dr inż. Marek Dźwiarek
Centralny Instytut Ochrony Pracy

PROBABILISTYCZNA OCENA BEZPIECZEŃSTWA FUNKCJONALNEGO SYSTEMÓW STEROWANIA MASZYN

Wyznaczenie odporności systemów sterowania na występowanie uszkodzeń przypadkowych jest zadaniem skomplikowanym i wymagającym zaangażowania doświadczonego i wysoko wykwalifikowanego personelu. Zaproponowane w referacie metody jakościowa i ilościowa pozwalają na wystarczająco dokładne oszacowanie osiągniętego SIL, także w przypadku dysponowania ograniczonymi informacjami dotyczącymi niezawodności poszczególnych elementów systemu. Mogą one być stosowane w procesie oceny SIL sterowników programowalnych maszyn.

PROBABILISTIC ASSESSMENT OF FUNCTIONAL SAFETY OF MACHINE CONTROL SYSTEM

Determination of the resistance of control systems to random failures is a difficult task, which can be fulfilled only by well skilled and trained personnel. The quantitative and qualitative methods proposed in the paper allow for estimation of the reached SIL with a sufficient accuracy, also in the case of lack of sufficient reliability data for particular components of the system. These methods can be used in the assessment process of SIL of a programmable control system.

1. WPROWADZENIE

W [1], [3] i [4] wykazano, że podstawowymi środkami uzyskiwania bezpieczeństwa funkcjonalnego są:

- stosowanie zasad systemu jakości w całym cyklu życia systemu, ze szczególnym uwzględnieniem etapu konstruowania;
- stosowanie elementów i podzespołów o określonej niezawodności oraz probabilistyczna ocena systemu;
- dobór architektury systemu oraz właściwych języków programowania i metod kodowania.

Jednym z elementów oceny poziomu bezpieczeństwa systemu będzie więc określenie prawdopodobieństwa utraty funkcji bezpieczeństwa. Może to być zrealizowane metodami jakościowymi lub ilościowymi. Przedstawione poniżej propozycje takich metod opracowane zostały w Centralnym Instytucie Ochrony pracy w ramach realizacji tematu badawczego „Opracowanie zasad i metod określania poziomu nienaruszalności bezpieczeństwa dla programowalnych systemów sterowania maszyn" [2].

2. ASPEKTY BEZPIECZEŃSTWA W SYSTEMACH STEROWANIA MASZYN

Dla konstruktora maszyny istotne znaczenie ma właściwe zrozumienie kwestii bezpieczeństwa operatora. Ważne jest zwłaszcza właściwe zrozumienie zależności pomiędzy bezpieczeństwem a niezawodnością, szczególnie w przypadku określania poziomu bezpieczeństwa poprzez wskaźniki niezawodnościowe, tak jak ma to miejsce przy ocenie bezpieczeństwa funkcjonalnego. Należy zwrócić uwagę, że bezpieczeństwo nie wymaga aby maszyna była sprawna, ale aby nie stwarzała zagrożeń. Oznacza to, że poziom ryzyka nie powinien przekraczać poziomu akceptowalnego, także w warunkach uszkodzenia maszyny. Tak więc wymagania dotyczące bezpieczeństwa będą się koncentrować na wytworzeniu systemu który nie powodowałby wypadków. Oznacza to, że z punktu widzenia bezpieczeństwa nie jest istotna częstość występowania defektów w ogóle, ale przede wszystkim prawdopodobieństwo obniżenia skuteczności realizacji funkcji bezpieczeństwa.

W IEC 61508-4:1998 p. 3.6.7 zdefiniowano „uszkodzenie niebezpieczne" jako uszkodzenie które może potencjalnie wprowadzić system związany z bezpieczeństwem w stan występowania zagrożenia lub utraty funkcji. W sensie tej definicji uszkodzenie które zostanie wykryte nie jest uszkodzeniem niebezpiecznym, jeśli konsekwencją jego wykrycia jest stan bezpieczny. Tak więc uszkodzenie jednego z kanałów układu redundancji nie należy traktować jako uszkodzenie niebezpieczne. W poprawnie zbudowanym systemie redundancji uszkodzenie albo jest wykrywane i urządzenie jest sprowadzane do stanu bezpiecznego, albo funkcja bezpieczeństwa jest nadal realizowana przez drugi, nadal sprawny kanał. W drugim przypadku skutkiem uszkodzenia jest obniżenie poziomu nienaruszalności bezpieczeństwa (SIL), ale bezpieczeństwo operatora jest nadal nadzorowane. Dopiero akumulacja niewykrytych uszkodzeń może spowodować utratę funkcji bezpieczeństwa, a więc stanowić będzie uszkodzenie niebezpieczne.

Istotne znaczenie ma także czas wykrycia uszkodzenia. Zazwyczaj zanim uszkodzenie zostanie wykryte mija pewien czas potrzebny na wykonanie diagnostyki systemu. Tak więc w systemie może występować uszkodzenie, które spowoduje upośledzenie funkcji bezpieczeństwa i zostanie wykryte dopiero po jakimś czasie. Uszkodzenia takie stają się uszkodzeniami niebezpiecznymi, jeśli przywołanie funkcji bezpieczeństwa nastąpi przed ich wykryciem. Natomiast jeśli uszkodzenie zostanie wykryte odpowiednio szybko, to nie powinno być rozpatrywane jako uszkodzenie niebezpieczne. Przy ocenie poziomu bezpieczeństwa funkcjonalnego ważne będzie więc właściwe zidentyfikowanie uszkodzeń niebezpiecznych, gdyż to one decydują w głównej mierze o osiągniętym SIL.

Programowalne systemy elektroniczne mają możliwość wykrywania defektów wewnętrznych zanim ujawnią się one jako niesprawność systemu. Możliwe rozwiązania zawierają zarówno środki układowe, jak i programowe. Różne metody wykrywania uszkodzeń charakteryzują się różną skutecznością. Każda metoda wykrywania defektów może być scharakteryzowana za pomocą jej najważniejszych parametrów: pokrycia diagnostycznego DC (diagnostic coverage) i częstotliwości sprawdzeń f_d. Parametry te odnoszą się zarówno do autotestów realizowanych automatycznie przez system, jak i do sprawdzeń wykonywanych przez użytkownika. W przypadku sprawdzeń okresowych, wykonywanych stosunkowo rzadko wygodniej jest używać czasu pomiędzy sprawdzeniami jako charakteryzującego je parametru. Parametry te powinny być podawane przez producenta urządzenia.

3. ILOŚCIOWA OCENA SYSTEMU

Poziomy nienaruszalności bezpieczeństwa definiowane są przez wskaźniki probabilistyczne. Określają one prawdopodobieństwo wystąpienia uszkodzenia niebezpiecznego w określonym

przedziale czasu. Tak więc ocena systemu wymagać będzie jego probabilistycznej analizy. Analizę taką można przeprowadzać różnymi metodami. Obecnie najbardziej rozpowszechnione i najbardziej skuteczne są:

- metoda drzewa defektów FTA (patrz IEC 61025:1990),
- analiza rodzajów uszkodzeń i ich skutków FMEA (patrz PN-IEC 60812:1994),
- metoda grafów Markova (patrz IEC 61165:1995),
- metoda HAZOP.

Norma IEC 61508-2:2000 rozróżnia dwa typy systemów: A i B. Do typu A zaliczane są systemy w których:

1. znane są wszystkie możliwe rodzaje uszkodzeń we wszystkich elementach, oraz
2. zachowanie systemu w warunkach defektu jest jednoznacznie określone, oraz
3. dostępne są dane statystyczne określające prawdopodobieństwo wystąpienia poszczególnych defektów.

Do typu B zalicza się urządzenia które nie spełniają przynajmniej jednego z powyższych warunków. Ponieważ obecnie dostępne są bazy danych zawierające informacje dotyczące pojedynczych elementów elektronicznych, możemy więc przyjąć, że urządzenia zbudowane z prostych pojedynczych elementów elektronicznych można będzie zaliczyć do typu A, pod warunkiem przeprowadzenia analizy wynikającej z wymagania 2. Brak wystarczających danych dotyczących mikroprocesorów i układów scalonych wielkiej skali integracji powoduje, że systemy zawierające elementy tego rodzaju należy zaliczyć do typu B. Analiza urządzeń typu A opierać się będzie na identyfikacji poszczególnych możliwych uszkodzeń oraz określaniu prawdopodobieństwa ich wystąpienia i zachowania się systemu. Do tego celu najbardziej odpowiednia jest analiza metodą FTA lub FMEA. W przypadku urządzeń typu B nie jest możliwe zidentyfikowanie poszczególnych defektów. Analiza opierać się będzie na określeniu zachowania się systemu w warunkach uszkodzenia. Obecnie najczęściej stosowaną metodą analizy układów typu B jest metoda grafów Markowa (patrz [5]).

4. MODELOWANIE SYSTEMÓW METODĄ MARKOVA

Ogólna zasada stosowania grafów Markova opisana jest w IEC 61165:1995. Metoda ta jest bardzo skutecznym narzędziem do analizy probabilistycznej systemów które mogą przyjmować wiele różnych stanów. W przypadku systemów związanych z bezpieczeństwem analiza dotyczyć będzie kwestii związanych z występowaniem uszkodzeń przypadkowych w sprzęcie. Tak więc graf nie będzie obejmował stanów funkcjonalnych systemu, ale stany dotyczące jego sprawności. Analizę należy przeprowadzać w odniesieniu do przewidywanego czasu użytkowania systemu „T_M", rozumianego jako czas przydatności systemu do realizacji funkcji związanych z bezpieczeństwem. Oczekiwanym rezultatem analizy jest określenie prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego w czasie 1h (w systemach o trybie pracy ciągłej) lub w czasie T_M (w systemach o trybie pracy „na żądanie").

Pełny model Markova składa się z dwu elementów: zbioru możliwych stanów Ψ oraz macierzy przejść $\boldsymbol{P} = [p_{ij}]$. Zbiór stanów Ψ powinien być pełny, to znaczy powinien zawierać wszystkie możliwe stany. Definicje poszczególnych stanów powinny być rozłączne. Elementy macierzy $\boldsymbol{P}$ określają prawdopodobieństwa przejścia z jednego stanu do drugiego. Zwykle model systemu przedstawiany jest w postaci graficznej. Przedstawienie takie, poprzez wizualizację, czyni model bardziej przejrzystym i ułatwia jego analizę. Prawdopodobieństwa przejść p_{ij} zawsze są określane w odniesieniu do określonego przedziału czasu Δt. Właściwy dobór Δt ma istotne znaczenie dla skuteczności zastosowanego modelu. Czas ten powinien być wystarczająco mały aby zidentyfikować wszystkie możliwe zjawiska w systemie.

Zazwyczaj jako Δt przyjmuje się czas pomiędzy kolejnymi przywołaniami funkcji bezpieczeństwa lub pomiędzy kolejnymi autotestami, w zależności od tego który jest mniejszy.

Niech S oznacza wektor stanu modelu:

$$S = [s_1, s_2, \ldots, s_n] \quad (1)$$

gdzie: s_i – prawdopodobieństwo osiągnięcia i-tego stanu.

Elementy wektora S będą się zmieniać wraz z upływem czasu. Jeśli ich aktualna wartość wynosi S_k, to po upływie jednostki czasu Δt przyjmą one wartość S_{k+1}:

$$S_{k+1} = S_k \cdot P \quad (2)$$

Przy rozpoczynaniu analizy systemu zakładamy, że znajduje się on stanie braku uszkodzeń S_0. Po upływie czasu $k\Delta t$ wektor stanu przyjmie wartość:

$$S_k = S_0 \cdot P^k \qquad \text{gdzie: } S_0 = [1, 0, \ldots, 0] \quad (3)$$

Przy określaniu SIL konieczne jest wyznaczenie prawdopodobieństwa wystąpienia uszkodzenia niebezpiecznego w przeciągu godziny lub pomiędzy przywołaniami. Tak więc k przyjmie wartość $1h/\Delta t$ lub $1/\Delta t{:}f_p$, gdzie f_p oznacza średnią częstotliwość przywołań.

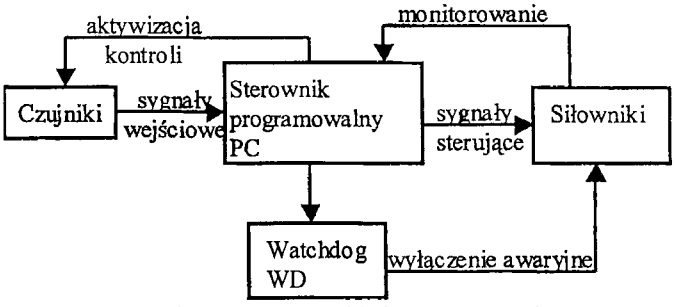
4.1. Określanie prawdopodobieństwa uszkodzeń

Przy określaniu poszczególnych elementów macierzy przejść P konieczna będzie znajomość prawdopodobieństwa uszkodzeń poszczególnych elementów lub podzespołów systemu. W praktyce zazwyczaj możliwe jest jedynie oszacowanie wartości odpowiednich wskaźników niezawodnościowych. W przypadku braku danych szczegółowych, dotyczących konkretnego elementu lub podzespołu wykorzystać można dane ogólne, określone dla elementów danego typu. Uzyskane w ten sposób wskaźniki mogą stanowić podstawę do wyznaczenia prawdopodobieństwa uszkodzenia zastosowanych elementów. Najprostszym sposobem oszacowania prawdopodobieństwa uszkodzenia elementów lub podzespołów typu B jest wykorzystanie wskaźnika średniego czasu pracy bezawaryjnej (MTTF). Możemy przyjąć że prawdopodobieństwo uszkodzenia elementu w przedziale czasu Δt wyniesie:

$$\lambda = \frac{\Delta t}{\text{MTTF}} \quad (4)$$

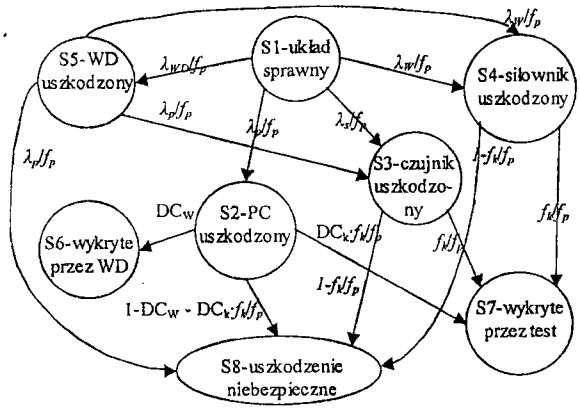
4.2. Przykład modelu typowej konfiguracji układowej

We wszystkich systemach można wyróżnić typowe, najczęściej powtarzające się konfiguracje elementów i podzespołów. Model całego systemu zawierał więc będzie szereg typowych fragmentów połączonych w całość odpowiadającą konkretnemu systemowi.



Rys. 1. Schemat blokowy układu programowalnego z monitorowaniem

Często spotykanym rozwiązaniem jest system programowalny z monitorowaniem. Schemat blokowy takiego systemu pokazany jest na rys. 1. W układzie tym sterownik programowalny generuje periodycznie sygnały aktywizujące kontrolę sprawności systemu. Oznaczmy przez f_k częstotliwość tej kontroli a pokrycie diagnostyczne tego sprawdzenia przez DC_K. Podobnie przez DC_W oznaczmy pokrycie diagnostyczne układu WD. Zauważmy, że uszkodzenie WD nie jest uszkodzeniem niebezpiecznym, ale powoduje że większa część możliwych uszkodzeń systemu programowalnego będzie stanowić uszkodzenia niebezpieczne. Uszkodzenia czujników lub elementów sterujących siłownikami staną się uszkodzeniami niebezpiecznymi, jeśli nie zostaną wykryte przed przywołaniem funkcji bezpieczeństwa. Prawdopodobieństwa tych uszkodzeń układu programowalnego, czujników, WD i elementów wykonawczych oznaczmy odpowiednio przez λ_p, λ_s, λ_{WD} i λ_W. Przedział czasu Δt dla którego przeprowadzana będzie analiza zależeć będzie od trybu pracy systemu, a także od wzajemnych zależności pomiędzy częstością przywołań f_p i częstością kontroli f_k.



Rys. 2. Model układu programowalnego z monitorowaniem

Model układu z periodycznym monitorowaniem o trybie pracy z dużą częstością przywołań f_p pokazany jest na rys. 2. W modelu tym stanami stabilnymi są stany S1, S5, S6 i S8. W przypadku gdy przed przywołaniem funkcji nastąpi wykrycie uszkodzenia przez periodyczne monitorowanie lub WD system przechodzi w stan bezpieczny S6 lub S7. Jeśli takie wykrycie nie nastąpi, system znajdzie się w stanie uszkodzenia niebezpiecznego S8. Nieco inna sytuacja ma miejsce w przypadku uszkodzenia WD (stan S5). Ponieważ samo uszkodzenie WD nie powoduje utraty funkcji bezpieczeństwa, więc system może trwale pozostawać w tym stanie. Zmiana stanu nastąpi dopiero po wystąpieniu uszkodzenia któregoś z pozostałych elementów systemu. Jednoczesne uszkodzenie WD i sterownika jest uszkodzeniem niebezpiecznym. Pozostałe uszkodzenia należy traktować jako potencjalnie niebezpieczne. Tak więc poziom nienaruszalności bezpieczeństwa określony będzie przez prawdopodobieństwo wystąpienia stanu S8 po upływie 1h:

$$SIL = s_8^k \qquad \text{gdzie}: k = 1\text{h} \cdot f_p \tag{5}$$

5. JAKOŚCIOWA OCENA SYSTEMU

Opisana powyżej ilościowa metoda oceny systemu wymaga zaangażowania ekspertów o dużej wiedzy i doświadczeniu, oraz dostępu do potwierdzonych baz danych statystycznych, co nie zawsze jest możliwe. W takim przypadku ocenę można przeprowadzić poprzez jakościowe oszacowanie struktury i parametrów systemu. W praktyce wyróżnić można kilka podstawowych struktur, które są najczęściej stosowane. Także parametry systemu można sklasyfikować w kilku podstawowych grupach. Najważniejsze właściwości systemów o typowej strukturze i typowych parametrach oszacowane zostały przez międzynarodowe grupy ekspertów. Wyniki tych prac w postaci stabelaryzowanej udostępniono w Załączniku B do

IEC 61508-6:2000. Mogą one stanowić podstawę do jakościowego oszacowania osiągniętego poziomu nienaruszalności bezpieczeństwa.

5.1. Klasyfikacja parametrów systemu

Podstawowymi parametrami decydującymi o poziomie nienaruszalności bezpieczeństwa systemu są:

- średni czas pracy bezawaryjnej MTTF poszczególnych podzespołów,
- pokrycie diagnostyczne DC,
- współczynnik uszkodzeń od wspólnej przyczyny β,
- częstość wyłączeń f_r,
- częstość konserwacji f_k.

Zazwyczaj dokładne określenie wartości tych parametrów, z wyjątkiem f_r i f_k, jest trudne do zrealizowania. Dużo łatwiej natomiast zaklasyfikować je do określonej grupy, np. małe, średnie, duże itp. Klasyfikacja taka jest pomocna w jakościowej ocenie systemu.

Pokrycie diagnostyczne DC opisuje jaka część uszkodzeń niebezpiecznych może być wykryta przez autotesty lub monitorowanie systemu. W IEC 61508-2:2000 przyjęto klasyfikację DC na następujące cztery grupy:

brak – DC = 0 małe – DC < 60% średnie – 60% < DC < 90% duże – DC > 90%.

Zazwyczaj projektant systemu jest w stanie określić do jakiej grupy można zaliczyć zastosowane przez niego autotesty.

Obecnie dostępne podzespoły i elementy elektroniczne wykonywane są w różnych wersjach niezawodnościowych. Przy braku precyzyjnych danych statystycznych można co najwyżej oszacować przewidywany zakres wartości MTTF. Ponieważ dla układów elektronicznych nie należy się spodziewać MTTF większych niż 100 lat, więc proponuje się określenie 3 zakresów czasu przewidywanej pracy bezawaryjnej:

mały – 3 do 10 lat, średni – 10 do 30 lat, duży – 30 do 100 lat.

5.2. Określanie poziomu nienaruszalności bezpieczeństwa

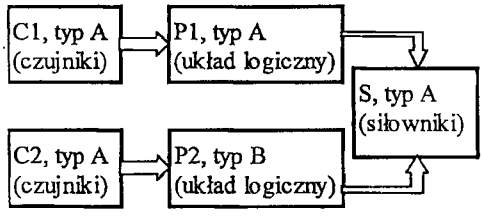
Najprostsza jakościowa metoda określania SIL polega ona na wydzieleniu w systemie podstawowych modułów. Następnie należy określić SIL każdego modułu. Dokonuje się tego na podstawie analizy tolerancji podzespołu na uszkodzenia oraz jego pokrycia diagnostycznego. Liczba tolerowanych uszkodzeń jest to największa liczba uszkodzeń których wystąpienie nie spowoduje utraty realizowanych funkcji. Liczba ta powinna być określona na podstawie analizy każdego podzespołu, na przykład metodą FMEA. W tablicy 1 określono SIL w zależności od pokrycia diagnostycznego DC oraz liczby tolerowanych uszkodzeń dla układów typu A i B. Niejednokrotnie, zwłaszcza dla układów typu B, określenie liczby tolerowanych uszkodzeń może być trudne do wykonania. W takim przypadku wygodnie jest posłużyć się wskaźnikami niezawodnościowymi. W IEC 61508-6 podane są średnie wartości prawdopodobieństwa uszkodzenia niebezpiecznego dla podstawowych konfiguracji: 1oo1, 1oo2, 2oo2, 1oo2D i 2oo3. Wartości te podane są w zależności od λ, DC i β, oraz dla różnych okresów konserwacji i periodycznych wyłączeń. Na tej podstawie można w prosty sposób uzyskać dane niezbędne do określenia SIL układu. Określenie SIL dla całego systemu zazwyczaj dokonuje się w kilku kolejnych krokach. W każdym kroku grupuje się podzespoły prostsze w zestawy bardziej złożone. SIL tych

podzespołów określa się na podstawie analizy SIL podzespołów prostszych. Postępowanie to powtarza się tak długo, aż cały system zostanie sprowadzony do poziomu jednego zespołu.

Tablica 1. Poziomy nienaruszalności bezpieczeństwa układów typu A i B.

Pokrycie diagnistyczne	Liczba tolerowanych uszkodzeń i typ układu					
	0		1		2	
	A	B	A	B	A	B
brak (0%)	SIL 1	-	SIL 2	SIL 1	SIL 3	SIL 2
małe (60%)	SIL 2	SIL 1	SIL 3	SIL 2	SIL 4	SIL 3
średnie (90%)	SIL 3	SIL 2	SIL 4	SIL 3	SIL 4	SIL 4
duże (99%)	SIL 4	SIL 3	SIL 4	SIL 4	SIL 4	SIL 4

5.4. Przykład jakościowej oceny systemu



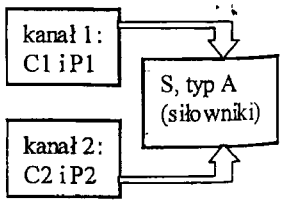
Rys. 3. Przykład podziału systemu na podzespoły

Na rys. 3 przedstawiono schemat blokowy systemu dwukanałowego. Posłuży on do zaprezentowania jakościowej metody oceny SIL. Kanał pierwszy składa się z układu czujników C1 i układu logicznego P1. Załóżmy, że są to układy typu A. Kanał drugi zawiera dodatkowy zestaw czujników C2 oraz układ logiczny typu B. Obydwa kanały sterują układem siłowników S. Układ ten jest typu A. W efekcie jest to system o dwu kanałach redundancji wykonanych w różnych technologiach, gdzie kanał 2-gi sterowany jest z użyciem sterownika programowalnego.

5.4.1. Określanie SIL dla podzespołów

Załóżmy, że w spełnione są następujące warunki:

C1 – nie odporny na uszkodzenia, DC – średnie,
P1 – odporny na 1 uszkodzenie, DC – brak,
C2 – odporny na 2 uszkodzenia, DC – brak,
P2 – nie odporny na uszkodzenia, DC – małe,
S – nie odporny na uszkodzenia, DC – małe



Rys. 4. Struktura układu po wstępnym grupowaniu

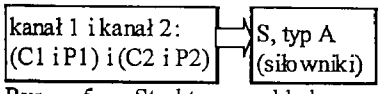
W warunkach tych, na podstawie tablicy 1, mamy: C1 – SIL 3, P1 – SIL 2, C2 – SIL 3, P2 – SIL 1 i S - SIL 2.

5.4.2. Grupowanie podsystemów

Po ustaleniu poziomu nienaruszalności bezpieczeństwa poszczególnych podzespołów można przystąpić do określenia SIL całego systemu. W tym celu należy pogrupować podzespoły w większe części systemu. Grupowanie powinno uwzględniać strukturę systemu i realizowane funkcje. W naszym przykładzie najbardziej bezpośrednie jest zgrupowanie C1 z P1 oraz C2 z P2. W efekcie uzyskujemy strukturę dwukanałową pokazaną na rys. 4. Następnie szacujemy SIL dla wszystkich, tak określonych podzespołów. W przypadku podzespołów połączonych szeregowo do realizacji jednej funkcji o poziomie nienaruszalności bezpieczeństwa decyduje podzespół o najmniejszym SIL. W naszym przypadku otrzymujemy:

kanał 1: C1 i P1 – SIL 2 (mniejszy z SIL 3 i SIL 2)
kanał 2: C2 i P2 – SIL 1 (mniejszy z SIL 3 i SIL 1)

Postępowanie to przeprowadzamy tak długo, dopóki cały system nie zostanie zredukowany do jednego zespołu. W opisywanym przykładzie krokiem następnym jest zgrupowanie kanałów 1 i 2 do jednego podzespołu. Kanały te połączone są w ten sposób, że w przypadku uszkodzenia jednego z nich funkcja bezpieczeństwa jest realizowana nadal przez kanał drugi. W efekcie SIL obu kanałów jest sumą dwu składowych. Mamy więc:



Rys. 5. Struktura układu po powtórnym grupowaniu podzespołów

kanał 1 i kanał 2: (C1 i P1) i (C2 i P2) – SIL 3 (SIL 2 + SIL1)

Otrzymana struktura pokazana jest na rys. 5. Ostatecznie, dla całego systemu otrzymujemy:

cały system: (C1 i P1) i (C2 i P2) i S – SIL 2 (mniejszy z SIL 3 i SIL 2)

Przykład powyższy pokazuje metodologię jakościowej oceny poziomu nienaruszalności bezpieczeństwa systemu. Metoda ta jest tym dokładniejsza, im bardziej szczegółowy jest wstępny podział systemu na podzespoły. Główną zaletą metody jest bezpośrednie wskazanie, które podzespoły systemu stanowią jego najsłabsze punkty, decydując o SIL całości. W naszym przypadku widzimy, że podzespół C2 ma SIL nieproporcjonalnie wysoki w stosunku do pozostałych podzespołów. Dokładnie ten sam wynik uzyskalibyśmy, gdy C2 był wykonany według wymagań dla SIL 2, a nawet SIL 1.

6. PODSUMOWANIE

Wyznaczenie odporności systemów sterowania na występowanie uszkodzeń przypadkowych jest zadaniem skomplikowanym i wymagającym zaangażowania doświadczonego i wysoko wykwalifikowanego personelu. Stosowanie precyzyjnych analiz probabilistycznych w rzeczywistych przypadkach jest praktycznie niewykonalne. Wynika to z wielu problemów, które nie są jeszcze obecnie wystarczająco dokładnie rozwiązane. Najważniejszymi z nich jest brak wystarczająco dokładnych i pełnych danych statystycznych i duże skomplikowanie procedur, które nawet dla prostych systemów powodują konieczność wykonania dużej ilości obliczeń. Dlatego też konieczne jest stosowanie procedur uproszczonych. Zaproponowane w referacie metody jakościowa i ilościowa pozwalają na wystarczająco dokładne oszacowanie osiągniętego SIL, także w przypadku dysponowania ograniczonymi informacjami dotyczącymi niezawodności poszczególnych elementów systemu. Mogą one być stosowane w procesie oceny poziomu nienaruszalności bezpieczeństwa prostych sterowników programowalnych maszyn.

LITERATURA

[1] Dźwiarek, M., (2000). Application of Complex Electronics in Machinery Control Systems. *Human Aspects of Advanced Manufacturing: Agility & Hybrid Automation*, 27-30 August, Kraków. 341-344.

[2] Dźwiarek, M., (2000). Opracowanie metod sprawdzania poziomu nienaruszalności bezpieczeństwa programowalnych systemów sterowania maszyn. SPR-1, zad. bad. 03.7.14. *Centralny Instytu Ochrony Pracy* CIOP, Warszawa.

[3] Dźwiarek, M., (2001). Aspekty bezpieczeństwa funkcjonalnego złożonych systemów sterowania maszyn. *Automation, 28-30 marca 2001, Warszawa.* 95-101.

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

[5] (2000): Safety-Related Complex Electronic Systems. Final report. Coordinator: INERIS, Partners: BIA, HSE, INRS, VTT, CETIM, INSHT – CNVM, SP, TÜV, SICK AG, JAY Electronique. *European Commission – DG XII.*