Weryfikacja poziomów nienaruszalności bezpieczeństwa SIL przykładowych struktur sprzętowych systemów SIS

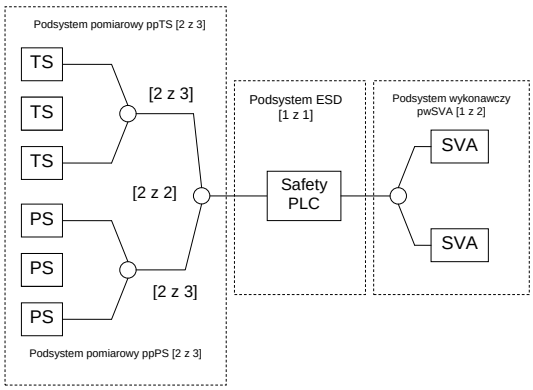
Warstwa sprzętowa realizująca funkcję bezpieczeństwa zapobiegającą powstaniu eksplozji zbiornika składa się z trzech podsystemów: pomiarowego w skład którego wchodzą dwie matryce detektorów ciśnienia PS i temperatury TS; podsystemu ESD, którego integralną częścią jest system przetwarzający dane (sterownik safety PLC, SRS (ang. *safety related system*) 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 rys. 1- system SIS (I), rys. 2 - system SIS (II) oraz rys. 3 - system SIS (III). Wartości PFD_{avg} dla systemu zabezpieczeniowego należy wyznaczyć z wykorzystaniem danych niezawodnościowych znajdujących się w tab. 1 (opracowanych na podstawie bazy danych OREDA i poradników SINTEF - Reliability Data for Safety Instrumented Systems, PDS DATA HANDBOOK 2010 EDITION).

W tablicy 1 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.

Tablica 1. Dane niezawodnościowe dla elementów systemu zabezpieczeniowego

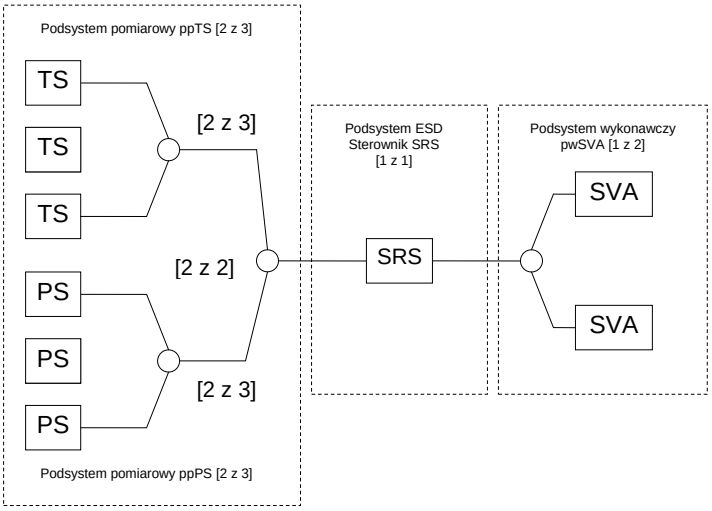
	SVA	**Safety PLC**	**SRS**	**PLC**	**PS**	**TS**
DC [%]	24	90	90	66	54	66
λ_{DU} [1/h]	$8 \cdot 10^{-7}$	$1 \cdot 10^{-6}$	$1 \cdot 10^{-7}$	$5 \cdot 10^{-6}$	$3 \cdot 10^{-7}$	$1.5 \cdot 10^{-6}$
MTTR [h]	8	8	8	8	8	8
T_I [h]	8760	8760	8760	8760	8760	8760
β	0.02	0.01	0.01	0.01	0.02	0.02

Na rys. 1 znajduje się pierwsza struktura sprzętowa systemu SIS (I), która oparta została na układzie sterownika bezpieczeństwa safety PLC.



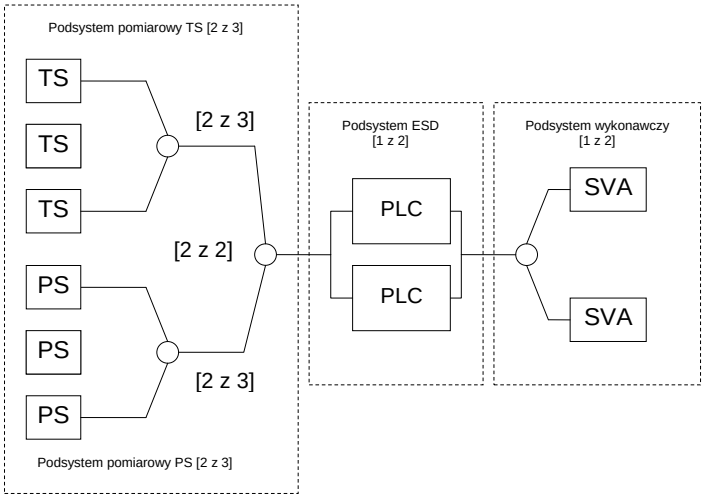
Rys. 1. Architektura systemu SIS (I) wyposażona w sterownik „safety PLC" (matryce detektorów pracują w konfiguracji 2 z 2)

W drugim z rozpatrywanych przypadków w systemie SIS (II) zastosowano w podsystemie ESD jednostkę SRS o lepszych parametrach niezawodnościowych od sterownika safety PLC (rys. 2).



Rys. 2. Architektura systemu SIS (II) wyposażona w układ SRS

Na rys. 3 przedstawiono system SIS (III), dla którego w podsystemie ESD zastosowano dwa sterowniki PLC w konfiguracji 1 z 2.



Rys. 3. Architektura systemu SIS (III) wyposażona w dwa sterowniki PLC (1 z 2)

Uwzględniając dane niezawodnościowe zawarte w tablicy 1 oraz korzystając z analizy drzew niezdatności FTA, należy dokonać weryfikacji SIL przedstawionych powyżej struktur sprzętowych SIS (I, II i III) znajdujących się na rysunkach 1, 2 i 3.

Badany system SIS realizuje funkcję bezpieczeństwa, dla której na podstawie analizy ryzyka określono poziom SIL3. Uzyskane w trakcie weryfikacji rezultaty, wraz z całościową specyfikacją sprzętową weryfikowanych systemów SIS należy zestawić w raporcie końcowym.

Informacje dodatkowe

Kryteria probabilistyczne wg PN-EN 61508 i PN-EN 61511

SIL	PFD_{avg}	PFH
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	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

SIL - poziom nienaruszalności bezpieczeństwa (ang. *safety integrity level*)

PFD_{avg} - przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na żądanie

PFH - prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę

Prawdopodobieństwo niezdatności (uszkodzenia systemu) można obliczyć wykorzystując technikę cięć minimalnych (uzyskanych z analizy FTA), korzystając z zależności:

$$Q_0 \approx \sum_{j=1}^{n} \prod_{i \in K_j} q_i$$

gdzie:

j – kolejne cięcie minimalne,
n – ilość cięć minimalnych,
i – kolejny element w cięciu minimalnym,
K_j – *j-te* cięcie minimalne,
q_i – wskaźnik niegotowości (prawdopodobieństwo uszkodzenia) *i-tego* elementu systemu.