CURRENT ISSUES OF FUNCTIONAL SAFETY AND CYBERSECURITY ANALYSIS OF INDUSTRIAL AND CRITICAL INFRASTRUCTURES

MARCIN ŚLIWIŃSKI, KAZIMIERZ T. KOSMOWSKI AND EMILIAN PIESIK

Faculty of Electrical and Control Engineering
Gdańsk University of Technology
G. Narutowicza 11/12, 80–233 Gdańsk, Poland

(received: 15 January 2019; revised: 31 January 2019;
accepted: 7 February 2019; published online: 18 February 2019)

Abstract: This article addresses some functional safety assessment procedures with cybersecurity aspects in critical industrial installations with regard to the functional safety requirements specified in standards IEC 61508 and IEC 61511. The functional safety management includes hazard identification, risk analysis and assessment, specification of overall safety requirements and definition of safety functions. Based on the risk assessment results, the safety integrity level (SIL) is determined for consecutive safety functions. These functions are implemented within the industrial control system (ICS) and/or the distributed control system (DCS) that consists of the basic process control system (BPCS) and/or the safety instrumented system (SIS). The determination of the required SIL related to the required risk mitigation is based on the semi-quantitative evaluation method. Verification of the SIL for the considered architectures of the BPCS and/or the SIS is supported by probabilistic models with appropriate data and model parameters including cybersecurity related aspects. The proposed approach is illustrated on the example of critical industrial installations.

Keywords: cybersecurity, functional safety, safety integrity level, security level, evaluation assurance level, industrial control system, safety instrumented system

DOI: https://doi.org/10.17466/tq2019/23.2/b

1. Introduction

Safety and security aspects consist of two different groups of functional requirements for control and protection systems. It is the reason why analyses of safety and security should not be integrated directly. The paper proposes an extension of the currently used methods of functional safety analysis. It can be done with an inclusion of the information security level assigned to the technical

system. One of the main objectives of functional safety analysis is to determine the required safety integrity level (SIL) for the safety-related functions to be realized by safety-related systems. According to IEC 61508 the interval probabilistic quantitative criterion is defined for each SIL (1–4). The functional safety analysis procedure usually does not include cybersecurity aspects. However, in the case of a distributed control and protection system it can have practical significance. It may affect the results of determining as well as verifying the SIL, taking into account functional safety analysis [1, 2]. The general procedure of functional safety with cybersecurity aspects is shown in Figure 1.

Functional safety, which is a part of overall safety, is aimed at reducing the risk of hazardous system operation to an acceptable or tolerable level by introducing a set of safety-related functions (SRFs). They are to be implemented by control and/or protection systems which are usually operating in a computer network using wired and/or wireless communication technologies.

These aspects are sometimes neglected in functional safety analyses [3–6]. The role of safety-related control and protection systems for risk reduction is nowadays obvious as they are designed to reduce the risks of accident scenarios, especially those with major consequences, *e.g.* from ten times to thousand and more times depending on the required risk mitigation [7, 8]. These systems belong to the category of industrial control systems (ICS). Some more important safety functions, substantially reducing the relevant risks, require the implementation of protection layers, according to the defense in depth (DinD) concept [8]. Requirements concerning cybersecurity related aspects will be considered regarding the requirements of a series of international standards, IEC 62443 [9], IEC, 63074 [10], ISO/IEC 15408 [11] ISO/IEC 27001 [12] and ISO/IEC 27002 [13]. The integrated risk analysis and the assessment methodology proposed are compatible with some known methods often used in practice, such as HAZOP (hazard and operability), LOPA (layer of protection analysis) and SVA (security vulnerability analysis) [14, 15]. Security related analyses of the ICS (industrial control system) during its design and operation as a distributed computer system (DCS) with relevant SCADA (supervisory control and data acquisition) functions are very important in hazardous plants, especially when they are considered within a critical infrastructure [16, 17].

The cybersecurity of information and software quality are becoming crucial issues in the design of digital systems for the control and protection in hazardous plants. There are still new challenges concerning the development of methods for advanced reliability and safety analysis. They include in particular the functional safety aspects of control and protection systems based on a programmable technology that offer advanced control and safety-related functionality. These systems are also vulnerable to cybersecurity problems, especially when they are used in industrial computer networks. The related issues that are discussed with some suggestions how to deal with them include: determining the safety integrity levels of safety functions, uncertainty representation and assessment for verifying

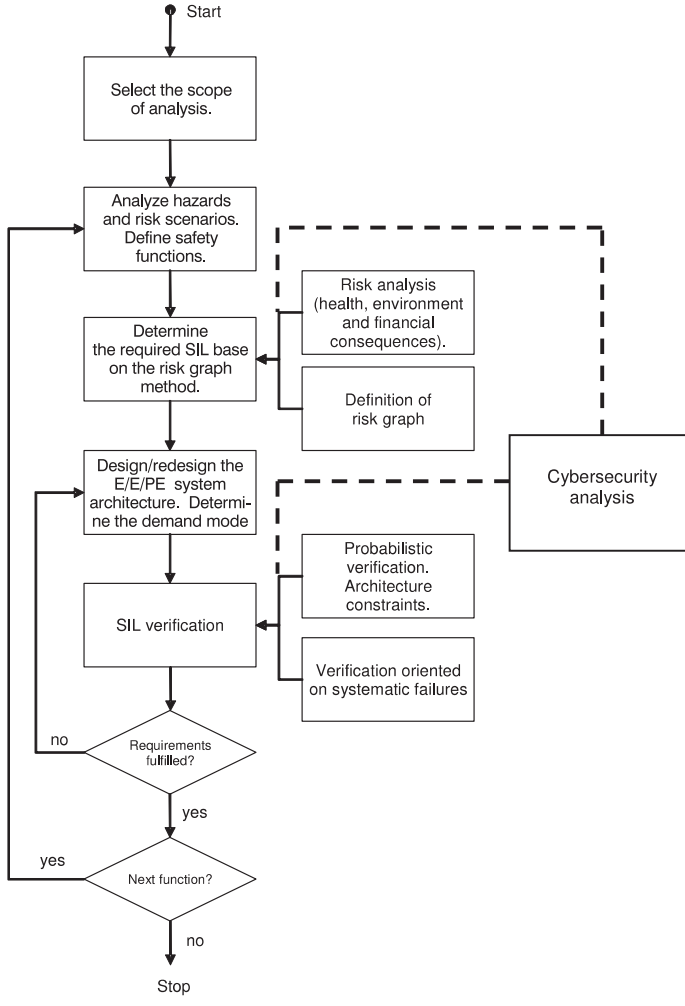

Figure 1. General flowchart illustrating proposed approach

the safety integrity levels, integrating the safety and security aspects in the programmable protection systems operating in a computer network [5, 16, 18, 19].

2. Functional safety and cybersecurity of industrial control system in critical installations

2.1. Functional safety management in lifecycle

The term *safety-related* (SR) applies to systems which perform a specified function(s) to ensure that the risk is maintained at an acceptable or tolerable level. Those functions are *safety-related functions* (SRFs). Two different requirements should be satisfied to ensure the functional safety [1, 2]:

- requirements imposed on the performance of safety-related functions;

- requirements for the safety integrity expressed by the probability that a given safety function is performed in a satisfactory way within a specified time.

The requirements for safety functions are determined taking into account the results of hazard identification, while the safety integrity requirements result from analysis of potential hazardous events. The higher the safety integrity level (SIL) for a given SRF, the lower the probability of failure on demand (PFD_{avg}) or the probability of danger failure per hour (PFH) needed to reduce the risk to the required level. Higher safety integrity levels impose stricter requirements on the design of a safety-related system [1, 2]. Most often, the safety function is performed using an electric, electronic and programmable electronic system (E/E/PES) or a safety instrumented system (SIS) [5, 7, 20].

A safety-related E/E/EPS comprises all the components that are necessary for the safety function performance, *i.e.*, starting from sensors, via logic control systems and interfaces, to controllers, including any safety critical operations undertaken by a human-operator. Standard IEC 61508 defines 4 performance levels for safety functions. Safety Integrity Level 1 (SIL1) is the lowest, while Safety Integrity Level 4 is the highest. The standard formulates in detail the requirements to be fulfilled for each safety integrity level to be achieved. At higher levels the requirements become stricter to reduce the relevant probability of PFD_{avg} or PFH of a given SRF.

In order to deal – in a systematic manner – with all activities necessary to achieve the required safety integrity for the safety functions to be carried out by the E/E/PES, the standard adopts an overall safety lifecycle scheme as shown in Figure 2 that is proposed as a technical framework [1, 4, 20, 21].

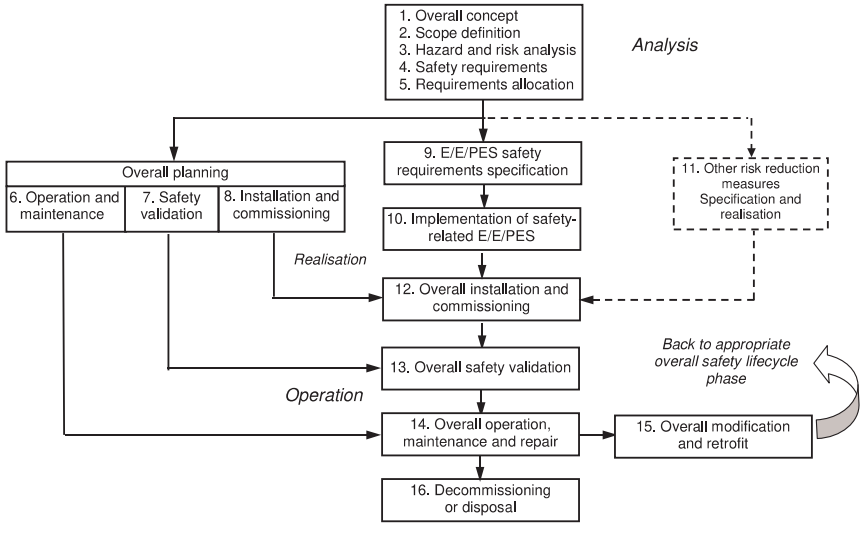

Figure 2. Overall functional safety-related lifecycle proposed in IEC 61508 [1]

For each safety-related E/E/PE system fulfilling a defined safety-related function of a given SIL, two probabilistic criteria are defined in the standard, namely:

- the average probability of failure (PFD_{avg}) to perform the design function on demand for a system operating in a low demand mode of operation;
- the probability of a dangerous failure per hour (PFH), *i.e.* the frequency for a system operating in a high demand or continuous mode of operation.

These numeric probabilistic criteria expressed as intervals for consecutive SILs and two modes of operation are presented in Table 1.

Table 1. Safety integrity levels and interval probabilistic criteria for safety-related systems [1]

Safety integrity level (SIL)	PFD_{avg} interval criteria for systems operating in low demand mode	PFH interval
SIL4	$[10^{-5}, 10^{-4})$	$[10^{-9}, 10^{-8})$
SIL3	$[10^{-4}, 10^{-3})$	$[10^{-8}, 10^{-7})$
SIL2	$[10^{-3}, 10^{-2})$	$[10^{-7}, 10^{-6})$
SIL1	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

A quantitative method for determining the SIL can be outlined as follows:

- determine the tolerable risk based on a defined risk matrix or risk graph;
- determine the risk with regard to the EUC (*equipment under control*);
- determine the necessary risk reduction to meet the tolerable risk level;
- allocate the necessary risk reduction to the E/E/PES and other risk reduction measures.

The relative risk reduction (for consequence $N = \text{const}$) is evaluated from the Formula (1)

$$r^F = R_t / R_{\text{np}} = F_t / F_{\text{np}} \tag{1}$$

where: R_t and F_t are the numerical targets for tolerable risk and frequency levels, respectively; R_{np} and F_{np} are the risk and frequency, respectively, of a hazardous event that could occur if the protective system is not present.

Taking into account (1) the relation can be written for PFD_{avg} of a given SRF operating in a low demand mode:

$$PFD_{avg} \leq F_t / F_{\text{np}} = r^F \tag{2}$$

where: PFD_{avg} is the average probability of failure on demand; the criteria interval values for consecutive SILs are presented in the second column of Table 1.

The necessary steps for determining the required SIL for given safety-related system (SRS) are as follows [1, 20, 22]:

- determine the frequency F_{np} (from the EUC risk without the addition of any protective features);
- determine the consequence (N) without the addition of any protective features;

- determine, using a defined risk matrix or risk graph, whether a tolerable risk level is achieved for the frequency (F_{np}) and the consequence (N) (it would require further investigation using the ALARP principle, depending on the risk class);
- determine the probability of failure on demand (PFD_{avg}) from (2) for the SRF to meet the necessary relative risk reduction (r^F); for the given consequence of the hazardous event considered.

According to IEC 61508 the safety validation should be performed in terms of the overall safety function requirements and the overall safety integrity requirements, taking into account the safety requirements allocation for the E/E/PE safety-related system in designing. Thus, in particular the PFD_{avg} value must be verified in the probabilistic modeling process for the considered architectures of a given E/E/PE safety-related system taking into account the probabilistic criteria specified in Table 1 for a given SIL.

2.2. Cybersecurity aspects in industrial control and protection systems

The main aspect of security is the protection of assets that include: information, data, the computer and peripherals, communication equipment and installations, power supplies, system programs, application programs, functions and procedures, documentation, *etc.* [23]. The risk is associated with some categories that have to be protected, for instance [12, 13]:

- *confidentiality*: ensuring that information is accessible only to authorized users;
- *integrity*: safeguarding the accuracy and completeness of data and processing methods;
- *availability*: ensuring that authorized users have access to the system and associated assets when required.

Sources of the damage, such as computer viruses, Trojan and spy software, hacking or denial of service attacks have become nowadays more dangerous and sophisticated [16, 24–28]. All those aspects should be included in the risk analyses [12, 15, 28]. The multipart standard ISO/IEC 15408 defines the criteria referred to as the Common Criteria (CC), to be used as the basis for evaluation of security properties of IT products and systems. The CC permit comparability between the results of independent security evaluations. This is done by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied thereto during the security evaluation.

The evaluation of an IT product or system is known as the Target of Evaluation (TOE). A defined TOE or TOEs include, but are not limited to, operating systems, computer networks, distributed systems, and applications [3, 4, 29, 30]. The CC address the protection of information from unauthorized disclosure, modification, or loss of use. The categories of protection related to these three types of security failure are commonly called, as has been mentioned above, *confidentiality*, *integrity*, and *availability* [11, 15].

The *Evaluation Assurance Level* (EAL) is a package of assurance requirements which covers a complete development of a product with a given level of strictness. The Common Criteria list seven levels, with EAL1 being the most basic (the cheapest to implement and evaluate) and EAL7 being the most strict (most expensive) levels. Higher EALs do not necessarily imply better security, they only mean that the claimed security assurance of the TOE has been more extensively validated [11, 24]. Each Evaluation Assurance Level can be described as: EAL1 – functionally tested; EAL2 – structurally tested; EAL3 – methodically tested and checked; EAL4 – methodically tested, designed and reviewed; EAL5 – semi-formally designed and tested; EAL6 – semi-formally verified design and tested; EAL7 – formally verified design and tested.

The results of a security analysis of a given control and protection system can be divided into some general categories, for example, a qualitative description with defined security levels such as: low level, medium level or high level of security. The aim of security analyses is to determine the EAL achievable for the considered solution of a system and/or network. The EAL determined for a given solution is taken into account during the functional safety analysis (see Table 2).

Table 2. Levels of security and corresponding EALs [3, 6, 31]

Evaluation Assurance Level	Security Level
EAL1	Low level
EAL2	Low level
EAL3	Medium level
EAL4	Medium level
EAL5	High level
EAL6	High level
EAL7	High level

The evaluation process establishes a level of confidence that the security functions of products and systems considered, and the assurance measures applied to them meet these requirements. The evaluation results may help developers and users to determine whether a product or a system is secure enough for the intended application and whether the security risks implicit in its use are tolerable.

Another approach to the security evaluation for industrial automation and control systems is IEC 62443. A concept of *Security Level* (SL) has been introduced in this normative document. There are four security levels (SL1 to 4) and they are assessed for a given security zone using a set of 7 functional requirements [9, 24, 25]. The IEC 62443 standard uses security levels as a qualitative approach to expressing security requirements. As shown in Table 3, there are four different security levels, which are characterized in terms of the threats against which they protect.

Table 3. Security Assurance Levels (SLs) [9]

SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation
SL3	Protection against intentional violation using sophisticated means with moderate resources, system specific skills a moderate motivation
SL4	Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

The SL is a relatively new security measure concerning control and protection of systems. It is evaluated based on a defined vector of seven requirements for a relevant security zone [9]:

$$\mathrm{SL} = \{\mathrm{AC}, \mathrm{UC}, \mathrm{DI}, \mathrm{DC}, \mathrm{RDF}, \mathrm{TRE}, \mathrm{RA}\} \tag{3}$$

where: AC – identification and authentication control, UC – use control, DI – data integrity DC – data confidentiality, RDF – restricted data flow, TRE – timely response to event, RA – resource availability.

Another security analysis method can be proposed on the basis of the SeSa (SecureSafety) approach, which has been designed by the Norwegian research institution SINTEF. Using SeSa rings related to security protection is another approach useful for the integration of functional safety and security aspects (Figure 3).

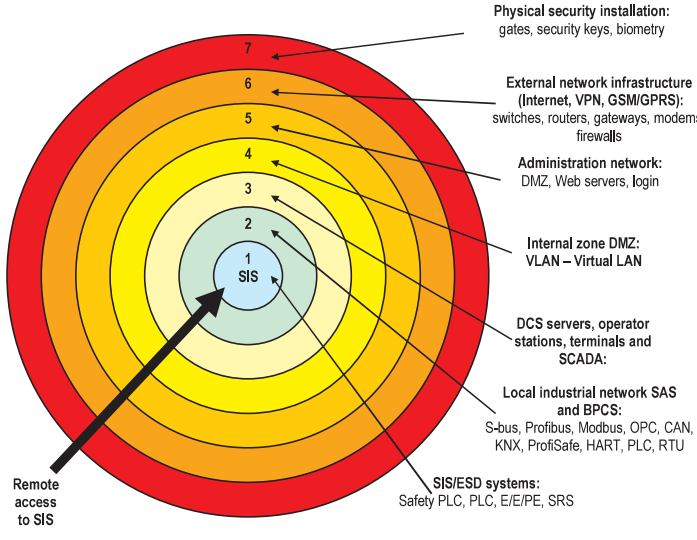

Figure 3. Rings of protection in SIS system [27]

It is dedicated to control systems and automatic protection devices used in offshore installations, monitored and managed remotely from the mainland

by generally available means of communication [27, 28, 31]. According to the series of standards IEC 61508 and IEC 61511 the *Safety Instrumented Systems* (SIS) are very important not only for safety, but also for security. An ICS system (*e.g.* BPCS or SIS) should have appropriate protection. This safeguard is strictly connected with the estimated levels of sensitivity and criticality. The strength of the security level may be determined by rings of protection (Figure 3). The number of rings of protection is increasing depending on the levels of security (EALs or SLs). The outer ring of protection is connected with the highest level of security. An important task of integrated functional safety and security analysis of such systems is verification of the required SIL taking into account the potential influence of the described security levels (EAL, SL or SeSa protection rings) [21, 22, 31].

3. Classification of process control and protection systems

A conventional control and protection system consists of a programmable logic controller (PLC), sensors, actuators, a control station with SCADA and a control station. The system components may be connected by different internal or external communication channels. The information sent between the PLC and the control station can be transferred by standard series or parallel communication protocols or other methods of communication, *e.g.* wireless GSM/GPRS.

Three main categories of distributed control and protection systems have been proposed, based on the presence of a computer system or an industrial network, its specification and type of data transfer methods [19, 31, 32]:

I. Systems installed in concentrated critical facilities using internal communication channels only (*e.g.* LAN);
II. Systems installed in concentrated or distributed critical plants, where the protection and monitoring system data is sent by internal communication channels and can be sent using external channels;
III. Systems installed in distributed critical installations, where data is sent mainly by external communication channels (Figure 4).

The standards IEC 61508 and IEC 61511 introduce some additional requirements concerning the data communication channels and security aspects in functional safety solutions. They describe two main communication channel types – white or black. The white channel means that the entire communications channel is designed, implemented and validated according to the requirements of IEC 61508. The black channel means that some parts of a communication channel are not designed, implemented and validated according to IEC 61508 [1, 2, 31].

4. Functional safety and cybersecurity integrated approach

4.1. Determining required safety integrity level

One of the main purposes of the functional safety analysis is to determine the safety integrity level (SIL) for a given safety-related function, which is to be

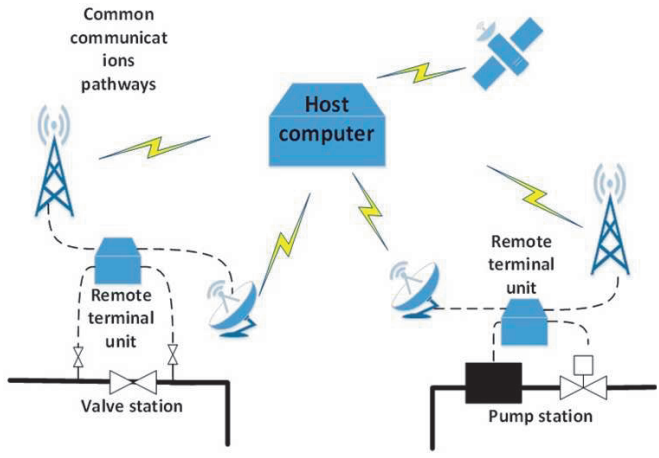

Figure 4. Data transfer in distributed industrial control systems for example pipeline infrastructure *e.g.* system category III [26]

implemented by the control and/or protection systems that are usually based on programmable electronic systems. They are playing an important role in many applications, including the control and protection of hazardous installations. However, a failure or incorrect operation of such critical components, controlling and/or protecting an industrial system could lead to a serious injury or even death of one or more people. In some cases it can lead to significant environmental damage or property loss. This is the reason why the risk analysis of the E/E/PE systems is so important.

These methods are qualitative or quantitative, which means that they use descriptive or quantified information about risk parameters. The standard proposes a qualitative risk graph method for determining qualitatively the SIL for a given safety-related system as the main method [1, 2]. It is very useful, nonetheless, special care should be taken when applying this method. A general scheme of considering the security analysis results is presented in Figure 5.

It is assumed that the security analysis, *e.g.* SVA (security vulnerability analysis) is carried out separately, and its result shows how secure an object or a control system is. The presented methodology has significant importance in control and protection systems which are distributed and use different wired or wireless communication channels.

The proposed method of SIL determination is based on risk graphs and allows building any risk graph schemes with a given number of risk parameters and their ranges expressed qualitatively, or preferably quantitatively. The safety–related systems usually operating in a computer network use wired and/or wireless communication technologies [17, 33]. These aspects are sometimes neglected in known functional safety analyses. The standard does not indicate directly how to consider the safety of communication channels in the functional safety analysis. There is no doubt that it is a real security problem. Additionally, safety and security aspects consist of two different groups of functional requirements for control

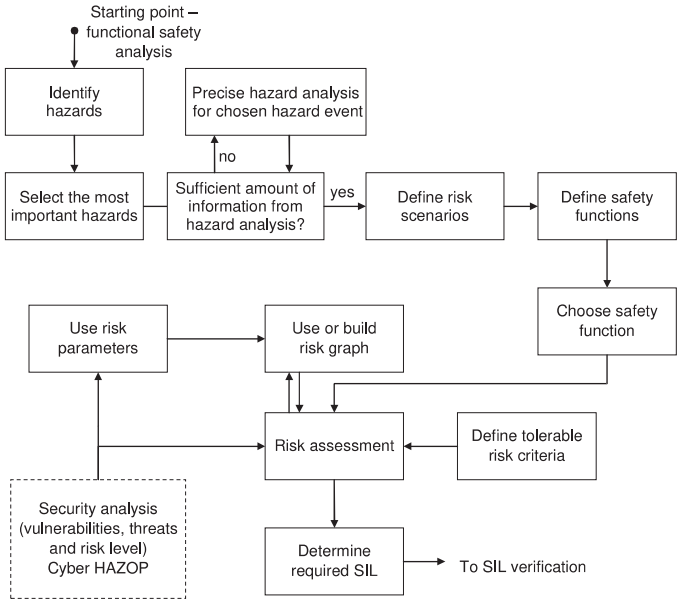

Figure 5. General procedure of SIL determination with security integration [6, 31]

and protection systems. It is the reason why analyses of safety and security should not be integrated directly. The proposed method of integration of both these aspects is based on the usage of cybersecurity analysis results as one of the inputs into the functional analysis method. In this case a functional safety analysis is superior and both analyses are done separately [31].

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 has been proposed. In this case it should include aspects of information security. This analysis is based on the obtained information from the process of identifying 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 of some of the consequences. Some of the risks associated with the frequency parameters involve most hardware reliability issues and the reliability of human activities as part of the technical system. The risk factor associated with communication and data transfer between different components of the system is usually ignored in this case. However, in some cases, it may be found that it can have quite a significant impact on the actual level of risk of a scheme

Risk is defined as:

$$R = f \times C \tag{4}$$

where the frequency f of the 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 terms of security can result in detecting the existence of certain vulnerabilities, which may increase the risks associated with the overall system. In most cases, this will result in increasing the frequency of occurrence of a certain scenario, therefore, assuming that the consequences are $C = \text{const}$. Then, it can be said that:

$$f \uparrow \rightarrow R \uparrow, \text{ when the system has a vulnerability} \uparrow \tag{5}$$

The system vulnerability can be measurable and expressed by the level of security, taking into account the countermeasures introduced to the system which may mitigate these vulnerabilities.

Considering the hazard identification stage in the system which is a very important part of defining the required safety-related functions, there is a need for determining the 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 the security level. Knowing that reducing the causes is very important to the safety of a technical facility, the security issue in that point should be treated very seriously.

The hazard identification method, such as HAZOP, can be extended with another factor related to the identified vulnerabilities of the system. This information may directly influence the calculation of the identified threat occurrence frequency related to the defined causes. An example is presented in Figure 6 [6, 31].

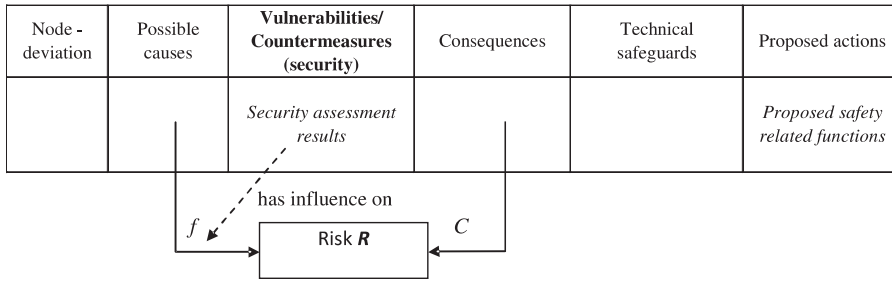

Figure 6. HAZOP with security information – Cyber HAZOP

The level of security which is to be used in the further risk assessment process (in terms of functional safety) has to be defined in such a way that its inclusion in these analyses should be 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 as it requires performing a number of studies on the prevalence of vulnerabilities in the system and the assignment of probabilities to them is needed [31, 34]. An example can illustrate the situation of implementing

the 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. This will reduce the SIL achieved by this system. Therefore, it becomes also necessary to adequately clarify the issue of individual protection layers in terms of their vulnerability to all kinds of threats associated with security issues.

An example of a functional safety analysis is presented below. It is based on a control system (shown in Figure 7), which consists of some basic components such as sensors, transmitters, programmable logic controllers and valves. It is a part of an oil fluid receiving system from a wellhead. The well fluid is heated in a preheater and then, after a pressure reduction process, it is supplied to the main heater and a separator. The additional bypass is provided to allow temperature control and maintain constant temperature of the fluid. The functional safety analysis relies on information taken from a process of hazard identification as well as further risk assessment for a designed or existing basic process control system. Some factors influence the frequency and some are responsible for consequences. The frequency parameter is basically associated with reliability of the control system equipment and human factors. The security aspects, which are associated with *e.g.* communication between equipment or restrictions in access to the system and associated assets, are usually omitted during this stage of analysis. However, they can significantly influence the final results. Hence, there should be a simple but effective method that would allow those aspects to be quickly appended to a typical functional safety analysis. It is very important especially in analyses of complex, distributed control systems.

Risk assessment could be done with many different methods, like risk graphs, risk matrixes, protection layer analysis, *etc.* In this paper the risk graph method will be described. A standard risk graph consisting of risk parameters relating to the consequences of the hazardous event (C), the frequency of, and exposure time in, the hazardous zone (F), the possibility of failing to avoid the hazardous event (P) and the probability of the unwanted occurrence of potential events that require the operation of a given E/E/PE safety-related system (W), is shown in Figure 8.

Taking into account the example control system (see Figure 7) and the possible accident scenarios associated with it, the safety-related function can be introduced. In this particular case a SIF related to the pressure increase hazardous scenario will be taken into consideration. From the risk assessment the safety integrity level for the given safety function overpressure protection pipeline was determined as SIL3.

4.2. Verification SIL with cybersecurity aspects

The proposed method to determine the SIL is based on risk graphs and allows building any risk graph schemes with a given number of risk parameters and their ranges expressed qualitatively or preferably quantitatively [6, 31, 35].

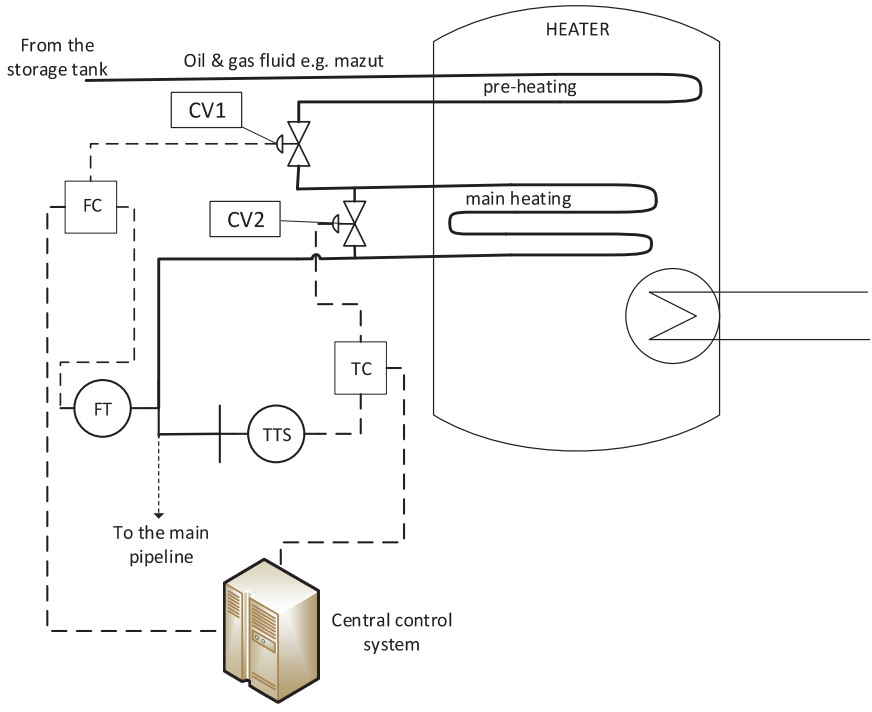

Figure 7. Example control system

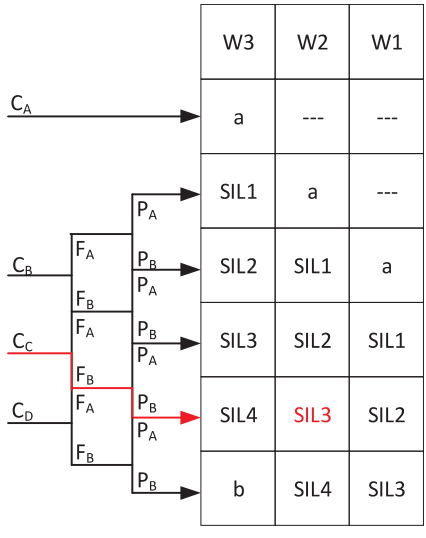

Figure 8. Determining SIL for safety function in overpressure protection pipeline

It is the quantitative method based on the reliability block diagram (RBD) that is often used to verify the SIL of an E/E/PE system or SIS. Taking into account

Table 4. Risk graph related data (Figure 8) [1, 2]

Risk parameter		Classification
Consequence (C)	C_A	Minor injury
	C_B	Serious permanent injury to one ore more persons, death to one person
	C_C	Death to several people
	C_D	Very many people killed
Frequency of, and exposure time in, the hazardous zone (F)	F_A	Rare to more often exposure in the hazardous zone
	F_B	Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the hazardous event (P)	P_A	Possible under certain conditions
	P_B	Almost impossible
Probability of the unwanted occurrence (W)	W_1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely
	W_2	A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely
	W_3	A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely

a method of minimal cut sets, the probability of failure to perform the design function on demand can be evaluated based on the following formula [18, 31]

$$\mathrm{PFD}(t) \simeq \sum_{j=1}^{n} Q_j(t) \simeq \sum_{j=1}^{n} \prod_{i \in K_j}^{n} q_i(t) \tag{6}$$

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

The average probability of failure to perform the design function on demand for the system in relation to formula (6), assuming that all subsystems are tested with the interval T_I, is calculated as follows:

$$\mathrm{PFD}_{\text{avg}} = \frac{1}{T_I} \int_0^{T_I} \mathrm{PFD}(t)dt \tag{7}$$

where: T_I – the proof test interval.

The probability per hour (frequency) of dangerous failure can be evaluated based on the formula as below [18, 31]:

$$\mathrm{PFH} \simeq \frac{\sum_{j=1}^{n} \left(1 - \sum_{\substack{i=1 \\ i \neq j}}^{n} Q_j(t)\right) \left(\sum_{j \in K_j} \frac{Q_j(t)}{q_i(t)} \left(1 - q_i(t)\right) \lambda_i\right)}{1 - \sum_{j=1}^{n} \prod_{i \in K_j}^{n} q_i(t)} \tag{8}$$

where: λi – the failure rate of the i^{th} subsystem.

Dependent failures in redundant systems increase significantly the probability of potential breakdowns. They should be included in the probabilistic modeling of E/E/PE (or SIS) systems. Another known problem is to determine the

value of β – the factor representing potential CCF (common cause failure) for a given redundant system. A knowledge-based approach can be applied for practical reasons, similarly as in IEC 61508, based on scoring the factors influencing potential dependent failures [36, 37]. There are also proposals to evaluate the β – factor depending on the architecture of the redundant systems considered

$$\beta_{koon} = \beta \cdot C_{koon} \tag{9}$$

where: β is the base factor for a simplest architecture 1oo2 and C_{koon} is a coefficient for the actual system architecture.

The following is assumed as the values of C_{koon}: $C_{1oo2} = 1$; $C_{1oo3} = 0.5$; $C_{2oo3} = 1.5$ (Table 5).

Table 5. $\beta_{(koon)}$ factor for redundant (*koon*) structures [1, 36]

		n			
		2	3	4	5
k	1	β	0.5β	0.3β	0.2β
	2	—	1.5β	0.6β	0.4β
	3	—	—	1.75β	0.8β
	4	—	—	—	β

The failure rate λ for a component (subsystem) of a *koon* system is the sum of the independent failure rate λ_I and the dependent failure rate λ_C:

$$\lambda = \lambda_I + \lambda_C \tag{10}$$

In such a case factor β is defined as follows:

$$\beta = \frac{\lambda_C}{\lambda} \tag{11}$$

Then, using (10) and (11) the dependent probability of failure can be calculated as follows:

$$q_C(t) = \beta \cdot q(t) \tag{12}$$

and the independent failure probability can be obtained from the following formula

$$q_I(t) = (1-\beta) \cdot q(t) \tag{13}$$

Figure 9 illustrates a block diagram for a 1*oo*2 structure including a dependent failure [36, 37].

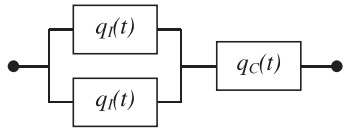

Figure 9. Reliability block diagram for 1oo2 system including dependent failure

On the basis of the formulas (6), (7) and (10)–(13) it is possible to calculate the probability of failure on demand for a 1*oo*2 system including common cause failures from the following equation:

$$\mathrm{PFD}_{\mathrm{avg}\,1oo2} \simeq [(1-\beta)\lambda_D]^2 \left(\frac{T_I^2}{3} + T_I\mathrm{MTTR} + \mathrm{MTTR}^2\right) + \beta\lambda_{\mathrm{DU}}\left(\frac{T_I}{2} + \mathrm{MTTR}\right) \tag{14}$$

where: T_I – the interval to perform periodical tests; MTTR– the mean time to repair; λ_D – the dangerous failure rate; λ_{DU} – the dangerous undetected failure rate.

The probability of a dangerous failure per hour for a 1*oo*2 architecture is evaluated taking in account (6) and (8) from the formula as below

$$\mathrm{PFH}_{1oo2} \simeq 2[(1-\beta)\lambda_D]^2 \left(\frac{T_I}{2} + \mathrm{MTTR}\right) + \beta\lambda_{\mathrm{DU}} \tag{15}$$

It is known that the overall subsystem's failure rate is calculated from the equation:

$$\lambda = \lambda_D + \lambda_S = \lambda_{\mathrm{DU}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{SU}} + \lambda_{\mathrm{SD}} \tag{16}$$

where: λ_D – the dangerous failure rate; λ_S – the safe failure rate; λ_{DU} – the dangerous undetected failure rate; λ_{DD} – the dangerous detected failure rate; λ_{SU} – the safe undetected failure rate; λ_{SD} – the safe detected failure rate.

The SIL is associated with safety aspects while the EAL, SL and SeSa are concerned with the information security level in the entire system performing monitoring, control and/or protection functions (Table 6). Table 6 shows potential corrections of the SIL for low, medium and high levels of safety-related (E/E/PE or SIS) system security. It is possible that undesirable external events or malicious acts may influence the system by threatening to perform safety-related functions in case of a low security level. Therefore, the low level of security might reduce the safety integrity level (SIL) when the SIL is to be verified. Thus, it is important to include security aspects in designing and verifying the programmable control and protection systems operating in an industrial network.

An integrated approach is proposed in which determining and verifying the safety integrity level (SIL) with levels of security (EAL and SL) is related to the system category (I, II or III). It is possible that undesirable external events and malicious acts may impair the system by threatening to perform safety-related functions in case of a low security level (Figure 10).

Such integrated approach is necessary because not including security aspects in designing safety-related control and/or protection systems operating in a network may result in deteriorating the security (lower SIL than required). In such cases the SIL verification, integrated with security aspects, is required (Figure 11). The security measures which may be taken into account during the functional safety analyses are also of prime importance. Some of them only have been presented

Table 6. SIL that can be claimed for a given EAL or SL for distributed control and protection systems of category II and (III) [19, 31]

Determined			Verified SIL for systems of category II & (III)			
cyber security factor			functional safety			
EAL	SL	Level of security	1	2	3	4
1	1	low	— (—)	SIL1 (—)	SIL2 (1)	SIL3 (2)
2	1		— (—)	SIL1 (—)	SIL2 (1)	SIL3 (2)
3	2	medium	SIL1 (—)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4	2		SIL1 (—)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	3	high	SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
6	4		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
7	4		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)

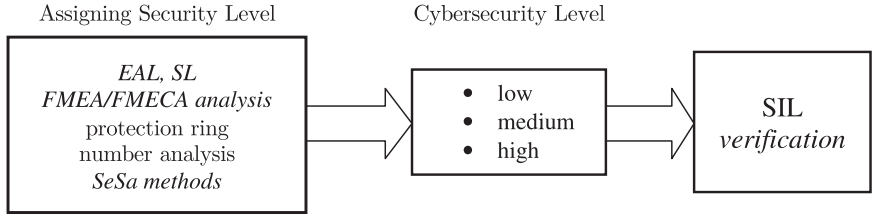

Figure 10. Assigning cybersecurity level in industrial network

in this project. A well-known concept of EAL, SL and SeSa is the basis for the presented methodology. However, there are also limitations of applying the common criteria and the EAL related measures may be insufficient for some solutions of programmable systems.

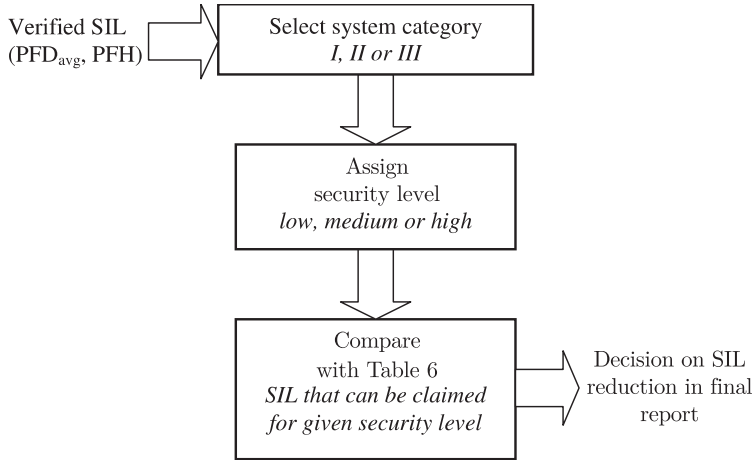

Figure 11. Safety integrity level verification Procedure including cybersecurity aspects

The EAL is usually related only to a single hardware or software component. This is the reason why other security models or descriptions should be taken into account. One of such models may the SL based approach which has been proposed lately and which is intended to describe, in an integrated way, the system security in relation to the functional safety concept.

5. Case study

Taking into account the example control system (see Figure 7) and the possible accident scenarios associated with it, the security-related function can be introduced. In this particular case a SIF related to the pressure increase hazardous scenario will be taken into further consideration.

Having the required SIL for this safety-related function, a proper architecture of the SIS should be designed. After this step, the proposed architecture has to be verified, i.e. checked, if it fulfills the requirements [23, 31, 37–40]. The process of SIL verification, similarly like SIL determination, usually does not include cybersecurity aspects. An important task of an integrated functional safety and security analysis of such systems is the verification of the required SIL taking into account the potential influence of the above described security levels, identified as the EAL, SL or SeSa protection rings. The SIL is associated with safety aspects while the EAL, SL and SeSa are concerned with the information security level of the entire system performing the monitoring, control and/or protection functions (see Table 6).

It is possible that undesirable external events or malicious acts may influence the system by threatening to perform the safety-related functions in case of a low security level. Therefore, the low level of security might reduce the safety integrity level (SIL) when the SIL is to be verified. Thus, it is important to include cybersecurity aspects in designing and verifying the programmable control and protection systems operating in an industrial network. In a situation of distributed control and/or protection systems operating in a network it is necessary to consider also potential failures within such network (Figure 12).

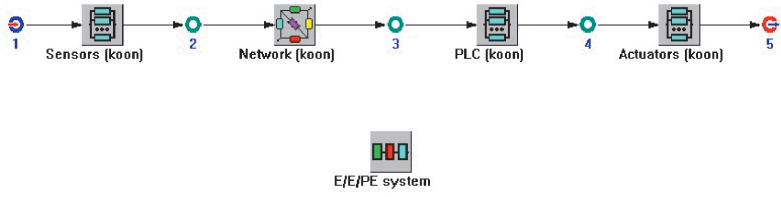

Figure 12. RBD model SIS (E/E/PE) system including industrial computer network

The average probability of failure on demand $\mathrm{PFD}_{\mathrm{avg}}$ is calculated according to the formula:

$$\mathrm{PFD}_{\mathrm{avgSYS}} \simeq \mathrm{PFD}_{\mathrm{avg}S} + \mathrm{PFD}_{\mathrm{avgNet}} + \mathrm{PFD}_{\mathrm{avgPLC}} + \mathrm{PFD}_{\mathrm{avg}A} \tag{17}$$

where: PFD_{avgSYS} – the average probability of failure on demand for the SIS system, PFD_{avgS} – the average probability of failure on demand for the sensor, PFD_{avgNet} – the average probability of failure on demand for the network, PFD_{avgPLC} – the average probability of failure on demand for the PLC, PFD_{avgA} – the average probability of failure on demand for the actuator.

Taking into account (17) it is obvious that the value of probability will be greater in a situation when a computer network is considered. Thus, the results obtained can influence the verified SIL (a lower value of SIL than in the case when the network is not considered). The modeling methods proposed in the IEC 61508 and IEC 61511 standards do not include the computer network components. Thus, the results obtained can be overoptimistic. A communication channel between controllers is represented by the block with the determined SIL.

An example of functional safety analysis is presented below. It is based on a control system (Figure 13), which consists of some basic components like sensors, programmable logic controllers and valves. It is a part of petrochemical critical installations. The communication between sensor logic controllers and actuators is implemented by wired devices vulnerable to cyber attacks.

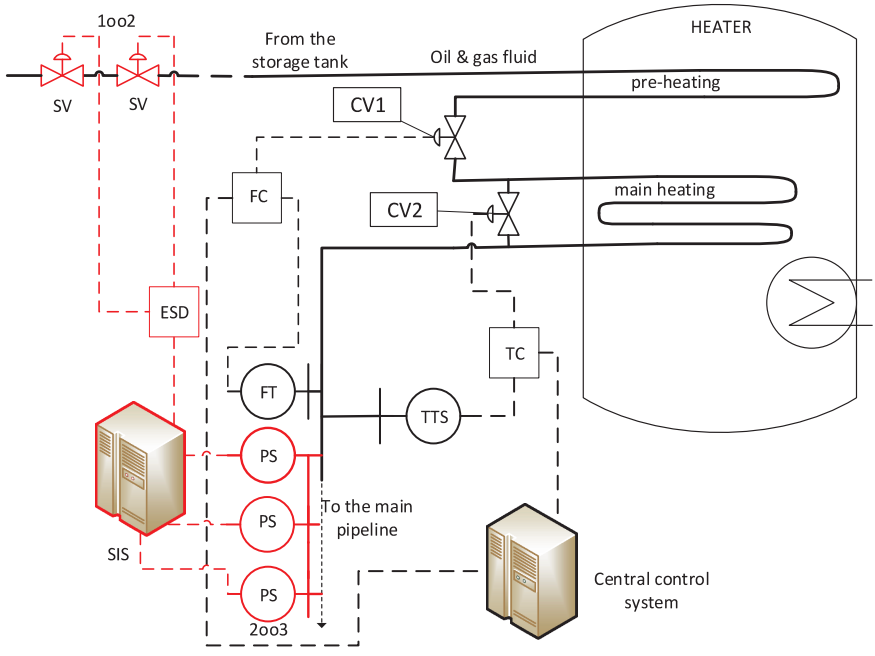

Figure 13. Example of a control and protection system with a safety instrumented system

In the risk assessment, the safety integrity level for safety function was determined as SIL3. In the industrial practice such a level requires usually to be designed using a more sophisticated configuration. The safety function (overpressure protection) is implemented in a distributed safety instrumented system (see Figure 14).

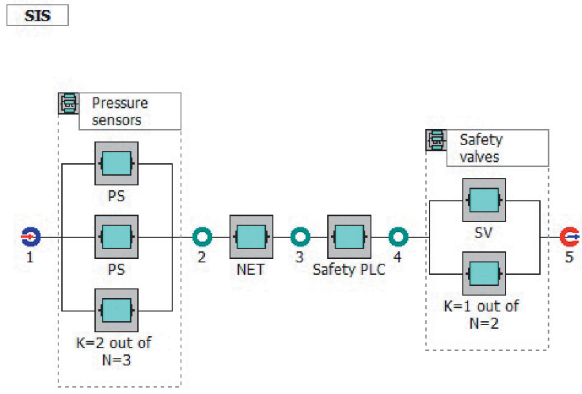

Figure 14. RBD model overpressure safety instrumented system SIS in a critical installation

The required SIL for the entire distributed E/E/PE or SIS system is determined in a process of risk analysis and evaluation. It has to be verified in the process of probabilistic modeling, taking into account its subsystems, including networks. The reliability data for SIS components is presented in Table 7 [8, 33, 41].

Table 7. Reliability data for SIS system components

	PS	NET	Safety PLC	SV
DC [%]	54	99	99	95
λ_{DU} [1/h]	$3 \cdot 10^{-7}$	$8 \cdot 10^{-8}$	$7 \cdot 10^{-8}$	$8 \cdot 10^{-7}$
T_1 [h]	8760	8760	8760	8760
β	0.02	0.01	0.01	0.02

The assessment of the result obtained for the SIS structure (Figure 14):

$$\begin{aligned} &\mathrm{PFD}_{\mathrm{avgSIS}} \simeq \\ &\mathrm{PFD}_{\mathrm{avgPS}(2oo3)} + \mathrm{PFD}_{\mathrm{avgNET}} + \mathrm{PFD}_{\mathrm{avgSafetyPLC}} + \mathrm{PFD}_{\mathrm{avgSV}(1oo2)} \simeq \\ &4.46 \cdot 10^{-5} + 3.5 \cdot 10^{-4} + 3.07 \cdot 10^{-4} + 8.22 \cdot 10^{-5} \simeq 7.84 \cdot 10^{-4} \Rightarrow \mathrm{SIL}\ 3 \end{aligned} \tag{18}$$

Thus, $\mathrm{PFD}_{\mathrm{avg}}$ is equal to $7.84 \cdot 10^{-4}$ fulfilling formally the requirements for random failures at the level of SIL3 (Table 8). The omission of cybersecurity aspects or communication network subsystems can lead to overoptimistic results, particularly in the case of distributed control and category II and III protection systems which is shown in this case study. The safety integrity level SIL3 for category III systems in those cases requires a high level of security (EAL ≥ 5 or SL ≥ 3). The presented example shows that including the cybersecurity analysis effect in the SIL verification process can influence its result. Low (for a cat. II safety-related system) as well as low and medium (for a cat. III safety-related system) cybersecurity levels can reduce the overall efficiency and decrease the SIL accordingly (see Table 6).

Table 8. SIL verification report for SIS overpressure protection system

System /subsystems/elements		*koon*	β [%]	PFD_{avg}	SIL
SIS	0	—	—	$7.84 \cdot 10^{-4}$	3
PS	.1	2*oo*3	3	$4.46 \cdot 1Q^{-5}$	4
PS	..2	—	—	$1.34 \cdot 1Q^{-3}$	2
PS	..2	—	—	$1.34 \cdot 10^{-3}$	2
PS	..2	—	—	$1.34 \cdot 10^{-3}$	2
NET	.1	1*oo*1	—	$3.5 \cdot 10^{-4}$	3
NET	..2	—	—	$3.5 \cdot 10^{-4}$	3
PLC	.1	1*oo*1	—	$3.07 \cdot 10^{-4}$	3
Safety PLC	..2	—	—	$3.07 \cdot 10^{-4}$	3
SVA	.1	1*oo*2	2	$8.22 \cdot 10^{-5}$	4
SVA	..2	—	—	$3.5 \cdot 10^{-3}$	2
SVA	..2	—	—	$3.5 \cdot 10^{-3}$	2

6. Conclusion

The procedure for functional safety management includes hazard identification, risk analysis and assessment, specification of safety requirements and definition of safety functions [1, 2]. These functions are implemented in a basic process control system (BPCS) and/or a safety instrumented system (SIS), within an industrial network system that consists of wireless and wired connection. The determination of the required SIL related to risk mitigation is based on the semi-quantitative evaluation method [1, 2, 39]. Verification of the SIL for the considered architectures of BPCS and/or SIS is supported by probabilistic modeling of appropriate data and model parameters including cybersecurity-related aspects [1, 31]. The proposed approach is based on functional safety aspects that are well known in process industries and the cybersecurity methodology [9, 11, 23–25]. A main problem with these topics is the influence of security aspects on functional safety analysis.

The cybersecurity aspect is considered as a risk parameter taken into account in the functional safety analysis. Under some circumstances the required SIL, which is related directly to the required risk reduction level in a technical facility, may be increased, especially for the distributed control systems, as they may be more exposed to inner and outer threats. This issue has been illustrated on the example of a modifiable risk graph with an additional risk parameter related directly to the determined level of cybersecurity. On the other hand, it should be also said that there is a verification issue of the required SIL for the designed safety-related system which implements the defined safety function. In this case the result of the security analysis can affect the calculated SIL directly.

The approach proposed is illustrated on an example of a critical installation. Comprehensive integration of the functional safety and cybersecurity analysis in

critical infrastructure installations is very important and it is currently a challenging issue. It is also a challenge to include cybersecurity aspects in designing distributed industrial control systems (ICS).

References

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

[2] IEC 61511, Functional safety 2016 *Safety Instrumented Systems for the Process Industry Sector. Parts 1–3*, International Electrotechnical Commission, Geneva

[3] Barnert T, Kosmowski K T and Śliwiński M 2010 *Proc. PSAM 10*, Seattle

[4] Barnert T, Kosmowski K T and Śliwiński M 2010 *A method for including the security aspects in the functional safety analysis of distributed control and protection systems*, ESREL, Rhodes, Greece

[5] Barnert T, Kosmowski K T and Śliwiński M 2012 *Journal of Polish Safety and Reliability Association*, Summer Safety and Reliability Seminars

[6] Barnert T and Śliwiński M 2013 *Functional safety and information security in the critical infrastructure objects and systems. Modern communication and data transfer systems for safety and security*, Wolters Kluwer, Warsaw

[7] Gruhn P and Cheddie H L 2006 *Safety Instrumented Systems: Design, Analysis and Justification*, Research Triangle Park: ISA – The Instrumentation, Systems and Automation Society

[8] Saleh J H and Cummings A M 2011 *Safety Science* **49** 64

[9] IEC 62443 2013 *Security for industrial automation and control systems. Parts 1–13*, International Electrotechnical Commission, Geneva

[10] IEC TR 63074 2019 *Safety of machinery – Security aspects to functional safety of safety-related control systems*, International Electrotechnical Commission, Geneva

[11] ISO/IEC 15408 2009 *Information technology, Security techniques – Evaluation criteria for IT security. Part 1–3*, International Organization for Standardization / International Electrotechnical Commission, Geneva

[12] ISO/IEC 27001 2007 *Information technology, Security techniques, Information security management systems*, International Organization for Standardization / International Electrotechnical Commission, Geneva

[13] ISO/IEC 27002 2013 *Information technology, Security techniques – Code of practice for information security management*, International Organization for Standardization International Electrotechnical Commission, Geneva

[14] Torres-Echeverria A C 2016 *Journal of Loss Prevention in the Process Industries* **41** 333

[15] ISO 31000 2018 *Risk management – Guidelines*, International Organization for Standardization, Geneva

[16] Piwowar J, Chatelet E and Laclemence P 2009 *Reliability Engineering & System Safety* **94** 1869

[17] Petersen S and Aakvaag N 2015 *Wireless Instrumentation for Safety Critical Systems, Technology, Standards, Solutions and Future Trends (SINTEF A26762)*, Norway, Trondheim

[18] Śliwiński M 2011 *Journal of Polish Safety Reliability Association* **3**

[19] Śliwiński M, Kosmowski K T and Piesik E 2015 *Verification of the safety integrity levels with regard of information security issues*, [in] Advanced Systems for Automation and Diagnostics, PWNT, Gdansk

[20] Kosmowski K T 2013 *Functional safety and reliability analysis methodology for hazardous industrial plants*, Gdansk University of Technology Publishers, Gdansk

[21] Missala T 2010 *Book of procedures for functional safety compliance evaluation of protection systems in the process industry. Report no. 8795*, PIAP, Warsaw

[22] Piesik E, Śliwiński M and Barnert T 2016 *Reliability Engineering & System Safety* **152** 259
[23] Hildebrandt H 2000 *Critical aspects of safety, availability and communication in the control of a subsea gas pipeline*, Requirements and Solutions HIMA
[24] SESAMO, Integrated 2014 *Design and Evaluation Methodology. Security and Safety modelling*, Artemis JU Grant Agr. no. 2295354
[25] MERgE Safety & Security 2016 *Recommendations for Security and Safety Co-engineering*, Multi-Concerns Interactions System Engineering ITEA2 Project #1 1011
[26] Goslin Ch 2008 *Maritime and port security*, Duos Technologies Inc., Jacksonville
[27] Grøtan T O, Jaatun M G, Øien K and Onshus T 2007 *The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems (SINTEF A1626)*, Norway, Trondheim
[28] Kanamaru H 2017 *Proc. SICE Annual Conference 2017*
[29] Kosmowski K T, Śliwiński M and Barnert T 2006 *Proc. European Safety & Reliability Conference – ESREL*, Taylor & Francis Group, London
[30] Białas A 2008 *Semiformal Common Criteria compliant IT security development framework, Studia Informatica*, Silesian University of Technology Press, Gliwice
[31] Śliwiński M 2018 *Functional safety and information security in the critical infrastructure systems and objects. Monographs 171*, Gdansk University of Technology Publishers, Gdansk
[32] Śliwinski M, Piesik E and Piesik J 2018 *IFAC Papers OnLine* **51** 1263
[33] Roos C J and Myers P E 2015 *The Engineer's Guide to Overfill Prevention. Emerson Process Management 2015 Edition*, Emerson
[34] Gabriel A, Ozansoy C and Shi J 2018 *Reliability Engineering and System Safety* **177** 148
[35] Fovino I N, Masera M and Cian A D 2009 *Reliability Engineering and System Safety* **94** 1394
[36] Hokstad P 2004 *Proc. European Safety & Reliability Conference*, Berlin
[37] Hoyland A and Rausand M 2004 *System Reliability Theory. Models and Statistical Methods. Second Edition*, John Wiley & Sons Inc., Hoboken, New Jersey
[38] Goble W and Cheddie H 2005 *Safety instrumented systems verification: Practical probabilistic calculations*, ISA
[39] Kumamoto H 2007 *Satisfying safety goals by probabilistic risk assessment. Springer Series in Reliability Engineering*, Springer, London
[40] Stavrianidis P 1992 *Reliability Engineering and System Safety* **39** 309
[41] SINTEF 2010 *Reliability Data for Safety Instrumented Systems – PDS Data Handbook. SINTEF 2010 edition*