Journal of KONBiN 3(6)2008
ISSN 1895-8281

DOI 10.2478/v10040-008-0056-0

SECURITY ASPECTS IN VERIFICATION OF THE SAFETY INTEGRITY LEVEL OF DISTRIBUTED CONTROL AND PROTECTION SYSTEMS

PROBLEMATYKA OCHRONY INFORMACJI PRZY WERYFIKACJI POZIOMU NIENARUSZALNOŚCI BEZPIECZEŃSTWA ROZPROSZONYCH SYSTEMÓW STEROWANIA I ZABEZPIECZEŃ

Barnert Tomasz[1], Kosmowski Kazimierz[2], Śliwiński Marcin[3]

Gdansk University of Technology, Faculty of Electrical and Control Engineering
G. Narutowicza 11/12, 80-952 Gdańsk

e-mails: (1) t.barnert@ely.pg.gda.pl, (2) k.kosmowski@ely.pg.gda.pl, (3) m.sliwinski@ely.pg.gda.pl

Abstract: 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) verification, based on so called differential factors, is presented. Taking into account SIL and the evaluation assurance level (EAL), which concerns the level of information security within entire system, two parametrical criterion function is defined for the SIL verification.

Keywords: safety, security, safety integrity level, evaluation assurance level

Streszczenie: W niniejszym artykule przedstawiono najważniejsze zagadnienia związane z weryfikacją poziomu nienaruszalności bezpieczeństwa SIL rozproszonych systemów sterowania i zabezpieczeń z uwzględnieniem aspektów ochrony informacji. Przedstawiono ilościową metodę weryfikacji poziomu SIL z wykorzystaniem wskaźników różnicowych oraz dwuparametrową funkcję kryterialną łączącą wymagania SIL oraz EAL (poziom uzasadnionego zaufania dla ochrony informacji).

Słowa kluczowe: bezpieczeństwo, ochrona informacji, poziom nienaruszalności bezpieczeństwa, poziom uzasadnionego zaufania

SECURITY ASPECTS IN VERIFICATION OF THE SAFETY INTEGRITY LEVEL OF DISTRIBUTED CONTROL AND PROTECTION SYSTEMS

1. Introduction

Quantitative methods are preferable for the SIL verification, especially when reliability data for analyzed system are known or acquired from various sources including experts. Virtually without exception the reliability data are incomplete or have significant uncertainty, not only at system's design stage, but also in initial period of its operation [1,3,8]. So, there are known problems with general reliability data adjustment for specific conditions as well as the database periodical updates during the system operation [6].

Nowadays the internal and external communication channels are more and more extensively used in technical systems. They improve their functionality but can deteriorate the safety and security if not properly designed and operated. From practical point of view it is necessary to integrate the safety and security aspects. In the paper the classification of computerized systems is proposed as the starting point for the further functional safety and security analyses [7].

2. Verification of safety integrity level

2.1. Probabilistic modelling of the E/E/PE systems

Taking into account a method of minimal cuts, the probability of failure to perform the design function on demand can be evaluated based on following formula

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

where: K_j – j-th minimal cut set (MCS), $Q_i(t)$ - probability of j-th minimal cut set; n – the number of MCS, $q_i(t)$ - probability of failure to perform the design function by i-th – subsystem or element.

The average probability of failure to perform the design function on demand for the system in relation to formula (1), assuming that all subsystems are tested with the interval T_I, is calculated as follows

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

The probability per hour (frequency) of a dangerous failure can be evaluated based on formula as below [2]

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

where: λ_i – the failure rate of i-th subsystem.

2.2. Sensitivity analysis of probabilistic models

An important aspect of the SIL verification is sensitivity analysis, i.e. how the changes of the model parameters influence final probabilistic results. For sensitivity analysis a method of partial flexibility function of many variables was applied. A demonstrative schema of probabilistic model of the E/E/PE system consisting of n-elements is shown on Fig. 1.

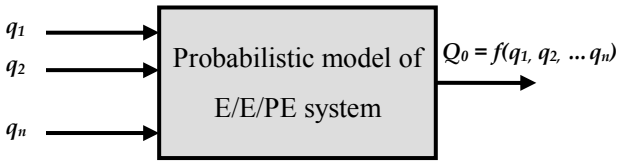


Fig. 1. A probabilistic model of the E/E/PE system

There is a question about percentage change of value Q_0 caused by percentage change of probabilistic model for *i*–th element. For $Q_0 = f(q_1, q_2, \ldots q_n)$, which is probabilistic model of the system, the partial flexibility function can be defined for *i*-th element ($i=1,2,\ldots,n$) as follows

$$MS_{q_i}^{WR} \cong \frac{q_i \cdot A_i}{f(q_1, q_2, ...q_n)} \cdot \frac{\partial f(q_1, q_2, ...q_n)}{\partial q_i} \tag{4}$$

where: A_i – the percentage value change for *i-th* element; thus, the sensitivity MS^{WR}_{qi} shows approximate percentage increment of value $Q_0 = f(q_1, q_2, ... q_n)$ in case of A_i percentage change of the value of q_i being a function of relevant parameters.

Knowing the value of MS^{WR}_{qi} it is possible, using the formula (4), to evaluate overall absolute increment from formula:

$$\begin{aligned} \Delta Q_0 &\cong \sum_{i=1}^{n} \Delta Q_{0q_i} = \sum_{i=1}^{n} MS_{q_i}^{WR} \cdot f(q_1, q_2, ...q_n) \\ &= \sum_{i=1}^{n} q_i \cdot A_i \cdot \frac{\partial f(q_1, q_2, ...q_n)}{\partial q_i} = \sum_{i=1}^{n} \Delta q_i \cdot w_i \end{aligned} \tag{5}$$

Using equation (5) the upper and lower bound of Q_0 [Q_0^l, Q_0^u] can be defined, based on changes of more important parameters with related weights w_i. A method proposed is presented in Fig. 2.

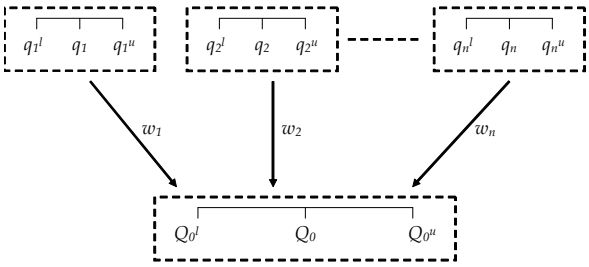


Fig. 2. The influence of elements' probability ranges on system probability uncertainty range

Knowing from statistical analysis or expert opinions the ranges of parameters in the probabilistic models it is possible to evaluate the ranges of PFD_{avg} [PFD_{avg}^l, PFD_{avg}^u] and PFH [PFH^l, PFH^u], i.e. relevant uncertainty intervals.

2.3. SIL verification under uncertainty

An useful index for verification of SIL is differential factor w_R. It contains information about position of PFD_{avg} or PFH point value in the criteria interval. It is the difference between values of criteria membership functions for the lower and upper bounds:

$$w_R = \mu_{SIL}^{l}(PFD_{avg}) - \mu_{SIL}^{u}(PFD_{avg}) \tag{6}$$

In case when the uncertainty ranges in determining PFD_{avg} (or PFH) are considered, two another indexes should be evaluated, namely two differential factors for the lower and upper bounds. Fig. 3 presents a general SIL verification method based on PFD_{avg} (or PFH) with uncertainty ranges. It is necessary to take into account the values of the lower and upper bounds for PFD_{avg} [$PFD_{avg}{}^{l}$, $PFD_{avg}{}^{u}$] (or PFH [PFH^{l}, PFH^{u}]).

$$\begin{aligned} w_R^l &= \mu_{SIL}^{l}(PFD_{avg}{}^{l}) - \mu_{SIL}^{u}(PFD_{avg}{}^{l}) \\ w_R^u &= \mu_{SIL}^{l}(PFD_{avg}{}^{u}) - \mu_{SIL}^{u}(PFD_{avg}{}^{u}) \end{aligned} \tag{7}$$

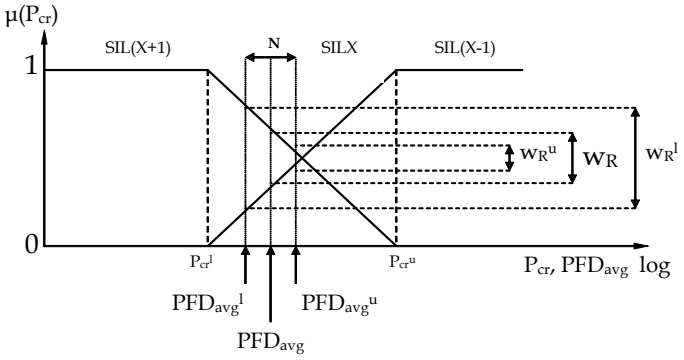


Fig. 3. The SIL level verification based on PFDavg (PFH) under uncertainty of results from probabilistic model

The verification of SIL level of the E/E/PE system, which probabilistic model consists of uncertainty is performed using a knowledge-based system. Its prototype is under development using MySQL software. The general idea is presented in Fig. 4.

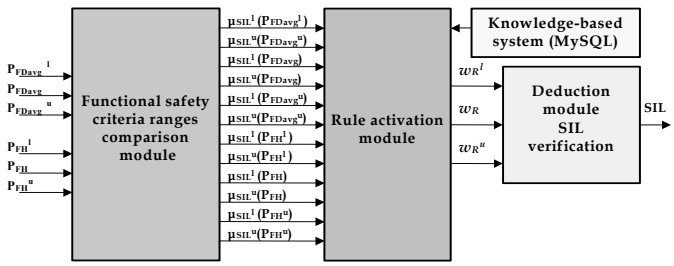


Fig. 4. SIL verification in situation of probabilistic modeling with assessing of uncertainty interval

Proposed in this section methods based on differential factors is helpful in an effective verification of required SIL of the E/E/PE system taking into account results of sensitivity analysis and/or assessment of uncertainty ranges obtained from probabilistic models developed.

3. Integrated functional safety and security analysis of the distributed control and protection systems

Some aspects of integrated functional safety and security analysis of the control and protection systems are described below. The presence of industrial computer network, its specification and type of data transfer methods are taken into account. There are three cases associated with some main categories of distributed control and protection systems:

I. Systems installed in concentrated critical objects using only the internal communication channels (e.g. local network LAN),
II. Systems installed in concentrated or distributed critical objects, where protection and monitoring system data are sent by internal communication channels and can be sent using external channels,
III. Systems installed in distributed critical objects, where data are sent only by external communication channels.

The requirements concerning a system to be analyzed is characterized by a two parametrical function $f_{i,j}$ [7]. The method of integrated functional safety and security analysis in distributed systems, which use various communication channels, is shown in Fig. 5. The function $f_{i,j}$ is taken into account in a further process of SIL (EAL) verification. The evaluation assurance level (EAL) is associated with a set of assurance requirements which covers the complete development of a product with a given level of strictness [5]. There are seven levels, with EAL1 being the most basic (the cheapest to implement and evaluate) and EAL7 being the most strict (the most expensive).

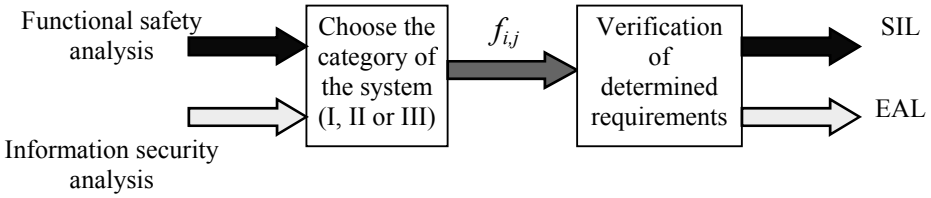


Fig. 5. Determining of function $f_{i,j}$ and verification of requirements [7]

Important task of integrated functional safety and security analysis of such systems is the verification of required SIL and EAL levels. The SIL is

connected with specific safety aspects while the EAL is concerned with level of information security of entire system performing monitoring, control and/or protection functions.

Table 1. SIL that can be claimed for given EAL for systems of II category (III category)

Determined		Verified SIL for II cat. (III cat.)			
security		*functional safety*			
EAL	level	1	2	3	4
1	basic	- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
2		- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
3	medium	SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4		SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	high	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)

It is possible that undesirable external events and malicious acts may influence the system by threatening to perform the safety-related functions in case of low security level. Thereby the low EAL may reduce the safety integrity level (SIL), and should be taken into account in the process of SIL verification.

4. Conclusion

The probabilistic models of E/E/PE systems, which are described in the IEC 61508 and IEC 61511, do not cover the uncertainty aspects of results obtained from these models. The method proposed in this paper take into consideration the sensitivity analysis of probabilistic models of E/E/PE systems as well as the uncertainty of probabilistic results obtained.

Uncertainty treating in risk analysis and probabilistic modeling is very important problem, especially in relation to the E/E/PE safety-related systems. It requires further research. A knowledge-based methods are in the development process for the SIL determination and the verification taking into account the diagnostic coverage of subsystems and modeling of dependencies (e.g. advanced β-factor method for modeling common cause failures).

There is also the challenge to include security aspects in designing the programmable control and protection systems operating in a network. An integrated approach is proposed, in which determining the required safety

integrity level (SIL) and evaluation assurance level (EAL) is related to the system category (I, II or III). Such integrated approach is justified, because not including security aspects in designing safety-related control and/or protection systems operating in network may result in deteriorating safety (lower SIL than required).

Due to importance of the problem for industrial practice further research should be undertaken to develop methodology and criteria integrating the safety and security aspects in designing and verifying the safety-related control and protection systems operating in networks.

Acknowledgement *The authors wish to thank the Ministry for Science and Higher Education in Warsaw for supporting the research and the Central Laboratory for Labour Protection (CIOP) for co-operation in preparing a research programme concerning the safety management of hazardous systems including functional safety aspects.*

References

1. Abrahamsson, M..: *Uncertainty in quantitative risk analysis – Characterisation and methods of treatment*. Report 1024. Lund. 2002
2. Barnert, T., Sliwinski, M.: *Methods for verification safety integrity level in control and protection systems*. Functional Safety Management in Critical Systems: 171-185. Jurata. Gdansk. 2007.
3. Beugin, J., Cauffriez, L., Renaux, D.: *A SIL quantification approach to complex systems for guided transportation*. Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2005 Gdynia - Sopot – Gdansk. London. 2005.
4. *IEC 61508. Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety related systems.* International Electrotechnical Commission (IEC). 1998
5. *ISO/IEC 15408: Information technology – Security techniques – Evaluation criteria for IT security.* 1999.
6. Kosmowski, K.T., Sliwinski, M.: *Methodology for functional safety assessment*. Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2005, Gdynia - Sopot – Gdansk. London. 2005.
7. Kosmowski, K.T., Sliwinski, M., Barnert, T.: *Functional safety and security assessment of the control and protection systems*. Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2006, Estoril. London. 2006.
8. Stavrianidis, P.: *Reliability and uncertainty analysis of hardware failures of programmable electronic system*. Reliability Engineering and System Safety Vol.39: 309 - 324. 1992.

PROBLEMATYKA OCHRONY INFORMACJI PRZY WERYFIKACJI POZIOMU NIENARUSZALNOŚCI BEZPIECZEŃSTWA ROZPROSZONYCH SYSTEMÓW STEROWANIA I ZABEZPIECZEŃ

1. Wstęp

Przy weryfikacji poziomu nienaruszalności bezpieczeństwa SIL szczególnie przydatne są metody ilościowe, w przypadku posiadania danych niezawodnościowych analizowanego systemu pochodzących z różnych źródeł, m.in. od ekspertów. W modelowaniu probabilistycznym systemów wykorzystywane dane są niepełne oraz obarczone niepewnością [1,3,8]. Istnieje problem z pozyskiwaniem danych niezawodnościowych oraz okresowym uaktualnianiem baz danych je przechowujących [6].

W systemach technicznych coraz częściej wykorzystywane są wewnętrzne oraz zewnętrzne kanały komunikacyjne. Poprawiają one funkcjonalność systemu, jednak mogą obniżyć jego ogólny poziom bezpieczeństwa, jeśli nie są zaprojektowane i użytkowane w odpowiedni sposób. W przypadku takich systemów istnieje konieczność integrowania aspektów bezpieczeństwa funkcjonalnego i ochrony informacji. W niniejszym artykule przedstawiono klasyfikacje skomputeryzowanych systemów sterowania i zabezpieczeń jako punkt wyjścia dla zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji [7].

2. Weryfikacja poziomu nienaruszalności bezpieczeństwa

2.1. Modelowanie probabilistyczne systemów E/E/PE

Biorąc pod uwagę metodę cięć minimalnych, prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez system zabezpieczeń można określić na podstawie zależności

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

gdzie: K_j – j-te cięcie minimalne (MCS), $Q_i(t)$ – prawdopodobieństwo wystąpienia j-tego cięcia minimalnego w funkcji czasu, n – ilość cięć MCS, $q_i(t)$ – prawdopodobieństwo uszkodzenia i-tego podsystemu lub elementu.

Wykorzystując zależność (1) można określić przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie, zakładając, że wszystkie podsystemy są testowane z czasem między testami okresowymi T_I, mającymi na celu wykrycie uszkodzeń niebezpiecznych.

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

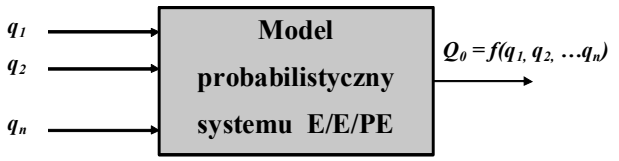
Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę może być oszacowane na podstawie wzoru poniżej [2]:

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

gdzie: λ_i – intensywność uszkodzeń *i*-tego podsystemu

2.2. Analiza wrażliwości modelu probabilistycznego

Do zbadania wrażliwości modelu probabilistycznego systemu sterowania lub zabezpieczeniowego, czyli wpływu poszczególnych elementów systemu na postać tego modelu, można zastosować zmodyfikowane pojęcie elastyczności cząstkowej funkcji wielu zmiennych. Na rys. 1 przedstawiony jest schemat poglądowy modelu probabilistycznego systemu E/E/PE zawierającego n elementów.



Rys. 1. Model probabilistyczny systemu E/E/PE

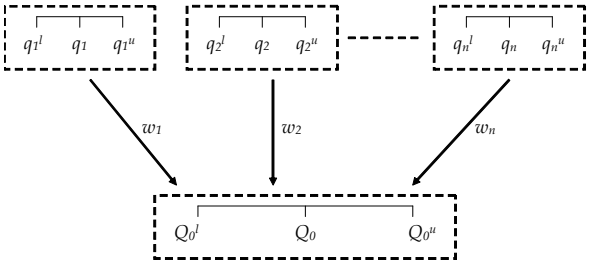
Powstaje pytanie jak procentowo zmieni się wartość Q_0 w wyniku *A* procentowej zmiany wartości *i*-tego elementu modelu. Dla funkcji wielu zmiennych $Q_0 = f(q_1, q_2, ... q_n)$ stanowiącej model probabilistyczny systemu E/E/PE, wykorzystując zmodyfikowane pojęcie elastyczności cząstkowej funkcji wielu zmiennych, można zdefiniować wrażliwość:

$$MS_{q_i}^{WR} \cong \frac{q_i \cdot A_i}{f(q_1, q_2, ...q_n)} \cdot \frac{\partial f(q_1, q_2, ...q_n)}{\partial q_i} \tag{4}$$

gdzie: A_i – procentowa zmiana wartości *i* tego elementu, wrażliwość MS^{WR}_{qi} – procentowy przyrost wartości funkcji $Q_0 = f(q_1, q_2, ... q_n)$, gdy wartość odpowiedniego parametru q_i ulegnie zmianie o A_i procent.
Znając wartość MS^{WR}_{qi} możliwe jest, korzystając z zależności (4), szacowanie całkowitego bezwzględnego przyrostu wartości funkcji:

$$\begin{aligned} \Delta Q_0 &\cong \sum_{i=1}^{n} \Delta Q_{0q_i} = \sum_{i=1}^{n} MS_{q_i}^{WR} \cdot f(q_1, q_2, ...q_n) \\ &= \sum_{i=1}^{n} q_i \cdot A_i \cdot \frac{\partial f(q_1, q_2, ...q_n)}{\partial q_i} = \sum_{i=1}^{n} \Delta q_i \cdot w_i \end{aligned} \tag{5}$$

Wykorzystując zależność (5) można określić dolną oraz górną granicę zmian wartości Q_0 $[Q_0^l, Q_0^u]$ na podstawie zmian wartości prawdopodobieństw poszczególnych elementów z uwzględnieniem wskaźników wagowych. Proponowana metoda przedstawiona jest na rys. 2.



Rys. 2. Wpływ przedziałów prawdopodobieństw elementów na zmianę wartości przedziału prawdopodobieństwa systemu

Znając, uzyskane z analizy statystycznej lub wiedzy ekspertów, zakresy parametrów modelu probabilistycznego można określić zmiany wartości prawdopodobieństw PFD_{avg} $[PFD_{avg}^l, PFD_{avg}^u]$ oraz PFH $[PFH^l, PFH^u]$, a zatem oszacować dla nich przedział niepewności.

2.3. Weryfikacja SIL z uwzględnieniem niepewności

Przy weryfikacji SIL użytecznym parametrem jest wskaźnik różnicowy w_R niosący informację na temat położenia punktowych wartości PFD_{avg} oraz

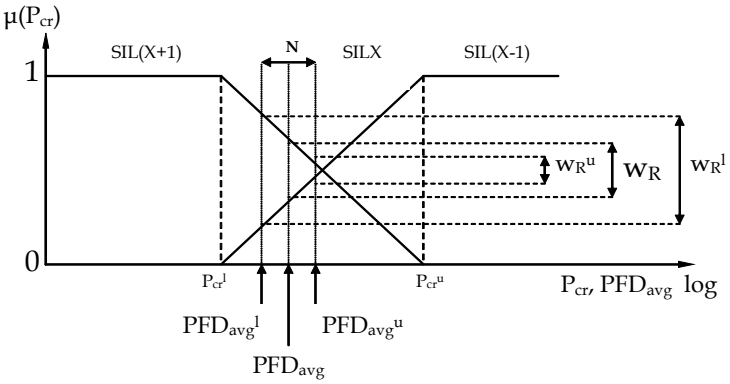
PFH w przedziale kryterialnym. Stanowi on różnicę pomiędzy wskaźnikami kryterialnymi funkcji przynależności dla dolnej i górnej granicy:

$$w_R = \mu_{SIL}^{l}(PFD_{avg}) - \mu_{SIL}^{u}(PFD_{avg}) \tag{6}$$

W przypadku uwzględnienia przedziału niepewności przy wyznaczaniu wartości PFD_{avg} (lub *PFH*), należy uwzględnić dwa dodatkowe wskaźniki różnicowe, dla dolnej i górnej granicy. Na rys. 3 przedstawiony został ogólny przypadek weryfikacji SIL na podstawie oszacowanej wartości PFD_{avg} (lub *PFH*) z uwzględnieniem przedziałów niepewności.

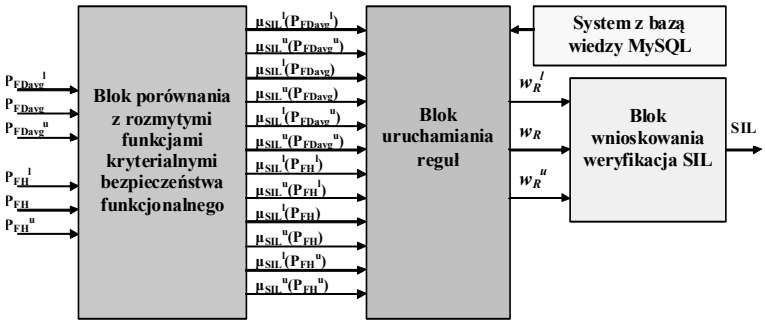
Należy uwzględnić wartości górnej i dolnej granicy dla PFD_{avg} [PFD_{avg}^{l}, PFD_{avg}^{u}] (lub *PFH* [PFH^{l}, PFH^{u}]).

$$\begin{aligned} w_R^l &= \mu_{SIL}^{l}(PFD_{avg}{}^{l}) - \mu_{SIL}^{u}(PFD_{avg}{}^{l}) \\ w_R^u &= \mu_{SIL}^{l}(PFD_{avg}{}^{u}) - \mu_{SIL}^{u}(PFD_{avg}{}^{u}) \end{aligned} \tag{7}$$



Rys. 3. Weryfikacja SIL bazująca na wartości *PFDavg* (*PFH*) z uwzględnieniem niepewności otrzymanych wyników z modelu probabilistycznego

Weryfikacja poziomu SIL systemu E/E/PE, którego model probabilistyczny uwzględnia niepewność, może być przeprowadzona z wykorzystaniem prototypowego systemu z bazą wiedzy MySQL. Ogólny schemat systemu przedstawiono na rys. 4.



Rys. 4. Weryfikacja poziomu SIL z uwzględnieniem niepewności modelu probabilistycznego

Zaproponowana metoda, wykorzystująca wskaźniki różnicowe, jest pomocna w efektywnej weryfikacji wymaganego poziomu SIL systemów E/E/PE z uwzględnieniem wyników analizy wrażliwości oraz/lub oszacowanych przedziałów niepewności uzyskanych z opracowanych modeli probabilistycznych.

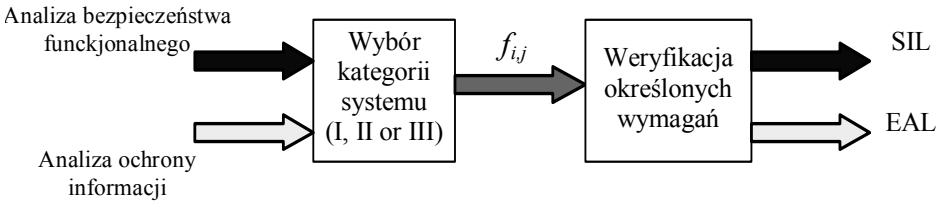
3. Zintegrowana analiza bezpieczeństwa funkcjonalnego oraz ochrony informacji rozproszonych systemów sterowania i zabezpieczeń

Niektóre zagadnienia zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji systemów sterowania i zabezpieczeń przedstawiono poniżej. Wzięto pod uwagę obecność przemysłowych sieci komputerowych oraz specyfikację i rodzaj wykorzystywanego kanału przesyłu informacji. Rozpatrzone zostały trzy przypadki dla trzech kategorii rozproszonych systemów sterowania i zabezpieczeń:

I. Systemy zainstalowane na obiektach krytycznych, wykorzystujące wyłącznie wewnętrzne kanały przesyłu informacji (np. sieć lokalna LAN),
II. Systemy zainstalowane na krytycznych obiektach skupionych lub rozproszonych, w których istnieją wewnętrzne kanały transmisji informacji i mogą być również wykorzystywane zewnętrzne kanały przesyłania danych,
III. Systemy zainstalowane na obiektach i w systemach infrastruktury krytycznej, w których wykorzystywane są wyłącznie zewnętrzne kanały transmisji danych.

Wymagania dla analizowanego systemu mogą być określone w postaci dwuparametrowej funkcji $f_{i,j}$ [7]. Metoda zintegrowanej analizy

bezpieczeństwa funkcjonalnego i ochrony informacji systemów rozproszonych, zawierających różne kanały komunikacyjne, jest przedstawiona na rys. 5. Funkcja $f_{i,j}$ jest wykorzystywana w późniejszym procesie weryfikacji poziomu SIL (EAL). Poziomy uzasadnionego zaufania (EAL) stanowią zbiór wymagań odnoszących się do całkowitego cyklu życia produktu, jakim jest system informatyczny [5]. Zdefiniowano siedem poziomów EAL, przy czym EAL1 jest poziomem podstawowym (najtańszy w implementacji), a EAL7 jest poziomem najwyższym (najbardziej rygorystyczny).



Rys. 5. Wyznaczenie funkcji $f_{i,j}$ oraz weryfikacja wymagań [7]

Istotnym zagadnieniem zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji tego typu systemów jest weryfikacja określonych uprzednio wymagań dotyczących SIL oraz EAL. Poziomy SIL odnoszą się do konkretnych funkcji bezpieczeństwa a poziomy EAL do ochrony informacji całego systemu monitorowania, sterowania i zabezpieczeń.

Tabela 1. Wynikowe SIL z uwzględnieniem poziomu EAL dla systemów II kategorii (III kategorii)

Określony		Weryfikowany SIL dla systemu II kat. (III kat.)			
ochrona informacji		*Bezpieczeństwo funkcjonalne*			
EAL	poziom	1	2	3	4
1	podstawowy	- (-)	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)

Można założyć, że niepożądane zdarzenia i działania z zewnątrz przy niskim poziomie ochrony informacji EAL mogą wpływać na niewypełnienie przez system funkcji bezpieczeństwa. Tak więc niski poziom uzasadnionego zaufania EAL, przy weryfikacji określonego poziomu SIL, może skutkować jego obniżeniem.

4. Podsumowanie

Modele probabilistyczne systemów E/E/PE, opisane w normach IEC 61508 oraz IEC 61511, nie uwzględniają niepewności. Metoda zaproponowana w artykule bierze pod uwagę zarówno analizę wrażliwości modeli probabilistycznych systemów E/E/PE, jak również niepewność uzyskanych wyników.

Uwzględnienie niepewności w procesie analizy ryzyka oraz modelowania probabilistycznego systemów E/E/PE związanych z bezpieczeństwem stanowi poważny problem i wymaga dalszych badań. Tworzony system z bazą wiedzy służący do określania i weryfikacji poziomów SIL powinien zapewnić uwzględnienie pokrycia diagnostycznego oraz uszkodzeń zależnych.

Szczególne wyzwanie stanowi uwzględnienie problematyki ochrony informacji w procesie projektowania programowalnych systemów sterowania i zabezpieczeń, wykorzystujących infrastrukturę sieciową. Zaproponowano zintegrowane podejście w określaniu wymagań SIL oraz EAL na podstawie klasyfikacji systemów na kategorie I, II lub III. Jest to uzasadnione, ponieważ nieuwzględnienie aspektów ochrony informacji przy projektowaniu systemów sterowania lub zabezpieczeń, wykorzystujących różne kanały przesyłu informacji, może doprowadzić do pogorszenia bezpieczeństwa całego systemu (określenie zbyt niskich wymagań SIL).

Z tego powodu powinno się podjąć dalsze prace badawcze, mające na celu opracowanie metod określania oraz weryfikacji wspólnych wymagań dla bezpieczeństwa funkcjonalnego i ochrony informacji w systemach sterowania i zabezpieczeń pracujących w sieci.

Spis literatury

1. Abrahamsson, M..: *Uncertainty in quantitative risk analysis – Characterisation and methods of treatment*. Report 1024. Lund. 2002.
2. Barnert, T., Sliwinski, M.: *Methods for verification safety integrity level in control and protection systems*. Functional Safety Management in Critical Systems: 171-185. Jurata. Gdansk. 2007.
3. Beugin, J., Cauffriez, L., Renaux, D.: *A SIL quantification approach to complex systems for guided transportation*. Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2005 Gdynia - Sopot – Gdansk. London. 2005.
4. *IEC 61508. Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety related systems.* International Electrotechnical Commission (IEC). 1998.
5. *ISO/IEC 15408: Information technology – Security techniques – Evaluation criteria for IT security.* 1999.
6. Kosmowski, K.T., Sliwinski, M.: *Methodology for functional safety assessment*. Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2005, Gdynia - Sopot – Gdansk. London. 2005.
7. Kosmowski, K.T., Sliwinski, M., Barnert, T.: *Functional safety and security assessment of the control and protection systems*. Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2006, Estoril. London. 2006.
8. Stavrianidis, P.: *Reliability and uncertainty analysis of hardware failures of programmable electronic system*. Reliability Engineering and System Safety Vol.39: 309 - 324. 1992.

M.Sc. **Tomasz Barnert**, received M.Sc. in 2005 from Gdansk University of Technology (GUT). From 2006 researcher and since 2008 assistant at Faculty of Electrical and Control Engineering, GUT. Specialization: functional safety and security of distributed control and protection systems.

Prof. **Kazimierz Kosmowski,** received Ph.D. in 1981 and D.Sc. in 2003 from Gdansk University of Technology (GUT). Since 2006 the manager of Division of Control Eng. at Faculty of Electrical and Control Eng. and since 2007 a vice-chairman of Polish Safety and Reliability Association (PSRA). Specialization: reliability and safety of technical systems, human reliability, functional safety of programmable control and protection systems.

Ph.D. **Marcin Śliwiński**, received Ph.D. in 2006 from Gdansk University of Technology (GUT). From 2001 researcher and since 2006 lecturer at Faculty of Electrical and Control Engineering, GUT. Specialization: functional safety of control and protection systems, probabilistic modeling of technical systems.