Barnert Tomasz

Kosmowski Kazimierz T.

Piesik Emilian

Śliwiński Marcin
Gdansk University of Technology, Gdansk, Poland

Security aspects in functional safety analysis

Keywords

functional safety, security, safety integrity level (SIL), evaluation assurance level (EAL), security assurance level (SAL), risk assessment, risk graphs, programmable control and protection systems

Abstract

A security level of distributed control and protection system may have a significant impact on the results of functional safety analysis. However, the issue of integrating the safety and security aspects is difficult and usually is neglected during the functional safety analysis. This article presents a method of functional safety analysis which takes into consideration a concept of integrating these two aspects. It is based on proposed classification of communication channels used in the computer system / network and the scope of such system distribution. The functional safety analysis is to be performed at every stage of system lifecycle, but one of the most important parts is defining required safety functions and determining the safety integrity level for them. The integration concept might be taken into account at this stage. The basis of a method proposed is the assumption that the security level is considered as a risk parameter in graphs of functional safety analyses.

1. Introduction

The functional safety management experts have 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, transfer of information in business and industrial networks, etc.) and physical access (access to prohibited areas, buildings, premises, safety equipment, etc.). General requirements for information security issues are included in the international normative documents like ISO/IEC 17799, ISO/IEC 15408, ISO/IEC 27001 and a new series of standards IEC 62443.

In practice, there is a need to integrate functional safety and security concepts during the appropriate analyses, like identification of potential hazards or assessment of risks. 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 described as some risk factor based on evaluation assurance level EAL (common criteria), SAL (security assurance level) or SeSa rings of protection. Similar integration can be done during the SIL verification phase for architectures considered. It is related to the proof of fulfilment the SIL requirements for safety systems implementing defined safety functions [2], [4], [6]-[7].

In this article it was assumed that the functional safety analysis of a technical installation is carried out as outlined in the paper [5]. The information of security assessment obtained for such installation is taken into account in evaluating the required level of risk reduction. Similarly, it will affect the resulting value of the safety integrity level (SIL) achieved in the verification process of proposed functional safety architecture.

2. Security concept used in functional safety analysis

Taking into account the operation requirements of a technical installation, its reliability and safety as well as the quality and security of data/information is of prime importance. Such installation may consist of different types of systems, directly affecting its performance. The main systems to be carefully considered include the monitoring, control and protection systems. They usually make use of different kinds of data communication channels made in appropriate techniques: wired and wireless.
Transmission of analogue and especially digital data for a long distance is no longer a barrier nowadays, hence is increasingly used within complex architecture of distributed control and monitoring systems. Such solution allows reducing the cost of building the system and at the same time increases its flexibility. However, it brings new problems and challenges such as the provision of reliable and secure paths to transfer data between the components of such a system. A schematic example of distributed industrial system is presented in *Figure 1*.

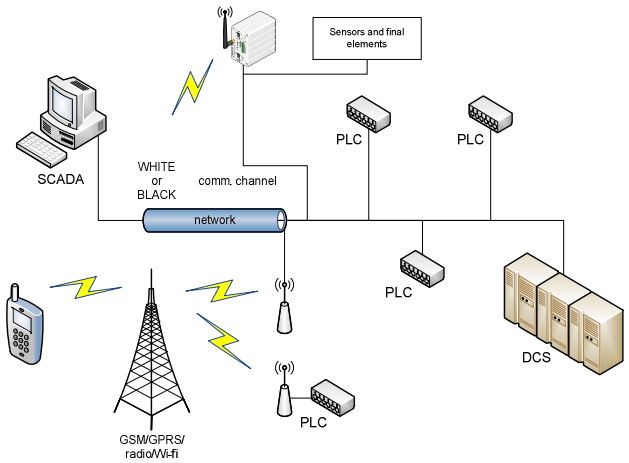

Figure 1. Industrial computer network

Distributed computer system may have different vulnerabilities related to an occurrence of faults threatening the functioning of the installation 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, some fault or failure 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 the analyses of interest. 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 is why a greater emphasis on the security issue should be taken into consideration, especially looking into [13]-[14]:

– *confidentiality* of data/information - providing access to resources only to authorized users,
– *integrity* of the data/information - ensuring the accuracy and completeness of the data processed and stored,
– *availability* of data/information - providing access to resources whenever it is needed.

Another important aspect of proposed methodology is a classification of distributed control and protection systems. Three main categories of such systems are distinguished, based on the presence of different kinds of industrial network, its specification and type of data transfer methods applied [4], [17]:

I. Systems installed in concentrated critical plants 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.

The standard 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, signalling and processing systems IEC 62280 standard (safety-related communication in closed transmission

systems). Also a new version of IEC 61511:2014 will be focused on security issues more.

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.

Another good source for security assessment of technical system is IEC 62443. A new concept of SAL (security assurance level) is introduced in this normative document. This parameter is related to the achieved security level. There are four security levels (comparable to SIL) and they are assessed for each security zone using the set of 7 functional requirements. The zones are related to [12]:

– FR 1 – identification and authentication control,
– FR 2 – use control,
– FR 3 – data integrity,
– FR 4 – data confidentiality,
– FR 5 – restricted data flow,
– FR 6 – timely response to event,
– FR 7 – resource availability.

SALs achieved for system, subsystem or device can be expressed as a vector of FR 1-FR 7 areas, such as:

SAL = {4,4,4,3,3,2,3}

The SAL in each zone should meet the requirements, if not, there should be some security countermeasures proposed.

3. Security measures in determining required SIL for safety-related function

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 on the consequences. 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, one may find that in some cases it can have quite a significant impact on the actual level of risk of the scheme.

The risk can be defined as [9]-[10]:

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

where the frequency f 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:

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

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 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 scenario.

Good protection of all kinds of information in the system, or (better to say) its absence in the analyzed plant, 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 of their occurrence may change in case of security level. Knowing that reducing the causes is very important to the safety of a plant, the security issue in that point should be treated very seriously.

The hazard identification method like HAZOP [11] can be extended with another factor related to identified vulnerabilities of the system. This information may directly influence the calculation of the identified threat occurrence frequency related to defined causes. An example is presented in *Figure 2*.

The level of security, which is 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*.

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 certain determined value of frequency or probability of its occurrence, which results directly from the analyzes carried out in the phase of hazard analysis (e.g. HAZOP).

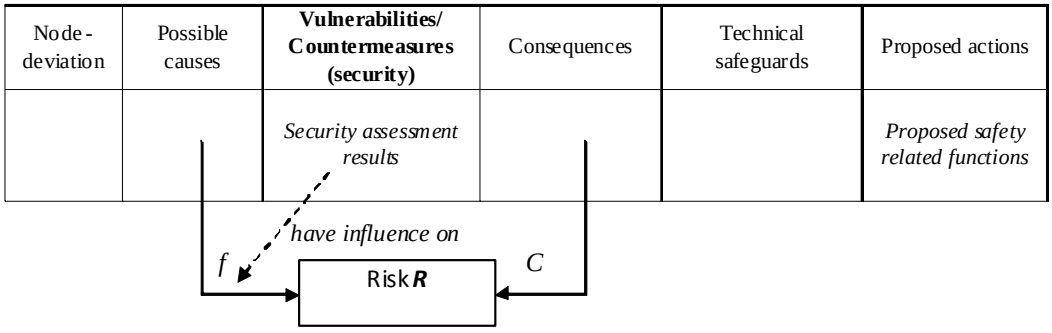

Figure 2. HAZOP with security information

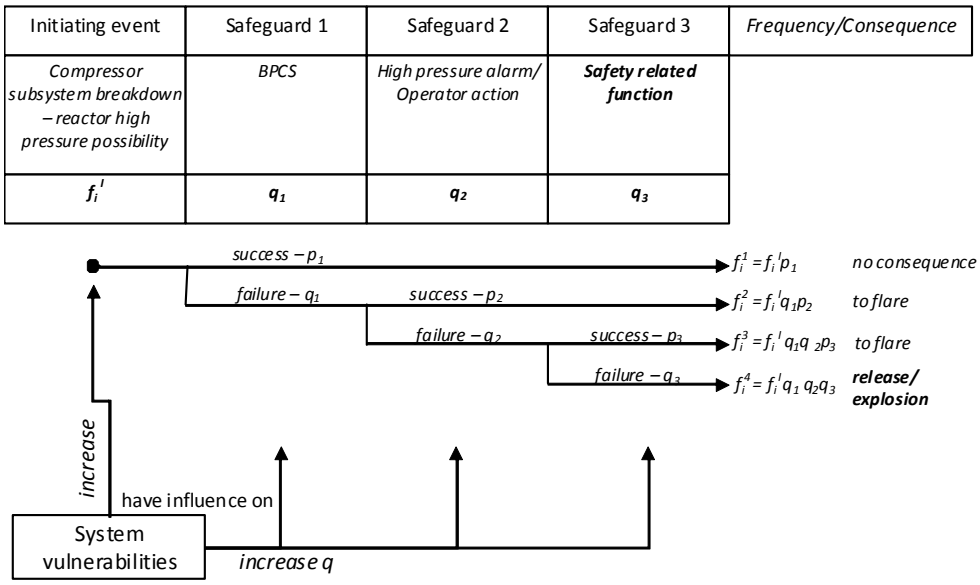

Figure 3. Example of event tree with definition of frequency and consequences for each event scenario with security impact on frequency of dangerous event or probability of failure on demand

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, the value can be specified 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 such case, the security level will affect the value $q = PFD_{avg}$ directly assigned to each layer.

An example can be illustrated by the situation of implementing the SIS layer designed for some safety-related functions. Inadequate protection of such 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 reduces the level of SIL achieved by this system. Therefore, it becomes necessary adequately clarify the issue of individual protection layer in terms of their vulnerability to all kinds of threats associated with the security issues.

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 some different methods, like risk graphs, risk matrixes, layers of protection analysis, etc. [18].

Below the risk graph method will be described. Standard risk graph consists of risk parameters related 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) which is equivalent to *W* parameter in IEC 61508's graph. It is shown in *Figure 4*.

In the 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 1* presents the categorization of levels of information security.

Used in this context, the modifiable risk graph method can be proposed. It takes into account the additional risk factor F^3 and it is illustrated in *Figure 5*.

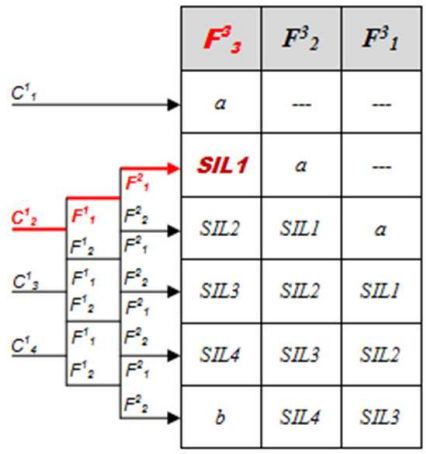

Figure 4. Example of standard risk graph [9]

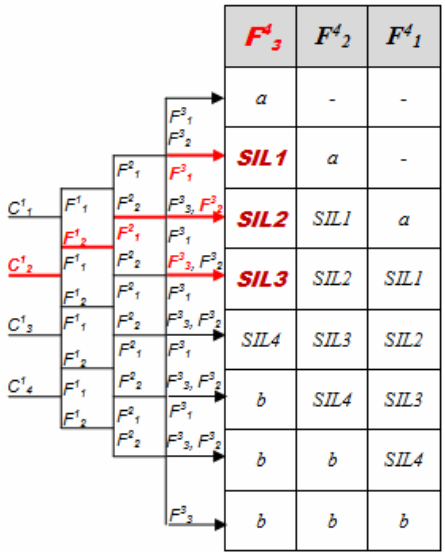

Figure 5. Example of risk graph with additional risk parameter related to security level [7]

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 a 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.

Table 1. Security level categorization based on EAL [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

The evaluation assurance level may be difficult to implement during risk assessment to the whole technical system. That is why other security risk measure can be taken into consideration. A well-suited security measure of technical control and protection system is SAL (security assurance level) [12] which is considered as vector of seven requirements for different security zones.
In this case there are four SAL levels and they may be used in proposed methodology instead of EAL consideration. *Table 2* shows the classification of system's security level on the basis of security assurance level. Each level of security is then related to the range of risk parameter F^3 similarly to the last example.

Table 2. Security level categorization based on SAL

SAL Level	Level of security	Risk parameter and its ranges
SAL1	Low level	F^3_3
SAL2	Medium level	F^3_2
SAL3	High level	F^3_1
SAL4	High level	F^3_1

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 *Table 3* should be defined as below:

Table 3. Simplified security level categorization based on EAL

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

The simplified version of risk graph described by the risk factor related to security assurance level SAL is based on the description presented in *Table 4*. It also takes into consideration only two ranges of risk parameter: unsatisfactory and satisfactory level of security in analysed system.

Table 4. Simplified security level categorization based on SAL

SAL Level	Level of security	Risk parameter and its ranges
SAL1	Unsatisfactory level	F^3_2
SAL2	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:

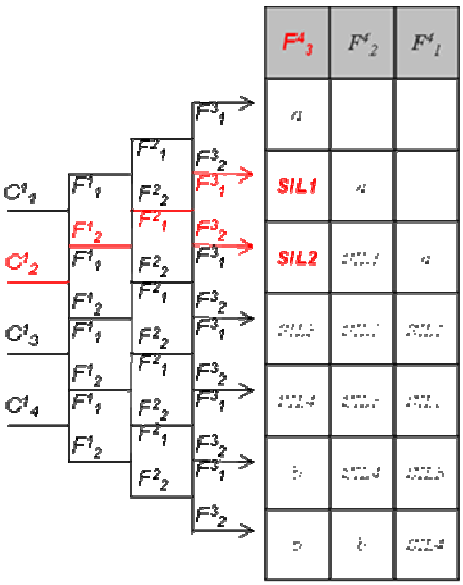

Figure 6. Example of risk graph with additional risk parameter related to security level (simplified version)

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 very important and it is currently a challenging issue [5]. In this article 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 was not 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], [15]-[16] 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.

The security measures which may be taken into account during the functional safety analyses are also of a prime importance. In this article some of them was presented. A well-known concept of EAL is the basis for presented methodology. But there are also limitations of *common criteria* and for some kind of programmable systems the EAL measure may be insufficient. Usually EAL is related only to single hardware or software element.

That is the reason why other security descriptions should be taken into account. One of them may be proposed lately the SAL measure indented to describe in an integrated way the system security. The SeSa rings of protection methodology is another example. All described above security measures can be valuable sources of input data for determining required safety integrity level of safety related functions considered.

Further research works have been undertaken to integrate outlined above aspects of safety and security in the design and operation of the programmable control and protection systems to develop a relatively simple methodology to be useful in industrial practice.

References

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

[2] Barnert, T., Kosmowski K.T. & Sliwiński, M. (2007). *Functional safety and security analysis of distributed control & protection systems.* (in Polish), PAK.

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

[4] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2008). Security aspects in verification of the safety integrity level of distributed control and protection systems. *Journal of KONBIN*, 150-176

[5] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2009). A knowledge-based approach for functional safety management. *Proc. European Safety & Reliability Conference – ESREL*, Taylor & Francis Group,Prague, Czech Republic.

[6] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2010). *Integrated functional safety and security analysis of process control and protection*

systems with regard to uncertainty issue. PSAM, Seattle, USA

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

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

[9] IEC 61508 (2010). Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, Parts 1-7. International Electrotechnical Commission, Geneva.

[10] IEC 61511 (2007). Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

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

[12] ISA/IEC 62443 (2013). Security for industrial automation and control systems.

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

[14] ISO/IEC 17779 (2000). Information technology - Code of practice for information security management.

[15] Jaatun, M.G., Grøtan, T.O. & Line, M.B. (2008). Secure Safety: Secure Remote Access to Critical Safety Systems in Offshore Installations. *Autonomic and Trusted Computing* 121–133.

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

[17] Kosmowski, K.T., Śliwiński, M. & Barnert, T. (2006). Functional safety and security assessment of the control and protection systems. *Proc. European Safety & Reliability Conference – ESREL*, Taylor & Francis Group, Estoril, , London.

[18] Missala, T. (2009). *Analysis of requirements and methods of risk assessment during determining required safety integrity level in functional safety normative documents*. Related documents and literature (in Polish), PIAP.

[19] US-Cert (2011). Control Systems Security Program (CSSP) - Overview of Cyber Vulnerabilities. Available: http://www.uscert.gov/control_systems/csvuls.html.