Bezpieczeństwo i kontrola w automatyce

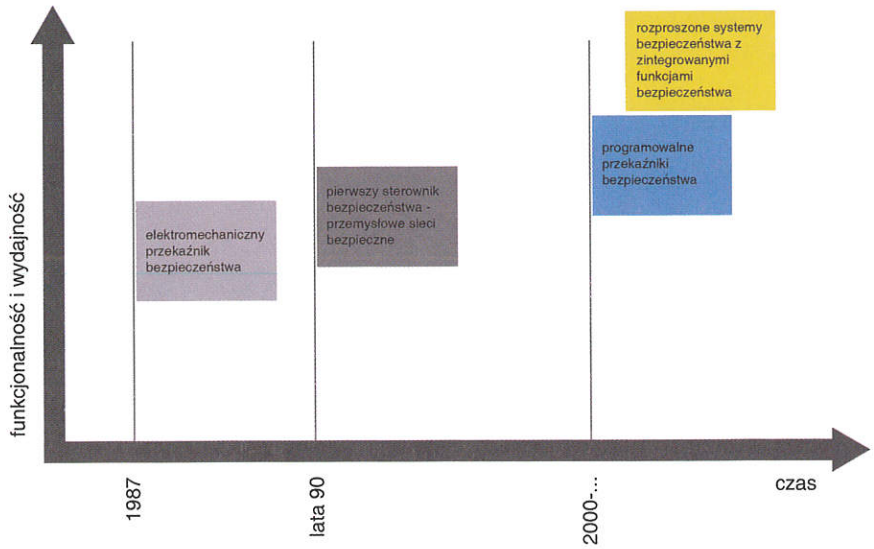
W ostatnich 30 latach nastąpił duży postęp w dziedzinie automatyki i budowy systemów sterowania, szczególnie w zakresie systemów odpowiedzialnych za bezpieczeństwo maszyn. Do lat 80. w zasadzie nie mówiono o systemach sterowania odpowiedzialnych za bezpieczeństwo. Od kiedy w 1987 r. pojawił się pierwszy elektromechaniczny przekaźnik bezpieczeństwa, systemy sterowania zaczęto dzielić na standardowe i odpowiedzialne za bezpieczeństwo.

Tomasz Otrębski

Wraz z rozwojem automatyzacji rosły wymagania. W latach 90. pojawił się pierwszy sterownik bezpieczeństwa – w pełni programowalna jednostka, która mogła obsłużyć zarówno część standardową aplikacji, jak i związaną z bezpieczeństwem. Intensywny rozwój programowalnych systemów bezpieczeństwa nastąpił z początkiem XXI w. Czołowi producenci, odpowiadając na potrzeby runku, wprowadzili do portfolio tzw. programowalne przekaźniki bezpieczeństwa, które dzięki prostemu interfejsowi opartemu na graficznych blokach – odpowiadających danym funkcjom bezpieczeństwa – były łatwe w programowaniu, a ponadto konkurencyjne cenowo w porównaniu ze sterownikami bezpieczeństwa, zaawansowanymi i przeznaczonymi do bardziej wymagających aplikacji. Prostą, pojedynczą maszynę, np. z trzema funkcjami bezpieczeństwa (osłona blokująca, kurtyna bezpieczeństwa oraz urządzenie zatrzymania awaryjnego) można było wyposażyć w jedną programowalną jednostkę (programowalny przekaźnik bezpieczeństwa) zamiast trzech oddzielnych modułów elektromechanicznych. Z końcem lat 90. zaczęto rozwijać również bezpieczne sieci przemysłowe. Rozległe obiektowo aplikacje wymagały od systemów związanych z bezpieczeństwem decentralizacji. Popularna wtedy sieć Profibus nie była w stanie bezpiecznie i niezawodnie przesyłać sygnałów z obiektu do jednostki centralnej. Pierwsze systemy rozproszone obsługujące sygnały bezpieczne pracowały w standardzie SafetyBUS p. Obecnie popularną komunikacją decentralną w obszarze systemów dotyczących bezpieczeństwa jest sieć PROFIsafe.

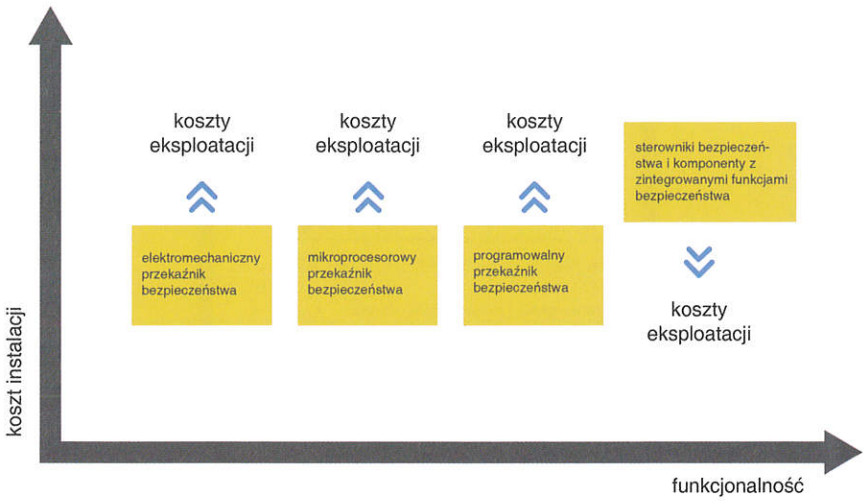
Od stycznika do programowalnej bezpiecznej logiki

W 1996 r. opublikowano normę EN 954-1, w której po raz pierwszy zdefiniowano niezawodność syste-



Rys. 1. Możliwości techniczne systemów sterowania związanych z bezpieczeństwem na przestrzeni lat

mów sterowania związanych z bezpieczeństwem w oparciu o tzw. kategorie. Przedstawiono pięć poziomów niezawodności: B oraz 1–4. Kategoria definiowała poziom odporności funkcji bezpieczeństwa na możliwe błędy. Z definicji poziom niezawodności oparty był na dobranym komponencie (kategorie B, 1–2) i strukturze (kategorie 3–4). Norma EN 954-1 nie opisywała systemów opartych na układach elektronicznych czy programowalnych. W latach 90. systemy sterowania odpowiedzialne za bezpieczeństwo budowane były w oparciu o systemy elektromechaniczne. Powszechnie stosowane były styczniki i różnego rodzaju łączniki elektromechaniczne. Występujące wówczas funkcje bezpieczeństwa to głównie osłony blokujące, osłony blokujące z urządzeniem ryglującym oraz oczywiście urządzenia zatrzymania awaryjnego jako uzupełniający środek ochronny. Coraz bardziej zaawansowana technologia i automatyzacja procesów produkcyjnych oraz rosnąca świadomość w obszarze bezpieczeństwa maszynowego spowodowały, że układy elektromechaniczne stawały się mało funkcjonalne. Trudno było realizować wyłącznie na nich logiczne funkcje bezpieczeństwa, kontrolę prędkości elementu niebezpiecznego, wartości przyspieszeń, kontrolę stanu zatrzymania itp. Niezbędne stały się programowalne układy logiczne. Obecnie poza autonomicznymi jednostkami programowalnymi, przeznaczonymi do realizacji funkcji bezpieczeństwa maszyn, producenci komponentów automatyki integrują w nich funkcje bezpieczeństwa, aby możliwe było łatwo i funkcjonalnie, a co za tym idzie wydajnie realizować zadania systemu sterowania odpowiedzialnego za bezpieczeństwo. Przykładowo powszechnie stosowane układy przekształtnikowe zasilające silniki asynchroniczne – zwane popularnie falownikami – mają obecnie zintegrowane funkcje bezpieczeństwa służące do bezpiecznego odłączenia napędu, nadzorowania procesu hamowania i ruchu, nadzorowania drogi i wiele innych. Bardziej zaawansowane systemy, oparte na serwonapędach, również mają zintegrowane funkcje bezpieczeństwa, które



Rys. 2. Zależność kosztów instalacji i funkcjonalności funkcji bezpieczeństwa w oparciu o różne rozwiązania techniczne

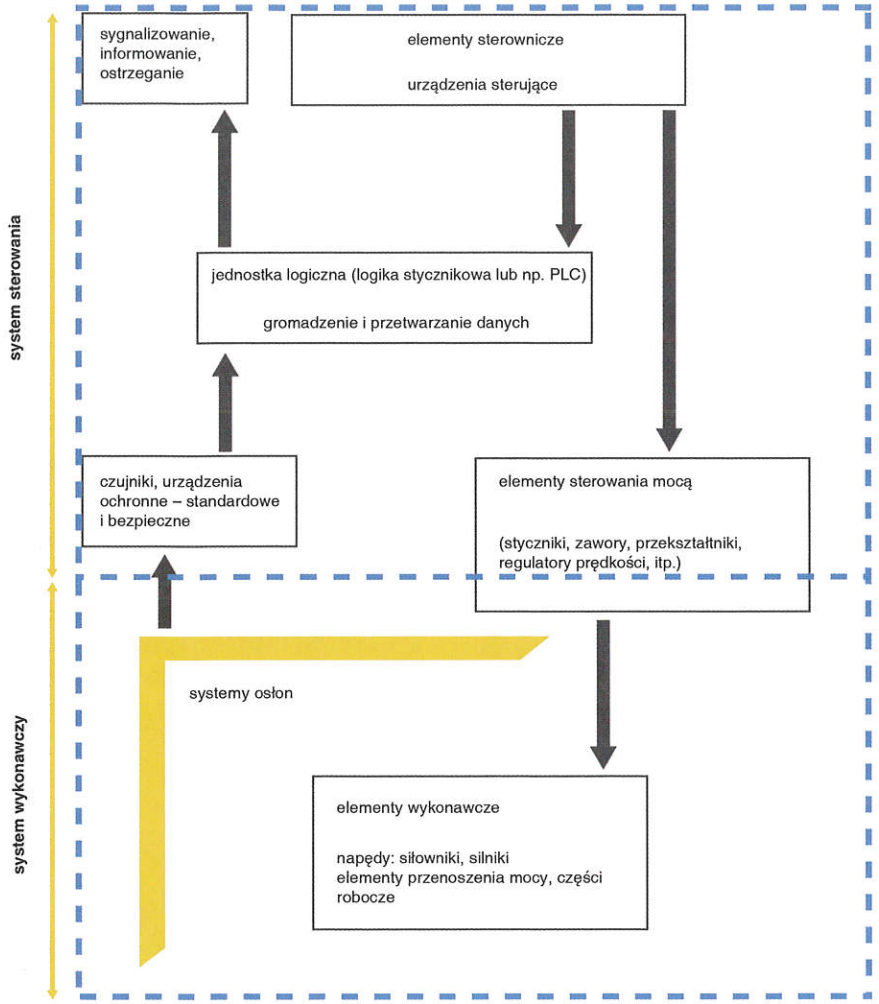
można parametryzować zgodnie z wymaganiami aplikacji. Stosując komponenty ze zintegrowanymi funkcjami bezpieczeństwa, można zbudować bardziej wydajne systemy sterowania, osiągnąć maksymalną funkcjonalność i zminimalizować czas diagnostyki. Jednocześnie można zapewnić dłuższą żywotność systemu sterowania dzięki zastosowaniu mniejszej liczby komponentów elektromechanicznych, których czas życia jest znacznie krótszy od elementów półprzewodnikowych, na których oparta jest realizacja parametryzowanych zintegrowanych funkcji bezpieczeństwa.

Funkcjonalność i wydajność systemów sterowania

Budując maszyny lub zautomatyzowane systemy produkcyjne, projektanci skupiają się na technologii, tak aby maszyna mogła wydajnie produkować. System bezpieczeństwa jest istotny, ale nie może przeszkadzać w osiągnięciu celu produkcyjnego i jakościowego. Dla niektórych maszyn, szczególnie prototypowych, osiągnięcie kompromisu w obszarze funkcjonalności, wydajności i bezpieczeństwa jest trudne. Im lepiej znamy proces produkcyjny, czyli technologię, tym łatwiej optymalizować projekt systemu sterowania.

Ważnym elementem przy projektowaniu systemu sterowania dla maszyn prototypowych jest przewidywanie funkcji, które nie są założone na etapie koncepcji, a mogą być potrzebne w fazie uruchamiania i pierwszych prób produkcyjnych. Systemy sterowania odpowiedzialne za bezpieczeństwo projektowane i wdrażane w latach 80. i początku 90. zazwyczaj miały ubogą funkcjonalność w zakresie bezpieczeństwa. Zdarzało się, że projektanci systemów sterowania uwzględniali jedynie funkcje bezpieczeństwa wyłączające całkowicie wszystkie energie maszyny. Przykładowo każde wejście w strefę niebezpieczną i otwarcie osłony blokującej odłączało wszystkie dostępne energie, co uniemożliwiało pracę z włączonymi napędami. Niestety, jeśli takie prace (np. nastawcze, serwisowe) po wejściu w strefę niebezpieczną były konieczne pojawiał się problem, który użytkownik musiał rozwiązać we własnym zakresie. Często w takiej sytuacji najprostszym dla użytkownika rozwiązaniem było mostkowanie wybranej osłony blokującej. Oznaczało to jednak duże ryzyko podczas wykonywania koniecznych prac pozaprodukcyjnych przy włączonych napędach.

Obecnie w przemyśle spotykamy się z dwoma przypadkami. Pierwszy dotyczy maszyn nowo projektowanych. Przy budowie maszyn łatwiej jest zarządzać procesem w fazie projektowania, gdyż nic fizycznie nie posiadamy i projekt zależy tylko od wiedzy inżynierskiej, wiedzy na temat technologii produkcji oraz budżetu na wyprodukowanie maszyny. Drugi przypadek dotyczy maszyn już użytkowanych, które chcemy modernizować ze względu



Rys. 3. Poglądowy schemat maszyny

na nowe wymagania produkcyjne lub z powodów bezpieczeństwa (tzw. procesy dostosowawcze).

W obu przypadkach musimy zdefiniować maszynę lub – w przypadku już istniejącej – nowe funkcje, tak aby możliwe było przeprowadzenie analizy i ewaluacji ryzyka, a finalnie – na podstawie oceny ryzyka – dobranie skutecznych środków bezpieczeństwa.

W zasadzie w każdym z obszarów budowy maszyny możemy mówić o optymalizacji pod względem funkcjonalności i wydajności. Na rys. 3 wyróżniono kilka obszarów:

- sygnalizowanie, informowanie i ostrzeganie,
- czujniki i urządzenia ochronne,
- elementy sterownicze i urządzenia sterujące,
- jednostka logiczna gromadząca i przetwarzająca dane,
- elementy sterowania mocą,
- elementy wykonawcze, np. siłowniki, silniki, mechanizmy robocze.

Zastosowanie odpowiednio dobranego, programowalnego panelu operatorskiego (HMI) umożliwi przygotowanie właściwej diagnostyki systemu sterowania, łącznie z częścią dotyczącą bezpieczeństwa. Łatwa i szybka diagnostyka skraca czas przestoju maszyny, a co za tym idzie – poprawia jej wydajność. Jak wiemy z praktyki, systemy sterowania odpowiedzialne za bezpieczeństwo – szczególnie te bardzo zaawansowane – są czułe na wszystko, co może powodować utratę funkcji bezpieczeństwa. Mogą wywoływać zatrzymanie maszyny, którego przyczyna nie jest łatwa do rozpoznania bez odpowiedniej diagnostyki.

Kolejnym obszarem, w którym można optymalizować system sterowania w zakresie funkcjonalności i wydajności są jednostki logiczne odpowiedzialne za wszystkie decyzje w systemie – zbierają dane z maszyny w postaci sygnałów binarnych bądź analogowych i odpowiednio je przetwarzają oraz analizują. Wybór właściwej jednostki (np. ze zintegrowaną częścią dotyczącą nadzorowania bezpieczeństwa i odpowiednimi blokami funkcyjnymi), umożliwiającej proste zaimplementowanie wymaganych dla aplikacji funkcji bezpieczeństwa, umożliwia łatwe przejście przez etap projektowania, wdrożenia i uruchomienia, a potem użytkowania i konserwacji. Użytkownik końcowy może łatwo diagnozować system, mając swobodny dostęp do niezbędnych informacji generowanych przez taką jednostkę logiczną. Mogą nią być programowalne przekaźniki bezpieczeństwa oraz sterowniki bezpieczeństwa z większymi możliwościami technicznymi (większa liczba I/O, krótsze czasy cyklu, możliwość pracy w sieci itp.).

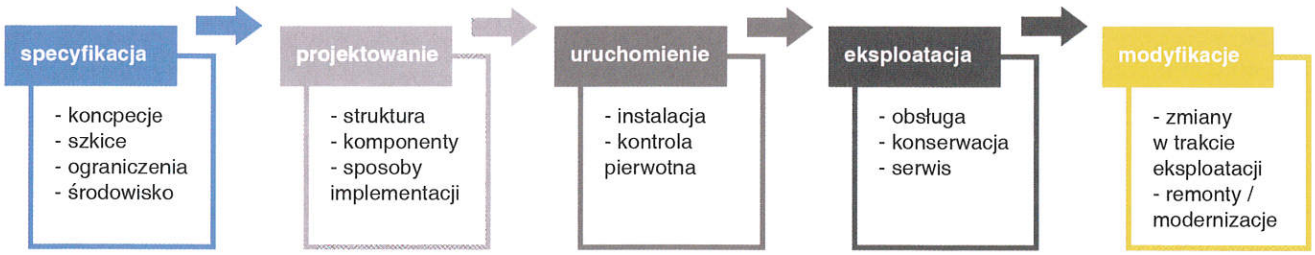
Obszar sterowania mocą, składający się np. z przekształtników zasilających silniki czy systemów serwonapędów, również może być zaprojektowany i wykonany bardziej lub mniej funkcjonalnie. Stosowanie napędów z odpowiednimi funkcjami bezpieczeństwa, takimi jak STO, SS1, SOS czy SLS, z pewnością zapewni większą funkcjonalność systemu napędowego i całego systemu sterowania – szczególnie, jeśli dla maszyny czy systemu produkcyjnego przewidujemy specjalne tryby pracy, w których konieczna jest praca przy włączonych napędach.

Przy projektowaniu systemów sterowania zawsze należy pamiętać o analizie funkcjonalności związanej ze współpracą części standardowej (technologicznej) systemu z częścią odpowiedzialną za bezpieczeństwo (SRP/SC – safety-related parts of control system).

Poprawne podejście do projektowania – fazy życia systemów sterowania

Tak jak każda z maszyn, również system sterowania ma fazy życia. Można je podzielić na specyfikację (koncepcję), projektowanie, uruchomienie, eksploatację i serwisowanie oraz modyfikacje w trakcie eksploatacji.

W pierwszej fazie należy precyzyjnie określić koncepcję systemu bezpieczeństwa, opisując wymagania funkcjonalne oraz poziomy nienaruszalno-



Rys. 4. Fazy życia systemu sterowania

ści. Należy pamiętać, iż w tej fazie nie osiągniemy pełnej identyfikacji wszystkich funkcji związanych z bezpieczeństwem – będzie to możliwe dopiero w fazie projektowania. Kluczowym zadaniem na tym etapie jest ocena ryzyka wraz z identyfikacją wszystkich zagrożeń. Celem, do jakiego powinno się dążyć w tej fazie, jest opisanie potrzebnych funkcji bezpieczeństwa oraz ich poziomów niezawodności wynikających z oceny ryzyka. Funkcje bezpieczeństwa decydują o zezwoleniu na pracę elementów niebezpiecznych i „odstawiają" maszynę w stan bezpieczny w sytuacjach zagrożenia. Pod uwagę – poza tradycyjną eksploatacją – trzeba wziąć wszystkie możliwe sposoby użytkowania maszyny, takie jak nastawianie, czyszczenie, konserwacje, serwisowanie. Wymagany poziom niezawodności danej funkcji bezpieczeństwa będzie zależał od poziomu występującego ryzyka, które musimy zredukować. Do wyznaczenia tych poziomów możemy posłużyć się grafem z normy PN-EN ISO 13849-1 (rys. 2).

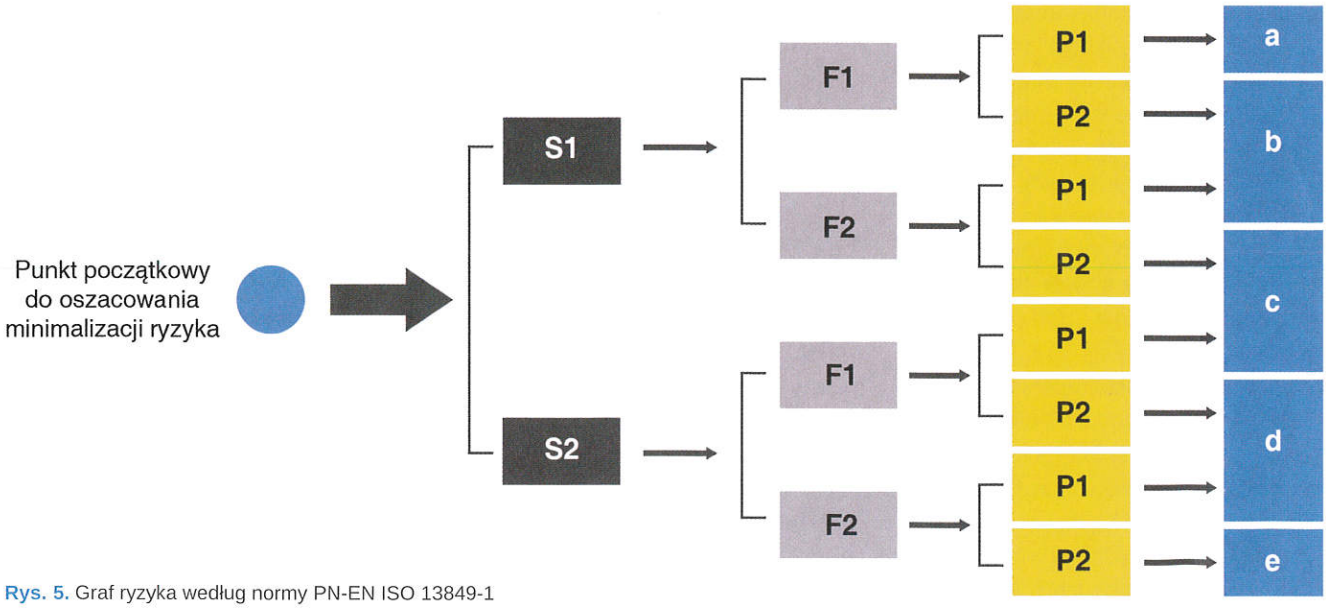
Kolejną fazą, po specyfikacji, jest projektowanie. Ten proces uszczegóławia wszystko, co zostało określone na etapie koncepcji i co wynika z przeprowadzonej oceny ryzyka oraz identyfikacji zagrożeń. Na tym etapie również możemy popełnić błędy, dlatego czasami stosuje się specjalne procedury weryfikacji i walidacji projektu, aby zminimalizować ryzyko wystąpienia błędu, szczególnie dla złożonych układów sterowania. To ostatni etap, w którym można przeanalizować funkcjonalność i wydajność systemu sterowania. Mając jasno postawiony w procesie specyfikacji cel, jakim jest osiągnięcie poziomu PL dla danej funkcji bezpieczeństwa, w procesie projektowania musimy odpowiednio dobrać wszystkie komponenty należące do łańcucha funkcji bezpieczeństwa.

Łańcuch funkcji bezpieczeństwa definiuje się jako złożenie trzech elementów: bloku wejściowego, bloku logiki i bloku wyjściowego. Każdy z nich może składać się z wielu fizycznych komponentów, jak czujniki bezpieczeństwa, kurtyny bezpieczeństwa, styczniki, elektromechaniczne przekaźniki bezpieczeństwa, programowalne przekaźniki bezpieczeństwa czy sterowniki bezpieczeństwa oraz – w obszarze wyjściowym – elektrozawory, falowniki czy jednostki mocy napędów. W języku opisowym identyfikujemy każdy z komponentów jako ogniwo łańcucha i tak je dobieramy, aby spełnić wymagania dotyczące kategorii, jakości (MTTFd) i pokrycia diagnostycznego (DC). Projektowanie i późniejsza implementacja również muszą uwzględnić pewne założenia opisane parametrem CCF, czyli odpornością na błędy o wspólnej przyczynie. Aby zapoznać się z procesem doboru i wy-

S – ciężkość urazów
S1 – lekkie (zwykle odwracalne) urazy
S2 – ciężkie (zwykle nieodwracalne) urazy z uwzględnieniem śmiertelnych

F – częstość narażenia i/lub czas jego trwania
F1 – rzadkie, do dość częstych i/lub krótki czas narażenia
F2 – częste, do ciągłych i/lub długi czas narażenia

P – możliwość przeciwdziałanie zagrożeniu
P1 – możliwe przeciwdziałanie zagrożeniu w określonych warunkach
P2 – możliwe przeciwdziałanie zagrożeniu z trudnością

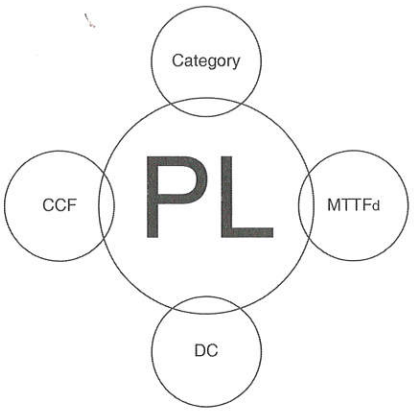


Rys. 5. Graf ryzyka według normy PN-EN ISO 13849-1

znaczania poziomu PL, należy sięgnąć do normy zharmonizowanej z dyrektywą maszynową PN-EN ISO 13849-1 (Bezpieczeństwo Maszyn. Elementy systemów sterowania związane z bezpieczeństwem. Część 1: Ogólne zasady projektowania). W bardziej złożonych układach sterowania dotyczących bezpieczeństwa stosowane są programowalne przekaźniki bezpieczeństwa lub sterowniki bezpieczeństwa. Dla takich układów niezbędna jest odpowiednia walidacja oprogramowania, również opisana w normie PN EN ISO 13849-1.

Po etapie projektowania następuje bardzo istotny etap realizacji projektu – faza instalacji i uruchomienia. Na tym etapie można popełnić wiele błędów, które mogą skutkować groźnymi wypadkami. Niezbędne jest stosowanie odpowiednich procedur, które np. za pomocą list kontrolnych weryfikują poprawność wykonania instalacji oraz zgodność z projektem. Nieodzowny jest też odpowiedni nadzór nad wykonaniem instalacji. Jednym z kluczowych elementów na etapie uruchomienia jest wykonanie testów funkcjonalnych, które powinny być precyzyjnie opracowane, tak aby umożliwiały wykrycie ewentualnych błędów popełnionych podczas procesu instalacji. Każda z czynności weryfikujących proces instalacji, jak również uruchomienia, łącznie z wykonaniem testów funkcjonalnych, powinna być oparta na stosownych dokumentach czy formularzach – zgodnie z zatwierdzonymi procedurami. Dokumenty powinny być podpisane przez osobę lub zespół, który wykonywał weryfikację i testy funkcjonalne, a następnie archiwizowane. Wszystkie zmiany w stosunku do projektu wykonawczego, jakie są wprowadzane w fazie instalacji również powinny być odpowiednio opisane, zatwierdzone i archiwizowane. Proces powinien być ponadto weryfikowany – w trakcie jego trwania – pod względem poprawności przebiegu oraz oceniany w celu ciągłego doskonalenia.

Oddanie maszyny do użytkowania oznacza przejście w fazę eksploatacji, składającej się poza klasyczną obsługą z czynności konserwacyjnych i serwisowych, należących najczęściej do służb utrzymania ruchu. W tej fazie



Rys. 6. Aspekty istotne przy wyznaczaniu poziomu PL dla funkcji bezpieczeństwa

rozpatrywane są aspekty dotyczące tylko utrzymania maszyn w ruchu – może to być prewencyjne utrzymanie ruchu lub usuwanie awarii. Aspekty związane z modyfikacjami lub innymi pracami, np. z zakresu dostosowania maszyn do nowych standardów, nie są elementem tego etapu życia systemu sterowania. Układy sterowania powinny być zaprojektowane tak, aby uwzględniały wszystkie możliwe czynności związane z konserwacją i serwisowaniem. Najbardziej narażone podczas tych prac są służby utrzymania ruchu, szczególnie kiedy działają pod presją czasu, usuwając awarie. Odpowiednie instrukcje, w których opisane są czynności, jakie należy wykonać przy usuwaniu danej awarii, wdrożenie specjalnych procedur i sprzętu zapobiegającego nieoczekiwanemu uruchomieniu maszyny podczas prac utrzymania ruchu (procedury Lock Out Tag Out) oraz stosowanie innych technik minimalizujących ryzyko pomyłki (w szczególności czytelna dokumentacja techniczna) są podstawą bezpiecznej pracy. Sterowanie powinno być odporne na możliwe do przewidzenia błędy, np. zamianę wtyczek czujników, zaworów itp.

Procesy produkcyjne mogą wymuszać dokonywanie pewnych zmian w maszynach i ich układach sterowania. Automatyzując procesy produkcyjne, łączymy maszyny w zespoły i dodajemy nowe funkcje. Czasami chęć skrócenia czasu cyklu wymusza wprowadzenie pewnych zmian w systemie sterowania. Wszystkie tego typu czynności nie są już tylko konserwacją maszyny czy jej serwisowaniem, lecz zmianami, które muszą być odpowiednio przeanalizowane, ocenione i zarejestrowane. Każda z przeprowadzonych modyfikacji musi być oceniona pod względem powstania nowych zagrożeń, a każda zmiana powinna mieć stosowną inżynierską ocenę ryzyka, której wynikiem musi być osiągnięcie ryzyka na poziomie dopuszczalnym. Często pomijany jest wpływ wprowadzonych zmian na system sterowania związany z bezpieczeństwem, co w ostateczności może prowadzić do wypadków. Dlatego przy modyfikacjach skutkujących nowymi zagrożeniami jesteśmy zobowiązani do doboru nowych, odpowiednich środków ochronnych, czyli musimy ponownie przejść fazę specyfikacji, projektowania i instalacji wraz z uruchomieniem. To również moment, w którym musimy myśleć o przyszłej funkcjonalności i wydajności systemu. Może się okazać, iż wprowadzenie zmiany w maszynie wymusi wymianę kompletnego systemu napędowego, ze względu na przyszłą funkcjonalność i wydajność. Ważne, aby jeszcze na etapie planowania i koncepcji wszystko dobrze przemyśleć i zaplanować odpowiedni budżet, który pozwoli na precyzyjną realizację zadania, czego efektem będzie bezpieczny, wydajny i funkcjonalny system sterowania.

Bezpieczeństwo, funkcjonalność i wydajność w układach sterowania maszyn osiągniemy wtedy, kiedy bardzo rzetelnie podejdziemy do każdej z faz życia systemu sterowania. Wiedza i doświadczenie inżynierów odpowiedzialnych za projektowanie i wdrażanie systemów sterowania oraz odpowiednie procedury, umożliwiające zweryfikowanie postępów prac na każdym etapie, są kluczowe w osiągnięciu celu, jakim jest wydajny i niezawodny układ sterowania.

Tomasz Otrębski

ELOKON
ul. Tytoniowa 22
04-228 Warszawa
tel. 22 812 71 38
e-mail: info@elokon.pl
www.elokon.com