dr inż. Marek Dźwiarek
Centralny Instytut Ochrony Pracy

Aspekty bezpieczeństwa funkcjonalnego złożonych systemów sterowania maszyn

Obecnie możemy zaobserwować gwałtowny wzrost zastosowań złożonych systemów elektronicznych na wszystkich poziomach złożoności maszyn. W przypadku urządzeń realizujących funkcje bezpieczeństwa szczególnie ważne jest ich zachowanie w warunkach defektu. Wiele instytutów i ośrodków naukowych prowadzi prace badawcze zmierzające do upowszechnienia nowoczesnych metod projektowania z wykorzystaniem najnowszych technologii, które umożliwiają realizowanie funkcji bezpieczeństwa w bardziej efektywny sposób. Szczególne znaczenie ma wymiana informacji oraz harmonizacja procedur badań i oceny urządzeń.

Functional safety of complex control system of machinery

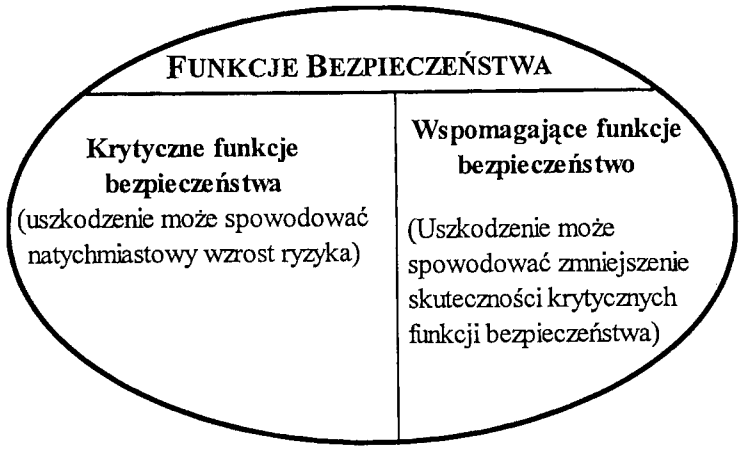
Nowadays there is a progress in the use of complex electronic systems at all levels of machine complexity. When we deal with devices performing safety functions, their behaviour under fault conditions is very important. Many research institutions carry out research programs to stimulate new designs employing advanced technology and engineering which will carry out protective functions in a more efficient way. Exchanging the results and harmonising the assessment procedures between different organisations and countries is of crucial importance.

1. WPROWADZENIE

Nowoczesne technologie umożliwiają konstruowanie coraz bardziej wydajnych i wielozadaniowych maszyn. Zwłaszcza komputery i złożone układy elektroniczne zastosowane do realizacji funkcji bezpieczeństwa umożliwiły znaczny wzrost skuteczności urządzeń ochronnych i systemów sterowania maszyn, zmniejszając jednocześnie ich koszt. Obecnie możemy zaobserwować gwałtowny wzrost zastosowań złożonych systemów elektronicznych na wszystkich poziomach złożoności maszyn, począwszy od prostych systemów wentylacji do najnowocześniejszych instalacji takich jak zautomatyzowane linie produkcji samochodów.

Zazwyczaj system sterowania maszyny realizuje zarówno funkcje bezpieczeństwa, jak i funkcje nie wpływające na bezpieczeństwo. Funkcje bezpieczeństwa są to funkcje których uszkodzenie może spowodować wzrost poziomu ryzyka. Z punktu widzenia bezpieczeństwa najlepsze są rozwiązania w których urządzenia ochronne są, w miarę możliwości, odseparowane od pozostałych układów systemu i połączone bezpośrednio z urządzeniami zasilającymi. Umożliwiają one zredukowanie wielkości i złożoności urządzeń bezpieczeństwa. Jednocześnie tworzą one bardziej logiczną strukturę. Jednak, w praktyce, nie

zawsze rozwiązania takie są możliwe i układy funkcjonalne zaangażowane są jednocześnie w realizację funkcji bezpieczeństwa.



Rys. 1. Podział funkcji bezpieczeństwa.

Funkcje bezpieczeństwa dzielimy na krytyczne funkcje bezpieczeństwa i wspomagające funkcje bezpieczeństwo (patrz rys. 1). Funkcje wspomagające bezpieczeństwo są to funkcje, których uszkodzenie nie powoduje natychmiastowego wzrostu poziomu ryzyka. Przykładem takiej funkcji jest automatyczne monitorowanie poprawności pracy czujnika położenia współpracującego z urządzeniem blokującym. Uszkodzenie funkcji wspomagających bezpieczeństwo może powodować zmniejszenie skuteczności realizacji funkcji krytycznych dla bezpieczeństwa.

Krytyczne funkcje bezpieczeństwa są to funkcje których uszkodzenie może powodować natychmiastowy wzrost poziomu ryzyka. Przykładem jest funkcja zatrzymania generowana przez elektroczułe urządzenie ochronne w reakcji na naruszenie strefy czułości. Funkcja taka jest implementowana do systemu jedynie ze względów bezpieczeństwa i nie uczestniczy w normalnej pracy maszyny.

Analizy wypadków spowodowanych przez niewłaściwe funkcjonowanie systemów sterowania prowadzone w Wielkiej Brytanii wykazały, że przyczyną znaczącej ich liczby były błędy popełnione podczas projektowania maszyny. Zazwyczaj błędy projektanta, których skutkiem jest niewłaściwa realizacja zakładanych funkcji ujawniają się jedynie w szczególnych warunkach, znacznie różniących się od typowych warunków pracy urządzenia. Przypadki takie są szczególnie niebezpieczne, ponieważ wpływają zarówno na nieprzewidywalne działanie urządzenia, jak i nietypowe zachowanie operatora. Sytuacjom takim nie można zapobiec poprzez stosowanie środków bezpieczeństwa na stanowisku pracy. Jedyną skuteczną metodą jest zapewnienie, że podczas procesu projektowania nie popełniono żadnych błędów oraz że zastosowano właściwe rozwiązania konstrukcyjne.

2. RODZAJE DEFEKTÓW

W przypadku urządzeń realizujących funkcje bezpieczeństwa szczególnie ważne jest ich zachowanie w warunkach defektu. System sterowania maszyny powinien być zaprojektowany tak, aby uszkodzenie obwodów elektronicznych lub ich zniszczenie nie powodowało sytuacji

niebezpiecznych [2]. Oznacza to, że podczas projektowania urządzenia uwzględnić należy wpływ uszkodzeń na działanie systemu, a projektant powinien zastosować odpowiednie środki zapobiegające wprowadzeniu sytuacji niebezpiecznych. Projektant systemu sterowania powinien zrealizować dwa cele:

- zaprojektować system który umożliwi realizowanie zadań funkcjonalnych maszyny, uwzględniając przy tym kwestie bezpieczeństwa,
- zaprojektować system który będzie realizował swoje funkcje w warunkach uszkodzenia w sposób przewidywalny, na określonym poziomie niezawodności, w całym cyklu życia maszyny.

Obecnie dostępne są podstawowe informacje pomocne projektantowi w osiągnięciu pierwszego celu, n.p PN-EN 292, PN-EN 1050 itp. Natomiast bardzo mało jest użytecznych informacji, które byłyby pomocne w realizacji celu drugiego.

Defekty można klasyfikować na różne sposoby. Podstawowym jest podział w zależności od ich przyczyn. Możemy wyróżnić dwie główne grupy defektów: przypadkowe i systematyczne. Defekty przypadkowe występują w przypadkowych chwilach czasu w związku ze zużywaniem lub psuciem się elementów wyposażenia. Złożone układy elektroniczne zawierają wiele elementów i podzespołów połączonych elektrycznie lub mechanicznie. Każdy podzespół wyposażenia charakteryzuje się inną niezawodnością, zależną od technologii wykonania, materiału oraz częstotliwości pracy. Określenie prawdopodobieństwa uszkodzenia takiego systemu jest możliwe, ale niezwykle trudne. Także szczegółowa analiza i symulacja wszystkich przewidywanych defektów może być praktycznie niemożliwa. Tak więc zapobieganie defektom powinno być realizowane poprzez stosowanie odpowiedniej architektury systemu.

Defekty systematyczne związane są z błędem człowieka (zarówno związanych z niewłaściwym działaniem, jak i z zaniechaniem działania) popełnionym w dowolnym etapie cyklu życia urządzenia. Powodują one wystąpienie sytuacji niebezpiecznych po wystąpieniu określonej kombinacji warunków zewnętrznych.

Podstawowymi przyczynami powstawania defektów systematycznych są:

- błędy specyfikacji – obejmują one pomyłki lub przeoczenia popełnione podczas analizy zagrożeń, oceny ryzyka, formułowania wymagań bezpieczeństwa, przygotowywania procesu projektowania, a także opracowywania planu walidacji.
- defekty wyposażenia – mogą powstać na dowolnym etapie projektowania, konstruowania, instalowania lub stosowania urządzenia. Obejmują one niewłaściwe projektowanie, zastosowanie nieodpowiednich elementów lub podzespołów, niedotrzymanie wymogów systemu jakości produkcji, stosowanie urządzenia niezgodnie z instrukcją itp.
- defekty oprogramowania – występują w związku z niewłaściwym sformułowaniem programu w fazie projektowania lub zastosowaniu sprzętu nieodpowiedniego do programu, ale mogą także być wprowadzone podczas późniejszych modyfikacji programu.

Ponieważ defekty systematyczne wprowadzają nieprzewidywalne właściwości systemu, nie jest możliwe do przewidzenia jak często będą one powodować niebezpieczne sytuacje. W odróżnieniu od uszkodzeń przypadkowych, metody symulacyjne przeważnie nie wystarczają do wykrycia defektów systematycznych. Tak więc podstawową metodą zapobiegania defektom systematycznym jest stosowanie odpowiedniego systemu jakości projektowania.

Ważnym źródłem defektów są uszkodzenia od wspólnej przyczyny (common case faults CCF). Są to jednoczesne uszkodzenia dwu lub więcej kanałów redundancji spowodowane tymi samymi przyczynami, np. wpływami środowiskowymi lub błędami projektanta. CCF zaliczamy do defektów systematycznych. Występowanie takich defektów ma istotne

znaczenie, gdyż nie znamy prostych sposobów zapobiegania im. Defekty te powodują obniżenie poziomu nienaruszalności bezpieczeństwa urządzeń ochronnych, także w przypadku redundancji wielokanałowej, zwłaszcza jeśli zastosowano identyczne układy w kilku gałęziach redundancji. Ich wpływ zależy od architektury systemu oraz od liczby realizowanych funkcji bezpieczeństwa. CCF występują zarówno w oprogramowaniu, jak i w sprzęcie. Jedną z metod zapobiegania im jest stosowanie w poszczególnych gałęziach redundancji różnych układów, wykonanych w różnych technologiach. Metoda ta może być także skuteczna w przypadku defektów oprogramowania.

3. ZAPOBIEGANIE DEFEKTOM.

W przypadku prostych systemów sterowania, wykonanych z użyciem technologii klasycznych, n.p. zbudowanych z prostych elementów i podzespołów elektrycznych, mechanicznych lub pneumatycznych, możliwa jest analiza wszystkich możliwych uszkodzeń oraz określenie ich skutków i reakcji maszyny. Metody analizy, a także rodzaje możliwych uszkodzeń rożnych elementów i podzespołów są dobrze znane. Najczęściej stosowane są metody FMEA lub FTA. Projektant systemu, dysponując skutecznymi metodami analizy konstruowanego urządzenia, może jednoznacznie określić jego zachowanie we wszystkich możliwych sytuacjach, a tym samym być pewnym poprawności projektu. Norma PN-EN 954-1 wprowadza behawioralną klasyfikację związanych z bezpieczeństwem elementów systemów sterowania maszyn [3]. Opiera się ona na tym, że różne urządzenia mogą pracować przy różnych poziomach ryzyka. PN-EN 954-1 dzieli urządzenia na 5 kategorii, w zależności od ich zachowania się w warunkach defektu. Podział ten jest niezależny od zastosowanej technologii, a zależy jedynie od odporności urządzenia na defekty, która określona jest przez strukturę urządzenia i jego niezawodność [7].

Do podstawowej kategorii B zaliczane są urządzenia wykonane odpowiednio do przewidywanego środowiska pracy, zgodnie z zaleceniami norm przedmiotowych. Defekt takich urządzeń zazwyczaj prowadzi do utraty funkcji bezpieczeństwa. Urządzenia kategorii 1 charakteryzują się podwyższoną odpornością na defekty, głównie w związku z zastosowaniem bardziej niezawodnych elementów i podzespołów. W urządzeniach kategorii 2, 3 i 4 wzrost odporności na defekty uzyskuje się poprzez rozbudową struktury urządzenia. W kategorii 2 realizowane jest to poprzez periodyczne sprawdzanie funkcji bezpieczeństwa. W kategorii 3 i 4 odporność uzyskiwana jest poprzez zapewnienie, że pojedynczy defekt nie spowoduje utraty funkcji bezpieczeństwa. W urządzeniach kategorii 3 pojedynczy defekt powinien być wykryty jeśli jest to uzasadnione, a w kategorii 4 jeśli jest to możliwe. Dodatkowo, powinna być określona reakcja urządzenia na akumulację defektów. Tak więc norma ściśle definiuje zachowanie się urządzeń każdej kategorii w warunkach defektu.

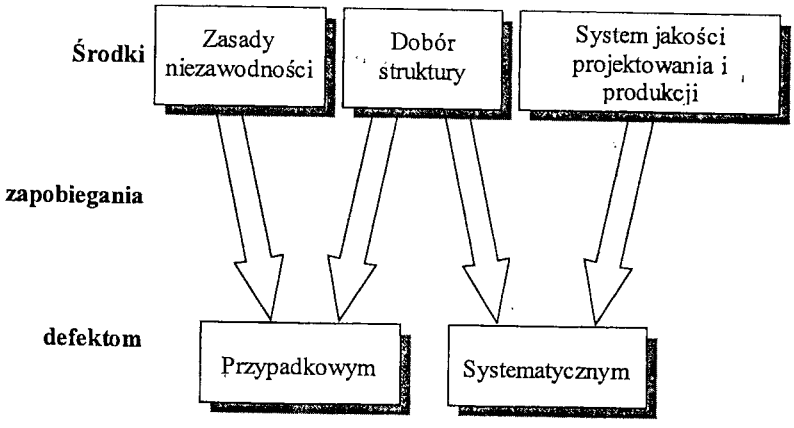
W przypadku złożonych urządzeń elektronicznych koncepcja zawarta w PN-EN 954-1, dotycząca jedynie zachowania w warunkach pojedynczego defektu, jest niewystarczająca i może prowadzić do nieporozumień. Systemy sterowania zbudowane w oparciu o nowoczesne technologie elektroniczne, takie jak ASIC lub mikroprocesory, są zbyt skomplikowane aby można było określić ich zachowanie w warunkach defektu. Dodatkowe problemy stanowią defekty oprogramowania. Dlatego też wprowadzono nowe podejście, pod nazwą „bezpieczeństwo funkcjonalne" [5]. Bezpieczeństwo funkcjonalne można scharakteryzować następująco:

- koncepcja stosuje się do systemów i funkcji wiążących się z zapewnieniem bezpieczeństwa;
- bezpieczeństwo funkcjonalne uzyskuje się poprzez eliminację, za pomocą działań

prewencyjnych, ewentualnych defektów systematycznych;

- drogą do uzyskania bezpieczeństwa funkcjonalnego jest przestrzeganie odpowiednich procedur przez odpowiednio wyszkolony personel;
- poprzez audity i ocenę realizowanych działań uzyskujemy pewność, że osiągnęliśmy wymagany poziom bezpieczeństwa funkcjonalnego;
- miernikiem osiągniętego poziomu bezpieczeństwa funkcjonalnego są wskaźniki probabilistyczne.

Wymagania bezpieczeństwa funkcjonalnego sformułowane są w normach IEC 61508: "Functional safety of electrical, electronic and programmable safety-related systems". Dokumenty te zostały opracowane z punktu widzenia dużych systemów sterowania procesami przemysłowymi, na przykład liniami produkcyjnymi w fabrykach chemicznych lub reaktorami w elektrowniach atomowych. Zasady sformułowane dla dużych systemów są zbyt skomplikowane, aby mogły być skutecznie stosowane w obszarze systemów sterowania maszyn. Dlatego też prowadzone są obecnie prace nad normą EN 62061, których celem jest określenie wymagań bezpieczeństwa funkcjonalnego dla programowalnych sterowników maszyn.



Rys. 2. Strategia zapobiegania defektom

Ogólna strategia zapobiegania defektom opiera się na zastosowaniu trzech podstawowych środków (patrz rys. 2):

- uwzględnienie wymagań niezawodnościowych,
- dobór właściwej struktury systemu,
- przestrzeganie zasad systemu jakości w całym cyklu życia urządzenia.

Poprzez uwzględnienie wymagań niezawodnościowych przy doborze elementów i podzespołów oraz w fazie produkcji możemy w znacznym stopniu ograniczyć występowanie defektów przypadkowych. Duże znaczenie ma także stosowanie „podstawowych" i „wypróbowanych" zasad i elementów bezpieczeństwa. Ponieważ, przy obecnym stanie wiedzy, złożone układy elektroniczne nie mogą rozpatrywane jako „wypróbowane elementy bezpieczeństwa, więc w ich przypadku należy stosować dodatkowe rozwiązania umożliwiające zwiększenie niezawodności systemu. Obecnie najbardziej rozpowszechnione są trzy podstawowe metody zwiększenia poziomu nienaruszalności bezpieczeństwa:

- techniki samokontroli;

- rozwiązania wielokanałowe;
- kombinacje obu tych technik.

Technika samokontroli realizowana jest poprzez zastosowanie różnorodnych autotestów, zarówno sprzętowych jak i programowych. W przypadku technik wielokanałowych w obszarze maszyn stosuje się zazwyczaj rozwiązania typu „1oon" lub „2oon". System „1oon" składa się z „n" kanałów, połączonych w ten sposób, że sprawne działanie 1-go kanału wystarcza do skutecznej realizacji zakładanych funkcji. W przypadku systemu „2oon" konieczne jest, aby co najmniej 2 kanały były sprawne. Właściwy dobór konfiguracji umożliwia osiągnięcie wyższej niezawodności systemu poprzez zredukowanie prawdopodobieństwa wystąpienia defektu prowadzącego do utraty funkcji bezpieczeństwa dzięki wykrywaniu uszkodzeń elementów i podzespołów.

Techniki wielokanałowe umożliwiają także zredukowanie wpływu uszkodzeń od wspólnej przyczyny, a także niektórych defektów systematycznych. Uzyskuje się to poprzez stosowanie różnych technologii w różnych kanałach redundancji. Skuteczne jest także wykonywanie projektu różnych kanałów przez niezależne zespołu projektantów.

Stosowanie systemów jakości jest podstawową metodą zapobiegania defektom systematycznym. Polega ona na szczegółowym dokumentowaniu wszystkich czynności wykonywanych w każdym etapie projektowania, konstruowania i walidacji urządzenia. Dotyczy to także kompetencji personelu, doboru podwykonawców, współpracy dostawcy z użytkownikiem, okresowych auditów itp. Szczególne znaczenie mają zasady opracowywania oprogramowania. Zazwyczaj nawet najprostsze programy zawierają błędy. Większość z nich jest wykrywana i usuwana w trakcie testów przeprowadzanych przez projektanta. Skuteczność eliminacji błędów oprogramowania może znacznie zwiększona poprzez zastosowanie procedur formalnych w każdym etapie tworzenia programu.

4. PODSUMOWANIE

Widzimy więc, że w procesie projektowania systemu sterowania maszyny zbudowanego ze złożonych systemów elektronicznych konieczne jest rozwiązanie wielu problemów technicznych i organizacyjnych. Wiele instytutów i ośrodków naukowych prowadzi prace badawcze zmierzające do upowszechnienia nowoczesnych metod projektowania z wykorzystaniem najnowszych technologii, które umożliwiają realizowanie funkcji bezpieczeństwa w bardziej efektywny sposób [6, 8, 1]. Prace te dotyczą głównie rozwiązania podstawowych prblemów związanych z projektowaniem i programowaniem systemów:

- zasady oceny probabilistycznej;
- podstawowe i wypróbowane zasady bezpieczeństwa;
- dobór struktury odpowiedniej do kategorii lub poziomu nienaruszalności bezpieczeństwa;
- organizacja ogólnego cyklu trwałości bezpieczeństwa w zależności od złożoności systemu i poziomu ryzyka;
- metodologia programowania.

Wraz z rozowjem nowych technologii pojawiają się nowe zadania badawcze dotyczące skuteczności realizacji funkcji bezpieczeństwa. Obecnie najwięcej problemów napotyka prawidłowe rozwiązanie następujących zagadnień:

- koordynacja sterowania w systemach rozproszonych,
- transmisja danych związanych z bezpieczeństwem w obrębie stanowiska pracy,

– bezprzewodowe sterowanie maszyną (np. zdalne sterowanie wyłączaniem awaryjnym) itp.

W najbliższej przyszłości należy spodziewać się problemów związanych ze stosowaniem do sterowania maszynami takich technologii jak: sieci neuronowe, Internet, metody logiki rozmytej, systemy wizyjne, systemy samoprogramujące i samokonfigurujące się, sterowanie maszyn głosem, itp. Technologie te formułują nowe zadania dla instytutów i jednostek badawczych. Postępujący proces globalizacji wymagać będzie zaawansowanej współpracy międzynarodowej. Szczególne znaczenie ma wymiana informacji oraz harmonizacja procedur badań i oceny urządzeń.

LITERATURA

[1] Carlsson, H., Jacobson, J., Ohlsson, M.: *Safety validation of computer-based machine control systems.* SP Report 1997:12.

[2] Ciccotelli , J: *Safety components: new requirements for 1997.* Raport INRS, 1997.

[3] Dźwiarek, M.: *Klasyfikacja systemów sterowania w zależności od zapewnianego poziomu bezpieczeństwa według EN954-1.* Pomiary, Automatyka, Robotyka 8/1997, str. 4-9.

[4] Hietikko, M., Kivipuro, M., Tiusanen, R.: *The safety assessment method for programmable electronics.* Raport VTT, Tampere, 1994.

[5] Missala, T.: *Functional safety of automation and robotics.* Pomiary, Automatyka, Robotyka 3/1997, str. 5-8.

[6] Reinert, D.: *Validation of functional safety of programmable electronic systems according to IEC 1508.* Raport BIA, 1995.

[7] Vautrin, J. P.: *The concept of EN 954 categories for the design and testing.*

[8] Vigneron C.: *Safety - dedicated programmable logic controllers, results of a survey carried out in 1997 in European organizations.* Raport INRS, 1997.