Kazimierz KOSMOWSKI, Marcin ŚLIWIŃSKI
POLITECHNIKA GDAŃSKA, WYDZIAŁ ELEKTROTECHNIKI I AUTOMATYKI, KATEDRA AUTOMATYKI

Analiza ryzyka i modelowanie probabilistyczne oparte na wiedzy w projektowaniu i użytkowaniu programowalnych systemów sterowania i zabezpieczeń

Dr hab. inż. Kazimierz KOSMOWSKI

W 1972 roku ukończył studia na Wydziale Elektrycznym Politechniki Gdańskiej. W roku 1981 obronił rozprawę doktorską, a rozprawę habilitacyjną w 2003 roku. Profesor nadzw. Politechniki Gdańskiej. Od 2006 roku pełni funkcję Kierownika Katedry Automatyki. Zajmuje się zagadnieniami niezawodności i bezpieczeństwa systemów technicznych, bezpieczeństwa funkcjonalnego programowalnych systemów sterowania i automatyki zabezpieczeniowej oraz niezawodności człowieka – operatora.

e-mail: k.kosmowski@ely.pg.gda.pl

Dr inż. Marcin ŚLIWIŃSKI

W 2001 roku ukończył studia na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej. W roku 2006 uzyskał stopień doktora nauk technicznych w zakresie automatyki i robotyki. Od 2006 roku pracuje na stanowisku adiunkta w Katedrze Automatyki na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej. Zajmuje się zagadnieniami bezpieczeństwa funkcjonalnego oraz badaniem i modelowaniem probabilistycznym nadmiarowych systemów sterowania i zabezpieczeń.

e-mail: m.sliwinski@ely.pg.gda.pl

Streszczenie

W niniejszym artykule przedstawiono wybrane zagadnienia związane z projektowaniem i użytkowaniem programowalnych systemów sterowania i zabezpieczeń. Są one wdrażane coraz częściej jako systemy elektryczne/ elektroniczne i programowalne elektroniczne (E/E/PE) zgodnie z koncepcją bezpieczeństwa funkcjonalnego, zarysowaną w normie IEC 61508 o charakterze ogólnym oraz normach sektorowych. Celem artykułu jest przedstawienie niektórych problemów związanych z określaniem wymaganego SIL (*safety integrity level*) projektowanej funkcji bezpieczeństwa i jego weryfikacją dla rozważanych architektur systemu E/E/PE.

Słowa kluczowe: analiza ryzyka, modelowanie probabilistyczne, poziom nienaruszalności bezpieczeństwa.

Risk Analysis and probabilistic modelling based on knowledge in designing and operation of the programmable control and protection systems

Abstract

In this paper the selected issues associated with the design and operation of the programmable control and protection systems are presented. They are more and more often implemented as electrical/electronic and programmable electronic systems (E/E/PE) according to a functional safety concept, described in the generic international standard IEC 61508 and some sectorial standards. The aim of this paper is outlining some issues related to determining required safety integrity level (SIL) of designed safety related function and verifying SIL for considered architectures of the E/E/PE system.

Keywords: risk analysis, probabilistic modeling, safety integrity level.

1. Wstęp

Zagadnienia projektowania i użytkowania systemów E/E/PE, aby spełniały one określone wymagania dotyczące niezawodności i bezpieczeństwa, przedstawia norma międzynarodowa IEC 61508 [1] o charakterze ogólnym. Powstają również sektorowe normy bezpieczeństwa funkcjonalnego, które uwzględniają specyfikę danego sektora, np. przemysłu procesowego [2], przemysłu maszynowego, transportu kolejowego i innych sektorów.

Niniejszy artykuł poświęcono wybranym zagadnieniom związanym z projektowaniem i użytkowaniem programowalnych systemów sterowania i zabezpieczeń. Przedstawia się metodę określania wymaganego poziomu SIL dla analizowanych funkcji bezpieczeństwa oraz metodę jego weryfikacji dla rozważanych architektur systemu E/E/PE. Zarządzanie bezpieczeństwem funkcjonalnym przeprowadza się w całym cyklu życia systemu. Analiza bezpieczeństwa wymaga korzystania z różnych źródeł informacji i wiedzy specjalistycznej w tym opinii ekspertów.

2. Analiza ryzyka i określanie wymaganego poziomu nienaruszalności bezpieczeństwa

Ryzyko związane z eksploatacją złożonego obiektu technicznego definiuje się zwykle jako możliwość (prawdopodobieństwo lub częstość) wystąpienia potencjalnych zdarzeń awaryjnych i strat wynikających z tych zdarzeń. Miarę ryzyka dla danego systemu technicznego wyznacza się na podstawie zbioru trójek [3]:

$$\Re = \{< S_k, F_k, N_k >\} \tag{1}$$

gdzie: S_k oznacza potencjalne *k*-te zdarzenie awaryjne (rozważa się zbiór scenariuszy awaryjnych), F_k jest częstością *k*-tego scenariusza (prawdopodobieństwo wystąpienia zdarzenia awaryjnego na jednostkę czasu, np. na rok [a^{-1}]), N_k oznacza niekorzystny skutek dla *k*-tego scenariusza, czyli szacowaną szkodę lub stratę, jak np. szacowane potencjalne obrażenia i/lub zejścia śmiertelne, skalę skażenia środowiska lub wielkość strat majątkowych (ekonomicznych).

Miarą ryzyka społecznego (grupowego) *R* związanego z potencjalnymi zdarzeniami awaryjnymi może być przeciętna strata, wyznaczana w jednostkach straty na rok

$$R = \sum_k F_k N_k \tag{2}$$

gdzie: F_k – częstość k-tego scenariusza awaryjnego [a^{-1}], N_k – prognozowana strata w wyniku *k*-tego scenariusza awaryjnego, np. oszacowana liczba poszkodowanych [*osób*] lub sumaryczne straty ekonomiczne wyrażane w jednostkach monetarnych [*zł*] lub [*$*].

Uzyskane oszacowania ryzyka indywidualnego [3] lub ryzyka społecznego ocenia się odpowiednio względem wartości lub funkcji kryterialnych i podejmuje decyzje mające na celu utrzymywanie racjonalnego poziomu ryzyka [4]. Stosuje się w tym celu m.in. zasadę ALARP (*as low as reasonably practicable*) [5]. Miarę ryzyka społecznego wyznacza się na podstawie tzw. matrycy ryzyka, służącej m.in. do wyznaczenia krzywej F-N, czyli dystrybuanty dopełniającej CCDF (*complementary cumulative distribution function*). Jest ona przedstawiana w podwójnie logarytmicznym układzie współrzędnych F i N. Proponuje się odpowiednie linie kryterialne ryzyka w takim układzie współrzędnych [4].

Poniżej rozważa się zmniejszenie ryzyka po wprowadzeniu tzw. opcji sterowania ryzykiem (OSR), względem opcji bazowej (B) [3]. Jedną z takich opcji może być zastosowanie systemów E/E/PE [1] lub SIS (*safety instrumented system*) [2], pełniących funkcje związane z bezpieczeństwem. Redukcję ryzyka w wyniku zmniej-

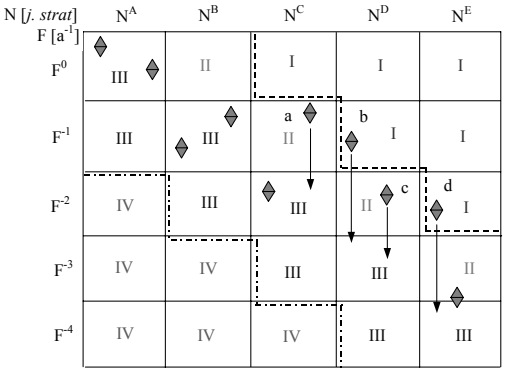
szenia częstości zdarzeń awaryjnych i/lub ich skutków oblicza się wówczas ze wzoru [3]

$$\Delta R^{OSR} = \sum_k F_k^B N_k^B (1 - r_k^{F;OSR} r_k^{N;OSR}) \quad (3)$$

gdzie: F_k^B, N_k^B - częstość [a^{-1}] i strata [*jedn. straty*] w wyniku *k*-tego scenariusza awaryjnego dla opcji bardziej B; $r_k^{F;OSR}$ - względna redukcja częstości *k*-tego scenariusza awaryjnego po wprowadzeniu OSR ($r_k^{F;OSR} = F_k^{OSR} / F_k^B$); $r_k^{N;OSR}$ - względne zmniejszenie straty związanej z *k*-tym scenariuszem awaryjnym po wprowadzeniu OSR ($r_k^{N;OSR} = N_k^{OSR} / N_k^B$); ΔR^{OSR} ma wymiar [*jedn. straty/rok*].

Łatwo zauważyć, że redukcja ryzyka określana w normie [1] metodą ilościową jest szczególnym przypadkiem wzoru (3), jeśli przyjąć, że uwzględnia się tylko jeden scenariusz awaryjny ($k = 1$) i zakłada się, że $r^{N;OSR} = 1$, czyli zastosowanie danej opcji redukcji ryzyka nie wpływa na poziom skutków zdarzenia awaryjnego (*N*), a jedynie na zmniejszenie jego częstości (*F*), $r^{F;OSR} << 1$.

Wyniki oszacowań ryzyka dla danego obiektu i uwzględnionych w analizie scenariuszy awaryjnych można przedstawić w matrycy ryzyka jak na rys. 1. Wyróżniono w tej matrycy 5 kategorii przedziałów częstości $F^0 \div F^4$ i 5 przedziałów skutków potencjalnych awarii $N^A \div N^E$. Kategorie umożliwiają klasyfikowanie wyników analizy ryzyka. Opis kategorii częstości zdarzeń i kategorii ich skutków z podaniem przykładowych wartości podano w tablicy 1.



Rys. 1. Ilustracja wyników analizy ryzyka przykładowego obiektu złożonego
Fig. 1. Illustration of the risk analysis results for given complex object

Tab. 1. Opis przyjętych kategorii częstości zdarzeń awaryjnych i kategorii ich skutków
Tab. 1. Description of assumed categories of accident frequencies and categories of consequences

Kategorie częstości zdarzenia	F^{-4}	F^{-3}	F^{-2}	F^{-1}	F^0
Określenie słowne kategorii częstości	Rzadkie	Mało prawdopodobne	Sporadyczne	Prawdopodobne	Częste
Przykładowe przedziały wartości [a^{-1}]	(10^{-5}, 10^{-4}]	(10^{-4}, 10^{-3}]	(10^{-3}, 10^{-2}]	(10^{-2}, 10^{-1}]	(10^{-1}, 10^{0}]
Kategorie skutku zdarzenia	N^A	N^B	N^C	N^D	N^E
Określenie słowne kategorii skutku	Marginalne	Małe	Duże	Krytyczne	Katastroficzne
Orientacyjna liczba poszkodowanych	Pojedyncze obrażenia	Liczne obrażenia	Pojedyncze zejście	Kilka zejść	Więcej niż kilka zejść

Na rys. 1 wyróżniono również cztery kategorie ryzyka potencjalnych zdarzeń awaryjnych:

I – ryzyko niedopuszczalne, którego nie można tolerować ze względu na stosunkowo dużą częstość zdarzenia awaryjnego i jego skutki,

II – ryzyko niepożądane, które należy redukować zgodnie z zasadą ALARP,

III – ryzyko tolerowane, jeśli koszt zmniejszenia ryzyka jest nieproporcjonalnie duży na jednostkę osiągniętych efektów, oraz

IV – ryzyko akceptowane (pomijalne).

Zaznaczone na rys. 1 punkty (F_k,N_k) odpowiadają kolejnym scenariuszom awaryjnym, które zostały zidentyfikowane w analizie ryzyka rozważanego obiektu złożonego. Jak widać w obszarach ryzyka niedopuszczalnego i niepożądanego znajdują się cztery punkty, oznaczone kolejnymi literami a, b, c, d według skutków. Jeśli przyjąć, w takiej analizie ryzyka nie uwzględniono systemów zabezpieczeniowych E/E/PE lub SIS realizujących określone funkcje bezpieczeństwa, to po ich wprowadzeniu nastąpi redukcja częstości F_k danego scenariusza awaryjnego w kierunku wskazanym strzałkami (założono pesymistyczne, że wprowadzenie systemu zabezpieczeniowego nie będzie powodować zmniejszenia skutku awarii N_k). Jak widać, należy zająć się przede wszystkim scenariuszami b oraz d, ponieważ znajdują się one w obszarze ryzyka niedopuszczalnego. Celowa jest redukcja ich częstości co najmniej 10 razy, a najlepiej 100 razy, co odpowiada wprowadzeniu systemu zabezpieczeniowego z poziomem nienaruszalności bezpieczeństwa 2 (SIL2). Punkty a oraz c leżą w obszarze ryzyka niepożądanego. W tych przypadkach należy wprowadzić system E/E/PE lub SIS charakteryzujący się co najmniej SIL1. Dla punktów znajdujących się w obszarze III należy przeprowadzić analizę ALARP.

Podejście opisane powyżej odpowiada metodzie ilościowej określania SIL systemu zabezpieczeń E/E/PE w normie generycznej [1]. Wymagania bezpieczeństwa funkcjonalnego mogą obejmować nie tylko system zabezpieczeń, ale również system sterowania BPCS (*basic process control system*), który powinien na przykład spełniać wymagania na poziome SIL1 [2]. W takim przypadku w analizie bezpieczeństwa funkcjonalnego należy uwzględniać również czynniki ludzkie i przeprowadzać analizę warstw zabezpieczeniowych, typu LOPA (*layer of protection analysis*) [2, 6, 7].

Tak więc, jeśli obiekt stwarza ryzyko na poziomie nieakceptowanym, ryzyko określonych scenariuszy awaryjnych musi zostać zredukowane do poziomu akceptowanego. Warunkiem koniecznym jest zredukowanie tego ryzyka do poziomu tolerowanego. Przy założeniu, że redukcję ryzyka do poziomu tolerowanego można uzyskać dzięki zastosowaniu systemu zabezpieczeń E/E/PE lub SIS otrzymuje się wzór na względną redukcję ryzyka r^R:

$$r^R = R_t / R_{np} \quad (4)$$

gdzie: R_{np} - ryzyko bez odpowiedniego zabezpieczenia; R_t - ryzyko tolerowane, przy czym przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez dany system zabezpieczeniowy na przywołanie P_{FDavg} powinno spełniać relację

$$P_{FDavg} \le F_t / F_{np} = r^F \quad (5)$$

gdzie: F_{np} - częstość zdarzenia z poziomem skutków N przed wprowadzeniem rozważanego zabezpieczenia; F_t - częstość potencjalnego zdarzenia awaryjnego, wynikająca z poziomu ryzyka R_t po wprowadzeniu tego zabezpieczenia, przy założeniu tych samych skutków N ($R_t = F_t N$); r^F - względna redukcja częstości

zdarzenia po zastosowaniu układu E/E/PE lub SIS jako dodatkowego zabezpieczenia.

Na podstawie obliczonej w ten sposób wartości P_{FDavg} określa się wymagany poziom SIL układu E/E/PE lub SIS [1, 2].

W analizie bezpieczeństwa funkcjonalnego istotne znaczenie ma więc określenie wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla obiektu (instalacji) podwyższonego ryzyka, a następnie zaprojektowanie takiego systemu zabezpieczeniowego, który spełni odpowiednie kryterium probabilistyczne. Badanie mające na celu wykazanie, że system zabezpieczeniowy spełnia wymagania określonego poziom SIL w procesie modelowania probabilistycznego nazywa się jego weryfikacją.

3. Weryfikacja poziomu nienaruszalności bezpieczeństwa SIL metodą ilościową

Model probabilistyczny projektowanego systemu można zbudować wykorzystując np. metodę grafu Markowa. W przypadku złożonych struktur bardziej efektywne staje się wykorzystanie techniki cięć minimalnych. Wówczas prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez system zabezpieczeń można określić na podstawie zależności:

$$P_{FD}(t) \approx \sum_{j=1}^{n} Q_j(t) \approx \sum_{j=1}^{n} \prod_{i \in K_j} q_i(t) \approx \sum_{j=1}^{n} \prod_{i \in K_j} \lambda_i \cdot t \qquad (6)$$

gdzie: $Q_j(t)$ - prawdopodobieństwo wystąpienia j – tego cięcia minimalnego w funkcji czasu; $q_i(t)$ - prawdopodobieństwo uszkodzenia i – tego elementu; λ_i - intensywność uszkodzeń i – tego elementu.

Wykorzystując zależność (6) oraz zakładając, że intensywność uszkodzeń λ odnosi się do uszkodzeń niebezpiecznych można określić przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie:

$$P_{FD\,avg} \approx \frac{1}{T_I} \int_0^{T_I} P_{FD}(t)dt \qquad (7)$$

gdzie: T_I - czas między testami okresowymi, mającymi na celu wykrycie uszkodzeń niebezpiecznych [1].

Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę określa wzór [8]:

$$P_{FH} \approx \frac{\sum_{j=1}^{n}(1-\sum_{\substack{i=1 \\ i\neq j}}^{n} Q_j(t))(\sum_{j\in K_j} \frac{Q_j(t)}{q_i(t)}(1-q_i(t))\lambda_i)}{1-\sum_{j=1}^{n}\prod_{i\in K_j} q_i(t)} \qquad (8)$$

Na podstawie wzorów (6÷8) można wyznaczyć różne miary probabilistyczne [8]. Na przykład, przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie dla systemu o strukturze 1 z 2 określa zależność:

$$P_{FDavg1z2} \approx [(1-\beta)\lambda_D]^2(\frac{T_I^2}{3} + T_I MTTR + MTTR^2) + \beta\lambda_{DU}(\frac{T_I}{2} + MTTR) \qquad (9)$$

gdzie: T_I - czas między testami; $MTTR$ - średni czas naprawy; β - współczynnik uszkodzeń zależnych; λ_D - intensywność uszkodzeń niebezpiecznych; λ_{DU} - intensywność uszkodzeń niebezpiecznych niewykrywalnych przez testy diagnostyczne.

Obliczenia dla danego systemu wykonano na podstawie danych z tab. 2, a wyniki ujęto w tab. 3. Jak widać duży wpływ na obliczenia ma wartość współczynnika uszkodzeń zależnych β.

Tab. 2. Dane niezawodnościowe dla danego systemu
Tab. 2. Reliability data for given system

Parametr	Podsystem pomiarowy (czujnik ciśnienia PS)	Podsystem przetwarzania danych (sterownik PLC)	Podsystem wykonawczy (zawór Z)
λ [1/h]	$5 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-4}$
T_I [rok]	1	1	1
$MTTR$ [h]	8	8	8
DC [%]	70	90	70

Tab. 3. P_{FDavg} dla różnych współczynników β w systemie E/E/PE z redundancją
Tab. 3. P_{FDavg} for different β factors for a redundant E/E/PE system

Podsystem	P_{FDavg}		
	$\beta = 0$	$\beta = 0.05$	$\beta = 0.1$
PS (1 z 2)	$1.46 \cdot 10^{-3}$	$3.06 \cdot 10^{-3}$	$4.66 \cdot 10^{-3}$
PLC (1 z 1)	$2.23 \cdot 10^{-3}$	$2.23 \cdot 10^{-3}$	$2.23 \cdot 10^{-3}$
Z (1 z 2)	$5.8 \cdot 10^{-3}$	$8.96 \cdot 10^{-3}$	$1.207 \cdot 10^{-2}$
System	$9.49 \cdot 10^{-3}$	$1.425 \cdot 10^{-2}$	$1.896 \cdot 10^{-2}$
SIL	2	1	1

W modelach probabilistycznych służących do weryfikacji określonych wymagań poziomów SIL dla systemów sterowania lub zabezpieczeń istotną rolę odgrywają dane niezawodnościowe. W wielu przypadkach przyjmuje się wartości przeciętne i otrzymuje się punktowe wartości prawdopodobieństw P_{FDavg} dla pracy systemu na przywołanie lub P_{FH} dla systemu pracującego w sposób ciągły [1]. Brak wiarygodnych danych niezawodnościowych oraz jednoznacznych zasad w przyjmowaniu wartości współczynnika uszkodzeń zależnych podsystemów β oraz pokrycia diagnostycznego DC elementów powoduje, że otrzymane wartości punktowe obarczone są niepewnością i przedstawiane np. poprzez dolną, środkową i górną wartość prawdopodobieństw P_{FDavg} lub P_{FH}.

Na rys. 2 przedstawiony został przykład weryfikacji SIL dla pracy systemu E/E/PE na przywołanie z uwzględnieniem niepewności danych niezawodnościowych. Celem przeprowadzenia weryfikacji z uwzględnieniem niepewności dotyczącej P_{FDavg} wprowadzono dodatkowe miary w postaci wskaźników różnicowych [8]. Wskaźnik różnicowy górny określa zależność:

$$w_R^g = \mu_{SIL}^d(P_{FDavg}^g) - \mu_{SIL}^g(P_{FDavg}^g) \qquad (10)$$

Wskaźnik różnicowy dla wartości P_{FDavg} przedstawia zależność:

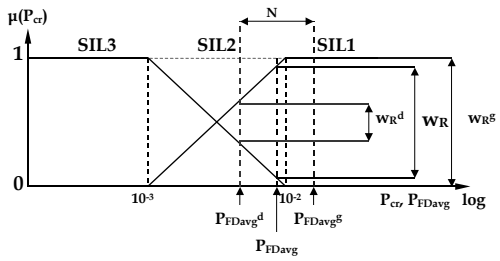
$$w_R = \mu_{SIL}^d(P_{FDavg}) - \mu_{SIL}^g(P_{FDavg}) \qquad (11)$$

Natomiast wskaźnik różnicowy dolny można wyznaczyć korzystając z zależności:

$$w_R^d = \mu_{SIL}^d(P_{FDavg}^d) - \mu_{SIL}^g(P_{FDavg}^d) \qquad (12)$$

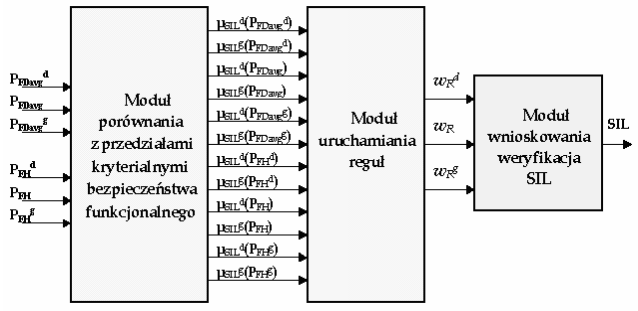
Na podstawie modelu probabilistycznego przykładowego systemu uzyskano punktową wartość przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie $P_{FD\,avg} = 9.49 \cdot 10^{-3}$ (dla $\beta = 0$). Przyjmując, że parametry niezawodnościowe modelu są obarczone niepewnością oszacowano wskaźnik $EF = 2$ (zastosowano rozkład logarytmo - normalny) [8]. Spowodowało to oszacowanie dolnej $P_{FDavg}^d = 4.75 \cdot 10^{-3}$ i górnej $P_{FDavg}^g = 1.9 \cdot 10^{-2}$ granicy względem punktowej wartości

przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie (rys. 2). Znając wartość punktową P_{FDavg}, dolną P^d_{FDavg} oraz górną P^g_{FDavg}, wykorzystując rozmyte przedziały kryterialne [8] dla poziomu SIL2, wyznacza się wskaźniki różnicowe: dolny, środkowy i górny, korzystając z zależności (10), (11) i (12) [8].



Rys. 2. Weryfikacja SIL z uwzględnieniem niepewności wyników modelowania probabilistycznego
Fig. 2. Verification of SIL level with regard to uncertainty of probabilistic modelling results

Dysponując wskaźnikami różnicowymi można weryfikować SIL na podstawie modelu probabilistycznego, w warunkach niepewności korzystając z modułu obliczeniowego i modułu wnioskowania przedstawionego na rys. 3.



Rys. 3. Moduł obliczeniowy i moduł wnioskowania do weryfikacji SIL [8]
Fig. 3. Calculation module and inference module for SIL level verification

Moduł wnioskowania do weryfikacji poziomów nienaruszalności bezpieczeństwa SIL w oparciu o wskaźniki różnicowe wykorzystuje zestaw dziesięciu reguł [8].

W rozpatrywanym przypadku wskaźnik różnicowy oraz wskaźniki różnicowe dolny i górny oblicza się następująco:

$$w_R^d = \mu_{SIL}^d(P_{FDavg}^d) - \mu_{SIL}^g(P_{FDavg}^d) = 0.38 - 0.62 = -0.24 \Rightarrow w_R^d < 0$$
$$w_R = \mu_{SIL}^d(P_{FDavg}) - \mu_{SIL}^g(P_{FDavg}) = 0.03 - 0.87 = -0.84 \Rightarrow w_R < 0$$
$$w_R^g = \mu_{SIL}^d(P_{FDavg}^g) - \mu_{SIL}^g(P_{FDavg}^g) = 0 - 1 = -1 \Rightarrow w_R^g = -1$$

zatem na podstawie jednej z reguł wykorzystywanej przez system weryfikacji

$$w_R^d < 0 \wedge w_R < 0 \wedge w_R^g = -1 \Rightarrow SIL(X-1)$$

rozpatrywany system automatyki zabezpieczeniowej nie spełnia wymagań SIL2, natomiast spełnia wymagania na poziomie SIL1.

W licznych przypadkach analiza ryzyka jest utrudniona z powodu dużej złożoności obiektu, albo braku lub niekompletności danych niezbędnych w modelowaniu probabilistycznym. Dotyczy to zwłaszcza nowoprojektowanych obiektów wraz z ich układami sterowania i zabezpieczeń. Trudności sprawia też uwzględnianie w analizie ryzyka czynników ludzkich i organizacyjnych w analizie ryzyka, które jak wiadomo istotnie wpływają na bezpieczeństwo systemów technicznych. Analizy mogą być wówczas jedynie przybliżone i wykorzystywać oprócz danych z różnych źródeł, również informację o charakterze jakościowym, pozyskaną od ekspertów. W takich przypadkach uzasadnione jest posługiwanie się w analizie ryzyka kategoriami, a ocenę ryzyka i określenie wymaganego SIL dla systemu E/E/PE lub SIS przeprowadza się metodą jakościową za pomocą grafu ryzyka [1, 2]. Weryfikację wymaganego poziomu SIL przeprowadza się wówczas również metodą jakościową, stosując metodę zwijania schematów blokowych niezawodnosci [1].

4. Podsumowanie

System sterowania w obiekcie podwyższonego ryzyka może być systemem związanym z bezpieczeństwem i powinien być on wówczas projektowany zgodnie z wymaganiami bezpieczeństwa funkcjonalnego, podobnie jak system automatyki zabezpieczeniowej [1, 2].

Podczas przeprowadzania analiz bezpieczeństwa korzysta się z szeroko rozumianej wiedzy technicznej i interdyscyplinarnej, o charakterze ogólnym i szczególnym oraz metod bazujących na informacji ilościowej i jakościowej. Artykuł poświęcono wybranym aspektom metodycznym rozwiązywania problemów w ramach zintegrowanych analiz bezpieczeństwa. Istotne znaczenie dla oceny ryzyka ma przyjmowanie akceptowanych poziomów ryzyka, co wpływa na poziom nienaruszalności bezpieczeństwa systemów E/E/PE lub SIS, a w konsekwencji na projekt ich architektury sprzętowej. Zarządzanie bezpieczeństwem przeprowadza się w cyklu życia z uwzględnieniem odpowiedniej strategii testowania i obsługi profilaktycznej podsystemów. W artykule wykorzystano najnowsze wyniki badań prowadzonych przez autorów.

5. Literatura

[1] IEC 61508:1998: Functional safety of electrical/ electronic/ programmable electronic safety-related systems, Parts 1-7. International Electrotechnical Commission (IEC), 1998.
[2] IEC 61511:2000: Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1-3. International Electrotechnical Commission.
[3] Kosmowski K.T.: Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych. Monografie 33. Politechnika Gdańska, 2003.
[4] Kosmowski K.T.: Functional safety concept for hazardous systems and new challenges, Journal of Loss Prevention in the Process Industries 19(2006) pp. 298/305, 2006.
[5] Kosmowski K.T., Śliwiński M.: Methodology for functional safety assessment, ESREL, Tri City, 2005.
[6] AIChE: Layers of Protection Analysis – Simplified Process Risk Assessment. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York 2001.
[7] AIChE: Guidelines for Safe Automation of Chemical Processes, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York 1993.
[8] Śliwiński M.: Metody analizy systemów sterowania i zabezpieczeń z uwzględnieniem kryteriów bezpieczeństwa funkcjonalnego. Politechnika Gdańska, 2006.

Artykuł recenzowany