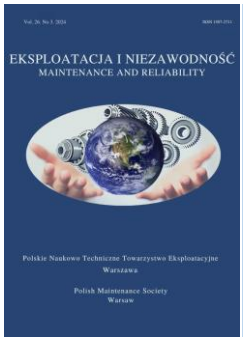

Eksploatacja i Niezawodnosc – Maintenance and Reliability

Volume 26 (2024), Issue 3

journal homepage: http://www.ein.org.pl

Article citation info:
Piesik E, Śliwiński M, Subramanian N, Zalewski J, Concept of Multifactor Method and Non-Functional Requirements Solution to Increase Resilience through Functional Safety with Cybersecurity Analysis, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2024: 26(3) http://doi.org/10.17531/ein/189454

Concept of Multifactor Method and Non-Functional Requirements Solution to Increase Resilience through Functional Safety with Cybersecurity Analysis

Indexed by: Web of Science Group

Emilian Piesik[a,*], Marcin Śliwiński[a], Narayanan Subramanian[b], Janusz Zalewski[c,d]

[a] Department of Control Engineering, Gdańsk University of Technology, Poland
[b] Computer Science, The University of Texas at Tyler, United States
[c] Department of Computing and Software Engineering, Florida Gulf Coast University, United States
[d] National Academy of AppliedSciences Ignacy Mościcki in Ciechanów, Poland

Highlights

- Integrated safety & security analysis is difficult and it is currently a challenging issue.
- Joint functional safety & cybersecurity analysis by applying the multifactor methodology.
- Integrated safety & cyber security analysis can minimize too optimistic results.
- Increasing resilience through integrated analysis of functional safety and cybersecurity.

Abstract

In the process of designing safety systems, an integrated approach in safety and cybersecurity analysis is necessary. The paper describes a new technique of increasing resilience through integrated analysis of functional safety and cybersecurity. It is a modeling methodology based on the combination of the multifactor method utilizing modified risk graphs, used previously for Safety Integrity Level (SIL) assessment, and the Non-Functional Requirements (NFR) approach. The NFR approach, based on the analysis of graphical representation of conceptual and physical components of the system, contributes a technique to include cybersecurity through the Softgoal Interdependency Graph. The assessment methodology is outlined in detail and applied to a case study involving an industrial control system. The analysis turns out to be effective in both aspects: confirming the findings of the multifactor approach based on modified risk graphs and complementing the traditional analysis to increase resilience in discovering and mitigating security vulnerabilities for SIL assessment by the use of NFR.

Keywords
energy efficient, Cybersecurity, system resilience, functional safety, NFR approach, safety integrity level.

1. Introduction

Resilience has been commonly linked to system safety [1]-[4]. Generally understood as the ability to bounce back, in the context of system safety resilience is the ability of a system to adjust so that it can sustain normal functioning in case of disturbances, translated into safe functioning in case of hazards. Functional safety is an important element of the system safety. It addresses those parts of safety that relate to the function of a system and ensures that the system causes no harm in response to its potential inputs or failures. The task of a safety related system in critical industrial installation is the reduction of risk according to accident scenarios.

In critical installations, safety functions are implemented through industrial automation and control systems. They are usually designed as the electrical and programmable electronic systems, according to the requirements of the IEC 61508 [5] and IEC 61511 [6] for safety instrumented systems (SIS). The critical task in the design of safety related systems is to mitigate the risks often through the implementation of layers of

(*) Corresponding author.
E-mail addresses: E. Piesik (ORCID: 0000-0002-1618-847X) emilian.piesik@pg.edu.pl, M. Śliwiński (ORCID: 0000-0001-7577-0526) marcin.sliwinski@pg.edu.pl, N. Subramanian (ORCID: 0000-0002-3963-9149) nsubramanian@uttyler.edu, J. Zalewski (ORCID: 0000-0002-2823-0153) ikswelaz@gmail.com

protection based on the concept of defense in depth (DinD) [7].

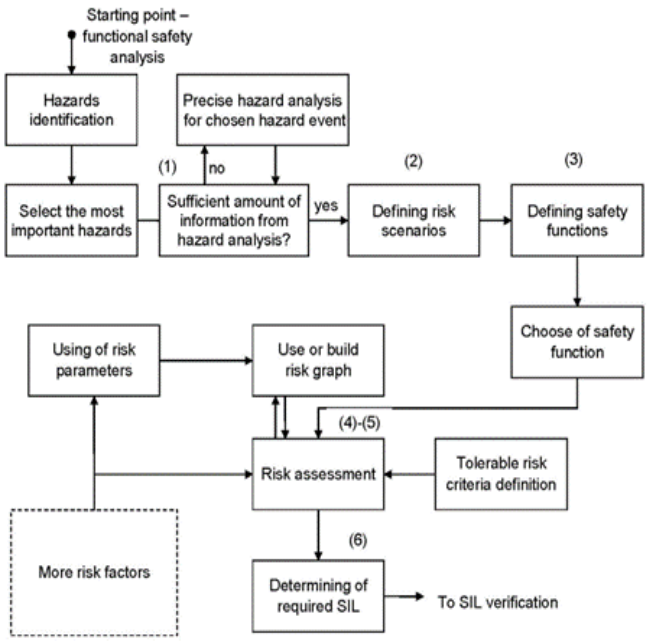

Fig. 1. The determination of SIL for selected risk parameter.

To meet the safety goals, the procedure for functional safety management includes several steps, such as hazard analysis, risk quantification and others. One of the most important activities in this analysis is to determine the Safety Integrity Level (SIL). Figure 1 explains essential aspects of determining the SIL by taking into account risk parameters.

After estimating a tolerable risk for the system in question, the diagram outlines steps that can be summarized as follows:

1) Identifying potential hazards.
2) Defining the essential risk scenarios.
3) Defining the safety functions.
4) Establishing an actual level of risk for a relevant system.
5) Expressing a reduction in the level of risk required for the assumed safety functions.
6) Representing a required level of reduction of risk as SIL.

Engineers use many methods to determine the level of SIL or any particular system used in a particular industry, where the most common are risk graphs and layer of protection analysis (LOPA) [8]-[10]. The problem is that with the recent spread of security threats to computer networks and interconnected devices, which may negatively impact safety of industrial control systems (ICS), it is natural that aspects of security have to be considered jointly with methods of evaluating SIL's, as well as incorporated into the entire process of safety analysis to increase resilience. Especially in high-risk installations and critical infrastructures, security analysis of the ICS and its design as distributed control system based on Supervisory Control And Data Acquisition (SCADA) are important.

Requirements related to security aspects are addressed in international standards IEC 62443 [11] and ISO 27000 [12], but they are not sufficient by themselves for use in safety critical systems. The study of literature reveals several approaches for joint assessment of safety and security, for example [13], but there are very few papers that discuss the process of including security into the determination of SIL [14]. One specific method that has been developed by two of the current authors and relies on using modified risk graphs [8], [15], appears to be effective but has some disadvantages, such as reliance on subjectivity in judgments.

System designers must take into consideration that, in cases of inadequate security, malicious acts and other undesirable external events may impair the system by negatively impacting its safety-related functions. Consequently, in terms of the process flow shown in Figure 1, security aspects can be added as separate activities in steps (4) and (5) of the risk analysis.

This paper proposes a more comprehensive method to joint functional safety and cybersecurity analysis by applying the multifactor methodology outlined in [16] complemented by the Non-Functional Requirements (NFR) approach [17]-[18]. Risk analysis methodology proposed here is compatible with practices often used in chemical industry, e.g., HAZID (hazard identification), HAZOP (hazard and operability analysis), SVA (security vulnerability analysis) and LOPA.

Functional safety is viewed as a part of overall system safety addressing the reduction of risk caused by critical systems working at a tolerable level of risk through the introduction of safety related functions. In practice, many safety instrumented systems (SIS) fit into the category of ICS. The safety-related functions are provided by the ICS and can be designed as electrical/electronic/programmable electronic systems (E/E/PES) according to the IEC 61508 [5] and/or safety instrumented systems according to the guidelines developed for the process industry and specified in IEC 61511 [6].

One of the most important activities in the analysis of such

systems is the determination of the Safety Integrity Level (SIL) of the system. With the increase in security threats existing methods of SIL evaluation have to include security aspects, which should be also incorporated into the entire process of safety analysis. In this work, we outline and recommend a comprehensive approach to joint functional safety and cybersecurity analysis by applying the multifactor methodology presented in [16] complemented by the Non-Functional Requirements (NFR) approach [17].

The rest of this paper is structured as follows. Section 2 outlines related work on integrated approaches to safety and security analysis, Section 3 presents and discusses the authors' approach to the determination of SIL's involving security aspects, by integrating the multifactor method with the principles of the NFR approach. Section 4 introduces the case study, Section 5 analyzes the case study applying the multifactor approach based on modified risk graphs to determination of SIL's with security aspects, and Section 6 integrates the multifactor method with the principles of the NFR approach. Section 7 reviews the results and Section 8 concludes the paper.

2. Related Work

System safety depends on the quality of the industrial installation that can be enhanced by applying protection layers, e.g., basic process control system, alarm system, human operator, and safety instrumented system. The causes of accidents in critical infrastructure depend on prospective weaknesses, initiation events, and internal hazards [15], [19]. The main task of the cybersecurity is to protect the system against potential threats (internal and external) that compromise its assets and the environment. Using rings of protection the risk is reduced to an acceptable level. These two issues, providing safety and providing security in engineering systems, have been treated separately for decades, as two individual domains. Nowadays, when inadequate security impacts safety, it is necessary to address them jointly. This section provides an verview of related issues and solutions.

2.1. General Literature Overview

he scientific literature on joint safety and security analysis has rown significantly during the last decade. It can be divided into everal categories. One group of papers concerns joint safety nd security risk analysis. Aven [20] attempted to develop a unified framework for such analysis based on the use of probability, defining risk as the combination of possible consequences and associated uncertainties. Based on the discussion of vulnerabilities, as an essential factor in security risk assessment, this framework is more a sketch forming a general background for risk assessment rather than an applicable procedure relying on a cohesive model of treating safety and security jointly.

Chockalingam et al. [21], coming from the perspective of dealing with security incidents that compromise system safety, offer a comprehensive literature review, identifying seven integrated risk assessment methods related safety and security. They are mostly based on extending the methods previously used by safety community, towards including security in the analysis. Most importantly, the authors point out that the methods reviewed differ in one significant aspect, that is, regarding the order of assessing safety and security risks. The study is considered a basis for establishing more effective methods for integrated assessment of safety and security risks.

Reichenbach et al. [22] point out that security aspects are usually not incorporated in the safety architecture nor in the safety development process. They propose to address this issue by advocating an approach for combination of safety and security analysis through the use the Threat Vulnerability and Risk Assessment (TVRA) and extending it to joint assessment of SIL's [23]. The essence of TVRA lies in the application of specific steps to evaluate the elements affecting risks introduced by threats. The authors illustrate effectiveness of this method by its application in a factory automation system.

Kriaa, in her dissertation [24], discusses risk analysis for joint treatment of safety and security aspects in order to optimize the risk management. Her focus is on cyberphysical systems, in particular, on SCADA architectures. She analyzed a couple dozen publications and identified two basic categories of joint risk assessment: process based and model based. The former category features two different perspectives for risk assessment: one relying on producing a set of requirements that define the system's safety and security functions, and another focused on separate development of requirements for safety and security, and then showing their interaction to identify and avoid conflicts. This survey and categorization led the author to the development of a canonical life-cycle model to integrate safety

and security. The essence of this model is the focus on non-functional requirements to do the risk analysis. The critical step in this process is to identify the hazardous or unsafe states of the system via hazard analysis, and then proceed to individual safety and security risk analyses, the former focused on failure mode analysis and the latter on threat and vulnerability analysis.

Other authors propose joint safety and security risk analysis for specific industries. For example, Abdo et al. [25] developed a comprehensive methodology based on a combination of bowtie analysis and attack trees and illustrated it with Industrial Control System (ICS) case study. Chen et al. [26] address risk assessment, including both safety and security, applied to a core flooder in a nuclear power plant. For this purpose, they propose using a nine-step risk assessment method similar to the one outlined in the NIST 800-30 document [27].

More systematic reviews on this subject have been published recently [28]-[30].

2.2. Cybersecurity in the Safety Lifecycle

To reach a high level of functional safety in the installation, it is assumed that throughout the safety lifecycle the safety level should be taken control of during the stages of developing the concept, design, operation, testing and maintenance of SIS as shown in Figure 2 [6].

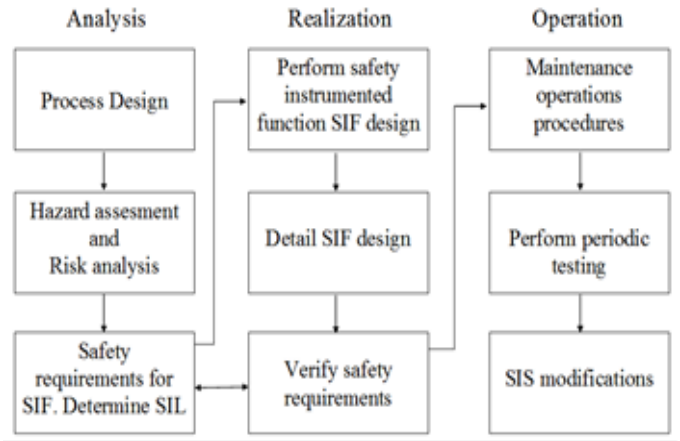

Fig. 2. Safety lifecycle with basic parts: analysis, realization, operation [6], [31] (SIF stands for Safety Instrumented Function).

Designing a safety system in accordance with the requirements in the safety lifecycle will reduce the risk of possible hazardous events in a critical installation. Examples of such installations are oil ports, LNG (liquefied natural gas) gas ports, petrochemical plants, and chemical installations.

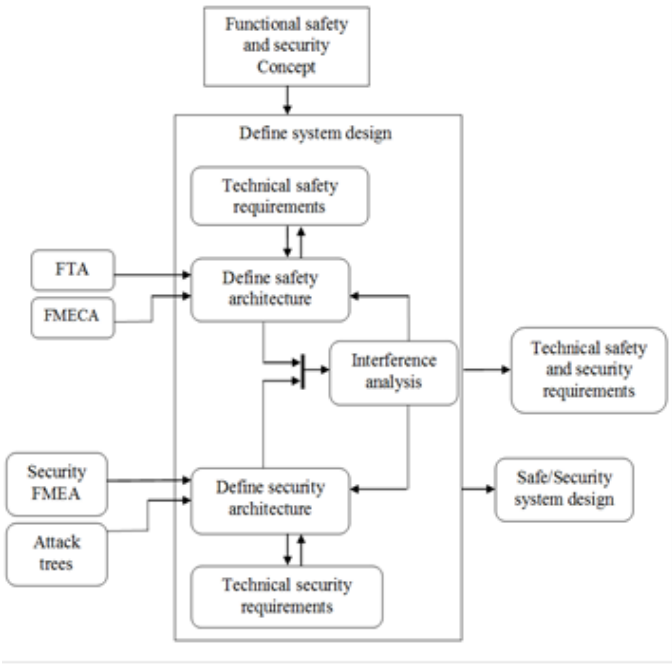

Fig. 3. Functional safety and cybersecurity activities of the system design stage [33].

The stage of designing a safety system comprises addressing the technical safety and cybersecurity requirements and defines a corresponding architecture [6], [32]-[33], as shown on a diagram in Figure 3.

Goals of the safety and security form a significant input in derivation of the requirements for functional safety and security. In this stage, first, the interference analysis is undertaken to identify their influences on each other.

Regarding the inclusion of cybersecurity aspects, the current authors pursued their own method focused on determination of SIL's based on modifiable risk graphs [15], with additional consideration of security assurance levels (SAL), evaluation assurance levels (EAL), and protection rings [8]. This was recently extended to the SIL verification of SIL's with cybersecurity factor [16]. The next section presents the authors' previous work in this regard and proposes integration of this method with the NFR approach.

3. Determination of Safety Integrity Levels

3.1. Industrial Automation and Protection Systems

A conventional automation and safety related system consists of logical elements, e.g., industrial computers, safety relay or programmable logic controllers, measurement elements, actuators and human machine interface (HMI). The main data transfer occurs between these elements (pressure sensors, flow

meters, temperatures sensors) and the control room. This involves the operator who is responsible for the process. A typical control and protection system being a part of the critical infrastructure incorporating various communication channels is shown Figure 4.

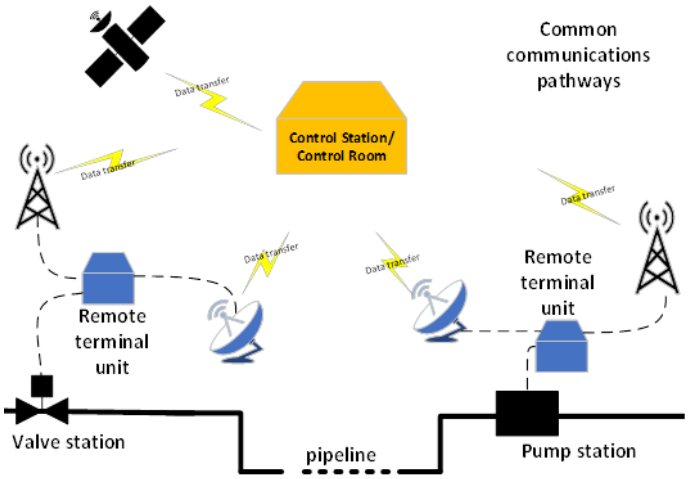

Fig. 4. Data transfer in different communication channels for distributed control systems.

Two safety related standards, IEC 61508 [5] or IEC 61511 [6], give more specific requirements related to the communication channels and cybersecurity in the context of control systems. These normative documents concern in general two types of communication channels. The first one is called the white channel, if designed, implemented and validated according to the requirements of IEC 61508. The second one is the black channel, which means that some parts of it have not been designed, implemented and validated according to IEC 61508.

Data transfer channels can be validated and implemented with the procedures that are included in the IEC 62280 standard [34] on railway communication, signaling and control systems applications [5]-[6]. This is because the communication channels in the process industry are very similar to those used in the railway safety, but in significant cases where the safety integrity level requirements are at the highest level, e.g., SIL-4, the design parameters are more sophisticated.

3.2. Determination and Verification Process of Safety ntegrity Levels with Cybersecurity Aspects: Overview

3.2.1. General

he assessment of safety integrity level for a given safety nction, to be implemented by the control or protection systems, is one of the most crucial functional safety goals. Because a potential failure of critical subsystems in industrial installation can occur due to a fault or incorrect action of such safety-related elements, the automation and industrial protection system could lead to dangerous accidents, and cause injury or death of people. It can also contribute to the environmental damage or property damage in the installation or outside the installation. This is a reason why technical risk analysis of the safety instrumented systems is so desirable.

This section introduces a case study of functional safety analysis. It involves critical installation shown on a piping and instrumentation (P&ID) diagram with the automation system illustrated in Fig. 5, which contains such components as data transmitters, controllers, and control valves.

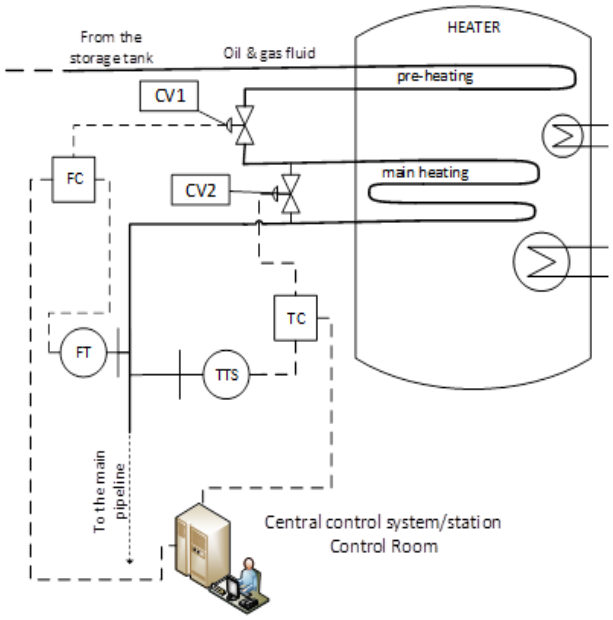

Fig. 5. P&ID scheme of critical installation with the control system.

Our previous approach to functional safety analysis used modifiable risk graphs, which let build any risk graph according to the risk parameters and its different range expressed in the semi-quantitative or qualitative way. The approach relies on data taken in the course of hazard detection as well as further risk assessment for designed or existing distributed control systems. Some parameters, as shown in Table 1, influence the frequency of hazardous incidents and some are responsible for their consequences. The frequency parameter is simplified, associated with block reliability of the automation system equipment and human reliability factors.

Table I. Data relating to risk graphs [5]-[6].

Risk parameter		Classification
Consequence (C^1)	C^1_1	Minor Injury
	C^1_2	Serious permanent injury to one or more persons, death to one
	C^1_3	Death to several people
	C^1_4	Very many people killed
Frequency of, and exposure time in the hazardous zone (F^1)	F^1_1	Rare to more often exposure in the hazardous zone
	F^1_2	Frequent to permanent exposure in the hazardous zone
Possibility of avoiding the hazardous event (F^2)	F^2_1	Possible under certain conditions
	F^2_2	Almost impossible
Probability od the unwanted occurrence (F^4)	F^4_1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely
	F^4_2	A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely
	F^4_3	A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely

The cybersecurity aspects are related, for example, to data transfer between hardware items or to restrictions in accessing the system and its components, and are not always taken into account at this stage. However, they may significantly add to the final score. Thus, it is desirable to have a basic but powerful method that allows including those concepts into functional safety assessment. It is very essential in the analysis of complex, distributed control systems. Although the risk estimation could be done with a number of different methods, in this work, the attention is focused on risk graphs.

Fig. 6 shows a typical risk graph addressing the risk parameters described in Table I, relating to consequences of the hazardous event (C1), frequency of, and exposure time in, the hazardous zone (F1), the possibility of failing to avoid the hazardous event (F2), and the probability of the unwanted occurrence of potential events that demand the operation of a given E/E/PE safety-related system (F4).

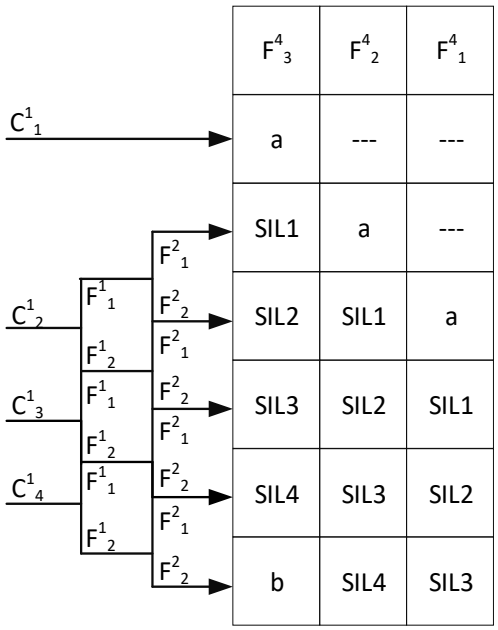

Fig. 6. Risk graph for determining SIL ('---' means no safety requirements, 'a' - no SIL requirements, 'b' - single safety system is not sufficient for SIL1-4).

3.2.2. Modifiable Risk Graphs

In the risk graph and computer-based model associated with it [5], [15], [37], it is possible to take into account certain cybersecurity results by building the risk graph for the control system when the internal and/or external industrial network is used. In a critical infrastructure some vulnerabilities may exist, which can generate an additional risk to a system that consist of different categories, e.g., human, economic and environmental. The results of cybersecurity assessment for a given protection system can be assigned, in the simplest case, to a few main classes, for example, using a qualitative definition of ranges, such as low, medium or high level of cybersecurity.

Coinciding with this view is the Evaluation Assurance Level (EAL) model, which includes the complete boundary conditions for developing a system according to defined level of strictness. ISO/IEC 15408 [35] lists seven such levels, from EAL1 as the most basic and cheapest to implement to EAL7 as the most expensive. Higher EAL levels do not necessarily mean improved security. They only mean that the security assurance of the target system has been more detailed and validated.

Table II. Cybersecurity Levels Corresponding to EAL's and Risk Parameter.

EAL	Level of cybersecurity L-low, M-Medium, H- High	Risk parameter and its ranges
1	L	F^3_3
2	L	F^3_3
3	M	F^3_2
4	M	F^3_2
5	H	F^3_1
6	H	F^3_1
7	H	F^3_1

In the considered method based on modifiable risk graphs, a standard set of risk indicators is taken into account, what is outlined in Section III.B.1 above and illustrated in Table 1. Table II incorporates an additional risk parameter, which represents the level of security (F3) mapped onto EAL levels.

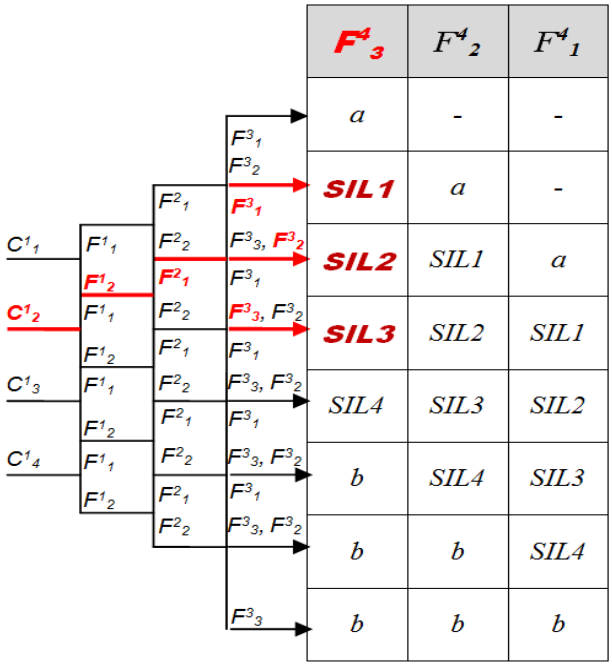

Fig. 7. Example of extended risk graph flow (the meaning of '-', a and b is the same as in Fig. 6).

The new risk graph with the fourth risk indicator, F^3, representing the level of cybersecurity, is presented in Fig. 7. The calibration of such method gives an opportunity to verify safety related requirements on the SIS system by calculating the Probability of Failure on Demand (PFD) [36]-[37].

3.3. The NFR Approach and Its Role

3.3.1Main Syntactic Concepts

Emergent system properties such as reliability, testability, flexibility, adaptability, safety, and security are typically classified as non-functional requirements (NFRs) [38]. The NFR approach considers such NFRs as softgoals that can be satisfied within a range but not in the absolute sense [12]. The ability to satisfy within a range is referred to as satisficing, borrowing the term from economics, first used by Simon in 1956 [39]. It means "finding a choice mechanism that will lead it to pursue a 'satisficing' path, a path that will permit satisfaction at some specified level…".

The NFR approach defines four types of satisficing: strongly ıtisficed (also called MAKE), weakly satisficed (HELP), ʻeakly not satisficed or weakly denied (HURT), strongly not ıtisficed or strongly denied (BREAK). When satisficing extent annot be determined then the satisficing type is UNKNOWN. hese satisficing types associated with a softgoal become the label for that softgoal – this means that a softgoal can have one of the five labels associated with it: MAKE, HELP, HURT, BREAK, and UNKNOWN [40].

Moreover, the softgoals for the system may be decomposed into child softgoals thereby creating a hierarchy of softgoals. This hierarchy may be created by decomposing a softgoal into its children in three ways: AND, OR, and refinement. In an AND-decomposition, the parent softgoal is decomposed into its child softgoals in a manner such that if even one of the children is denied (HURT or BREAK) then the parent is denied as well. In other words, the parent is satisficed only if all children are satisficed. In an OR-decomposition, the parent is satisficed (MAKE or HELP) even if only a single child softgoal is satisficed. In a refinement of a parent softgoal, the satisficing type of the child propagates to the parent, that is, the parent has the same type of satisficing as the child.

The NFR approach provides a framework for determining the extent to which a system's NFR softgoals have been satisficed by the constituents of the system. For this purpose, three types of softgoals are defined:

- the NFR softgoals that represent system's non-functional requirements;
- the operationalizing softgoals corresponding to the elements of the system such as components, connections, and constraints, and
- the claim softgoals (also called argumentative softgoals) that capture the rationale or justifications for extent of satisficing by constituents of the system.

Each of these softgoals may be decomposed into hierarchies, so that one may have a hierarchy of NFR softgoals, a hierarchy of operationalizing softgoals, and ahierarchy of claim softgoals.

The relationship between a parent and a child softgoal is captured by a contribution, and the contribution propagates labels from the child softgoal to the parent softgoal. Contributions can have one of four types of labels similar to that of a softgoal: MAKE, HELP, HURT and BREAK. Contributions are directional and they propagate labels from one softgoal to another depending on the contribution label as well as the from-softgoal label.

Thus, for example, a MAKE-labeled contribution will propagate a MAKE label from a softgoal as a MAKE to its parent, while a BREAK-labeled contribution will propagate

a MAKE label from the child as a BREAK to its parent. Contributions can also form a chain, in the sense that one contribution can propagate a label to another.

The final part in applying the NFR approach is the set of propagation rules that capture how labels are propagated from one element of the NFR approach to the other. Thus, propagation of labels from one softgoal to another across decompositions, as well as how contributions propagate labels, is captured by propagation rules.

Since several propagation rules can be developed based on various combinations of softgoals, decompositions, contributions, and labels, for a specific problem, only relevant rules that are a subset of all possible rules are used. The propagation rules adopted in this paper are listed in the Appendix. For their broader discussion, the reader is referred to earlier papers [17], [18].

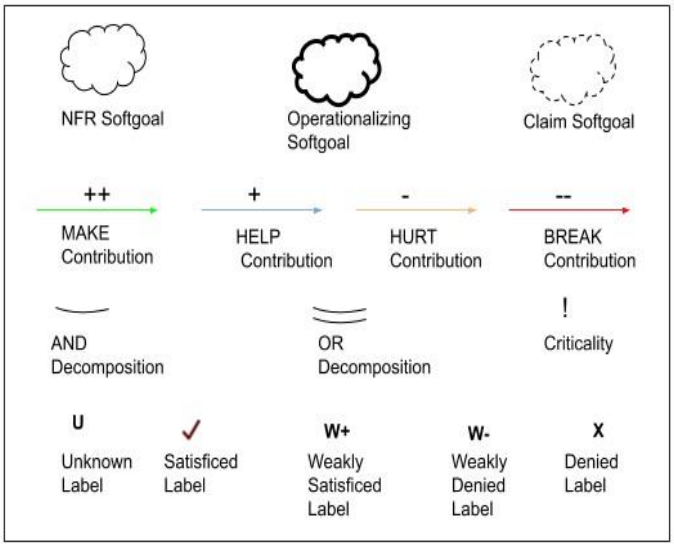

Fig. 8. Partial ontology of the NFR approach.

Relationships between different components of the NFR approach may be captured in the form of a special graph named the Softgoal Interdependency Graph (SIG). The ontology of the NFR approach is presented in Figure 8. In a typical SIG, NFR softgoal hierarchy appears at the top, operationalizing softgoal hierarchy appears at the bottom, while contribution hierarchy ppears in-between. In addition, the criticality symbol can be sed to indicate high priority softgoals or contributions.

3.3.2. The Procedure

he essence of the NFR approach is goal-orientation. The root FR softgoals (at the top) are the goals to be reached by the design of the system that meets the operationalizing softgoals. In this paper, the objectives considered are safety and security for industrial automation systems, therefore, the NFR approach will evaluate the extent to which safety and security are achieved by the automation system under consideration.

The procedure in the NFR approach consists of five steps that can be applied iteratively for evaluating safety and security:

1) Decomposition of Safety NFR.
2) Decomposition of Security NFR.
3) Decomposition of the architecture of the system under consideration into its corresponding operationalizing softgoals
4) Determination of contributions to the NFR softgoals made by the operationalizing softgoals.
5) Evaluation of the combined safety and security done by following the propagation rules and determining the propagation of labels to the root softgoals.

The first step relies on decomposition of the NFR safety into its softgoal hierarchy based on the system's safety requirements. Then, one proceeds with decomposition of the NFR security into its softgoals based on the system's security requirements. The third step relies on decomposition of the architecture of the industrial automation system into its components, connections and constraints, by creating a hierarchy of corresponding operationalizing softgoals. Next, contributions made by the operationalizing softgoals to the NFR softgoals are determined, so are justifications for these contributions in the form of claim softgoals. The last step relies on applying the propagation rules for labels all through the SIG to evaluate the system's joint safety and security.

The root of the SIG constitutes the Integrated SIL (ISIL) NFR softgoal capturing the combined satisficing of safety and security. Table III illustrates the correspondence between SIL numbers and the extent of satisficing of the ISIL NFR softgoals.

Table III. Mapping the Softgoal Labels onto SIL Numbers.

ISIL NFR Softgoal Label	Equivalent SIL number
V Satisficed	4
W+ Weakly Satisficed	3
W- Weakly Denied	2
X Denied	1

In the next section we outline briefly the application of the combination of NFR approach and the multifactor methodology based on modifiable risk graphs [15] to the joint functional

safety and cybersecurity analysis in a case study of an industrial automation system shown in Figure 5.

3.4. The Integrated View

In the integrated functional safety and security analysis of safety-related systems, the required SIL can be validated by considering the potential influence of security levels, described as the SAL, EAL, SecureSafety (SeSa) protection rings or another method, such as LOPA [15]-[16]. The SIL itself is concerned with safety aspects, while the SAL, EAL and SeSa relate to the information security level of the entire system for monitoring, protection or control functions. This section presents the summary of the application of the studied methods.

It is quite probable that malicious acts or other undesirable external events may negatively impact the system by obstructing it, so in case of low security it won't be able to perform the safety-related functions. In such case, the insufficient security might reduce the SIL level, when the SIL is to be validated. Consequently, it becomes clear that security aspects should be included in designing programmable control and protection systems operating in an industrial network.

An integrated method is proposed by using the NFR approach, in which determining and validating the SIL with additional consideration of security levels (SAL, EAL or SeSa) is related to systems that operate in closed or distributed critical facilities, where system data are transferred not only by internal channels but can be transmitted outside through external channels.

Fig. 9 shows the logical principle of dealing with malicious acts and undesirable external events that may negatively impact the system operation by obstructing its ability (in case of insufficient security) to perform safety-related functions.

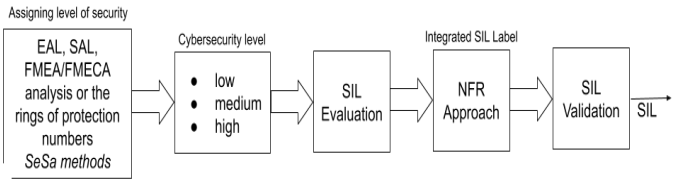

Fig. 9. Assigning the level of cybersecurity in industrial network.

Table IV shows the suggested corrections of SIL for three levels of security in safety-related systems (E/E/PE or SIS).

Table IV. SIL for distributed control and protection systems [15] - [16]

Determined cybersecurity factor				Verified SIL for functional safety			
EAL	**SAL**	**Protection rings**	**Level of security**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
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)

Where the NFR approach comes into play is the determination of SIL for the cybersecurity factors and their levels from Table IV.

Table V. SIL evaluation in the NFR approach and its mapping to Table IV

Extent of Satisficing Safety → **↓ Extent of Satisficing Security ↓**	**Level of Security**	X (denied)	W-	W+	V (satisficed)
X (denied)	Low	SIL1	SIL1	SIL1	SIL1
W- (weakly denied)	Medium	SIL1	SIL2	SIL2	SIL2
W+ (weakly satisficed)	Med/High	SIL1	SIL2	SIL3	SIL3
V (satisficed)	High	SIL1	SIL2	SIL3	SIL4

This mapping is shown in Table V, with one additional level for EAL-5 and SAL-3, named Med/High, which complements the SIL evaluation per Table IV. This integrated approach is beneficial, since in designing safety-related systems making use of a communication network, any omissions in assessing security may lead to establishing lower SIL than required, that is, deterioration of safety.

In summary, taking into account the security measures during the functional safety analyses is always of primary importance. In this work, well-known concepts of SAL, EAL and SeSa form the basis for respective assessments. But it is clear that in applying the Common Criteria (EAL's) [35] for some designs of programmable systems the EAL related considerations may be insufficient. For example, EAL usually relates to a single component, while the system aspects may be more important. This is a good reason for looking into other security models, and here the NFR approach plays its role.

4. Case Study Selection

The oil sea port installation shown in Figure 10 is one of the most typical examples that illustrate the breadth of functional safety and cybersecurity integrated approach. Its major part is the fuel base consisting of tanks, engineering station, pipelines,

truck, ship and railway fuel terminals, and is subject to hazards, such as explosion atmosphere, electric sparks in distributed installation and electromagnetic fields. A segment of the installation considered here consists of three liquid fuels tanks and one buffer tank, all connected to the main pipeline. The medium (e.g., oil) transfer occurs between the tanks and a loading station.

The elements of the system can be linked by various internal or external channels of communication. The data exchanged from the programmable logic controller (PLC) to the control station can be sent via wireless links, such as radio modems, satellite technology or GSM/GPRS. The main reason to use wireless connectivity is that several components of the large distributed installation do not have the capability to use the wired connections.

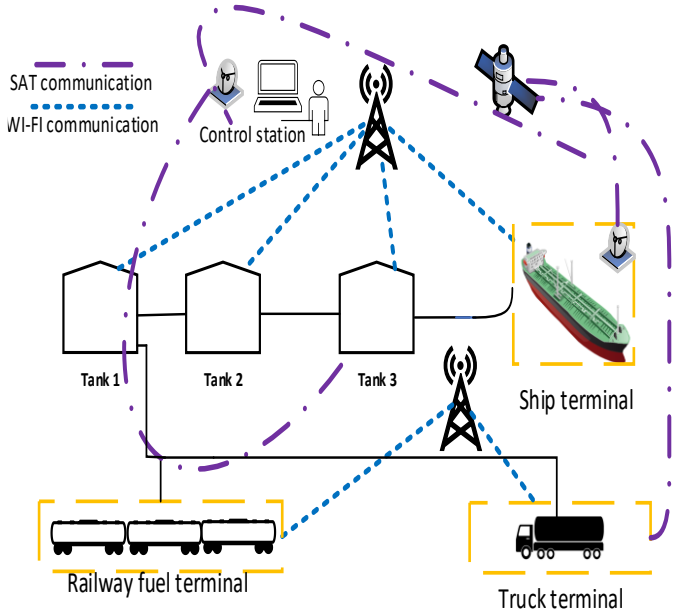

Fig. 10. Industrial data transfer in DCS for the oil pipeline infrastructure with control station.

The installation is highly distributed and the control and protection system involves satellite and wireless communication. There may be several potential safety problems in this kind of installation. The main issues are: tank overfill prevention, high pressure oil transfer, leaks of pipelines, communication and data transfer errors, etc. The human operator supervising the operation is also an important element to consider as a source of errors [41].

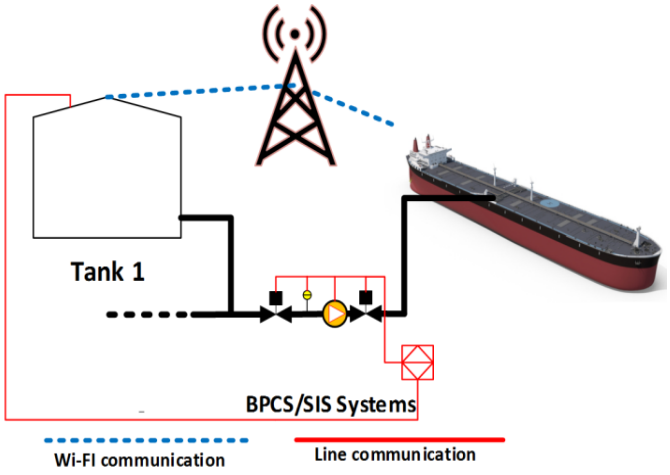

Fig. 11. Example of oil seaport installations with critical infrastructure SIS and basic process control systems.

The SIS addressed in the series of international standards [5]-[6] has to be considered not only from the safety perspective, but also in a view of security aspects. In this regard, the SeSa methods related to cybersecurity protection make a valuable methodology for the integrated considerations on functional safety and cybersecurity [5]-[6], [16].

For the system illustrated in Figure 10, the SIL determination is related to safety aspects, while SAL and EAL concern the data cybersecurity level of the system providing monitoring, control and safety functions.

In a reduced system illustrated in Figure 11, the essential role is played by the communication channels, both wireless and wired. Wireless communication is used to transfer data about control parameters in the tanks. A wired channel exists to transmit values of the fuel level in the tank as well as the control fuel flow in the core system [31], [42].

5. Case Study Analysis with Multifactor Method

In the case of decentralized control and protection systems communicating via the network, potential failures in such a network should be considered, as shown in the reliability block diagram (RBD) in Figure 12.

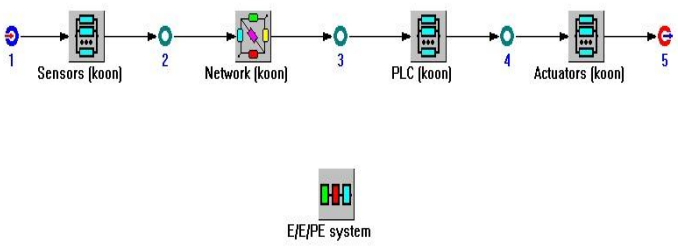

Fig. 12. RBD model of SIS system with the industrial network.

The average probability of failure on demand PFD_{avg} is calculated according to the formula based on IEC 61511 [6]:

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

where PFD_{avgSYS} is calculated for the entire SIS system, PFD_{avgS} – same for the sensor, PFD_{avgNet} – same for the network, PFD_{avgPLC} – same for the PLC, and PFD_{avgA} – for the actuator.

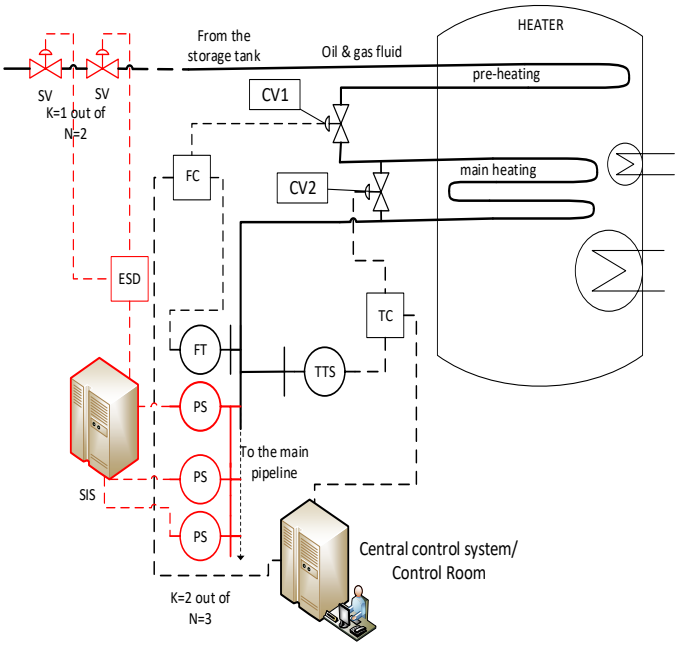

Fig. 13. P&ID critical installation with DCS and SIS.

Based on formula (1), it is evident that the probability of failure will be higher when the computer network will be included in the model. Therefore, the results achieved may affect the validated SIL (a lower SIL value than in case when the network is not included). However, the modelling approaches considered in IEC 61508 and IEC 61511 do not fully cover computer network components. The results achieved applying the standards may be therefore too optimistic.

A case study of the analysis of functional safety is shown next. It concerns a control system in Figure 13, extending those discussed previously. It constitutes a critical element of a maritime petrochemical installation and comprises the essential components, such as sensors, valves and rogrammable logic controllers.

Based on the risk assessment for assumed safety function of ıe overpressure safety heater in an offshore installation, using ıe risk graph method, the safety integrity level has been etermined as SIL3. In industrial applications this level usually eeds to be developed in a more sophisticated configuration.

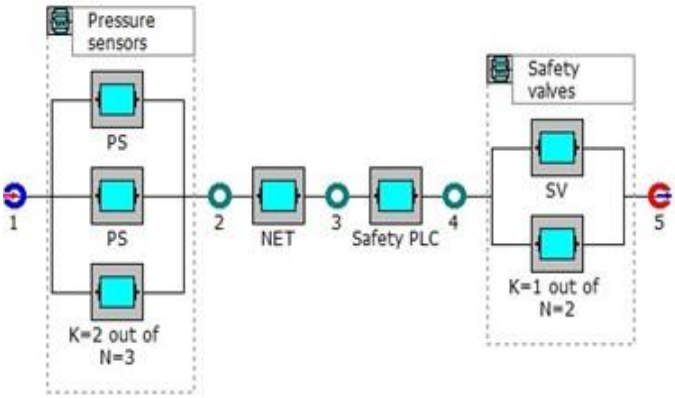

Fig. 14. Reliability block diagram for overpressure protection safety instrumented system (SIS).

This safety function for overpressure protection is carried out in a distributed SIS system as shown in Figure 14.

Table VI. Reliability data for SIS system elements based on PDS Data Handbook [43].

	PS	NET	SafetyPLC	SV
DC [%]	53	98	99	96
λ_{DU} [h^{-1}]	$3.05 \cdot 10^{-7}$	$8 \cdot 10^{-8}$	$7 \cdot 10^{-8}$	$8.02 \cdot 10^{-7}$
T_I [a]	1	1	1	1
β [%]	2	1	1	2

The required SIL for the combined E/E/PE and SIS system is determined by risk analysis and assessment. The verification of SIL includes the probabilistic model with the industrial network. The reliability data for the SIS elements, obtained using the methodology explained in [43], are presented in Table VI.

The assessment of results indicates that for the SIS configuration in Figure 14 the correct SIL is at the level SIL-3

$$PFD_{avgSIS} \cong PFD_{avgPS(2oo3)} + PFD_{avgNET} + PFD_{avgSafetyPLC} + PFD_{avgSV(1oo2)} \cong 4.46 \cdot 10^{-5} + 3.5 \cdot 10^{-4} + 3.1 \cdot 10^{-4} + 8.22 \cdot 10^{-5} \cong 7.87 \cdot 10^{-4} \Rightarrow SIL3 \quad (2)$$

Table VII. The SIL verification for SIS overpressure protection system

System components		k oo n	β [%]	PFD_{avg}	SIL
SIS	**0**	-	-	**$7.87 \cdot 10^{-4}$**	**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**	-	**$3.1 \cdot 10^{-4}$**	**3**
Safety PLC	..2	-	-	$3.1 \cdot 10^{-4}$	3
SV	**.1**	**1 oo 2**	**2**	**$8.22 \cdot 10^{-5}$**	**4**
SV	..2	-	-	$3.5 \cdot 10^{-3}$	2
SV	..2	-	-	$3.5 \cdot 10^{-3}$	2

Therefore, the PFD_{avg} equal $7.87 \cdot 10^{-4}$ is formally fulfilling the requirements for random failures at SIL3 level. The results are summarized in Table VII. Omission of certain communication subsystems or networks may lead to over-optimistic results, especially for distributed control and protection systems.

6. Validation Using the NFR Approach

Figure 15 presents the SIG built for the presented control system in Figure 13. The first two steps of applying the NFR approach involve the decomposition of the NFR hierarchy, subsequently for Safety and for Security. The top node represents the root NFR softgoal, the Integrated SIL (ISIL). It is AND-decomposed into two child nodes (softgoals for Safety and Security), indicated by the single arc. The Security softgoal is further OR-decomposed into its softgoals of Evaluation Assurance Level (EAL), Security Assurance Level (SAL), and Layers of Protection Analysis (LOPA), indicated by the double arcs. The Safety softgoal is AND-decomposed further into Low Failure Rate, Reliability and Redundancy softgoals, as reflected on the diagram.

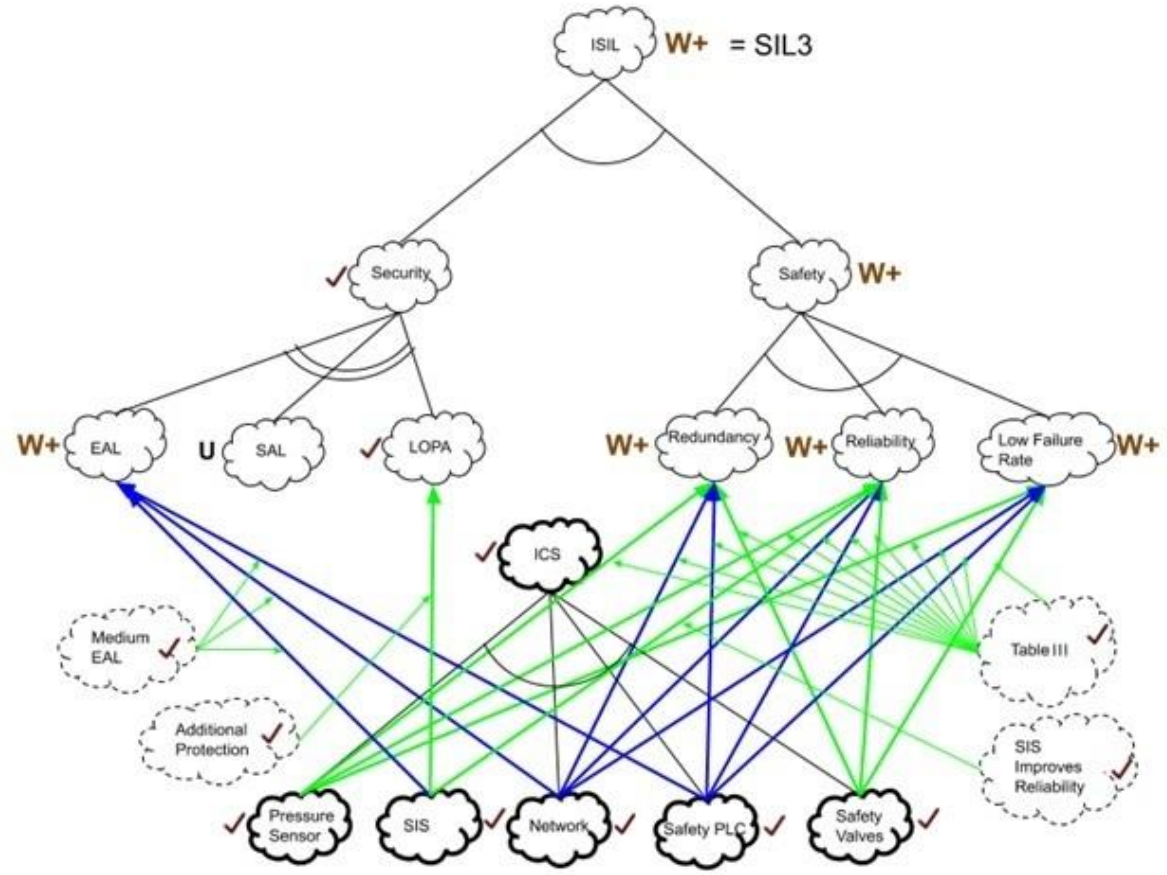

Fig. 15. SIG corresponding to the heater pressure system in Figure 13.

The bottom of Figure 15 shows thick-bordered cloud shapes reflecting the decomposition hierarchy for operationalizing softgoals. This constitutes the third step in the NFR approach. The root of these cloud shapes represents the ICS perationalizing softgoal of Figure 13. It is further AND-ecomposed into the five components constituting the ICS: afety Valves, Safety PLC, Network, SIS, and Pressure Sensor.

The fourth step of the NFR approach relies on the etermination of the contributions of the operationalizing oftgoals to the NFR softgoals. Table VIII presents these contributions as well as their rationale. On the Security side, the EAL NFR softgoal receives HELP contributions from respective operationalizing softgoals: SIS, Network, and Safety PLC (rows 1-3).

All contributions are HELP, as a SIL of 3 in Table VII is assumed to correspond to medium EAL; and the NFR softgoal LOPA receives a MAKE contribution (row 4) from the SIS operationalizing softgoal because SIS provides an additional layer of protection. On the Safety side, SIS operationalizing softgoal contributes a MAKE to Reliability NFR softgoal (row

6) since the presence of a SIS improves a system's reliability.

Table VIII. Rationale for contributions in SIG of Figure 15

Number	From Operationalizing Softgoal	To NFR Softgoal	Contribution	Justification
1	SIS	EAL	HELP	SIL3 in Table VII corresponds to medium EAL
2	Network	EAL	HELP	SIL3 in Table VII corresponds to medium EAL
3	Safety PLC	EAL	HELP	SIL3 in Table VII corresponds to medium EAL
4	SIS	LOPA	MAKE	SIS provides additional layer of protection
5	Pressure Sensor	Redundancy, Reliability, Low failure rate	MAKE	Table VII
6	SIS	Reliability	MAKE	SIS improves system reliability
7	Network	Redundancy, Reliability, Low failure rate	HELP	Table VII
8	Safety PLC	Redundancy, Reliability, Low failure rate	HELP	Table VII
9	Safety Valves	Redundancy, Reliability, Low failure rate	MAKE	Table VII

The Network and Safety PLC operationalizing softgoals contribute HELP to each of the NFR softgoals (rows 7 and 8): Low Failure Rate, Reliability and Redundancy, for the reasons given in Table VII. Also on the Safety side, Pressure Sensor and Safety Valves (as per rows 5 and 9 in Table VIII) provide MAKE contributions to the three NFR softgoals. Again, as before, the reasons are shown in Table VII. The concluding phase in the NFR approach involves the application of propagation rules to see how the NFR softgoals are satisficed. The satisficing extent of softgoals for the SIG in Figure 15 along with respective propagation rules for making the decision is shown in Table IX.

Rows 1 through 4 of Table IX indicate that the four claim softgoals (Figure 15, marked by dash-bordered shapes) are satisficed by assumption. Row 5 shows that respective child operationalizing softgoals marked in Figure 15 are satisficed as well, as they correspond to components of the ICS (illustrated in Figure 13). As indicated in row 6 the parent operationalizing softgoal ICS is satisficed as well, by propagation rule R8 (see Appendix), since all its children feed it with satisficed labels.

Table IX. Label propagation in the SIG of Figure 15.

Number	SIG Element (Fig. 7)	Satisficing Extent	Propagation Rule Applied
1	Claim softgoal "Medium EAL"	Satisficed	Assumption – claims are assumed to be satisficed
2	Claim softgoal "Additional Protection"	Satisficed	Assumption – claims are assumed to be satisficed
3	Claim softgoal "Table II"	Satisficed	Assumption – claims are assumed to be satisficed
4	Claim softgoal "SIS Improves Reliability"	Satisficed	Assumption – claims are assumed to be satisficed
5	Operationalizing softgoals Pressure Sensor, SIS, Network, Safety PLC, and Safety Valves	Satisficed	They are components of the ICS and they exist.
6	Operationalizing softgoal ICS	Satisficed	R8
7	All contributions in Figure 15	Remain same	R12 – since their supporting claim softgoals (rows 1 through 4) are satisficed.
8	NFR softgoal EAL	Weakly Satisficed	By R3, EAL receives W+ contributions from its children; by R11, the final label for EAL is W+
9	NFR softgoal SAL	Unknown	R6
10	NFR softgoal LOPA	Satisficed	R2
11	NFR softgoals Redundancy and Low Failure Rate	Weakly Satisficed	Receives two satisficed contributions and two W+ contributions from its children; by R11, the final label is W+
12	NFR softgoal Reliability	Weakly Satisficed	Receives three satisficed contributions and two W+ contributions from its children; by R11, the final label is W+
13	NFR softgoal Security	Satisficed	R7 and R9
14	NFR softgoal Safety	Weakly Satisficed	R8
15	NFR softgoal ISIL	Weakly Satisficed	R8

Row 7 of the table indicates that all contributions in Figure 5 preserve the types of label propagation, since by rule R12 ıeir support claim softgoals are satisficed, as shown in rows 1 ırough 4 of the table. As shown in row 8, the NFR softgoal EAL is weakly satisficed (W+), by propagation rules R3 and R11, because the operationalizing softgoals feed into it the weakly satisficed labels. As shown in row 9, by rule R6, NFR softgoal SAL has the Unknown label. In turn, as indicated in

row 10, the NFR softgoal LOPA has the satisficed label by rule R2. As row 11 shows, both NFR softgoals Low Failure Rate and Redundancy receive two weakly and two fully satisficed labels, so R1 determines that the final labels are weakly satisficed.

As row 12 shows, the NFR softgoal Reliability receives two weakly satisficed labels and three satisficed labels, so its final label is weakly satisficed, by rule R11. Based on rule R7, which states that softgoals with Unknown label are considered denied when used in an OR contribution to their parent, row 13 indicates that the Security parent NFR softgoal is weakly satisficed by applying rule R9. Similarly, row 14 shows that the parent NFR softgoal Safety, receiving an AND-contribution from its children, is by rule R8 weakly satisficed as well.

Finally, as shown in row 15, the application of rule R8 leads to the root NFR softgoal ISIL being weakly satisficed. Consistent with the correspondence of SIL and ISIL levels, this reasoning reveals that the integrated SIL for the analyzed system of Figure 13 is SIL3, which is confirmed by the previous discussion of the multifactor method.

7. Discussion of Results

7.1. The Integrated View

The two techniques acting in tandem as in Figure 9 resemble the maker-checker approach to SIL validation – one technique creates a SIL value and the other validates the value. In the case study both techniques using completely different approaches confirmed the SIL to be 3. The data used by the two techniques are also different – risk graphs use statistical values such as those given in Table VI, while the NFR approach uses data from requirements, design, implementation, and quality assurance.

Therefore, if the two approaches validate the SIL then there is a high degree of confidence in the SIL value since several complementary factors of the system under test have been considered, which results in a comprehensive evaluation. Both techniques are amenable to automation since spreadsheet programs can be used to store and compute values for each technique. These spreadsheets can also maintain historical record of SIL changes due to various system updates or performance degradation. More importantly, the combined use of these techniques permits the user to analyze the reasons for any changes to SIL values – by a careful read of the parameters for evaluation in the two techniques a detailed picture emerges that clearly points to the user the rationale for the changes.

7.2. Re-evaluation of SIG Labels

Claim softgoals are assumed to be satisficed (rows 1 to 4 of Table IX). However, what happens when additional evidence indicates that one or more of these assumptions are invalid? For example, if it is discovered in the future that SIS's EAL falls to low category due to poor manufacturing or performance degradation, then 'Medium EAL' claim softgoal is not satisficed (or denied). In that case, the contribution which this claim justifies (the HELP contribution between SIS and EAL) will also be affected. That is, the propagation rule R12 (see Appendix) will no longer be true (as assumed in row 7 of Table IX). In this case the label propagated by this contribution will be a modification of R12. It will become HURT (even though SIS is still satisficed) and, therefore, the final label for EAL will be weakly denied (W-) by propagation rule R11.

Similarly, this evidence for SIS means that contributions to LOPA and Reliability NFR softgoals may also be weakened to HURT, which means the labels for both LOPA and Reliability become W- (by propagation rules R4 and R11, respectively).

This means the label for Security NFR softgoal will become W- (by rule R9) and so will the label for Safety NFR softgoal become W- (by rule R8). Consequently, the label for ISIL, the root NFR softgoal, becomes W- (again by rule R8), which corresponds to SIL level of 2, as indicated by correspondence between SIL and ISIL levels outlined in articles [41], [44]. Therefore, any change in our knowledge of the system can be immediately captured by the SIG and the current value of SIL may be updated by a renewed propagation of labels. The new information also includes changes in any of the rationale in Table VIII or modification of SIG itself by addition of new softgoals, labels, decompositions, and/or contributions.

7.3. Inconsistent Result Management

It is probable that the SIL evaluated by the risk graph analysis approach may not match the one evaluated by the NFR approach. This eventuality gives an excellent opportunity to study the system information in greater detail to understand reasons for this discrepancy. Two possibilities arise. In the sequential application of the techniques (as shown in Figure 9), there is a correction loop added, as shown in Figure 16.

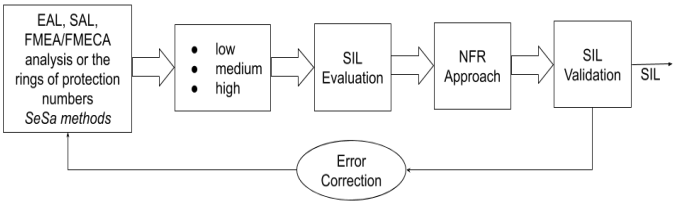

Fig. 16. Error correction for sequential application of the two techniques.

This means the reasons for SIL differences are identified and any corrections needed for re-evaluation are applied to both the risk graph approach and then the NFR approach, Hopefully, this re-evaluation produces consistent results else the loop is repeated. However, during each correction loop, greater information of the system is revealed and this helps to better understand the SIL values obtained. If the techniques are applied in parallel, then the correction loop becomes the one shown in Figure 17.

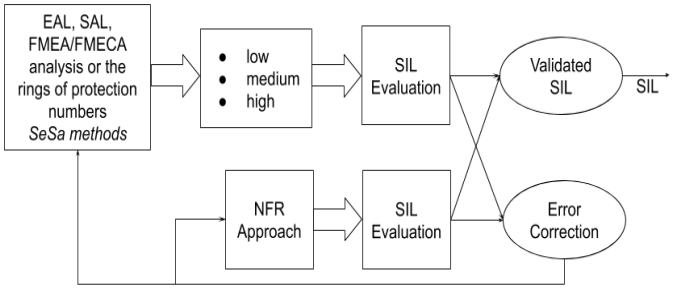

Fig. 17. Error correction for parallel application of the two techniques.

7.4. Concept of method validation

The reliability data used in the computation of the overpressure protection safety instrumented system (SIS) technical object was taken on the grounds of the authors' background as well as based on existing solutions, equipment producers' documents and reliability databases. The authors used experience based on realized Failure mode, effects, and criticality analysis FMECA of model control and protection systems. In terms of integrated functional safety and cybersecurity analysis in the context of determining the required safety integrity level SIL including cyber security aspects was based on the authors Risk Cube shown in Fig. 18 [45]. Authors Risk Cube approach integration of functional safety and cybersecurity issues at the risk analysis stage allows to validate the results of the integrated approach presented in this work.

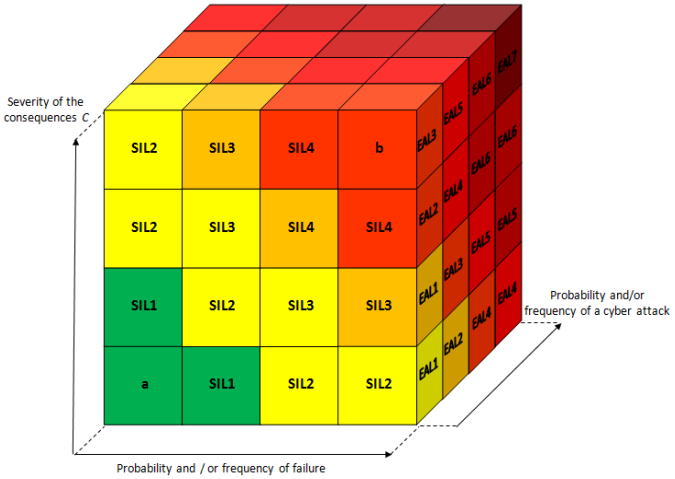

Fig. 18. Example Risk Cube SIL-EAL [45].

8. Conclusion

Dealing in an integrated and comprehensive way with the functional safety and cybersecurity analysis in critical installations is extremely important to increase resilience and remains a challenging issue. It is relatively common during the early stages of analysis to omit the security issues related to data communication and access restrictions to the system and its associated components. Nevertheless, these aspects, when neglected, may significantly impact safety and negatively influence the results of analysis. In this article, a methodology to integrate the functional safety and security issues was presented and outlined for the calculation of SIL's.

The article confirms that the proposed methodology, despite different approaches, generates coincident final results. It was proven from a case study that the statistical and reliability approach is adequate for NFR. Thus, this provides a basis for future comparative studies on the application of the proposed method to other cases oriented to critical infrastructure facilities, machinery, mining, nuclear and also automotive and aviation. In these times of increased hacking attacks on distributed control and safety systems, an integrated approach in functional safety and cyber security analysis is necessary. The proposed methodology complements existing approaches in this area. Another challenge will be to consider the impact of artificial intelligence (AI) on the functioning of control and safety systems in high-risk facilities.

The cybersecurity aspect is regarded as a risk factor in the analysis of functional safety. In some cases, the required SIL, associated strictly with the required level of risk reduction in

a plant facility, may be raised, particularly for distributed control systems, as they can be more vulnerable to internal and external threats. This problem is shown by the model of a modifiable risk graph with an additional risk characteristic which is directly related to a specific level of cybersecurity.

Presented in these article A new technique for determination of SIL's and its validation has been developed and proven to work, based on a combination of modifiable risk graphs, integrated with the NFR approach as a complementary technique. It also has to be said that there is a formal issue of verifying the SIL required for a safety related system that performs a specific safety function. This may be the subject of a separate study.

Work on the application of this approach in integrating safety and cybersecurity aspects for designing and operating programmable control and protection systems in industrial practice has been undertaken. The specific goal is to make it practical for use in complex systems. Another step in the evaluation of the proposed approach to safety and cybersecurity analysis is to consider a human operator as a factor.

Human aspects are an important part of every safety-critical system. Information from the alarm systems and process control systems goes to the human operator who interprets it. In determining functional safety requirements processes, the operator can be considered as an independent protection layer. In the future it could be included in the validation process. The challenge in that process is to integrate cybersecurity and human error according to the functional safety and the vast expansion requirements in the ongoing industrial revolution known as Industry 4.0

References

1. N. M. Pilanawithana, Y. Feng, K. London, P. Zhang, "Developing resilience for safety management systems in building repair and maintenance: A conceptual model", Safety Science, vol. 152, 2022, https://doi.org/10.1016/j.ssci.2022.105768.
2. D.-H. Ham, "Safety-II and Resilience Engineering in a Nutshell: An Introductory Guide to Their Concepts and Methods." Safety and Health at Work, vol. 12, pp. 10-19, 2021. https://doi.org/10.1016/j.shaw.2020.11.004
3. D. J. Provan, D. D. Woods, S. W. A. Dekker, A. J. Rae, "Safety II professionals: How resilience engineering can transform safety practice," Reliability Engineering and System Safety, vol. 195, https://doi.org/10.1016/j.ress.2019.106740
4. I, Ed-daoui, A. El Hami, M. Itmi, N. Hmina, T. Mazri, "Resilience assessment as a foundation for systems-of-systems safety evaluation: Application to an economic infrastructure." Safety Science, vol. 115, pp. 446–456, 2019, https://doi.org/10.1016/j.ssci.2019.02.030
5. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. IEC 61508, Geneva, 2010.
6. Functional safety: Safety Instrumented Systems for the Process Industry Sector. IEC 61511, Geneva, 2015.
7. J.H. Saleh, A.M. Cummings, "Safety in the mining industry and the unfinished legacy of mining accidents," Safety Science, vol. 49, pp. 764-777, 2011. https://doi.org/10.1016/j.ssci.2011.02.017
8. M. Śliwiński, E. Piesik, "Integrated functional safety and cybersecurity analysis," IFAC Papers OnLine, vol. 51, pp. 1263–1270, 2018. https://doi.org/10.1016/j.ifacol.2018.09.572
9. A.C. Torres-Echeverria, "Use of LOPA and risk graphs for determination of SIL," J. of Loss Prevention in the Process Industries, vol. 41, pp. 333-343, 2016. https://doi.org/10.1016/j.jlp.2015.12.007
10. A. Gabriel, C. Ozansoy, J. Shi, "SIL determination and calculation – new developments," Reliability Engineering and System Safety, vol. 177, pp. 148-161, 2018. https://doi.org/10.1016/j.ress.2018.04.028
11. Security for industrial automation and control systems. IEC 62443, Geneva, 2013.
12. Information technology -- Information security management systems – Overview and vocabulary. ISO/IEC 27000, Geneva, 2018.
13. S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, Y. Halgand, "Approaches combining safety and security for industrial control systems," Reliability Engineering and System Safety, vol. 139, pp. 156–178, July 2015. https://doi.org/10.1016/j.ress.2015.02.008
14. J. Braband, "What's Security Level got to do with Safety Integrity Level?" Proc. ERTS 2016, Toulouse, France, January 27-29, 2016.
15. E. Piesik, M. Śliwiński, T. Barnert, "Determining the safety integrity level of systems with security aspects," Reliability Engineering and System Safety, vol. 152, pp. 259-272, 2016. https://doi.org/10.1016/j.ress.2016.03.018
16. M. Śliwiński, "Verification of safety integrity level for safety-related functions enhanced with security aspects," Process Safety and Environmental Protection, vol. 118, pp. 79-92, 2018. https://doi.org/10.1016/j.psep.2018.06.016

17. N. Subramanian, J. Zalewski, “Quantitative Evaluation of Safety and Security in Cyberphysical Systems Using NFR Approach,” IEEE Systems Journal, vol. 10, no. 2, pp. 397-409, 2016. https://doi.org/10.1109/JSYST.2013.2294628
18. N. Subramanian, J. Zalewski, ”Use of the NFR Approach to Safety and Security Analysis of Control Chains in SCADA,” IFAC Papers OnLine, vol. 51, no. 6, pp. 214–219, 2018. https://doi.org/10.1016/j.ifacol.2018.07.156
19. K.T. Kosmowski, ”A methodology for functional safety and reliability analysis in hazardous industrial plants,” GUT, Gdansk, 2013.
20. T. Aven, ”A Framework for Risk Analysis Covering both Safety and Security,” Rel. Engineering & Systems Safety, vol. 92, pp. 745-754, 2007. https://doi.org/10.1016/j.ress.2006.03.008
21. S. Chockalingam et al., ”A Survey of Integrated Safety and Security Risk Assessment Methods.” Proc. CRITIS 2016, Paris, October 10–12, 2016, pp. 50-62. https://doi.org/10.1007/978-3-319-71368-7_5
22. F. Reichenbach et al., ”Pragmatic Approach to Joint Safety and Security Risk Analysis.” Proc. 2012 IEEE 23rd Intern. Symposium on Software Reliability, Dallas, Texas, November 27-30, 2012, pp. 239-244. https://doi.org/10.1109/ISSREW.2012.98
23. CYBER Methods and protocols. Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA). Technical Specs, ETSI TS 102 165-1. European Telecommunications Standards Institute, 2017.
24. S. Kriaa, Safety and Security Modeling for Joint Risk Assessment in Cyberphysical Systems. Ph.D dissertation, Université Paris-Saclay, Paris, France, 2016.
25. [25] H. Abdo et al., ”Safety and Security Risk Analysis Approach to Industrial Control Systems,” Computers and Security, vol. 72, pp. 175-195, 2018. https://doi.org/10.1016/j.cose.2017.09.004
26. Y. Chen et al., ”Unified Security and Safety Risk Assessment – A Case Study on Nuclear Power Plants.” Proc. TSA 2014, Taichung, Taiwan, June 9-10, 2014, pp. 22-28. https://doi.org/10.1109/TSA.2014.13
27. Guide for Conducting Risk Assessments. Report NIST SP 800-30 Rev. 1, NIST, Gaithersburg, MD, September 2012.
28. Z. Ji, S.-H. Yang, Y. Cao, Y. Wang, C. Zhou, L. Yue, Y. Zhang, “Harmonizing safety and security risk analysis and prevention in cyber-physical systems,” Process Safety and Environmental Protection, vol. 148, pp. 1279–1291, 2021. https://doi.org/10.1016/j.psep.2021.03.004
29. T. Oueidat, J.-M, Flaus, F. Massé, “A review of combined safety and security risk analysis approaches,” Proc. ICCAS 2020, International Conference on Control, Automation and Diagnosis, Paris, Oct. 7-9, 2020. https://doi.org/10.1109/ICCAD49821.2020.9260512
30. X. Lyu, Y. Ding, S.-H. Yang, “Safety and security risk assessment in cyberphysical systems,” IET Cyber-Physical Systems: Theory & Applications, vol. 4, issue 3, pp. 221-232, 2019. https://doi.org/10.1049/iet-cps.2018.5068
31. W. Goble, H. Cheddie, Safety instrumented systems verification: Practical probabilistic calculations. ISA, 2015.
32. T.O. Grøtan, M.G. Jaatun, K. Øien, T. Onshus, The SeSa Method for Assessing Secure Access to Safety Instrumented Systems, Report SINTEF A1626. Trondheim, 2007.
33. SESAMO. Security and Safety Modelling. Artemis JU Grant Agreement 295354, April 2014.
34. Railway applications – Safety related communication in transmission systems. IEC 62280, Geneva, 2014.
35. Information technology Security techniques – Evaluation criteria for IT security. ISO/IEC 15408, Geneva, 1999.
36. P. Gruhn, H.L. Cheddie, Design, Analysis and Justification of Safety Instrumented Systems. 2nd Edition. ISA, 2006.
37. D.J. Smith, Reliability, Practical Methods for Maintainability and Risk. 9th Edition. Elsevier, London, 2017.
38. L. Chung, B.A. Nixon, E. Yu, J. Mylopoulos, Software Engineering with Non-Functional Requirements in Software Engineering, Kluwer, Boston, Mass., 2000. https://doi.org/10.1007/978-1-4615-5269-7
39. H.A. Simon, ”Rational Choice and the Structure of the Environment”, Psychological Review, vol. 63, no. 2, pp. 129-138, 1956. https://doi.org/10.1037/h0042769
40. N. Subramanian, J. Zalewski, ”Safety and Security Integrated SIL Evaluation Using the NFR Approach,” Integrating Research and Practice in Software Engineering, Springer, 2020, pp. 53-68. https://doi.org/10.1007/978-3-030-26574-8_5
41. E. Piesik, M. Śliwiński, T. Barnert, ”Determining and verifying the SIL of the safety instrumented systems with security aspects,” Reliability Engineering and System Safety, vol. 152, pp. 259-272, 2016. https://doi.org/10.1016/j.ress.2016.03.018
42. P. Hildebrandt, Critical aspects of safety, availability and communication in subsea gas pipelines, HIMA, 2000.
43. SINTEF. Reliability Data for Safety Instrumented Systems. PDS Data Handbook. SINTEF, Trondheim, 2010.

44. M. Śliwiński, K. Kosmowski, E. Piesik, “Current issues of the functional safety and cyber security analysis of the industrial and critical infrastructures,” Task Quarterly, vol. 23, no. 2, pp. 209-232, 2019.
45. M. Śliwiński, E. Piesik, “Designing Control and Protection Systems with Regard to Integrated Functional Safety and Cybersecurity Aspects.” ENERGIES, 14, pp. 2227-2250, 2021, https://doi.org/10.3390/en14082227