Bezpieczeństwo w układach sterowania maszyn

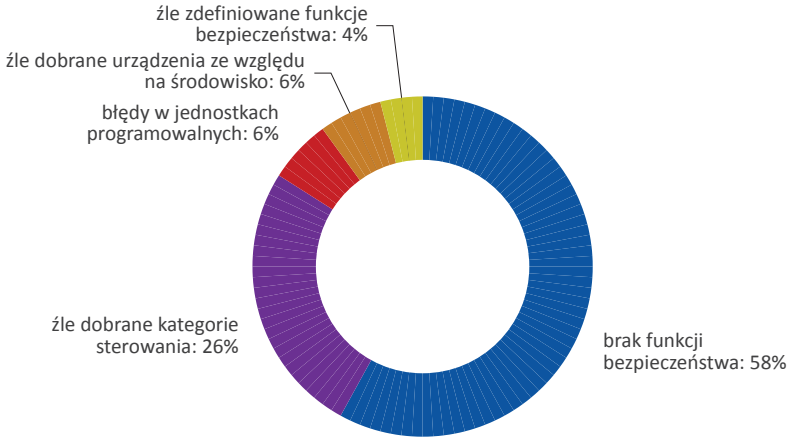
W zależności od poziomu zaawansowania maszyny układ sterowania może mieć znaczący wpływ na bezpieczeństwo obsługujących je pracowników.

Tomasz Otrębski

Zaawansowane technologie i procesy przemysłowe zmuszają producentów maszyn do projektowania skomplikowanych systemów sterowania. Tylko takie zaawansowane systemy są w stanie obsłużyć takie maszyny i zapewnić ich sprawne i efektywne funkcjonowanie.

Jeżeli proces produkcyjny jest dodatkowo związany z występowaniem dużych energii niszczących, dynamicznych procesów z obsługą znacznych momentów sił itp., maszyny muszą mieć odpowiednio zaprojektowany system odpowiedzialny za bezpieczeństwo, będący integralną częścią systemu sterowania maszyny.

Rys. 1. Częstość występowania różnych przyczyn wypadków związanych z układami sterowania



Źródło: archiwum autora

Projektowanie układów sterowania według przepisów

Prawo w swoich zapisach bardzo ogólnie definiuje układy sterowania odpowiedzialne za bezpieczeństwo. W obszarze eksploatacyjnym, czyli dotyczącym użytkowników maszyn, należy posługiwać 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 znajduje się tylko jeden paragraf dotyczący układów sterowania:

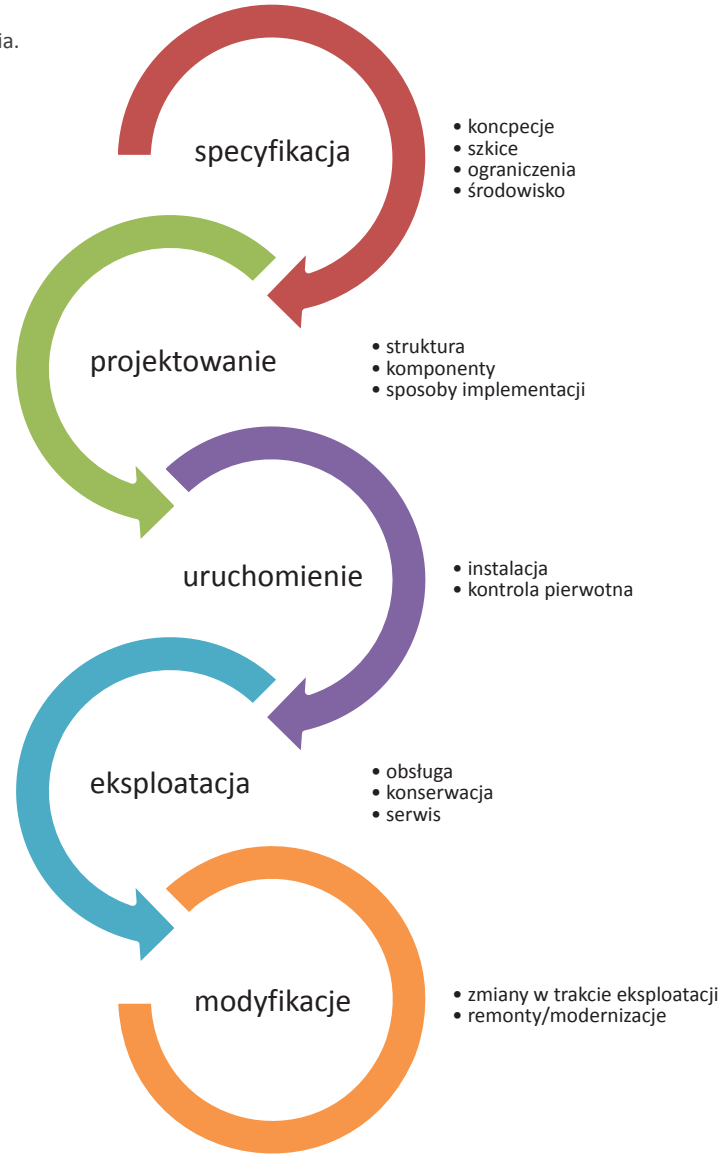
„§ 11. Układy sterowania maszyn powinny zapewniać bezpieczeństwo i być dobierane z uwzględnianiem możliwych uszkodzeń, defektów oraz ograniczeń, jakie można przewidzieć w planowanych warunkach użytkowania maszyny".

Zapis ten jest bardzo ogólny i pozostawia projektantom układów sterowania otwarte pole do działania 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 zatem doświadczenie osób projektujących układy sterowania.

Wypadki a układy sterowania

Projektanci budujący maszyny powinni się kierować tzw. triadą bezpieczeństwa. W pierwszym kroku triady należy wykorzystać możliwość zbudowania maszyny w oparciu o konstrukcję bezpieczną samą w sobie – zmniejszając siły, prędkości – generalnie dążyć do zmniejszania wartości wspomnianych energii niszczących.

Nie jest to łatwe, dlatego najczęściej redukcję ryzyka realizuje się przez zastosowanie odpowiednich środków ochronnych, o których mówi drugi krok triady. Środki ochronne to m.in. urządzenia odgradzające i nieodgradzające, bezpośrednio związane z systemem sterowania



Rys. 2. Fazy życia systemu sterowania. Źródło: archiwum autora

odpowiedzialnym za bezpieczeństwo. Ich doboru dokonuje się podczas ewaluacji ryzyka w procesie jego oceny i analizy. Tylko poprawnie przeprowadzona ocena ryzyka pozwala na właściwy dobór skutecznych środków ochronnych.

Analiza wypadków w przemyśle wykazuje, że w większości ich przyczyną były błędy, których można było uniknąć po dokonaniu rzetelnej oceny ryzyka. Słaba ocena ryzyka poza tym, że prowadzi do utraty bezpieczeństwa i powstawania sytuacji niebezpiecznych, z wypadkami włącznie, nie pozwala dobrać skutecznego systemu sterowania odpowiedzialnego za bezpieczeństwo. Zaleca się zawsze inwestowanie w środki, które pomogą wyeliminować problemy, po to, by uniknąć kosztów usuwania skutków tych problemów.

Systemy sterowania odpowiedzialne za bezpieczeństwo powinny być projektowane z należytą starannością, najlepiej pod nadzorem inżynierów, którzy mają już doświadczenie w zakresie bezpieczeństwa maszyn i 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 takich urządzeń, jak np. serwonapędy, elektrozawory pneumatyczne lub hydrauliczne i inne urządzenia decydujące o ruchach maszyn, również tych niebezpiecznych. Każdy z elementów musi być starannie dobrany bez względu na to, czy chodzi o prosty jednokanałowy obwód bezpieczeństwa, czy zaawansowany programowalny system. Faza projektowania powinna uwzględniać 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.

Częstość występowania przyczyn wypadków związanych z układami sterowania przedstawiono na **rys. 1**.

Pomimo dobrego projektu układ sterowania odpowiedzialny za bezpieczeństwo może zostać osłabiony przez stosowanie nieodpowiednich procedur związanych z wykonywaniem prac w utrzymaniu ruchu (konserwacje i serwisowanie) oraz prac związanych z modyfikacjami. Kluczowym elementem są odpowiednie szkolenia pracowników, szczególnie tych odpowiedzialnych za konserwacje, serwisowanie i modyfikacje. Brak lub niestosowanie się do odpowiednich procedur i słaby nadzór nad tymi procedurami może prowadzić do niebezpiecznych usterek układów sterowania.

Fazy życia systemów sterowania

Tak jak każda z maszyn, również system sterowania ma swoje fazy życia. Można je opisać w następujący sposób: specyfikacja (koncepcje), projektowanie, uruchomienie, eksploatacja i serwisowanie, modyfikacje i zmiany w trakcie eksploatacji. Przedstawiono je na **rys. 2**, natomiast **rys. 3** ilustruje udział błędów powodujących niebezpieczne sytuacje w poszczególnych fazach życia układu sterowania.

Aby odpowiednio panować nad każdą z faz życia układu sterowania, należy położyć nacisk na sposób i politykę kształtowania bezpieczeństwa z 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.

Specyfikacja

W pierwszej fazie należy precyzyjnie opisać koncepcję systemu bezpieczeństwa, koncentrując się na wymaganiach funkcjonalnych oraz poziomach nienaruszalności bezpieczeństwa – tych wynikających z normy PN-EN 61508, w odniesieniu do elektrycznych, elektronicznych i programowalnych rozwiązań służących poprawie bezpieczeństwa. Należy pamiętać, że w tej fazie nie można osiągnąć pełnej identyfikacji wszystkich funkcji związanych z bezpieczeństwem – będzie to możliwe dopiero w fazie projektowania. Najważniejszym zadaniem w tej fazie jest ocena ryzyka wraz z identyfikacją wszystkich zagrożeń. Celem, do jakiego trzeba 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. Dokonując specyfikacji, należy brać pod uwagę – poza normalną eksploatacją – wszystkie możliwe sposoby użytkowania maszyny, takie jak nastawianie, czyszczenie, konserwacje, serwisowanie. Wymagany poziom niezawodności danej funkcji bezpieczeństwa będzie zależał od poziomu występującego ryzyka, które należy zredukować. Do wyznaczenia tych poziomów można posłużyć się grafem z normy PN-EN ISO 13849-1 (**rys. 4**).

Projektowanie

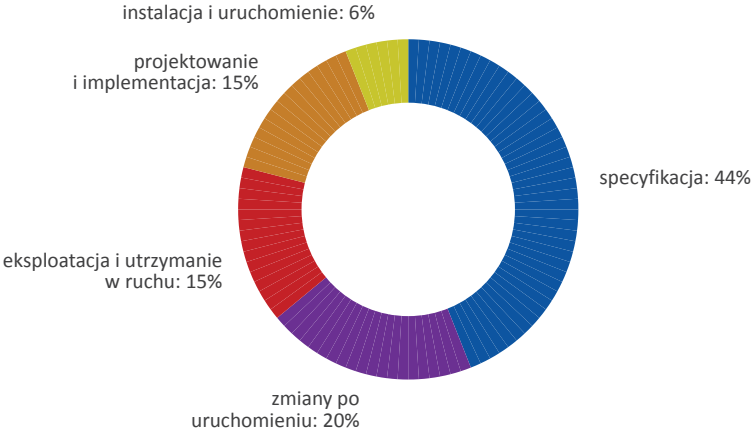
Kolejną fazą jest projektowanie. Ten proces uszczegóławia wszystko to, co zostało zebrane na etapie koncepcyjnym i co wynika z przeprowadzonej oceny ryzyka oraz identyfikacji zagrożeń. Na tym etapie również można popełnić błędy i dlatego czasami stosuje się specjalne procedury weryfikacji i walidacji projektu, aby zminimalizować to ryzyko, szczególnie w odniesieniu do złożonych układów sterowania. Mając jasno postawiony w procesie specyfikacji cel, jakim jest poziom PL dla danej funkcji bezpieczeństwa, w procesie projektowania trzeba odpowiednio dobrać wszystkie komponenty należące do łańcucha funkcji bezpieczeństwa (**rys. 5**). Poziom PL, zdefiniowany w normie PN-EN ISO 13849-1, to miara niezawodności funkcji bezpieczeństwa, czyli poziom zapewnienia bezpieczeństwa lub poziom działania. PL dzieli się na pięć poziomów (a–e). PL e oznacza najlepszą niezawodność i jest równoznaczny z wymaganym przy najwyższym poziomie zagrożenia.

Ogólnie łańcuch funkcji bezpieczeństwa definiuje się jako złożenie trzech elementów: bloku wejściowego, bloku logiki i bloku wyjściowego. Każdy z tych bloków może się składać z wielu fizycznych komponentów, takich 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 identyfikuje się każdy z tych komponentów jako ogniwo łańcucha i tak dobiera, aby spełnić wymagania związane z kategorią, jakością (MTTFd) i pokryciem diagnostycznym (DC). Rzetelność procesu projektowania i późniejszej implementacji również wymaga spełnienia pewnych założeń opisanych parametrem CCF, czyli odpornością na błędy o wspólnej przyczynie. Proces doboru i wyznaczania poziomu PL opisany został w normie zharmonizowanej z dyrektywą maszynową PN-EN ISO 13849-1. 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.

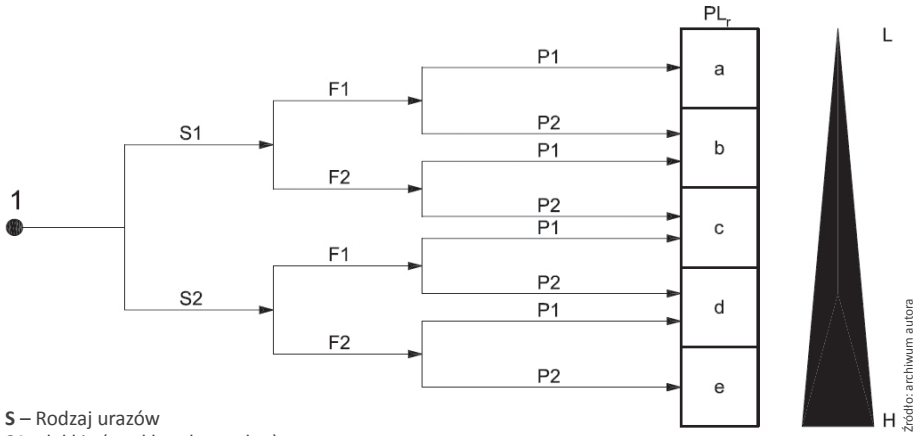
Uruchomienie

Po etapie projektowania następuje faza instalacji i uruchomienia. Jest to bardzo istotny etap realizacji projektu. W tej fazie można popełnić wiele błędów, które 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 instalacj, jak i uruchomienia, włącznie z wykonaniem testów funkcjonalnych, powinna być oparta na stosownych dokumentach czy formularzach, 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,

Rys. 3. Udział błędów powodujących niebezpieczne sytuacje w zależności od fazy życia układu sterowania



Źródło: archiwum autora



S – Rodzaj 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

↗ **Rys. 4.** Graf ryzyka według normy PN-EN ISO 13849-1.

zatwierdzone i archiwizowane. Cały ten proces powinien być dodatkowo weryfikowany pod względem poprawności przebiegu – w czasie jego trwania – oraz oceniany w celu ciągłego doskonalenia.

Eksploatacja
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 rozpatruje się aspekty związane tylko z utrzymaniem maszyn w ruchu – może to być prewencyjne utrzymanie ruchu lub usuwanie awarii. Aspekty związane z modyfikacjami lub innymi pracami związanymi z np. dostosowaniem maszyn do nowych standardów, nie zawierają się w tym etapie życia systemu sterowania.

Układy sterowania powinny być tak zaprojektowane, aby uwzględniały wszystkie możliwe czynności związane z konserwacją i serwisowaniem. Służby UR są najbardziej narażone podczas tych prac, szczególnie kiedy działają pod presją czasu, usuwając awarie. Podstawą bezpiecznej pracy są: odpowiednie instrukcje, w których opisuje się czynności, jakie należy wykonać, usuwając daną awarię, stosowanie specjalnych procedur i sprzętu zapobiegającego nieoczekiwanemu uruchomieniu maszyny podczas prac w utrzymaniu ruchu (procedury lockout/tagout) oraz stosowanie innych technik minimalizujących pomyłki, w szczególności dbanie o czytelność dokumentacji technicznej. Sterowanie powinno być odporne na możliwe do przewidzenia błędy, np. zamianę wtyczek czujników, zaworów itp.

Modyfikacje
Procesy produkcyjne mogą wymuszać dokonywanie pewnych zmian w maszynach i ich układach sterowania. Dokonując automatyzacji procesów produkcyjnych, łączy się maszyny w zespoły, dodaje nowe funkcje. Czasami dążenie do 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 mieć stosowną inżynierską ocenę ryzyka, której wynikiem musi być zapewnienie dopuszczalnego poziomu ryzyka.

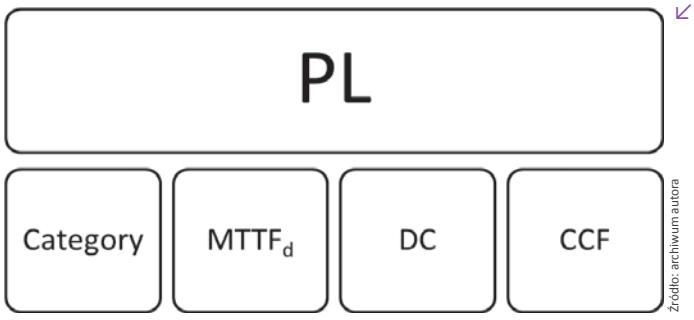
Przy modyfikacjach, które wprowadzają nowe zagrożenia, należy dobrać odpowiednie środki ochronne, czyli przejść fazę specyfikacji, projektowania i instalacji wraz z uruchomieniem.

Podsumowanie

Bezpieczeństwo w układach sterowania maszyn można osiągnąć pod warunkiem, że w bardzo rzetelny sposób podejdzie się do każdej z faz życia systemu sterowania. 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 sprzętu i oprogramowania 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, minimalizują ryzyko popełnienia błędu.

W każdej fazie życia systemu sterowania potrzebny jest zespół specjalistów, którzy mogą pracować w oparciu o prze-



↙ **Rys. 5.** Aspekty skojarzone przy wyznaczaniu poziomu PL dla funkcji bezpieczeństwa.

myślane procedury. Tylko w taki sposób można osiągnąć cel, jakim jest zapewnienie bezpieczeństwa.

Tomasz Otrębski zatrudniony jest w Elokon Polska na stanowisku kierownika Regionu Południe. Jest specjalistą 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. Trener i wykładowca od 2003 r. Prowadzi szkolenia z budowy systemów sterowania oraz z systemów sterowania związanych z bezpieczeństwem.

Online

Więcej artykułów na temat bezpieczeństwa w produkcji znajdą Państwo na naszej stronie internetowej w zakładce „Bezpieczeństwo”: **www.utrzymanieruchu.pl**

Literatura

1. Dyrektywa Parlamentu Europejskiego i Rady 2009/104/WE z dnia 16 września 2009 r. dotycząca minimalnych wymagań w dziedzinie bezpieczeństwa i higieny użytkowania sprzętu roboczego przez pracowników podczas pracy (druga dyrektywa szczegółowa w rozumieniu art. 16 ust. 1. dyrektywy 89/391/EWG) (Dz.Urz. L 260 z 3.10.2009 r., s. 5–19).
2. 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 (Dz.U. z 2002 nr 191, poz. 1596, ze zm.).
3. Health and Safety Executive, „Out of control. Why control systems go wrong and how to prevent failure”, Sudbury 2003.
4. M. Dźwiarek, „An Analysis of Accidents Caused by Improper Functioning of Machine Control Systems”, „International Journal of Occupational Safety and Ergonomics”, 2004, Vol. 10, No. 2, pp. 129–136.
5. PN-EN 61508, „Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem”.
6. PN-EN ISO 13849-1, „Bezpieczeństwo Maszyn. Elementy systemów sterowania związane z bezpieczeństwem. Część 1: Ogólne zasady projektowania”.