoją własną wewnętrzną diagnostykę i dokonują samosprawdzenia w celu zapewnienia prawidłowego działania. W związku z tym mogą być oceniane jako elementy bezpieczeństwa zgodne z kategorią 2, 3 lub 4 bez stosowania żadnych dodatkowych środków.

Uwzględnianie i wykluczanie defektów

Analiza bezpieczeństwa, wymaga szczegółowej analizy defektów i gruntownego zrozumienia działania systemu bezpieczeństwa w przypadku wystąpienia defektów. Normy ISO 13849-1 i ISO 13849-2 zawierają szczegółowe informacje dotyczące uwzględniania i wykluczania błędów.

Jeśli defekt prowadzi do uszkodzenia kolejnych elementów, pierwszy defekt oraz wszystkie kolejne powinny być uważane za pojedynczy defekt.

Jeśli dwa lub więcej defektów ma tę samą przyczynę, również są one traktowane jak jeden defekt. Nazywa się to wspólną przyczyną defektów.

Jednoczesne wystąpienie dwóch lub większej liczby niezależnych defektów jest uważane za wysoce nieprawdopodobne i nie jest brane pod uwagę w niniejszej analizie.

Wykluczenia defektów

Normy EN ISO 13849-1 i IEC 62061 zezwalają na wykluczenia defektów przy klasyfikowaniu systemu bezpieczeństwa, jeżeli można wykazać, że wystąpienie tego defektu jest mało prawdopodobne. Istotne jest to, że tam gdzie stosuje się wykluczenia defektów, muszą być one właściwie uzasadnione i odpowiednie w stosunku do przewidywanego czasu życia systemu bezpieczeństwa. Im wyższy poziom ryzyka chronionego przez system bezpieczeństwa, tym bardziej surowe są wymagania dla uzasadnień wykluczania defektów. Zawsze powodowało to pewne zamieszanie związane z określonymi typami wykluczeń defektów, które mogą lub nie mogą być użyte. Jak już zauważyliśmy w tym rozdziale, najnowsze normy i przewodniki wyjaśniły niektóre aspekty tego zagadnienia.

Ogólnie rzecz biorąc, zgodnie z raportem ISO TR 23849 nie jest normalnie przyjętą praktyką, aby poziom PLe lub SIL 3 funkcji bezpieczeństwa realizowanej przez system bezpieczeństwa był uzyskiwany poprzez wykluczanie defektów. Jest to uzależnione od zastosowanej technologii oraz docelowego środowiska pracy. Dlatego też ważne jest, aby projektant podjął dodatkowe środki w zakresie stosowania wykluczania defektów wraz ze wzrostem poziomu PL lub SIL. Na przykład wykluczanie defektów nie dotyczy przypadku mechanicznych aspektów elektromechanicznych wyłączników krańcowych oraz wyłączników ręcznych (np. przycisków stopu awaryjnego) w celu osiągnięcia poziomu PLe lub SIL 3. Wykluczenia, które mogą być zastosowane do specyficznych defektów mechanicznych (np. zużycie, korozja, pęknięcia) są opisane w tabeli A.4 normy ISO 13849-2. Na przykład system osłony blokującej, który musi uzyskać poziom PLe lub SIL 3 będzie musiał wykazywać tolerancję na co najmniej jeden defekt (np. dwa konwencjonalne wyłączniki krańcowe), aby osiągnąć ten poziom, ponieważ wykluczenie defektu takiego jak uszkodzenie głowicy wyłącznika nie jest normalnie uzasadnione. Może być jednak dopuszczalne wykluczenie innych defektów, jak zwarcie obwodu w szafie sterowniczej zaprojektowanej zgodnie z odpowiednimi normami.

Kategorie zatrzymania zgodnie z normą IEC/EN 60204-1 i NFPA 79

Niefortunne i mylące jest to, że termin „kategoria" związany z systemami sterowania bezpieczeństwa ma dwa różne znaczenia. Jak dotąd omówiliśmy kategorie pochodzące z normy EN 954-1. Stanowią one klasyfikację działania systemu bezpieczeństwa po wystąpieniu defektu.

Występuje również klasyfikacja znana jako „kategorie zatrzymania", która wywodzi się z norm IEC/EN 60204-1 i NFPA 79. Istnieją trzy kategorie zatrzymania.

Zatrzymanie kategorii 0 wymaga natychmiastowego odłączenia zasilania od napędów. Jest ona czasami rozpatrywana jako niekontrolowane zatrzymanie, ponieważ w pewnych sytuacjach ruch może trwać jakiś czas, gdyż silnik zatrzymuje się wybiegiem.

Zatrzymanie kategorii 1 wymaga utrzymania zasilania w celu umożliwienia hamowania, aż do zatrzymania, a następnie odłączenia zasilania od napędu. Uwaga: Więcej informacji na temat zatrzymania kategorii 1a i 1b można znaleźć w normie.IEC 60204-1.

Zatrzymanie kategorii 2 to zatrzymanie kontrolowane przy pozostawieniu zasilania napędów maszyny. Kategoria 2 to normalne zatrzymanie produkcyjne.

Należy zwrócić uwagę, że jedynie kategorie zatrzymania 0 lub 1 mogą być używane jako stop awaryjny. Wybór jednej spośród tych dwóch kategorii powinien być uzależniony od oceny ryzyka.

Wszystkie przykłady obwodów, które zostały przedstawione uprzednio w tym rozdziale, stosowały zatrzymanie kategorii 0. Zatrzymanie kategorii 1 jest uzyskiwane z wyjściami zwłocznymi do końcowego odłączenia zasilania. Systemom zatrzymywania kategorii 1 często towarzyszą osłony blokujące z ryglowaniem. Osłona jest zaryglowana w położeniu zamkniętym aż do momentu, gdy maszyna osiągnie stan bezpieczny (tj. zostanie zatrzymana).

Zatrzymanie maszyny bez właściwego uwzględnienia sterownika programowalnego może spowodować nieoczekiwany restart i poważne uszkodzenie maszyny i używanych narzędzi. Sterownik PLC typu standardowego (bez funkcji bezpieczeństwa) nie może realizować zatrzymania związanego z bezpieczeństwem. Wymagane jest użycie innych metod.

Dwa możliwe rozwiązania dla zatrzymania kategorii 1 są podane poniżej:

1. Przekaźniki bezpieczeństwa z wyjściami zwłocznymi

Stosowane są przekaźniki bezpieczeństwa z wyjściami bezzwłocznymi i zwłocznymi. Wyjścia bezzwłoczne są podłączone do wejść sterownika programowanego (np. PLC lub „zezwolenia" przemiennika), natomiast wyjścia zwłoczne do stycznika głównego. Aktywacja wyłącznika blokującego powoduje otwarcie wyjść bezzwłocznych przekaźnika bezpieczeństwa. Sygnalizuje to sterownikowi konieczność wykonania prawidłowej procedury zatrzymania. Po upłynięciu krótkiego, ale wystarczającego czasu potrzebnego do wykonania tej procedury, wyjścia zwłoczne przekaźnika bezpieczeństwa zmieniają stan i odłączają zasilanie od stycznika głównego.

Uwaga: Czas opóźnienia wyjść przekaźnika bezpieczeństwa musi uwzględniać obliczony całkowity czas zatrzymania. Jest to szczególnie ważne, gdy uzyskana wartość jest używana do określania umiejscowienia urządzenia przy obliczaniu odległości bezpiecznej

2. Sterowniki programowalne (PLC) bezpieczeństwa

Logikę i wymagane funkcje czasowe można wprowadzić w wygodny sposób przy użyciu sterownika bezpieczeństwa, takiego jak GuardLogix.

Wymagania dotyczące systemów sterowania bezpieczeństwem w USA

Niezawodnie sterowane

Najwyższy poziom ograniczenia ryzyka w normach dla robotów w USA i Kanadzie jest uzyskiwany przez systemy sterowania związane z bezpieczeństwem, spełniające wymagania niezawodności sterowania. Niezawodne systemy sterowania związane z bezpieczeństwem mają architekturę dwukanałową z nadzorowaniem. Funkcja zatrzymania robota nie może zostać przerwana przez żaden defekt pojedynczego elementu, w tym również w nadzorowaniu.

Nadzorowanie powinno wygenerować polecenie stopu po wykryciu defektu. Jeśli zagrożenie występuje po zatrzymaniu ruchu, należy to sygnalizować. System bezpieczeństwa musi pozostać w stanie bezpiecznym, aż do momentu usunięcia defektu. Najlepiej, gdy defekt jest wykrywany w momencie wystąpienia uszkodzenia. Jeśli spełnienie tego warunku nie jest możliwe, defekt powinien być wykryty podczas kolejnego przywołania systemu bezpieczeństwa. Jeśli istnieje duże prawdopodobieństwo defektów wywołanych wspólną przyczyną, należy wziąć to pod uwagę.

Wymagania kanadyjskie różnią się od wymagań w USA, ponieważ dodano w nich dwa dodatkowe wymagania. Po pierwsze, systemy sterowania związane z bezpieczeństwem powinny działać niezależnie od normalnych programowalnych systemów sterowania. Po drugie, obejście lub pominięcie systemu bezpieczeństwa nie może być łatwe bez wykrycia.

Komentarze dotyczące niezawodności sterowania

Najbardziej istotnymi aspektami niezawodności sterowania są odporność na pojedyncze defekty i monitorowanie (wykrywanie defektów). Wymagania określają, jak system bezpieczeństwa powinien odpowiadać na wystąpienie „defektu pojedynczego”, „dowolnego defektu pojedynczego” lub „dowolnego pojedynczego defektu komponentu”.

Odnośnie do defektów należy wziąć pod uwagę trzy bardzo ważne założenia: (1) nie wszystkie błędy są wykrywane, (2) dodanie terminu „komponent” powoduje powstanie komplikacji związanej z oprzewodowaniem oraz (3) oprzewodowanie stanowi integralną część systemu bezpieczeństwa. Defekty okablowania mogą prowadzić do utraty funkcji bezpieczeństwa.

Uzyskanie niezawodności sterowania ma na celu zapewnienie prawidłowego działania systemu bezpieczeństwa w obecności defektu. Jeśli defekt zostanie wykryty, system

bezpieczeństwa musi wykonać bezpieczne działanie, powiadomić o defekcie oraz zapobiec dalszej pracy maszyny, aż do momentu usunięcia defektu. Jeśli defekt nie zostanie wykryty, funkcja bezpieczeństwa musi być nadal dostępna podczas kolejnego przywołania.

Rozdział 10: Przykłady rozwiązań

Przegląd – wstępnie opracowane funkcje bezpieczeństwa dla maszyn

Funkcje bezpieczeństwa maszyn – takie jak stop awaryjny, osłony blokujące czy wykrywanie obecności – wymagają wielu elementów składowych, w tym czujników lub urządzeń wejściowych, urządzeń logicznych oraz urządzeń wyjściowych. Elementy te wspólnie realizują poziom zabezpieczeń wyznaczany jako poziom zapewnienia bezpieczeństw (PL) zgodnie z normą EN ISO 13849-1.

W tym rozdziale przedstawiamy jedną z wielu wstępnie opracowanych funkcji bezpieczeństwa dla maszyn, stworzoną przez firmę Rockwell Automation. Każdy z dokumentów zawiera wytyczne dla poszczególnych funkcji bezpieczeństwa, oparte na wymaganiach funkcjonalnych, doborze urządzeń i wymaganiach względem poziomu zapewnienia bezpieczeństwa, z uwzględnieniem schematu połączeń, konfiguracji, planu weryfikacji i walidacji oraz obliczeń poziomu bezpieczeństwa.

Dokumenty z opracowanymi funkcjami bezpieczeństwa są bezpłatne i można je pobrać ze strony internetowej firmy Rockwell Automation.

www.rockwellautomation.com, under Solutions & Services > Safety Solutions.

Opisana poniżej funkcja bezpieczeństwa jest oparta na wyłączniku blokującym monitorującym osłonę, z konfigurowalnym przekaźnikiem bezpieczeństwa. Zastosowane produkty: Bezkontaktowy wyłącznik blokujący SensaGuard z kodowaniem RFID, połączony z konfigurowalnym przekaźnikiem bezpieczeństwa Guardmaster 440C-CR30. Jako urządzenia wyjściowe zastosowano styczniki bezpieczeństwa 100S-C.
Ta wstępnie opracowana funkcja bezpieczeństwa zapewnia CAT. 4, PLe wg (EN) ISO 13849-1.

Numer katalogowy oryginalnego wydania dokumentu: SAFETY-AT133C-EN-P

Opis bezpieczeństwa funkcjonalnego

Pracownicy są chronieni przed niebezpiecznym ruchem przez osłonę stałą. Niezbędny dostęp do strefy niebezpiecznej jest zapewniony dzięki osłonie uchylnej. Osłona jest nadzorowana przez wyłącznik blokujący SensaGuard, podłączony do wejść konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik 440C-CR30 steruje dwoma połączonymi szeregowo stycznikami bezpieczeństwa 100S-C, które z kolei załączają zasilanie silnika będącego źródłem niebezpiecznego ruchu. W każdym przypadku otwarcia osłony system bezpieczeństwa odłącza zasilanie silnika. Silnik i napędzany przez niego niebezpieczny ruch przechodzą w fazę wybiegu (kategoria

zatrzymania 0). Silnik nie może zostać ponownie uruchomiony, jeśli osłona pozostanie otwarta. Po zamknięciu osłony silnik może zostać ponownie uruchomiony przez naciśnięcie i zwolnienie przycisku resetu przekaźnika 440C-CR30, a następnie użycie zewnętrznej funkcji Start w celu przywrócenia zasilania silnika przez styczniki 100S-C.

Wyłącznik SensaGuard monitoruje stan osłony (otwarta lub zamknięta). SensaGuard monitoruje również dwa wyjścia OSSD pod kątem defektów. Przekaźnik 440C-CR30 sprawdza sygnały wejściowe z wyłącznika SensaGuard pod kątem wykrycia defektów, a także monitoruje stan sygnałów resetu i sprzężenia zwrotnego ze styczników 100S-C. Przekaźnik sprawdza również, czy na jego własnych wyjściach nie pojawiły się defekty. Wyjścia te sterują stycznikami 100S-C. Po wykryciu defektu przekaźnik 440C-CR30 wyłącza swoje wyjścia i odłącza zasilanie silnika. Przekaźnik nie zresetuje się do chwili usunięcia defektu.

Zestawienie materiałów

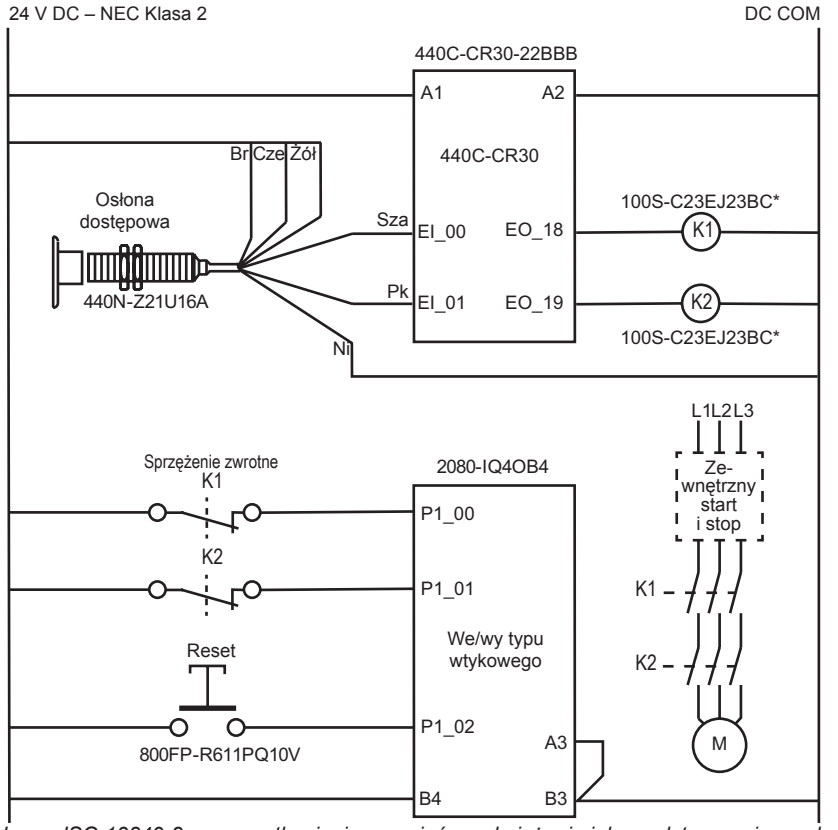
W tej aplikacji zastosowano następujące produkty.

Numer katalogowy	Opis	Ilość
440N-Z21S16B	Wyłącznik SensaGuard, plastik 18 mm, 2 x PNP, maks. 0,2 A, kabel 10 m	1
800FP-R611	Przycisk resetu 800F, plastik, okrągły (typu 4/4X/13, IP66), niebieski, R, pakowany standardowo	1
2080-IQ4OB4	Moduł 4 wejścia / 4 wyjścia cyfrowe	1
1761-CBL-PM02	Kabel do programowania konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30	1
440C-CR30-22BBB	Programowo konfigurowalny przekaźnik bezpieczeństwa Guardmaster 440C-CR30, PLe SIL 3, 22 we/wy bezpieczeństwa, wbudowany port szeregowy, port USB do programowania, 2 sloty wtykowe, 24 V DC	1
100S-C23EJ23BC	Stycznik bezpieczeństwa MCS 100S-C, 23 A, 24 V DC (z cewką elektryczną), zestyki rozwidlone	2

Przegląd systemu

Wyłącznik blokujący SensaGuard jest zastosowany do potwierdzenia, że osłona ochronna znajduje się w bezpiecznym stanie zamkniętym. Jeśli osłona nie jest zamknięta, niebezpieczny ruch zostaje zatrzymany lub uniemożliwiony. Oprócz monitorowania stanu osłony ochronnej wyłącznik SensaGuard sprawdza swoje wyjścia pod kątem wykrycia wszelkiego typu defektów. Programowalny przekaźnik bezpieczeństwa 440C-CR30 na wejściach z podłączonym wyłącznikiem SensaGuard wykrywa również przerwanie przewodu, defekt jednego kanału i zwarcia do potencjału 0 V.

Programowalny przekaźnik bezpieczeństwa 440C-CR30 testem impulsowym monitoruje wyjścia sterujące stycznikami bezpieczeństwa, wykrywając wszystkie stany defektów. Prawidłowy, bezpieczny stan styczników bezpieczeństwa K1 i K2 jest potwierdzany przez konfigurowalny przekaźnik bezpieczeństwa 440C-CR30, który monitoruje sygnały sprzężenia zwrotnego w instrukcji SMF2 przed załączeniem styczników.



**Norma ISO 13849-2 wymaga tłumienia przepięć na obciążeniu jako podstawowej zasady bezpieczeństwa.*
Odpowiednie tłumienie zapewnia cewka elektryczna „EJ".

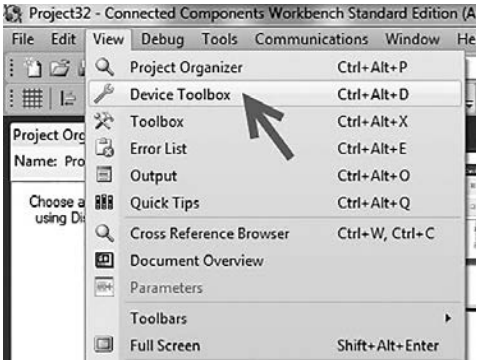
Konfiguracja

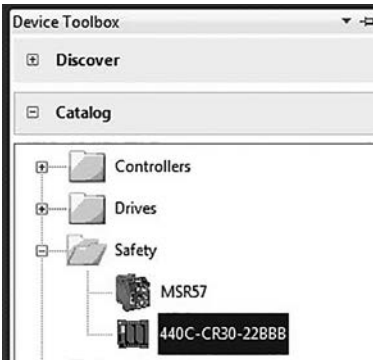
Przekaźnik 440C-CR30 jest konfigurowany za pomocą oprogramowania Connected Components Workbench™, w wersji 6.01 lub nowszej. Szczegółowy opis każdego etapu wykracza poza zakres tego dokumentu. Przyjmuje się, że użytkownik zna oprogramowanie Connected Components Workbench.

Konfiguracja przekaźnika 440C-CR30

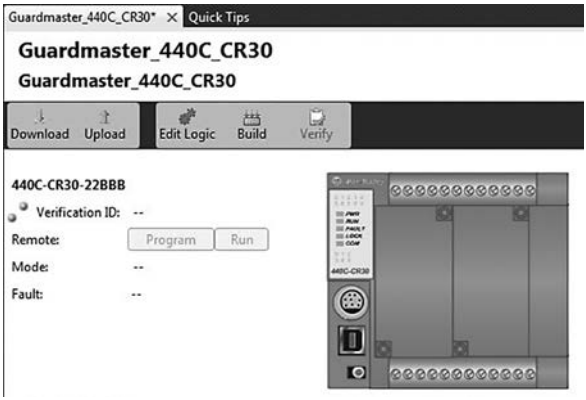
W celu skonfigurowania przekaźnika Guardmaster 440C-CR30 za pomocą oprogramowania Connected Components Workbench należy wykonać następujące kroki.

1. W oprogramowaniu Connected Component Workbench wybierz View (widok), a następnie Device Toolbox (zestaw narzędzi). W oknie Device Toolbox wybierz 440C-CR30-22BBB.

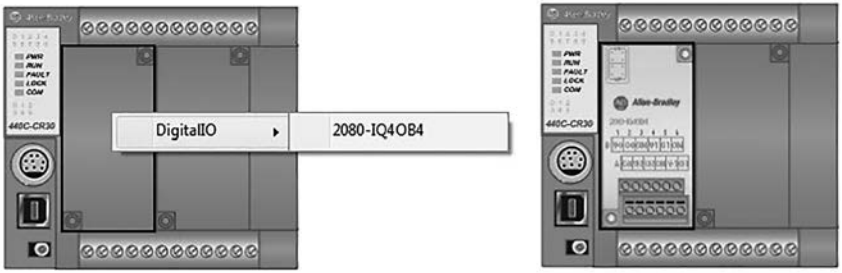




2. W oknie Project Organizer (organizator projektu) kliknij dwukrotnie Guardmaster_400C_CR30*.

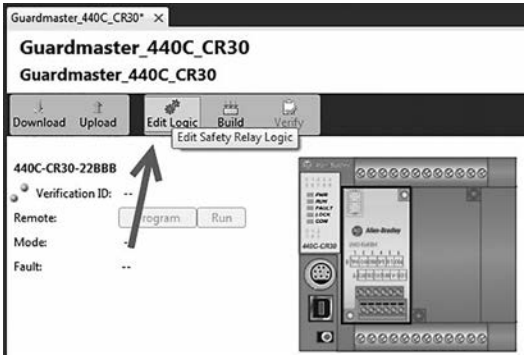


3. Aby dodać moduł wtykowy we/wy wymagany przez ten obwód, prawym przyciskiem myszy kliknij lewe pole modułów wtykowych i wybierz moduł 2080-IQ4OB4.

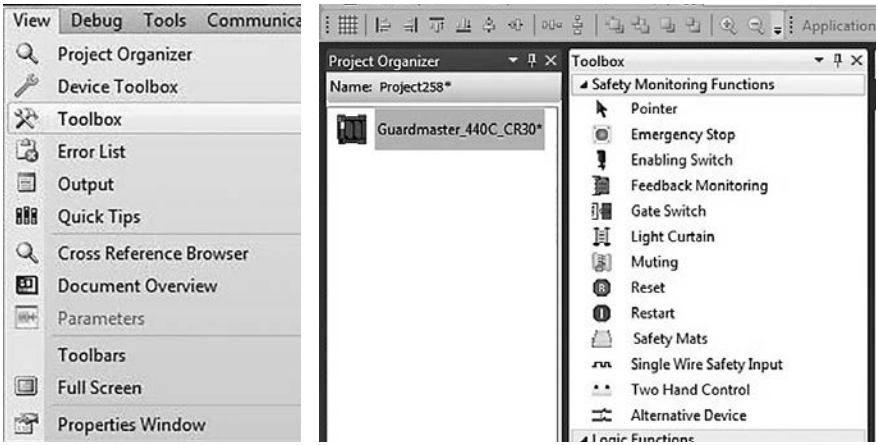


WSKAZÓWKA: Moduł we/wy jest szary, ponieważ nie jest to moduł we/wy bezpieczeństwa. W omawianej tutaj aplikacji zastosowanie jego jest możliwe, gdyż modułu nie używa się do podłączenia sygnałów bezpieczeństwa. Wejścia takie jak sprzężenie zwrotne czy przycisk resetu nie są uważane za sygnały wejściowe bezpieczeństwa sensu stricto. Użycie standardowych wejść/wyjść dla tych sygnałów nie związanych z bezpieczeństwem pozwala na zaoszczędzenie ograniczonych ilościowo wejść i wyjść dla rzeczywistych sygnałów bezpieczeństwa.

4. Kliknij przycisk Edit Logic (edytuj logikę), aby otworzyć ekran roboczy oprogramowania Connected Components Workbench. Pojawi się pusty obszar roboczy.



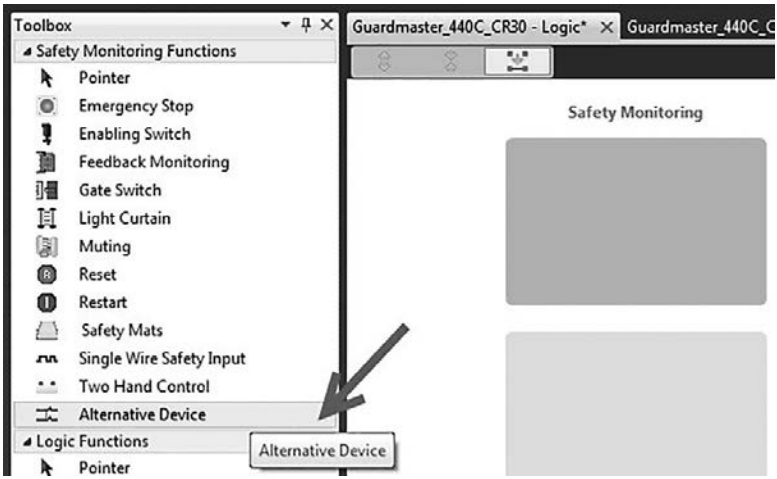
5. Z menu rozwijalnego View wybierz Toolbox (zestaw narzędzi). Okno Toolbox pojawi się w obszarze roboczym.



Konfiguracja wejść

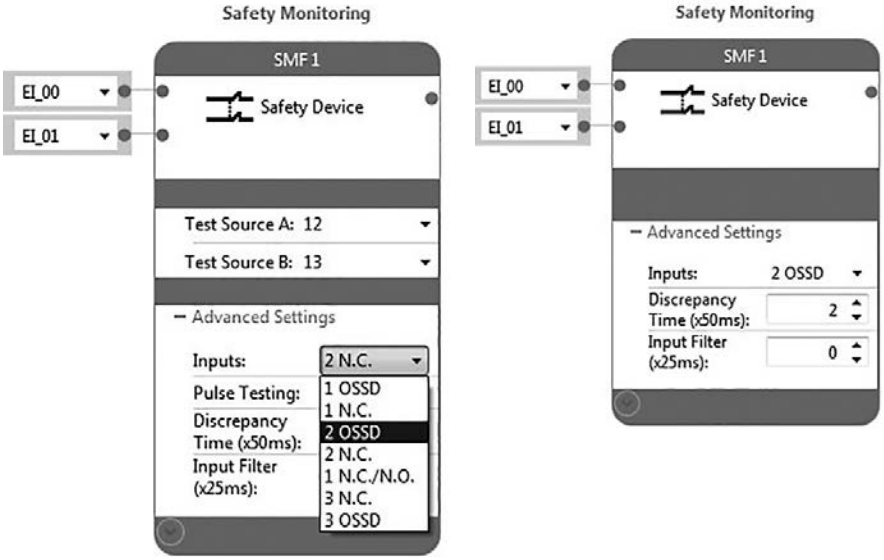
W oknie Toolbox nie występuje funkcja monitorowania bezpieczeństwa SensaGuard (Safety Monitoring Function) Aby ją skonfigurować, należy wykonać następujące kroki.

1. Wybierz Alternative Device (urządzenie alternatywne). Przeciągnij je na zielony prostokąt w kolumnie Safety Monitoring i upuść.

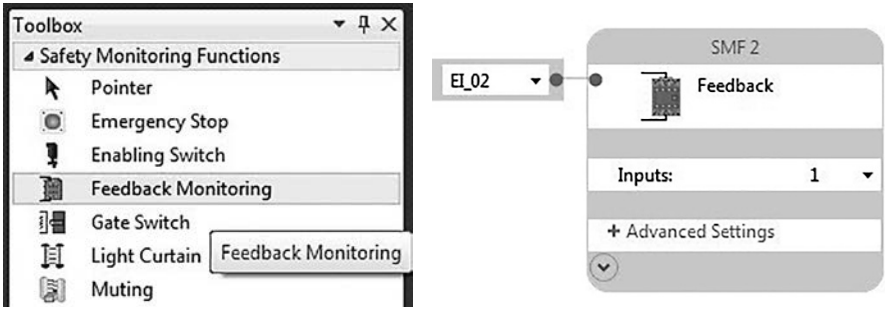


Oprogramowanie Connected Components Workbench automatycznie przypisze do urządzenia pierwsze dwa dostępne wejścia, EI_00 i EI_01. Należy je pozostawić niezmienione. Oprogramowanie Connected Components Workbench automatycznie przypisuje do tego bloku numer funkcji SMF1. Domyślnie program zakłada elektromechaniczny typ urządzenia i przypisuje źródła testu (Test Resources). Wyłącznik SensaGuard ma dwa wyjścia OSSD i nie wymaga źródeł testu.

2. W celu prawidłowej konfiguracji bloku otwórz Advanced Settings (ustawienia zaawansowane) i wybierz 2 OSSD z menu rozwijalnego. Skonfigurowany blok wygląda jak na rysunku.

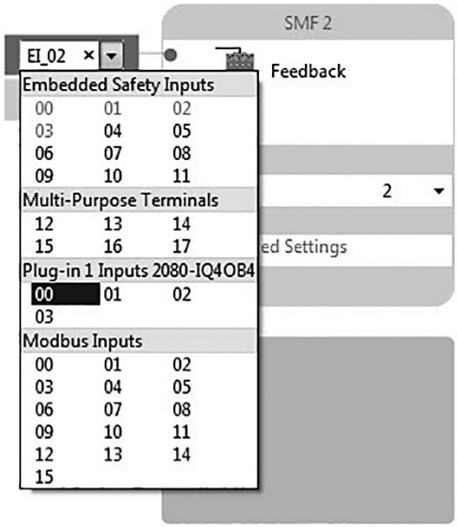


3. Kliknij, przeciągnij i upuść funkcję monitorowania bezpieczeństwa Feedback Monitoring do kolumny Safety Monitoring poniżej bloku SensaGuard w oknie roboczym.

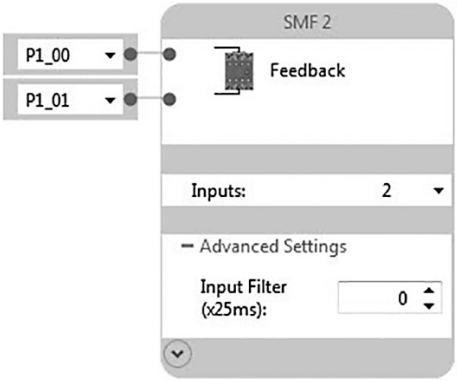


Należy zauważyć, że oprogramowanie Connected Components Workbench przypisuje ją do zacisku wejścia EI_02, następnego wolnego zacisku wejść bezpieczeństwa (Safety Input). Oprogramowanie zakłada, że jest to pojedyncze wejście i automatycznie przypisuje numer funkcji SMF2 do tego bloku.

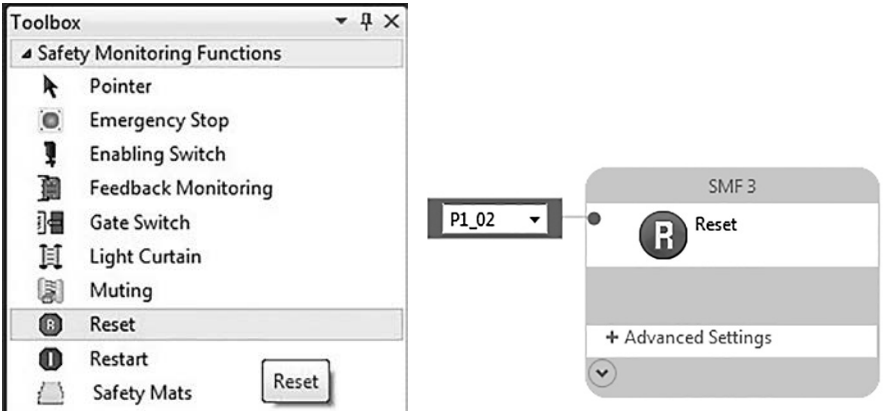
4. Ponieważ obwód wymaga dwóch wejść, po jednym z każdego stycznika, zmień liczbę sygnałów wejściowych na 2, czyli jeden zestyk rozwierny w każdym ze styczników 100S.



5. Przypisz sygnały wejściowe do zacisków wtykowych P1_00 i P1_01. Dzięki temu nie musimy używać wejść bezpieczeństwa dla sygnałów sprzężenia zwrotnego.



6. Kliknij, przeciągnij i upuść funkcję monitorowania bezpieczeństwa Reset do kolumny Safety Monitoring poniżej bloku Feedback w oknie roboczym.

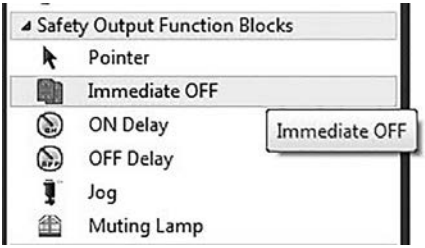


Oprogramowanie Connected Components Workbench automatycznie przypisze do tego bloku numer funkcji SMF3. Zmień przypisanie sygnału Reset do zacisku wejściowego P1_02.

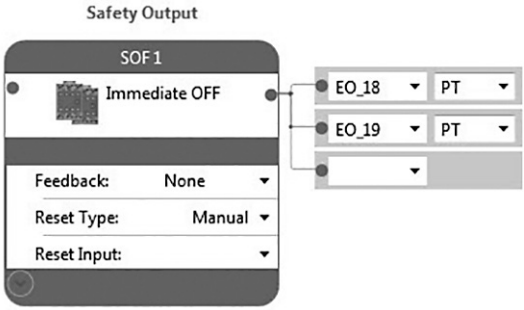
Konfiguracja wyjść

W celu skonfigurowania wyjść należy wykonać następujące kroki.

1. Kliknij i przeciągnij funkcję Immediate OFF (wyłączenie natychmiastowe) z menu bloków funkcyjnych wyjść bezpieczeństwa (Safety Output Function Blocks) okna Toolbox.

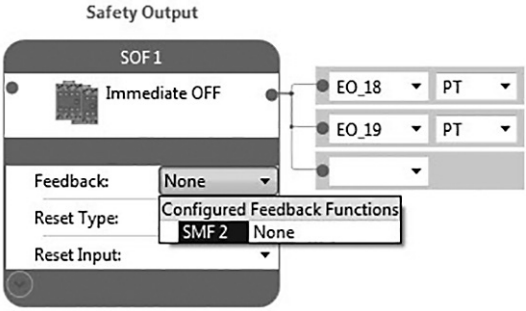


2. Upuść ją w górnym bloku kolumny Safety Output (wyjścia bezpieczeństwa).

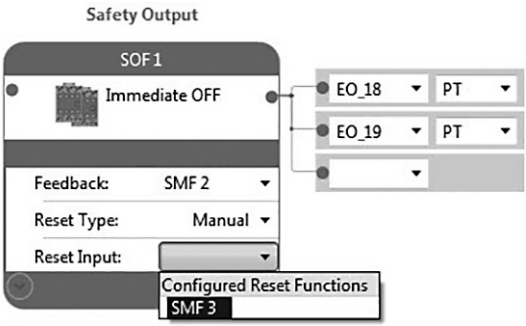


Oprogramowanie Connected Components Workbench automatycznie przypisze zaciski wyjściowe EO_18 i EO_19. Testowanie impulsowe jest skonfigurowane domyślnie. Domyślnym typem resetowania (Reset Type) jest reset ręczny (Manual). Należy pozostawić wartości tych ustawień.

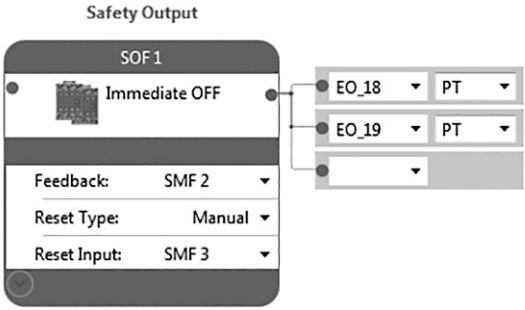
3. Wybierz SMF2 z menu rozwijalnego sprzężenia zwrotnego (Feedback).



4. Wybierz SMF3 z menu rozwijalnego wejścia resetu (Reset Input).



Konfiguracja wyjść bezpieczeństwa jest zakończona.

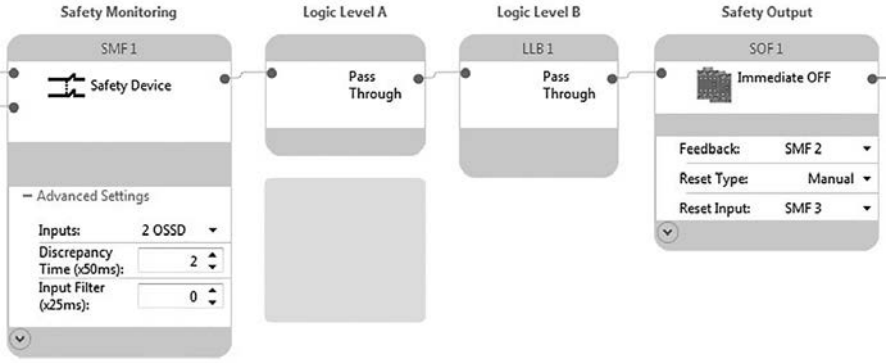


Konfiguracja logiki

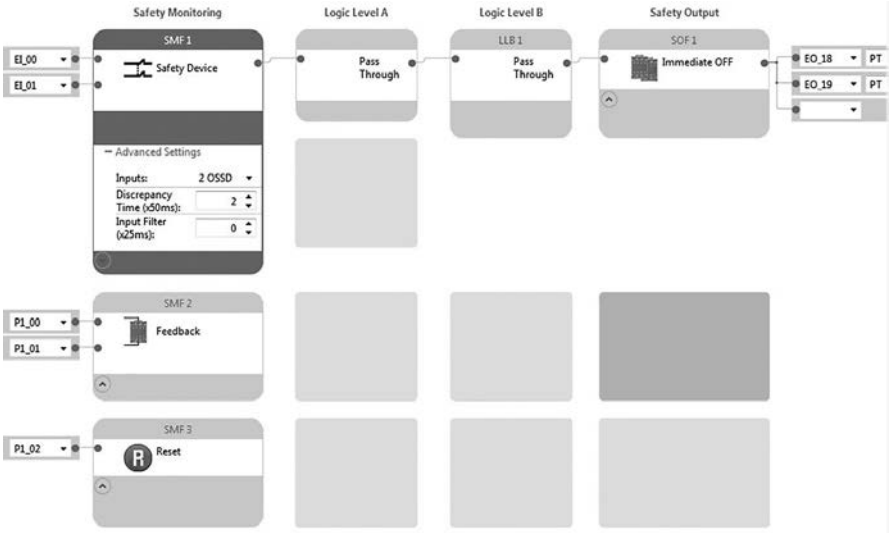
Sekcja logiki określa, w jaki sposób wyjścia bezpieczeństwa odpowiadają na wejścia monitorowania bezpieczeństwa. W naszym przypadku wyjścia bezpieczeństwa odpowiadają bezpośrednio wejściom monitorowania bezpieczeństwa.

1. Kliknij niebieski punkt po prawej stronie bloku wejściowego monitorowania bezpieczeństwa wyłącznika SensaGuard. Jego kolor zmieni się na szary.

2. Kliknij niebieski punkt po lewej stronie bloku wyjścia bezpieczeństwa, aby połączyć logikę.

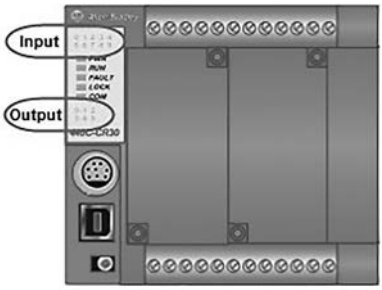


Po zakończeniu logika wygląda jak na rysunku poniżej.



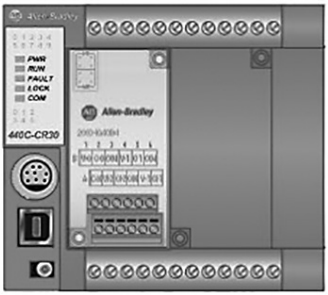
Konfigurowanie wskaźników stanu

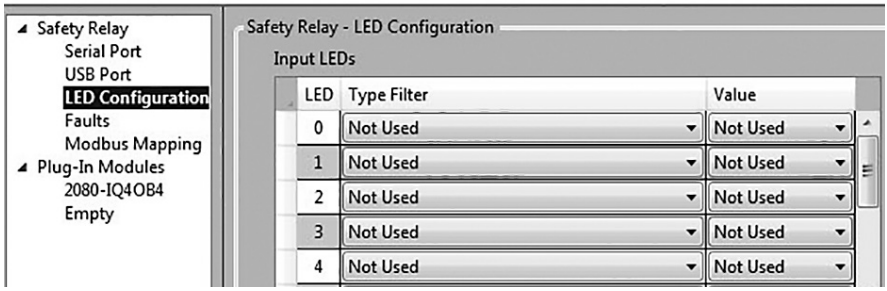
Konfigurowalny przekaźnik bezpieczeństwa 440C-CR30 jest wyposażony w dziesięć konfigurowanych przez użytkownika diodowych wskaźników stanu wejść i sześć konfigurowanych przez użytkownika diodowych wskaźników stanu wyjść. W wielu przypadkach mogą się one okazać bardzo pomocne w procesie instalacji, przekazania do eksploatacji, monitorowania oraz wykrywania i usuwania usterek konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30. Nie wpływają w żaden sposób na działanie układu, a ich konfiguracja nie jest niezbędna; są jednak łatwe do ustawienia i zalecaną praktyką jest ich stosowanie.



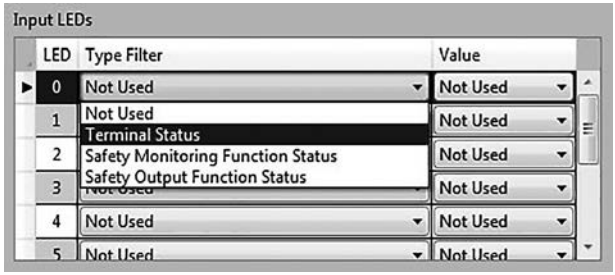
1. Kliknij Guardmaster_440C_CR30*.

2. Wybierz LED Configuration (konfiguracja LED).

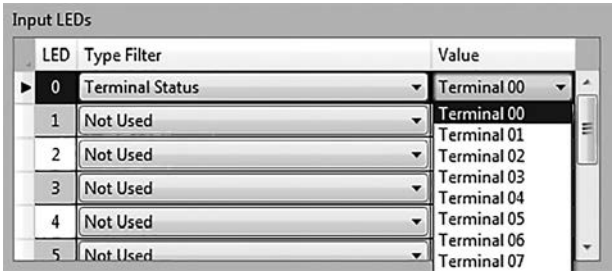




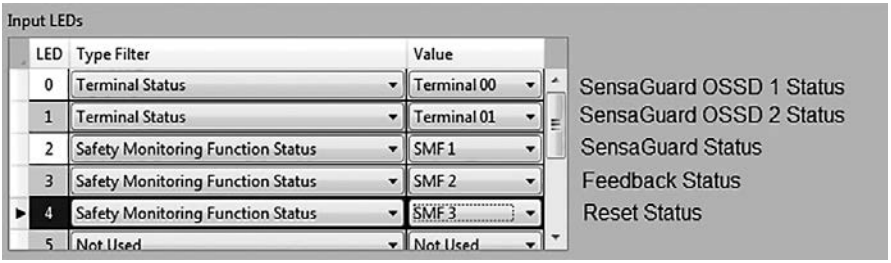
3. W polu Type Filter (filtr typu) wybierz Terminal Status dla diodowego wskaźnika stanu LED 0.



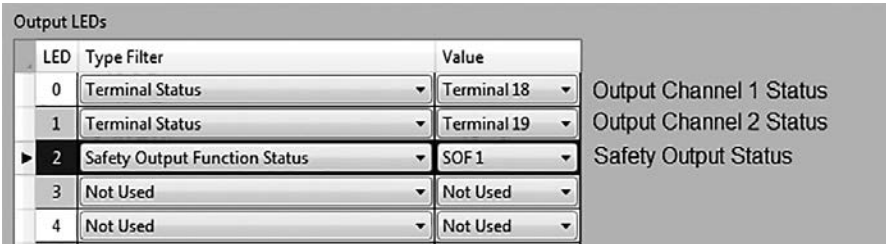
4. Dla LED 0 wybierz Terminal 00 z rozwijanego menu Value (wartość). Diodowy wskaźnik stanu LED 0 jest teraz skonfigurowany do wskazywania stanu zacisku 00.



5. Przypisz następne cztery wejściowe diody LED (1–4) w taki sam sposób. Diodowe wskaźniki stanu wejść są teraz skonfigurowane.



6. Przypisz trzy wyjściowe diody LED w następujący sposób.

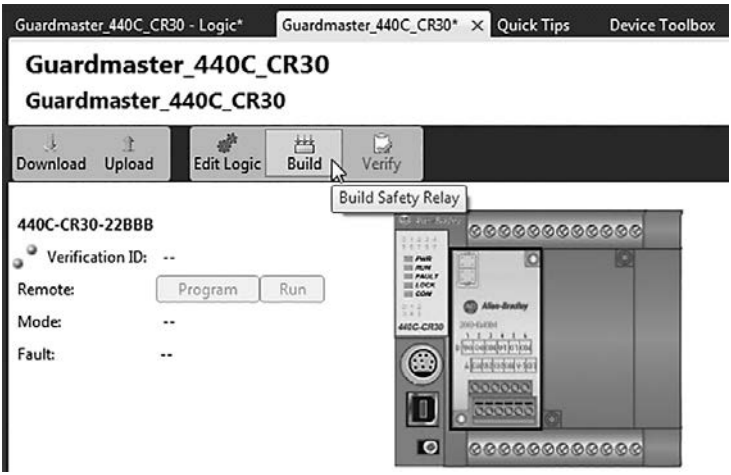


Potwierdzenie poprawności programu (Build)

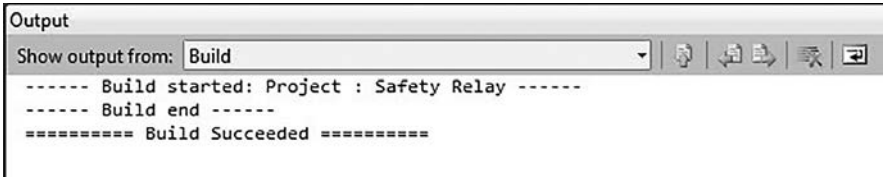
Potwierdzenie poprawności logiki należy przeprowadzić w przedstawionych poniżej krokach, korzystając z funkcji Build (kompilacja) oprogramowania Connected Components Workbench.

1. Kliknij Guardmaster_440C_CR30 w menu powyżej obszaru roboczego.

2. Kliknij Build.



Komunikat Build Succeeded (kompilacja zakończona sukcesem) potwierdza poprawność konfiguracji.



Jeżeli podczas kompilacji zostanie wykryty błąd lub przeoczenie, na wyświetlaczu pojawi się komunikat błędu podający jego szczegóły, co umożliwi korektę. Po skorygowaniu błędu należy powtórzyć kompilację

Zapisywanie i pobieranie projektu

Zapisywanie i pobieranie projektu należy przeprowadzić w następujących krokach.

1. Z menu File (plik) wybierz Save as (zapisz jako), aby zapisać projekt.

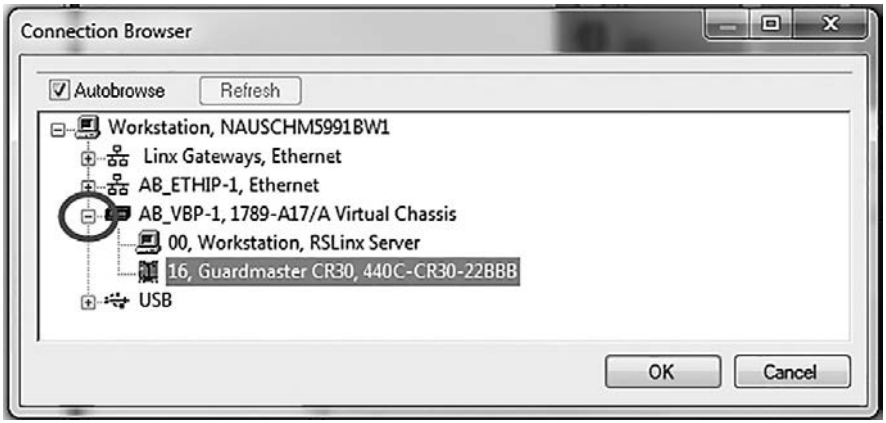
2. W oknie Project Organizer (organizator projektu) podwójnie kliknij Guardmaster_440C_CR30 w celu otwarcia obszaru roboczego.

3. Włącz zasilanie przekaźnika bezpieczeństwa 440C-CR30.

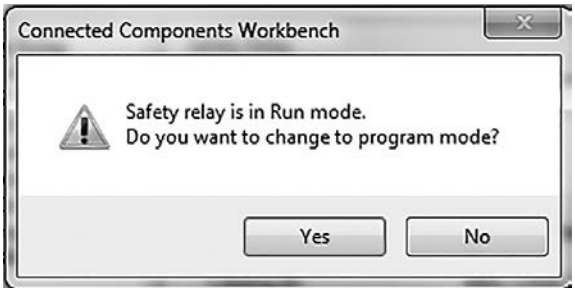
4. Podłącz kabel USB do przekaźnika 440C-CR30.

5. Kliknij Download (załaduj).

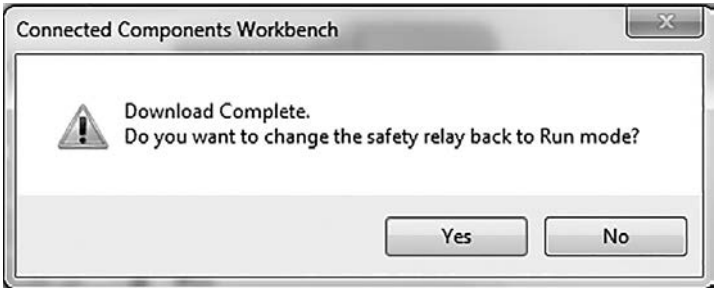
6. W oknie Connection Browser (przeglądarka połączeń) rozwiń AB_VBP-1 Virtual Chassis i wybierz Guardmaster 440C-CR30-22BBB. Kliknij OK.



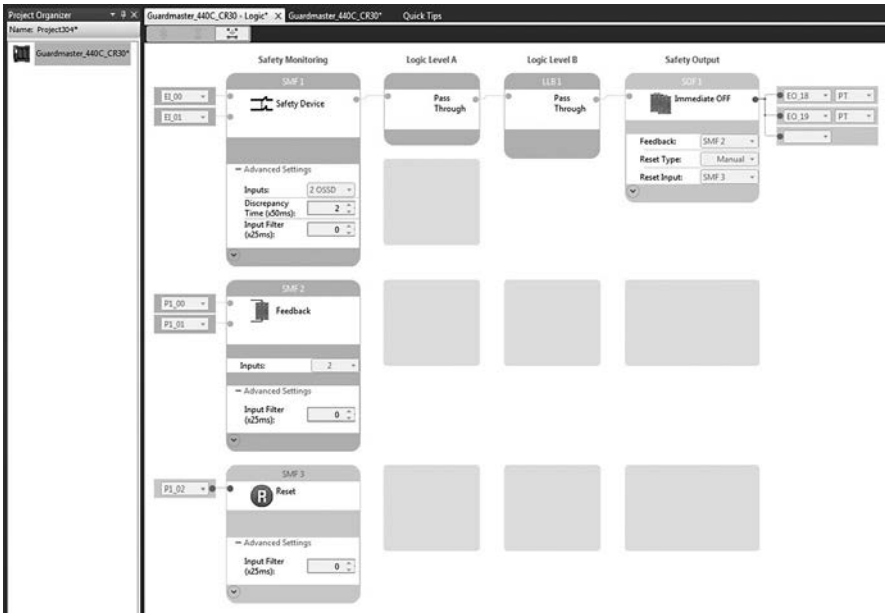
7. Kliknij Yes (tak), aby zmienić tryb z Run (praca) na Program (programowanie).



8. Gdy ładowanie zostanie zakończone, kliknij Yes (tak), aby z powrotem zmienić tryb pracy.



9. Kliknij Edit Logic (edycja logiki), aby wyświetlić diagnostykę online.

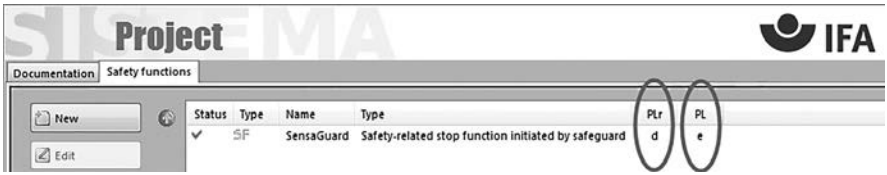


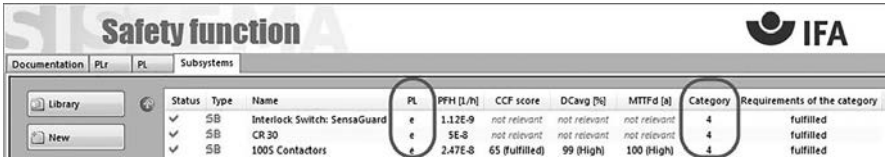
Kolor zielony wskazuje, że blok działa prawidłowo albo że zacisk wejściowy lub wyjściowy jest w stanie załączenia. Kolor zielony migający wskazuje, że funkcja wyjść bezpieczeństwa jest gotowa na zresetowanie.
Tryb diagnostyki online przekaźnika 440C-CR30 może być bardzo pomocny podczas procedury weryfikacji.

10. Przed przystąpieniem do weryfikacji konfiguracji należy zapoznać się z informacjami dotyczącymi obliczania poziomu zapewnienia bezpieczeństwa oraz z planem weryfikacji i walidacji.

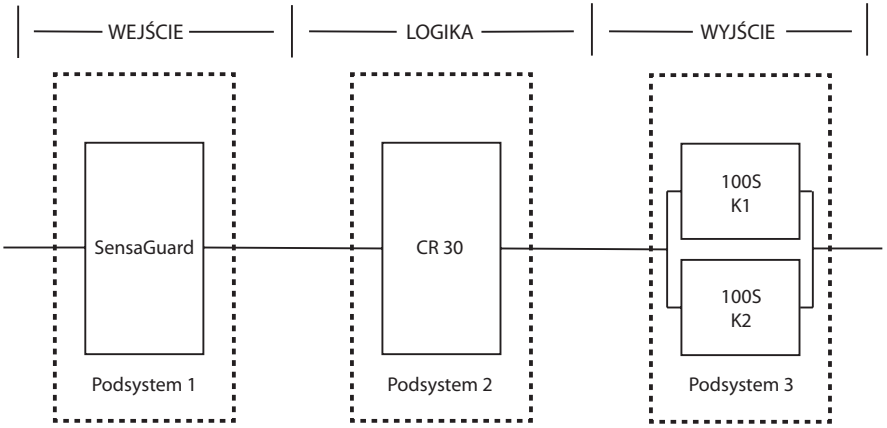
Określenie poziomu zapewnienia bezpieczeństwa (PL)

Jeśli nasza zaprojektowana funkcja zatrzymania bezpiecznego zostanie prawidłowo zaimplementowana, może uzyskać kategorię 4, poziom zapewnienia bezpieczeństwa PLe, zgodnie z ISO 13849-1: 2008, co można potwierdzić z pomocą narzędzia obliczeniowego SISTEMA.
Minimalny wymagany poziom zapewnienia bezpieczeństwa (PLr) dla tej funkcji, wynikający z oceny ryzyka, wynosi PLd.





Bezpieczne zatrzymanie zainicjowane przez funkcję bezpieczeństwa osłony ochronnej może być zamodelowane w niezastępujący sposób:



Ponieważ styczniki to urządzenia elektromechaniczne, dane dla nich zawierają następujące parametry:

- Średni czas do defektu niebezpiecznego ($MTTF_D$)
- Pokrycie diagnostyczne (DCavg)
- Wspólna przyczyna defektów (CCF)

Ocena bezpieczeństwa funkcjonalnego urządzeń elektromechanicznych bierze pod uwagę:

- Jak często urządzenia te są przełączane
- Czy są one skutecznie monitorowane pod kątem defektów
- Czy zostały one właściwie wyspecyfikowane i zainstalowane

Narzędzie programowe SISTEMA oblicza MTTFd przy użyciu B10d dla styczników i oszacowanej częstotliwości łączeniowej, wprowadzonej podczas tworzenia projektu SISTEMA.

DCavg (99%) dla styczników zostaje wybrane z tabeli urządzeń wyjściowych normy ISO 13849-1 załącznik E – Monitorowanie bezpośrednie.

Wartość CCF zostaje wygenerowana za pomocą procedury punktowania przedstawionej w załączniku F normy ISO 13849-1. Kompletną procedurę punktowania należy przeprowadzić podczas rzeczywistego wdrożenia aplikacji. Minimalna liczba punktów powinna wynosić 65.

Plan weryfikacji i walidacji

Weryfikacja i walidacja odgrywają ważną rolę jako czynniki unikania błędów podczas projektowania i realizacji systemu bezpieczeństwa. Wymagania dla weryfikacji i walidacji przedstawia norma ISO 13849-2. Norma wymaga przedstawienia udokumentowanego planu, potwierdzającego spełnienie wszystkich wymagań funkcjonalnych dotyczących bezpieczeństwa.

Weryfikacja to analiza utworzonego systemu sterowania bezpieczeństwa. Poziom zapewnienia bezpieczeństwa (PL) systemu sterowania bezpieczeństwa powinien być wyznaczony w celu potwierdzenia, że system ten osiągnął wymagany poziom zapewniania bezpieczeństwa (PLr). Narzędzie programowe SISTEMA jest zwykle używane do wykonywania tych obliczeń, a także zapewnia pomoc w realizacji wymagań normy ISO 13849-1.

Walidacja stanowi test funkcjonalny systemu sterowania bezpieczeństwa potwierdzający, że system spełnia wyspecyfikowane wymagania dla funkcji bezpieczeństwa. System sterowania bezpieczeństwa powinien być testowany w celu potwierdzenia, że odpowiedź wszystkich wyjść związanych z bezpieczeństwem jest właściwa dla odpowiednich sygnałów wejściowych bezpieczeństwa. Test funkcjonalny obejmuje normalne warunki pracy, a także potencjalne błędy wprowadzane przez symulowanie defektów. Dokumentem zawierającym wyniki walidacji systemu sterowania bezpieczeństwa jest zazwyczaj lista kontrolna.

Przed przystąpieniem do walidacji systemu należy uzyskać potwierdzenie, że konfigurowalny przekaźnik bezpieczeństwa Guardmaster 440C-CR30 został oprzewodowany i skonfigurowany zgodnie z instrukcją instalacji.

Lista kontrolna weryfikacji i walidacji

Ogólne informacje o maszynach Opis	
Nazwa/numer modelu maszyny	
Numer seryjny maszyny	
Nazwa/nazwisko klienta	
Data testu	
Nazwiska testerów	
Numer schematu	
Urządzenia wejściowe	440N-Z21S16B
Konfigurowalny przekaźnik bezpieczeństwa	440C-CR30-22BBB
Przemiennik częstotliwości	
Stycznik bezpieczeństwa	100S-C23EJ23BC

Konfiguracja oprzewodowania i przekaźnika bezpieczeństwa			
Krok testu	**Weryfikacja**	**Wynik**	**Zmiany/ modyfikacje**
1	Upewnij się, że specyfikacje wszystkich komponentów są właściwe dla danego zastosowania. Zobacz „Podstawowe zasady bezpieczeństwa" i „Sprawdzone zasady bezpieczeństwa" w normie ISO 13849-2.		
2	Sprawdź wzrokowo obwód przekaźnika bezpieczeństwa w celu potwierdzenia, że został on oprzewodowany zgodnie ze schematem w dokumentacji.		
3	Potwierdź, że konfiguracja konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30 jest prawidłowa i zgodna z przeznaczeniem.		

Weryfikacja pracy w trybie normalnym – System bezpieczeństwa prawidłowo reaguje na wszystkie normalne sygnały wejściowe uruchomienia, zatrzymania, resetowania, zatrzymania awaryjnego i wyłącznika SensaGuard.			
Krok testu	**Weryfikacja**	**Wynik**	**Zmiany/ modyfikacje**
1	Upewnij się, że nikt nie przebywa w obszarze chronionym.		
2	Potwierdź, że niebezpieczny ruch jest zatrzymany.		
3	Potwierdzić, że drzwi zostały zamknięte.		
4	Włącz zasilanie systemu bezpieczeństwa.		
5	Potwierdź, że diodowe wskaźniki stanu zacisku 00, zacisku 01 i SMF1 przekaźnika bezpieczeństwa 440C-CR30 świecą na zielono. Potwierdź, że wszystkie wskaźniki stanu wyjścia są wyłączone. Potwierdź, że diodowe wskaźniki Power (zasilanie) i Run (praca) świecą na zielono. Sprawdź właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
6	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Potwierdź, że diodowe wskaźniki stanu zacisków 18, 19 i bloku SOF1 świecą na zielono. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
7	Upewnij się, że niebezpieczny ruch nie został wznowiony po załączeniu zasilania.		
8	Wciśnij i zwolnij przycisk Start napędu. Potwierdź, że rozpoczyna się niebezpieczny ruch, a maszyna podejmuje pracę.		

9	Naciśnij zewnętrzny przycisk Stop. Maszyna musi zatrzymać się w normalny sposób, zgodnie z konfiguracją. System bezpieczeństwa nie powinien zareagować.		
10	Wciśnij i zwolnij zewnętrzny przycisk Start. Potwierdzić, że rozpoczyna się niebezpieczny ruch, a maszyna podejmuje pracę.		
11	Otwórz osłonę ochronną. System bezpieczeństwa powinien wyzwolić się. Niebezpieczny ruch powinien zostać zatrzymany w czasie poniżej 0,7 sekundy. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
12	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Konfigurowalny przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
13	Zamknij osłonę ochronną. Maszyna nie powinna uruchomić się. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
14	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Blok SOF1 przekaźnika bezpieczeństwa 440C-CR30 powinien się pobudzić. Niebezpieczny ruch nie może się uruchomić. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
15	Wciśnij i zwolnij zewnętrzny przycisk Start. Upewnij się, że silnik został załączony, a maszyna podjęła pracę.		

Walidacja bezpiecznej odpowiedzi na działanie nienormalne – System bezpieczeństwa prawidłowo reaguje na wszystkie możliwe do przewidzenia defekty z odpowiednią diagnostyką.

Testy wyłącznika SensaGuard i konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30

Krok testu	Weryfikacja	Wynik	Zmiany/ modyfikacje
1	Osłona ochronna powinna być zamknięta. Podczas trwania niebezpiecznego ruchu usuń przewód OSSD1 wyjścia wyłącznika SensaGuard z zacisku EI_00 przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik bezpieczeństwa 440C-CR30 powinien natychmiast wyzwolić się. Czerwony diodowy wskaźnik stanu defektu przekaźnika powinien migać. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
2	Ponownie podłącz przewód do zacisku E1_00. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować. Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
3	Otwórz i zamknij osłonę ochronną. Czerwony diodowy wskaźnik stanu defektu powinien wyłączyć się. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
4	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Blok SOF1 przekaźnika bezpieczeństwa 440C-CR30 powinien zostać wzbudzony. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		

5	Naciśnij zewnętrzny przycisk Start. Maszyna powinna uruchomić się. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench. Ten krok jest opcjonalny w kolejnych testach walidacyjnych wyłącznika SensaGuard (kroki 6–27).		
6	Przy zamkniętej osłonie ochronnej podłącz wyjście OSSD 1 do napięcia 24 V DC. Po około 40 sekundach wyłącznik SensaGuard wyzwoli się błędem. Przekaźnik bezpieczeństwa 440C-CR30 wyzwoli się błędem. Czerwony diodowy wskaźnik stanu defektu przekaźnika powinien migać. Wskaźnik stanu wyłącznika SensaGuard powinien migać na czerwono. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
7	Odłącz wyjście OSSD 1 od napięcia 24 V DC. Wyłącznik SensaGuard ani przekaźnik bezpieczeństwa 440C-CR30 nie powinny zareagować. Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Wyłącznik SensaGuard ani przekaźnik bezpieczeństwa 440C-CR30 nie powinny zareagować. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
8	Wyłącz i załącz zasilanie wyłącznika SensaGuard. Po około pięciu sekundach od ponownego załączenia zasilania wyłącznika SensaGuard jego diodowy wskaźnik stanu powinien zaświecić ciągłym światłem zielonym. Migający czerwony diodowy wskaźnik błędu przekaźnika bezpieczeństwa 440C-CR30 powinien się wyłączyć. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
9	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
10	Podłącz OSSD 1 do DC COM. Przekaźnik bezpieczeństwa 440C-CR30 natychmiast wyzwoli się błędem. Czerwone światło zatrzymania bezpiecznego (Safe Stop) na wieży świetlnej załączy się. Pomarańczowe światło Gate 1 na wieży świetlnej załączy się. Czerwony diodowy wskaźnik stanu defektu przekaźnika powinien migać. Wskaźnik stanu wyłącznika SensaGuard powinien migać na czerwono.		
11	Odłącz wyjście OSSD1 od DC COM. Wyłącznik SensaGuard ani przekaźnik bezpieczeństwa 440C-CR30 nie powinny zareagować. Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Wyłącznik SensaGuard ani przekaźnik bezpieczeństwa 440C-CR30 nie powinny zareagować.		
12	Wyłącz i załącz zasilanie wyłącznika SensaGuard. Po około pięciu sekundach od ponownego załączenia zasilania wyłącznika SensaGuard jego diodowy wskaźnik stanu powinien zaświecić ciągłym światłem zielonym. Pomarańczowe światło Gate 1 na wieży świetlnej wyłączy się. Czerwone światło bezpiecznego zatrzymania (Safe Off) na wieży świetlnej pozostaje załączone. Migający czerwony diodowy wskaźnik błędu przekaźnika bezpieczeństwa 440C-CR30 powinien się wyłączyć.		
13	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Blok SOF1 przekaźnika bezpieczeństwa 440C-CR30 powinien podać napięcie na styczniki. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
14 do 27	Powtórzyć kroki od 1 do 13, używając EI _01 w miejsce EI_00 i OSSD 2 w miejsce OSSD 1.		

28	Podłącz wyjścia OSSD 1 do OSSD 2 (zacisk EI_00 do zacisku EI_01). Po około 50 sekundach wyłącznik SensaGuard wyzwoli się błędem. Przekaźnik bezpieczeństwa 440C-CR30 wyzwoli się błędem. Wskaźnik stanu wyłącznika SensaGuard powinien migać na czerwono. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
29	Rozłącz wyjścia OSSD 1 i OSSD 2. Wyłącznik SensaGuard ani przekaźnik bezpieczeństwa 440C-CR30 nie powinny zareagować. Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Wyłącznik SensaGuard ani przekaźnik bezpieczeństwa 440C-CR30 nie powinny zareagować.		
30	Wyłącz i załącz zasilanie wyłącznika SensaGuard. Po około pięciu sekundach od ponownego załączenia zasilania wyłącznika SensaGuard jego diodowy wskaźnik stanu powinien zaświecić ciągłym światłem zielonym. Migający czerwony diodowy wskaźnik błędu przekaźnika bezpieczeństwa 440C-CR30 powinien się wyłączyć. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
31	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Czerwone światło zatrzymania bezpiecznego (Safe Stop) na wieży świetlnej powinno wyłączyć się. Blok SOF1 przekaźnika bezpieczeństwa 440C-CR30 powinien podać napięcie na styczniki. Sprawdź wszystkie diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		

Walidacja bezpiecznej odpowiedzi na działanie nienormalne – System bezpieczeństwa prawidłowo reaguje na wszystkie możliwe do przewidzenia defekty z odpowiednią diagnostyką.

Testy konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30

Krok testu	Weryfikacja	Wynik	Zmiany/ modyfikacje
1	Podczas pracy maszyny przerwać połączenie między zaciskiem EO_18 konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30 a zaciskiem A1 cewki K1. Niebezpieczny ruch musi zwolnić do zatrzymania.		
2	Nacisnąć zewnętrzny przycisk Stop. Przywrócić połączenie. Nacisnąć zewnętrzny przycisk Start, aby wznowić niebezpieczny ruch.		
3	W czasie trwania niebezpiecznego ruchu podłączyć zacisk A1 cewki K1 do napięcia 24 V DC. Po około 18 sekundach musi zadziałać przekaźnik bezpieczeństwa 440C-CR30. Stycznik K2 musi zostać wyłączony spod napięcia. Niebezpieczny ruch zwalnia do zatrzymania. Czerwony diodowy wskaźnik stanu błędów przekaźnika 440C-CR30 świeci.		
4	Odłączyć zacisk A1 cewki K1 od napięcia 24 V DC. Nacisnąć i zwolnić przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować.		
5	Włączyć zasilanie przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik reaguje. Diodowy wskaźnik stanu błędów przekaźnika 440C-CR30 nie świeci.		
6	Wcisnąć i zwolnić przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Nacisnąć zewnętrzny przycisk Start. Niebezpieczny ruch musi zostać wznowiony.		
7	Podczas pracy maszyny zewrzeć zacisk A1 cewki K1 ze wspólną masą DC. Przekaźnik bezpieczeństwa 440C-CR30 musi zadziałać. Czerwony diodowy wskaźnik stanu błędów przekaźnika 440C-CR30 świeci.		
8	Odłączyć zacisk A1 cewki K1 od wspólnej masy DC. Nacisnąć i zwolnić przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować.		
9	Włączyć zasilanie przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik bezpieczeństwa 440C-CR30 reaguje. Diodowy wskaźnik stanu błędów przekaźnika bezpieczeństwa 440C-CR30 nie świeci.		

10	Wcisnąć i zwolnić przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Nacisnąć zewnętrzny przycisk Start. Niebezpieczny ruch zostaje wznowiony.		
11 do 21	Powtórzyć kroki od 1 do 10, zamieniając EO_18 na EO_19 i K1 na K2.		
22	Połączyć zacisk A1 cewki K1 z zaciskiem A1 cewki K2. Po około 18 sekundach musi zadziałać przekaźnik bezpieczeństwa 440C-CR30. Niebezpieczny ruch zwalnia do zatrzymania. Czerwony diodowy wskaźnik stanu błędów przekaźnika 440C-CR30 świeci.		
23	Odłączyć zacisk A1 cewki K1 od zacisku A1 cewki K2. Wcisnąć i zwolnić przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować.		
24	Włączyć zasilanie przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik reaguje. Diodowy wskaźnik stanu błędów przekaźnika bezpieczeństwa 440C-CR30 nie świeci.		
25	Wcisnąć i zwolnić przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Nacisnąć zewnętrzny przycisk Start. Niebezpieczny ruch musi zostać wznowiony.		

Walidacja bezpiecznej odpowiedzi na działanie nienormalne – System bezpieczeństwa prawidłowo reaguje na wszystkie możliwe do przewidzenia defekty z odpowiednią diagnostyką.

Sprzężenie zwrotne stycznika – Testy konfigurowalnego przekaźnika bezpieczeństwa 440C-CR30

Krok testu	Weryfikacja	Wynik	Zmiany/ modyfikacje
1	Podczas normalnej pracy maszyny usuń połączenie sprzężenia zwrotnego stycznika K1 z zacisku P1_00. Maszyna nie powinna przerwać pracy.		
2	Otwórz osłonę ochronną. System bezpieczeństwa powinien wyzwolić się. Niebezpieczny ruch powinien zostać zatrzymany w czasie poniżej 0,7 sekundy. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
3	Zamknij osłonę ochronną. Maszyna nie powinna uruchomić się. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
4	Wciśnij i zwolnij przycisk Reset przekaźnika bezpieczeństwa 440C-CR30. Przekaźnik bezpieczeństwa 440C-CR30 nie powinien zareagować. Sprawdź diodowe wskaźniki stanu pod kątem prawidłowego działania oraz właściwy stan przekaźnika bezpieczeństwa 440C-CR30 za pomocą oprogramowania Connected Components Workbench.		
5	Przywróć podłączenie do zacisku P1_00. Wyłącz i załącz zasilanie przekaźnika 440C-CR30. Naciśnij przycisk resetowania przekaźnika 440C-CR30. Wyjścia przekaźnika 440C-CR30 powinny zostać wzbudzone. Wciśnij i zwolnij zewnętrzny przycisk Start. Upewnij się, że silnik został załączony, a maszyna podjęła pracę.		
6	Powtórzyć kroki od 1 do 5 dla połączenia sprzężenia zwrotnego stycznika K2 i zacisku P1_01.		

Weryfikacja konfiguracji

System powinien sprawdzić konfigurację każdej indywidualnej aplikacji za pomocą komendy Verify (weryfikuj). Jeśli konfigurowalny przekaźnik bezpieczeństwa 440C-CR30 nie zostanie zweryfikowany, po 24 godzinach działania przejdzie w stan Stop.

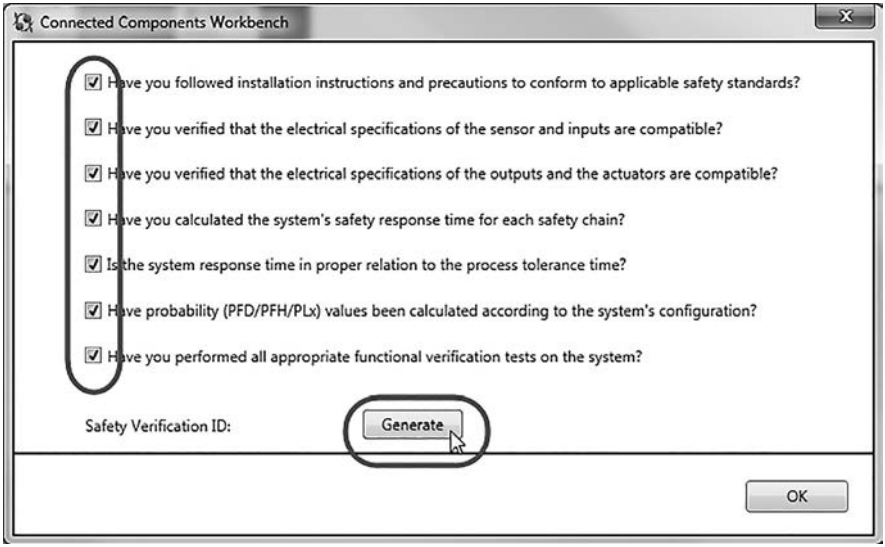
UWAGA: Procedura weryfikacji musi zostać udokumentowana i zapisana w dokumentacji technicznej systemu bezpieczeństwa.

Załadowanie i weryfikacja konfiguracji odbywa się w przedstawionych poniżej krokach.

1. Upewnij się, że przekaźnik 440C-CR30 jest zasilany i podłączony do stacji roboczej za pośrednictwem kabla USB.
2. Upewnij się, że w prawym górnym narożniku zakładki Connected Components Workbench widnieje potwierdzenie połączenia z przekaźnikiem 440C-CR30. Jeśli nie, kliknąć Connect to Device (połącz z urządzeniem), aby nawiązać połączenie oprogramowania.

3. Kliknij Verify (weryfikuj).

4. Odpowiedz na wszystkie pytania i zaznacz przyporządkowane pola. Kliknij Generate.

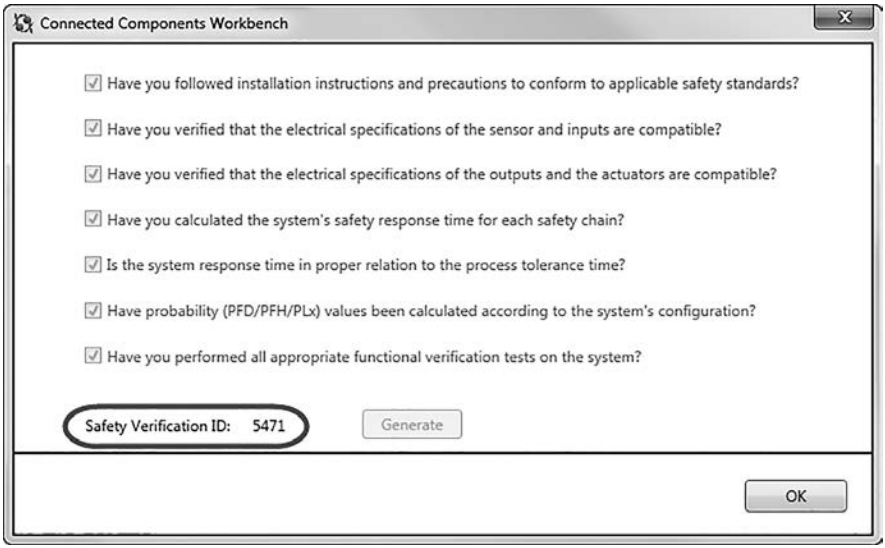


WAŻNE: Aby wygenerować numer identyfikacyjny (ID) weryfikacji, należy zaznaczyć wszystkie okienka.

6. Kliknij Yes (tak), aby kontynuować weryfikację.

7. Kliknij Yes (tak), aby zmienić na tryb Run (praca).

8. Zapisz numer ID weryfikacji bezpieczeństwa w dokumentacji maszyny.



Procedura ta stanowi informację zwrotną dla przekaźnika 440C-CR30, potwierdzającą zakończenie weryfikacji systemu i testów funkcjonalnych. Unikalny identyfikator weryfikacji może być wykorzystany do sprawdzenia, czy dokonano zmian pliku konfiguracyjnego. Wszelkie zmiany konfiguracji skutkują anulowaniem numeru ID weryfikacji bezpieczeństwa. Każdy kolejna procedura weryfikacji generuje nowy numer ID. Numer ID weryfikacji bezpieczeństwa jest wyświetlany przez oprogramowanie Connected Component Workbench tylko wtedy, gdy istnieje połączenie z przekaźnikiem 440C-CR30.

Rozdział 11: Produkty, narzędzia i usługi

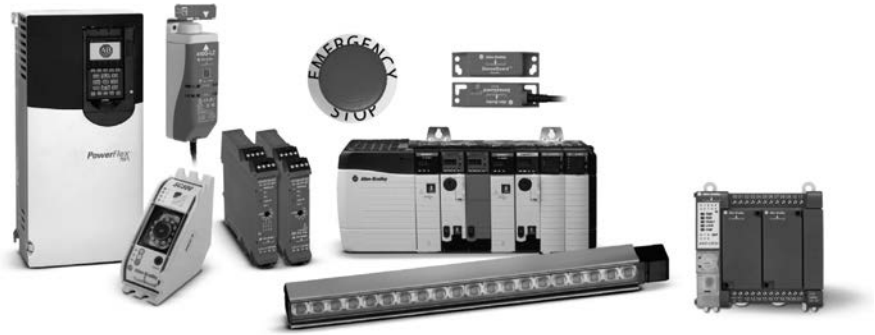
Przegląd

Firma Rockwell Automation jest wiodącym światowym dostawcą rozwiązań z zakresu zasilania, sterowania oraz informatyki przemysłowej, zapewniającą swoim klientom wsparcie w wielu branżach przemysłu od ponad 100 lat. Część jej oferty z zakresu automatyki przemysłowej stanowią kompleksowe technologie, narzędzia i usługi związane z bezpieczeństwem maszyn.

Produkty i technologie dla Państwa aplikacji

Firma Rockwell Automation zapewnia najobszerniejszą ofertę rozwiązań w zakresie bezpieczeństwa maszyn i może dostarczyć wszystkie trzy elementy składowe systemu bezpieczeństwa (urządzenia wejściowe, sterowanie logiczne i końcowe elementy zasilające).

Dostępne produkty i technologie obejmują:



Urządzenia wejściowe bezpieczeństwa

- **Urządzenia wykrywające obecność**
  Urządzenia wykrywające obecność lokalizują obiekty i osoby znajdujące się w pobliżu stref zagrożenia. Można wśród nich wymienić: kurtyny świetlne bezpieczeństwa, skanery laserowe bezpieczeństwa, czujniki wykrywania rąk, maty i listwy czułe na nacisk.

- **Wyłączniki blokujące bezpieczeństwa**
  Wyłączniki bezpieczeństwa zostały zaprojektowane i skonstruowane zgodnie ze światowymi normami niezawodności, stabilności i jakości. Wyłączniki bezpieczeństwa obejmują wyłączniki blokujące, wyłączniki krańcowe oraz urządzenia stopu awaryjnego.

- **Urządzenia stopu awaryjnego i wyzwalające**
  Przyciski stopu awaryjnego to szeroki zakres przycisków grzybkowych o wymuszonym przełączaniu zestyków. Urządzenia zezwalające i wyłączniki linkowe to elementy funkcji awaryjnych dostępne wzdłuż całego obszaru aplikacji lub też przenoszone, co umożliwia operatorowi swobodne przemieszczanie się po obszarze aplikacji bezpieczeństwa.

- **Interfejs operatora**
  Interfejsy operatora umożliwiają operatorom interakcję z aplikacją i dysponują dodatkowymi, dedykowanymi funkcjami bezpieczeństwa.

Kontrolery logiki bezpieczeństwa

- **Przekaźniki bezpieczeństwa (ze stałą funkcją lub konfigurowalne)**
  Przekaźniki bezpieczeństwa sprawdzają i monitorują system bezpieczeństwa, czego wynikiem jest zezwolenie na uruchomienie maszyny lub polecenie jej zatrzymania. Przekaźniki bezpieczeństwa ze stałą funkcją są najbardziej ekonomicznym rozwiązaniem dla mniejszych maszyn, dla których potrzebne jest dedykowane urządzenie logiczne obsługujące funkcję bezpieczeństwa. Modułowe i konfigurowalne przekaźniki bezpieczeństwa są preferowane w zastosowaniach, w których wymagana jest duża liczba różnych urządzeń ochronnych oraz minimalne sterowanie strefowe.

- **Zintegrowane sterowniki bezpieczeństwa**
  Sterowniki PLC bezpieczeństwa wykorzystują zalety tradycyjnych systemów PLC w aplikacjach bezpieczeństwa. Zastępują zwykłe instalacje przekaźnikowe, których zadaniem jest zmiana stanu zautomatyzowanego procesu na stan bezpieczny. Sterowniki PLC bezpieczeństwa umożliwiają wykonanie programów standardowych, jak i związanych z bezpieczeństwem w pojedynczej kasecie sterownikowej. Zapewnia to elastyczność programowania oraz znajome i łatwe w użyciu środowisko dla programistów. Rozwiązania w dziedzinie sterowników bezpieczeństwa obejmują otwarte i zintegrowane tryby sterowania, zapewniające bezpieczeństwo maszyn oraz ochronę środków trwałych.

- **Urządzenia we/wy bezpieczeństwa**
  Produkty bezpieczeństwa z rodziny Guard I/O™ oferują wszystkie zalety tradycyjnych rozproszonych we/wy, zostały jednak stworzone specjalnie do systemów bezpieczeństwa. Zmniejszają one koszty oprzewodowania i skracają czas rozruchu maszyn i cel robotów, a szeroki zakres funkcjonalności pozwala na instalację zarówno w szafach sterowniczych, jak i bezpośrednio na maszynie.

Elementy wykonawcze bezpieczeństwa

- **Styczniki i rozruszniki bezpieczeństwa**
  Rozproszone rozruszniki silnikowe ArmorStart® zapewniają kategorię 4 funkcji bezpieczeństwa, a jednocześnie dają się zintegrować z układem bezpieczeństwa DeviceNet™ On-Machine™. Styczniki i przekaźniki bezpieczeństwa umożliwiają ochronę pracowników przed niezamierzonym uruchomieniem maszyn i utratą funkcji bezpieczeństwa.

- **Przemienniki częstotliwości PowerFlex®**
  Przemienniki PowerFlex są dostępne z wbudowanymi funkcjami bezpieczeństwa. Przemienniki PowerFlex 525 dysponują standardowo funkcją bezpiecznego wyłączenia momentu. Funkcja Safe Torque-Off jest też opcjonalnie na wyposażeniu przemienników PowerFlex z serii 40P, 70, 700H, 700S, a także 750, które również obsługują funkcję monitorowania prędkości bezpiecznej.

- **Serwonapędy Kinetix®**
  Wszystkie serwonapędy Kinetix 300, 6000, 6200, 6500 i 7000 są wyposażone we wbudowane funkcje bezpieczeństwa. Zadaniem funkcji bezpiecznego wyłączenia momentu jest wyłączenie wyjścia napędu w celu usunięcia momentu obrotowego silnika, jednak bez wyłączenia zasilania całej maszyny. Monitorowanie prędkości bezpiecznej umożliwia użytkownikom ograniczenie i nadzorowanie prędkości aplikacji w celu umożliwienia operatorom bezpiecznego wykonania niektórych czynności bez całkowitego zatrzymania maszyny.

Systemy łączeniowe/sieci komunikacyjne

- **Systemy połączeniowe „Quick connect”**
  Trójniki i rozgałęźniki, bloki rozdzielcze oraz terminatory z rodziny Guardmaster® stanowią część systemu łączeniowego dedykowanego bezpieczeństwu maszyn.

- **GuardLink™**
  GuardLink to protokół komunikacyjny bezpieczeństwa wykorzystujący standardowe okablowanie w topologii „trunk and drop” i złącza typu „plug and play”. Umożliwia komunikację między urządzeniami bezpieczeństwa dla celów diagnostyki i sterowania (np. polecenia zdalnego resetowania i odryglowania) z wykorzystaniem pojedynczego kabla. Do kabla o długości do 1000 m można podłączyć do 32 urządzeń. Urządzenia bezpieczeństwa marki Allen-Bradley wyposażone w technologię GuardLink umożliwiają użytkownikowi dostęp do danych systemu bezpieczeństwa, jak również umożliwiają dostęp do tych danych przez sieć EtherNet/IP. GuardLink pomaga uprościć konfigurację systemu, zredukować oprzewodowanie i poszerzyć informacje diagnostyczne dla celów konserwacji i eksploatacji.

- **Bezpieczeństwo przez sieć EtherNet/IP**
  Sieć EtherNet/IP™ zapewnia systemy komunikacyjne obejmujące cały zakład przy użyciu otwartych przemysłowych technologii sieciowych. Umożliwia sterowanie i uzyskiwanie informacji w czasie rzeczywistym w aplikacjach dyskretnych, ciągłych procesowych, szarżowych, bezpieczeństwa, napędowych, pozycjonujących i wysokiej dostępności. Sieciami EtherNet/IP można połączyć urządzenia takie, jak rozruszniki silnikowe i czujniki ze sterownikami i interfejsami HMI, a także – w szerszym zakresie – całe przedsiębiorstwo. Umożliwiają one komunikację w zastosowaniach przemysłowych i poza nimi, za pomocą jednej, wspólnej infrastruktury sieciowej.

Pomocne narzędzia

Szeroka gama narzędzi wspierających zgodność z normami bezpieczeństwa, zmniejszających ryzyko obrażeń i poprawiających wydajność.

Safety Automation Builder

Safety Automation Builder to BEZPŁATNE narzędzie programowe umożliwiające uproszczenie i walidację projektu systemu bezpieczeństwa maszyny, co wiąże się ze zmniejszeniem kosztów i oszczędnością czasu. Integracja z oprogramowaniem do oceny ryzyka RASWin zapewnia użytkownikom spójne, niezawodne i udokumentowane zarządzanie cyklem życia bezpieczeństwa funkcjonalnego. Safety Automation Builder umożliwia optymalizację projektu systemu bezpieczeństwa, podniesienie poziomu zgodności i zmniejszenie kosztów – prowadzi użytkownika przez opracowanie systemów bezpieczeństwa z uwzględnieniem ich układu, wyboru produktów i analizy bezpieczeństwa, aby zapewnić spełnienie przez maszynę wymagań poziomu wydajności (PL) określonych przez ogólnoświatową normę EN ISO 13849-1.

RASWin

Oprogramowanie RASWin wspomaga użytkowników w zarządzaniu cyklem życia bezpieczeństwa funkcjonalnego, organizowaniu informacji na każdym etapie procesu oraz walidacji maszyny. RASWin łączy etapy cyklu życia systemu bezpieczeństwa, w tym specyfikacji funkcji bezpieczeństwa, wymaganego poziomu zapewnienia bezpieczeństwa (PLr), obliczeń poziomu zapewnienia bezpieczeństwa PLr, walidacji obwodów bezpieczeństwa i dokumentacji, a także wykluczeń błędów systematycznych.

Kalkulator poziomu wydajności SISTEMA

Narzędzie SISTEMA, opracowane przez Instytut Bezpieczeństwa i Higieny Pracy niemieckiego Towarzystwa Ubezpieczeń od Wypadków IFA, automatyzuje obliczenia poziomu zapewnienia bezpieczeństwa PL dla elementów układu sterowania maszyny związanych z bezpieczeństwem zgodnie z EN ISO 13849-1. Dane produktów bezpieczeństwa firmy Rockwell Automation są dostępne w postaci biblioteki, której można użyć bezpośrednio w narzędziu programowym SISTEMA. Takie połączenie daje projektantom maszyn i systemów kompleksowe, oszczędzające czas wsparcia w procesie oceny bezpieczeństwa zgodnie z EN ISO 13849-1. Funkcja eksportu

w pakiecie Safety Automation Builder pozwala na łatwy import projektu systemu bezpieczeństwa do programu SISTEMA w celu uzyskania niezależnej weryfikacji wymaganego poziomu wydajności PL.

Wstępnie opracowane funkcje bezpieczeństwa dla maszyn

Funkcje bezpieczeństwa maszyn wymagają użycia wielu elementów, takich jak czujniki lub urządzenia wejściowe, urządzenia logiki oraz urządzenia wyjściowe. Razem elementy te zapewniają poziom ochrony obliczony jako poziom zapewnienia bezpieczeństwa zgodnie z EN ISO 13849-1. Firma Rockwell Automation opracowała wiele dokumentów dotyczących funkcji bezpieczeństwa, z których każdy podaje wytyczne dla poszczególnych funkcji bezpieczeństwa w oparciu o wymagania funkcjonalne, dobór urządzeń i wymagany poziom PL. Zawierają one konfigurację i schemat podłączeń, plan weryfikacji i walidacji oraz obliczenia poziomu zapewnienia bezpieczeństwa.

Wskaźnik dojrzałości systemu bezpieczeństwa

Wskaźnik Safety Maturity Index™ (dojrzałości systemu bezpieczeństwa) stanowi wszechstronną ocenę efektywności kultury bezpieczeństwa, procesów i procedur zgodności oraz inwestycji kapitałowych w dziedzinie technologii bezpieczeństwa. Pozwala on firmom na zrozumienie bieżącego poziomu efektywności oraz tego, jakie kroki należy podjąć, aby uzyskać poprawę bezpieczeństwa i zyskowności firmy.

Usługi i doświadczenie zapewniają wsparcie

Jako największy na świecie dostawca rozwiązań z zakresu bezpieczeństwa przemysłowego firma Rockwell Automation pomaga zmniejszyć liczbę wypadków i obniżyć koszty przy jednoczesnym poprawieniu wydajności w każdej fazie cyklu życia systemu bezpieczeństwa.

Usługi w zakresie bezpieczeństwa są wykonywane przez ekspertów doświadczonych w dziedzinie bezpieczeństwa maszyn, z których wielu posiada certyfikaty TÜV Rheinland. Rockwell Automation zatrudnia również ekspertów TÜV w zakresie bezpieczeństwa funkcjonalnego, inżynierów i techników, którzy pomagają klientom holistycznie zarządzać cyklem życia systemu bezpieczeństwa.

Cykl życia systemu bezpieczeństwa to jasno zdefiniowany proces, który pomaga zmaksymalizować produktywność i poprawić bezpieczeństwo przez określenie kroków niezbędnych do oceny i zmniejszenia ryzyka związanego z użyciem maszyn. Z cyklem życia systemu bezpieczeństwa można zapoznać się lub pobrać go w ramach niniejszego dokumentu.

Niektóre dostępne usługi to:

- **Ocena bezpieczeństwa**
  Usługi wspomagające szacowanie ryzyka w zakładzie oraz podejmowanie świadomych decyzji wpływających na poprawę bezpieczeństwa pracowników i maszyn.

- **Usługi projektowe**
  Kompleksowe projektowanie obwodów, prawidłowe zastosowanie urządzeń i sprawdzanie projektów mające na celu zwiększenie ogólnego bezpieczeństwa.

- **Usługi w zakresie instalacji i walidacji**
  Potwierdzenie, że systemy pracują w zakresie określonych parametrów i norm.

- **Szkolenie w zakresie bezpieczeństwa**
  Wszechstronne programy szkoleniowe prowadzone przez czołowych ekspertów branżowych.

- **Usługi dostosowane do potrzeb**
  Dotyczą one aplikacji, technologii, platform i konfiguracji opracowanych przez klienta.

Dlaczego wybrać Rockwell Automation

Połączenie dziedzin bezpieczeństwa i automatyki przynosi korzyści dzięki zwiększonej wydajności na wielu etapach procesu produkcyjnego, od zaprojektowania i przetestowania urządzeń, przez ich właściwy montaż, rozruch, eksploatację i konserwację, po modyfikacje i wycofanie z użycia. Wszystkie te etapy można zoptymalizować przez prawidłowe zastosowanie rozwiązań bezpieczeństwa.

Jako światowy lider w dziedzinie automatyki i bezpieczeństwa przemysłowego oraz innowator technologiczny firma Rockwell Automation jest w idealnym położeniu do wspierania bardziej efektywnych, bezpieczniejszych i wydajniejszych rozwiązań w dziedzinie produkcji.

Dzięki wieloletniemu doświadczeniu w dziedzinie automatyki i bezpieczeństwa, wiedzy na temat aplikacji oraz przez zastosowanie wiodących zasad zawartych w normach bezpieczeństwa, takich jak ISO 12000, EN ISO 13849-1 i IEC 62061, Rockwell Automation jest w stanie zapewnić pomoc w zakresie wyboru, integracji, szkolenia i wsparcia rozwiązań bezpieczeństwa maszyn, procesów technologicznych i systemów elektrycznych.

www.rockwellautomation.com

Centra Techniczne Napędów, Sterowania i Informatyki

Ameryka Północna i Południowa: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europa/Bliski Wschód/Afryka: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Azja/Australia/Oceania: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Polska: Rockwell Automation, Ul.Powązkowska 44C, 01-797 Warszawa, Tel: (48) 22 32 60 700, Fax: (48) 22 32 60 710, www.rockwellautomation.pl

Publikacja: SAFEBK-RM002C-EN-P – listopad 2016

© 2016 Rockw--ell Automation, Inc. Wszystkie prawa zastrzeżone.