Temat:

Weryfikacja nienaruszalności bezpieczeństwa SIL struktury sprzętowej realizującej funkcje bezpieczeństwa

Kryteria probabilistyczne bezpieczeństwa funkcjonalnego

Wartości PFD_{avg} dla czterech poziomów nienaruszalności bezpieczeństwa SIL zestawiono w tabeli 1 (rodzaj pracy rzadkiego przywołania do działania). Warto zwrócić uwagę na fakt, iż uzyskanie poziomu SIL2 dla struktury sprzętowej realizującej funkcje bezpieczeństwa może okazać się niemożliwe bez zastosowania nadmiarowości strukturalnej, a spełnienie warunków SIL3, a zwłaszcza SIL4 wymaga rozbudowanych środków nadmiarowych i jest zwykle niezwykle trudnym i dużym wyzwaniem koncepcyjnym, technicznym oraz organizacyjnym.

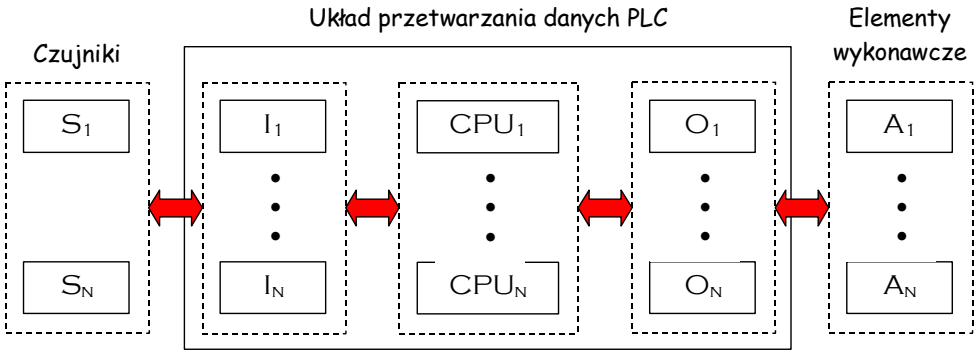
Tabela 1. Poziomy nienaruszalności bezpieczeństwa SIL i przedziałowe kryteria probabilistyczne dla systemów E/E/PE

SIL	P_{FDavg}	P_{FH}
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	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

W przypadku rodzaju pracy częstego przywołania do działania lub działania ciągłego systemu rozważa się kryterium probabilistyczne zgodnie z trzecią kolumną tabeli 1, czyli prawdopodobieństwa uszkodzenia niebezpiecznego na godzinę *PFH*. Należy zaznaczyć, że proponowany w normie PN-EN 61508 podział rodzajów pracy z rzadkim oraz częstym przywołaniem systemu do działania nie zawsze jest uzasadniony, co wymaga odpowiedniego potraktowania w modelowaniu probabilistycznym systemu i jego ocenie.

Należy podkreślić, że stosowanie struktur nadmiarowych w systemie E/E/PE wpływa na zwiększenie częstości zadziałań nieuzasadnionych systemu zabezpieczeń, w wyniku których mogą powstać straty produkcyjne i ekonomiczne. Częstość zadziałań nieuzasadnionych *PFS* wzrośnie w przybliżeniu dwukrotnie po zastosowaniu podsystemu o architekturze 1 z 2 zamiast 1 z 1. Nieuzasadnione odstawienie instalacji, a następnie jej uruchamianie wiąże się z ryzykiem wystąpienia stanów niebezpiecznych w innych podsystemach co wymaga stosowania analiz i ocen ryzyka.

Ilościowa weryfikacja SIL – dobór architektury sprzętowej systemu zabezpieczeniowego realizującego funkcje bezpieczeństwa



Rys. 1. Ogólna struktura systemu zabezpieczeniowego zrealizowana w oparciu o sterowniki PLC, o podsystemach w konfiguracji (k z n)

Rozdział intensywności uszkodzeń na intensywność uszkodzeń bezpiecznych λ_S i niebezpiecznych λ_D:

$$\lambda = \lambda_S + \lambda_D \tag{1}$$

Wskaźnik uszkodzeń bezpiecznych *FS*:

$$FS = \frac{\lambda_S}{\lambda} \tag{2}$$

Zatem:

$$\lambda_S = FS \cdot \lambda \tag{3}$$

$$\lambda_D = (1 - FS) \cdot \lambda \tag{4}$$

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \tag{5}$$

Wskaźnik pokrycia diagnostycznego *DC*:

$$DC = \frac{\lambda_{DD}}{\lambda_D} \tag{6}$$

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

$$\lambda_{DU} = (1 - DC) \cdot \lambda_D = (1 - DC)(1 - FS) \cdot \lambda \tag{8}$$

Zatem:

$$\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU} \tag{9}$$

Całkowita intensywność uszkodzeń jest sumą intensywności uszkodzeń niebezpiecznych wykrywalnych przez testy diagnostyczne λ_{DD}, niebezpiecznych niewykrywalnych λ_{DU}, bezpiecznych wykrywalnych λ_{SD} i bezpiecznych niewykrywalnych λ_{SU}.

P_{FDavg} i P_{FH} całego systemu jest sumą składowych prawdopodobieństw dla poszczególnych podsystemów:

$$P_{FDavgSYS} = P_{FDavgS} + P_{FDavgPLC} + P_{FDavgA} \tag{10}$$

$$P_{FHSYS} = P_{FHS} + P_{FHPLC} + P_{FHA} \tag{11}$$

Modele probabilistyczne dla przykładowych struktur wg IEC 61508:

Struktura 1 z 1:

$$\begin{aligned} &P_{FDavg1z1} = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \\ &gdzie: \\ &t_{CE} = \frac{\lambda_{DU}}{\lambda_D}(\frac{T_I}{2} + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR \\ &zatem: \\ &P_{FDavg1z1} = \frac{\lambda_{DU} T_I}{2} + \lambda_D MTTR \end{aligned} \tag{12}$$

$$P_{FH1z1} = \lambda_{DU} \tag{13}$$

Struktura 1 z 2:

$$\begin{aligned} &P_{FDavg1z2} = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU} (\frac{T_I}{2} + MTTR) \\ &gdzie: \\ &t_{GE} = \frac{\lambda_{DU}}{\lambda_D}(\frac{T_I}{3} + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR \\ &\beta = 2 \cdot \beta_D \end{aligned} \tag{14}$$

T_I – czas między testami

MTTR – średni czas naprawy

β - współczynnik uszkodzeń zależnych

$$P_{FH1z2} = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D \lambda_{DD} + \beta \lambda_{DU} \tag{15}$$

Struktura 2 z 2:

$$P_{FDavg2z2} = 2(\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} \tag{16}$$

$$P_{FH2z2} = 2 \cdot \lambda_{DU} \tag{17}$$

Struktura 2 z 3:

$$P_{FDavg2z3} = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(\frac{T_I}{2} + MTTR) \tag{18}$$

$$P_{FH2z3} = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} + \beta_D \lambda_{DD} + \beta\lambda_{DU} \tag{19}$$

Dla układów nienaprawialnych MTTR = ∞, zależności są następujące:

Struktura 1 z 1:

$$P_{FDavg1z1} = \frac{\lambda_{DU} \cdot T_I}{2} \tag{20}$$

Struktura 1 z 2:

$$P_{FDavg1z2} = \frac{(\lambda_{DU} \cdot T_I)^2}{3} + \beta \cdot \lambda_{DU} \cdot \frac{T_I}{2} \tag{21}$$

Struktura 2 z 2:

$$P_{FDavg2z2} = \lambda_{DU} \cdot T_I \tag{22}$$

Struktura 1 z 3

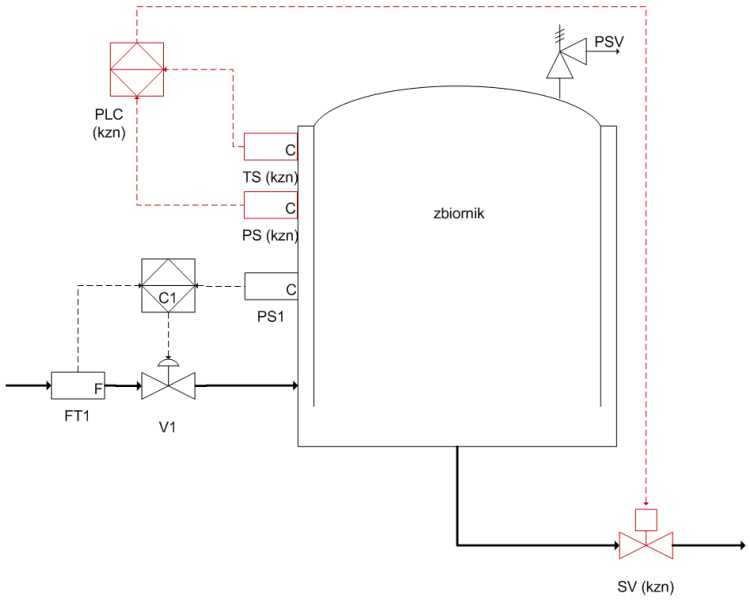
$$P_{FDavg1z3} = \frac{(\lambda_{DU} \cdot T_I)^3}{4} + \beta \cdot \lambda_{DU} \cdot \frac{T_I}{2} \tag{23}$$

Struktura 2 z 3:

$$P_{FDavg2z3} = (\lambda_{DU} \cdot T_I)^2 + \beta \cdot \lambda_{DU} \cdot \frac{T_I}{2} \tag{24}$$

Zadanie

1. Dla przykładowego systemu związanego z bezpieczeństwem E/E/PE (rys. 1) realizującego wybraną funkcję bezpieczeństwa (ochrona reaktora przed wybuchem), dla której określono w procesie oceny ryzyka wymagania na poziomie SIL3, należy zweryfikować poziom nienaruszalności bezpieczeństwa SIL, czyli sprawdzić czy zaproponowana struktura sprzętowa spełnia te wymagania (SIL3).
   W pierwszej kolejności poziom SIL sprawdzić należy dla struktury zbudowanej z pojedynczych elementów, tzn. bez zastosowania nadmiarowości sprzętowej. Następnie wprowadzić należy poprawną redundancję do wybranego podsystemu (np. pomiarowego, logicznego, wykonawczego) i powtórzyć analizę, aż do uzyskania spełnienia wymagań na poziom nienaruszalności bezpieczeństwa.
   Do weryfikacji wykorzystać należy metodę FTA (ang. *Fault Tree Analysis*).



Rys. 2. Obiekt z systemami BPCS i SIS (Wymagania dla systemu zabezpieczeń SIL3 określone na podstawie analizy ryzyka)

Tablica 2. Dane niezawodnościowe elementów systemu SIS

	DI	CPU	DO	Zawór	PS	TS
λ [1/h]	1.2E-06	2,2E-06	6.5E-07	1.60E-06	4.00E-06	2.00E-06
FS [%]	50%	50%	50%	50%	50%	50%
λ_D [1/h]	5.46E-07	1.04E-06	3.10E-07	6.50E-07	2.00E-06	1.00E-06
λ_S [1/h]	5.46E-07	1.04E-06	3.10E-07	6.50E-07	2.00E-06	1.00E-06
DC [%]	90%	90%	90%	90%	90%	90%
λ_{DD} [1/h]	4.91E-07	9.38E-07	2.79E-07	5.85E-07	1.80E-06	9.00E-07
λ_{DU} [1/h]	5.46E-08	1.04E-07	3.10E-08	6.50E-08	2.00E-07	1.00E-07
λ_{SD} [1/h]	4.91E-07	9.38E-07	2.79E-07	5.85E-07	1.80E-06	9.00E-07
λ_{SU} [1/h]	5.46E-08	1.04E-07	3.10E-08	6.50E-08	2.00E-07	1.00E-07
MTTR[h]	8	8	8	8	8	8
T_I [rok]	1	1	1	1	1	1
β	0.02	0.02	0.02	0.02	0.02	0.02

$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgPLC} + PFD_{avgA}$$

2. Dla zdefiniowanych funkcji bezpieczeństwa (lab 1), dla których przeprowadzona została ocena ryzyka wraz z określeniem wymaganych poziomów SIL (lab 2), zaproponować struktury sprzętowe realizujące te funkcje (oprzeć się w głównej mierze na zdefiniowanym dla nich wcześniej opisie funkcjonalnym).
3. Wykonać weryfikację poziomów SIL dla zaproponowanych struktur sprzętowych realizujących funkcje bezpieczeństwa. W przypadku nie spełnienia wymagań przez zaprojektowany system zaproponować redundancję sprzętową wybranego podsystemu (np. pomiarowego, logicznego, wykonawczego) i zweryfikować jej poziom SIL.