Śliwiński Marcin

Piesik Emilian
Gdańsk University of Technology , Gdansk, Poland

Integrated approach for functional safety and cyber security management in maritime critical infrastructures

Keywords

Maritime infrastructure, functional safety, cyber security, SIL, SAL, EAL, industrial control systems

Abstract

The work is devoted important issues of the management in maritime critical infrastructure of functional safety analysis, in particular the safety integrity level (SIL) verification of safety functions to be implemented within the distributed control and protection systems with regard to cyber security aspects. A method based on quantitative and qualitative information is proposed for the SIL (IEC 61508, 61511) verification with regard of the evaluation assurance levels (EAL) (ISO/IEC 15408), the security assurance levels (SAL) (IEC 62443), and the number of protection rings described in the Secure Safety (SeSa-SINTEF) methodology. The proposed approach will be composed of the following items: process and procedure based safety and cyber security management, integrated safety and security assessment of industrial control system (ICS) of the maritime critical infrastructure. Proposed methodology is illustrated on case study that based on the part of installation critical maritime infrastructure.

1. Introduction

The procedure for functional safety management includes the hazard identification, risk analysis and assessment, specification of safety requirements and definition of safety functions [9]-[10]. These functions are implemented in basic process control system (BPCS) and/or safety instrumented system (SIS), within industrial network system that consists of the wireless connection and wire connection. Determination of required SIL related to the risk mitigation is based on semi-quantitative evaluation method [6], [9]-[10]. Verification of SIL for considered architectures of BPCS and/or SIS is supported by probabilistic modelling for appropriate data and model parameters including security-related aspects [1], [10]. Proposed approach based on functional safety aspects that are well known in process industries and cyber security methodology [11]-[12], [18]. Main problem of these topic is influence security aspects on functional safety analysis. The approach proposed is illustrated on example part of critical installations. The control and protection systems of the installations and relevant maritime critical infrastructures are potentially vulnerable to cyber-attacks (e.g. malicious association, denial of service, network injection), as they are distributed and perform complex functions of supervisory control and data acquisition (SCADA) [4], [6]. Current topic that requires further research includes the interface between safety and security. The report discusses these issues on example of knowledge based proactive functional safety and cyber security management system.

2. Safety and cyber security of industrial control system in critical installations

Safety is concerned with preventing accidents by iden tifying potential weaknesses, initiating events, interna l hazards and potentially hazardous states and then id entifying and applying appropriate mitigation solutio ns to reduce relevant risks to tolerable levels [13], [17]. Security is concerned with protecting assets against internal and external threats and vulnerabilities that c ompromise the assets, environment and employees. A ssets are protected using controls that reduce the risk t o an acceptable level. The safety lifecycle is an engi neering process that contains the steps needed to achi eve high levels of functional safety during: conceptio n, design, operation, testing and maintenance of SIS [10] An industrial control system designed according t

o safety lifecycle requirements and procedures will m itigate relevant risks of potential hazardous events in an industrial installation and process e.g. pumping oil and gas station in and oil port infrastructure. Simplifi ed version of the safety lifecycle with regard to publi cations [4], [10], [15], [23] (*Figure 1*).

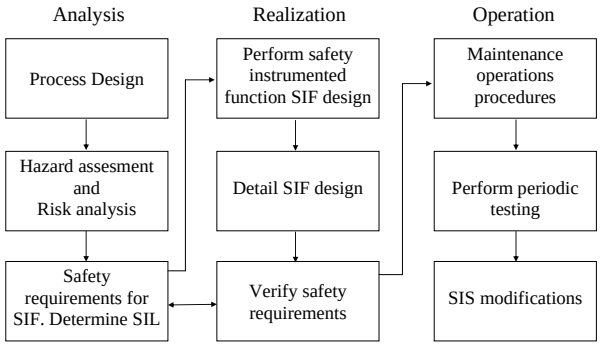

Figure 1. Simplified diagram of functional safety lifecycle

Some safety requirements are met with support of ext ernal risk reduction facilities, including solutions like changes in process design, physical protection barrier s, dikes, and emergency management plans. Safety re quirements are met partly by the safety-related techno logy other than safety instrumented systems (SIS), su ch as relief valves, alarms, and other specific-safety d evices.

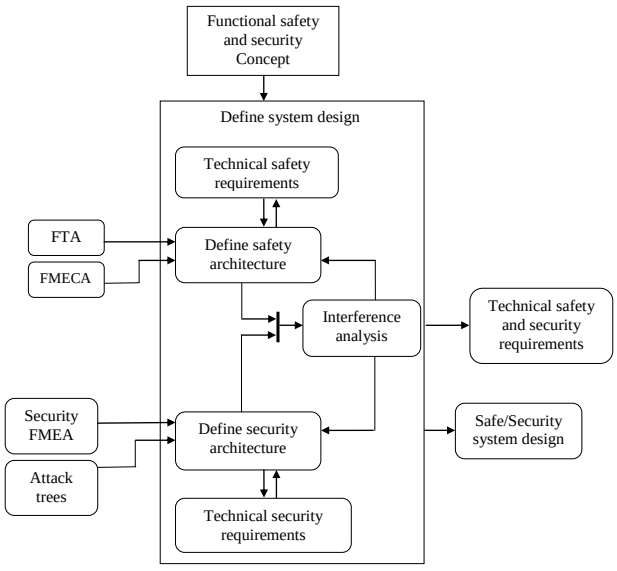

Figure 2. Safety and security activities of the system design phase

Remaining safety-related requirements are assigned t o the safety instrumented functions (SIF) implemente d as SIS of specified safety integrity level (SIL).

The system design phase comprises the activities to d erive technical safety and security requirements out o f the functional requirement and to define a correspon ding architecture [10], [18] (*Figure 2*).

The safety and security goals are now the input to der ive functional safety and security requirements. In thi s phase first the interference analyses have to be unde rtaken in order to identify their impact on each other.

In the safety area, supporting methods to derive techn ical requirements and analyze the system architecture include qualitative and quantitative Fault Tree Analys is (FTA) and Failure Mode and Effects Analysis (FM EA). A SIS management system should include the a spects specific to safety instrumented systems [10], [1 8].

Supervisory control and data acquisition (SCADA) re fers to the transmission of pipeline control parameters (such as pressures, flows, temperatures, and product c ompositions) at sufficient points along the pipeline to allow monitoring of the line from a single location (*F igure 3*) [6].

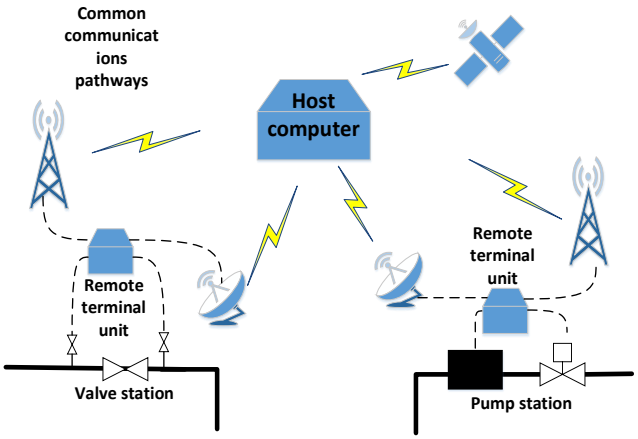

Figure 3. Data transfer in distributed industrial contr ol systems for an example pipeline infrastructure

In many cases, it also includes the transmission of dat a from the central monitoring location e.g. an oil port infrastructure to some points, e.g. pipelines and tanks , along the line to allow for remote operation of valve s, pumps, motors, etc.

3. Classification of the process control and protection systems

A conventional control and protection system consist s of a programmable logic controller (PLC), sensors, actuators, a control station with SCADA and a contro l station. Another important element of a control and protection system is the human operator who is super vising its operation. The system elements may be con nected by different internal or external communicatio n channels. The information sent between the PLC an d the control station can be transferred by standard se ries or parallel communication protocols or other met hods of communication, e.g. wireless GSM/GPRS. T

he control and protections system's in the oil sea port infrastructures may be connected by different internal and/or external communication channels (*Figure 4*).

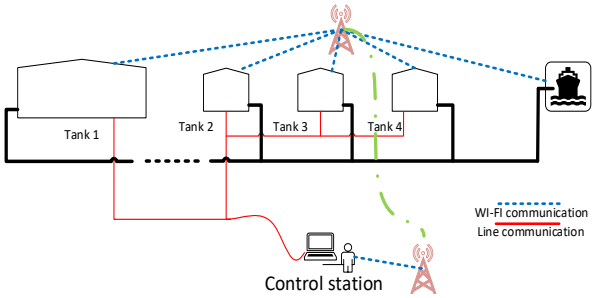

Figure 4. Data transfer in distributed industrial contro l systems for the oil pipeline infrastructure

Control station refers to the transmission of pipeline o perational data (such as pressures, flows, temperature s, and product compositions) at sufficient points alon g the pipeline to allow monitoring of the line from a s ingle.

Three main categories of distributed control and prote ction systems have been proposed, based on the prese nce of a computer system or an industrial network, its specification and type of data transfer methods:

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 mon itoring system data is sent by internal communicat ion channels and can be sent using external cha nnels;
III. Systems installed in distributed critical inst allations, where data is sent mainly by external co mmunication channels.

IEC 61508 and IEC 61511 introduce some additional requirements concerning the data communication cha nnels and security aspects in functional safety solutio ns. They describe two main communication channel t ypes - white or black. The white channel means that t he entire communications channel is designed, imple mented and validated according to the requirements o f IEC 61508. The black channel means that some part s of a communication channel are not designed, imple mented and validated according to IEC 61508. In suc h case, communication interfaces should be impleme nted according to the IEC 62280 standard on railway communication, signalling and processing system app lications (safety-related communication in closed tran smission systems) [1]-[2], [9]-[10].

4. Functional safety and cyber security integrated approach

The requirements for safety functions are determined taking into account the results of hazards identification, while the safety integrity requirements result from analysis of potential hazardous events. The higher the safety integrity level (SIL) is for given safety-related functions (SRF) the lower probability of failure on demand (PFD_{avg}) or probability of danger failure per hour (PFH) is required to reduce the risk to required level. Higher safety integrity levels impose more strict requirements on the design of a safety-related system. The term safety-related (SR) applies to the systems, which perform a specified function(s) to ensure that the risk is maintained at an acceptable or tolerable level. Those functions are the SRF. Two different requirements should be satisfied to ensure the functional safety [9]-[10]:

- requirements imposed on the performance of safety-related functions,
- requirements for the safety integrity expressed by the probability that given safety function is performed in satisfactory way within a specified time.

The safety-related E/E/EPS comprises all the elements that are necessary for the safety function performance, i.e., 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 the safety functions. The safety integrity level 1 (SIL1) is the lowest one, while the safety integrity level 4 is the highest level. The standard formulates in detail requirements to be fulfilled for each safety integrity level to be achieved. At higher levels the requirements become more strict to reduce relevant probability of PFD_{avg} or PFH of given SRF.

For each safety-related E/E/PE system fulfilling defined safety-related function of 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 the system operating in a low demand mode of operation,
- the probability of a dangerous failure per hour (PFH), i.e. the frequency for the 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* [9]-[10].

Table 1. Safety integrity levels and interval probabilis tic criteria for safety-related systems

Safety integrity level (SIL)	PFD_{avg} interval criteria for systems operating in a low demand mode	PFH interval criteria for systems operating in a high demand or continuous mode
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 SIL can be ou tlined as follows:
- determine the tolerable risk based on defined risk matrix or risk graph;
- determine the risk with regard to the EUC (equ ipment 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.

Results of security analysis for given control and prot ection system can be divided into some general categ ories, for example a qualitative description with defin ed security levels like: low level, medium level or hig h level of security. The aim of security analyses is to determine EAL achievable for considered solution of the system and/or network. The EAL determined for given solution is taken into account during functional safety analysis (*Table 2*) [3], [12], [14], [17].

Table 2. Levels of security and corresponding EALs

Evaluation assurance level	Level of security
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 confiden ce that the security functions of products and systems considered, and the assurance measures applied to the m meet these requirements. The evaluation results ma y help the developers and users to determine whether the product or system is secure enough for their inten ded application and whether the security risks implici t in its use are tolerable.

Another approach for security evaluation for industri al automation and control systems is IEC 62443. A co ncept of Security Assurance Level (SAL) has been in troduced in this normative document. There are four s ecurity levels (SAL1 to 4) and they are assessed for g iven security zone using the set of 7 functional requir ements (1) [11], [18]. The IEC 62443 standard uses s ecurity 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 that they protect against.

Table 3. Security assurance levels SALs

SAL level	Level of cyber security
SAL1	Protection against casual or coincidental violation
SAL2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation
SAL3	Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation
SAL4	Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivation

The SAL is a relatively new security measure concer ning the control and protection systems. It is evaluate d based on a defined vector of seven requirements for relevant cyber security zone [11]:

$$SAL = \{AC \quad UC \quad DI \quad DC \quad RDF \quad TRE \quad RA\}, \quad (1)$$

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 method of the security analysis can be proposed on the basis of the SeSa (Secure Safety) approach, which was designed by the Norwegian research institution SINTEF. It is dedicated to the control systems and automatic protection devices used in the offshore installations, monitored and managed remotely from the mainland by generally available means of communication [5], [19]. The SIS according to the series of standards IEC 61508 and IEC 61511 are very important not only for the safety, but also security aspects should be also taken into account. Using the SeSa rings related to security protection is another approach useful for the integration of functional safety and security aspects (*Figure 5*).

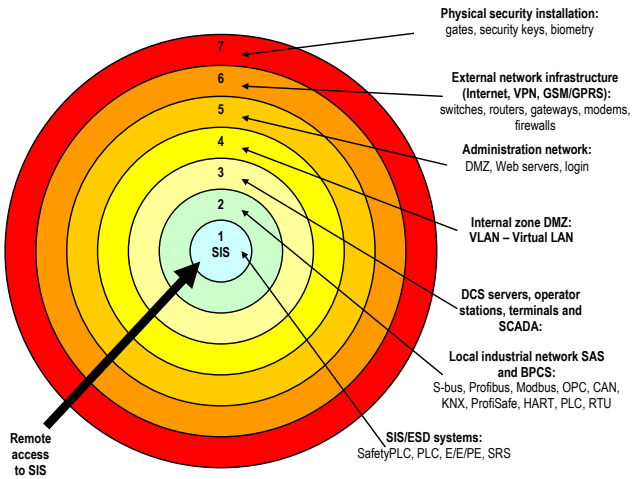

Figure 5. Rings of the protection in the SIS system [2

], [5]

An important task of integrated functional safety and security analysis of such systems is the verification of required SIL taking into account the potential influence of described above security levels, described the EAL, SAL or SeSa protection rings [3], [15], [16], [21].

5. Procedure of functional safety and cyber security management in maritime critical infrastructures

Although the concepts concerning the safety and security of information technology (IT) infrastructure are generally outlined in standards [9], [12], respectively, additional research effort should be undertaken to develop integrated, system oriented approach. Following problems require special attention [1]:

- development of integrated safety and security policy;
- modeling the system performance with regard to safety and security aspects;
- integrated risk assessment with regard to quantitative and qualitative information, identifying the factors influencing risk.

As was mentioned earlier, the result of security analysis is dependent on identified vulnerabilities and designed countermeasures. Both those factors are responsible for final level of security taken into account in the functional safety risk assessment process, a general procedure is presented (*Figure 6*). 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 SIL for given safety-related system as a main one.

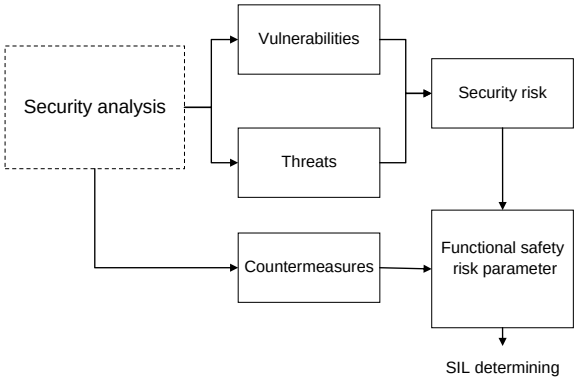

Figure 6. Procedure using security factors in functional safety analysis [2]

This method is very useful, but special care should be taken into account during applying the method. A general scheme of consideration the security analysis results is presented (*Figure 7*). It is assumed that the security analysis, e.g. SVA (security vulnerability analysis) is carried out separately, and its result shows how secure the object or control system is. Presented methodology has a significant importance in control and protection systems which are distributed and use different wire or wireless communication channels.

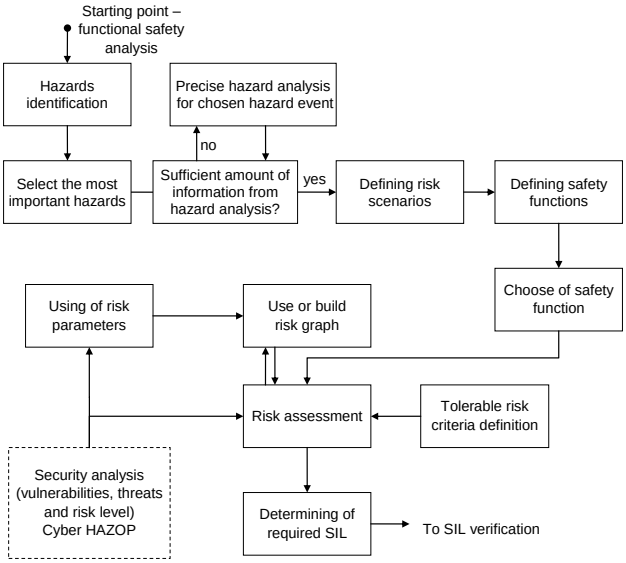

Figure 7. A general procedure of SIL determining with the cyber security integration

Proposed method of the SIL determination is based o n modifiable risk graphs, which allows building any r isk graph schemes with given number of the risk para meters and their ranges expressed qualitatively or pre ferably quantitatively [2]-[3], [17]. For verifying SIL of the E/E/PE system or SIS the quantitative method based on the reliability block diagram (RBD) is often used. Taking into account a method of minimal cut se ts, the probability of failure to perform the design fun ction on demand can be evaluated based on following formula [17], [20]

$$PFD(t) \cong \sum_{j=1}^{n} Q_j(t) \approx \sum_{j=1}^{n} \prod_{i \in K_j} q_i(t), \qquad (2)$$

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

The average probability of failure to perform the design function on demand for the system in relation

to formula (2), assuming that all subsystems are tested with the interval T_I, is calculated as follows:

$$PFD_{avg} = \frac{1}{T_I}\int_0^{T_I} PFD(t)dt\,, \tag{3}$$

where: T_I - proof test interval.

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

$$PFH \cong \frac{\sum_{j=1}^{n}(1-\sum_{\substack{i=1\\ i\neq j}}^{n} Q_j(t))(\sum_{j\in K_j}\frac{Q_j(t)}{q_i(t)}(1-q_i(t))\lambda_i)}{1-\sum_{j=1}^{n}\prod_{i\in K_j} q_i(t)} \tag{4}$$

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

Dependent failures in redundant systems increase significantly probability of potential breakdowns. They should be included in probabilistic modeling of E/E/PE (or SIS) systems. There is also known problem to determine the value of β - factor representing potential *CCF* (common cause failure) for given redundant system. For practical reasons a knowledge-based approach can be applied, similarly as in IEC 61508, based on scoring of factors influencing potential dependent failures [7]- [8], [17], [20]. There are also proposals evaluate β - factor depending on architecture of redundant systems considered

$$\beta_{koon} = \beta \cdot C_{koon} \tag{5}$$

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

As values of C_{koon} following have been assumed: $C_{1oo2}=1$; $C_{1oo3}=0.5$; $C_{2oo3}=1.5$ (*Table 4*).

Table 4. The $\beta_{(koon)}$ factor for redundant (*koon*) structu res [9]

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

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

$$\lambda = \lambda_I + \lambda_C\,. \tag{6}$$

In such case the factor β is defined as follows

$$\beta = \frac{\lambda_C}{\lambda}\,. \tag{7}$$

Regarding (6) and (7) the dependent failure rate is calculated from equation:

$$\lambda_C = \beta \cdot \lambda. \tag{8}$$

Whereas independent failure rate is obtained from formula:

$$\lambda_I = (1-\beta)\cdot\lambda. \tag{9}$$

Then using (8) and (9) the dependent probability of failure can be calculated as follows

$$q_C(t) = \beta \cdot q(t) \tag{10}$$

and independent failure probability from following formula

$$q_I(t) = (1-\beta)\cdot q(t). \tag{11}$$

Figure 8 illustrates a block diagram for 1oo2 structure including dependent failure [7]-[8], [17].

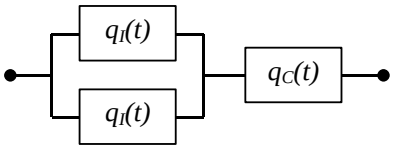

Figure 8. Reliability block diagram for 1oo2 system including dependent failure

On the basis of formulas (2), (3) and (6÷11) it is possible to calculate the probability of failure on demand for 1oo2 system including common cause failures from following equation

$$PFD_{avg1oo2} \cong [(1-\beta)\lambda_D]^2(\frac{T_I^2}{3} + T_I MTTR + \\ + MTTR^2) + \beta\lambda_{DU}(\frac{T_I}{2} + MTTR), \tag{12}$$

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 1oo2 architecture is evaluated taking in account (2) and (4) from the formula as below

$$PFH_{1oo2} \cong 2[(1-\beta)\lambda_D]^2\left(\frac{T_I}{2} + MTTR\right) + \beta\lambda_{DU} \quad (13)$$

It is known, the overall subsystem's failure rate is calculated from the equation (*Figure 9*):

$$\lambda = \lambda_D + \lambda_S = \lambda_{DU} + \lambda_{DD} + \lambda_{SU} + \lambda_{SD} \quad (14)$$

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 danger undetected rate is evaluated on the basis of diagnostic coverage (DC) coefficient, e.g. from the formula:

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} = \frac{\lambda_{DD}}{\lambda_D} \quad (15)$$

There are substantial problems in evaluating DC for some components (subsystems), especially sensors and actuators.

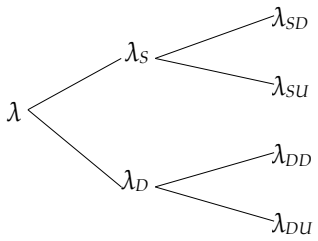

Figure 9. The overall subsystems failure rate

The SIL is associated with safety aspects while the EAL, SAL and SeSa is concerned with level of information security of entire system performing monitoring, control and/or protection functions (*Table 5*).

Table 5. SIL that can be claimed for given EAL, SAL or SeSa protection rings for distributed control and protection systems of category II and (III) [17], [22]

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

Table 5 shows the potential corrections of SIL for low, medium and high level 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 the safety-related functions in case of low security level. Thereby 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 safety integrity level (SIL) with levels of security (EAL, SAL and SeSa) 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 the safety-related functions in case of low security level (*Figure 10*).

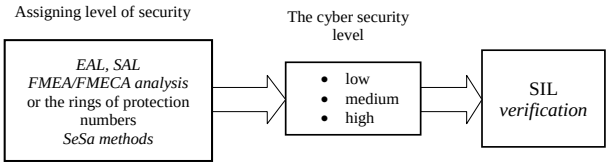

Figure 10. Assigning level of cyber security in industrial network

Such integrated approach is necessary, because not including security aspects in designing safety-related control and/or protection systems operating in network may result in deteriorating safety (lower SIL than required). In such cases the SIL verification, integrated with security aspects, is necessary (*Figure 11*).

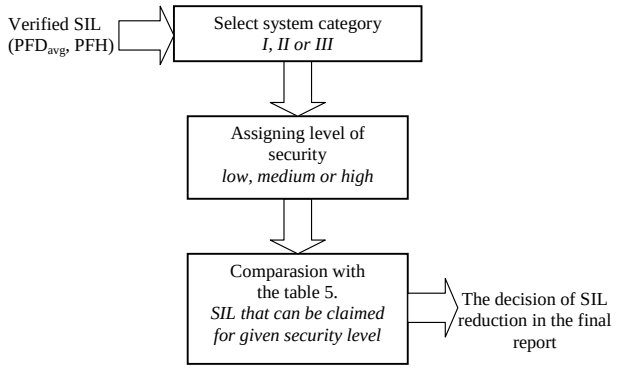

Figure 11. Procedure of the safety integrity level verification including the security aspects

The security measures which may be taken into account during the functional safety analyses are also of a prime importance. In this project only some of them have been presented. A well-known concept of EAL, SAL and SeSa is the basis for presented methodology. But there are also limitations of in applying the common criteria and for some solutions of programmable systems the EAL related measures may be insufficient. Usually EAL is related only to single hardware or software element. That is the reason why other security models or descriptions should be taken into account. One of them may be proposed lately the SAL based approach, indented to describe in an integrated way the system security in relation to functional safety concept.

6. Case study

The Safety Instrumented Systems (SIS) according to the series of standards IEC 61508 and IEC 61511 are very important not only for the safety, but also security aspects should be also taken into account using the SeSa rings related to security protection is another approach useful for the integration of functional safety and cyber security aspects [2], [17]. Another important element is the human operator, who supervises the operation [22]-[23]. The system's elements may be connected by different internal and/or external communication channels (*Figure 12*). The information sending and receiving between PLC and the control station can be transferred by wireless communication, such as radio-modems, satellite or GSM/GPRS technology. The part of the oil sea port installation is one of most representative example to illustrated the scope of functional safety and cyber security integrated approach.

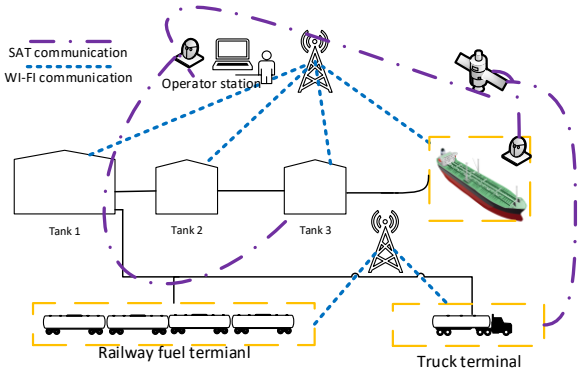

Figure 12. Data transfer in distributed industrial control systems for the oil pipeline infrastructure

The part of the oil sea port installation is one of most representative example to illustrated the scope of functional safety and cyber security integrated approach. Main part of fuel base consist of tanks, pipeline infrastructure, engineering station, truck terminal, railway fuel terminal. connection e.g. explosion atmosphere, electromagnetic fields and electric spark in distributed installation. Main reason is that some parts of the large distributed installation are without option to use the line connection. Presented installation is distributed and control and protection system is III category (wireless and satellite). It is presented on *Figure 12*. There are a lot of problems in that kind of installation. Main of the problem is high pressure oil transfer, overfill prevention tanks, pipe line leak, human errors, and common communication errors. Simulation processes was made via computer simulation environment Flownex software. CFD model for the oil seaport pipeline infrastructure is presented on *Figure 13*.

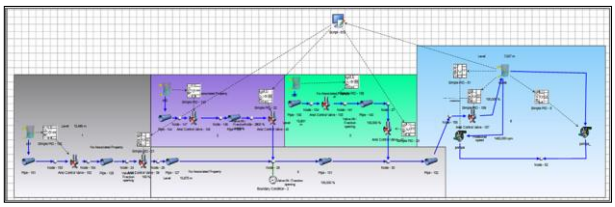

Figure 13. Flownex CFD model for the oil pipeline infrastructure

The SIL is associated with safety aspects while the EAL and SAL is concerned with level of information security of entire system performing monitoring, control and/or protection functions. *Table 5* shows the potential corrections of SIL for low, medium and high level of safety-related (E/E/PE or SIS) system security.
Considered part of the installation refers to the liquid fuels base consisting of three tanks and one buffer storage tank. The system is connected to the main

pipeline. Fuel transfer takes place between the tanks and a loading position. In the illustrated system (*Figure 14*), there is a two-way communication connection are wired and wireless. Wireless connections are used to transmit information on the level of fuel in the tanks. In the case of a wired connection also exists to measure the liquid level in the tank and the core system control fuel flow [4], [6].

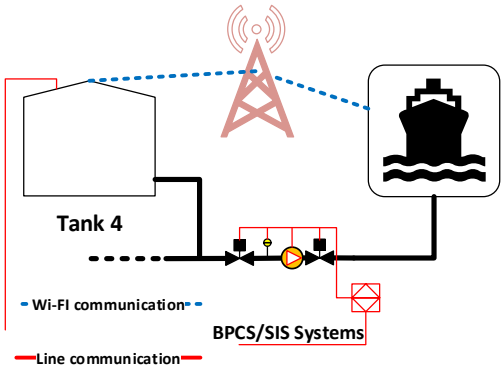

Figure 14. Example of oil seaport installations with critical infrastructure including BPCS and SIS systems

In situation of distributed control and/or protection systems operating in a network it is necessary to consider also potential failures within such network (*Figure 15*).

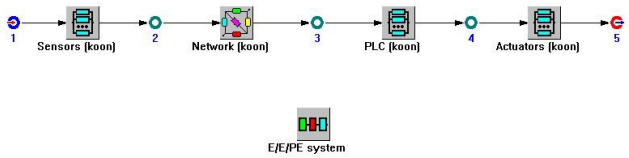

Figure 15. RBD model SIS (E/E/PE) system including the industrial computer network

The average probability of failure on demand PFD_{avg} is calculated according to formula:

$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgNet} + \\ + PFD_{avgPLC} + PFD_{avgA} \quad (16)$$

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

Taking into account (16) it is obvious that the value of probability will be greater in situation if considering the computer network. Thus, the results obtained can influence verified SIL (lower value of SIL than in the case without considering network). The modeling methods proposed in the IEC 61508 and IEC 61511 standard do not include the computer network elements. Thus, the results obtained can be too optimistic. A communication channel between controllers was represented by the block with determined SIL.

An example of functional safety analysis that is presented below. It is based on a control system (*Figure 16*), which consists of some basic components like sensors, programmable logic controllers and valves. It is a part of an maritime petrochemical critical installations.

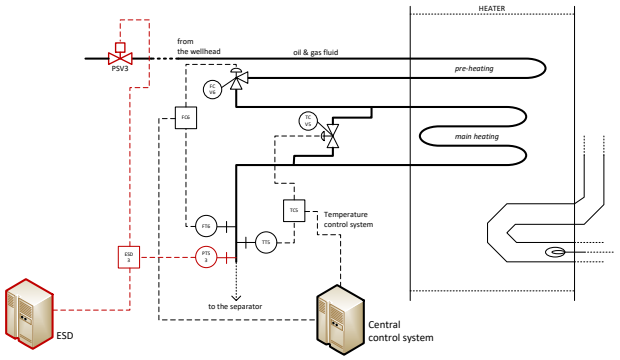

Figure 16. Data transfer in distributed industrial control systems

From the risk assessment the safety integrity level for given safety function overpressure protection heater in maritime critical installation was determined as SIL3. In industrial practice such level requires usually to be designed using a more sophisticated configuration. Safety function (overpressure protection) is implemented in distributed safety instrumented system SIS (*Figure 17*).

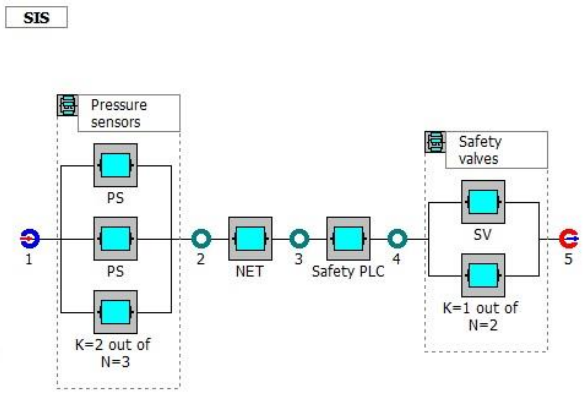

Figure 17. RBD model overpressure safety instrumented system SIS in the critical installation

The required SIL for 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. Reliability data for SIS elements are presented in *Table 6* [2], [19].

Table 6. Reliability data for elements SIS system

	PS	NET	SafetyPLC	SVA
DC [%]	54	99	90	95
λ_{DU} [1/h]	$3 \cdot 10^{-7}$	$8 \cdot 10^{-8}$	$7 \cdot 10^{-7}$	$8 \cdot 10^{-7}$
T_I [h]	8760	8760	8760	8760
β	0.02	0.01	0.01	0.02

Table 7. The SIL verification report for SIS overpressure protection system

System /subsystems/elements		**k oo n**	**β [%]**	**PFD_{avg}**	**SIL**
SIS	**0**	-	-	**$9.15 \cdot 10^{-4}$**	**3**
PS	**.1**	**2 oo 3**	**3**	**$4.46 \cdot 10^{-5}$**	**4**
PS	..2	-	-	$1.34 \cdot 10^{-3}$	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**	-	**$4.38 \cdot 10^{-4}$**	**3**
Safety PLC	..2	-	-	$4.38 \cdot 10^{-4}$	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

Assessment of the result obtained shows that for the SIS structure (*Figure 17*) is:

$$\begin{aligned} PFD_{avgSIS} &\cong PFD_{avgPS(2oo3)} + PFD_{avgNET} + \\ &+ PFD_{avgSafetyPLC} + PFD_{avgSV(1oo2)} \cong \\ &\cong 4.46 \cdot 10^{-5} + 3.5 \cdot 10^{-4} + 4.38 \cdot 10^{-4} + \\ &+ 8.22 \cdot 10^{-5} \cong 9.15 \cdot 10^{-4} \Rightarrow SIL3 \end{aligned} \tag{17}$$

Thus, the PFD_{avg} is equal $9.15 \cdot 10^{-4}$ fulfilling formally requirements for random failures on level of SIL3. The omission of some subsystems or communication network can lead to too optimistic results, particularly in case of distributed control and protection systems of category II and III.

Human operator in that case is an important part of th e system. But in determining functional safety require ments processes the operator is treat an independent p rotection layer. Information from the alarm systems a nd basic process control system goes to the human op erator. Human error probability was calculated by the Spar-H method it is one of most useful method of hu man reliability analysis in functional safety it consist of two parts diagnosis and action for the human [13], [22]. Calculated human error probability according to the available time is these value 0.268. In the future it should be include to the verification process. Challen ge in that process is integrated cyber security aspects and human error probability according to the function al safety. Nowadays popular problems is the cyber att acks to the industrial control systems through differen t communication channel, of course vulnerability thre ats include the attacks to the SCADA systems can ta ke significant influence to the human action and in co nsequence it will lead to dangerous situation e.g. econ omical, environmental, health losses.

7. Conclusions

A comprehensive integration of the functional safety and cyber security analysis in maritime critical infrastructures is very important and it is currently a challenging issue. In this project an attempt to integrate the functional safety and security issue was presented. 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. 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. The next step of evaluation the proposed approach safety & cyber security integrated it to include human as a hazard factor.

Acknowledgments

The paper presents the results developed in the scope of the HAZARD project titled “Mitigating the Effects of Emergencies in Baltic Sea Region Ports” that has received funding from the Interreg Baltic Sea Region Programme 2014-2020 under grant agreement No #R023. https://blogit.utu.fi/hazard/

"Scientific work granted by **Poland’s Ministry of Science and High Education** from financial resources for science in the years 2016-2019 awarded for the implementation of an international co-financed project."

References

[1] Barnert, T., Kosmowski, K.T., Śliwiński, M. (2010). *Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issues*. Proceedings of PSAM 2010, Seattle.

[2] Barnert, T., Śliwiński, M. (2013). *Functional safety and information security in the critical infrastructure objects and systems* (in Polish), Modern communication and data transfer systems for safety and security. Wolters Kluwer, 476-507.

[3] Barnert, T., Kosmowski, K.T., Piesik, E., Śliwiński, M. (2014). *Security aspects in functional safety analysis*. Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, Volume 5, Number 1.

[4] Goble, W., Cheddie, H. (2005). *Safety instrumented systems verification*: Practical probabilistic calculations. ISA.

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

[6] Hildebrandt, P. (2000). *Critical aspects of safety, availability and communication in the control of a subsea gas pipeline*, Requirements and Solutions HIMA.

[7] Hokstad, P. (2004). *A generalisation of the beta factor model*, Proceedings of the European Safety & Reliability Conference, Berlin.

[8] Hoyland, A., Rausand, M. (2004). *System Reliability Theory*. Models and Statistical Methods, Second Edition, John Wiley & Sons, Inc, New York.

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

[10] IEC 61511. (2015*). Functional safety: Safety Instrumented Systems for the Process Industry Sector*. Parts 1-3, International Electrotechnical Commission, Geneva.

[11] IEC 62443. (2013). *Security for industrial automation and control systems*. Parts 1-13, International Electrotechnical Commission, Geneva.

[12] ISO/IEC 15408. (1999). *Information technology Security techniques – Evaluation criteria for IT security*. Part 1-3. International Electrotechnical Commission, Geneva.

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

[14] 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, London.

[15] Kosmowski, K.T., Śliwiński, M., Piesik, E., Gołębiewski, D. (2016). *Procedure based proactive functional safety management for the risk mitigation of hazardous events in the oil port installations including insurance aspects*. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars.

[16] NIH. (2002). *Security Level Designatio*n, National Institutes of Health.

[17] Piesik, E., Śliwiński, M., Barnert, T. (2016). *Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects*, Reliability Engineering & System Safety, 152, 259-272.

[18] SESAMO. (2014). *Integrated Design and Evaluation Methodology*. Security and Safety modelling. Artemis JU Grant Agr. no. 2295354.

[19] SINTEF. (2010). *Reliability Data for Safety Instrumented Systems* - PDS Data Handbook. SINTEF 2010 edition.

[20] Śliwiński, M. (2006). *Methods of risk analysis based on functional safety aspects for the control and protection systems*. GUT, Gdańsk.

[21] Śliwiński, M., Kosmowski, K.T., Piesik, E. (2015). *Verification of the safety integrity levels with regard of information security issues* (in Polish), In: Advanced Systems for Automation and Diagnostics, PWNT, Gdańsk.

[22] Śliwiński, M., Piesik, E. (2017). *Procedure based functional safety and information security management of industrial automation and control systems on example of the oil port installations*, Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars.

[23] Śliwiński, M., Piesik, E. (2018). *Functional safety with cyber security for the control and protection systems on example of the oil port infrastructure*, Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars.