XXIV Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE 2014

Oddział Gdański PTETiS

WERYFIKACJA POZIOMÓW NIENARUSZALNOŚCI BEZPIECZEŃSTWA Z UWZGLĘDNIENIEM ASPEKTÓW OCHRONY INFORMACJI

Marcin ŚLIWIŃSKI[1], Tomasz BARNERT[2], Emilian PIESIK[3]

1. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: 58 347 14 35 fax: 58 347 24 87 e-mail: m.sliwinski@ely.pg.gda.pl
2. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: 58 347 14 35 fax: 58 347 24 87 e-mail: t.barnert@ely.pg.gda.pl
3. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: 58 347 14 35 fax: 58 347 24 87 e-mail: e.piesik@ely.pg.gda.pl

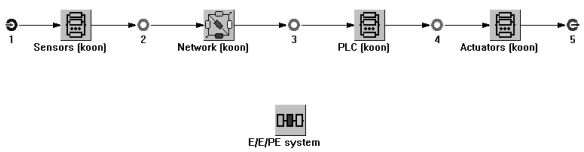
Streszczenie: Poszczególnym poziomom SIL projektowanego systemu elektrycznego/elektronicznego/programowalnego elektr onicznego E/E/PE (BPCS lub SIS) odpowiadają ilościowe kryteria probabilistyczne. Dowód spełnienia przez system zabezpieczeń wymagań SIL nazywa się weryfikacją. Model probabilistyczny dowolnego systemu zabezpieczeń SIS można przedstawić za pomocą schematów blokowych niezawodności RBD, grafów Markowa, równań uproszczonych oraz drzew niezdatności FTA. W niniejszym referacie przedstawiono wykorzystanie metod (w ramach aktualizacji metodyki analiz bezpieczeństwa funkcjonalnego) weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji m.in. poprzez wykorzystanie w tym procesie poziomów uzasadnionego zaufania EAL, lub przypisaniu analizowanemu systemowi stopnia ochrony informacji na podstawie liczby pierścieni zabezpieczeniowo ochronnych wg metodyki SeSa - SINTEF, wraz z uwzględnieniem klasyfikacji systemów rozproszonych, w module weryfikacji SIL autorskiego oprogramowania ProSIL-EAL.

Słowa kluczowe: SIL, EAL, SeSa, modelowanie, weryfikacja.

1. WIADOMOŚCI OGÓLNE

1.1. Wprowadzenie

W modelowaniu probabilistycznym rozproszonych systemów sterowania DCS lub automatyki zabezpieczeniowej SIS należy uwzględnić infrastrukturę przemysłowej sieci komputerowej. Budując taki model można wykorzystać technikę ścieżek, cięć minimalnych lub schematów blokowych niezawodności [1, 2, 3, 4, 6]. Na rysunku 1 znajduje się model systemu SIS w postaci schematów blokowych niezawodności RBD (ang. *reliability block diagram*).



Rys. 1. Schemat blokowy niezawodności systemu SIS

Po uwzględnieniu struktury fizycznej sieci komputerowej w rozproszonym systemie sterowania lub zabezpieczeń prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie można wyznaczyć stosując zależność [1, 3, 4, 6]:

$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgNet} + PFD_{avgPLC} + PFD_{avgA} \qquad (1)$$

gdzie: PFD_{avgSYS} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie systemu E/E/PE (BPCS lub SIS); PFD_{avgS} – podsystemu pomiarowego; PFD_{avgNet} – warstwy sieciowej; PFD_{avgPLC} – sterownika programowalnego i PFD_{avgA} – podsystemu elementów wykonawczych.

1.2. Klasyfikacja rozproszonych systemów E/E/PE

Na potrzeby integracji zagadnień bezpieczeństwa funkcjonalnego (*safety*) i ochrony informacji (*security*) dokonano klasyfikacji systemów E/E/PE na trzy kategorie [1]:

I. Systemy zainstalowane w obiektach krytycznych skupionych (np. rafinerie, instalacje chemiczne, obiekty wojskowe), wykorzystujące wyłącznie wewnętrzne kanały przesyłu informacji (np. sieć lokalną),

II. Systemy zainstalowane w krytycznych obiektach rozproszonych (np. rurociągi, gazociągi, system energetyczny), w których istnieją wewnętrzne kanały transmisji informacji i mogą być wykorzystywane również zewnętrzne kanały przesyłania danych,

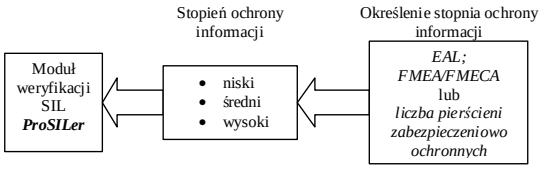
III. Systemy zainstalowane w obiektach i w systemach infrastruktury krytycznej (np. systemy transportowe - kolej, lotnictwo, transport morski itd.), w których wykorzystywane są wyłącznie zewnętrzne kanały transmisji danych.

Proponowana klasyfikacja opiera się na identyfikacji sposobu transmisji danych pomiędzy poszczególnymi elementami analizowanych systemów.

1.3. Przypisanie stopnia ochrony informacji

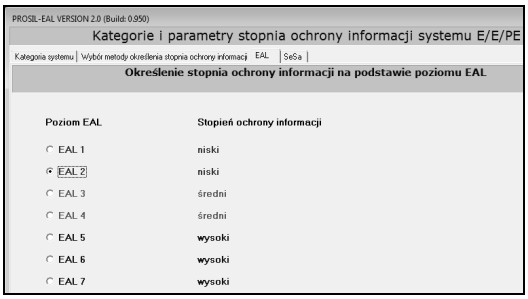
W przypadku weryfikacji SIL powstaje zasadnicze pytanie, w jaki sposób uwzględnić zagadnienia ochrony informacji. Czy poprzez integrację SIL i EAL, czy też wyznaczając stopień ochrony informacji (niski, średni lub wysoki) w inny sposób. Na przykład przez wykonywanie dla każdego prototypowego rozproszonego systemu E/E/PE (BPCS, DCS lub SIS) szczegółowej analizy rodzajów, skutków i krytyczności uszkodzeń FMECA (ang. *failure mode*,

effect and criticality analysis) umożliwiającej zbadanie wpływu infrastruktury sieciowej na brak wykonania funkcji bezpieczeństwa przez system SIS [1] (rys 2).



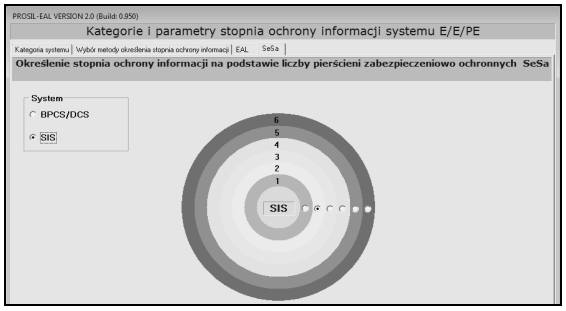
Rys. 2. Przypisanie stopnia ochrony informacji

Na rys. 3 przedstawiono kategoryzację poziomów ochrony informacji z wykorzystaniem poziomów uzasadnionego zaufania EAL [5, 7].



Rys. 3. Okno określenia stopnia ochrony informacji wg Common Criteria ISO/IEC 15408 w aplikacji ProSIL-EAL

W danym przypadku typ i liczba podatności na zagrożenia mają źródło w przedstawionej wcześniej klasyfikacji na kategorie rozpatrywanych systemów sterowania i zabezpieczeń (I, II i III kategorii). Innym podejściem jest zastosowanie metodyki SeSa (ang. *SecureSafety*) opracowanej przez SINTEF, w której bierze się pod uwagę pierścienie zabezpieczeniowo ochronne (rys. 4) [7, 8].



Rys. 4. Pierścienie zabezpieczeniowo ochronne w systemach BPCS, DCS i SIS wyposażonych w przemysłową sieć komputerową (aplikacja ProSIL-EAL)

Przy weryfikacji SIL w centralnej części znajduje się system SIS, natomiast stopień ochrony informacji (niski, średni lub wysoki) określa się na podstawie liczby pierścieni wokół niego.

2. WERYFIKACJA SIL Z UWZGLĘDNIENIEM OCHRONY INFORMACJI

2.1. Zweryfikowany SIL z uwzględnieniem stopnia ochrony informacji

W procesie weryfikacji poziomy SIL odnoszą się do struktury sprzętowej systemu SIS realizującego konkretne funkcje bezpieczeństwa (np. ochrona reaktora przed eksplozją). Przyjęto, że niepożądane zdarzenia i działania z zewnątrz przy niskim stopniu ochrony informacji (np. EAL1 lub 2) mogą wpływać niekorzystnie na wypełnienie przez system SIS funkcji bezpieczeństwa.

W tablicy 1 przedstawiono propozycję takiej zależności dla systemów II oraz III kategorii. W nawiasie znajdują się zmodyfikowane poziomy SIL dla systemu III kategorii, gdyż jest on bardziej podatny na działania z zewnątrz.

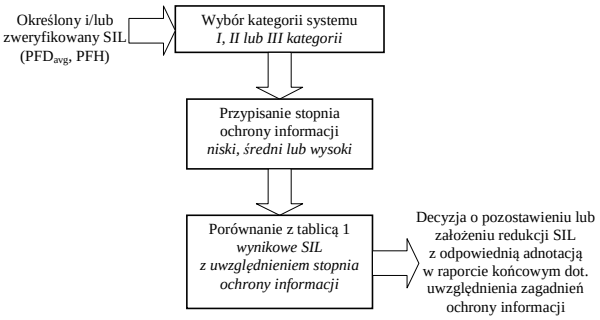
Tablica 1. Wynikowe poziomy SIL z uwzględnieniem poziomów EAL dla systemów II i III kategorii [1, 7]

		Weryfikowany SIL dla systemu II kat. (III kat.)			
Ochrona informacji		*Bezpieczeństwo funkcjonalne*			
EAL	poziom	1	2	3	4
1	niski	- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
2		- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
3	średni	SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4		SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	wysoki	SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
6		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
7		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)

Niski poziom uzasadnionego zaufania EAL, przy weryfikacji określonego poziomu SIL, może w rezultacie skutkować jego obniżeniem.

2.2. Procedura weryfikacji SIL

Schemat procedury weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji przedstawiono na rys. 5 [1, 7].

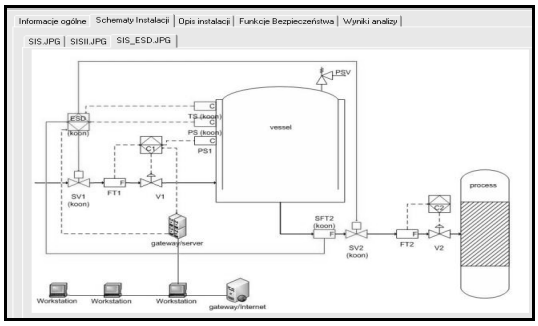


Rys. 5. Procedura weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji

Przed uwzględnieniem zagadnień ochrony informacji w procesie weryfikacji SIL powinien być zweryfikowany SIL w sposób jakościowy lub ilościowy. Następnie należy dokonać określenia kategorii (I, II lub III) systemu realizującego funkcję lub funkcje bezpieczeństwa. W przypadku systemu I kategorii zagadnienia związane z ochroną informacji nie będą rozpatrywane (zweryfikowany SIL pozostaje bez zmian). W przypadku wyboru systemu II lub III kategorii, należy przejść do kolejnego kroku związanego z przypisaniem stopnia ochrony informacji (niski, średni lub wysoki), który uzależniony jest od poziomu uzasadnionego zaufania EAL lub liczby pierścieni zabezpieczeniowo ochronnych (1 pierścień – niski, od 2 do 4 średni, powyżej 5 wysoki). Następnie wynikowy SIL z uwzględnieniem przypisanego stopnia ochrony informacji dla systemów II i III kategorii należy porównać z tab. 1 alokującą SIL poddany weryfikacji przed uwzględnieniem stopnia ochrony informacji, na wynikowy SIL z uwzględnieniem stopnia ochrony informacji. W wyniku czego uzyskuje się decyzję o założeniu redukcji SIL z odpowiednią adnotacją w raporcie końcowym dot. uwzględnienia zagadnień ochrony informacji [1, 7].

2.3. Przykład weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji

Weryfikację SIL z uwzględnieniem zagadnień ochrony informacji przeprowadzono z wykorzystaniem autorskiego oprogramowania ProSIL-EAL będącego rozbudowaną wersją narzędzia komputerowego ProSIL [3].



Rys. 6. ProSIL-EAL – schemat P&ID rozpatrywanej instalacji wraz z systemem sterowania BPCS i zabezpieczeń SIS

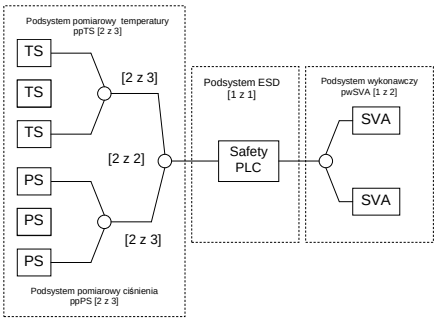
Na podstawie analizy ryzyka określono wymagania poziomu nienaruszalności SIL3 dla funkcji bezpieczeństwa wykonywanej przez system SIS [4, 6]. W nawiązaniu do procedury weryfikacji SIL przedstawionej na rys. 5, na początku należy przeprowadzić tę czynność metodą klasyczną [4, 6]. W tablicy 2 zestawiono dane niezawodnościowe elementów systemu SIS poddanego weryfikacji.

Tablica 2. Dane niezawodnościowe dla elementów systemu zabezpieczeniowego [1, 3, 7, 9]

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

W danym przypadku zostały poddane analizie dwie struktury przykładowego systemu SIS, których schematy przedstawione zostały na rysunkach 7 SIS(I) i 8 SIS(II). Wartości PFD_{avg} dla analizowanych struktur zostały wyznaczone z wykorzystaniem autorskiego oprogramowania ProSIL-EAL.

Na rys. 7 znajduje się pierwsza struktura sprzętowa systemu SIS (I), która oparta została na układzie sterownika bezpieczeństwa *safety* PLC.



Rys. 7. Architektura systemu SIS (I) wyposażona w sterownik „safety PLC" (matryce detektorów pracują w konfiguracji 2 z 2)

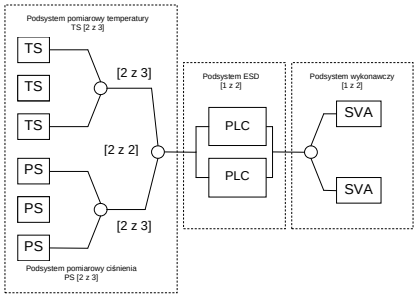
Uwzględniając dane niezawodnościowe zawarte w tablicy 2 uzyskano wyniki, które wraz z całościową specyfikacją sprzętową systemu SIS (I) zestawiono w raporcie końcowym znajdującym się w tablicy 3.

Tablica 3. Raport wynikowy weryfikacji SIL dla systemu SIS (I)

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

$$PFD_{avgSIS(I)} \cong PFD_{avgTS(2z3)} + PFD_{avgPS(2z3)} + PFD_{avgSafetyPLC} + PFD_{avgSVA(1z2)} \cong$$
$$\cong 2.93\cdot10^{-5} + 3.11\cdot10^{-5} + 4.44\cdot10^{-3} + 7.14\cdot10^{-5} \cong 4.57\cdot10^{-3}$$

Z powyższego wynika, że struktura sprzętowa systemu SIS(I) nie spełnia wymagań SIL3. Na rys. 8 przedstawiono system SIS (II), dla którego w podsystemie ESD zastosowano dwa sterowniki PLC w konfiguracji 1 z 2.

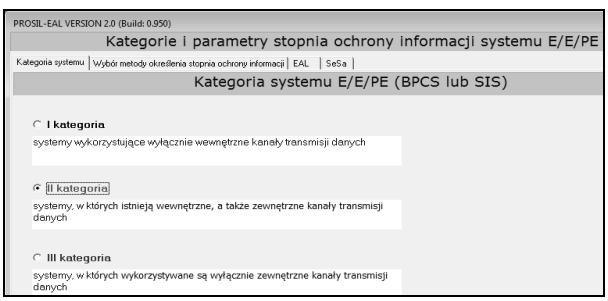


Rys. 8. Architektura systemu SIS (II) wyposażona w dwa sterowniki PLC (pracujące w konfiguracji 1 z 2)

$$PFD_{avgSIS(II)} \cong PFD_{avgTS(2z3)} + PFD_{avgPS(2z3)} + PFD_{avgPLC(1z2)} + PFD_{avgSVA(1z2)} \cong$$
$$\cong 2.93\cdot10^{-5} + 3.11\cdot10^{-5} + 6\cdot10^{-4} + 7.14\cdot10^{-5} \cong 7.32\cdot10^{-4}$$

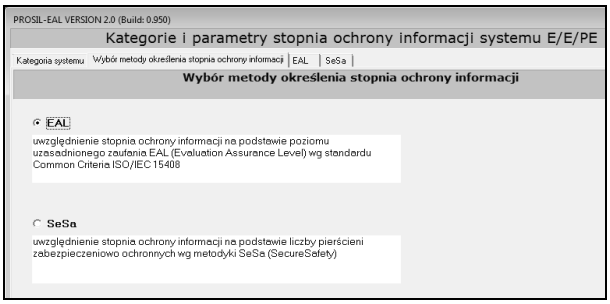
System SIS (II) zrealizowany z wykorzystaniem standardowych sterowników programowalnych PLC z redundancją w podsystemie ESD spełnia wymagania SIL3. Punktowa wartość prawdopodobieństwa $PFD_{avgSIS(II)} = 7.32 \cdot 10^{-4}$ mieści się w przedziale kryterialnym odpowiadającym poziomowi SIL3. Jest to początek procedury weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji przedstawionej na rys. 5.

W aplikacji ProSIL-EAL pierwszą czynnością w analizie, wg przedstawionej wcześniej metodyki jest określenie kategorii systemu (rys. 9).



Rys. 9. Okno wyboru kategorii systemu E/E/PE (BPCS lub SIS) w aplikacji ProSIL-EAL

Następnie należy dokonać wyboru jednej z dwóch metod określenia stopnia ochrony informacji, przypisanej do analizowanego systemu SIS w przypadku weryfikacji SIL (rys. 10).



Rys. 10. Okno wyboru metody określenia stopnia ochrony informacji w aplikacji ProSIL-EAL na potrzeby analiz bezpieczeństwa funkcjonalnego - EAL lub SeSa

W danym przypadku poziom uzasadnionego zaufania dla rozpatrywanego systemu spełniał wymagania EAL2 zatem stopień ochrony informacji jest niski. Kolejnym krokiem jest "zmapowanie" powyższych informacji do tablicy 1, zawierającej wynikowe SILe (po procesie weryfikacji) z uwzględnieniem stopnia ochrony informacji i kategorii rozpatrywanego systemu. W danym przypadku $PFD_{avg} = 7.32 \cdot 10^{-4}$ (SIL3), system II kategorii z niskim stopniem ochrony informacji (EAL2) – zatem weryfikowany poziom nienaruszalności po uwzględnieniu aspektów ochrony informacji to SIL2. Zestawienie uzyskanych wyników przedstawiono w tabl. 4.

Tablica 4. Raport wynikowy weryfikacji SIL z uwzględnieniem aspektów ochrony informacji – dla systemu II kategorii SIS(III)

SIS	**Zweryfikowany SIL**	
EAL/stopień ochrony informacji	**bez ochrony informacji**	**z ochroną informacji**
brak/brak (podejście klasyczne)	SIL3	-
EAL2/niski	SIL3	SIL2
EAL3/średni	SIL3	SIL3

Aby spełnić wymagania kryterialne SIL3 postawione systemowi SIS, należy zwiększyć stopień ochrony informacji systemu SIS(II) do średniego (równy lub większy od EAL3, bądź wg SeSa – 2 lub więcej pierścieni zabezpieczeniowo ochronnych).

Zaprezentowany przykład przedstawia możliwość uwzględnienia zagadnień związanych z ochroną informacji w procesie weryfikacji SIL. Z powyższego widać, że kluczową rolę w proponowanym postępowaniu (wg tabl. 1) odgrywa kategoria rozpatrywanego systemu SIS. W danym przypadku był to system II kategorii. Gdyby rozpatrywany system należał do III kategorii, wówczas otrzymany poziom SIL zredukowałby się do SIL1 (aby zapewnić spełnienie wymagań SIL3 trzeba by było zapewnić ochronę informacji zdefiniowaną wysokim stopniem – EAL5 wg common criteria, lub powyżej 5 pierścieni zabezpieczeniowo ochronnych wg metodyki SeSa). Wykorzystując podejście przedstawione powyżej można dokonać weryfikacji określonego poziomu SIL dla punktowej wartości PFD_{avg} (lub PFH) uzyskanej dla systemu SIS z uwzględnieniem aspektów ochrony informacji.

3. PODSUMOWANIE

W niniejszym referacie przedstawiono podejście metodyczne integracji analizy i oceny bezpieczeństwa funkcjonalnego rozproszonych systemów sterowania, i zabezpieczeń w obiektach infrastruktury krytycznej w nawiązaniu do wymagań norm PN-EN 61508 i PN-EN 61511 z uwzględnieniem zasad ochrony informacji według ISO/IEC 15408 (poziomy EAL) oraz metodyki SeSa SINTEF, na przykładzie procesu weryfikacji poziomów SIL. Zaprezentowane podejście stanowi aktualizację metodyki zawartej w normach PN-EN 61508 oraz PN-EN 61511 i zostało zaimplementowane w programie ProSIL-EAL.

4. BIBLIOGRAFIA

1. Barnert T., Śliwiński M.: Bezpieczeństwo funkcjonalne i ochrona informacji w obiektach i systemach infrastruktury krytycznej, Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa, str. 476-507. Wolters Kluwer, 2013.
2. Barnert T., Kosmowski K.T., Śliwiński M.: Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issues. PSAM, Seattle, USA, 2010.
3. Śliwiński M., Barnert T., Piesik E.: Wspomagana komputerowo weryfikacja poziomu nienaruszalności bezpieczeństwa z wykorzystaniem autorskiej aplikacji ProSIL, ZNWEiA PG Nr 36, Gdańsk 2013.
4. IEC 61511:2015 Ed.2: Functional safety – Safety instrumented systems for the process industry sector.
5. ISO/IEC 15408:1999: Information technology – Security techniques – Evaluation criteria for IT security Part 1÷3.
6. PN-EN 61508:2010. Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1-7. PKN.
7. Projekt VI.B.10: Opracowanie metod i narzędzi do wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym i ochroną informacji, Gdańsk 2013.
8. SINTEF.: The SeSa method for assessing secure remote access to safety instrumented systems. A1626, 2007.
9. Reliability Data for Safety Instrumented Systems - PDS Data Handbook. SINTEF 2010 Edition.

SECURITY ASPECTS IN VERIFICATION OF THE SAFETY INTEGRITY LEVEL

Key-words: safety integrity level (SIL), evaluation assurance level (EAL), SeSa, probabilistic modelling, verification

The article addresses some important issues of the functional safety analysis, namely the safety integrity level (SIL) verification of distributed control and protection systems with regard to security aspects. A quantitative method for SIL (IEC 61508, 61511) verification, based on so called evaluation assurance levels (EAL) and Secure Safety (SeSa) methodology, is presented. In this article is described a prototype ProSIL-EAL software system for computer-aided functional safety management. In ProSIL-EAL the methods (e.g. veryfying the SIL level of SIS) concerning functional safety analysis in the process of the design and operation of Safety Instrumented Systems (SIS) with security aspects are implemented according to PN-EN 61508, PN-EN 61511, ISO/IEC 15408 standards and SeSa - SINTEF methodology.