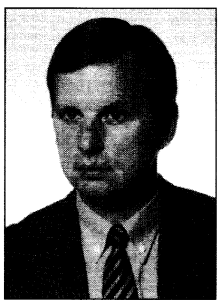
Kazimierz T. KOSMOWSKI, Maciej KOZYRA, Marcin ŚLIWIŃSKI
POLITECHNIKA GDAŃSKA, WYDZIAŁ ELEKTROTECHNIKI I AUTOMATYKI, KATEDRA AUTOMATYKI

Ocena bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń

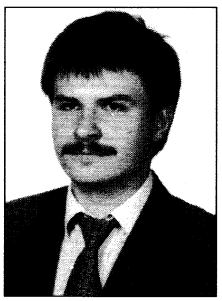
Dr inż. Kazimierz T. KOSMOWSKI



W 1972 ukończył studia Wyższe na Wydziale Elektrycznym Politechniki Gdańskiej. W roku 1981 uzyskał stopień doktora nauk technicznych w zakresie elektrotechniki. Od 1981 roku pracuje na stanowisku adiunkta w Katedrze Automatyki Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej. Prowadzi badania z zakresu niezawodności i bezpieczeństwa systemów, niezawodności człowieka, systemów z bazą wiedzy oraz komputerowych systemów wspomagania decyzji. Jest członkiem zarządu Polskiego Towarzystwa Bezpieczeństwa i Niezawodności.

kazkos@ely.pg.gda.pl

Mgr inż. Marcin ŚLIWIŃSKI



W 2001 roku ukończył studia na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej. Od 2001 roku jest doktorantem w Katedrze Automatyki Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej. Przygotowuje rozprawę doktorską nt. „Metodyka projektowania systemów sterowania z uwzględnieniem bezpieczeństwa funkcjonalnego".

msgdw@wp.pl

Streszczenie

W niniejszym artykule przedstawia się wybrane zagadnienia związane z oceną bezpieczeństwa funkcjonalnego w nawiązaniu do normy międzynarodowej IEC 61508. Podkreśla się znaczenie ilościowego modelowania probabilistycznego systemów elektrycznych, elektronicznych i programowalnych elektronicznych (E/E/PE). Ilustruje się wyznaczanie poziomu nienaruszalności bezpieczeństwa dla dwóch przykładowych systemów sterowania i zabezpieczeń. Podkreśla się również znaczenie założeń i wartości parametrów przyjmowanych w analizach. W związku z kłopotami interpretacyjnymi i trudnościami stosowania normy IEC 61508 podkreśla się znaczenie opracowania zasad przewodnich, które ułatwią wdrażanie racjonalnych ekonomiczne rozwiązań bezpieczeństwa funkcjonalnego w praktyce.

Abstract

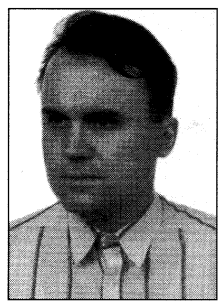
In this paper selected issues related to functional safety assessment in relation to international standard IEC 61508 are presented. The significance of quantitative probabilistic modelling of electrical, electronic, programmable electronic (E/E/PE) systems is emphasised. Determining the safety integrity level of control and protection systems is illustrated on two examples. The meaning of assumptions and values of parameters in analyses is also emphasised. Due to difficulties in interpreting and using the standard IEC 61508, the significance of elaborating the guiding principles that will make easier to develop economically rational solutions of functional safety in practice is emphasised.

Słowa kluczowe: bezpieczeństwo funkcjonalne; niezawodność; systemy elektryczne, elektroniczne i elektroniczne programowalne; systemy sterowania i zabezpieczeń
Keywords: functional safety; reliability; electrical, electronic and programmable electronic systems; control and protection systems

1. Wprowadzenie

Systemy komputerowe są stosowane od wielu lat w różnych obszarach techniki do wypełniania różnorakich funkcji wspomagania decyzji i / lub sterowania. Pod koniec lat 80-tych wzrosło wyraźnie zainteresowanie powierzaniem systemom komputerowym, w tym systemom zawierających jednostki programowalne, również funkcji związanych z bezpieczeństwem. Obecnie systemy zawierające elementy elektryczne, elektroniczne i programowalne elektroniczne (E/E/PE) są coraz szerzej stosowane do wypełniania różnych funkcji bezpieczeństwa w rozmaitych obszarach techniki i innych zastosowań [1, 9, 11].

Inż. Maciej KOZYRA



W 1994 roku ukończył studia Wyższe na Wydziale Elektrycznym Wyższej Szkoły Morskiej w Gdyni. Od 1989 roku pracuje na Politechnice Gdańskiej, obecnie na stanowisku starszego specjalisty w Katedrze Automatyki Wydziału Elektrotechniki i Automatyki. Aktywnie współpracuje z przemysłem w dziedzinie diagnostyki przemysłowej i automatyzacji procesów przemysłowych.

mkozyra@ely.pg.gda.pl

Ukazuje się coraz więcej referatów i artykułów na temat różnych aspektów bezpieczeństwa funkcjonalnego [1, 2, 4, 6, 7, 10, 15]. Wskazuje się jednak dość często na pewne trudności związane z interpretowaniem i stosowaniem w praktyce normy IEC 61508. W niniejszym referacie sygnalizuje się problemy związane z określaniem poziomu nienaruszalności bezpieczeństwa SIL (*Safety Integrity Level*). Przyjęty poziom SIL, liczba od 1 do 4, implikuje ilościowe kryteria probabilistyczne na niewypełnienie przez system E/E/PE funkcji bezpieczeństwa.

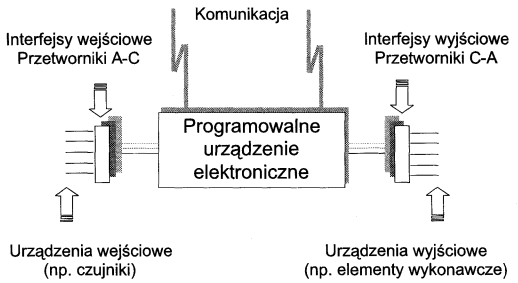
Postuluje się uwzględnianie w tych analizach oceny czynników ludzkich i organizacyjnych, które zwykle istotnie wpływają na wyniki modelowania probabilistycznego i analizy ryzyka systemów związanych z bezpieczeństwem [5].

2. Norma międzynarodowa IEC 61508

2.1. Podstawowe terminy dotyczące bezpieczeństwa funkcjonalnego

Poniżej zestawiono wybrane pojęcia i określenia dotyczące oceny bezpieczeństwa [11]:
Ryzyko - kombinacja prawdopodobieństwa wystąpienia szkody i ciężkości tej szkody.
Ryzyko tolerowane - ryzyko, które jest akceptowane w określonym kontekście, opartym na aktualnych wartościach społecznych.
Ryzyko resztkowe - ryzyko pozostające po zastosowaniu środków bezpieczeństwa.
Bezpieczeństwo - nie występowanie ryzyka nieakceptowanego.
Bezpieczeństwo funkcjonalne - część bezpieczeństwa całkowitego, odnosząca się do wyposażenia sterowanego (*EUC - equipment under control*) i systemu sterowania EUC, która zależy od prawidłowego działania systemów E/E/PE (*elektrycznych / elektronicznych / programowalnych elektronicznych*) związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem wykonanych w innych technikach i zewnętrznych środków zmniejszenia ryzyka.
Poziom nienaruszalności bezpieczeństwa (*SIL - safety integrity level*) poziom dyskretny (jeden z czterech możliwych) do wyszczególnienia wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które mają być alokowane w systemach E/E/PE związanych z bezpieczeństwem.

Rys. 1 przedstawia schemat typowego programowalnego systemu elektronicznego (PES) według normy IEC 61508, współpracującego z urządzeniami wejściowymi, wyjściowymi i pomocniczymi.

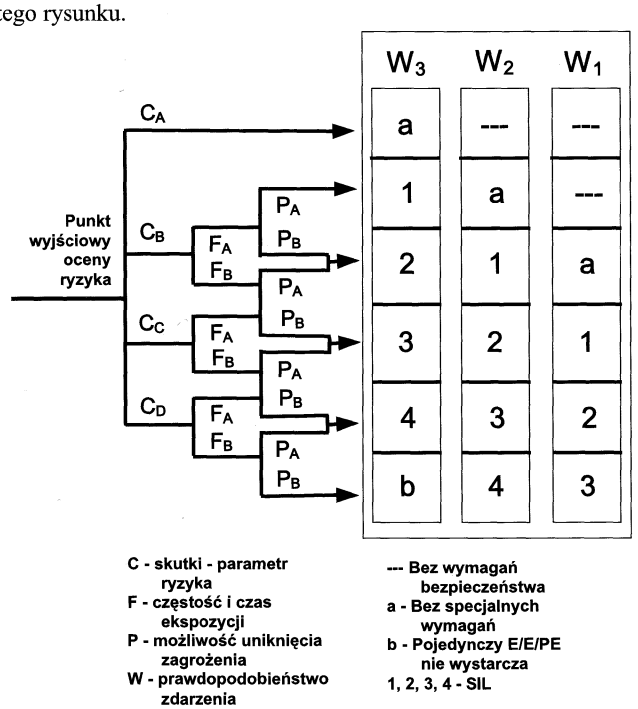


Rys. 1. Programowalny system elektroniczny
Fig. 1. Programmable electronic system

Należy podkreślić, że zarządzanie bezpieczeństwem w systemach technicznych zgodnie z normą IEC 61508, polegające na ocenie możliwości zmniejszania ryzyka, obejmuje nie tylko układy E/E/PE, ale również inne środki zmniejszania ryzyka.

2.2. Wymagania dla systemów E/E/PE i ocena rozwiązań projektowych

W analizie bezpieczeństwa systemu kluczowe znaczenie ma określenie poziomu nienaruszalności bezpieczeństwa SIL (*safety integrity level*). Zgodnie z normą IEC 61508 poziom SIL można określać metodą ilościową i metodą jakościową. W zgrubnej ocenie tego poziomu duże praktyczne znaczenie ma metoda grafu ryzyka o charakterze jakościowym. Sugerowany w normie IEC 61508 do tego celu graf znajduje się na rys. 2. Poziom SIL przy takim podejściu zależy od czterech parametrów C, F, P i W, które opisano w dolnej części tego rysunku.



Rys. 2. Graf ryzyka według IEC 61508
Fig. 2. Risk graph according to IEC 61508

Poszczególnym poziomom SIL systemu E/E/PE odpowiadają ilościowe kryteria probabilistyczne, które zestawiono w tabeli 1 w kolumnie 2 (rodzaj pracy rzadkiego przywoływania systemu do działania) lub w kolumnie 3 (rodzaj pracy częstego przywoływania systemu do działania lub działania ciągłego). Kolumna trzecia tabeli 1 zawiera przedziały kryterialne dotyczące częstości uszkodzeń niebezpiecznych w systemie. Projektowanie systemów spełniających kryterium SIL3, a szczególnie SIL4, jest w praktyce bardzo trudne i wymaga stosowania struktur nadmiarowych, a także eliminowania w systemie potencjalnych uszkodzeń zależnych.

Tabela. 1. Poziomy nienaruszalności bezpieczeństwa i kryteria probabilistyczne dla systemów związanych z bezpieczeństwem według normy IEC 61508
Table 1. Safety integrity levels and probabilistic criteria for safety-related systems according to IEC 61508

Poziom nienaruszalności bezpieczeństwa SIL	Przeciętne prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie P_{FDavg} (tryb rzadkiego przywołania do działania)	Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę F_{FD} (tryb częstego przywoływania do działania lub działania ciągłego)
4	$[10^{-5}, 10^{-4})$	$[10^{-9}, 10^{-8})$
3	$[10^{-4}, 10^{-3})$	$[10^{-8}, 10^{-7})$
2	$[10^{-3}, 10^{-2})$	$[10^{-7}, 10^{-6})$
1	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

3. Miary probabilistyczne w analizie systemu i ich wyznaczanie

3.1. Miary probabilistyczne stosowane w metodzie FMECA

FMECA (*Failure Mode, Effect and Criticality Analysis*) [13, 14] jest metodą indukcyjną analizy nieuszkadzalności i bezpieczeństwa systemu o stosunkowo małej złożoności, która umożliwia określenie kolejności zdarzeń spowodowanych przez możliwe, w tym wcześniej zidentyfikowane w podobnych systemach, rodzaje uszkodzeń i ich skutki. Niektóre narzędzia komputerowe wspomagające analizę umożliwiają klasyfikację i grupowanie uszkodzeń według możliwości ich wykrycia, przeprowadzenia testów funkcjonalnych, czy też naprawy lub wymiany elementów [8, 13, 14].

Wyniki analizy rodzajów skutków i krytyczności uszkodzeń obejmują oszacowania miar probabilistycznych. Jedną z nich jest parametr β, oznaczajacy prawdopodobieństwo warunkowe wystąpienia wyróżnionego skutku końcowego zdarzenia krytycznego, zgodnie z przyjętą klasyfikacją krytyczności, pod warunkiem wystąpienia danego rodzaju uszkodzenia. Następnym parametrem, ocenianym w analizie krytyczności, jest współczynnik rodzaju uszkodzenia α definiowany jako iloraz

$$\alpha_k = \frac{\lambda_k}{\lambda_p} \tag{1}$$

gdzie: λ_k - intensywność uszkodzeń danego rodzaju, λ_p - całkowita intensywność uszkodzeń badanego podsystemu

Gdy rozpatrywane są wszystkie potencjalne rodzaje uszkodzeń danego podsystemu, wówczas suma wartości α_k będzie równa 1. Intensywność uszkodzeń podsystemu λ_p szacuje się, jeśli to tylko możliwe, na podstawie danych statystycznych dotyczących uszkadzalności podsystemów (urządzeń) danej kategorii, lub na podstawie odpowiedniego przewodnika [12].

Na podstawie analizy krytyczności według standardu [13] wyznacza się tzw. liczbę krytyczności C_m dla danego rodzaju uszkodzenia podsystemu

$$C_m = \beta\alpha\lambda_p t \tag{2}$$

gdzie: β - prawdopodobienstwo warunkowe wystąpienia wyróżnionego skutku końcowego zdarzenia krytycznego, α - współczynnik rodzaju uszkodzenia, λ_p - całkowita intensywność uszkodzeń elementu, oraz t - rozważany czasu trwania misji podsystemu dla szczególnego poziomu krytyczności i rozważanej fazy misji systemu).

W przypadku podsystemów o wysokim poziomie nieuszkadzalnosci, C_m ma znaczenie prawdopodobieństwa wystąpienia danego rodzaju uszkodzenia, a $C_m / t = \beta\alpha\lambda_p$ jest częstością jego wystąpienia (prawdopodobieństwem na jednostkę czasu).

Liczbę krytyczności C_r dla danego podsystemu definiuje się jako

$$C_r = \sum_i (C_m)_i = \sum_{i=1}^{n} (\beta\alpha\lambda_p t)_i \tag{3}$$

gdzie: n - liczba uwzględnionych w analizie rodzajów uszkodzeń.

W przypadku podsystemów o wysokim poziomie nieuszkadzalnosci, C_r ma znaczenie prawdopodobieństwa wystąpienia stanu nienormalnego podsystemu, a C_r/t jest częstością jego wystąpienia (prawdopodobieństwem na jednostkę czasu).

3.2. Miary probabilistyczne w ocenie systemów związanych z bezpieczeństwem

Intensywność uszkodzeń λ [1/h] podsystemów obejmuje uszkodzenia niebezpieczne i uszkodzenia bezpieczne [2, 10]

$$\lambda = \lambda_S + \lambda_D \tag{4}$$

gdzie: λ_S - intensywność uszkodzeń bezpiecznych [1/h], λ_D - intensywność uszkodzeń niebezpiecznych [1/h].

Udział (współczynnik wagowy) *FS* uszkodzeń bezpiecznych definiuje się jako

$$FS = \frac{\lambda_S}{\lambda} \tag{5}$$

Znając intensywność uszkodzeń λ podsystemu i udział uszkodzeń bezpiecznych FS można napisać wzory na częstość uszkodzeń bezpiecznych

$$\lambda_S = FS \cdot \lambda \tag{6}$$

i częstość uszkodzeń niebezpiecznych

$$\lambda_D = (1 - FS) \cdot \lambda \tag{7}$$

Uszkodzenia niebezpieczne podsystemu mogą być wykrywalne (*DD - dangerous detected*) lub niewykrywalne przez automatyczne testy diagnostyczne (*DU - dangerous undetected*). Można więc napisać

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{8}$$

gdzie: λ_{DD} - intensywność uszkodzeń wykrywalnych przez automatyczne testy diagnostyczne, λ_{DU} - intensywność uszkodzeń niewykrywalnych przez automatyczne testy diagnostyczne.

Na podstawie normy IEC 61508 [11] pokrycie diagnostyczne (DC - *diagnostic coverage*) dotyczące podsystemu definiuje się następująco

$$DC = \frac{\lambda_{DD}}{\lambda_D} \tag{9}$$

Uwzględniając (4)÷(9) można napisać wzory na intensywność uszkodzeń niebezpiecznych wykrywalnych przez testy diagnostyczne

$$\lambda_{DD} = DC \cdot \lambda_D = DC(1 - FS) \cdot \lambda \tag{10}$$

i niewykrywalnych przez testy diagnostyczne

$$\lambda_{DU} = (1 - DC) \cdot \lambda_D = (1 - DC)(1 - FS) \cdot \lambda \tag{11}$$

Przy założeniu, że pokrycie diagnostyczne odnosi się również do uszkodzeń bezpiecznych, wprowadzić można pojęcie uszkodzenia bezpiecznego wykrywalnego (*SD - safe detected*)

$$\lambda_{SD} = DC \cdot \lambda_S = DC \cdot FS \cdot \lambda \tag{12}$$

i uszkodzenia bezpiecznego niewykrywalnego (*SU - safe undetected*).

$$\lambda_{SU} = (1 - DC) \cdot \lambda_S = (1 - DC) \cdot FS \cdot \lambda \tag{13}$$

Sumaryczna przeciętna wartość intensywności uszkodzeń podsystemu jest sumą przeciętnych wartości intensywności cząstkowych określonych wzorami (10)÷(13).

$$\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU} \tag{14}$$

Znając wartości tych intensywności można wyznaczyć następujące miary probabilistyczne podsystemów E/E/PE:

(A) przeciętne prawdopodobieństwo P_{FDavg} niewypełnienia zaprojektowanej funkcji realizowanej na przywołanie (w przypadku rodzaju pracy na rzadkie przywołanie);

(B) prawdopodobieństwo niebezpiecznego uszkodzenia na godzinę F_{FD} (w przypadku rodzaju pracy na częste przywołanie lub ciągłego).

(C) częstość uszkodzenia bezpiecznego prowadzącego do nieuzasadnionego zadziałania systemu zabezpieczeń (F_{FS}),

(D) niedyspozycyjność systemu spowodowana uszkodzeniami bezpiecznymi systemu zabezpieczeń (P_{FS}).

Średnie prawdopodobieństwo P_{FDavg} wyznacza się ze wzoru

$$P_{FDavg} \cong P_{FDavg}^{FT} + P_{FD}^{AT} + P_{FD}^{HE} \tag{15}$$

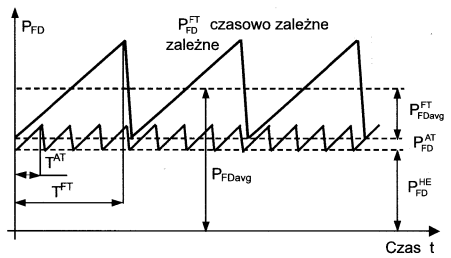
gdzie: P_{FDavg}^{FT} - prawdopodobieństwo niewypełnienia funkcji z powodu uszkodzenia bezpiecznego wykrywanego okresowo podczas sprawdzającego testu funkcjonalnego (*functional test - FT*), P_{FD}^{AT} - prawdopodobieństwo niewypełnienia funkcji związane z naprawą po wykryciu uszkodzenia podsystemu przez test automatyczny (*automatic test - AT*) wykonywany stosunkowo często, P_{FD}^{HE} - prawdopodobieństwo zdarzenia, że podsystem nie wypełni funkcji na przywołanie niezależnie od przeprowadzonych testów wykrywających uszkodzenie sprzętu z powodu błędu człowieka (*human error - HE*).

Przyjęto, że prawdopodobieństwo błędu człowieka ma dwie składowe, dotyczące błędu popełnionego podczas projektowania systemu i błędu operatora przeprowadzającego test funkcjonalny, a mianowicie:

$$P_{FD}^{HE} \cong P_{FD}^{DE} + P_{FD}^{OE} \tag{16}$$

gdzie: P_{FD}^{DE} - prawdopodobieństwo niewypełnienia funkcji z powodu błędu utajonego, popełnionego w czasie projektowania podsystemu (*design error - DE*), P_{FD}^{OE} - prawdopodobieństwo niewypełnienia funkcji z powodu błędu człowieka-operatora (*operator error - OE*), popełnionego podczas przeprowadzania testu funkcjonalnego podsystemu.

Składowe prawdopodobieństwa P_{FDavg} i ich interpretację w przypadkach zależności od interwałów przeprowadzania testu automatycznego (T^{AT}) i testu funkcjonalnego (T^{FT}) przedstawiono na rys. 3.



Rys. 3. Składowe przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa przez podsystem E/E/PE

Fig. 3. Elements of average probability of the E/E/PE subsystem failure on demand

Poniżej zestawiono wzory na wyznaczanie wartości miar probabilistycznych systemów E/E/PE o przykładowych architekturach:

Podsystem 1oo1:

$$P_{FDavg}^{1oo1} \cong \frac{\lambda_{DU} \cdot T^{FT}}{2} + \lambda_{DD} T_{DD} + P_{FD}^{HE} \tag{17}$$

gdzie: T_{DD} - przeciętny czas naprawy / odnowy systemu uszkodzenia niebezpiecznego wykrywalnego przez test automatyczny lub przeprowadzany przez operatora stosunkowo często: $T^{AT} << T^{FT}$ (rys. 3).

$$F_{FD}^{1oo1} \cong \lambda_{DU} \tag{18}$$

$$F_{FS}^{1oo1} \cong \lambda_{SD} + \lambda_{SU} + \lambda_{DD} \tag{19}$$

$$P_{FS}^{1oo1} \cong F_{FS}^{1oo1} T_{FS} \tag{20}$$

gdzie: T_{FS} - średni czas identyfikacji uszkodzenia oraz naprawy i przywrócenia funkcji systemu.

Analiza wykazała, że w wyznaczaniu miar probabilistycznych struktur złożonych dominują uszkodzenia zależne i dlatego uzasadnione jest stosowanie wzorów uproszczonych.

Podsystem 1oo2:

$$P_{FDavg}^{1oo2} \cong (\beta \lambda_{DU} T^{FT})/2 + \beta_C \lambda_{DD} T_{DD} + \beta_H P_{FD}^{HE} \tag{21}$$

gdzie: β_C - współczynnik uszkodzenia zależnego (grupowego) spowodowanego wspólną przyczyną (ang. *common cause failure*),

β_H - współczynnik błędu zależnego człowieka-operatora przeprowadzającego test systemu z redundancją.

$$F_{FD}^{1oo2} \cong \beta_C \lambda_{DU} \quad (22)$$

$$F_{FS}^{1oo2} \cong 2(\lambda_{SD} + \lambda_{SU} + \lambda_{DD}) \quad (23)$$

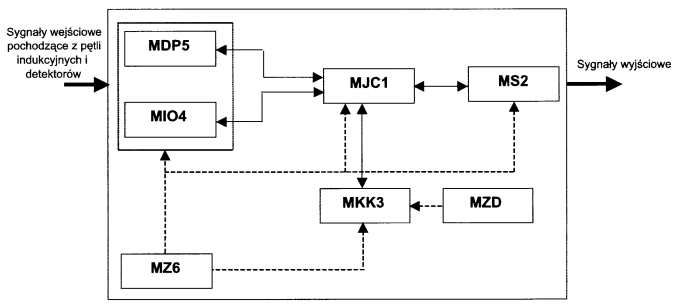
$$P_{FS}^{1oo2} \cong F_{FS}^{1oo2} T_{FS} \quad (24)$$

Postaci wzorów na wymienione powyżej miary probabilistyczne zależą w niektórych przypadkach istotnie od filozofii projektowej systemu i zastosowanych środków diagnostyki podczas eksploatacji [2, 10].

4. Przykłady analizy systemów związanych z bezpieczeństwem

4.1. System sygnalizacji świetlnej

Dla sterownika sygnalizacji świetlnej, przedstawionego na rys. 4, została przeprowadzona analiza FMECA [8, 12]. Sterownik ten jest typowym układem w skład którego wchodzą następujące moduły:
- moduł jednostki centralnej MJC1, realizujący algorytm sterowania i komunikacji z układem lokalnym;
- moduł sterujący MS2, sterujący bezpośrednio obwodami sygnalizatorów oraz nadzorujący ich stan;
- moduł wykrywania „kolizji" MKK3, sprawujący kontrolę nad pracą sterownika;
- moduł wejść i wyjść dwustanowych MIO4n (na przykład wejścia z zewnętrznych detektorów ruchu, sygnałów koordynacji innych sterowników, obsługi przycisków dla pieszych itd.);
- moduł detekcji pojazdów MDP5, służący do wykrywania obecności pojazdów przez pętle indukcyjne;
- zasilacz MZ6, realizujący funkcję w stanie normalnym.



Rys. 4. Przykładowy sterownik sygnalizacji świetlnej
Fig. 4. An example of the light signalling controller

W obliczeniach przyjęto czas trwania misji t=10000 h. W tabeli 2 znajdują się z wyniki z analizy FMECA dla przykładowego sterownika sygnalizacji świetlnej.

Tabela 2. Wyniki analizy FMECA dla przykładowego sterownika sygnalizacji świetlnej
Table 2. Results of the FMECA analysis for an example of light signalling controller

Lp.	Nazwa efektu końcowego	Krytyczność	λ_p [1/10^6 h]	α	λ_k [1/10^6 h]	β
1	Ciągłe światło żółte	I	100.9	0.00867	0.875	0.00871
2	Fałszywy tryb awaryjny	II	100.9	0.29671	29.938	0.25872
3	Niepełne sterowanie sygnalizacji świetlnej	II	100.9	0.20218	20.400	0.18454
4	Całkowity brak kontroli	II	100.9	0.01982	2.000	0.01980
5	Awaryjne żółte światło pulsujące	III	100.9	0.31405	31.687	0.27158
6	Brak koordynacji z pobliskim skrzyżowaniem	IV	100.9	0.15857	16.000	0.14786
Suma				1.000000	100.9	

Z tabeli tej wynika, że najbardziej krytycznym skutkiem końcowym, rozpatrywanego układu sterowania sygnalizacją świetlną, jest ciągłe światło żółte. Poziom krytyczności w tym przypadku wynosi I, natomiast prawdopodobieństwo wystąpienia tego zdarzenia jest stosunkowo niskie i wynosi β=0.00867 przy wartości wskaźnika rodzaju uszkodzenia α=0.00875. Najmniej krytycznym skutkiem końcowym jest brak koordynacji z pobliskim skrzyżowaniem. Stopień krytyczności wynosi dla tego przypadku IV, prawdopodobieństwo wystąpienia skutku końcowego jest stosunkowo wysokie i wynosi β=0.148, a wskaznik rodzaju uszkodzenia α=0.159. Intensywność uszkodzeń dla najbardziej krytycznego skutku końcowego, jakim jest ciągłe światło żółte występujące na skrzyżowaniu, wynosi λ=0.875 [1/(10^6 h)].

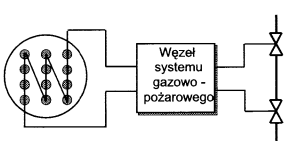
Rozważany sterownik sygnalizacji świetlnej pracuje w sposób ciągły, zatem uzyskany wynik λ=0.875 [1/(10^6 h)] dla najbardziej krytycznego zdarzenia, mieści się w zakresie <10^{-7},10^{-6}), odpowiadającym SIL 2, chociaż jest w pobliżu dolnej granicy tego przedziału, a górnej granicy przedziału odpowiadającemu SIL1.

Przeprowadzana jakościowa ocena ryzyka dla rozważanego systemu wykazała, że system sygnalizacji powinien spełniać kryterium odpowiadające SIL 2. Czyli w zasadzie spełnia on to kryterium. Jednak, biorąc pod uwagę niepewności występujące w oszacowaniach ilościowych, należałoby ocenić spełnienie kryterium probabilistycznego korzystając nie z oszacowań punktowych (zwykle wartości średnie), lecz z metody oszacowań przedziałowych [5]. Jest to tym bardziej uzasadnione, jeśli rozważyć w modelu probabilistycznym systemu potencjalny wpływ czynników technicznych, środowiskowych i ludzkich na system.

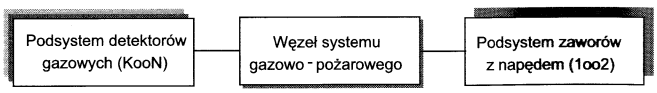
Jak wspomniano, metoda FMECA jest przydatna we wstępnej ocenie bezpieczeństwa funkcjonalnego systemów o stosunkowo małej złożoności. W ocenie bardziej złożonych systemów niezbędne jest korzystanie z zaawansowanych narzędzi komputerowych [8].

4.2. System detekcji gazu

Rozważa się przykładowy system zabezpieczeń przedstawiony schematycznie na rys. 5, a jego schemat blokowy znajduje się na rys. 6.



Rys. 5. Przykładowy system zabezpieczeń
Fig. 5. An example of the protection system



Rys. 6. Schemat blokowy systemu zabezpieczeń
Fig. 6. Block diagram of the protection system

Przeprowadzono analizę porównawczą układu o schemacie blokowym z rys. 6 dla struktury podsystemu detektorów 2oo3, węzła systemu gazowo pożarowego 1oo1 i podsystemu zaworów 1oo2. Dane przyjęte w obliczeniach w nawiązaniu do raportu [4] znajdują się w tablicy 3, a uzyskane wyniki ujęto w tabeli 4.

Jak widać w tabeli 4, uwzględnienie uszkodzeń zależnych z przykładowymi wartościami współczynnika β wpływa istotnie na uzyskane wyniki. Na przykład, dla β=0.05 P_{Fdavg}=0.010, a więc uwzględniając tabelę 1 odpowiada to mniejszej wartości granicznej SIL=1 (0.01), która jest również większą wartością graniczną SIL2. Po uwzględnieniu w modelu prawdopodobieństwa błędu człowieka, uzyskano wartość 0.0136, która odpowiada SIL1.

Uzyskane wyniki świadczą, że założenia dotyczące wartości parametrów modelu probabilistycznego mogą wpływać znacząco na poziom nienaruszalności bezpieczeństwa SIL. Istotna staje się dlatego analiza wrażliwości i niepewności modelu probabilistycznego.

Tabela 3. Dane do obliczeń
Table 3. Data for calculations

Podsystem	λ_D [1/h]	DC	λ_{DD} [1/h]	λ_{DU} [1/h]	T_{DD} [h]	T^{FT} [h]	P^{HE}
Detektory gazowe 2oo3	$3x10^{-6}$	50%	$1.5x10^{-6}$	$1.5x10^{-6}$	8	8760	0.001
Węzeł gazowo-pożarowy 1oo1	$2x10^{-5}$	90%	$1.8x10^{-5}$	$2x10^{-6}$	8	8760	0.003
Zawory z napędem 1oo2	$3x10^{-6}$	0%	0	$3x10^{-6}$	8	8760	0.001

Tabela 4. Wyniki uzyskane dla różnych parametrów modelu probabilistycznego systemu
Table 4. Results obtained for different parameters of the system probabilistic model

Podsystem	P_{FDavg}			P_{Fdavg} (P^{HE})		
	β=0.1	β=0.05	β=0.01	β=0.1	β=0.05	β=0.01
Detektory gazowe 2oo3	0.001975	0.000987	0.000197	0.00207	0.001037	0.000207
Węzeł gazowo-pożarowy 1oo1	0.008900	0.008900	0.008900	0.11900	0.119000	0.119000
Zawory z napędem 1oo2	0.001314	0.000657	0.000131	0.00141	0.000707	0.000141
System	0.012189	0.010544	0.009228	0.0154	0.0136	0.0123

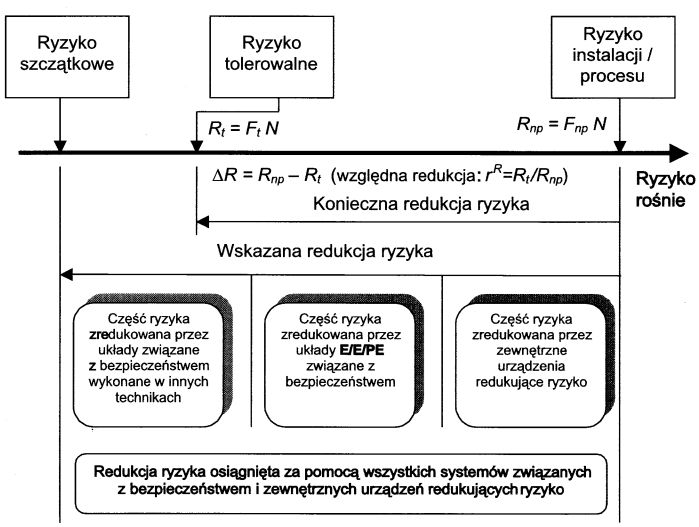
5. Koncepcja redukcji ryzyka wg normy IEC 61508

Na rys. 7 przedstawiono koncepcję redukowania ryzyka według normy 61508. Przy założeniu, że redukcję ryzyka do poziomu tolerowanego można uzyskać dzięki zastosowaniu układu E/E/PE otrzymuje się (dla tego samego poziomu skutków N) wzór na względną redukcję ryzyka

$$r^R = R_t / R_{np} = F_t / F_{np} = r^F = P_{FDavg} \qquad (25)$$

gdzie: R_{np} - ryzyko bez zastosowania środków zabezpieczeniowych, F_{np} - częstość zdarzenia z poziomem skutków N przed wprowadzeniu środka zabezpieczeniowego, R_t - ryzyko tolerowane, F_t - częstość potencjalnego zdarzenia awaryjnego po wprowadzeniu zabezpieczenia (wynikającą z poziomu R_t), r^F - względna redukcja częstości rozważanych zdarzeń.

W monografii [5] przedstawiono metodę oceny opcji sterowania ryzykiem (OSR) na podstawie modelu ryzyka zawierającego wyróżnione kategorie scenariuszy awaryjnych. Jedną z możliwych opcji może być przeprojektowanie systemu E/E/PE związanego z bezpieczeństwem, aby uzyskać wyższy poziom SIL. Należy jednak pamiętać, że dla wyższych poziomów SIL wzrasta częstość zadziałań niepotrzebnych F^{FS}, a więc potencjalnych strat w procesie produkcji.



Rys. 7. Ogólna koncepcja zmniejszania ryzyka według normy IEC 61508
Fig. 7. General concept of the risk reduction according to IEC 61508

6. Wnioski końcowe

Norma IEC 61508 ma rosnące znaczenie w projektowaniu i eksploatacji systemów związanych z bezpieczeństwem. Artykuł poświęcono wybranym aspektom stosowania tej normy w modelowaniu probabilistycznym systemów sterowania i zabezpieczeń oraz wyznaczania poziomów nienaruszalności bezpieczeństwa. Podkreślono znaczenie ilościowego modelowania probabilistycznego systemów elektrycznych, elektronicznych i programowalnych elektronicznych (E/E/PE). Zilustrowano wyznaczanie poziomu nienaruszalności bezpieczeństwa dla dwóch przykładowych systemów sterowania i zabezpieczeń. Podkreślono znaczenie założeń i wartości parametrów przyjmowanych w analizach. W związku z kłopotami interpretacyjnymi i trudnościami stosowania normy IEC 61508 podkreśla się znaczenie opracowania zasad przewodnich, które ułatwią wdrażanie racjonalnych ekonomiczne rozwiązań bezpieczeństwa funkcjonalnego w praktyce.

Literatura

[1] J. Górski: Bezpieczeństwo przemysłowych zastosowań komputerów. Materiały III Krajowej Konferencji Naukowo-Technicznej „Diagnostyka Procesów Przemysłowych" (red. naukowa Z. Kowalczyk), Jurata / Gdańsk, 1998, ss. 201-212.
[2] W. Groble: Using smart transmitters in safety protection applications, Moore Products Co. 1999.
[3] Ch. Kirchsteiger., G. Cojazzi (eds): Promotion of technical harmonization on risk-based decision-making. Proceedings of a Workshop (22-24 May 2000, Stresa, Italy), Parts: 1 & 2, European Commission, DG JRC, Ispra, 2000.
[4] G.K. Hansen, R. Aarř: Reliability quantification of computer-based safety systems. An introduction to PDS. SINTEF Industrial Management. Report No. STF37 A97434. Trondheim, 1997.
[5] K.T. Kosmowski: Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych. Monografie 33. Politechnika Gdańska, 2003.
[6] K.T. Kosmowski: Risk analysis and functional safety assessment with regard to human and organisational factors. SIPI (Safety In the Process Industries): Materiały warsztatów międzynarodowych (ed. M. Dźwiarek, K.T. Kosmowski, T. Missala): Gdynia, 28-29 maja 2003.
[7] T. Kunicki, B. Matus, A. Zabielski: Nowoczesne tendencje w dziedzinie zapewnienia bezpieczeństwa na instalacjach chemicznych. Nowoczesne Gazownictwo 2(VI), 2001.
[8] R. Lezion: Care reliability planning and simulation tools. BQR Reliability Engineering Ltd, 2000.
[9] T. Missala: Seria norm 61508. Wprowadzenie. SIPI (Safety In the Process Industries): Materiały warsztatów międzynarodowych (ed. M. Dźwiarek, K.T. Kosmowski, T. Missala): Gdynia, 28-29 maja 2003.
[10] P. Stavrianidis: Reliability and uncertainty analysis of hardware failures of programmable electronic system. Reliability Engineering and System Safety, 1992
[11] IEC 61508: Functional safety of electrical/electronic/programmable electronic (E/E/PE) safety related systems. Parts 1-7. International Electrotechnical Commission (IEC), 1998.
[12] MIL-HDBK-217F. Reliability Prediction of Electronic Equipment. Washington: U.S. Department of Defence 1991.
[13] MIL-STD-1629A. Procedures for performing a failure mode, effects and criticality analysis. Department of Defence, Washington 1980.
[14] PN-IEC 812: Analysis techniques for system reliability - procedure for failure mode and effect analysis (FMEA), 1994.
[15] SIPI (*Safety In the Process Industries*): Materiały warsztatów międzynarodowych (ed. M. Dźwiarek, K.T. Kosmowski, T. Missala): Gdynia, 28-29 maja 2003.

Title: Functional safety assessment of the control and protection systems

Artykuł recenzowany