Bezpieczne konstrukcje układów sterowania maszyn

W nawiązaniu do wielokrotnie przywoływanej na łamach ATESTU „europejskiej koncepcji bezpieczeństwa maszyn", warto przypomnieć, że za kształtowanie bezpieczeństwa maszyn w środowisku zawodowym odpowiadają ich producenci i użytkownicy.

Mariusz Głowicki

dyrektor operacyjny w firmie ELOKON Polska, konstruktor systemów bezpieczeństwa, współpracuje z działającym przy PKN Komitecie Technicznym nr 50 ds. Automatyki i Robotyki Przemysłowej

Wymagania prawne wspierające skuteczną realizację wspomnianej koncepcji sformułowano w dyrektywach ekonomicznych i socjalnych. Obecnie dla tzw. nowych maszyn ich projektanci, producenci i dostawcy są zobligowani do spełnienia wymagań zasadniczych dyrektywy 2006/42/WE wdrożonej do prawa krajowego przez rozporządzenie Ministra Gospodarki z 21 października 2008 r. Normy zharmonizowane z dyrektywą są narzędziem do wypełnienia jej wymagań.

Dla drugiej grupy adresatów – użytkowników, a praktycznie pracodawców, maszyny stanowią jeden z elementów stanowisk pracy. Minimalne wymagania stawiane pracodawcom w zakresie bezpieczeństwa sprzętu roboczego zawarto w dyrektywie 2009/104/WE wdrożonej do prawa krajowego przez rozporządzenie Ministra Gospodarki z 30 października 2002 r. Zapisy dyrektywy mają również zastosowanie do tzw. starych maszyn, w przypadku Polski wyprodukowanych i wprowadzonych do obrotu po raz pierwszy przed 1 maja 2004 r.

Dzięki opisanemu wyżej podejściu w ciągu ostatnich kilku lat wśród producentów i użytkowników maszyn znacznie wzrosła wiedza na temat wymagań stawianym maszynom. Znajduje to realne przełożenie na sposoby ich bezpieczniejszej konstrukcji, rodzaje wykorzystywanego w nich wyposażenia i podzespołów, niezależnie czy dotyczy to pierwotnej budowy, czy przebudowy – modernizacji. Oczywiście zasadniczą funkcją maszyny jest umożliwienie uzyskania konkretnego produktu, ale jednocześnie konieczne jest przy tym zachowanie stosownych wymagań bezpieczeństwa.

Związek oceny ryzyka i wymagań stawianych układom sterowania

Obserwując przemysł i galopującą w nim automatyzację, nie można nie zgodzić się ze stwierdzeniem, że lwia część „bezpieczeństwa maszyny" jest zawarta w strukturze i sposobie działania jej układu sterowania. Jego poprawna konstrukcja i dobór właściwej dla danej aplikacji aparatury jest tutaj bardzo istotny. Należy podkreślić, że układ sterowania, przynajmniej w zakresie funkcji bezpieczeństwa, powinien być zawsze zaprojektowany i wykonany na podstawie wyników wcześniej przeprowadzonego, wymaganego przez dyrektywy procesu oceny ryzyka. Ocena ryzyka, jak i inne wymagania dyrektyw i norm mogą czasami bardzo rozbudować wstępnie zakładany układ sterowania technologicznego.

Ponieważ większość czytelników ATESTU doskonale porusza się w zagadnieniach oceny ryzyka, sądzę, że nie ma potrzeby opisywania tego zagadnienia. Celem artykułu jest przybliżenie czytelnikom podstawowych informacji w obszarze „bezpiecznych konstrukcji układów sterowania maszyn". Nawiązując do oceny ryzyka warto jedynie podkreślić, że rzetelne przeprowadzenie tego procesu, a w szczególności jednego z jej kroków – identyfikacji zagrożeń, stanowi bazę do stworzenia algorytmu zachowania maszyny w danej sytuacji zagrożenia, czyli potencjalnej chwili, kiedy operator będzie bezpośrednio narażony na kontakt z czynnikiem zagrażającym. Praktycznie algorytm ten jest sprowadzony do często przywoływanego w normach terminu *funkcji bezpieczeństwa* maszyny, czyli ogółu działań związanych z redukcją ryzyka.

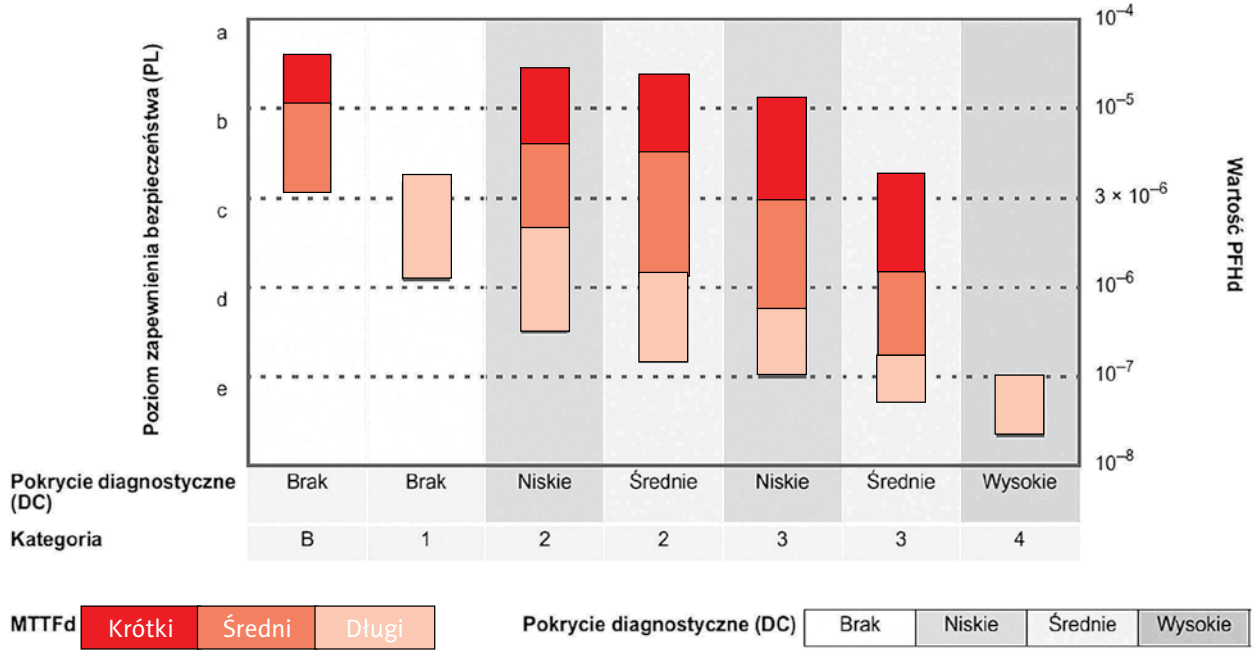
Ocena ryzyka powinna – poza zidentyfikowaniem zagrożeń i nadaniem odpowiadającej im wartości ryzyka – jednocześnie narzucić wymagania dotyczące układów sterowania, niezbędne jeżeli później zdecydowanoby się na redukcję ryzyka przy wykorzystaniu funkcji sterujących realizowanych przez elementy włączane w układy sterowania. Z punktu widzenia doboru komponentów do układu sterowania bezpieczeństwa najistotniejszym elementem całego procesu oceny ryzyka jest więc pierwotne oszacowanie ryzyka, ponieważ to właśnie wtedy zostają ustalone wymagania co do niezawodności i architektury wykorzystanej aparatury.

Specyfikację konstrukcji obwodów sterowania odpowiedzialnych za bezpieczeństwo określają obecnie dwie normy (obie zharmonizowane z dyrektywą 2006/42/WE): PN-EN ISO 13849-1, operująca parametrem niezawodności *Performance Level (PL)*, oraz PN-EN 62061, gdzie tę rolę pełni *Safety Integrity Level (SIL)*, czyli poziom nienaruszalności bezpieczeństwa. Decyzja, która z norm zostanie wybrana powinna być uzależniona od możliwości aplikacji, ale i wiedzy konstruktora.

Niezawodność układów bezpieczeństwa

Fundamentem pewności działania układów sterowania odpowiedzialnych za realizacje funkcji bezpieczeństwa jest ich skonstruowanie na podstawie normy PN-EN ISO 13849-1 lub normy PN-EN 62061.

W przypadku pierwszej z nich skuteczność działania obwodów jest opisywana parametrem *Performance Level*, który defi- →



Zależności pomiędzy parametrami składowymi Performance Level

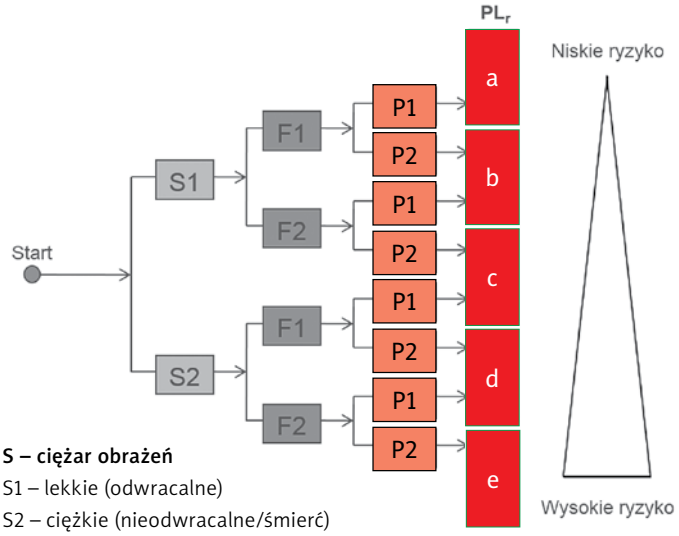
niuje 5 poziomów od „a" do „e" zależnych od poziomu ryzyka, określających wymagania jakościowe związane z zachowaniem się obiektu w razie wystąpienia uszkodzenia (*Kategoria*) oraz wymagania ilościowe opisane elementami niezawodności: *Mean Time To Dangerous Failure* (MTTFd) – średni czas do wystąpienia niebezpiecznego uszkodzenia, *Diagnostic Coverage* (DC) – pokrycie diagnostyczne i *Common Cause Failure* (CCF) – uszkodzenia spowodowane wspólną przyczyną.

Norma PN-EN 62061 jest tzw. normą sektorową dla normy PN-EN 61508 poruszającej w szerokim zakresie zagadnienie bezpieczeństwa funkcjonalnego. PN-EN 62061 dotyczy wyłącznie specyfiki sektora maszynowego. Ma ułatwiać określanie niezawodności działania systemów elektrycznego sterowania związanych z bezpieczeństwem w odniesieniu do znaczących zagrożeń generowanych przez maszyny.

Safety Integrity Level przedstawiony w normie PN-EN 62061 to poziom dyskretny (dla sektora maszyn jeden z trzech możliwych SIL 1 – SIL 3). Poziom ten podobnie jak *Performance Level* w przypadku PN-EN ISO 13849-1 określa zdolność układu do realizacji funkcji bezpieczeństwa, i jest również określany poprzez pewne parametry składowe, do których możemy zaliczyć architekturę podsystemów wchodzących w skład obwodu, jak i ich: wskaźniki uszkodzeń bezpiecznych SFF, strumienie uszkodzeń λ, współczynnik uszkodzeń spowodowanych wspólną przyczyną β czy pokrycie diagnostyczne DC.

Ponieważ norma PN-EN 62061 rozpatruje obwody bezpieczeństwa wykonane wyłącznie w szeroko rozumianej technice elektrycznej, nie może ona w pełni zapanować nad bezpieczeństwem maszynowym. Wszędzie tam, gdzie w obwodach bezpieczeństwa konieczne jest wykorzystanie elementów nieelektrycznych – np. zaworów pneumatycznych w celu zatrzymania określonych siłowników, konieczne jest stosowanie normy PN-EN ISO 13849-1. Mimo poświęcenia normy PN-EN 62061 tylko technice elektrycznej, znalazła ona szerokie zastosowanie wśród producentów wyposażenia bezpieczeństwa, takiego jak sterowniki czy przekaźniki. Obie przywołane normy umożliwiają wzajemne – wymienne stosowanie, ale niestety każda z nich przedstawia odrębną metodę szacowania ryzyka. Często doprowadza to do ustalania różnych wymagań dla obwodów bezpieczeństwa. Jak wskazuje praktyka, aby świadomie zapanować nad tą sytuacją, najlepszym krokiem jest stosowanie jednej spójnej metody oceny ryzyka (np. opracowanej na własne potrzeby).

Podsumowując, w dużym uproszczeniu można powiedzieć, że wraz ze wzrostem ryzyka w danej strefie maszyny w celu jego ograniczenia konieczne będzie zminimalizowanie prawdopodobieństwa wystąpienia zdarzenia niebezpiecznego. To może być osiągnięte przez wykonanie



S – ciężar obrażeń
S1 – lekkie (odwracalne)
S2 – ciężkie (nieodwracalne/śmierć)
F – częstotliwość i/lub czas ekspozycji na zagrożenie
F1 – rzadko lub średnio
F2 – często lub ciągle
P – możliwość uniknięcia zagrożenia lub ograniczenia szkód
P1 – możliwe w określonych warunkach
P2 – prawie niemożliwe

Graf szacowania ryzyka – PL, wg PN-EN ISO 13849-1

obwodów bezpieczeństwa nadzorujących strefę na coraz to wyższym (bardziej niezawodnym) *Performance Level* lub *Safety Integrity Level*. Z tego względu przed decyzją o wyborze konkretnego rozwiązania bezpieczeństwa konieczna jest wiedza na temat potrzeb z procesu oceny ryzyka. Wśród dostępnych na rynku elementów można znaleźć zarówno cechujące się niską niezawodnością (stosunkowo tanie), np. standardowe czujniki technologicznie, jak i układy takie jak programowalne sterowniki bezpieczeństwa umożliwiające stworzenie najbardziej niezawodnych, redundantnych i monitorowanych struktur (stosunkowo drogich) funkcji bezpieczeństwa – PL e przy Kategorii 4 wg PN-EN ISO 13849-1, czy SIL 3 wg PN-EN 62061. Tylko dobra ocena ryzyka pozwoli zoptymalizować wybór w obszarze cena – możliwości.

Funkcje bezpieczeństwa

Nawiązując do definicji zawartych w normach, za funkcję bezpieczeństwa maszyny uważa się taką, której wadliwa realizacja może powodować natychmiastowy wzrost ryzyka. Tak jak zostało to opisane wcześniej, na funkcje bezpieczeństwa maszyny składają się zasady reakcji maszyny w wyniku wystąpienia sytuacji zagrożenia dla operatora.

Każda z funkcji bezpieczeństwa powinna być zbudowana na odpowiednim poziomie niezawodności, na podstawie wyników procesu oceny ryzyka i wytycznych normy PN-EN ISO 13849-1 lub PN-EN 62061. Elementami realizującymi funkcje bezpieczeństwa są tzw. podsystemy, które dzieli się najczęściej na trzy grupy: wejściowe, logiczne i wyjściowe.

Do typowych podsystemów wejściowych w obwodach

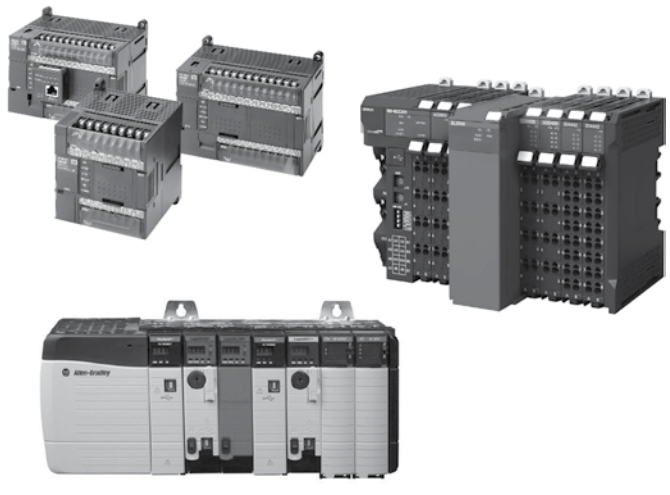
Bloki strukturalne funkcji bezpieczeństwa

bezpieczeństwa zaliczamy takie elementy, jak urządzenia zatrzymywania awaryjnego, urządzenia blokujące i blokujące z ryglowaniem sprzężone z osłonami, elektroczułe urządzenia optoelektroniczne i wiele innych. Wśród elementów logicznych wyróżniamy m.in. przekaźnikowe moduły bezpieczeństwa, programowalne sterowniki bezpieczeństwa, ale również w określonych aplikacjach mogą znaleźć się tutaj zwykłe programowalne sterowniki lub kombinacje styczników i przekaźników. Ostatnią z grup reprezentują najczęściej: styczniki, elektrozawory pneumatyczne i hydrauliczne, napędy elektryczne. Warto dodać, że sam element wykonujący ruch – np. siłownik pneumatyczny czy silnik elektryczny nie jest częścią łańcucha realizującego funkcję bezpieczeństwa, lecz jedynie czynnikiem przez nią nadzorowanym.

Bardzo często zdarza się, że jeden podsystem (niezależnie od przynależności do grupy) może być częścią kilku łańcuchów realizujących funkcje bezpieczeństwa. Przykładowo jedno urządzenie zatrzymywania awaryjnego może zarówno inicjować zatrzymanie awaryjne określonego napędu elektrycznego w jednej ze stref maszyny, jak i innych siłowników pneumatycznych w strefie sąsiedniej. Z punktu widzenia konstrukcji i analiz obwodów bezpieczeństwa maszyn będą to osobne funkcje. Co więcej, ze względu na różne możliwe ciężkości urazów powodowane przez te elementy ruchome, również o prawdopodobnie innych zakładanych wcześniej na etapie oceny ryzyka, jak i finalnie uzyskanych parametrach PL/SIL. Znakomitym przykładem takiego komponentu jest programowalny sterownik bezpieczeństwa. W zależności od indywidualnych cech danego modelu może on być podsystemem umożliwiającym realizację określonej liczby funkcji w tym samym czasie. Wynika to oczywiście w głównej mierze z liczby jednocześnie obsługiwanych wejść/wyjść oraz oczekiwań co do parametrów PL/SIL dla samych funkcji bezpieczeństwa.

Do najczęstszych przykładów funkcji bezpieczeństwa można zaliczyć: zatrzymanie ruchu niebezpiecznego wyzwolonego przez techniczny środek ochronny – np. w wyniku otwarcia osłony blokującej; reset manualny w celu anulowania wcześniejszej komendy zatrzymania, wyzwalany przez zamierzone działanie na przycisk przed ponownym restartem określonych ruchów; muting – celowa i okresowa dezaktywacja danego technicznego środka ochronnego (np. kurtyn świetlnych) w celu umożliwienia wykonania określonej operacji technologicznej, dzięki wykorzystaniu innych odpowiednich czujników; monitorowanie przełączania takich elementów jak styczniki czy elektrozawory; monitorowanie prędkości ruchu elementów niebezpiecznych przy jednoczesnej pracy z urządzeniem zezwalającym wyposażonym w dodatkowe przyciski pełniące rolę urządzeń sterowanych podtrzymywanych; zatrzymywanie awaryjne.

Wszystkie powyższe funkcje mogą być zrealizowane z wykorzystaniem programowalnych sterowników bezpieczeństwa. Decyzja o wyborze sterownika bezpieczeństwa powinna być poparta m.in. analizą liczby funkcji bezpieczeństwa, którą należy zaimplementować w układzie sterowania maszyny. Z punktu widzenia kosztów, czasami może okazać się bowiem, że przy relatywnie małej liczbie funkcji bezpieczeństwa na maszynie bardziej opłacalne może być zastosowanie pewnej liczby modułów przekaźnikowych bezpieczeństwa.



Przykłady sterowników bezpieczeństwa

Reasumując, aby poprawnie dobrać zabezpieczenie na maszynie musimy przeprowadzić ocenę ryzyka i spełnić wymagania odpowiednich norm związanych z techniką bezpieczeństwa. Warto dodać, że w przypadku niektórych maszyn – stanowisk pracy, poza zrealizowaniem zaleceń ze wspomnianych norm niezbędne może być również sięgnięcie do norm szczegółowych typu C zharmonizowanych z Dyrektywą Maszynową 2006/42/WE, gdzie z reguły określone są precyzyjne wymagania stawiane danym rozwiązaniom technicznym związanym z bezpieczeństwem.