Śliwiński Marcin
Politechnika Gdańska, Gdańsk, Polska

Integrity level verification for safety-related functions
Weryfikacja poziomu nienaruszalności funkcji związanych z bezpieczeństwem

Keywords / Słowa kluczowe

functional safety, safety integrity level verification
bezpieczeństwo funkcjonalne, weryfikacja poziomu nienaruszalności bezpieczeństwa

Abstract

This article describes methods for the safety integrity level (SIL) verification of safety-related functions with regard to probabilistic criteria given in international standards IEC 61508 and IEC 61511. These functions are realized using the electrical, electronic and programmable electronic (E/E/PE) systems or safety instrumented systems (SIS). Some methods are proposed for quantitative probabilistic modelling taking into account potential dependent failures in redundant systems with diverse channels within subsystems. The analyses of safety-related systems include testing and maintenance planning of subsystems, in particular the sensors and actuators with regard to the probabilistic criteria defined for given SIL. The methods are illustrated on some examples of systems from industrial hazardous plants.

1. Wprowadzenie

Funkcje związane z bezpieczeństwem realizowane są przez systemy sterowania i zabezpieczeń zawierające elementy elektryczne, elektroniczne i programowalne elektroniczne (E/E/PE). Systemy te są jednym ze środków pozwalających na zmniejszenie ryzyka pochodzącego od instalacji technicznej i procesu. Istnieje problem właściwego zaprojektowania systemu E/E/PE realizującego funkcje związane z bezpieczeństwem. Problematyka dotycząca weryfikacji poziomów nienaruszalności bezpieczeństwa SIL (ang. *Safety Integrity Level*) zawarta jest w części szóstej normy PN-EN 61508.

2. Modelowanie probabilistyczne systemów E/E/PE realizujących funkcje związane z bezpieczeństwem

Poszczególnym poziomom SIL projektowanego systemu E/E/PE realizującego funkcje związane z bezpieczeństwem odpowiadają ilościowe kryteria probabilistyczne. W analizie bezpieczeństwa funkcjonalnego kluczowe znaczenie ma określenie poziomu nienaruszalności bezpieczeństwa SIL dla obiektu (instalacji) podwyższonego ryzyka, a następnie zaprojektowanie takiego systemu zabezpieczeniowego, który spełni te wymagania. Przeprowadzenie dowodu spełnienia przez system zabezpieczeniowy wymagań na określony poziom SIL nazywa się weryfikacją.

Model probabilistyczny dowolnego systemu sterowania lub zabezpieczeń można przedstawić za pomocą schematów blokowych niezawodności RBD (ang. *Reliability Block Diagram*), grafów Markowa, równań uproszczonych oraz drzew niezdatności FTA (ang. *Fault Tree Analysis*) z wykorzystaniem struktury ścieżek lub cięć minimalnych [1], [2], [3]. W przypadku gdy system rozpatrywany jest z punktu widzenia jego uszkadzalności wygodnym podejściem jest skorzystanie z metody cięć minimalnych.

Biorąc pod uwagę metodę cięć minimalnych, prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez system zabezpieczeniowy realizujący funkcje związane z bezpieczeństwem można określić na podstawie zależności

$$PFD(t) \approx \sum_{j=1}^{n} Q_j(t) \approx \sum_{j=1}^{n} \prod_{i \in K_j} q_i(t) \qquad (1)$$

gdzie K_j jest *j*-tym cięciem minimalnym (MC), $Q_i(t)$ oznacza prawdopodobieństwo wystąpienia *j* – tego cięcia minimalnego w funkcji czasu, *n* jest luczbą MC, $q_i(t)$ oznacza prawdopodobieństwo uszkodzenia i-*t*ego podsystemu lub elementu w *j*–tym cięciu minimalnym.
Wykorzystując zależność (1) można określić przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie, zakładając, że poszczególne podsystemy są testowane z czasem między testami okresowymi T_I, mającymi na celu wykrycie uszkodzeń niebezpiecznych

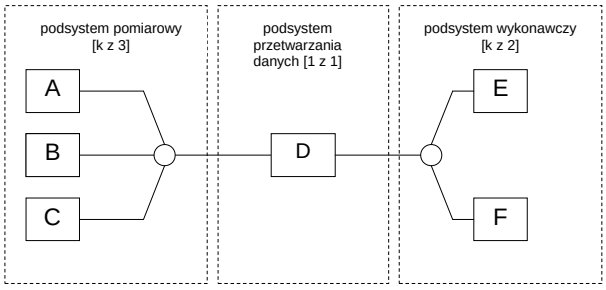
$$PFD_{avg} = \frac{1}{T_I} \int_0^{T_I} PFD(t)dt \qquad (2)$$

gdzie T_I jest interwałem przeprowadzania testów.
Prawdopodobieństwo uszkodzenia systemu na godzinę dla trybu pracy ciągłej lub częstego przywołania do działania można wyznaczyć [16] na podstawie wzoru

$$PFH \approx \frac{\sum_{j=1}^{n}(1-\sum_{\substack{i=1 \\ i\neq j}}^{n} Q_j(t))(\sum_{j\in K_j} \frac{Q_j(t)}{q_i(t)}(1-q_i(t))\lambda_i)}{1-\sum_{j=1}^{n}\prod_{i\in K_j} q_i(t)} \qquad (3)$$

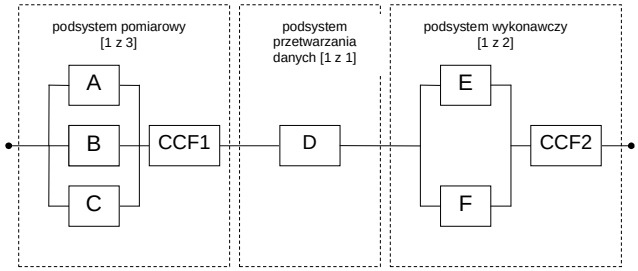
gdzie λ_i jest intensywnością uszkodzeń *i*–tego podsystemu/elementu.

Architektura sprzętu realizującego funkcję bezpieczeństwa jest przedstawiana za pomocą schematu blokowego z wyróżnieniem podsystemów i modułów. Na *Rysunku 1* przedstawiono strukturę przykładowego systemu E/E/PE [10], [11], [14].



Rysunek 1. Przykładowa struktura systemu E/E/PE lub SIS

W systemie E/E/PE lub SIS wyróżnia się trzy podsystemy: pomiarowy, przetwarzania danych oraz wykonawczy. Przedstawiona struktura składa się z trzech czujników A, B, C konfiguracji k z 3, podsystemu logicznego D (np. sterownika PLC) oraz elementów wykonawczych E oraz F (k z 2).
Na *Rysunku 2* przedstawiono system zabezpieczeniowy SIS (ang. *Safety Instrumented System*) w postaci schematu blokowego niezawodności przy założeniu, że podsystem pomiarowy posiada konfigurację 1 z 3, a podsystem wykonawczy 1 z 2.

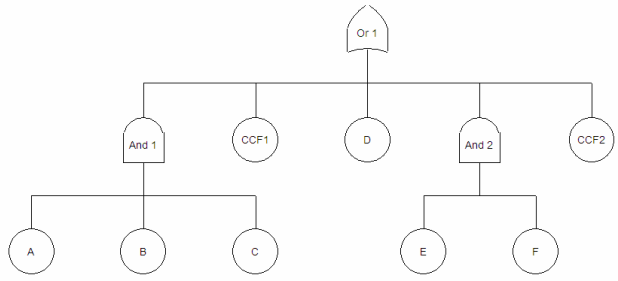


Rysunek 2. Schemat blokowy niezawodności RBD przykładowej struktury systemu E/E/PE lub SIS

Na powyższym schemacie uwzględniono uszkodzenia o wspólnej przyczynie CCF (ang. *common cause failure*) dla podsystemu pomiarowego CCF 1 oraz CCF 2 dla podsystemu wykonawczego od elementów E i F. W systemie z rys. 2 można wyróżnić pięć cięć minimalnych:

{A, B, C}; {CCF1}; {D}; {E, F}; {CCF2}

Na *Rysunku 3* znajduje się drzewo niezdatności systemu E/E/PE lub SIS z *Rysunku 3* z uwzględnieniem uszkodzeń o wspólnej przyczynie.



Rysunek 3. Drzewo niezdatności systemu E/E/PE lub SIS

Przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie PFD_{avg} dla systemu z *Rysunku 2* można w przybliżeniu wyznaczyć ze wzoru

$$PFD_{avg} \cong PFD_{avg}^{ABC} + PFD_{avg}^{CCF1} + PFD_{avg}^{D} + PFD_{avg}^{EF} + PFD_{avg}^{CCF2} \qquad (4)$$

Analogicznie prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę *PFH* (dla systemu pracującego w trybie częstego przywołania lub ciągłym)

$$PFH \cong PFH^{ABC} + PFH^{CCF1} + PFH^{D} + PFH^{EF} + PFH^{CCF2} \quad (5)$$

Korzystając z metody cięć minimalnych przy określaniu prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie *PFD(t)*, a następnie wartości PFD_{avg} i *PFH* można zaproponować dwa podejścia. Pierwsze bazuje na klasycznej metodzie uwzględnienia uszkodzeń zależnych, w której współczynnik β zastosowany w modelu probabilistycznym związany jest ze schematem zastępczym rozpatrywanego układu. Drugie podejście uwzględnia uszkodzenia zależne, a więc i obecność współczynnika β w sposób wynikający z drzewa niezdatności dla rozpatrywanego podsystemu [2], [4], [6].

3. Uszkodzenia zależne w modelowaniu probabilistycznym systemów E/E/PE i SIS z nadmiarowością strukturalną

W modelowaniu probabilistycznym systemów E/E/PE z nadmiarowością strukturalną w module weryfikacji SIL uwzględniono wpływ uszkodzeń zależnych, poprzez zastosowanie współczynnika β (modelu beta). Wykorzystane zostały różne sposoby przyjmowania współczynnika β w zależności od aktualnej architektury systemu nadmiarowego [10]

$$\beta_{kzn} = \beta \cdot C_{kzn} \quad (6)$$

gdzie β stanowi współczynnik bazowy dla najprostszej struktury 1 z 2, natomiast C_{kzn} jest mnożnikiem uzależnionym od rozpatrywanej architektury podsystemu i odpowiednio wynosi: $C_{1z2} = 1$, $C_{1z3} = 0.5$, $C_{2z3} = 1.5$.
Wartość współczynnika bazowego β przyjmowana jest w zależności od podsystemu z jakim aktualnie ma się do czynienia oraz od tego gdzie dany system ma zostać zainstalowany. W przypadku podsystemu przetwarzającego informację (PLC) współczynnik β mieści się w granicach: $0.5\% < \beta < 5\%$, dla układu czujników i elementów wykonawczych: $1\% < \beta < 10\%$, dla modułów wejść/wyjść: $1\% < \beta < 50\%$.Wartości współczynnika β określa się na podstawie systemu punktowego i tablic estymacji znajdujących się w części szóstej normy PN - EN 61508-6 oraz w normie PN-EN 62061 [11].
W *Tabeli 1* przedstawiono sposób wyznaczenia współczynnika uszkodzeń zależnych dla struktur nadmiarowych $\beta_{(k\,z\,n)}$ z wykorzystaniem współczynnika bazowego β obliczonego na podstawie punktowych tablic estymacji (według norm PN-EN 61508 i 62061) [10], [11], [13]. Przyjęto wartość maksymalną n = *5*, a współczynnik bazowy β wyznacza się na podstawie punktowych tablic estymacji (IEC 61508-6, 2010) [10].

Tabela 1. Wyznaczenie współczynnika $\beta_{(k\,z\,n)}$ dla struktur nadmiarowych *k z n*

		n			
		2	*3*	*4*	*5*
k	*1*	β	$0.5\,\beta$	$0.3\,\beta$	$0.2\,\beta$
	2	-	$1.5\,\beta$	$0.6\,\beta$	$0.4\,\beta$
	3	-	-	$1.75\,\beta$	$0.8\,\beta$
	4	-	-	-	β

Intensywność uszkodzeń λ elementu (podsystemu) o strukturze *k z n* jest sumą intensywności uszkodzeń niezależnych λ_I oraz zależnych λ_C

$$\lambda = \lambda_I + \lambda_C \quad (7)$$

Współczynnik β określa równanie

$$\beta = \frac{\lambda_C}{\lambda} \quad (8)$$

Biorąc pod uwagę równania (7) oraz (8) intensywność uszkodzeń zależnych

$$\lambda_C = \beta \cdot \lambda \quad (9)$$

Zatem intensywność uszkodzeń niezależnych

$$\lambda_I = (1-\beta) \cdot \lambda \quad (10)$$

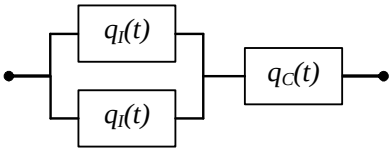
Korzystając z intensywności uszkodzeń wyrażonych zależnościami (9) oraz (10) prawdopodobieństwo uszkodzeń zależnych można wyznaczyć z równania

$$q_C(t) = \beta \cdot q(t) \quad (11)$$

A prawdopodobieństwo uszkodzeń niezależnych z zależności

$$q_I(t) = (1-\beta) \cdot q(t) \quad (12)$$

Na *Rysunku 4* przedstawiony jest schemat blokowy systemu o strukturze 1 z 2 z uwzględnieniem uszkodzeń zależnych C.



Rysunek 4. Schemat blokowy niezawodności systemu o architekturze 1 z 2

Przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie dla struktury 1 z 2 z uwzględnieniem uszkodzeń o wspólnej przyczynie [12], [16] określa zależność

$$PFD_{avg1z2} \cong [(1-\beta)\lambda_D]^2(\frac{T_I^2}{3} + T_I MTTR + \\ + MTTR^2) + \beta\lambda_{DU}(\frac{T_I}{2} + MTTR) \quad (13)$$

Gdzie T_I jest czasem, między testami; *MTTR* oznacza średni czas naprawy; λ_D jest intensywnością uszkodzeń niebezpiecznych; natomiast λ_{DU} jest intensywnością uszkodzeń niebezpiecznych niewykrywalnych.
Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę dla struktury 1 z 2 po uwzględnieniu uszkodzeń zależnych można obliczyć ze wzoru

$$PFH_{1z2} \cong 2[(1-\beta)\lambda_D]^2(\frac{T_I}{2} + MTTR) + \beta\lambda_{DU} \quad (14)$$

Zależności proponowane w normie PN-EN 61508 dotyczą jedynie przypadku, w którym poszczególne podsystemy układu sterowania/zabezpieczeniowego składają się z jednakowych elementów. Przykładowo takich samych: czujników, układów przetwarzania, elementów wykonawczych. Postać modelu probabilistycznego systemu sterowania lub zabezpieczeniowego komplikuje się znacznie, jeżeli poszczególne podsystemy składają się z *n* różnych elementów. Zależności proponowane przez PN-EN 61508 są więc w danym przypadku niewystarczające.
Zastosowanie metodyki bazującej w oparciu o technikę cięć minimalnych wyznaczonych dla rozpatrywanego systemu umożliwia zbudowanie modeli probabilistycznych przy dowolnej konfiguracji podsystemów złożonych z różnych elementów. Pojęcie różnych elementów w danym przypadku będzie równoznaczne z tym, iż każdy z nich będzie charakteryzował się różną intensywnością uszkodzeń λ. W modelach probabilistycznych systemów, w których każdy element jest inny tzn. posiada różną intensywność uszkodzeń, tak samo jak poprzednio ważnym parametrem jest współczynnik uszkodzeń zależnych β.
Jednakże zamodelowanie i uwzględnienie go w finalnej postaci modelu dla konkretnej struktury stwarza wiele problemów i nie jest zadaniem trywialnym. W przypadku modeli probabilistycznych systemów sterowania i zabezpieczeń dla struktur 1 z 2, 2 z 3, 4 z 6, *k z n*, przy założeniu, że k < n należy uwzględnić współczynnik uszkodzeń zależnych β, którego model przedstawiony został poniżej.
Intensywność uszkodzeń systemu λ o strukturze nadmiarowej *k z n*, składającego się z *n* różnych elementów można przedstawić [3], [7], [8], [9], [16] w postaci sumy przeciętnej intensywności uszkodzeń niezależnych λ_{Iavg} oraz intensywności uszkodzeń zależnych λ_C

$$\lambda = \lambda_{Iavg} + \lambda_C \quad (15)$$

Współczynnik β ma postać

$$\beta = \frac{\lambda_C}{\lambda_C + \lambda_{Iavg}} = \frac{\lambda_C}{\lambda} \quad (16)$$

wykorzystując (15) oraz (16) intensywność uszkodzeń zależnych wyraża równanie

$$\lambda_C = \beta \cdot \lambda \quad (17)$$

natomiast przeciętna intensywność uszkodzeń niezależnych

$$\lambda_{Iavg} = (1-\beta) \cdot \lambda \quad (18)$$

Przeciętną intensywność uszkodzeń λ_{Iavg} można przedstawić w postaci

$$\lambda_{Iavg} = \frac{\sum_{i=1}^{n}\lambda_{Ii}}{n} = \frac{\sum_{i=1}^{n}(1-\beta)\lambda_i}{n} \quad (19)$$

gdzie: λ_{Ii} jest intensywnością uszkodzeń niezależnych dla pojedynczego *i–tego* elementu; a *n* liczbą elementów.
Uwzględniając zależności (17) i (19) intensywność uszkodzeń zależnych λ_C przyjmie następującą postać

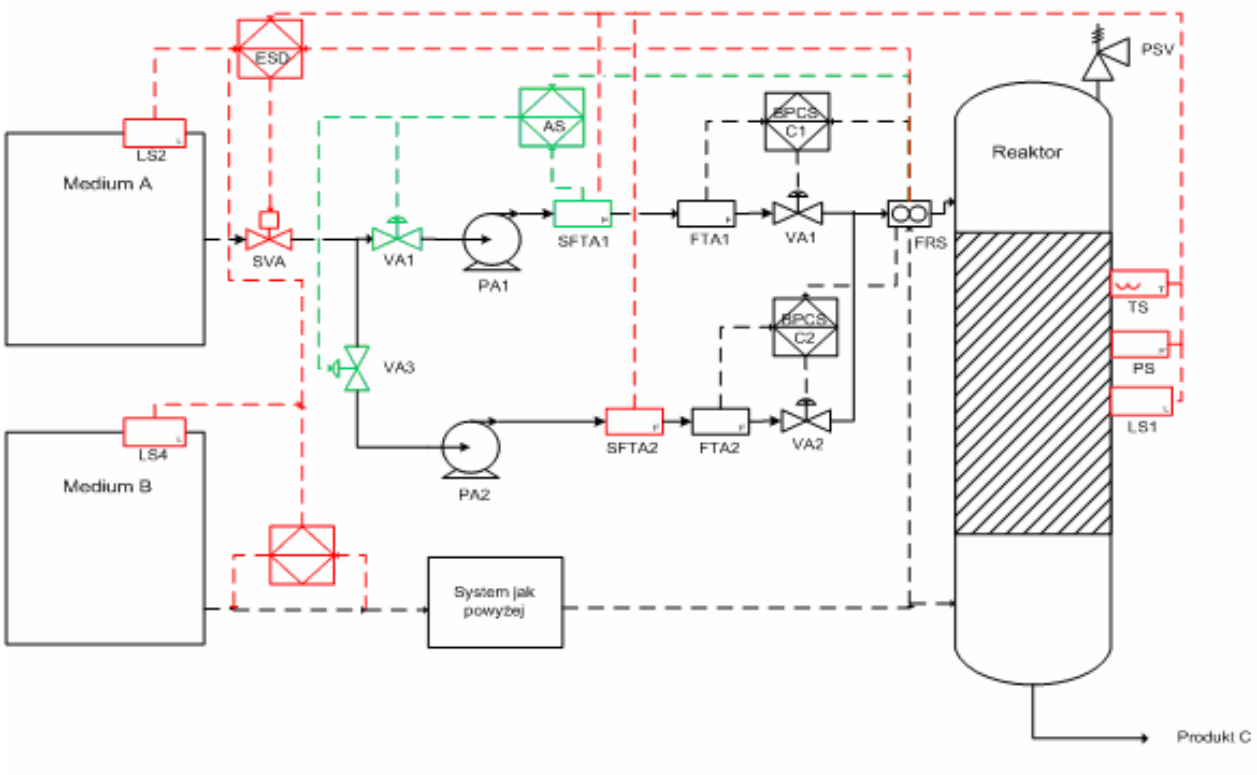
$$\lambda_C = \frac{\beta\lambda_{Iavg}}{(1-\beta)} = \frac{\beta(\frac{\sum_{i=1}^{n}\lambda_{Ii}}{n})}{(1-\beta)} = \frac{\beta(1-\beta)(\frac{\sum_{i=1}^{n}\lambda_i}{n})}{(1-\beta)} \qquad (18)$$

$$\lambda_C = \beta(\frac{\sum_{i=1}^{n}\lambda_i}{n})$$

Powyżej został przedstawiony ogólny model dla współczynnika β. Uwzględnienie w budowanym modelu uszkodzeń CCF ma zasadnicze znaczenie. W sytuacji gdy układ będzie się składał z takich samych elementów wówczas zależności zostaną sprowadzone do postaci przedstawionej równaniami opisującymi przypadek dla takich samych elementów.

4. Przykład weryfikacji SIL

Instalacja technologiczna (*Rysunrk 5*). składa się ze zbiornika wysokociśnieniowego, dwóch zbiorników z substancjami A i B oraz rurociągów transportujących substancje ze zbiorników A i B do zbiornika wysokociśnieniowego, w którym zachodzi reakcja chemiczna. W wyniku reakcji i wymieszania substancji A i B otrzymywany jest produkt C



Rysunek 5. Przykładowa instalacja wraz z systemem sterowania i zabezpieczeń

Każdy rurociąg jest wyposażony w zestaw czujników mierzących najważniejsze zmienne procesowe oraz elementów wykonawczych wykonujących odpowiednie do kontekstu sytuacji funkcje. Aby proces mógł przebiegać w sposób bezpieczny łatwopalne medium A powinno być dostarczane bez przerwy do zbiornika reakcyjnego w ilości większej od łatwopalnego medium B, aby nie doprowadzić do wybuchu. Reakcja mieszania musi odbywać się w określonej temperaturze oraz przy odpowiednim ciśnieniu.

Zbyt duże ciśnienie w zbiorniku reaktora może doprowadzić do eksplozji. Na podstawie analizy ryzyka określono wymagania dla funkcji bezpieczeństwa na poziomie SIL3. Projektowana część sprzętowa realizująca funkcję bezpieczeństwa, która zapobiega eksplozji reaktora musi spełniać kryteria probabilistyczne odpowiadające poziomowi SIL3 dla systemu rzadkiego przywołania do działania.

Warstwa sprzętowa realizująca funkcję bezpieczeństwa zapobiegającą powstaniu eksplozji zbiornika składa się z trzech podsystemów: pomiarowego w skład którego wchodzą dwie matryce detektorów ciśnienia PS i temperatury TS; podsystemu ESD, którego integralną częścią jest system przetwarzający dane (sterownik Safety PLC, SRS lub PLC) oraz układu wykonawczego – w tym przypadku zaworu SVA odcinającego dopływ medium do reaktora.

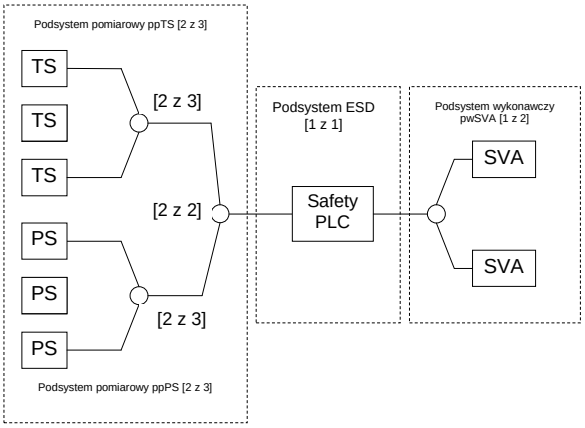
Konfiguracja architektury warstwy sprzętowej realizującej funkcję bezpieczeństwa może wymagać nadmiarowości strukturalnej. W danym przypadku

zostaną poddane analizie struktury przykładowych systemów SIS, których schematy przedstawione zostały na *Rysunku 6* system SIS (I), *Rysunku 7* system SIS (II) oraz *Rysunku 8* system SIS (III). Wymagania stawiane dla układu zabezpieczeniowego są na poziomie SIL3. Wartości PFD_{avg} dla systemu zabezpieczeniowego zostały wyznaczone z wykorzystaniem danych niezawodnościowych znajdujących się bazie danych Pro-SIL. W *Tabeli 2* zestawiono dane niezawodnościowe elementów systemów SIS poddanych weryfikacji.
W danym przypadku rozpatrzone zostaną trzy różne podsystemy ESD w skład których wchodzić będą sterownik Safety PLC; system SRS oraz standardowy sterownik przemysłowy PLC.

Tabela 2. Dane niezawodnościowe dla elementów systemu zabezpieczeniowego [17], [18]

	SVA	**Safety PLC**	**SRS**	**PLC**	**PS**	**TS**
DC [%]	24	90	90	66	54	66
λ_{DU} [1/h]	$8\cdot10^{-7}$	$1\cdot10^{-6}$	$1\cdot10^{-7}$	$5\cdot10^{-6}$	$3\cdot10^{-7}$	$3\cdot10^{-6}$
MTTR [h]	8	8	8	8	8	8
T_I [h]	8760	8760	8760	8760	8760	8760
β	0.02	0.01	0.01	0.01	0.02	0.02

Na *Rysunku 6* znajduje się pierwsza struktura sprzętowa systemu SIS (I), która opiera została na układzie sterownika bezpieczeństwa safety PLC.

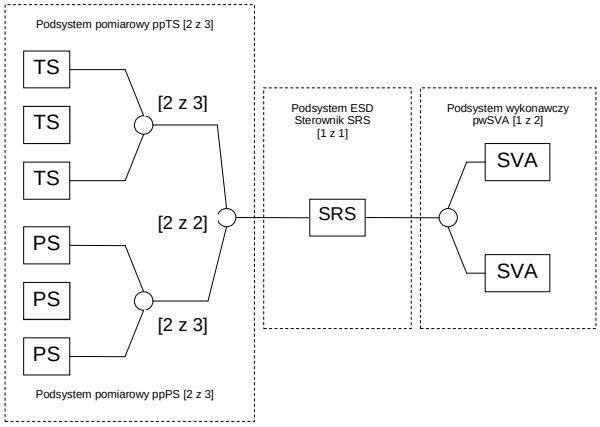


Rysunek 6. Architektura systemu SIS (I) wyposażona w sterownik „safety PLC" (matryce detektorów pracują w konfiguracji 2 z 2)

Tabela 3. Raport wynikowy weryfikacji SIL dla systemu SIS (I) metodą CM

System /podsystem /element		**k z n**	**β [%]**	**PFD_{avg}**	**SIL**	**x_i [%] PFD_{avgS}**
SIS (I)	**0**	**-**	**-**	**$4.57\cdot10^{-3}$**	**2**	**100**
ppTS	**.1**	**2 z 3**	**3**	**$2.93\cdot10^{-5}$**	**4**	**0.641**
TS	..2	-	-	$1.53\cdot10^{-3}$	2	-
TS	..2	-	-	$1.53\cdot10^{-3}$	2	-
TS	..2	-	-	$1.53\cdot10^{-3}$	2	-
ppPS	**.1**	**2 z 3**	**3**	**$3.11\cdot10^{-5}$**	**4**	**0.681**
PS	..2	-	-	$1.58\cdot10^{-3}$	2	-
PS	..2	-	-	$1.58\cdot10^{-3}$	2	-
PS	..2	-	-	$1.58\cdot10^{-3}$	2	-
ESD	**.1**	**1 z 1**	**-**	**$4.44\cdot10^{-3}$**	**2**	**97.2**
Safety PLC	..2	-	-	$4.44\cdot10^{-3}$	2	-
pwSV	**.1**	**1 z 2**	**2**	**$7.14\cdot10^{-5}$**	**4**	**1.56**
SVA	..2	-	-	$3.5\cdot10^{-3}$	2	-
SVA	..2	-	-	$3.5\cdot10^{-3}$	2	-

Uwzględniając dane niezawodnościowe zawarte w *Tabeli 2* uzyskano wyniki, które wraz z całościową specyfikacją sprzętową systemu SIS (I) zestawiono w raporcie wynikowym znajdującym się w *Tabeli 3.*
Z powyższego raportu wynika, że struktura sprzętowa systemu SIS (I) nie spełnia wymagań SIL3. Duży udział w tym stanie rzeczy ma zastosowanie sterownika Safety PLC w podsystemie ESD bez nadmiarowości strukturalnych.
W drugim z rozpatrywanych przypadków w systemie SIS (II) zastosowano w podsystemie ESD jednostkę SRS o lepszych parametrach niezawodnościowych od sterownika Safety PLC (*Rysunek 7*).



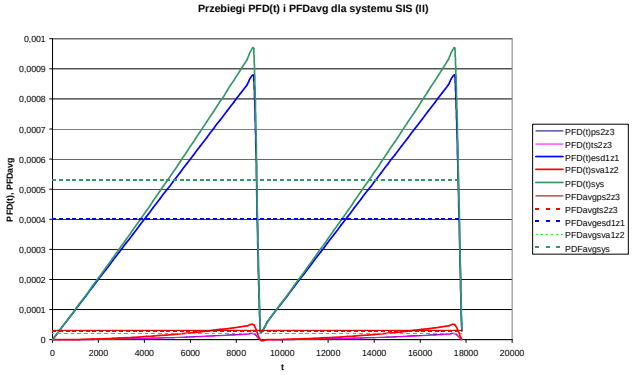
Rysunek 7. Architektura systemu SIS (II) wyposażona w sterownik SRS

Szczegółowy raport z weryfikacji struktury sprzętowej SIS (II) realizującej funkcję bezpieczeństwa znajduje się w *Tabeli 4.*

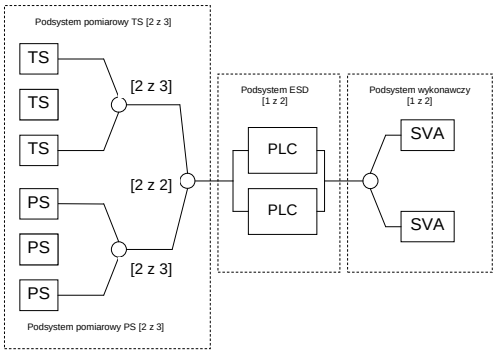
Tabela 4. Raport wynikowy weryfikacji SIL dla systemu SIS (II) metodą cięć minimalnych

System /podsystem		k z n	β [%]	PFD_{avg}	SIL	x_i [%] PFD_{avgS}
SIS(II)	**0**	-	-	$5.32 \cdot 10^{-4}$	3	**100**
ppTS	**.1**	**2 z 3**	**3**	$\mathbf{2.93 \cdot 10^{-5}}$	**4**	**5.51**
TS	..2	-	-	$1.53 \cdot 10^{-3}$	2	-
TS	..2	-	-	$1.53 \cdot 10^{-3}$	2	-
TS	..2	-	-	$1.53 \cdot 10^{-3}$	2	-
ppPS	**.1**	**2 z 3**	**3**	$\mathbf{3.11 \cdot 10^{-5}}$	**4**	**5.85**
PS	..2	-	-	$1.58 \cdot 10^{-3}$	2	-
PS	..2	-	-	$1.58 \cdot 10^{-3}$	2	-
PS	..2	-	-	$1.58 \cdot 10^{-3}$	2	-
ESD	**.1**	**1 z 1**	**-**	$\mathbf{0.4 \cdot 10^{-3}}$	**3**	**75.2**
SRS	..2	-	-	$0.4 \cdot 10^{-3}$	3	-
pwSV	**.1**	**1 z 2**	**2**	$\mathbf{7.14 \cdot 10^{-5}}$	**4**	**13.4**
SVA	..2	-	-	$3.5 \cdot 10^{-3}$	2	-
SVA	..2	-	-	$3.5 \cdot 10^{-3}$	2	-

Pomimo braku nadmiarowości w konfiguracji systemu ESD system SIS (II) spełnia wymagania SIL3. Na rys. 8 przedstawiono przebiegi czasowe wartości PFD(t) dla systemu SIS (II) oraz jego podsystemów. Na *Rysunku 9* przedstawiono system SIS (III), dla którego w podsystemie ESD zastosowano dwa sterowniki PLC w konfiguracji 1 z 2.



Rysunek 8. Przebiegi PFD(t) oraz wartości PFD_{avg} dla systemu SIS (II)



Rysunek 9. Architektura systemu SIS (III) wyposażona w dwa sterowniki PLC (1 z 2)

Tabela 5. Raport wynikowy weryfikacji SIL dla systemu SIS (III) na podstawie Pro-SIL (wg metody cięć minimalnych (CM))

System /podsystem /element		k z n	β [%]	PFD_{avg}	SIL	x_i [%] PFD_{avgS}
SIS (III)	**0**	-	-	$7.32 \cdot 10^{-4}$	3	100
ppTS	**.1**	**2 z 3**	**3**	$\mathbf{2.93 \cdot 10^{-5}}$	**4**	**4**
TS	..2	-	-	$1.53 \cdot 10^{-3}$	2	-
TS	..2	-	-	$1.53 \cdot 10^{-3}$	2	-
TS	..2	-	-	$1.53 \cdot 10^{-3}$	2	-
ppPS	**.1**	**2 z 3**	**3**	$\mathbf{3.11 \cdot 10^{-5}}$	**4**	**4.25**
PS	..2	-	-	$1.58 \cdot 10^{-3}$	2	-
PS	..2	-	-	$1.58 \cdot 10^{-3}$	2	-
PS	..2	-	-	$1.58 \cdot 10^{-3}$	2	-
ESD	**.1**	**1 z 2**	**1**	$\mathbf{6 \cdot 10^{-4}}$	**3**	**82**
PLC	..2	-	-	$2.19 \cdot 10^{-2}$	1	-
PLC	..2	-	-	$2.19 \cdot 10^{-2}$	1	-
pwSV	**.1**	**1 z 2**	**2**	$\mathbf{7.14 \cdot 10^{-5}}$	**4**	**9.75**
SVA	..2	-	-	$3.5 \cdot 10^{-3}$	2	-
SVA	..2	-	-	$3.5 \cdot 10^{-3}$	2	-

Szczegółowy raport z weryfikacji warstwy sprzętowej systemu SIS (III) znajduje się w *Tabeli 5.*

Raporty z weryfikacji SIL przedstawione powyżej dla trzech systemów SIS pracujących w trybie pracy rzadkiego przywołania zawierają procentowy udział wartości PFD_{avg} podsystemu/elementu w ogólnej wartości $PFD_{avg\,S}$ wyznaczonej dla systemu (ostatnia kolumna) na podstawie zależności

$$x_i = \frac{PFD_{avgi}(PFH)_i}{PFD_{avgsys}(PFH)_{sys}} \cdot 100\% \qquad (19)$$

Zależność (19) prezentuje procentowy udział wartości PFD_{avg} lub PFH podsystemu/elementu w ogólnej wartości PFD_{avg} lub PFH wyznaczonej dla części sprzętowej systemu realizującego funkcje bezpieczeństwa.

System SIS (III) zrealizowany z wykorzystaniem standardowych sterowników programowalnych PLC z redundancją w podsystemie ESD spełnia wymagania SIL3 i jest rozwiązaniem tańszym aniżeli system SIS (II) z systemem SRS w podsystemie ESD.

5. Podsumowanie

W niniejszym artykule przedstawiono wybrane zagadnienia związane z weryfikacją poziomów nienaruszalności funkcji związanych z bezpieczeństwem. Zaprezentowano modele

probabilistyczne systemów E/E/PE wykorzystywane przy ilościowej weryfikacji SIL zbudowane z wykorzystaniem techniki drzew niezdatności i schematów blokowych niezawodności. Ważnym aspektem przy ilościowej weryfikacji SIL jest właściwe uwzględnienie uszkodzeń zależnych z wykorzystaniem modelu β. W danym przypadku należy zwrócić szczególną uwagę na współczynnik korekcyjny uzależniony od architektury rozpatrywanego systemu.

Metody opisane w niniejszym artykule zostały zaimplementowane do budowy modułu weryfikacji SIL w aplikacji Pro-SIL. Moduł weryfikacji SIL (Pro-SILer), który pozwala na szybką weryfikację poziomów nienaruszalności bezpieczeństwa SIL systemów (E/E/PE) o dowolnej konfiguracji sprzętowej z uwzględnieniem zagadnień niepewności i ochrony informacji [15], [16], [18].

Dalsze prace dotyczące procesu weryfikacji SIL powinny przede wszystkim skupić się na opracowaniu skutecznych metod uwzględniających w modelach probabilistycznych w sposób czytelny wpływ uszkodzeń zależnych i błędów człowieka [1], [5]. Nie można pominąć tych aspektów w modelach probabilistycznych, gdyż uzyskane wyniki będą zbyt optymistyczne w stosunku do sytuacji w rzeczywistej instalacji przemysłowej.

Podziękowanie

Autor niniejszego artykułu dziękuje Ministerstwu Nauki i Szkolnictwa Wyższego za wsparcie badań oraz Centralnemu Laboratorium Ochrony Pracy – Państwowemu Instytutowi Badawczemu za współpracę w przygotowaniu projektu badawczego VI.B.10 do realizacji w latach 2011-13 dotyczącego zarządzania bezpieczeństwem funkcjonalnym w obiektach podwyższonego ryzyka z włączeniem zagadnień zabezpieczeń / ochrony i niezawodności człowieka.

Bibliografia

[1] Barnert, T., Kosmowski, K. & Śliwiński, M. (2006). Methodological aspects of functional safety assessment. *Zagadnienia Eksploatacji Maszyn*. Instytut Technologii Eksploatacji - Państwowy Instytut Badawczy.

[2] Barnert, T & Śliwiński, M. (2007). *Methods for verification safety integrity level in control and protection systems, Functional Safety Management in Critical Systems*. Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk, s. 171-185.

[3] Barnert, T., Kosmowski, K.T. & Śliwiński, M (2008). Determining and verifying the safety integrity level of the control and protection systems under uncertainty. *Maeriały konferencji ESREL 2008 European Safety & Reliability Conference*, Walencja.

[4] Braband, J. & Griebel, S. (2004). Safety Analysis according to IEC 61508 – Putting it into Practice. *Materiały European Safety & Reliability Conference*, Berlin.

[5] Carey, M. (2001). *Proposed framework for addressing human factors in IEC 61508*. Health & Safety Executive.

[6] Cheddie, H. (2002). The safety analysis of redundant safety instrumented functions (SIF) with incomplete or partial testing. exida.com.

[7] Hokstad, P. (2004). A generalisation of the beta factor model. *Materiały European Safety & Reliability Conference*, Berlin.

[8] Hokstad, P. (2005). Probability of Failure on Demand (PFD) – the formulas of IEC 61508 with focus on the 1oo2D voting. *Materiały European Safety & Reliability Conference, ESREL 2005* Gdynia - Sopot – Gdańsk, 2005 Taylor & Francis Group, London.

[9] Høyland, A. & Rausand, M. (1994). *System Reliability Theory. Models and Statistical Methods*. New York: John Wiley & Sons, Inc.

[10] IEC 61508 (2010). Functional safety of electrical/electronic/programmable electronic safety – related systems. Parts 1-7. International Electrotechnical Commission (IEC).

[11] IEC 62061 (2005). Safety of machinery – Functional safety of safety-related electrical/ electronic and programmable electronic control systems (E/E/PE). International Electrotechnical Commission (IEC).

[12] Kosmowski, K.T., Śliwiński, M. & Zabielski, A. (2004). Obliczanie wartości PFD dla funkcji bezpieczeństwa obwodu SIS o różnych konfiguracjach. Konferencja – Zarządzanie bezpieczeństwem funkcjonalnym, Jurata.

[13] PN-EN 61508 (2004). Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1-7. PKN.

[14] PN-EN 61511 (2004). Bezpiecz. funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3. Polski Komitet Normalizacyjny.

[15] Stavrianidis, P. (1992). Reliability and uncertainty analysis of hardware failures of programmable electronic system. *Reliability Engineering and System Safety* 39, 309 - 324.

[16] Sliwinski, M. (2005). Designing control and protection systems with regard to functional

safety aspects. *Proc. IEEE International Conference on Technologies for Homeland Security and Safety TEHOSS 2005*, Gdansk.

[17] Reliability Data for Safety Instrumented Systems - PDS Data Handbook. (2010). Edition, ISBN 978-82-14-04849-0, SINTEF A13502.

[18] Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook. (2010). Edition, ISBN 978-82-14-04849-0, SINTEF A13502.