Advances in Reliability, Safety and Security, Part 8 – Kołowrocki, Magryta-Mut (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-20-3 (printed), ISBN 978-83-68136-07-4 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Integrated Approach For Functional Safety And Cyber Security Analysis

Tomasz Barnert[a], Emilian Piesik[b], Jan Piesik[c], Marcin Śliwiński[b]

[a]*EKO-KONSULT,, Gdańsk, Poland*
[b]*Gdańsk Univeristy of Technology, Gdańsk, Poland*
[c]*Michelin Poland, Olsztyn, Poland*

Abstract

The paper is devoted to some important issues of the functional safety analysis, in particular the safety integrity level (SIL) verification process. It is related to the safety instrumented functions to be implemented within the distributed control and protection systems with regard to security aspects. A method based on quantitative and qualitative information is proposed for the SIL (IEC 61508:2010; 61511, 2015) verification with regard of the evaluation assurance levels (EAL) the security assurance levels (SAL) (IEC 62443, 2013), and the number of protection rings described in the Secure Safety (SeSa-SINTEF) methodology. The proposed approach will be composed of the following items: process and procedure-based safety and security management, integrated safety and security assessment of industrial control system (ICS) of the critical infrastructure.

Keywords: safety integrity level, SIL, safety instrumented system, SIS, industrial control system, functonal safety, cyber security

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 (IEC 61508, 2010; 61511, 2015). These functions are implemented in basic process control system (BPCS) and/or safety instrumented system (SIS), within industrial network system that consists of the wireless connection and wire connection. Determination of required SIL related to the risk mitigation is based on semi-quantitative evaluation method (Hildebrandt, 2010; IEC 61508, 2010; 61511, 2015). 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 (Barnert et al., 2010; 61511, 2015). Proposed approach based on functional safety aspects that are well known in process industries and cyber security methodology (IEC 62443, 2013; SESAMO, 2014). Main problem of these topic is influence cybersecurity aspects on functional safety analysis. Current topic that requires further research includes the interface between safety and cybersecurity. The article discusses these issues on example of knowledge based proactive functional safety and cybersecurity management system.

2. Functional safety and cyber security of industrial control systems

Functional 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 (Kosmowski et al. 2006; Kosmowski, 2013; Piesik et al., 2016). 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. 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 (61511, 2015). 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 industry infrastructure. Simplified version of the safety lifecycle with regard to publications (Goble, Cheddie, 2005; 61511, 2015) (see Figure 1).

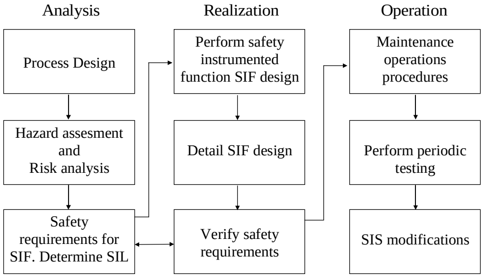
Analysis
Realization
Operation
Process Design
Hazard assesment and Risk analysis
Safety requirements for SIF. Determine SIL
Perform safety instrumented function SIF design
Detail SIF design
Verify safety requirements
Maintenance operations procedures
Perform periodic testing
SIS modifications

Fig. 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, 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 (61511, 2015; SESAMO, 2014) (Fig. 2).

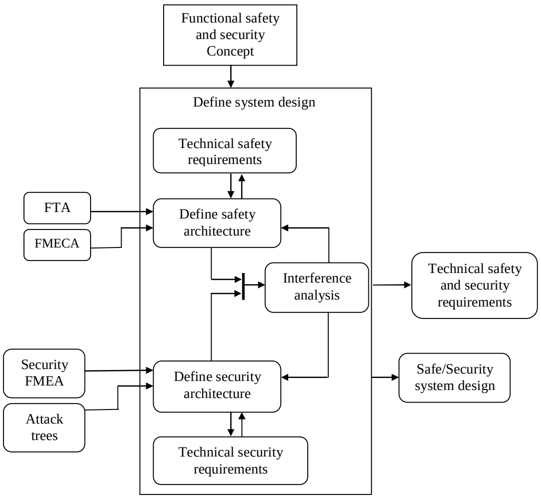
Functional safety and security Concept
Define system design
Technical safety requirements
FTA
FMECA
Define safety architecture
Interference analysis
Technical safety and security requirements
Security FMEA
Attack trees
Define security architecture
Safe/Security system design
Technical security requirements

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

The safety and security goals are now the input to derive functional safety and cybersecurity 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.

Supervisory control and data acquisition (SCADA) refers to the transmission of pipeline control parameters (such as pressures, flows, temperatures, and product compositions) at sufficient points along the pipeline to allow monitoring of the line from a single location (Figure 3) (Hildebrandt, 2000).

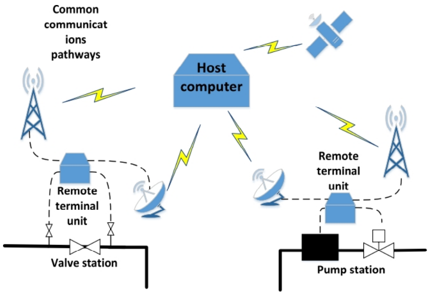

Fig. 3. Data transfer in distributed industrial control systems for an example pipeline infrastructure.

In many cases, it also includes the transmission of data from the central monitoring location e.g. control station distributed oil and gas infrastructure e.g. pipelines and tanks, along the line to allow for remote operation of valves, pumps, motors, etc.

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

Although the concepts concerning the safety and security of information technology (IT) infrastructure are generally outlined in standards, respectively, additional research effort should be undertaken to develop integrated, system-oriented approach. Following problems require special attention (Barnert et al., 2010):

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

As was mentioned earlier, the result of security analysis is dependent on identified vulnerabilities and designed countermeasures. Both those factors are responsible for final level of security taken into account in the functional safety risk assessment process, a general procedure is presented (Figure 4). 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.

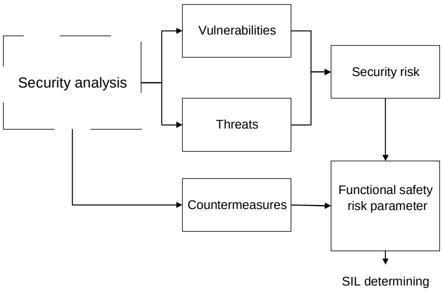

Fig. 4. Procedure using security factors in functional safety analysis (Barnert, Śliwiński, 2013).

This method is very useful, but special care should be taken into account during applying the method. A general scheme of consideration the security analysis results is presented (Figure 5). 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.

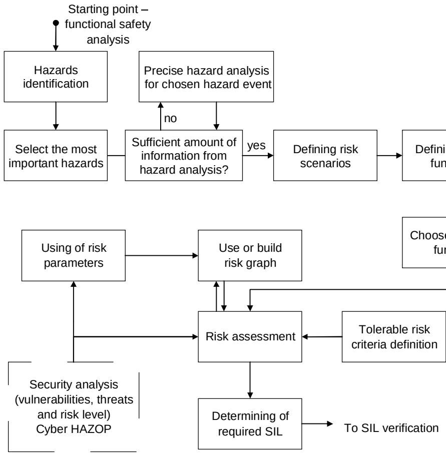
Starting point – functional safety analysis
Hazards identification
Precise hazard analysis for chosen hazard event
no
Select the most important hazards
Sufficient amount of information from hazard analysis?
yes
Defining risk scenarios
Defining safety functions
Choose of safety function
Using of risk parameters
Use or build risk graph
Risk assessment
Tolerable risk criteria definition
Security analysis (vulnerabilities, threats and risk level) Cyber HAZOP
Determining of required SIL
To SIL verification

Fig. 5. A general procedure of SIL determining with the cyber security integration.

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 (Barnert et al., 2014; Piesik et al., 2016). 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 (Piesik et al., 2016).

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

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

The average probability of failure to perform the design function on demand for the system in relation to formula (2), assuming that all subsystems are tested with the interval T_I, is calculated as follows:

$$PFD_{avg} = \frac{1}{T_I}\int_0^{T_I} PFD(t)dt \tag{2}$$

where: T_I - proof test interval.

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

$$PFH \approx \frac{\sum_{j=1}^{n}(1-\sum_{\substack{i=1\\ i\neq j}}^{n} Q_j(t))(\sum_{j\in K_j}\frac{Q_j(t)}{q_i(t)}(1-q_i(t))\lambda_i)}{1-\sum_{j=1}^{n}\prod_{i\in K_j} q_i(t)} \tag{3}$$

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

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 1).

Table 1. SIL that can be claimed for given EAL, SAL or SeSa protection rings 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	Protection rings	Level of security	1	2	3	4
1	1	1	low	- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
2	1	2		- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
3	2	3	medium	SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4	2	4		SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	3	5	high	SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
6	4	6		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
7	4	7		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)

Table 1 shows the potential corrections of SIL for low, medium and high level of safety-related (E/E/PE or SIS) system security. It is possible that undesirable external events or malicious acts may influence the system by threatening to perform the safety-related functions in case of low security level. Thereby the low level of security might reduce the safety integrity level (SIL) when the SIL is to be verified. Thus, it is important to include security aspects in designing and verifying the programmable control and protection systems operating in an industrial network.

An integrated approach is proposed, in which determining and verifying safety integrity level (SIL) with levels of security (EAL, SAL and SeSa (Grøtan et al., 2007)) is related to the system category (I, II or III). It is possible that undesirable external events and malicious acts may impair the system by threatening to perform the safety-related functions in case of low security level (Figure 6).

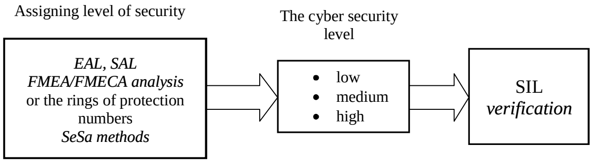

Fig. 6. Assigning level of cyber security in industrial network.

Such integrated approach is necessary, because not including security aspects in designing safety-related control and/or protection systems operating in network may result in deteriorating safety (lower SIL than required). In such cases the SIL verification, integrated with security aspects, is necessary (Figure 7).

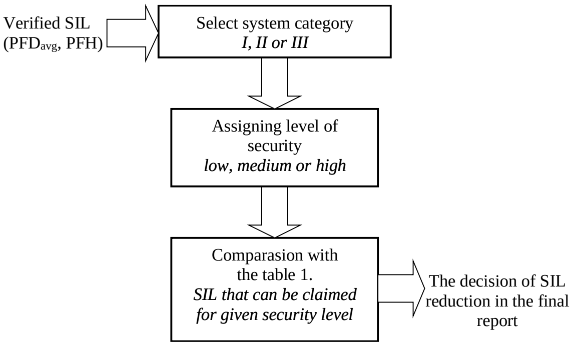
Verified SIL
(PFD$_{avg}$, PFH)
Select system category
I, II or III
Assigning level of security
low, medium or high
Comparasion with the table 1.
SIL that can be claimed for given security level
The decision of SIL reduction in the final report

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

4. Case study

The Safety Instrumented Systems (SIS) according to the series of standards IEC 61508 and IEC 61511 are very important not only for the safety, but also security aspects should be also taken into account using the SeSa rings related to security protection is another approach useful for the integration of functional safety and cyber security aspects.

Another important element is the human operator, who supervises the operation. The system's elements may be connected by different internal and/or external communication channels. 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.

In situation of distributed control and/or protection systems operating in a network it is necessary to consider also potential failures within such network (Fig. 8).

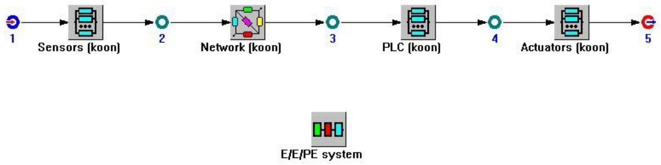

Fig. 8. RBD model SIS (E/E/PE) system including the industrial computer network.

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

$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgNet} + PFD_{avgPLC} + PFD_{avgA} \tag{4}$$

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.

An example of functional safety analysis that is presented below. It is based on a control system (Fig. 9), which consists of some basic components like sensors, programmable logic controllers and valves. It is a part of an maritime petrochemical critical installations.

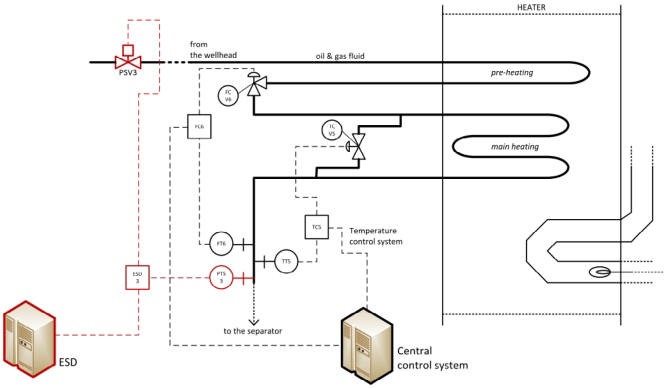

Fig. 9. Data transfer in distributed industrial control systems.

From the risk assessment the safety integrity level for given safety function overpressure protection heater in maritime critical installation was determined as SIL3. In industrial practice such level requires usually to be designed using a more sophisticated configuration. Safety function (overpressure protection) is implemented in distributed safety instrumented system SIS (Figure 10).

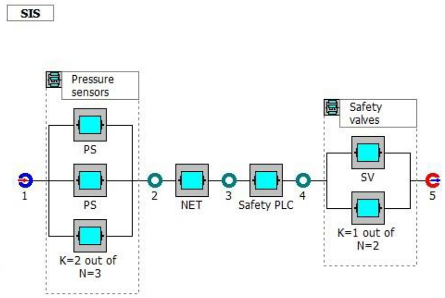

Fig. 10. RBD model overpressure safety instrumented system SIS in the critical installation.

The required SIL for entire distributed E/E/PE or SIS system is determined in a process of risk analysis and evaluation. It has to be verified in the process of probabilistic modeling, taking into account its subsystems including networks. Reliability data for SIS elements are presented in Table 2 (SINTEF, 2021).

Table 2. Reliability data for elements SIS system.

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

Table 3. The SIL verification report for SIS overpressure protection system.

System /subsystems/elements		**k oo n**	**β [%]**	**PFD$_{avg}$**	**SIL**
SIS	**0**	-	-	**$9.15{\cdot}10^{-4}$**	**3**
PS	**.1**	**2 oo 3**	**3**	**$4.46{\cdot}10^{-5}$**	**4**
PS	..2	-	-	$1.34{\cdot}10^{-3}$	2
PS	..2	-	-	$1.34{\cdot}10^{-3}$	2
PS	..2	-	-	$1.34{\cdot}10^{-3}$	2
NET	**.1**	**1 oo 1**	-	**$3.5{\cdot}10^{-4}$**	**3**
NET	..2	-	-	$3.5{\cdot}10^{-4}$	3
PLC	**.1**	**1 oo 1**	-	**$4.38{\cdot}10^{-4}$**	**3**
Safety PLC	..2	-	-	$4.38{\cdot}10^{-4}$	3
SVA	**.1**	**1 oo 2**	**2**	**$8.22{\cdot}10^{-5}$**	**4**
SVA	..2	-	-	$3.5{\cdot}10^{-3}$	2
SVA	..2	-	-	$3.5{\cdot}10^{-3}$	2

Assessment of the result obtained shows that for the SIS structure (Figure 10) is:

$$PFD_{avgSIS} \cong PFD_{avgPS(2oo3)} + PFD_{avgNET} + PFD_{avgSafetyPLC} + PFD_{avgSV(1oo2)} \cong$$

$$\cong 4.46 \cdot 10^{-5} + 3.5 \cdot 10^{-4} + 4.38 \cdot 10^{-4} + 8.22 \cdot 10^{-5} \cong 9.15 \cdot 10^{-4} \Rightarrow SIL3 \qquad (5)$$

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

Human operator in that case is an important part of the system. But in determining functional safety requirements processes the operator is treat an independent protection layer. Information from the alarm systems and basic process control system goes to the human operator. Human error probability was calculated by the Spar-H method it is one of most useful method of human reliability analysis in functional safety it consist of two parts diagnosis and action for the human (Kosmowski, 2013). Calculated human error probability according to the available time is these value 0.268. In the future it should be include to the verification process. Challenge in that process is integrated cyber security aspects and human error probability according to the functional safety. Nowadays popular problems is the cyberattacks to the industrial control systems through different communication channel, of course vulnerability threats include the attacks to the SCADA systems can take significant influence to the human action and in consequence it will lead to dangerous situation e.g. economical, environmental, health losses.

5. Conclusions

A comprehensive integration of the functional safety and cyber security analysis in maritime critical infrastructures is very important and it is currently a challenging issue. In this project an attempt to integrate the functional safety and security issue was presented. The security aspects, which are associated with e.g. communication between equipment or restrictions in access to the system and associated assets, are usually omitted during this stage of analysis. However, they can significantly influence the final results. Further research works have been undertaken to integrate outlined above aspects of safety and security in the design and operation of the programmable control and protection systems to develop a relatively simple methodology to be useful in industrial practice. The next step of evaluation the proposed approach safety & cyber security integrated it to include human as a hazard factor.

References

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 10th International Conference on Probabilistic Safety Assessment and Management 2010, 278-289.

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.

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

Goble, W., Cheddie, H. 2005. Safety instrumented systems verification: Practical probabilistic calculations. ISA.

Grøtan, T.O., Jaatun, M.G., Øien, K., Onshus, T. 2007. The SeSa Method for Assessing Secure Remote Access to Safety Instrumented Systems. SINTEF Report A1626, Trondheim.

Hildebrandt, P. 2000. Critical aspects of safety, availability and communication in the control of a subsea gas pipeline. Requirements and Solutions HIMA.

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

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

IEC 62443. 2013. Security for industrial automation and control systems. Parts 1-13, International Electrotechnical Commission, Geneva.

Kosmowski, K.T. 2013. Functional safety and reliability analysis methodology for hazardous industrial plants. Gdansk University of Technology Publishers, Gdańsk.

Kosmowski, K.T., Śliwiński, M., Barnert, T. 2006. Functional safety and security assessment of the control and protection systems. Safety and Reliability for Managing Risk : Proceedings of the European Safety and Reliability Conference (ESREL 2006), vol. 3, 2633-2640.

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, vol. 152, 259-272.

SESAMO. 2014. Integrated Design and Evaluation Methodology. Security and Safety modelling. Artemis JU Grant Agr. no. 2295354.

SINTEF. 2021. Reliability Data for Safety Instrumented Systems - PDS Data Handbook. SINTEF.