Bezpieczeństwo w układach sterowania maszyn

TOMASZ OTRĘBSKI
kierownik Regionu Południe, specjalista ds. inżynierii bezpieczeństwa maszyn i procesów, Elokon Polska

Sterowanie w maszynach jest kluczowym elementem bezpieczeństwa. W zależności od poziomu zaawansowania maszyny układ sterowania może mieć znaczący wpływ na bezpieczeństwo ludzi z obsługi. Wysokie technologie i procesy przemysłowe zmuszają producentów maszyn do projektowania skomplikowanych systemów sterowania. Tylko takie zaawansowane systemy sterowania są w stanie obsłużyć technologię.

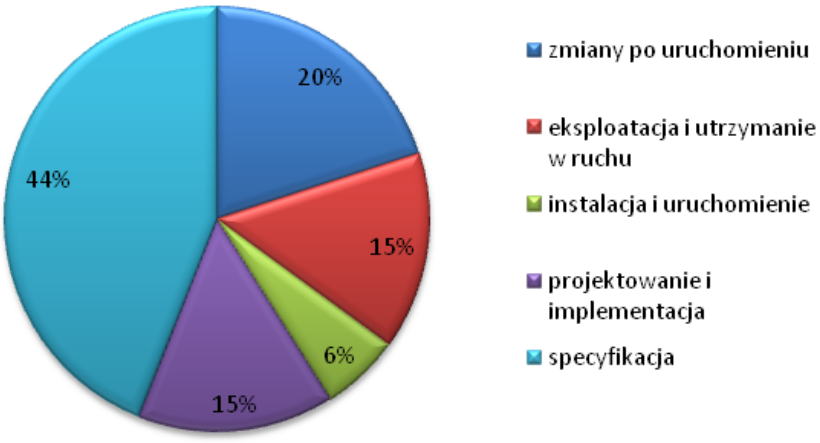
Jeżeli proces produkcyjny związany jest z dużymi energiami niszczącymi, maszyny muszą posiadać odpowiednio zaprojektowany system odpowiedzialny za bezpieczeństwo – jako część systemu sterowania maszyny. Prawo w swoich zapisach bardzo ogólnie definiuje układy sterowania odpowiedzialne za bezpieczeństwo. W obszarze eksploatacyjnym, czyli dotyczącym wszystkich użytkowników maszyn, posługujemy się dyrektywą narzędziową 2009/104/WE, która została wdrożona przez rozporządzenie Ministra Gospodarki z dnia 30 października 2002 r. w sprawie minimalnych wymagań dotyczących bezpieczeństwa i higieny pracy w zakresie użytkowania maszyn przez pracowników podczas pracy. W rozporządzeniu tym w rozdziale 3 znajdziemy tylko jeden paragraf, który mówi o układach sterownia (patrz § 11 obok).

Zapis jest bardzo ogólny i pozostawia projektantom układów sterowania otwartą drogę w kwestiach technicznych, co zmusza do posiłkowania się literaturą w zakresie projektowania bezpiecznych systemów sterowania, w tym normami opisującymi te zagadnienia. Dużą rolę w osiągnięciu celu odgrywa doświadczenie osób projektujących układy sterowania.

Wypadki a układy sterowania

Projektanci budujący maszyny powinni kierować się tzw. triadą bezpieczeństwa. W pierwszym kroku triady należy wykorzystać możliwości zbudowania maszyny w oparciu o konstrukcję bezpieczną samą w sobie – zmniejszając siły, prędkości – generalnie dążyć do zmniejszania energii niszczących. Nie jest to łatwe, dlatego najczęściej redukcję ryzyka realizuje się poprzez zastosowanie odpowiednich środków ochronnych, o których mówi drugi krok triady. Środki ochronne to m.in. urządzenia odgradzające i nieodgradzające bezpośrednio związane z systemem sterowania odpowiedzialnym za bezpieczeństwo. Ich doboru dokonuje się podczas ewaluacji ryzyka w procesie oceny ryzyka. Tylko poprawnie przeprowadzona ocena ryzyka pozwoli na właściwy dobór skutecznych środków ochronnych. Analiza wypadków wykazuje, że w większości sytuacji przyczyną były błędy, których można było uniknąć, przeprowadzając rzetelną ocenę ryzyka. Częstym błędem, który w efekcie może prowadzić do utraty bezpieczeństwa i sytuacji niebezpiecznych, włącznie z wypadkami, jest słaba ocena ryzyka, która finalnie nie pozwala dobrać skutecznego systemu sterowania odpowiedzialnego za bezpieczeństwo. Zawsze zaleca się inwestowanie w środki, które pomogą wyeliminować problemy po to, aby nie płacić za usuwanie skutków wy-

§ 11. Układy sterowania maszyn powinny zapewniać bezpieczeństwo i być dobierane z uwzględnieniem możliwych uszkodzeń, defektów oraz ograniczeń, jakie można przewidzieć w planowanych warunkach użytkowania maszyny.



Tomasz Otrębski

Absolwent Wydziału Elektrycznego Politechniki Śląskiej w Gliwicach. Zatrudniony w Elokon Polska na stanowisku kierownika Regionu Południe. Specjalista ds. inżynierii bezpieczeństwa maszyn i procesów. Ma ponad 13-letnie doświadczenie jako projektant systemów sterowania i zasilania w obszarze maszynowym, specjalista ds. automatyki, specjalista ds. bezpieczeństwa maszyn.

Rys. 1. Udział błędów powodujących niebezpieczne sytuacje w zależności od fazy życia układu sterowania

wołanych tymi problemami, co zawsze będzie droższe.

Systemy sterowania odpowiedzialne za bezpieczeństwo powinny być projektowane z należytą starannością, najlepiej pod nadzorem inżynierów doświadczonych w zakresie bezpieczeństwa maszyn, którzy są w stanie zadbać o każdy szczegół projektu. Od doboru czujników (wyposażenie ochronne), które decydują o prawidłowej aktywizacji, przez jednostki logiczne, które weryfikują stany aktywizatorów, po elementy wyjściowe i wykonawcze, jakimi są styczniki, zaawansowana elektronika w postaci np. serwozasilaczy, elektrozawory pneumatyczne lub hydrauliczne

Aby odpowiednio panować nad każdą z faz życia układu sterowania, ważny jest sposób i polityka kształtowania bezpieczeństwa w zakładzie produkcyjnym, a tym samym czynnik ludzki.

i inne urządzenia decydujące o ruchach niebezpiecznych. Każdy z elementów musi być starannie dobrany bez względu na to, czy mamy do czynienia z prostym jednokanałowym obwodem bezpieczeństwa, czy zaawansowanym programowalnym systemem. Faza projektowania powinna brać pod uwagę błędy w niedoszacowaniu niezawodności w oparciu o strukturę, błędy w doborze komponentów, które powinny być sprawdzone w technice bezpieczeństwa, brak lub nieodpowiednią walidację oprogramowania, pominięcie lub słabą analizę wpływu czynnika ludzkiego. Dobry projekt może wyeliminować lub zredukować możliwość wystąpienia błędu związanego z normalną obsługą lub konserwacją.

Pomimo dobrego projektu układ sterowania odpowiedzialny za bezpieczeństwo może zostać osłabiony poprzez stosowanie nieodpowiednich procedur związanych z wykonywaniem prac utrzymaniowo-ruchowych (konserwacje i serwisowanie) oraz prac związanych z modyfikacjami. Kluczem w tej kwestii są odpowiednie szkolenia pracowników, szczególnie tych odpowiedzialnych za konserwacje, serwisowanie i modyfikacje. Brak lub niestosowanie się do odpowiednich procedur czy słaby nadzór nad tymi procedurami mogą prowadzić do niebezpiecznych usterek układów sterowania.

Fazy życia systemów sterowania

Tak jak każda z maszyn, również system sterowania ma swoje fazy życia. Możemy je opisać w następujący sposób: specyfikacja (koncepcje), projektowanie, uruchomienie, eksploatacja i serwisowanie, modyfikacje i zmiany w trakcie eksploatacji.

Aby odpowiednio panować nad każdą z faz życia układu sterowania, ważny jest sposób i polityka kształtowania bezpieczeństwa w zakładzie produkcyjnym, a tym samym czynnik ludzki. Każda z podanych faz musi być nadzorowana poprzez odpowiednie procedury weryfikacyjne dostosowane do potrzeb danego zakładu, czyli użytkownika maszyn.

W pierwszej fazie należy precyzyjnie rozpisać koncepcję systemu bezpieczeństwa, opisując wymagania funkcjonalne oraz poziomy nienaruszalności. Należy pamiętać, że w tej fazie nie osiągniemy pełnej identyfikacji wszystkich funkcji związanych z bezpieczeństwem, co będzie możliwe dopiero w fazie projektowania. Kluczowym zada-

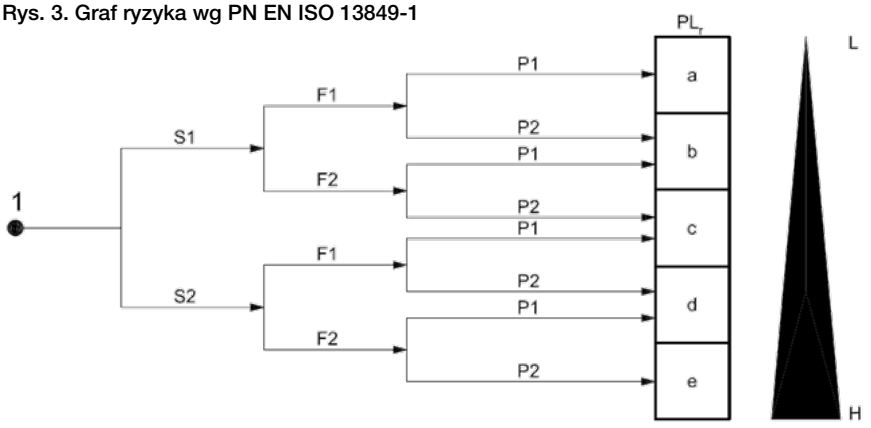
Rys. 2. Fazy życia systemu sterowania

niem w tej fazie jest ocena ryzyka wraz z identyfikacją wszystkich zagrożeń. Celem, do jakiego powinniśmy dążyć na tym etapie, 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. Specyfikując, musimy brać pod uwagę – poza normalna eksploatacją – wszystkie możliwe sposoby użytkowania maszyny, takie jak nastawianie, czyszczenie, konserwacje, serwisowanie. Wymagany poziom niezawodność 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. 3).

Kolejną fazą po specyfikowaniu jest projektowanie. Ten proces uszczegóławia wszystko to, co zostało zebrane na etapie koncepcyjnym i co wynika z przeprowadzonej oceny ryzyka oraz identyfikacji zagrożeń. Na tym etapie również możemy popełnić błędy i dlatego czasami stosuje się specjalne procedury weryfikacji i walidacji projektu, aby zminimalizować możliwość popełnienia błędu, szczególnie dla złożonych układów sterowania. Mając jasno postawiony w procesie specyfikacji cel, jakim jest poziom PL dla danej funkcji bezpieczeństwa, w procesie projektowania musimy odpowiednio dobrać wszystkie komponenty należące do łańcucha funkcji bezpieczeństwa. Ogólnie łańcuch funkcji bezpieczeństwa definiuje się jako złożenie trzech elementów: bloku wejściowego, bloku logiki i bloku wyjściowego. Każdy z tych bloków może składać się z wielu fizycznych komponentów, jak czujniki bezpieczeństwa, kurtyny bezpieczeństwa, styczniki, elektromechaniczne przekaźniki bezpieczeństwa, programowalne przekaźniki bezpieczeństwa czy też sterowniki bezpieczeństwa oraz w obszarze wyjściowym elektrozawory, falowniki czy jednostki mocy napędów. W języku opisowym identyfikujemy każdy z komponentów jako ogniwo naszego łańcucha i tak dobieramy, aby spełnić wymagania związane z kategorią, jakością (MTTFd) i pokryciem diagnostycznym (DC). Rzetelność procesu projektowania i późniejszej implementacji również musi spełnić pewne założenia opisane parametrem CCF, czyli odpornością na błędy o wspólnej przyczynie. Aby zapoznać się z procesem doboru i wyznaczania poziomu PL, odsyłam 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 związanych z bezpieczeństwem stosowane są programowalne przekaźniki bezpieczeństwa lub sterowniki bezpieczeństwa. Dla takich układów niezbędna będzie odpowiednia walidacja oprogramowania również opisana w normie PN EN ISO 13849-1.

Po etapie projektowania następuje faza instalacji i uruchomienia. Jest to bardzo istotny etap realizacji całego projektu. Można tu popełnić wiele błędów, które

Rys. 3. Graf ryzyka wg PN EN ISO 13849-1



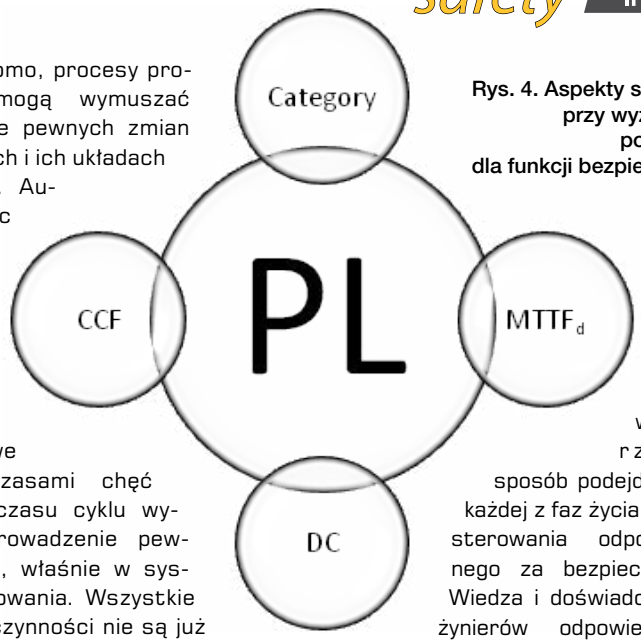
S – ciężkość urazów
S1 – lekkie (zwykle odwracalne) urazy
S2 – ciężkie (zwykle nieodwracalne) urazy z uwzględnieniem śmiertelnych

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 przeciwdziałania zagrożeniu
P1 – możliwe w określonych warunkach
P2 – możliwe z trudnością

mogą skutkować groźnymi wypadkami. Niezbędne jest stosowanie odpowiednich procedur, które za pomocą np. list kontrolnych, weryfikują poprawność wykonania instalacji oraz zgodność z projektem. Nieodzowny jest odpowiedni nadzór nad wykonaniem instalacji. Jednym z kluczowych elementów już 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 zarówno proces instalacji, jak również uruchomienia włącznie z wykonaniem testów funkcjonalnych powinna być oparta o stosowne dokumenty czy formularze zgodnie z zatwierdzonymi procedurami. Dokumenty takie powinny być podpisane przez osobę lub zespół, który wykonywał weryfikację i testy funkcjonalne, a następnie archiwizowane. Wszystkie zmiany w stosunku do projektu wykonawczego, jakie wprowadza się w fazie instalacji, również powinny być odpowiednio opisane, zatwierdzone i archiwizowane. Cały ten proces powinien być weryfikowany pod względem poprawności przebiegu – w trakcie jego trwania – oraz oceniany w celu ciągłego doskonalenia.

Oddanie maszyny do użytkowania oznacza przejście w fazę normalnej eksploatacji składającej się – poza normalną obsługą – z czynności konserwacyjnych i serwisowych, należących najczęściej do służb utrzymania ruchu. W tej fazie rozpatrujemy aspekty związane tylko z utrzymaniem maszyn w ruchu, może to być prewencyjne utrzymanie ruchu lub usuwanie awarii. Aspekty dotyczące modyfikacji lub innych prac, np. dostosowania maszyn do nowych standardów, nie zawierają się w tym etapie życia systemu sterowania. Układy sterowania powinien być tak zaprojektowany, aby uwzględniał wszystkie możliwe czynności związane z konserwacją i serwisowaniem. Służby utrzymania ruchu są najbardziej narażone podczas tych prac, szczególnie, kiedy usuwając awarie, działają pod presją czasu. Odpowiednie instrukcje, w których opisuje się czynności, jakie należy wykonać, eliminując daną awarię, stosowanie specjalnych procedur i sprzętu zapobiegającego nieoczekiwanemu uruchomieniu maszyny podczas prac utrzymania ruchu (procedury *lock out tag out*) oraz stosowanie innych technik minimalizujących 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.



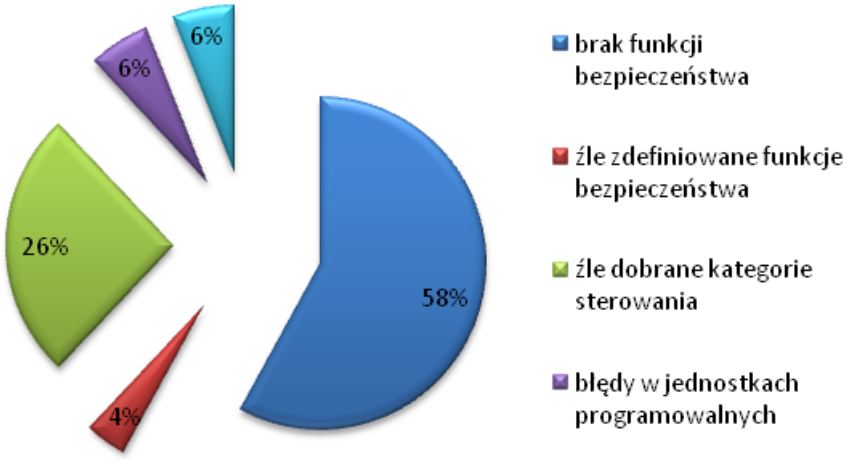
Rys. 4. Aspekty skojarzone przy wyznaczaniu poziomu PL dla funkcji bezpieczeństwa

Jak wiadomo, procesy produkcyjne mogą wymuszać dokonywanie pewnych zmian w maszynach i ich układach sterowania. Automatyzując procesy produkcyjne, łączymy maszyny w zespoły, dodajemy nowe funkcje. Czasami chęć skrócenia czasu cyklu wymusza wprowadzenie pewnych zmian, właśnie w systemie sterowania. Wszystkie tego typu czynności nie są już tylko konserwacją maszyny czy jej serwisowaniem, są zmianami, które muszą być odpowiednio analizowane, oceniane i rejestrowane. Każda z przeprowadzonych modyfikacji musi być oceniona pod względem powstawania nowych zagrożeń. Każda zmiana powinna posiadać 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. Tak naprawdę przy modyfikacjach, które wprowadzają nowe zagrożenia, jesteśmy zobowiązani do doboru nowych, odpowiednich środków ochronnych, czyli musimy przejść fazę specyfikacji, projektowania i instalacji wraz z uruchomieniem.

Bezpieczeństwo w układach sterowania maszyn osiągniemy wtedy, kiedy w bardzo rzetelny sposób podejdziemy do każdej z faz życia systemu sterowania odpowiedzialnego za bezpieczeństwo. Wiedza i doświadczenie inżynierów odpowiedzialnych za projektowanie i wdrażanie systemów bezpieczeństwa oraz odpowiednie procedury pozwalające zweryfikować postępy prac na każdym etapie są kluczowe w osiągnięciu celu, jakim jest niezawodny układ sterowania. Przeprowadzenie poprawnej walidacji hardware'u i software'u pozwala wykryć błędy w fazie projektowania lub instalacji i uruchomienia.

Wyszkolone i doświadczone służby utrzymania ruchu, pracujące zgodnie z wypracowanymi procedurami dotyczącymi procesów oceny ryzyka, identyfikacji zagrożeń, dokumentowania zmian w dokumentacji, minimalizują popełnienie błędu.

W każdej fazie życia systemu sterowania potrzebujemy zespołu specjalistów, którzy mogą pracować w oparciu o przemyślane procedury i tylko w taki sposób jesteśmy w stanie osiągnąć cel – zapewnić bezpieczeństwo.



Ryc. 5. Częstość występowania różnych przyczyn wypadków związanych z układami sterowania