**Śliwiński Marcin**
*Gdańsk University of Technology , Gdansk, Poland*

**Piesik Emilian**
*Gdańsk University of Technology , Gdansk, Poland*

# Procedure based functional safety and information security management of industrial automation and control systems on example of the oil port installations

**Keywords**

functional safety, security, cyber HAZOP, industrial control systems, oil port installations

**Abstract**

The approach addresses selected technical and organization aspects of risk mitigation in the oil port installations with regard to functional safety and security requirements specified in standards IEC 61508, IEC 61511 and IEC 62443. The procedure for functional safety management includes the hazard identification, risk analysis and assessment, specification of overall safety requirements and definition of safety functions. Based on the risk evaluation results the safety integrity level (SIL) and security assurance level (SAL) will be determined for consecutive safety functions. The proposed approach will be composed of the following items: process and procedure based safety and security management, example of procedure based safety management including insurance, integrated safety and security assessment of industrial control system (ICS) of the oil port pipelines, tanks and critical infrastructure.

## 1. Introduction

These article presented technical and organization aspects of risk mitigation in the oil port installations with regard to functional safety requirements specified in standards IEC 61508 and IEC 61511. The procedure for functional safety management includes the hazard identification, risk analysis and assessment, specification of safety requirements and definition of safety functions [8, 9].

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 line connection. Determination of required SIL related to the risk mitigation is based on semi-quantitative evaluation method [7, 8, 9]. Verification of SIL for considered architectures of BPCS and/or SIS is supported by probabilistic modeling for appropriate data and model parameters including security-related aspects [1, 2, 13]. The approach proposed is illustrated on example of oil port installations. The control and protection systems of the oil port installations and relevant critical infrastructure are potentially vulnerable to cyber attacks, as they are distributed and perform complex functions of supervisory control and data acquisition (SCADA) [5, 7, 15]. It is outlined how to mitigate some risks using the E/E/PE and/or SIS systems that implement defined safety related functions. These systems operate in industrial computer network (ICS).

## 2. Functional safety analysis including security aspects

One of the main objectives of functional safety analysis is determining of required safety integrity level (SIL) for the safety-related functions to be realized by safety-related systems. According to IEC 61508 to each SIL (1÷4) the interval probabilistic quantitative criterion is defined (*Table 1*) [8, 9].

*Table 1*. Safety integrity levels and probabilistic criteria for the E/E/PE systems [8, 9]

| SIL | $PFD_{avg}$ | PFH |
|---|---|---|
| 4 | [ $10^{-5}$, $10^{-4}$ ) | [ $10^{-9}$, $10^{-8}$ ) |
| 3 | [ $10^{-4}$, $10^{-3}$ ) | [ $10^{-8}$, $10^{-7}$ ) |
| 2 | [ $10^{-3}$, $10^{-2}$ ) | [ $10^{-7}$, $10^{-6}$ ) |
| 1 | [ $10^{-2}$, $10^{-1}$ ) | [ $10^{-6}$, $10^{-5}$ ) |

If the risk associated with given hazardous system is too high, it is necessary to reduce it to an acceptable level using electric / electronic/ programmable electronic (E/E/PE) system or safety instrumented system (SIS). Decreasing risk to the tolerable level is the main and necessary condition of risk reducing process. To obtain this, appropriate architecture of E/E/PE system or SIS must be designed and verified in probabilistic modeling process with regard to probabilistic criterion for given SIL. The procedure of determination and verification of SIL is shown in *Figure 1*.

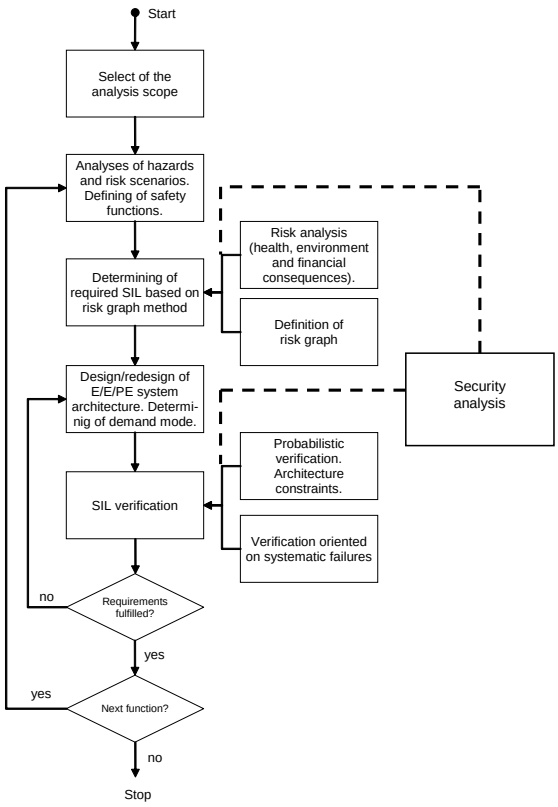


*Figure 1*. Functional safety analysis procedure with the information security aspects [1, 2]

For compliance with probabilistic criteria two methods of SIL verification are proposed in IEC 61508 – qualitative and quantitative. There is a general consensus that qualitative methods should be used only at initial stage of the system design and in cases of reliability data shortage. Quantitative methods are preferable for verification of SIL, especially when reliability data for analyzed system are known, usually acquired from various sources including expert opinions [4, 8, 9].

In the process of the SIL verification using quantitative method it is needed to evaluate the average probability $PFD_{avg}$ of failure to perform the design function on demand for the system operating in low demand mode of operation or the probability of dangerous failure per hour (the frequency) PFH for the system operating in a high demand mode operation.

Functional safety analysis procedure usually doesn't include security aspects. But in case of distributed control and protection system it can have a practical significance. It may affect the results of determining as well as verification of SIL, taking into account functional safety analysis.

The security analysis concept is proposed in the standard ISO/IEC 15408. Security is considered with the protection from threats, where threats are categorized as the potential for abuse of assets. All categories of threats should be considered, but in the domain of security usually greater attention is given to those threats that are related to malicious or other human activities [3, 11].

The multipart standard ISO/IEC 15408 defines 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 permits comparability between the results of independent security evaluations. It does so by providing a common set of requirements for the security functions of IT products and systems for assurance measures applied to them during a security evaluation. Evaluation Assurance Level (EAL) is a package of assurance requirements which covers the complete development of a product with a given level of strictness. Common Criteria lists seven levels, with EAL1 being the most basic (the cheapest to evaluate and implement) and EAL7 being the most strict (the most expensive).

Higher EAL levels do not necessarily imply better security, they only mean that the claimed security assurance of the TOE (target of evaluation) has been more extensively validated.

The 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*) [2, 3, 11].

MOST WIEDZY Downloaded from mostwiedzy.pl

*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 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 the developers and users to determine whether the product or system is secure enough for their intended application and whether the security risks implicit in its use are tolerable.
Another approach for security evaluation for industrial automation and control systems (e.g. oil seaports) is IEC 62443. A concept of *Security Assurance Level* SAL has been introduced in this normative document. There are four security levels (SAL1 to 4) and they are assessed for given security zone using the set of 7 functional requirements [10].
The SAL is a relatively new security measure concerning the control and protection systems. It is evaluated based on a defined vector of seven requirements for relevant security zone:

$$SAL = \left\{ AC \quad UC \quad DI \quad DC \quad RDF \quad TRE \quad RA \right\} \tag{1}$$

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 (*SecureSafety*) 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 [6, 7, 16].
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.

## 3. Procedure of functional safety and security management in the oil seaport installations

The ICS play an important role in reconfigurable oil port installations and distributed external installations. In this distributed computer network the quality of safety related software of the Supervisory Control And Data Acquisition (SCADA) system will be of special interest.
A new method will be proposed for integrated determining the SIL (safety integrity level) and the SAL (security assurance level) for consecutive safety functions mitigating relevant risks. The analyses and assessments will take into account qualitative and/or quantitative information as regards the categories of hazardous events frequencies and potential losses in relation to defined risk graphs. Knowing the risk mitigation potential and uncertainty involved the insurance related decision making are carried out according to existing insurance company procedures used in insurance practice.
About 20 procedures have been preliminary specified. Examples of such procedures (PR) are as follows: PR FSS-01 Definition of installation including EUC and its environment; PR FSS-02 Hazard identification, risk analysis and assessment, overall safety requirements and definition of safety functions; PR FSS-07 Requirements for inspections, testing of safety related systems and maintenance activities; PR FSS-11 Overall security related analysis of the ICS during the design and operation of distributed computer network; PR INS-01 Requirements for overall preliminary description of the oil port installations, environment, infrastructure, hazards and threats, organizational factors and legal aspects for insurance purposes; PR INS-04 Integration of information from relevant sources and models for insurance related risk assessment for underwriting and indicating potential for technical and organizational improvements to mitigate relevant risks [9, 14].
Safety functions are to be implemented by the control and/or protection systems which are usually based on programmable electronic systems (conventional computers, programmable logic controllers - PLCs and specialized microprocessors). They are playing an important role in many applications, including the control and protection of hazardous systems. However, a failure or incorrect operation of such critical elements, controlling and/or protecting an industrial system could lead to serious injury or even the death of one or more people. In some cases it can lead to a significant environmental damage or property loss too. That's the reason why the risk analysis of the E/E/PE systems is so important [7, 8, 9, 12].

MOST WIEDZY Downloaded from mostwiedzy.pl

Having the result of security analysis for a control system, it can be divided into some general categories, for example a qualitative descriptive ranges like: low level of security, medium level of security or high level of security. If the security analysis is performed on the basis of [16], the corresponding SAL, SeSa (ring of protection methodology) or evaluation assurance level EAL can be determined. In this case this EAL can be taken into account in functional safety analysis too (see *Table 2*) [16]. 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 on *Figure. 4.*

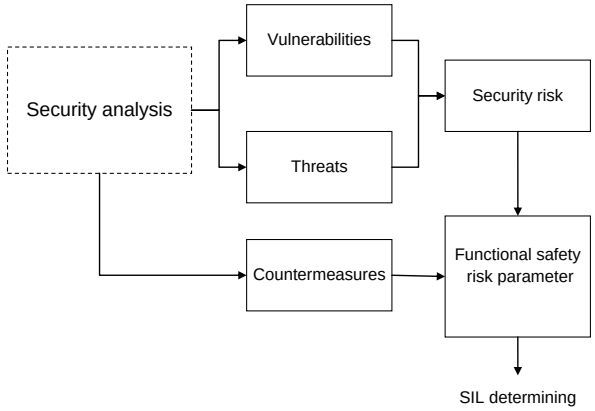


*Figure 4.* Procedure using security factors in functional safety analysis [3, 13]

A SIL is determined based on a number of quantitative factors in combination with qualitative factors during development process and safety life cycle management. There are several methods to determine SIL for a chosen safety function. Some of the popular ones are: Risk Matrix, Risk Graph, Layers of Protection Analysis (LOPA).
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. 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 on *Figure 4.*

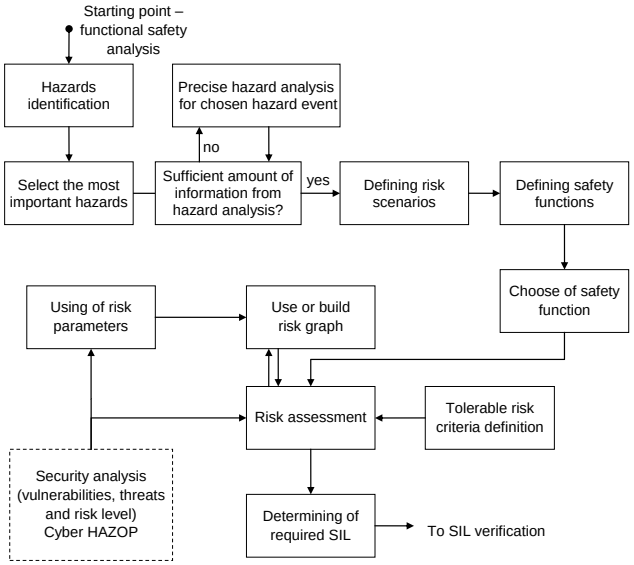


*Figure 5.* A general procedure of SIL determining with security integration

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.
Proposed method of the SIL determination is based on modifiable risk graphs, which allows building any risk graph schemes with given number of the risk parameters and their ranges expressed qualitatively or preferably quantitatively. The safety–related systems usually operating in a computer network using the wire and/or wireless communication technologies. In known functional safety analyses these aspects are sometimes neglected. The standard doesn't 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 group of functional requirements for the control and protection systems. It is the reason why the analyses of safety and security shouldn't be integrated directly. The proposed method of integration of these both aspects is based on usage of security analysis results as one of the inputs in functional analysis method. In this case a functional safety analysis is superior one and both analyses are done separately.
The control and protections system's in the oil sea port infrastructures may be connected by different internal and/or external communication channels (*Figure 6*).

MOST WIEDZY Downloaded from mostwiedzy.pl

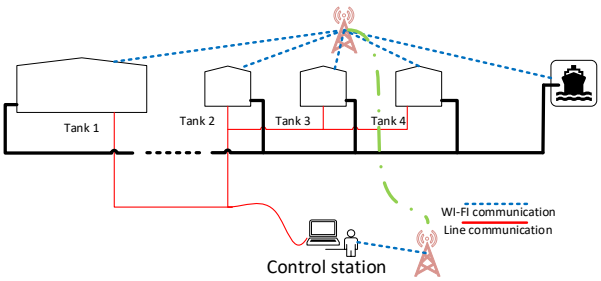


*Figure 6.* Data transfer in distributed industrial control systems for the oil pipeline infrastructure

Control station refers to the transmission of pipeline operational data (such as pressures, flows, temperatures, and product compositions) at sufficient points along the pipeline to allow monitoring of the line from a single.

In many cases, it also includes the transmission of data 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 valves, pumps, motors, etc.

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

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

In the oil seaport installation two categories distributed control system: II and III are distinguished (see *Figure*. 6).

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. 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 3*).

*Table 3.* SIL that can be claimed for given EAL, SAL or SeSa protection rings for systems of category II and (III)

| **Determined** | | | | **Verified SIL for II cat. (III cat.)** | | | |
|---|---|---|---|---|---|---|---|
| security | | | | ***functional safety*** | | | |
| **EAL** | **SAL** | **Protection rings** | **Level of security** | **1** | **2** | **3** | **4** |
| 1 | 1 | 1 | low | - (-) | SIL1 (-) | SIL2 (1) | SIL3 (2) |
| 2 | 1 | 1 | | - (-) | SIL1 (-) | SIL2 (1) | SIL3 (2) |
| 3 | 2 | 2 | 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) |

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.

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 as shown *in Figure 7* [17].



MOST WIEDZY Downloaded from mostwiedzy.pl

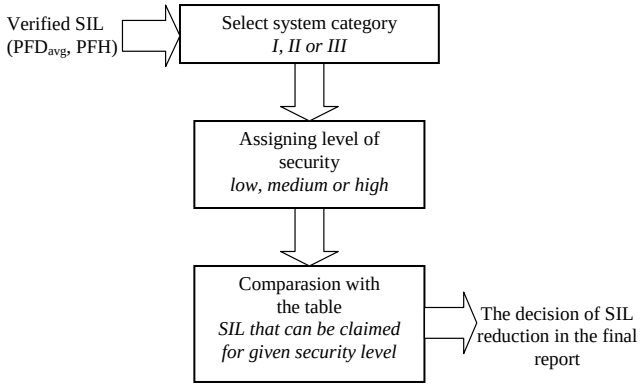


*Figure 7.* Procedure of the safety integrity level verification including the security aspects

The security measures which may be taken into account during the functional safety analyses are also of a prime importance. In this article 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* [15] 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.
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 security aspects.

## 4. Functional safety analysis with regard security aspect on example of oil sea port

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 (*see Figure. 8*), 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, 7, 15].

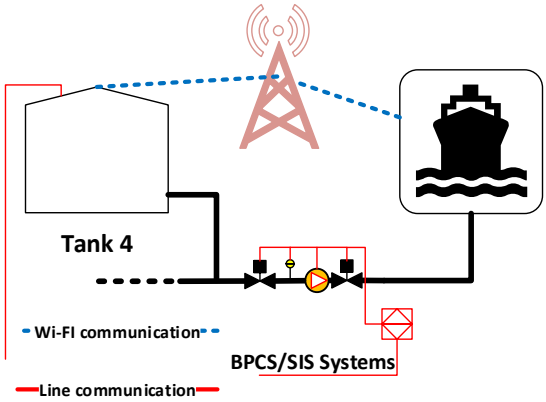


*Figure 8.* Example of oil seaport installations with critical infrastructure including BPCS and SIS systems

The safety integrity requirements apply to the *safety functions* (SF) implemented in the E/E/PE systems or SIS. The SIL of given SF is expressed by a natural number from 1 to 4 and it is related to the necessary risk reduction when the SF is implemented. The allocation of safety requirements to safety functions using the E/E/PE safety-related systems, and other technology safety-related systems or external risk reduction facilities.
An industrial control system designed according to safety lifecycle requirements and procedures will mitigate relevant risks of potential hazardous events in an industrial installation and process e.g. pumping oil and gas station in and oil port infrastructure.
Some safety requirements are met with support of external risk reduction facilities, including solutions like changes in process design, physical protection barriers, dikes, and emergency management plans. Safety requirements are met partly by the safety-related technology other than safety instrumented systems (SIS), such as relief valves, rupture disks, alarms, and other specific-safety devices. Remaining safety-related requirements are assigned to the *safety instrumented functions* (SIF) implemented as SIS of specified *safety integrity level* (SIL).

The safety and security goals are now the input to derive functional safety and security requirements. In this phase first the interference analyses have to be undertaken in order to identify their impact on each other. In the safety area, supporting methods to derive technical requirements and analyze the system architecture include qualitative and quantitative *Fault Tree Analysis* (FTA) and *Failure Mode and Effects Analysis* (FMEA). A SIS management system should include the aspects specific to safety instrumented systems.

MOST WIEDZY Downloaded from mostwiedzy.pl

In situation of distributed control and/or protection systems operating in a network it is necessary to consider also potential failures within such network. The average probability of failure on demand $PFD_{avg}$ is calculated according to formula:

$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgNet} + PFD_{avgPLC} + PFD_{avgA} \quad (1)$$

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 (1) 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.

From the risk assessment the safety integrity level for given safety function overpressure protection pipeline was determined as SIL3. In industrial practice such level requires usually to be designed using a more sophisticated configuration.

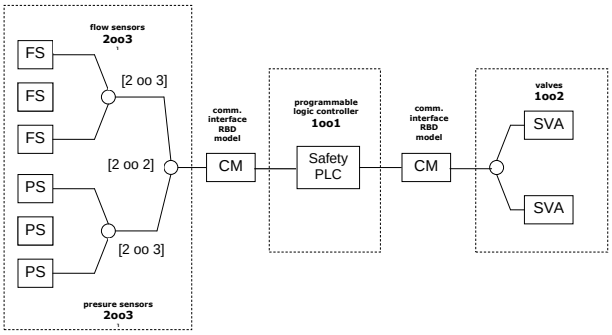


*Figure 9.* Sea oil port to fuel base overpressure pipeline protection SIS system (I)

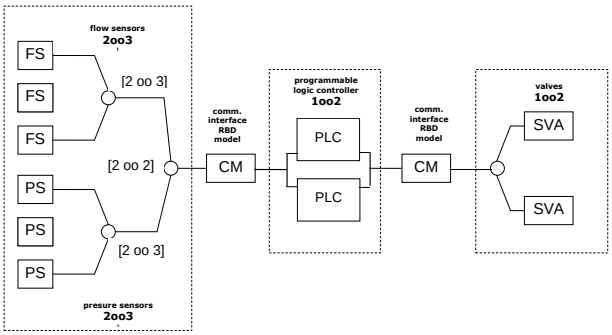


*Figure 10.* Sea oil port to fuel base overpressure pipeline protection SIS system (II)

Safety function (overpressure protection pipeline in the oil seaport) is implemented in distributed safety instrumented systems (see *Figure 9 and 10* ).

The required SIL for entire distributed E/E/PE or SIS system is determined in a process of risk analysis and evaluation.

*Table 4.* Reliability data for elements SIS system

| | PS | FS | CM | Safety PLC | SRS | SV |
|---|---|---|---|---|---|---|
| DC [%] | 54 | 66 | 90 | 90 | 90 | 24 |
| $\lambda_{DU}$ [1/h] | $3\cdot10^{-7}$ | $3\cdot10^{-6}$ | $1\cdot10^{-7}$ | $1\cdot10^{-6}$ | $1\cdot10^{-7}$ | $8\cdot10^{-7}$ |
| $T_I$ [h] | 8760 | 8760 | 4380 | 8760 | 8760 | 8760 |
| $\beta$ | 0.02 | 0.02 | 0.01 | 0.01 | 0.01 | 0.02 |

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 4*.

For verifying SIL of the E/E/PE system or SIS the quantitative method based on the reliability block diagram (RBD) is often used. There is also known problem to determine the value of $\beta$-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 [3, 7, 17].

Presented above case is rather a simple one. It is known that the probability measure of E/E/PE (or SIS) failure is generally a function of some variables, e.g. $PFD_{avgi} = f(\lambda_i, \beta_i, MTTR_i, DC_i, T_{Ii})$. Each parameter of probabilistic model influences to some extent the system failure probability. Final values of $PFD_{avg}$ (or PFH) depend on respective parameters, and are very sensitive to $\beta$ factor representing potential dependent failures [17].

*Table 5.* The SIL verification report for SIS (I)

| **System /podsystem /element** | | **k oo n** | **β [%]** | **$PFD_{avg}$** | **SIL** |
|---|---|---|---|---|---|
| **SIS (I)** | **0** | **-** | **-** | **$4.79\cdot10^{-3}$** | **2** |
| **FS** | **.1** | **2 oo 3** | **3** | **$2.93\cdot10^{-5}$** | **4** |
| FS | ..2 | - | - | $1.53\cdot10^{-3}$ | 2 |
| FS | ..2 | - | - | $1.53\cdot10^{-3}$ | 2 |
| FS | ..2 | - | - | $1.53\cdot10^{-3}$ | 2 |
| **PS** | **.1** | **2 oo 3** | **3** | **$3.11\cdot10^{-5}$** | **4** |
| PS | ..2 | - | - | $1.58\cdot10^{-3}$ | 2 |
| PS | ..2 | - | - | $1.58\cdot10^{-3}$ | 2 |
| PS | ..2 | - | - | $1.58\cdot10^{-3}$ | 2 |
| **CM** | **.1** | **1 oo 1** | **-** | **$2.19\cdot10^{-4}$** | **3** |
| CM | ..2 | - | - | $2.19\cdot10^{-4}$ | 3 |
| **PLC** | **.1** | **1 oo 1** | **-** | **$4.44\cdot10^{-3}$** | **2** |



MOST WIEDZY Downloaded from mostwiedzy.pl

| | | | | | |
|---|---|---|---|---|---|
| Safety PLC | ..2 | - | - | $4.44 \cdot 10^{-3}$ | 2 |
| **SV** | **.1** | **1 oo 2** | **2** | $\mathbf{7.14 \cdot 10^{-5}}$ | **4** |
| SVA | ..2 | - | - | $3.5 \cdot 10^{-3}$ | 2 |
| SVA | ..2 | - | - | $3.5 \cdot 10^{-3}$ | 2 |

Therefore, its reliable operation is dependent on correct functioning of each subsystem.

*Table 6.* The SIL verification report for SIS (II)

| System /podsystem | | k oo n | β [%] | $PFD_{avg}$ | SIL |
|---|---|---|---|---|---|
| **SIS(II)** | **0** | **-** | **-** | $\mathbf{7.89 \cdot 10^{-4}}$ | **3** |
| **FS** | **.1** | **2 oo 3** | **3** | $\mathbf{2.93 \cdot 10^{-5}}$ | **4** |
| FS | ..2 | - | - | $1.53 \cdot 10^{-3}$ | 2 |
| FS | ..2 | - | - | $1.53 \cdot 10^{-3}$ | 2 |
| FS | ..2 | - | - | $1.53 \cdot 10^{-3}$ | 2 |
| **PS** | **.1** | **2 oo 3** | **3** | $\mathbf{3.11 \cdot 10^{-5}}$ | **4** |
| PS | ..2 | - | - | $1.58 \cdot 10^{-3}$ | 2 |
| PS | ..2 | - | - | $1.58 \cdot 10^{-3}$ | 2 |
| PS | ..2 | - | - | $1.58 \cdot 10^{-3}$ | 2 |
| **CM** | **.1** | **1 oo 1** | **-** | $\mathbf{2.19 \cdot 10^{-4}}$ | **3** |
| CM | ..2 | - | - | $2.19 \cdot 10^{-4}$ | 3 |
| **PLC** | **.1** | **1 oo 1** | **-** | $\mathbf{4.38 \cdot 10^{-4}}$ | **3** |
| SRS | ..2 | - | - | $4.38 \cdot 10^{-4}$ | 3 |
| **SV** | **.1** | **1 oo 2** | **2** | $\mathbf{7.14 \cdot 10^{-5}}$ | **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 on *Figure 9* is:

$$PFD_{avgSIS} \cong PFD_{avgFS(2oo3)} + PFD_{avgPS(2oo3)} + PFD_{avgCM} + \\ + PFD_{avgPLC(1oo2)} + PFD_{avgSV(1oo2)} \cong 2.93 \cdot 10^{-5} + 3.11 \cdot 10^{-5} + \\ + 2.19 \cdot 10^{-4} + 4.38 \cdot 10^{-4} + 7.14 \cdot 10^{-5} \cong 7.89 \cdot 10^{-4}$$

Thus, the $PFD_{avg}$ is equal $7{,}89 \cdot 10^{-4}$ 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.

## 5. Conclusion

The role of safety-related control and protection systems for the risk mitigation is nowadays obvious, because are designed to reduce the risks of accident scenarios, especially those with major consequences many times, e.g. from ten times to thousand and more times depending on required risk mitigation. These systems belong to the category of *industrial control systems* (ICS).
They implement a set of safety functions and can be designed as the electrical / electronic / programmable electronic systems (E/E/PES) regarding generic standard IEC 61508 and/or the safety instrumented systems (SIS) with regard to requirements of IEC 61511 developed for the process industry. Requirements concerning security related aspects will be considered regarding requirements of series of international standards IEC 62443 an ISO 27000.
An integrated risk analysis and assessment methodology proposed is compatible with some known methods used often in practice, such as HAZOP (*hazard and operability*) , LOPA (*layer of protection analysis*) and SVA (*security vulnerability analysis*). The methodology is applied to selected oil port installations including ICS functions designed and implemented to mitigate relevant risks.

## Acknowledgements

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/

## 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 10*, Seattle.
[2] Barnert, T., Kosmowski, K.T. & Śliwiński, M. (2010). A method for including the security aspects in the functional safety analysis of distributed control and protection systems. *ESREL, Rhodes, Greece.*
[3] 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.
[4] Goble, W. & Cheddie, H. (2005). *Safety instrumented systems verification: Practical probabilistic calculations*. ISA.
[5] Goslin, Ch. (2008). *Maritime and port security*. Duos Technologies, Inc., Jacksonville.
[6] Grøtan, T.O., Jaatun, M.G., Øien, K. & Onshus, T. (2007). *The SeSa Method for Assesing Secure Remote Access to Safety Instrumented Systems (SINTEF A1626).* Trondheim, Norway.
[7] Hildebrandt, P. (2000). *Critical aspects of safety, availability and communication in the control of*

MOST WIEDZY Downloaded from mostwiedzy.pl

*a subsea gas pipeline, Requirements and Solutions* HIMA.

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

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

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

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

[12] ISO 31000 (2009). *Risk management - Principles and guidelines*. International Organization for Standardization, Geneva.

[13] 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, Estoril.* Taylor & Francis Group, London.

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

[15] Schneider Electric (2014): *Pipeline Management Solution An Integrated Solution for Pipeline Operators*

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

[17] 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.

MOST WIEDZY Downloaded from mostwiedzy.pl

MOST WIEDZY Downloaded from mostwiedzy.pl