Kosmowski Kazimierz T.

Śliwiński Marcin

Piesik Emilian
Gdańsk University of Technology, Gdansk, Poland

Gołębiewski Dariusz
PZU Group, Warsaw, Poland

Procedure based proactive functional safety management for the risk mitigation of hazardous events in the oil port installations including insurance aspects

Keywords

functional safety, security, industrial control systems, oil port installations, risk evaluation, insurance

Abstract

This article addresses selected 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 overall safety requirements and definition of *safety functions*. Based on risk assessment results the *safety integrity level* (SIL) is determined for consecutive safety functions. These functions are implemented within *industrial control system* (ICS) that consists of the *basic process control system* (BPCS) and/or *safety instrumented system* (SIS). Determination of required SIL related to required risk mitigation is based on semi-quantitative evaluation method. Verification of SIL for considered architectures of BPCS and/or SIS is supported by probabilistic models with appropriate data and model parameters including security-related aspects. The approach proposed is illustrated on example of oil port installations. In final part of the article the insurance aspects are discussed in managing risks, as some risks are to be transferred to an insurance company.

1. Introduction

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. Some more important safety functions, reducing substantially relevant risks, require implementing of protection layers, according to a concept of *defence in depth* (DinD).

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.

Security related analyses of the ICS during its design and operation as *distributed computer system* (DCS) with relevant SCADA (*supervisory control and data acquisition*) functions are very important in hazardous plants and oil ports, especially when they

are considered within *critical infrastructure* (CI). In final part of the article the insurance aspects are discussed in managing risks, as some risks should be transferred to the insurance company.

2. Process and procedure based integrated management

2.1. Process based integrated management

A process based integrated management system enhances traditional quality management, and, when properly implemented, enables the organization to satisfy external requirements for certification of the management systems of interest.

The process based approach proposed can be compatible with implemented in practice the *quality, environment and safety at work* (QES) *management systems* developed according to requirements of known series of standards, respectively: ISO 9000, ISO 14000 and OHSAS 18000.

The IAEA publication [11] suggests the implementation of a *process based management system* may involve either the creation of a new system in interested countries or organizations or transition from a mature *quality assurance/quality control/quality management* (QA/QC/QM) system to a process based management system. Below an integrated management system is proposed that includes also the security aspects, i.e. the *quality, environment, safety and security* (QESS) *management system* (MS).

Existing processes in industrial plants, both *business and operational*, may be grouped into *executive, core and support processes* [11]. The problem is how to identify the core processes, e.g. processes that have the greatest impact on performance (safety, security, health, environment, quality, cost, business and innovation). This requires indicating critical outputs of the organization and processes that deliver these outputs. The *management processes* shape and manage the core and support processes distinguished in given organization.

The issue will be illustrated on several distinguished processes and procedures that support integrated QESS management on example of the *functional safety and security management* in life cycle including the implementation and operation of the *industrial control systems* (ICS) to mitigate relevant risks of potential hazardous events.

These systems are designed as the *electrical, electronic and programmable electronic systems* (E/E/PES) regarding IEC 61508 [12] and/or *the safety instrumented systems* (SIS) taking into account requirements of IEC 61511 [13]. Requirements concerning security related aspects will be specified regarding requirements specified in series of international standards IEC 62443 [14], ISO/IEC 27000 series: *Information technology - Information security management systems*, and ISO 31000 [16] on *Risk management - Principles and guidelines*.

The ICS play an important role in the oil port installations [8], [27] and pipelines of external distributed installations [9]-[10], [21], [25]. In distributed computer network the quality of software of the *Supervisory Control And Data Acquisition* (SCADA) system is of special interest as regards functionality, safety and security [1]-[3]. In evaluation of the *human-system interface* (HSI) and the *alarm system* (AS) of ICS/SCADA system the EEMUA requirements concerning *human factors* (HF) and *human reliability analysis* (HRA) are taken into account based on results of current research [18], [22].

The risk analysis and assessment methods undertaken using the QESS related models, applied to the oil port installations and their protection systems that mitigate relevant risks, are compatible with known methodologies of HAZOP (*hazard and operability*), LOPA (*layer of protection analysis*) and SVA (*security vulnerability analysis*) [4]. Principles and requirements concerning the risk management proposed in international standard ISO 31000 [16] have been also taken into account.

Process classes and particular processes considered include*:*

Executive Processes (EP)
- *EP-1 Manage the entire business,*
- *EP-2 Manage the processes and procedures,*
- *EP-3 Assess and improve performance,*
- *EP-4 Manage external relationships, etc.,*

Core Processes (CP)
- *CP-1 Control and monitor equipment,*
- *CP-2 Control emissions and effluents,*
- *CP-3 Plan and schedule services, tests and maintenance,*
- *CP-4 Manage functional safety and reliability of the control and protection systems,*
- *CP-5 Manage security of site,*
- *CP-6 Manage vulnerability and security of computer network, and*

Support Processes (SP)
- *SP-1 Provide human resources and training,*
- *SP-2 Provide personnel safety services,*
- *SP-3 Provide IT services,*
- *SP-4 Provide environmental services,*
- *SP-5 Provide emergency preparedness services, etc.*

2.2. Example of procedure based functional safety management including insurance

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 is shown in *Figure 1*.

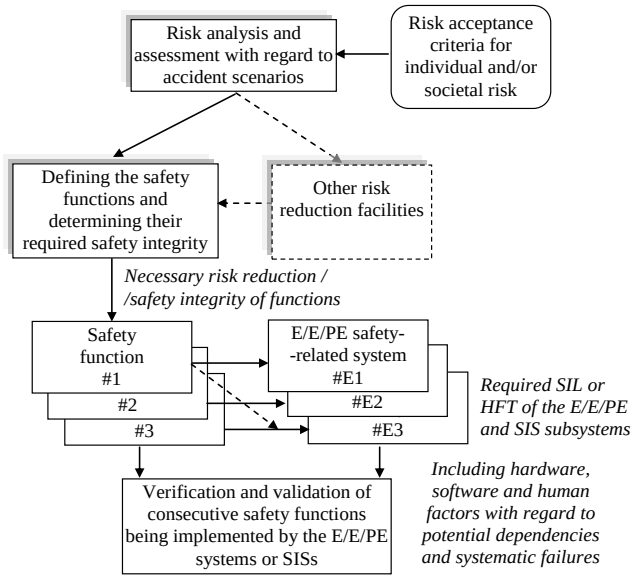

Figure 1. Allocation of requirements to the E/E/PE safety-related systems

Below an approach is proposed for integrated determining the *safety integrity level* (SIL) and the *security assurance level* (SAL) for consecutive safety functions mitigating relevant risks. The analyses and assessments are based on 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 information supporting the insurance related decision making is presented according to existing practice in an insurance company.

First idea, known to authors of this article, to draw up a book of procedures for functional safety compliance evaluation of protection systems in the process industry was proposed by Missala in 2010. The number of 23 preliminary procedures has been proposed by Missala [20].

Below a modified approach is outlined that distinguishes two categories of procedures. About 20 procedures have been preliminary specified. Examples of *procedures* (PR) related to the process *CP-4* specified above 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.

Procedures to be drawn up for the purpose of evaluation of insurance variants of hazardous plants are proposed as follows [6]-[7]:

PR INS-01 Requirements for overall description of the port installations, environment, infrastructure, hazards and threats, organizational culture;

PR INS-02 Requirements for insurance audit and model based evaluation of risks for underwriting and indicating solutions of technical and organizational improvements to mitigate relevant risks.

3. Safety and security of ICS in oil port installations

Safety 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 [4], [18].

Security 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 [16], [26].

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 *safety instrumented systems* [13].

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. Simplified version of the safety lifecycle with regard to publications [5], [13], is shown in *Figure 2.*

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 (see *Figure 3*) comprises the activities to derive technical safety and security requirements out of the functional requirement and to define a corresponding architecture [9], [24].

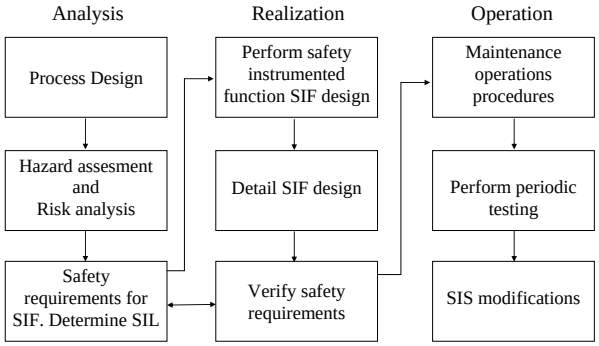

Figure 2. Simplified diagram of functional safety lifecycle

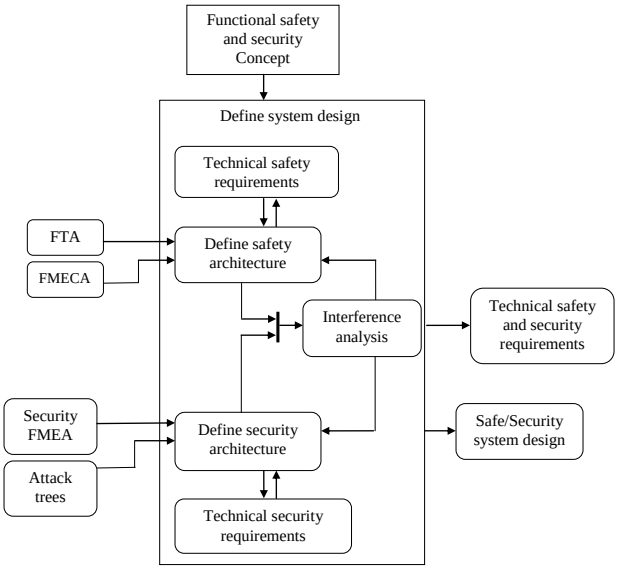

Figure 3. Safety and security activities of the system design phase

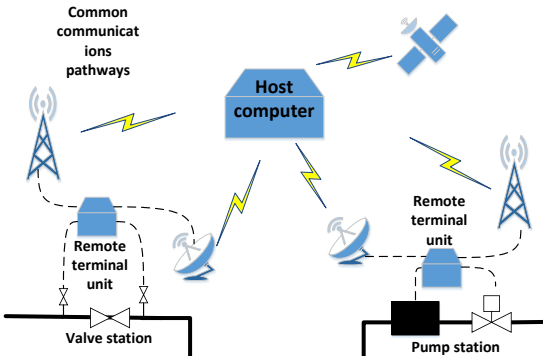

Figure 4. Data transfer in distributed industrial control systems for the oil pipeline infrastructure [21]

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) [24]. A SIS management system should include the aspects specific to safety instrumented systems [13], [24].

*Supervisory control and data acquisition (*SCADA) 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 location (see *Figure 4*) [10], [21].

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. [25].

4. Security aspects and functional safety control system of the oil port pipelines

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 [10], [25]-[26]. Another important element is the human operator, who supervises the operation [22]. The system's elements may be connected by different internal and/or external communication channels (*Figure 5*).

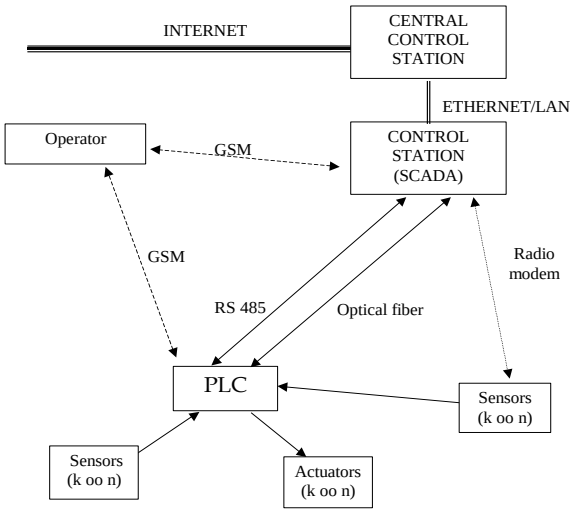

Figure 5. Distributed control and protection system consisting of different industrial communication networks

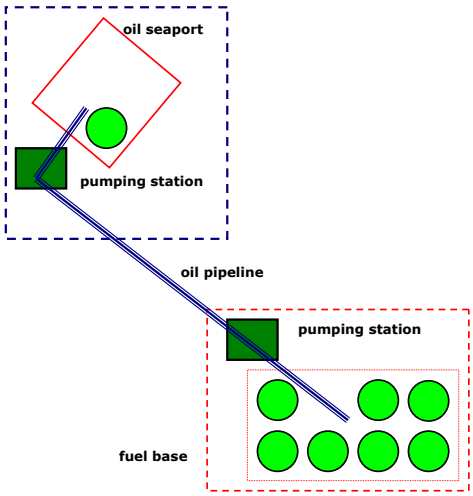

Figure 6. Example of oil seaport installations with critical infrastructure

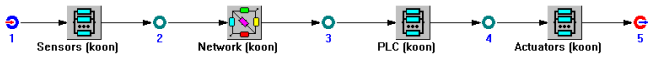

Figure 7. Reliability block diagram of E/E/PE safety-related system operating in network

The information sending and receiving between PLC and the control station can be transferred by standard series or parallel communication protocols or other methods of communication, such as wireless GSM/GPRS.

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 [1]-[3], [17], [26]:

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 (*Figure 6*).

In second edition of standards IEC 61511:2015 [13] and IEC 61508:2010 [12] some additional requirements concerning the data communication channels in functional safety solutions are specified. The standard [12] distinguishes two main types of communication channels, namely *white* channel or *black* one. A *white* one means that the entire communications channel is designed, implemented and validated according to IEC 61508 requirements. The *black* one means that some parts of communication channel are not designed, implemented and validated according to IEC 61508.

The control or protection system that doesn't operate in a complex industrial network, may be modeled probabilistically using conventional methods, e.g. a method of reliability block diagrams (RBD), the Markov Graph method or a method based on minimal sets of paths or cuts.

In conventional approach the probabilistic model of given complex protection system (E/E/PE or SIS) is being developed on the basis of models for subsystems: the *sensors* (S), *programmable logic controllers* (PLC) and *actuators* (A). *Figure 7* illustrates the RBD of distributed E/E/PE safety-related system within a simple network [4], [26].

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

For the configuration of protection system shown in *Figure 7* 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.

Safety function (overpressure protection pipeline in the oil seaport) is implemented in distributed safety instrumented system (see *Figure 8*).

In the *Figure 9* is presented architecture communication module for distributed SIS system.

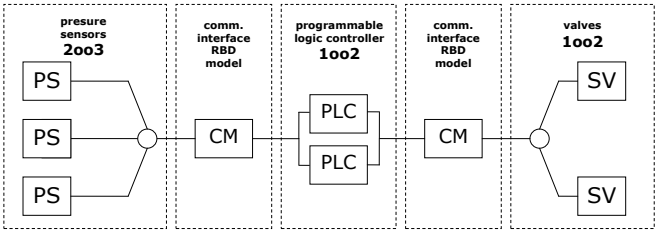

Figure 8. Overpressure pipeline protection SIS system (seaport - oil pipeline - fuel base) with industrial communication network

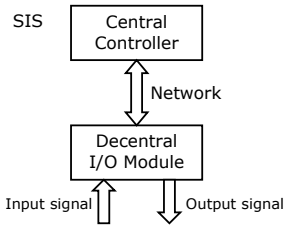

Figure 9. Internal network between the central controller and I/O modules in the SIS system

The required SIL for entire distributed E/E/PE or SIS system is determined in a process of risk analysis and evaluation [18].

Table 1. Reliability data for elements SIS system

	PS	CM	PLC	SV
DC [%]	54	90	66	24
λ_{DU} [1/h]	$3 \cdot 10^{-7}$	$1 \cdot 10^{-7}$	$5 \cdot 10^{-6}$	$8 \cdot 10^{-7}$
T_I [h]	8760	4380	8760	8760
β	0.02	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 date for SIS elements are presented in *Table 1*.
For given system a proper architecture is considered to meet the SIL requirement for entire system. The communication channel is created by serial link of relevant subsystems. Therefore, its reliable operation is dependent on correct functioning of each subsystem. Assessment of the result obtained shows that for the SIS structure in *Figure 8* is:

$$PFD_{avgSIS} \cong PFD_{avgPS(2oo3)} + PFD_{avgCM} + PFD_{avgPLC(1oo2)} + PFD_{avgSV(1oo2)}$$
$$\cong 3.11 \cdot 10^{-5} + 2.19 \cdot 10^{-4} + 6 \cdot 10^{-4} + 7.14 \cdot 10^{-5} \cong 9.215 \cdot 10^{-4}$$

Thus, the PFD_{avg} is equal $9{,}215 \cdot 10^{-4}$ 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 [19], [26].

5. Integrated safety and security analysis in industrial computer network

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 [3].
A security analysis concept was proposed in the standard ISO/IEC 15408 [15]. Security is considered with the protection from threats, where threats are categorized as the potential for abuse of assets. Some categories of threats are considered. In the domain of security usually greater attention is given to those threats that are related to malicious or other human intentional activities.
The *Evaluation Assurance Level* (EAL) denotes a package of assurance requirements, which covers the complete development of a product with a given level of strictness. *Common Criteria* (CC) lists seven levels, with EAL1 being the most basic (cheapest to evaluate and implement) and EAL7 being the most strict (most expensive). Higher EAL levels do not necessarily imply better security, they only mean that the claimed security assurance of the target of evaluation (TOE) 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 [17] (see *Table 2*).

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 [14]. 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.
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:

$$SAL = \{AC \quad UC \quad DI \quad DC \quad RDF \quad TRE \quad RA\} \tag{2}$$

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 [9]. 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 [3].
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 [12]-[13]. Using the SeSa rings related to security protection is another approach useful for the integration of functional safety and security aspects (*Figure 10*).

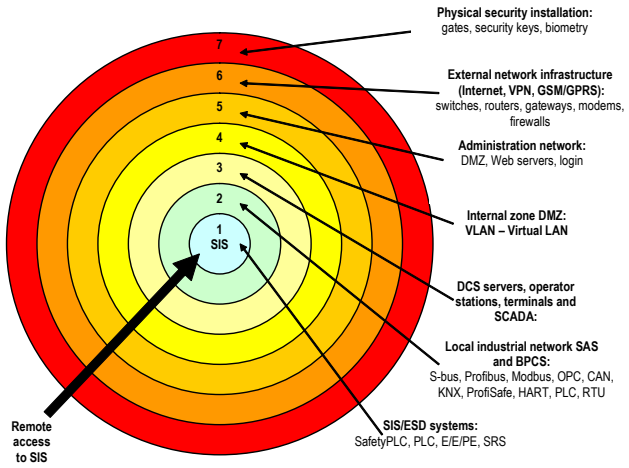

Figure 10. Rings of the protection in SIS system [3], [26]

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 (see *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.

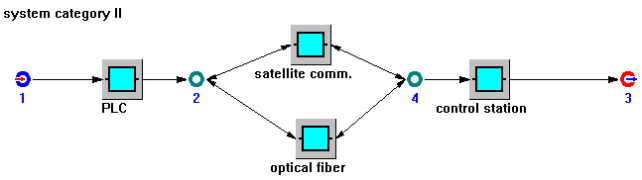

Figure 11. An oil port critical infrastructure pipeline control and protection system of category II

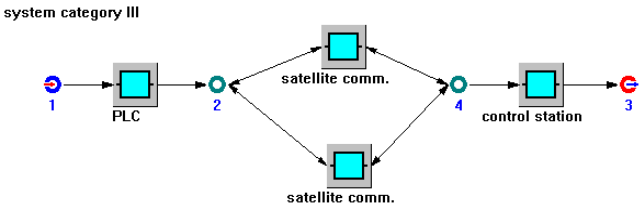

Figure 12. A pipeline control and protection system of III category with redundant external communication channels

Figure 11 presents an example of the system of second category. It uses internal optical fiber and external satellite communication for sending and receiving data between safety PLC and the control station of an oil pipeline.

Second example (*Figure 12*) presents system of third category with redundant 1oo2 external satellite communication channels between PLC and control station.

Another example of the control and protection system in oil port is shown in *Figure 13*. In this example a SIF was defined related to control and reduce potential overpressure for hazardous scenario considered. Having a required SIL for this safety-related function, a proper architecture of SIS can be designed.

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 1*5.

After this analysis, the proposed architecture has to be verified, i.e. checked if it fulfills specified requirements. The process of SIL verification, similarly like SIL determination, usually doesn't include in industrial practice the security aspects.

But when SIS uses some communication channels this problem should be taken into account. Such SIS system is presented in *Figure 14*. In such case there is a challenge to include security aspects in designing and verifying SIL of the programmable control and protection system operating in a network that implements given safety function.

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 [14] based approach, indented to describe in an integrated way the system security in relation to functional safety concept [12]-[13].

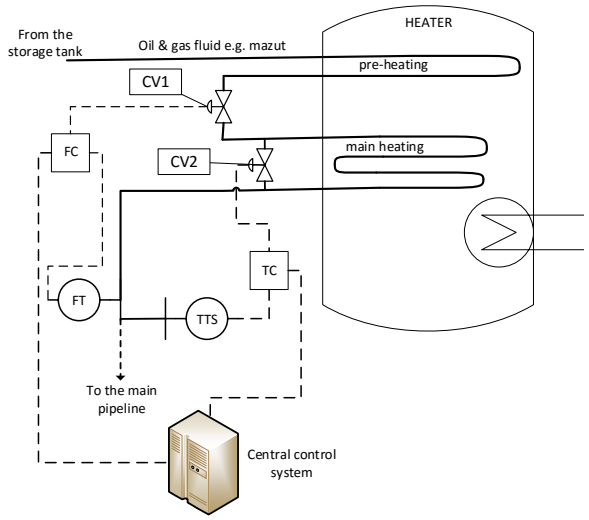

Figure. 13. An example of the control and protection system for reducing potential overpressure

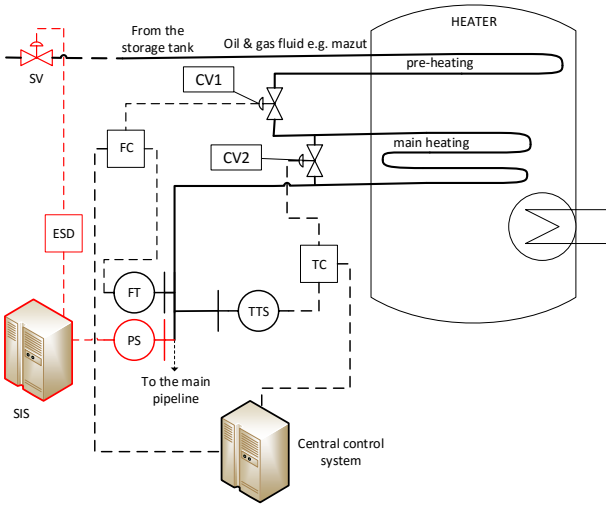

Figure. 14. An example of the control and protection system with communication channels

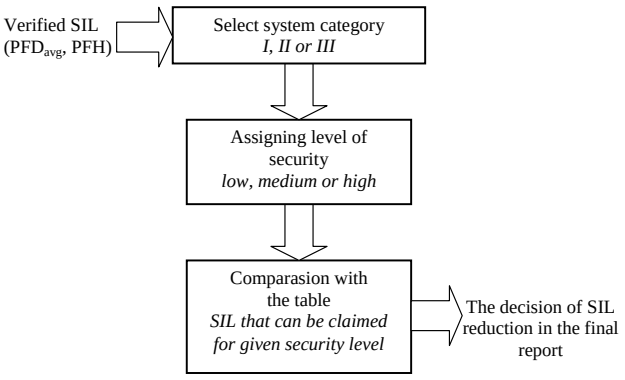

Figure 15. Procedure of the safety integrity level verification including the security aspects [3], [26]

6. Risk management and insurance

Some risks evaluated in the risk management process of given hazardous plant or seaport cannot be sufficiently reduced using technical and organisational solutions, and should be transferred to an insurance company [6]-[7].

Insurance related procedures provide methods for financial control in process of risk management whereby risk of loss is transferred to another party through a contract risk bearer. A proactive approach to the risk mitigation efforts can reduce insurer' uncertainty and make business more attractive.

The insurance companies pay more attention to create integrated methods of risk analysis and take into account comprehensive factors of the company activities. Insurers are more willing to base their decisions on the expertise provided by the experts called the *risk engineers.*

The *risk engineers* provide a comprehensive approach to risk management helping to protect business against threats rather than simply insuring against it. They begin with risk identification and then grade these exposures to create a strategic *risk-management plan*. The risk engineers are then able to suggest improvements based on in-depth industry knowledge and risk insight to help creating an *effective loss-prevention strategy*.

The scope of interest of risk analysis depends on insurer liability. The specific of oil seaports require advanced and integrated approach to the process. The achievement and demonstration of safety of operations in installations of oil seaports generate a number of unique problems not normally found in similar land based industry.

The oil ports are the interface between the bulk transportation of large quantities of hazardous substances in ships and the land based industries they serve. These hazardous substances are carried in sufficient quantities in ships to create a major hazard from fire, explosion and toxic effects. The industries served by the ships, for reasons of convenience and economy, often have large processing and storage facilities adjacent to the berths or waterways used by the ships. The use of consequence analysis to achieve this is described with reference to particular hazards in ports and the problems of applying these techniques for the marine environment.

An important part in the oil ports infrastructure analysis is safety related system and the level of certainty that the required safe response or action will take place when it is needed. This is normally determined as the likelihood that the safety loop will fail to act. Engineers during an *insurance survey* gather both quantitative or qualitative data and risk factors. The insurer released reports are a way to document the plant being considered using a systematic approach to identify and evaluate the effects of undesirable events and component failures to determine what could reduce or eliminate the chance for failures. Then, more probable events and their consequences are to be evaluated [6]-[7].

7. Summary

Selected 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 have been described. The procedure for functional safety management includes the hazard identification, risk analysis and assessment, specification of safety requirements and definition of *safety functions*. Based on risk assessment results the *safety integrity level* (SIL) is determined for consecutive safety functions.

These functions are implemented within *industrial control system* (ICS) that consists of the *basic process control system* (BPCS) and/or *safety instrumented system* (SIS). Determination of required SIL related to the risk mitigation is based on semi-quantitative evaluation method. 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. The approach proposed is illustrated on example of oil port installations.

The purpose is to make rational decisions concerning critical oil seaport installations including safety and security-related from the conceptual design stage. Then, relevant decisions are to be undertaken during plant operation in the frame of integrated security and safety management system. Thus, developing the *integrated management system* (IMS) is proposed that includes the *quality, environment, safety and security* (QESS) aspects.

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). 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). .

In this context the insurance aspects are discussed in managing risks, as some risks are transferred to an insurance company. The insurance companies pay more attention to create integrated methods of risk analysis and take into account comprehensive factors of the company activities.

Additional research effort should be undertaken to develop next generation of more compatible and

preferably integrated functional safety and security analysis methods and models based on a set of processes and procedures developed according to current quality management requirements including an interface between more formal risk evaluation methods and those used in insurance companies.

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. *Proc. 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] CCPS (2008). *Guidelines for Hazard Evaluation Procedures.* New York: Center for Chemical Process Safety. Wiley-Interscience, A John Wiley & Sons, Hoboken.

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

[6] Gołębiewski, D. & Kosmowski, K.T. (2005). Risk analysis for insurance of technical systems. *ESREL, Advances in Safety and Reliability* (ed. Kołowrocki), A.A. Balkema Publishers, Taylor & Francis Group, London, 683-687.

[7] Gołębiewski, D. (2010). *Insurance Audit, Practical methods of risk analysis* (*in Polish*). Poltext Publishers, Warsaw.

[8] Goslin, Ch. (2008). *Maritime and port security*. Duos Technologies, Inc., Jacksonville.

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

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

[11] IAEA (2015). *Development and implementation of a process based management system*. Nuclear Energy Series Report NG-T-1.3. International Atomic Energy Agency, Vienna.

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

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

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

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

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

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

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

[19] Mahan, R. E., et al. (2011). *Secure Data Transfer Guidance for Industrial Control and SCADA Systems*. PNNL-20776, Pacific Northwest National Laboratory, Richland.

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

[21] Muhlbauer, K. (2004). *Pipeline Risk Management Manual Ideas, Techniques, and Resources*, Third edition, Elsevier.

[22] Piesik, E. & Śliwiński, M. (2015). Human reliability analysis with the alarm management aspects *(in Polish), The Scientific Papers of Faculty Electrical and Control Engineering.* Gdańsk University of Technology Publishers, 47, 143-146.

[23] Piwowar, J., Chatelet, E. & Laclemence, P. (2009). *An efficient process to reduce infrastructure vulnerabilities facing malevolence*, Reliability Elsevier, Engineering and System Safety 94, 1869–1877.

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

[25] Spouge, J. (1999). *A Guide to quantitative risk assessment for offshore installations*, DNV Technica.

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

[27] UN (2006). *Maritime security: elements of an analytical framework for compliance measurement and risk assessment.* United Nations, New York and Geneva.