Śliwiński Marcin

Piesik Emilian
Gdańsk University of Technology , Gdansk, Poland

Functional safety with cybersecurity for the control and protection systems on example of the oil port infrastructure

Keywords

functional safety, cybersecurity, SIL, SAL, industrial control systems, oil port infrastructure

Abstract

Safety and cybersecurity aspects consist of two different group of functional requirements for the industrial control and protection systems in the oil port installation. It is the main reason why the analyses of safety and cybersecurity shouldn't be integrated directly. These article presented some important issues of the functional safety analysis with regard to cybersecurity aspects in the oil seaport infrastructure. The proposed approach will be composed of the following items: process and procedure based safety and cybersecurity management, integrated safety and cybersecurity assessment of industrial control system (ICS). The problem is illustrated on practical example of the part oil seaport installation. 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).

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 between the sensors, logic controllers and actuators.

Safety aspects is concerned with preventing accidents by identifying potential weaknesses, initiating events, internal hazards and potentially hazardous states and then identifying and applying appropriate mitigation solutions to reduce relevant risks to tolerable levels [1, 14]. Cybersecurity is concerned with protecting assets against internal and external threats and vulnerabilities that compromise the assets, environment and employees. Assets are protected using controls that reduce the risk to an acceptable level. The safety lifecycle is an engineering process that contains the steps needed to achieve high levels of functional safety during: conception, design, operation, testing and maintenance of SIS [10] a specially in the oil port installation. 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 example pumping oil and gas station in t oil port infrastructure. Simplified version of the safety lifecycle with regard to publications [4, 10] (*Figure 1*).

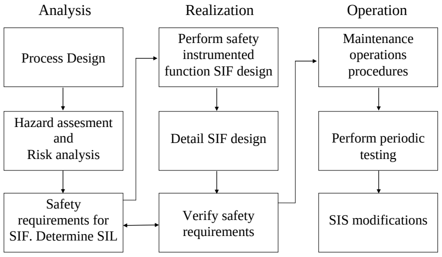
Analysis
Realization
Operation
Process Design
Perform safety instrumented function SIF design
Maintenance operations procedures
Hazard assesment and Risk analysis
Detail SIF design
Perform periodic testing
Safety requirements for SIF. Determine SIL
Verify safety requirements
SIS modifications

Figure. 1. Simplified diagram of functional safety lifecycle

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 system design phase comprises the activities to derive technical safety and security requirements out of the functional requirement and to define a corresponding architecture [10, 18] (*Figure 2*).

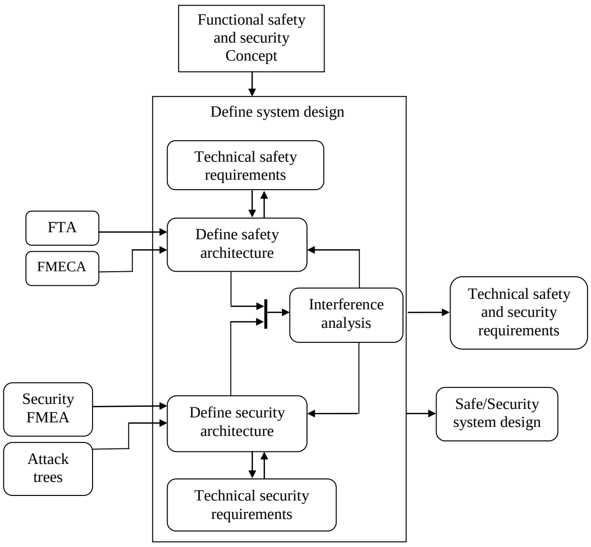
Functional safety and security Concept
Define system design
Technical safety requirements
FTA
FMECA
Define safety architecture
Interference analysis
Technical safety and security requirements
Security FMEA
Attack trees
Define security architecture
Safe/Security system design
Technical security requirements

Figure. 2. Safety and security activities of the system design phase [11, 18]

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 [10, 18].

2. Classification of data transfer type in the process control and protection systems

A conventional control and protection system consists of a programmable logic controller (PLC), sensors, actuators, a control station with supervisory control and data acquisition (SCADA) and a control station. Another important element of a control and protection system is the human operator who is supervising its operation. The system elements 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 [2, 3].

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:

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.

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. In such case, communication interfaces should be implemented according to the IEC 62280 standard on railway communication, signaling and processing system applications (safety-related communication in closed transmission systems) [2, 3, 9, 10].

3. The functional safety & cyber security requirements

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 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 safety-related functions

(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 probabilistic 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 outlined as follows:

- determine the tolerable risk based on 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.

Results of security analysis for given control and protection system can be divided into some general categories, for example a qualitative description with defined security levels like: low level, medium level or high 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*) [12].

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 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 (1) [11, 18]. 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 that they protect against.

Table 3. Security assurance levels SALs

Security assurance level (SAL)	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 concerning the control and protection systems. It is evaluated based on a defined vector of seven requirements for relevant security zone [11]:

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

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.

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 or SAL [16, 20].

Although the concepts concerning the safety and security of IT 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 [2]:

- 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.

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.

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).

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 [3, 20]. 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 sets, the probability of failure to perform the design function on demand can be evaluated based on following formula [1, 20]:

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

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:

$$PFD_{avg} = \frac{1}{T_I} \int_{0}^{T_I} PFD(t)dt \qquad (3)$$

where: T_I - proof test interval.

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

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

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

4. Case study

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. [17]. A conventional control and protection system consists of programmable logic controller (PLC), sensors, actuators, control station with supervisory control, data acquisition system (SCADA) for monitoring and control, and the control station [5, 6, 18]. Another important element is the human operator, who supervises the operation [9, 10]. The system's elements may be connected by different

internal and/or external communication channels (*Figure 3*).
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.

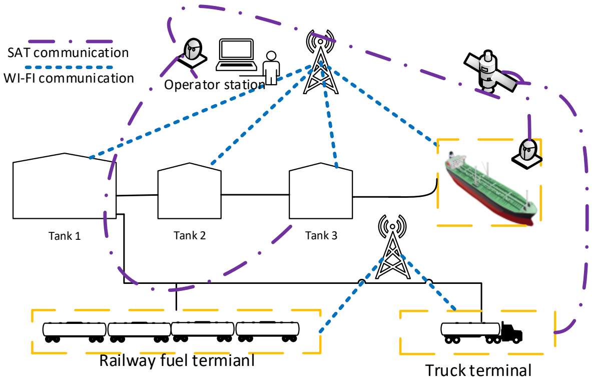

Figure 3. Data transfer in distributed industrial control systems for the oil pipeline infrastructure

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 fig. 3. 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 4*.

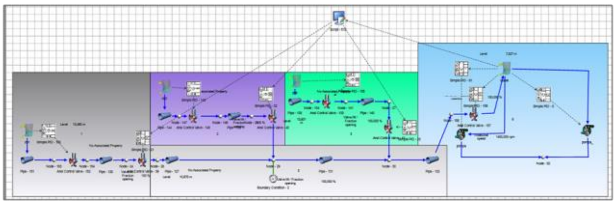

Figure 4. Flownex CFD model for the oil pipeline infrastructure

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 4* shows the potential corrections of SIL for low, medium and high level of safety-related (E/E/PE or SIS) system security.

Table 4. SIL that can be claimed for given EAL or SAL for distributed control and protection systems of category II and (III)

Determined			Verified SIL for systems of category II & (III)			
cyber security factor			functional safety			
EAL	SAL	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)

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 and SAL) 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 presented cases the SIL verification, integrated with security aspects, is necessary as shown in *Figure 5*.

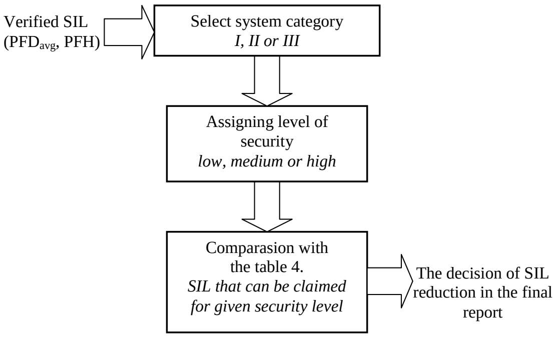
Verified SIL (PFD$_{avg}$, PFH)
Select system category *I, II or III*
Assigning level of security *low, medium or high*
Comparasion with the table 4. *SIL that can be claimed for given security level*
The decision of SIL reduction in the final report

Figure 5. 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 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:

$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgNet} + PFD_{avgPLC} + PFD_{avgA} \quad (5)$$

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.

The required SIL for entire distributed SIS systems 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 systems elements are presented in *Table 5*.

Table 5. Reliability data for elements SIS system

	FS	LS	PS	WiFi	SAT	Safety PLC	Stop SR	SVA
DC [%]	66	90	54	99	99	90	90	24
λ_{DU} [1/h]	$1.1\cdot10^{-6}$	$1.2\cdot10^{-6}$	$4\cdot10^{-7}$	$5\cdot10^{-7}$	$3\cdot10^{-7}$	$1.5\cdot10^{-7}$	$1\cdot10^{-6}$	$9\cdot10^{-7}$
T_I [h]	8760	8760	8760	8760	8760	8760	8760	8760
β	0.02	0.02	0.02	0.01	0.01	0.01	0.02	0.02

From the risk assessment the safety integrity level for first safety function *"overpressure protection oil pipeline in oil seaport 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 I (*Figure 6*).

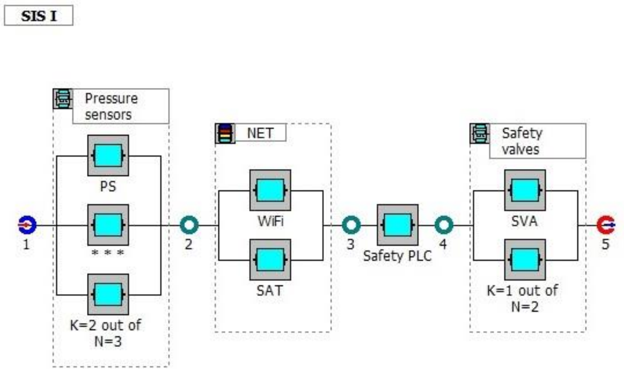

Figure 6. SIS I - overpressure pipeline safety instrumented system in the oil critical installation (RBD model)

Table 6. The SIL verification report for SIS I

System /subsystems/ elements		**koon**	**β [%]**	**PFD$_{avg}$**	**SIL**
SIS I	**0**	**-**	**-**	**$8.33\cdot10^{-4}$**	**3**
S	**.1**	**2oo3**	**3**	**$6.18\cdot10^{-5}$**	**4**
PS	..2	-	-	$1.75\cdot10^{-3}$	2
PS	..2	-	-	$1.75\cdot10^{-3}$	2
PS	..2	-	-	$1.75\cdot10^{-3}$	2
NET	**.1**	**1oo2**	**1**	**$1.987\cdot10^{-5}$**	**4**
WiFi	..2	-	-	$2.19\cdot10^{-3}$	2
SAT	..2	-	-	$1.314\cdot10^{-3}$	2
PLC	**.1**	**1oo1**	**-**	**$6.57\cdot10^{-4}$**	**3**
Safety PLC	..2	-	-	$6.57\cdot10^{-4}$	3
A	**.1**	**1oo2**	**2**	**$9.44\cdot10^{-5}$**	**4**
SVA	..2	-	-	$3.942\cdot10^{-3}$	2
SVA	..2	-	-	$3.942\cdot10^{-3}$	2

Assessment of the result obtained shows that for the SIS structure on *Figure 6* is:

$$\begin{aligned} & PFD_{avgSIS(I)} \cong PFD_{avgPS(2oo3)} + PFD_{avgNET(1oo2)} + PFD_{avgPLC} + \\ & + PFD_{avgSVA(1oo2)} \cong 6.18\cdot10^{-5} + 1.987\cdot10^{-5} + \\ & + 6.57\cdot10^{-4} + 9.44\cdot10^{-5} \cong 8.33\cdot10^{-4} \Rightarrow SIL3 \end{aligned}$$

Thus, the PFD$_{avg}$ is equal $8.33\cdot10^{-4}$ 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. Safety integrity level SIL3 for III category systems in those case required high level of security (see Table 4 - EAL ≥ 5 or SAL ≥ 3).
From the risk assessment the safety integrity level for safety function *"overfill prevention in the oil seaport*

critical installation" (fuel tank) was determined as SIL3. Safety function (overfill prevention) is implemented in distributed safety instrumented system SIS II (*Figure 7*).

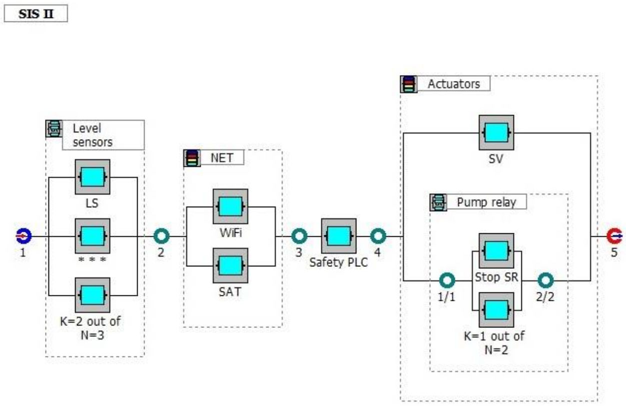

Figure 7. SIS II - fuel tank overfill prevention in the oil seaport critical installation (RBD model)

Table 7. The SIL verification report for SIS II

System /subsystems/ elements		koon	β [%]	PFD$_{avg}$	SIL
SIS II	**0**	**-**	**-**	**$9.3\cdot10^{-4}$**	**3**
S	**.1**	**2oo3**	**3**	**$2.4\cdot10^{-4}$**	**3**
LS	..2	-	-	$5.256\cdot10^{-3}$	2
LS	..2	-	-	$5.256\cdot10^{-3}$	2
LS	..2	-	-	$5.256\cdot10^{-3}$	2
NET	**.1**	**1oo2**	**1**	**$1.987\cdot10^{-5}$**	**4**
WiFi	..2	-	-	$2.19\cdot10^{-3}$	2
SAT	..2	-	-	$1.314\cdot10^{-3}$	2
PLC	**.1**	**1oo1**	**-**	**$6.57\cdot10^{-4}$**	**3**
Safety PLC	..2	-	-	$6.57\cdot10^{-4}$	3
A	**.1**	**1oo2**	**2**	**$1.34\cdot10^{-5}$**	**4**
SV	***..2***	***1oo1***	**-**	***$3.942\cdot10^{-3}$***	***2***
SVA	..3	-	-	$3.942\cdot10^{-3}$	2
Pump relay	***..2***	***1oo2***	***2***	***$1.07\cdot10^{-4}$***	***3***
SR	..3	-	-	$4.38\cdot10^{-3}$	2
SR	..3	-	-	$4.38\cdot10^{-3}$	2

Assessment of the result obtained shows that for the SIS structure on *Figure 7* is:

$$PFD_{avgSIS(II)} \cong PFD_{avgLS(2oo3)} + PFD_{avgNET(1oo2)} + PFD_{avgPLC} + \\ + PFD_{avgA(1oo2)} \cong 2.4\cdot10^{-4} + 1.987\cdot10^{-5} + \\ + 6.57\cdot10^{-4} + 1.34\cdot10^{-4} \cong 9.3\cdot10^{-4} \Rightarrow SIL3$$

From the risk assessment the safety integrity level for first safety function *under pressure protection oil pipeline (leak)* was determined as SIL3. Safety function (under pressure - fuel oil pipeline leak) is implemented in distributed safety instrumented system SIS III (*Figure 8*).

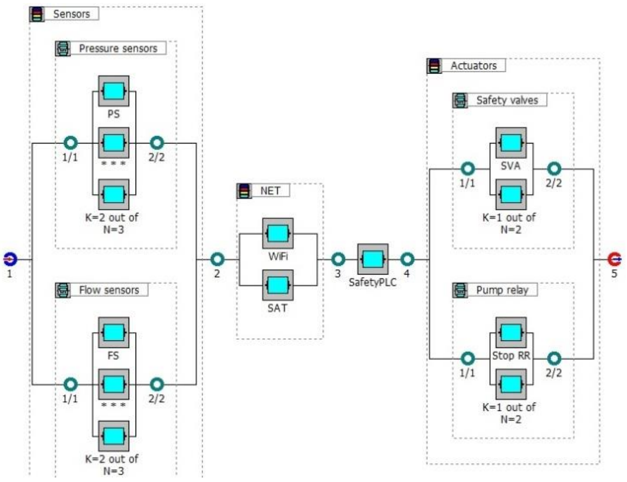

Figure 8. SIS III - fuel tank under pressure oil pipeline leak prevention (RBD model)

Table 8. The SIL verification report for SIS III

System /subsystems/ elements		koon	β [%]	PFD$_{avg}$	SIL
SIS III	**0**	**-**	**-**	**$9.55\cdot10^{-4}$**	**3**
S	**.1**	**2oo2**	**-**	**$2.76\cdot10^{-4}$**	**3**
PS	..2	**2oo3**	**3**	**$6.18\cdot10^{-5}$**	**4**
PS	...3	-	-	$1.75\cdot10^{-3}$	2
PS	...3	-	-	$1.75\cdot10^{-3}$	2
PS	...3	-	-	$1.75\cdot10^{-3}$	2
FS	..2	**2oo3**	**3**	**$2.14\cdot10^{-4}$**	**3**
FS	...3	-	-	$4.82\cdot10^{-3}$	2
FS	...3	-	-	$4.82\cdot10^{-3}$	2
FS	...3	-	-	$4.82\cdot10^{-3}$	2
NET	**.1**	**1oo2**	**1**	**$1.987\cdot10^{-5}$**	**4**
WiFi	..2	-	-	$2.19\cdot10^{-3}$	2
SAT	..2	-	-	$1.314\cdot10^{-3}$	2
PLC	**.1**	**1oo1**	**-**	**$6.57\cdot10^{-4}$**	**3**
Safety PLC	..2	-	-	$6.57\cdot10^{-4}$	3
A	**.1**	**1oo2**	**2**	**$2.02\cdot10^{-6}$**	**b**
SV	***..2***	***1oo2***	***2***	***$9.44\cdot10^{-5}$***	***4***
SVA	..3	-	-	$3.942\cdot10^{-3}$	2
SVA	..3	-	-	$3.942\cdot10^{-3}$	2
Pump relay	***..2***	***1oo2***	***2***	***$1.07\cdot10^{-4}$***	***3***
SR	..3	-	-	$4.38\cdot10^{-3}$	2
SR	..3	-	-	$4.38\cdot10^{-3}$	2

Assessment of the result obtained shows that for the SIS structure on *Figure 8* is:

$$PFD_{avgSIS(II)} \cong PFD_{avgLS(2oo3)} + PFD_{avgNET(1oo2)} + PFD_{avgPLC} + \\ + PFD_{avgA(1oo2)} \cong 2.76\cdot10^{-4} + 1.987\cdot10^{-5} + \\ + 6.57\cdot10^{-4} + 2.02\cdot10^{-6} \cong 9.55\cdot10^{-4} \Rightarrow SIL3$$

Human – operator is the part of the system in oil seaport installation. Diagnosis, decision and operator action can take an important impact in normal use of installation. Especially at abnormal or critical situation human –operator takes responsibility of systems. At oil seaport operator with alarm system are one of the main protection layers. The efficiency of the system depends on the operator's faults. A large percentage of technical problems occurring in oil port infrastructure are related to operator's errors and performance shaping factors (PSF). Therefore, the human PSF should be properly shaped via e.g training and procedures. Nowadays there is a problem how to calculate the human error probability and reduce the risk of the human errors to guarantee the required safety level. That problem can take the main part of the research in the future.

5. Summary

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 ISO/IEC 15408 an IEC 62443.

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] 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.

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

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

[15] Missala, T. (2010). *Book of procedures for functional safety compliance evaluation of*

protection systems in the process industry. Report no. 8795, PIAP, Warsaw.

[16] 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.

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

[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., 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.