Journal of KONBiN 1(21)2012
ISSN 1895-8281
DOI 10.2478/jok-2013-0003

THE IMPACT OF SECURITY ASPECTS ON FUNCTIONAL SAFETY ANALYSIS

WPŁYW ASPEKTÓW OCHRONY INFORMACJI NA WYNIKI ANALIZ BEZPIECZEŃSTWA FUNKCJONALNEGO

Tomasz Barnert, Kazimierz T. Kosmowski, Marcin Śliwiński

Gdansk University of Technology, Faculty of Electrical and Control Engineering
e-mail: t.barnert@ely.pg.gda.pl, k.kosmowski@ely.pg.gda.pl, m.sliwinski@ely.pg.gda.pl

***Abstract**: It can be said that a distributed control and protection system's security level may have a significant impact on functional safety analyses and their results. However the issue of integrating those both aspects are difficult and usually is neglected during functional safety analyses. Known methods of functional safety analyses don't take into consideration this kind of concept also. This paper discusses an attempt to integrate safety and security aspects with respect to functional safety analysis as a main one. It is based on proposed classification of communication channels used in the system and the level of system distribution. The functional safety analysis is performed at every stage of system lifecycle. The most important part is related to description of required safety functions and determining required safety integrity level for them. Moreover the proposed concept should be taken into account on this stage, and assume that security should be considered as a risk parameter used in the functional safety analysis. On the other hand there is a verification of required SIL for designed safety-related system which implements safety function where security should be taken into consideration as well.*

***Keywords:** functional safety, security, SIL, EAL, risk assessment, risk graphs*

***Streszczenie:** W artykule tym stwierdza się, iż poziom ochrony informacji w rozproszonych systemów sterowania i zabezpieczeń może mieć znaczący wpływ na wyniki analiz bezpieczeństwa funkcjonalnego, przeprowadzanych dla tego typu systemów. W analizach tego typu zagadnienia ochrony informacji zazwyczaj są pomijane. W artykule przedstawiono propozycję integrowania zagadnień ochrony informacji oraz bezpieczeństwa funkcjonalnego. Bazuje ona na klasyfikacji kanałów komunikacji systemów sterowania i zabezpieczeń jak również poziomu ich zdecentralizowania. Analizy bezpieczeństwa funkcjonalnego powinny być przeprowadzane na każdym etapie w cyklu życia systemu. Jednym z ważniejszych etapów jest określanie wymagań SIL dla zdefiniowanych funkcji bezpieczeństwa. Zaproponowana koncepcja analizy zakłada, że czynnik związany z ochroną informacji powinien być traktowany jako jeden z parametrów ryzyka systemu. O poziomie ochrony informacji należy również pamiętać przy weryfikacji struktury sprzętowej realizującej funkcje bezpieczeństwa.*

***Słowa kluczowe:** bezpieczeństwo funkcjonalne, ochrona informacji, SIL, EAL, ocena ryzyka, grafy ryzyka*

1. Introduction

The functional safety management recently emphasized the importance of security aspects in technical systems, especially those that implement important monitoring, control and protection functions. It concerns two aspects: the protection of information (in the form of data, documentation and access to information, wired and wireless business and industrial networks, etc.) and physical access (access to prohibited areas, buildings, premises, equipment, etc.). General requirements for information security issues in general are included in the international normative documents like ISO/IEC 15408, ISO/IEC 17799 and PN-ISO/IEC 27001

In practice, there is a need to integrate functional safety and security concepts during carrying out the appropriate analyses, like identifying potential hazards or risk assessment process. As a result of such analyses the potential solutions reducing the risk to tolerable level can be proposed. An approach which is described in this paper proposes the relation between the safety integrity level (SIL) and the level of security of analyzed system. So, in other words, in this concept each identified safety related function should have a determined required SIL, which usually can be dependent on system security level. Similar integration can be done during SIL verification phase. It is related to the proof process of fulfillment of SIL requirements for safety-related systems implementing safety functions [2, 4, 6, 7].

It should be mentioned that in this article the assumption that the functional safety of a technical object should be treated mainly was made [5]. The information security assessment results obtained for this system will be taken into account during estimating the current required level of risk reduction in terms of functional safety analysis. Similarly, it will affect the resulting value of the safety integrity level SIL achieved in the verification process.

2. Security in the context of functional safety

Taking into account an aspect of functioning the technical object, quality and safety of data/information is critical to its operation. Technical object may consist of different types of systems, directly affecting its performance. The main systems of this type are most often the control and monitoring systems. They usually make use of different kinds of data communication channels made in different techniques: wired and wireless. Transmission of analog and especially digital data for a long distance is no longer a barrier nowadays, hence is increasingly used in the structure of distributed control and monitoring systems. This solution allows to reduce the cost of building the system and at the same time increases its flexibility. However, it brings new challenges and problems such as the provision of a reliable and secure way to transfer data between the components of such a system. A schematic example of distributed system is presented in Figure 1.

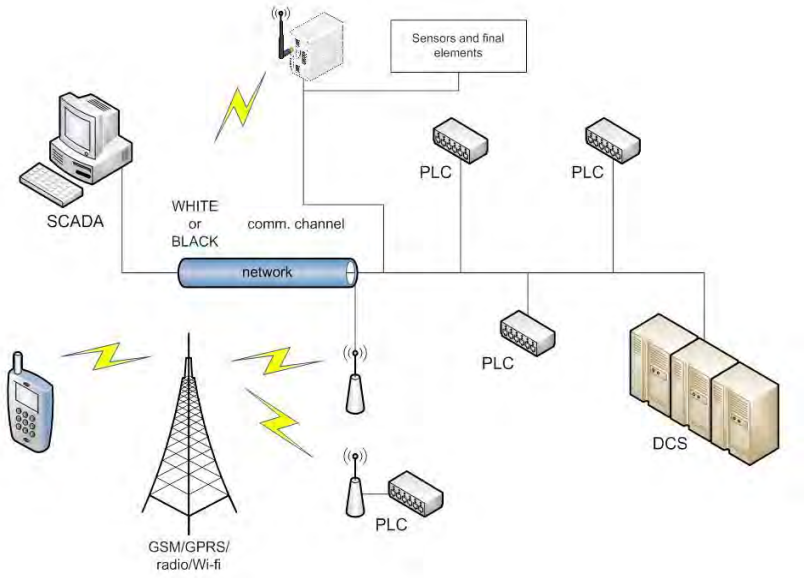

Fig. 1. Industrial computer network

Distributed system may have different vulnerabilities related to an occurrence of faults threatening the functioning of the technical object from the traditional one [19]. This is closely related to the use of a larger number of data channels that can be exposed to various types of interference, including the destructive nature of intentional action. It is worth recalling the fact that the functional safety analysis designed to determine the requirements for defined safety related function consists of hazard identification process as well as the evaluation of system risk, including the allocation of the required SIL. Thus, any fault states in the system resulting from malfunctioning of communication channels, as well as the intentional, malicious action on the system, should be taken into account in the analysis of functional safety. There is therefore a need to develop a methodology that allows the inclusion of these issues in these analyzes. The classification of vulnerability of distributed systems and their impact on the value of risk also should be taken into account.

This article proposes developing a classification of technical systems from the point of view of the use of different communication channels. A degree of exposure to disruption of their work (including the malicious actions) may be very different and should be defined. That's why a greater emphasis on the security issue should be taken into consideration, especially looking into [12, 13]:

– confidentiality of data/information - providing access to resources only to authorized users,

- integrity of the data/information - ensure the accuracy and completeness of the data processed and stored,
- availability of data/information - providing access to resources whenever it's needed.

Another important aspect of proposed methodology is a classification of distributed control and protection systems. Three main categories of such systems were proposed, based on the presence of different kinds of industrial network, its specification and type of data transfer methods [4, 14]:

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 plants, where the protection and monitoring system data are sent by internal communication channels and can be sent using external channels,
III. Systems installed in distributed critical installations, where data are sent only by external communication channels.

A new version of IEC 61508:2010 introduces some additional requirements concerning the data communication channels in functional safety solutions. It describes two main communication channel types – white or black one. A white channel means that the entire communications channel is designed, implemented and validated according to IEC 61508 requirements. The black one means that some parts of communication channel are not designed, implemented and validated according to IEC 61508. In that case, communication interfaces should be implemented according to the railway applications communication, signaling and processing systems IEC 62280 standard (Safety-related communication in closed transmission systems).

The security analysis concept is proposed in the standard ISO/IEC 15408. Security is considered with the protection from threats, where threats are categorized as the potential for abuse of assets. All categories of threats should be considered, but in the domain of security usually greater attention is given to those threats that are related to malicious or other human intentional activities. The Evaluation Assurance Level (EAL) is a package of assurance requirements, which covers the complete development of a product with a given level of strictness. Common Criteria (ISO/IEC 15408) lists seven levels, with EAL1 being the most basic (cheapest to evaluate and implement) and EAL7 being the most strict (most expensive). But it should be taken into account very carefully, because higher EAL levels do not necessarily imply better security, they only mean that the claimed security assurance of the TOE (*target of evaluation*) has been more extensively validated.

The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements. The evaluation results may help the developers and users to determine whether the product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.
If the security analysis is performed on the basis of ISO/IEC 15408, the corresponding EAL should be determined. In this case this EAL can be taken into account in functional safety analysis.

3. Determining required SIL for safety-related functions with security taken into consideration

Given the typical definition of risk used in the risk assessment process, presented as a combination of frequency or probability of a dangerous event and its consequences, the simplified method of determining the required SIL for safety functions was proposed. In this case in should include aspects of information security. This analysis is based on the obtained information from the process of identifying the risks in technical systems, as well as assessing the level of risk associated with it. Some of the risk factors to be taken into account when carrying out this type of analysis, have an impact on the estimated value of the frequency or likelihood, some of the consequences. Some of the risks associated with the frequency parameters applies most hardware reliability issues and the reliability of human activities as part of the technical system. Risk factor associated with communication and data transfer between different elements of the system in this case is usually ignored. However, you may find that in some cases it can have quite a significant impact on the actual level of risk of the scheme.
The risk is defined as [15, 17]:

$$\boldsymbol{R} = f \times C \tag{1}$$

where the frequency of occurrence of some scenario associated with certain consequences C is dependent on several factors, including the reliability of technical solutions used in the analyzed system. Analyzing such a system in term of security can result in detecting the existence of certain vulnerabilities, which may increase the risks associated with overall system. In most cases, this will result in increasing the frequency of certain scenario occurrence, therefore, assuming that the consequences are $C = const$. Then it can be said that:

$$f \uparrow \;\rightarrow\; \boldsymbol{R} \uparrow \text{, when vulnerability of system } \uparrow \tag{2}$$

The vulnerability of the system can be measurable and expressed by the level of security, taking into account the countermeasures introduced to the system which may mitigated these vulnerabilities.
Considering the stage of identifying hazards in the system which is very important part of defining required safety-related functions, there is a need of determining possible causes, consequences and frequency of occurrence for every described hazard or scenario. Good protection of all kinds of information in the system, or (better to say) its absence in the analyzed object, will affect the part related to the causes. Consequences related to those hazards remain the same, unless we consider the effects of sabotage such as barriers, emergency procedures, etc., but the frequency or possibility of their occurrence may change in case of security level. Knowing that reducing the causes is very important to the safety of a technical object, the security issue in that point should be treated very seriously.
The hazard identification method like HAZOP [9] can be extended with another factor related to identified vulnerabilities of the system. These information may directly influence the calculation of the identified threat occurrence frequency related to defined causes. Some example is presented in Figure 2.

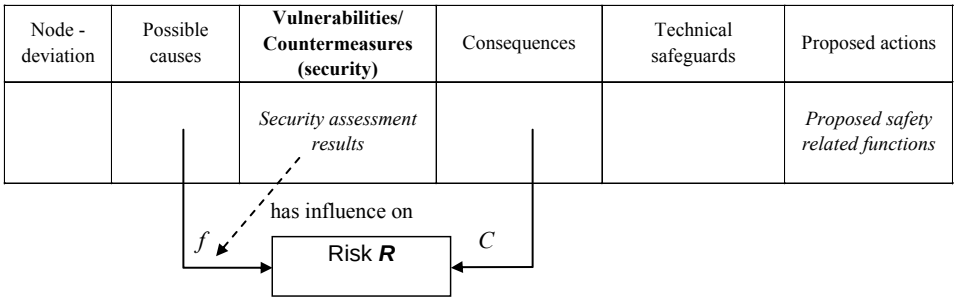

Fig. 2. HAZOP with security information

The level of security, which is to be used in the further risk assessment process (in terms of functional safety), have to be defined in such a way that its inclusion in these analyzes should be done fast and simple. Depending on the methods used in the analysis of functional safety, a quantitative or qualitative value describing the level of security is required. The quantitative analysis is usually much more expensive and difficult, because it requires performing a number of studies on the prevalence of vulnerabilities in the system and the assignment of probabilities to them is needed. One of the methods used in quantitative security analysis is Attack Tree.

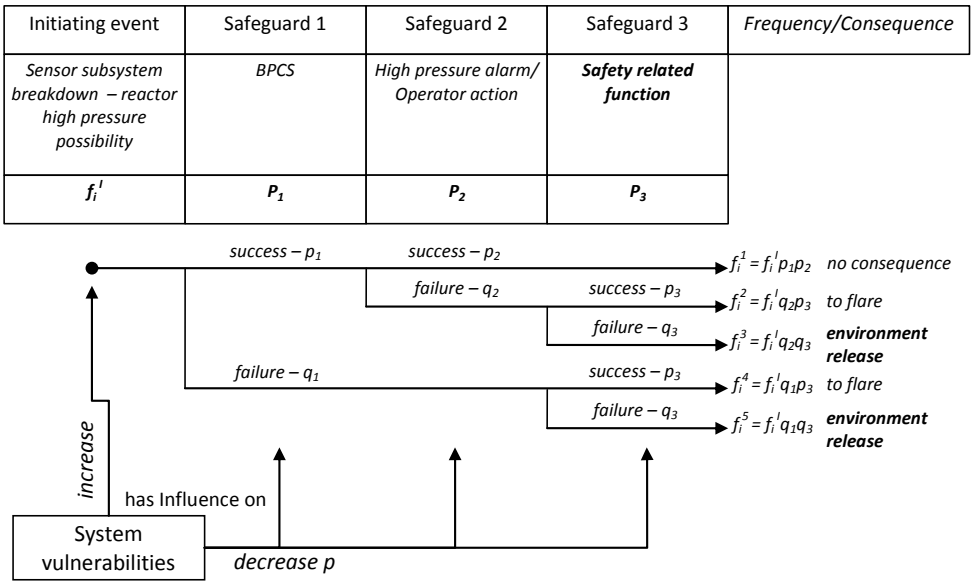

Fig. 3. Example of event tree with definition of frequency and consequences for each event scenario with security impact on frequency of dangerous event

Considering some scenarios and knowing the numerical values assigned to the initiating events frequencies as well as the probabilities of response of various layers of protection designed or already implemented in the system, the LOPA analysis can be done [1].

The initiating events which are defined in the scenario have determined certain value of frequency or probability of occurrence, which results directly from the analyzes carried out in the phase of hazard analysis (e.g. HAZOP). In accordance, the frequency of such events can be increased, depending on the degree of security level (vulnerabilities, which are not adequately protected). Through the analysis of information security, for example by using Attack Tree method, the probability of initiating events and hazards occurrence assigned to system vulnerabilities may be assessed. In this case, it can be specified the value by which the initiating event frequency is increased. Another aspect of this type of analysis is the impact of security on the correct operation of each of the analyzed protective layers. It may be a situation in which the existing system vulnerabilities will cause the possibility of interference in the functioning of the layers and their malfunction. In this case, the security level will affect the value PFD_{avg} directly assigned to each layer. An example can be illustrated by the situation of implementing SIS layer designed for safety-related functions. Inadequate protection of such a system to prevent intentional action from the outside (assuming that there are some serious

vulnerabilities which allow it) will reduce the reliability of the response of such a system. That reduce the level of SIL achieved by this system. Therefore, it becomes necessary to also adequately clarified the issue of individual protection layers in terms of their vulnerability to all kinds of threats associated with the security issues.

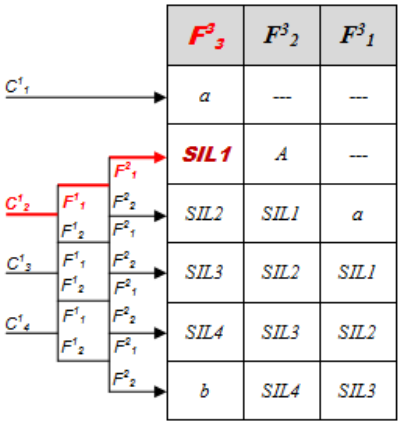

Fig. 4. Example of standard risk graph [16]

In the case of qualitative method, which certainly does not give as accurate results as the semi-quantitative or quantitative methods, but provides a quick estimate of the SIL requirements, the extension of the risk graph method was proposed [3]. With the ability to add certain risk parameters relating to aspects of information security (rather the results of the security analysis to determine how safe the system is in terms of security) a method of functional safety analysis related to the security level was obtained. The risk assessment could be done with many different methods, like risk graphs, risk matrixes, layers of protection analysis, etc. [18]. In this paper the risk graph method will be described. Standard risk graph consisting of risk parameters relating to consequences (C^1), frequency and duration of stay in the danger zone (F^1), the ability to avoid dangerous situation (F^2) and the probability of occurrence of a hazard without the use of safety-related system (F^3), is shown in Figure 4.

In distributed control and protection systems, there may be various kinds of vulnerabilities which may be closely related to the use of different communication channels. The security analysis in such a case is to help identify them and also suggest some solutions to counteract them. Given the mentioned earlier assumption that functional safety issues are treated mainly in this case, the vulnerabilities and implemented countermeasure in analyzed system may in some way affect the measured and defined level of required SIL. Having the results of the security

analysis of control system for example, they can be divided into several main ranges with the use of qualitative or quantitative description. If the analysis of information security is done in accordance with ISO-IEC 15408 the EAL can be determined for such a system. The obtained EAL could also be taken into account in the analysis of functional safety. Table 2 presents the categorization of levels of information security.

Table 1. Security level categorization [7]

EAL Level	Level of security	Risk parameter and its ranges
EAL1	Low level	F^3_3
EAL2	Low level	F^3_3
EAL3	Medium level	F^3_2
EAL4	Medium level	F^3_2
EAL5	High level	F^3_1
EAL6	High level	F^3_1
EAL7	High level	F^3_1

Used in this context, the modifiable risk graph method can be considered. It takes into account the additional risk factor F^3 and it is illustrated in Figure 10. Proper calibration of such a graph is related to detection of too low security level occurring in the analyzed system. It leads to increase the SIL requirements for E/E/PE safety-related system which implements defined safety-related function. This means that the less secure system is, the likelihood of occurrence of potential dangerous events is greater. In addition to the standard reasons of unreliable operation of the equipment like failures, faults, etc., the malicious action on such a system should be taken into consideration as an another factor increasing frequency of system's failure. This situation can obviously lead to some serious consequences. In this case, the frequency or likelihood of occurrence of an dangerous scenario is of course higher. Therefore, the safety-related function which is designed to protect the system, its components and the environment by minimizing the risks, must meet more stringent conditions. Mainly it is associated with the granting of a higher required safety integrity level on the system that implements designed safety-related functions.

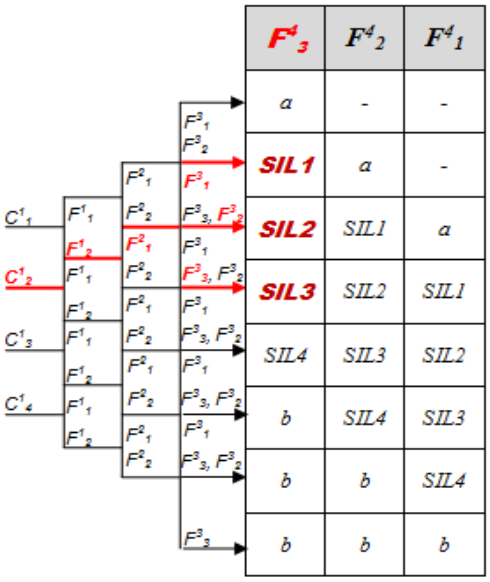

Fig. 5. Example of risk graph with additional risk parameter related to security level [7]

Proposal presented above can be considered as a conservative one and may give very stringent requirements. Because the levels EAL5-EAL7 are rarely achievable in practice, some modification to the proposed method can be included. This assumption is based on using EALs and description of only practicable levels of security. Then the Table 2 should be defined as below:

Table 2. Simplified security level categorization

EAL level	Level of security	Risk parameter and its ranges
EAL1	Unsatisfactory level	F^3_2
EAL2	Unsatisfactory level	F^3_2
EAL3	Satisfactory level	F^3_1
EAL4	Satisfactory level	F^3_1

In this case reference can be made to described earlier in this article the classification of technical systems using various communication channels. This classification shows that the most vulnerable system belongs to III category (i.e. it is only use external communication channels). For these systems, the establishment of more rigorous risk assessment can be justified. However, for

systems classified as category I and II more tolerant version can be used. This would look as follows:

– I and II category systems

→ lower vulnerability → tolerant method (Table 2)

– III category systems

→ higher vulnerability → strict method (Table 1)

Then, the risk graph should look like:

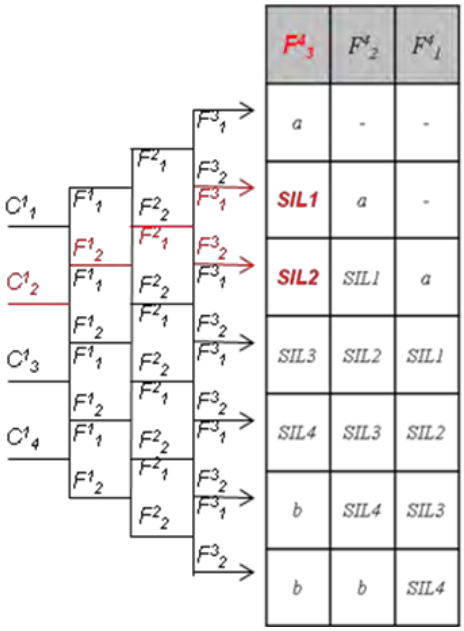

Fig. 6. Example of risk graph with additional risk parameter related to the security level (simplified version)

That means that lack of proper security solutions implemented in the system affects on increasing the required level of safety integrity for concerned safety-related function.

4. Conclusion

A comprehensive integration of the functional safety and security analysis is quite difficult and it is currently a challenging issue [5]. In this paper an attempt to integrate the functional safety and security issue was presented. The process of determining required safety integrity level of given safety function under security consideration was illustrated. The security aspect is considered as a risk parameter taken into account in the functional safety analysis. Under some circumstances

required SIL, which is related directly to the level of required risk reduction in the technical object, may be increased, especially for the distributed control systems, because they may be more exposed to the inner and outer threats. This issue was illustrated on the example of modifiable risk graph with additional risk parameter related directly to the determined level of security.
It should be also said, that on the other hand there is a verification issue of required SIL for designed safety-related system, which implements defined safety function [3, 4]. This problem wasn't described above, but it is another challenge. In this case the result of security analysis can affect calculated SIL directly [2]. In this case level of security can be described on the basis of SeSa (*SecureSafety*) methodology, which was designed by the Norwegian research organization SINTEF [8, 10, 11] and is dedicated to control systems and automatic protection devices used in the offshore, monitored and managed remotely from the mainland by generally available means of communication. Another method of integration security with functional safety during verification of SIL is considering uncertainty of probabilistic model parameters. Security can influence on uncertainty of results obtained from analyses. Thus, the security aspects are some kind of boundary conditions in the process of determining required SIL for given safety-related function and its verification in overall functional safety analyses.

5. Literature

[1] AIChE: Layers of Protection Analysis – Simplified Process Risk Assessment, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York 2001.

[2] Barnert T., Kosmowski K.T., Sliwinski M., Analiza bezpieczeństwa funkcjonalnego i ochrony informacji w rozproszonych systemach komputerowych pełniących funkcje sterowania i zabezpieczeń, Pomiary Automatyka Kontrola PAK, 2007

[3] Barnert T., Kosmowski K., Śliwiński M., Determining and veryfying safety integrity level under uncertainty, Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2008, Valencia, Hiszpania

[4] Barnert T., Kosmowski K.T., Sliwinski M. Security aspects in verification of the safety integrity level of distributed control and protection systems, Journal of KONBIN, Air Force Institute of Technology, Warsaw, 150-176, 2008

[5] Barnert T., Kosmowski K.T., Śliwiński M.: A knowledge-based approach for functional safety management, Taylor & Francis Group, European Safety & Reliability Conference ESREL, Praga, Czechy 2009.

[6] Barnert T., Kosmowski K.T., Sliwinski M., Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issue, PSAM 2010, Seattle, USA, 2010

[7] Barnert T., Kosmowski K.T., Śliwiński M., „A method for including the security aspects in the functional safety analysis of distributed control and protection systems”, Proceedings of European Safety & Reliability Conference, Rhodos, Greece, 2010

[8] Grøtan T.O., Jaatun M.G., Øien K., Onshus T., The SaSa Method for Assesing Secure Remote Access to Safety Instrumented Systems (SINTEF A1626), 2007, Trondheim, Norway.

[9] IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide. International Electrotechnical Commision (IEC), 2001.

[10] Jaatun M.G., Grøtan T.O., Line M.B., Secure Safety: Secure Remote Access to Critical Safety Systems in Offshore Installations, w: Autonomic and Trusted Computing, 2008, Springer Berlin Heidelberg, Berlin, Heidelberg, s. 121–133.

[11] Jaatun M.G., Line M.B., Grøtan T.O., Secure remote access to autonomous safety systems; A good practice approach. Int. J. Auton. Adapt. Commun. Syst., 2009, t. 2, s. 297–312.

[12] ISO/IEC 17779:2000: Information technology - Code of practice for information security management.

[13] ISO/IEC 15408:1999: Information technology — Security techniques — Evaluation criteria for IT security Part 1-3.

[14] Kosmowski K.T., Sliwinski M., Barnert T. Functional safety and security assessment of the control and protection systems, European Safety & Reliability Conference, ESREL 2006 Estoril, Taylor & Francis Group, London, 2006

[15] PN-EN 61508:2004. Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1-7. Warszawa: PKN.

[16] PN-EN 61508:2010. Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1-7. Warszawa: PKN.

[17] PN-EN 61511:2007. Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3, PKN, Warszawa

[18] Missala T.: Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa zawartych w normach bezpieczeństwa funkcjonalnego, normach związanych z nimi oraz literaturze, PIAP, Warszawa 2009.

[19] US-Cert, Control Systems Security Program (CSSP) - Overview of Cyber Vulnerabilities (http://www.us-cert.gov/control_systems/csvuls.html)

Acknowledgements

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 – National Research Institute (CIOP-PIB) for cooperation during preparation and realization of a research project VI.B.10 for 2011-13 concerning the safety management of hazardous systems including the functional safety aspects as well as human reliability and security issues.

***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 aimed at risk assessment and determining required safety integrity level (SIL); 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 to 2012 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 aimed at SIL verification, probabilistic modeling of technical systems*