energies

Article

Designing Control and Protection Systems with Regard to Integrated Functional Safety and Cybersecurity Aspects

Marcin Śliwiński and Emilian Piesik *

Faculty of Electrical and Control Engineering, Gdańsk University of Technology, 80-233 Gdansk, Poland;
marcin.sliwinski@pg.edu.pl
* Correspondence: emilian.piesik@pg.edu.pl

Abstract: This article addresses current problems of risk analysis and probabilistic modelling for functional safety management in the life cycle of safety-related systems. Two main stages in the lifecycle of these systems are distinguished, namely the design and operation. The risk analysis and probabilistic modelling differ in these stages in view of available knowledge and data. Due to the complexity and uncertainty involved, both qualitative and quantitative information can be useful in risk analysis and probabilistic modelling. Some methodological aspects of the functional safety assessment are outlined that include modelling of dependent failures or cybersecurity and verifying the safety integrity level (SIL) under uncertainty. It is illustrated how the assumptions in the process of risk analysis and probabilistic modelling influence results obtained and, therefore, potentially the decisions taken in functional safety management. Programmable control and safety systems play an important role in mitigating and controlling risks in the operation of hazardous installations. This paper presents ways to deal with safety hazards involving such systems to be considered in risk analysis and integrated functional safety and cybersecurity management.

Keywords: functional safety; cybersecurity; risk cube; SIL; determination; verification; SIS

Citation: Śliwiński, M.; Piesik, E. Designing Control and Protection Systems with Regard to Integrated Functional Safety and Cybersecurity Aspects. *Energies* **2021**, *14*, 2227. https://doi.org/10.3390/en14082227

Academic Editor: Ali Mehrizi-Sani

Received: 1 March 2021
Accepted: 14 April 2021
Published: 16 April 2021

1. Introduction

Emerging threats have significant potential to destructively impact the operation of technical systems, hazardous facilities, and critical infrastructure systems or networks. Therefore, the risks of major accidents with severe consequences that can happen in hazardous industrial plants have to be systematically assessed and properly managed across the entire life cycle [1–3]. Safety and security issues are two different groups of functional requirements for industrial systems. It is one of the main causes that the analyses of safety and cybersecurity should not be integrated directly. They should be integrated with one of the specified approaches Common Criteria approach, SecureSafety (SeSa) methodology, the Ring protection model, and ISO-IEC 62443 standard technology. The guidelines and specified information of this method are presented in publications [1,2]. This article presents one of the proposed approaches that consists of integrated analysis safety and security in probabilistic modelling in the safety integrity level verification process. This integrated methodology has limited application in information technology (IT) applications, but has a lot of opportunities in operational technologies (OT) application. The proposed integrated approach is useful in the engineering design process control as well as in protection systems. Of course, it can also be used in all life cycles of critical installations. It is clear that automation systems in process installations have integral systematic proof tests, and the most sophisticated construction of the safety control systems. These systems are the most vulnerable to cyber-attacks via an industrial computer network.

One of the main objectives of functional safety analysis is determining the required safety integrity level (SIL) for the safety-related functions to be realized by safety-related systems. According to IEC 61508, to each SIL (1 ÷ 4) the interval probabilistic quantitative criterion is defined. Functional safety analysis procedure usually does not include security aspects. In the case of a distributed control and protection system, it can have practical significance, and may affect the results of determination as well as verifying SIL, taking into account functional safety analysis [1,2].

An important part of the safety and security management system is the functional safety and security sub-system. Its purpose is to reduce some risks using safety-related technology of the programmable control and protection systems, such as electric/electronic/programmable electronic (E/E/PE) systems [4] or safety instrumented systems (SISs) [5]. These systems are applied for implementing defined safety-related functions (SRF) and are characterized by appropriate configuration/architecture to fulfil relevant safety integrity requirements.

If the layers of protection in a hazardous plant have to be applied due to high risk, then the layer of protection analysis (LOPA) is of interest [6,7]. In such a plant, an alarm system (AS) should be properly designed to include a relevant human-system interface. An important issue is to design a safety-related decision support system. This article addresses some methodological issues of the functional safety and security analysis and management in hazardous plants, as well as those in which the layer of protection according to defense in depths (DinD) concept is applied in industrial installation [5]. Cybersecurity factors contribute positively to maintaining the high reliability and productivity of industrial plants [8,9]. If these factors are not properly considered and shaped in practice, they can influence the system negatively, either before or during abnormal situations and potential accidents [1].

We emphasize that the functional safety and cybersecurity management in a life cycle should be treated as a complex interdisciplinary problem with a number of coordinated tasks requiring integration of relevant knowledge and data from various sources using suitable and effective methods with regard to uncertainty issues [8,10]. Some important areas of functional safety analysis and management are identified that require additional research effort to develop more integrated methods and tools (next-generation) that would support functional safety analysts, designers, and users of functional safety technology in a more compatible way [11,12]. The results of this effort would be valuable for functional safety specialists [13], who face methodological difficulties, such as designers or operators in the industry [14–16].

2. Issues of Determining the Required Safety Integrity Level of Safety Functions

2.1. Functional Safety Requirements

The SIL of given safety-related functions (SRF) is presented by numbers 1 to 4 and is bound to the needed risk reduction when the SRF is implemented in regard to IEC standards [1]. The assignment of safety requirements to protection function using the E/E/PE, and other technologies (Figure 1) [4,17].

For safety functions implemented using the safety-related system two types of interval probabilistic criteria are defined in the IEC 61508 standard given (Table 1) for two modes of operation [4,5]:

- the probability of failure (average) PFD_{avg} for the safety function system operating on demand; or
- the frequency (probability of a dangerous failure per hour) *PFH*.

Table 1. SIL probabilistic criteria.

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

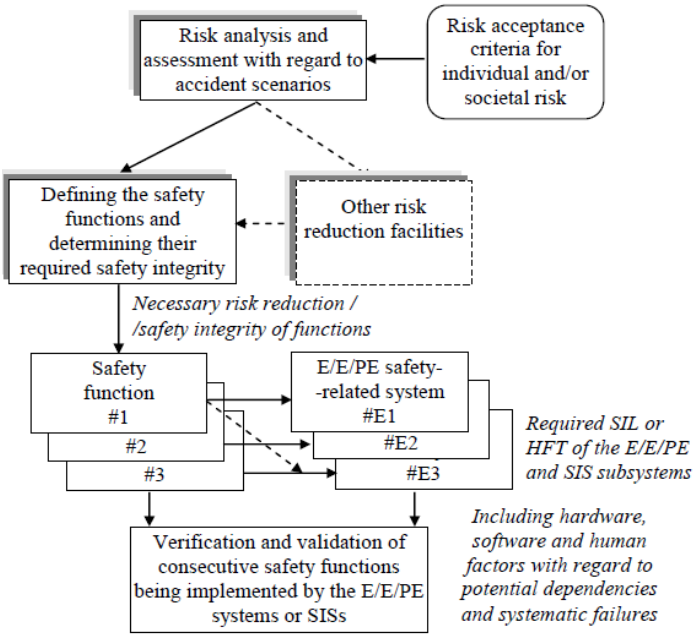
Risk analysis and assessment with regard to accident scenarios
Risk acceptance criteria for individual and/or societal risk
Defining the safety functions and determining their required safety integrity
Other risk reduction facilities
Necessary risk reduction / /safety integrity of functions
Safety function #1
#2
#3
E/E/PE safety--related system #E1
#E2
#E3
Required SIL or HFT of the E/E/PE and SIS subsystems
Verification and validation of consecutive safety functions being implemented by the E/E/PE systems or SISs
Including hardware, software and human factors with regard to potential dependencies and systematic failures

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

The typical configuration of a safety system (Figure 2) that consists of three subsystems, generally of koon configuration: (A) sensors, (B) safety PLC (Programmable Logic Controller), and (C) final elements.

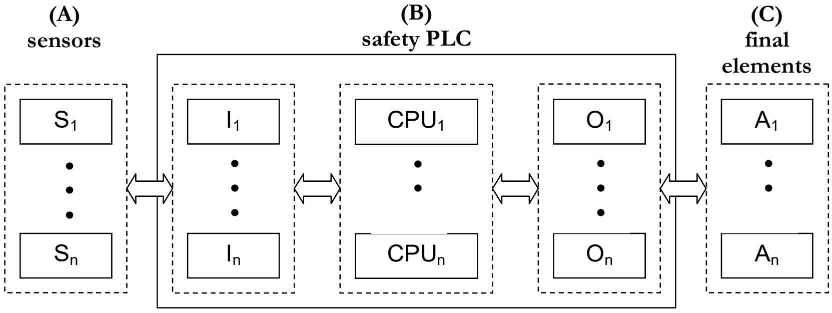

Figure 2. General configuration of a safety system (**A**)—sensors, (**B**)—safety PLC, (**C**)—final elements.

The risk of potential hazardous events can be rationally reduced in the context of evaluated categories of the frequency of unwanted occurrence (*W*) and consequences (*N*) (Table 2) [4]. The total probability of safety system failure for the case considered has to be reduced to the value shown on the right side of the arrow ↓ (to obtain reduced frequency (*F*) of given category from a to d). As shown, the required SIL level of the defined safety function to be implemented depends on the possibility of failing to avoid a hazardous event using other safety measures (x, y, or *z* as described below Table 2) [17]. In cases denoted as b a single SIS is not enough, and an additional protection layer has to be designed.

The risk matrix defined (Table 2) can be modified, e.g., to take into account some societal values and an aversion to major accidents with serious consequences. It would change SIL requirements to be assigned to the E/E/PE or SIS (increased SIL—high consequences), or the necessity to design an additional safety layer.

To fulfil requirements of a higher SIL (3 or 4) assigned to the safety function the appropriate configuration of the E/E/EP system or SIS is to be designed, e.g., 1oo2, 2oo3, or 2oo4.

Table 2. Example of an extended risk matrix for determining safety integrity level.

Categories: **Fatality →** **Frequency ↓**	$\mathbf{N_A}$ $(10^{-3}, 10^{-2}]$ **Injury**	$\mathbf{N_B}$ $(10^{-2}, 10^{-1}]$ **More Injuries**	$\mathbf{N_C}$ $(10^{-1}, 1]$ **Single Fatality**	$\mathbf{N_D}$ **(1, 10]** **Several Fatalities**	$\mathbf{N_E}$ $(10, 10^2]$ **Many Fatalities**
W_3 $[a^{-1}]$, F^d (1, 10] Frequent	a	$SIL3^x$ $SIL2^y$; $\downarrow 10^{-3}$ $SIL1^x$	$SIL4^z$ $SIL3^y$; $\downarrow 10^{-4}$ $SIL2^x$	b^z $SIL4^y$; $\downarrow 10^{-5}$ $SIL3^x$	b^z b^y b^x
W_2 $[a^{-1}]$, F^c $(10^{-1}, 1]$ Probable		$SIL2^z$ $SIL1^y$; $\downarrow 10^{-2}$ a^x	$SIL3^z$ $SIL2^y$; $\downarrow 10^{-3}$ $SIL1^x$	$SIL4^z$ $SIL3^y$; $\downarrow 10^{-4}$ SIL2x	b^z $SIL4^y$; $\downarrow 10^{-5}$ $SIL3^x$
W_1 $[a^{-1}]$, F^b $(10^{-2}, 10^{-1}]$ Occasional		$SIL1^z$ a^y; $\downarrow 10^{-1}$	$SIL2^z$ $SIL1^y$; $\downarrow 10^{-2}$ a^x	SIL3x $SIL2^y$; $\downarrow 10^{-3}$ $SIL1^x$	$SIL4^z$ $SIL3^y$; $\downarrow 10^{-4}$ $SIL2^x$
W_0 $[a^{-1}]$, F^a $(10^{-3}, 10^{-2}]$ Seldom			$SIL1^z$ a^y; $\downarrow 10^{-1}$	$SIL2^z$ $SIL1^y$; $\downarrow 10^{-2}$ a^x	$SIL3^x$ $SIL2^y$; $\downarrow 10^{-3}$ $SIL1^x$

2.2. *Cybersecurity Approach*

In cybersecurity there are two main approaches: Evaluation Assurance Level (EAL) and Security Assurance Level (SAL). Evaluation Assurance Level (EAL) based on Common Criteria standard [18], with EAL1 the minimal requirements to EAL7 high requirements. Each Evaluation Assurance Level can be described as: EAL1- functionally tested; EAL2—structurally tested; EAL3—methodically tested and checked; EAL4—methodically tested, designed and reviewed; EAL5—semi-formally designed and tested; EAL6—semi-formally verified design and tested; EAL7—formally verified design and tested [18].

Another approach to cybersecurity evaluation for industrial control systems (ICS) is IEC 62443 [3]. A definition of Security Assurance Level (SAL) has been introduced in this standard. There are four security levels (SAL1 to 4) and they are assessed for a given security zone using a set of 7 functional requirements (Table 3).

Table 3. Cybersecurity levels (SAL).

SAL1	Protection against casual or coincidental violation
SAL2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation
SAL3	Protection against intentional violation using sophisticated means with moderate resources, system-specific skills and moderate motivation
SAL4	Protection against intentional violation using sophisticated means with extended resources, system-specific skills, and high motivation

The SAL is a cybersecurity measure concerning industrial control systems ICS. It is evaluated on a defined vector of seven requirements for a relevant cybersecurity zone [3]:

$$SAL = \{AC, UC, DI, DC, RDF, TRE, RA\} \tag{1}$$

where: *AC*—identification control, *UC*—use control, *DI*—data integrity *DC*—data confidentiality, *RDF*—restricted data flow, *TRE*—timely response, *RA*—resource availability.

Results of a cybersecurity analysis of a given industrial control system can be divided into some general categories, for example, a qualitative description with defined cybersecurity levels such as: low, medium, or high-level of cybersecurity [9]. The EAL [18] or SAL [3] determined for a given solution is taken into account during the functional safety analysis (Table 4) [9].

Table 4. Levels of cybersecurity (EALs and SALs).

Evaluation Assurance Level	Security Assurance Level	Cybersecurity
EAL1	SAL1	Low
EAL2	SAL1	Low
EAL3	SAL2	Medium
EAL4	SAL2	Medium
EAL5	SAL3	High
EAL6	SAL4	High
EAL7	SAL4	High

Due to the nature of threats and known vulnerabilities the security risk assessment shall be event-driven or under periodic cybersecurity review [19]. The possible effects of a security risk(s) (Figure 3) in this context to a safety-related control system [19,20].

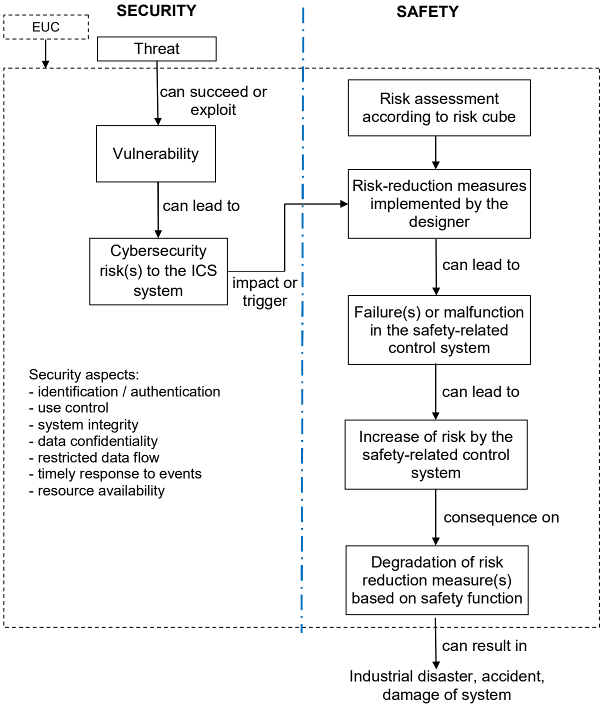
SECURITY
SAFETY
EUC
Threat
can succeed or exploit
Vulnerability
can lead to
Cybersecurity risk(s) to the ICS system
impact or trigger
Security aspects:
- identification / authentication
- use control
- system integrity
- data confidentiality
- restricted data flow
- timely response to events
- resource availability
Risk assessment according to risk cube
Risk-reduction measures implemented by the designer
can lead to
Failure(s) or malfunction in the safety-related control system
can lead to
Increase of risk by the safety-related control system
consequence on
Degradation of risk reduction measure(s) based on safety function
can result in
Industrial disaster, accident, damage of system

Figure 3. Relationship between functional safety and cybersecurity of ICS systems [19,20].

The safety risk assessment should be made in advance of any cybersecurity risk considerations [19]. The results: inherently safe design measures and safeguarding and risk reduction measures of a machine should then be analyzed regarding possible vulnerabilities against cyber-attacks (threats). The following are guidelines for the step-by-step approach to limit or restrict IT security threats and vulnerabilities [19,20].

Requirements concerning cybersecurity-related aspects will be considered regarding the requirements of a series of international standards, IEC 62443 [3], IEC, 63074 [20], ISO/IEC 15408 [18], ISO/IEC 27000 [21], ISO/IEC 27001 [22] and ISO/IEC 27005 [23]. In general, a security risk assessment is based on a product/system in its environment to which threats and known vulnerabilities are applied [24]. This activity aims to define relevant (counter) measures to fulfil the overall security objectives [24–27].

Some of the risk factors to be taken into account when carrying out this type of analysis have an impact on the estimated value of the frequency or likelihood of some of the consequences [28]. The risk is defined as:

$$R = F \times C \tag{2}$$

where the frequency F of occurrence of some scenario associated with certain consequences C is dependent on several factors, including the reliability of technical solutions used in the analyzed system [9].

Analyzing such a system in terms of cybersecurity can result in detecting the existence of certain vulnerabilities, which may increase the risks associated with the overall system. In most cases, this will result in increasing the frequency of occurrence of a certain scenario, therefore, assuming that the consequences are C = const. Then, it can be said that:

$$F^{\Uparrow} \to R^{\Uparrow} \Leftrightarrow V^{\Uparrow} \tag{3}$$

The system vulnerability can be measurable and expressed by the level of security, taking into account the countermeasures introduced to the system which may mitigate these vulnerabilities [11,27]. Considering the stage of identifying hazards in the system, which is a very important part of defining the required safety-related functions, there is a need for determining the possible causes, consequences, and frequency of occurrence for every described hazard or scenario [29].

2.3. The Risk Cube Methodology

The vulnerability of a system can be measurable and expressed through the level of information protection taking into account the countermeasures put in place to mitigate this vulnerability [1,30].

The risk of human, environmental and economic losses in the functional safety analysis is determined by taking into account the identified environmental hazards and technical disturbances (internal disturbances caused by human errors or external disturbances from the industrial installation).

In a broader perspective, the complementary analysis of information security should take into account threats related to the unfriendly intentions of intruders located inside or outside a given facility, as well as possible terrorist activities under certain conditions [1,2]. The risk measure R_{ij} in the annual period and for the i-th threat and the j-defined emergency scenario in the considered facility/system is proposed to be determined in accordance with the formula:

$$R_{ij} = f_i \cdot V_{ij} \cdot C_{ij} \tag{4}$$

where: f_i—frequency of occurrence of the i-th hazard situation (an event initiating an abnormal emergency situation) due to the intentional action; V_{ij}—the vulnerability of a given object, expressed by the conditional probability that the i-th level of effects, emergency for this hazard situation, will occur; C_{ij}—a measure of the consequences (e.g., human, environmental or economic losses) resulting from the emergency event under consideration; economic risk has a monetary unit value per year.

The vulnerability can be reduced by using appropriate technical (security rings, security technologies) and organisational solutions (e.g., training programs, procedures in the security management system). The risk is similarly defined in the context of functional safety:

$$R_{kj} = f_k \cdot PFD_{kj} \cdot C_{kj} \tag{5}$$

where: f_k—the frequency of k-th risk situation due to internal or external interference; PFD_{kj}—the probability of failure to perform the safety-related function on demand for the system of the j-th level of effect; PFD_{kj} is determined based on models in reference to the requirements of the general standard IEC 61508 or sector standard IEC 61511.

Based on (4) and (5), assuming the additionality of the risk measures, the measure of aggregate risk associated with j-th level of effect can be estimated from the relationship:

$$R_j = \sum_i R_{ij} + \sum_k R_{kj} \tag{6}$$

The determined risk measures can be used in the analysis of costs and effects of the proposed solutions of security systems, including layers of protection and ring ones, for functional safety and information security solutions, respectively. The practical importance, but also the challenge of developing new methods of risk analysis and assessment for the integrated functional safety and information security management of computer control and protection systems in conditions of usually high uncertainty should be stressed [9,31].

Table 5 contains a risk matrix on specific issues related to industrial network cybersecurity and its impact on the operation of the critical infrastructure system. The risk degree of R_{cs} (cs—cybersecurity) in a given case is related to the security assurance level SAL.

Table 5. Risk Matrix Regarding Cybersecurity Issues at the Critical Infrastructure Facility.

The Degree of Risk R_{cs} and the Associated Security Assurance Level SAL		**Probability and/or Frequency of a Cyber-Attack**			
		Low	**Medium**	**High**	**Very High**
Severity of the consequences C	catastrophic	medium R_{cs} SAL2	high R_{cs} SAL3	very high R_{cs} SAL4	very high R_{cs} SAL4
	critical	medium R_{cs} SAL2	high R_{cs} SAL3	very high R_{cs} SAL4	very high R_{cs} SAL4
	marginal	low R_{cs} SAL1	medium R_{cs} SAL2	medium R_{cs} SAL2	high R_{cs} SAL3
	minor	low R_{cs} SAL1	low R_{cs} SAL2	medium R_{cs} SAL2	high R_{cs} SAL3

Table 6 presents a risk matrix regarding information security issues in the critical infrastructure facility [2]. The degree of risk R_{sec} (low, medium, high, or very high) in a given case is related to the evaluation assurance level EAL.

Table 6. Risk Matrix Regarding Information Security Issues in a Critical Infrastructure Facility.

The Degree of R_{sec} Risk and the Associated Evaluation Assurance Level EAL		**Probability and/or Frequency of a Cyber-Attack**			
		Low	**Medium**	**High**	**Very High**
Severity of the consequences C	catastrophic	medium R_{sec} EAL3	high R_{sec} EAL5	very high R_{sec} EAL6	very high R_{sec} EAL7
	critical	medium R_{sec} EAL2	medium R_{sec} EAL4	very high R_{sec} EAL6	very high R_{sec} EAL6
	marginal	low R_{sec} EAL1	medium R_{sec} EAL3	high R_{sec} EAL5	high R_{sec} EAL5
	minor	low R_{sec} EAL1	low R_{sec} EAL2	medium R_{sec} EAL4	medium R_{sec} EAL4

The next table (Table 7) presents the risk matrix regarding functional safety issues. The degree of risk R_{fs} (fs—functional safety) in a given case is referenced in safety integrity level SIL.

Table 7. Risk Matrix for Functional Safety Issues.

R_{fs} Risk and Associated SIL Safety Integrity Level		**Probability and/or Frequency of Failure**			
		Low	**Medium**	**High**	**Very High**
Severity of the consequences C	catastrophic	medium R_{fs} SIL2	high R_{fs} SIL3	very high R_{fs} SIL4	very high R_{fs} b
	critical	medium R_{fs} SIL2	high R_{fs} SIL3	very high R_{fs} SIL4	very high R_{fs} SIL4
	marginal	low R_{fs} SIL1	medium R_{fs} SIL2	high R_{fs} SIL3	high R_{fs} SIL3
	minor	very low R_{fs} a	low R_{fs} SIL1	medium R_{fs} SIL2	medium R_{fs} SIL2

Assuming that the criticality of consequences for functional safety and cybersecurity impacts are the same C_{fs} = C_{cs} = C, the integration can be presented as a Risk Cube.

The proposed integration of functional safety and cybersecurity issues at the risk analysis stage (Figures 4 and 5).

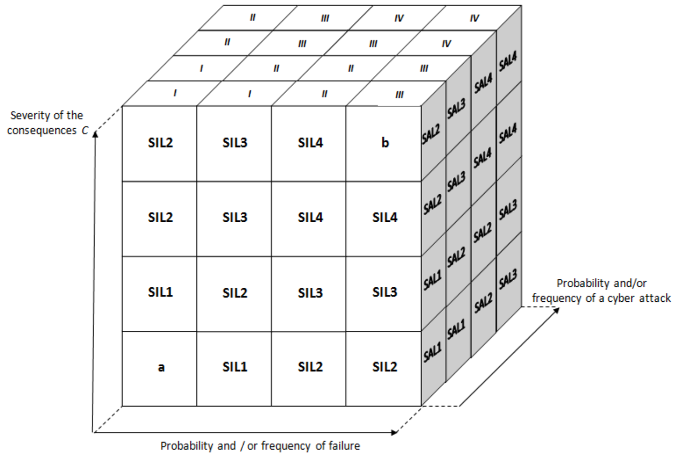

Figure 4. Risk Cube (SIL-SAL).

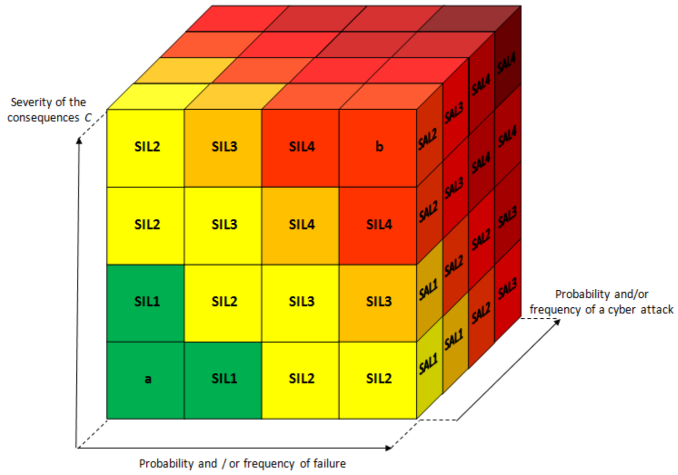

Figure 5. Risk Cube SIL-SAL (col.).

In this case:

$$\begin{aligned} &R = R_{fs} + R_{cs} = \\ &= C_{fs} \cdot P_{fs}\left(or\ F_{fs}\right) + C_{cs} \cdot P_{cs}\left(or\ F_{cs}\right) = \\ &= C \cdot P\left(or\ F\right) \end{aligned} \tag{7}$$

Assuming that C_{fs} = C_{cs} = C:

$$R = C \cdot \left(P_{fs}\left(or\ F_{fs}\right) + P_{cs} \cdot \left(or\ F_{cs}\right)\right) \tag{8}$$

where: R—risk; R_{fs}—risk related to functional safety aspects; R_{cs}—risk related to cyber threats; C—criticality of effects; C_{fs}—criticality of consequences related to functional safety aspects; C_{cs}—criticality of consequences related to cyber threats; P_{fs}—the probability of failure; P_{cs}—the probability of a cyber-attack; F_{fs}—frequency of failure; F_{cs}—frequency of a cyber-attack.

As above, functional safety and information security issues (expressed through the evaluation assurance level EAL) are integrated. Assuming that the criticality of consequences for functional safety and information security are the same C_{fs} = C_{sec} = C, the integrated approach is presented in Figures 6 and 7 (Risk Cube (SIL-EAL)).

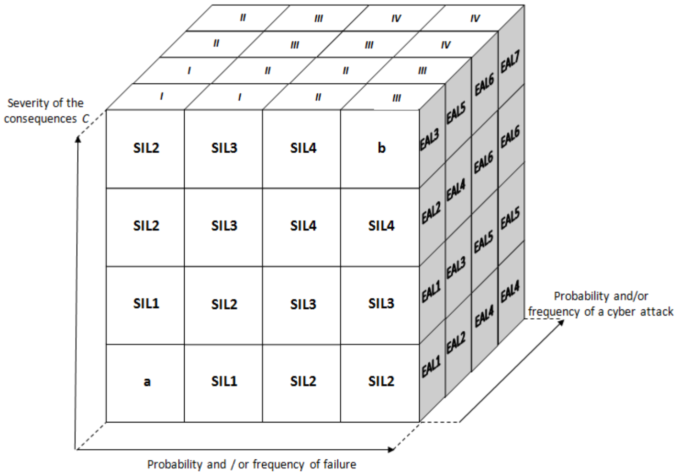

Figure 6. Risk Cube (SIL-EAL).

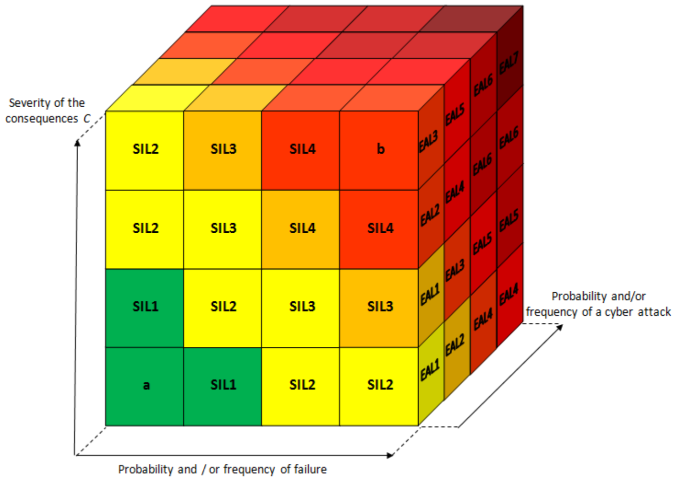

Figure 7. Risk Cube SIL-EAL (col.).

In this case:

$$\begin{aligned} R &= R_{fs} + R_{sec} = \\ &= C_{fs} \cdot P_{fs}\left(or\ F_{fs}\right) + C_{sec} \cdot P_{sec}\left(or\ F_{sec}\right) = \\ &= C \cdot P\left(or\ F\right) \end{aligned} \tag{9}$$

Assuming that C_{fs} = C_{sec} = C:

$$R = C \cdot \left(P_{fs}\left(or\ F_{fs}\right) + P_{sec} \cdot \left(or\ F_{sec}\right)\right) \tag{10}$$

Taking into account the definition of risk as a combination of the frequency or probability of the occurrence of a failure event and the consequences of that event, a simplified method is proposed below to determine the required SIL, taking into account information security and cybersecurity aspects.

Such an analysis is based on data obtained in the process of hazard identification occurring in the technical system, as well as an estimation of the level of risk associated with them. Some of the risk factors taken into account in carrying out such analysis have an impact on the estimated value of frequency or probability [30]. The part of the risk related to frequency parameters most often concerns the issues of hardware reliability [32,33].

In the process of integration of functional safety issues with information security, the concept of the so-called two-parameter function can be used [2]. If a low level of information security is estimated in the critical infrastructure system under consideration, the SIL requirements for the safety function may change. For the SIL requirements to remain unchanged, it becomes necessary to reduce the risks associated with the level of information security [34]. This involves raising the cybersecurity requirements (e.g., higher EAL level) for the system under analysis.

2.4. SIL Determining with Cybersecurity Aspects

The functional safety and cybersecurity goals are now the input to derive functional safety and security requirements [11,35]. Both of those factors are responsible for the final level of security taken into account in the functional safety risk assessment process (Figure 8).

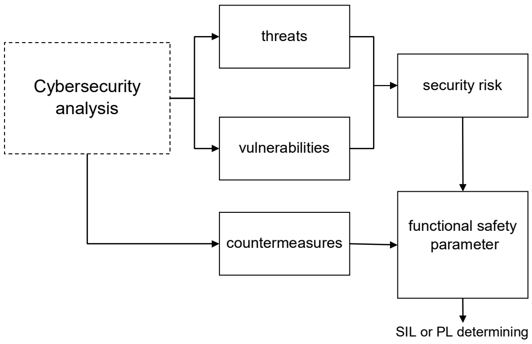

Figure 8. Procedure using cybersecurity factors in safety analysis [13].

The SIL or PL is determined based on several quantitative factors in conjunction with qualitative factors during the process of development and safety life cycle management. There are several methods to determine the SIL or PL for a chosen safety function. Some of the popular ones include: Risk Matrix, Risk Graph [4,5,11,26,30].

A general scheme of considering the security analysis results in the SIL or PL determining process is important to present the approach (Figure 9).

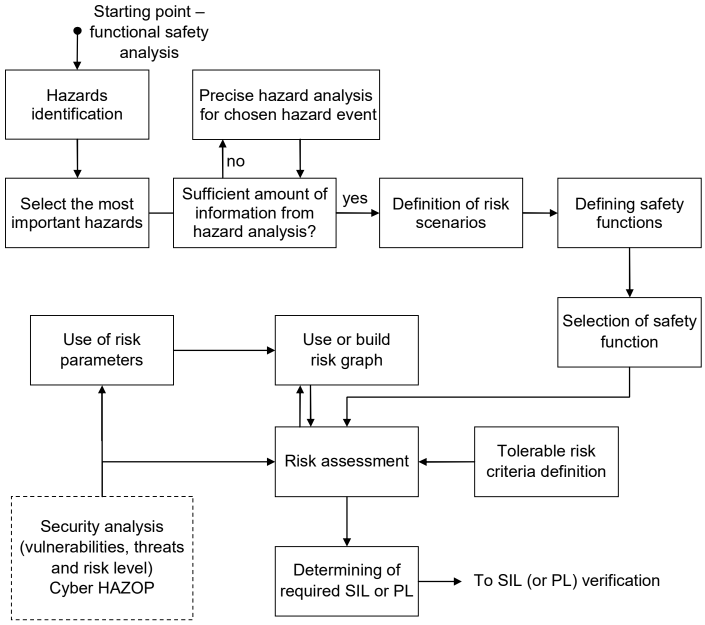
Starting point – functional safety analysis
Hazards identification
Precise hazard analysis for chosen hazard event
no
Select the most important hazards
Sufficient amount of information from hazard analysis?
yes
Definition of risk scenarios
Defining safety functions
Selection of safety function
Use of 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 or PL
To SIL (or PL) verification

Figure 9. The procedure of SIL or PL determining the cybersecurity aspects.

3. Safety Integrity Level Calculation

3.1. Probabilistic Modelling of Safety-Related Subsystems

The quantitative method based on the reliability block diagram (RBD) is used for verifying SIL. The probability of failure to perform the design safety function on demand can be evaluated the following formula:

$$\begin{aligned} &PFD(t) \cong \left(1 - e^{-\lambda_{\mathrm{D}} \cdot t}\right) \cong \\ &\cong 1 - 1 + \lambda_{\mathrm{D}} \cdot t - \tfrac{\lambda_{\mathrm{D}}^2 \cdot t^2}{2!} + \tfrac{\lambda_{\mathrm{D}}^3 \cdot t^3}{3!} + \ldots \\ &when\ \lambda_{\mathrm{D}} \cdot t << 1 \\ &PFD(t) \cong \left(1 - e^{-\lambda_{\mathrm{D}} \cdot t}\right) \cong \lambda_{\mathrm{D}} \cdot t \end{aligned} \tag{11}$$

where: λ_{D}—dangerous failure rate; t—time.

The average probability, assuming that all subsystems are tested with the T_{I}, is calculated as formula (12) [4]:

$$PFD_{\mathrm{avg}} = \frac{1}{T_{\mathrm{I}}} \int_0^{T_{\mathrm{I}}} PFD(t) dt \tag{12}$$

where: T_{I}—test interval.

The frequency of a dangerous failure can be evaluated based on a formula as shown below:

$$\begin{aligned} &PFH \cong \tfrac{F(t)}{t} \underset{t \in (0,T)}{\Rightarrow} \tfrac{F(T)}{T} \cong \tfrac{1 - R(T)}{T} = \\ &= 1 - \frac{\exp\left(-\int_0^T \lambda(t)\, dt\right)}{T} = \frac{1 - \exp\left(-\lambda_{\mathrm{avg}} \cdot T\right)}{T} \\ &when\ \lambda_{\mathrm{avg}} \cdot T << 1 \\ &PFH \cong \tfrac{\lambda_{\mathrm{avg}} \cdot T}{T} = \lambda_{\mathrm{avg}} \end{aligned} \tag{13}$$

where: λ_{avg}—average failure rate; T—time interval.

The architecture of equipment performing the safety function is represented by block diagrams distinguishing between subsystems and modules [36,37]. An example of the physical form of the E/E/PE system structure (BPCS or SIS) is shown in Figure 10.

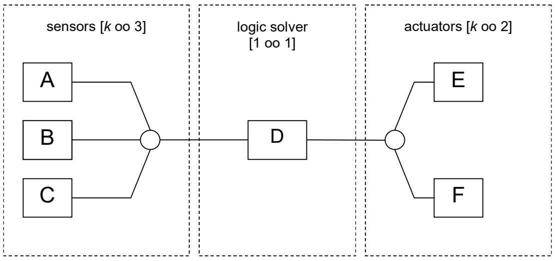

Figure 10. Example structure of the E/E/PE system (SIS or BPCS).

There are three subsystems in the E/E/PE BPCS or SIS: sensors, logic solvers, and actuators. The presented structure consists of three sensors A, B, C configuration koo3, logical subsystem D (e.g., PLC), and actuators E and F (koo2).

Figure 11 shows an example of the structure of an E/E/PE or SIS system in the form of a reliability block diagram, assuming that the sensors subsystem has a configuration 1oo3 and the actuators subsystem a configuration 1oo2.

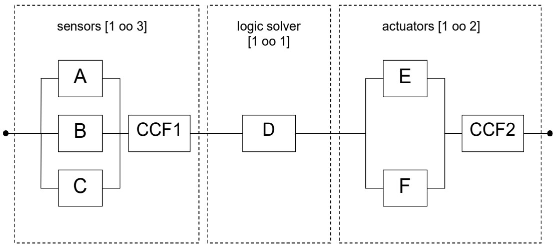

Figure 11. Reliability block diagram RBD of an example E/E/PE or SIS system structure.

In the above diagram the common cause failure (CCF) for the sensors' subsystem from elements A, B and C and for the actuators' subsystem CCF2 from elements E and F is considered [4,36,38]. In the system from Figure 10, five minimum cuts can be distinguished: {A, B, C}; {CCF1}; {D}; {E, F}; {CCF2}

Figure 12 shows the E/E/PE or SIS system fault tree from Figure 11 including the common cause failure.

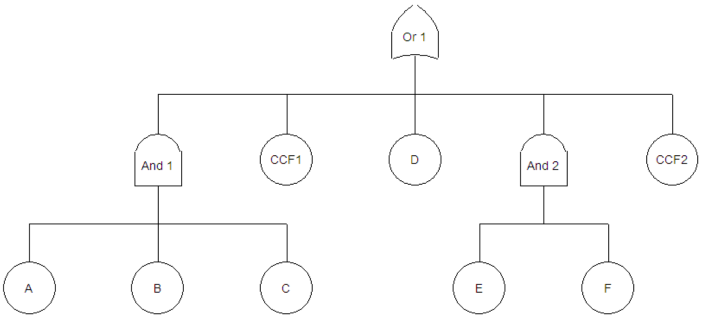

Figure 12. Fault tree for SIS system.

The average probability of failure on demand safety function for the system in Figure 11 can be determined from the sum of the probabilities for the individual subsystems.

$$PFD_{\text{avg}} \cong PFD_{\text{avg}}^{\text{ABC}} + PFD_{\text{avg}}^{\text{CCF1}} + PFD_{\text{avg}}^{\text{D}} + PFD_{\text{avg}}^{\text{EF}} + PFD_{\text{avg}}^{\text{CCF2}} \tag{14}$$

Similarly, the average frequency of a dangerous failure per hour *PFH* (for the system operating in high demand or continuous mode) can be determined as:

$$PFH \cong PFH^{\text{ABC}} + PFH^{\text{CCF1}} + PFH^{\text{D}} + PFH^{\text{EF}} + PFH^{\text{CCF2}} \tag{15}$$

An example of the programmable electronic system with two channels (Figure 13) [4].

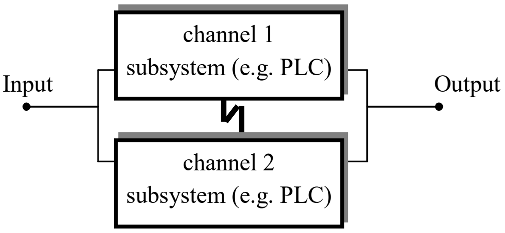

Figure 13. Programmable electronic system with two channels.

If the potential common cause failures were not included in the probabilistic evaluation of the system, the safety integrity level of the entire system would be incorrectly determined (or verified) [32,35–38]. The illustration of the contribution of common cause failures to the failures of individual channels and the entire 1oo2 system (Figure 14).

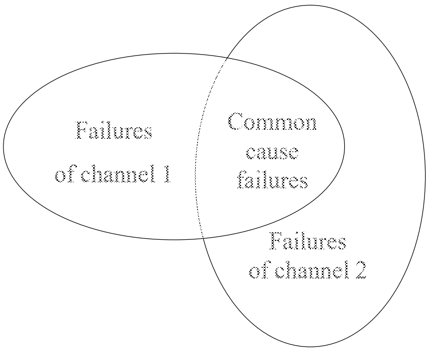

Figure 14. Contribution of common cause failures to the failures of individual channels and the entire 1oo2 system [4,36,38].

The β factor method is usually used in the modelling of potential common cause failures. The β factor method (Figure 15) can be also used to estimate the rate of the common cause failures, applicable to two channels operating in parallel with regard to the random hardware failures of these two channels [37,38].

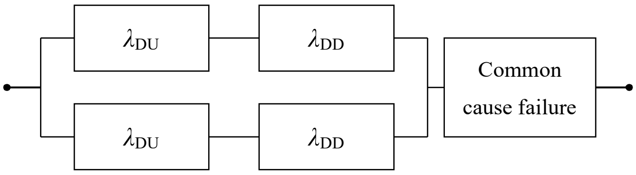

Figure 15. Reliability block diagram for 1oo2 E/E/PE system.

The channel equivalent mean downtime t_{CE} is evaluated from the equation [4]:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_I}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{16}$$

where: t_{CE}—a channel equivalent mean downtime for 1oo2 architecture; λ_D—dangerous failure rate; λ_{DD}—dangerous detected failure rate; λ_{DU}—dangerous undetected failure rate; T_I—proof test interval; MTTR—mean time to repair.

The voted group equivalent mean downtime t_{GE} is expressed from the equation:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_I}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{17}$$

where t_{GE}—the voted group equivalent mean downtime for 1oo2 architecture.

Taking into account Equations (16) and (17), the relations for the average probability of failure on demand for the 1oo2 architecture system is as follows:

$$PFD_{\text{avg}1oo2} \cong 2 \cdot [(1-\beta)\,\lambda_D]^2 t_{CE} \cdot t_{GE} + \beta \cdot \lambda_{DU}\left(\frac{T_I}{2} + MTTR\right) \tag{18}$$

where: β—factor for common cause failure.

$$PFH_{1oo2} \cong 2 \cdot [(1-\beta)\,\lambda_D]^2 t_{CE} + \beta \cdot \lambda_{DU} \tag{19}$$

The failure rate λ of a system with an excess structure koon, consisting of n different elements, can be presented as the sum of the average independent failure rate λ_{Iavg} and the dependent failure rate λ_C

$$\lambda = \lambda_{\text{Iavg}} + \lambda_C \tag{20}$$

where: λ_{Iavg}—average independent failure rate; λ_C—dependent failure rate.

The β factor takes the form:

$$\beta = \frac{\lambda_C}{\lambda_C + \lambda_{Iavg}} = \frac{\lambda_C}{\lambda} \tag{21}$$

Using formulas (20) and (21), the dependent failure rate can be described by the equation:

$$\lambda_C = \beta \cdot \lambda \tag{22}$$

The average independent failure rate λ_{Iavg} can be presented by the formula:

$$\lambda_{Iavg} = \frac{\sum\limits_{i=1}^{n} \lambda_{Ii}}{n} = \frac{\sum\limits_{i=1}^{n} (1-\beta)\lambda_i}{n} \tag{23}$$

where: λ_{Ii}—average independent failure rate for a single i-th element; n—number of elements.

Taking into account formulas (22) and (23), the dependent failure rate λ_C can be described as follows:

$$\begin{gathered} \lambda_C = \frac{\beta \cdot \lambda_{Iavg}}{(1-\beta)} = \frac{\beta\left(\frac{\sum\limits_{i=1}^{n} \lambda_{Ii}}{n}\right)}{(1-\beta)} = \frac{\beta\left(1-\beta)(\frac{\sum\limits_{i=1}^{n} \lambda_i}{n}\right)}{(1-\beta)} \\ \lambda_C = \beta\left(\frac{\sum\limits_{i=1}^{n} \lambda_i}{n}\right) \end{gathered} \tag{24}$$

Considering the average value of the independent failure rate $\lambda_{Iavg}{}^{g}$ as the geometric mean, the dependent failure rate can be determined from the formula below:

$$\begin{gathered} \lambda_{C^g} = \frac{\beta \cdot \lambda_{Iavg}{}^{g}}{(1-\beta)} = \frac{\beta \cdot \sqrt[n]{\lambda_{I1} \cdot \lambda_{I2} \cdot \ldots} \cdot \lambda_{In}}{(1-\beta)} = \\ = \frac{\beta \cdot (1-\beta) \cdot \sqrt[n]{\lambda_1 \cdot \lambda_2 \cdot \ldots} \cdot \lambda_n}{(1-\beta)} \\ \lambda_{C^g} = \beta \cdot \sqrt[n]{\lambda_1 \cdot \lambda_2 \cdot \ldots} \cdot \lambda_n \end{gathered} \tag{25}$$

The general β model is presented above. It is essential to take into account the common cause of failure in the constructed model. When the system will be composed of the same elements, the above formulas will be reduced to the form presented in the equations describing the case for identical elements. For the determination of the base value β for configuration 1oo2, the IEC 61508-6 score boards may be used [4].

3.2. Examples of Functional Safety Analysis with Cybersecurity

The high-pressure tank with liquid gas is considered, equipped with the E/E/PE safety-related system. The piping and instrumentation diagram (P&ID) with a safety loop of the protection system (Figure 16).

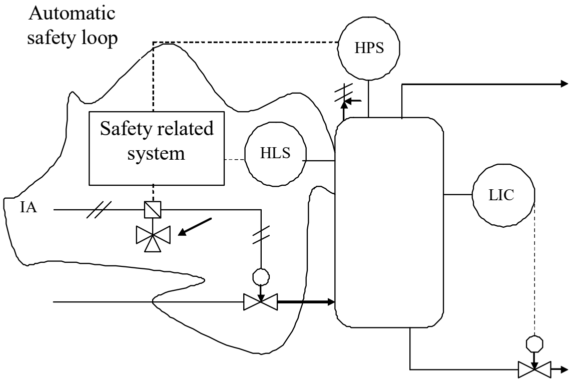

Figure 16. P&ID of a high-pressure tank.

The E/E/PE safety-related system protecting the high-pressure tank should fulfil the requirement, according to the risk analysis results, of the safety integrity level SIL3 [10^{-4}, 10^{-3}) (Table 1). This system consists of the subsystems: the sensor, logic solver, and final element Figure 17.

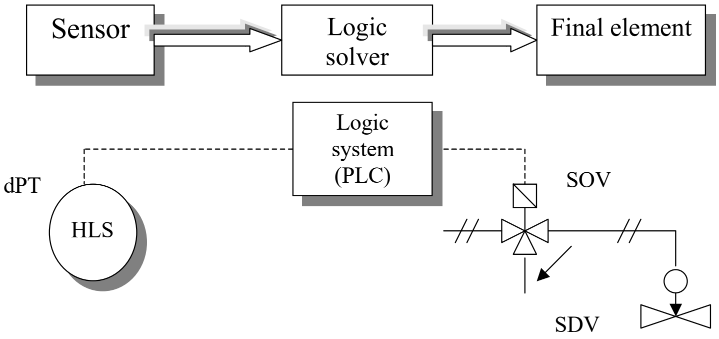

Figure 17. Automatic safety-related loop of E/E/PES.

In Figure 17. dPT—the pressure converter; I/I—the transducer, PLC—the programmable logic controller; SOV—the solenoid open valve; SDV—the shutdown valve; HLS—the high-level sensor.

Table 8 shows the data assumed for the automatic safety function considered. The initial calculations showed that for a single sensor in this system it is not possible to fulfil the requirement of SIL3.

Table 8. Reliability data.

Subsystem	dPT	I/I	PLC	SDV	SOV
λ_{DU} [h^{-1}]	2.24×10^{-7}	1.1×10^{-7}	5.2×10^{-11}	1×10^{-7}	1.14×10^{-8}
T_I [y]	1	1	1	1	1

Therefore, two paths of a sensor–converter (redundant architecture 1oo2) were then considered. The results (Table 9) of PFD_{avg} are given for modified E/E/PE system with redundant sensors and different β factors assumed.

According to the results obtained, the E/E/PE safety-related system fulfils the criterion of SIL3. Taking into account the different values of β factor for the pressure converter dPT and transducer I/I, the results vary significantly. For instance, for β = 0.05 the value of PFD_{avg} for the sensor subsystem changes by an order of magnitude, and β = 0.1 PFD_{avg} the change is two orders of magnitude.

Table 9. Results for different β factor for redundant E/E/PE system.

Subsystem	***PFDavg***		
	$\beta = 0$	$\beta = 0.05$	$\beta = 0.1$
dPT (1oo2)	1.28×10^{-6}	5.02×10^{-5}	9.92×10^{-5}
I/I (1oo2)	3.09×10^{-7}	2.44×10^{-5}	4.84×10^{-5}
PLC	2.28×10^{-7}	2.28×10^{-7}	2.28×10^{-7}
SDV	4.38×10^{-4}	4.38×10^{-4}	4.38×10^{-4}
SOV	4.99×10^{-5}	4.99×10^{-5}	4.99×10^{-5}
System	5.38×10^{-4}	5.63×10^{-4}	6.36×10^{-4}
SIL	3	3	3

When the cybersecurity error failure event and related beta factor will be incorporated into the probabilistic model $PFD_{\text{avg}}{}^{\text{CS}} = 0.01$), the value of PFD_{avg} for the E/E/PE system changes significantly [39,40]. For the case of $\beta = 0.1$, it is about 2×10^{-3}. Taking into account the last column of Table 10 with PFD_{avg} treated as the previous case, the SIL level of an E/E/PE system decreased from SIL3 to SIL2. Thus, incorporating dependency of events to the probabilistic model of the E/E/PE system usually increases significantly the PFD_{avg} contributing to decreasing related SIL.

Table 10. Reliability data.

	PS	**TS**	**DI**	**CPU**	**DO**	**V**
λ **[h^{-1}]**	4×10^{-6}	2×10^{-6}	1.2×10^{-6}	2.2×10^{-6}	6.5×10^{-7}	1.6×10^{-6}
***FS* [%]**	50%	50%	50%	50%	50%	50%
λ_D **[h^{-1}]**	2×10^{-6}	1×10^{-6}	5.46×10^{-7}	1.04×10^{-6}	3.1×10^{-7}	6.5×10^{-7}
λ_S **[h^{-1}]**	2×10^{-6}	1×10^{-6}	5.46×10^{-7}	1.04×10^{-6}	3.1×10^{-7}	6.5×10^{-7}
***DC* [%]**	90%	90%	90%	90%	90%	90%
λ_{DD} **[h^{-1}]**	1.8×10^{-6}	9×10^{-7}	4.91×10^{-7}	9.38×10^{-7}	2.79×10^{-7}	5.85×10^{-7}
λ_{DU} **[h^{-1}]**	2×10^{-7}	1×10^{-7}	5.46×10^{-8}	1.04×10^{-7}	3.1×10^{-8}	6.5×10^{-8}
λ_{SD} **[h^{-1}]**	1.8×10^{-6}	9×10^{-7}	4.91×10^{-7}	9.38×10^{-7}	2.79×10^{-7}	5.85×10^{-7}
λ_{SU} **[h^{-1}]**	2×10^{-7}	1×10^{-7}	5.46×10^{-8}	1.04×10^{-7}	3.1×10^{-8}	6.5×10^{-8}
***MTTR* [h]**	8	8	8	8	8	8
T_I **[y]**	1	1	1	1	1	1
β	0.02	0.02	0.02	0.02	0.02	0.02

The contribution of probabilities described above on the average failure probability on demand PFD_{avg} is shown in Figure 18. In this figure, T_{AT} is the interval of periodic automatic tests of a subsystem and T_{I} is the interval to carry out the functional tests of a subsystem.

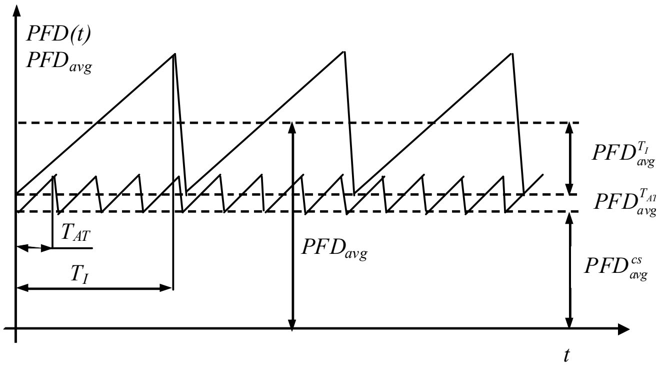

Figure 18. Elements of the average probability of an E/E/PE subsystem failure on demand.

In this figure, T_{AT} is the interval of periodic automatic tests of a subsystem and T_{I} is the interval to carry out the functional tests of a subsystem.

4. Verification of SIL under Uncertainty

As mentioned, for verifying the SIL the results of probabilistic modelling of the E/E/PE safety-related system are to be compared with the probabilistic criteria given in Table 1. In practice, these results are often the point values and, in some cases, can have values just on the upper/lower limits of intervals for consecutive SILs.

The results from a probabilistic model depend on its parameters, which in general are characterized by uncertainty, expressed by a distribution or interval. PFD_{avg} is averaged in time, not for uncertain parameters of the model.

The results of probabilistic modelling can be represented by intervals (Figure 19) by the bold interval. In general, such an interval can be fuzzy, having some interesting properties. A method to verify uncertain results with fuzzy interval criteria is proposed in the monographs [1,2].

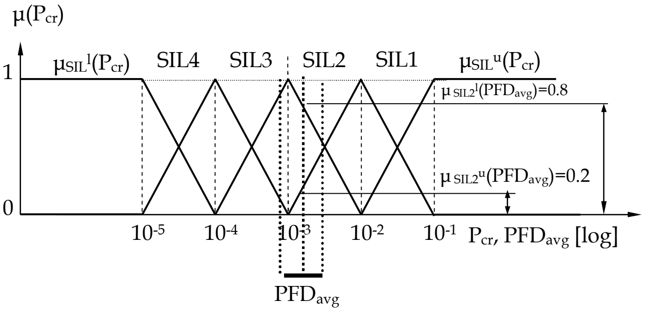

Figure 19. Verification of safety integrity level for a point value of PFD_{avg}.

Below, a proposal is outlined for simplified verification of SIL for given E/E/PE system for the case when only point value of PFD_{avg} is known but uncertainty issue will be incorporated in the verifying process through a more conservative determination of SIL. For instance, the point value of PFD_{avg} was compared with fuzzy criteria values, l—lower and u—upper, (Figure 19) represented using the relevant membership function of a fuzzy criterion (for the given SIL), respectively $\mu_{\mathrm{SIL}}{}^{1}(P_{\mathrm{cr}})$ and $\mu_{\mathrm{SIL}}{}^{\mathrm{u}}(P_{\mathrm{cr}})$.

In this figure, if we consider, for instance, SIL2, $\mu_{\mathrm{SIL2}}{}^{1}(PFD_{\mathrm{avg}})$ as the possible level to fulfil SIL2 lower limit probabilistic criterion; $\mu_{\mathrm{SIL2}}{}^{\mathrm{u}}(PFD_{\mathrm{avg}})$—the possibility level) to fulfil SIL2 upper limit probabilistic criterion. When $\mu_{\mathrm{SIL1}}(PFD_{\mathrm{avg}})$ and $\mu_{\mathrm{SIL}}{}^{\mathrm{u}}(PFD_{\mathrm{avg}})$ are equal to 0.5 the SIL level is indicated unconditionally. When the $\mu_{\mathrm{SIL2}}{}^{1}(PFD_{\mathrm{avg}})$ and $\mu_{\mathrm{SIL2}}{}^{\mathrm{u}}(PFD_{\mathrm{avg}})$ are close to 0 or 1 (lower/upper limits of the probability interval), the SIL is determined conservatively (lower level of SIL assumed) or additional analysis is undertaken concerning assumptions and sensitivity analyses of the probabilistic model.

PFD_{avg} in formula (12) for a subsystem of the given architecture is calculated e.g., according to formula (18). If the value of probability PFD_{avgSYS} is lower than a relevant probabilistic criterion value for given SIL (Table 1), then the designed safety-related system is considered as fulfilling this criterion.

The structure (Figures 20 and 21) of three E/E/PE safety-related systems that consist of subsystems: the pressure sensors (PS) of architecture (2oo3), the temperature sensors (TS) of architecture (2oo3), and valves (V) with redundancy (1oo2) and different structures of central processor unit (CPU), digital input modules (DI) and digital output modules (DO). In structure I the digital input module DI is 1oo2, CPU is 1oo1, and DO is 1oo1.

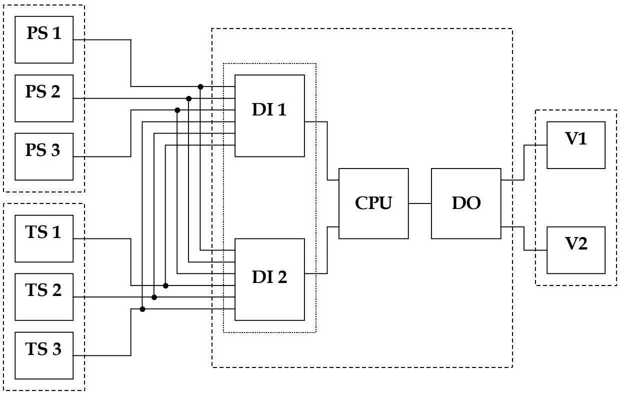

Figure 20. The structure I of E/E/PE safety-related system.

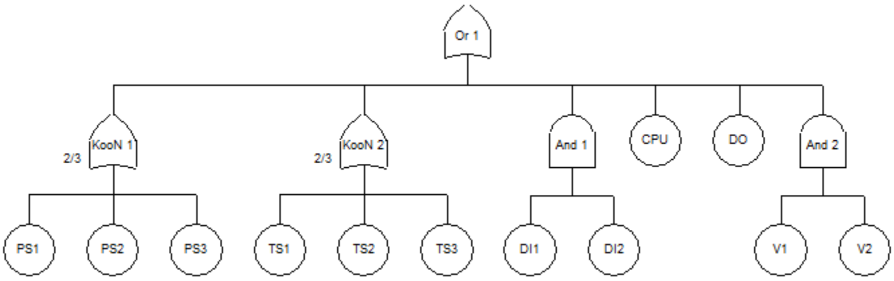

Figure 21. FT structure I model of E/E/PE safety-related system.

For the system in Figure 20 there are 10 minimal cuts sets:

$K_1 = \{\mathrm{PS1}, \mathrm{PS2}\}, K_2 = \{\mathrm{PS1}, \mathrm{PS3}\}, K_3 = \{\mathrm{PS2}, \mathrm{PS3}\}, K_4 = \{\mathrm{TS1}, \mathrm{TS2}\}, K_5 = \{\mathrm{TS1}, \mathrm{TS3}\},$
$K_6 = \{\mathrm{TS2}, \mathrm{TS3}\}, K_7 = \{\mathrm{DI1}, \mathrm{DI2}\}, K_8 = \{\mathrm{CPU}\}, K_9 = \{\mathrm{DO}\}, K_{10} = \{\mathrm{V1}, \mathrm{V2}\}$

Therefore, the probability of *PFD*(t) takes the form:

$$\begin{aligned} PFD(t) \cong\ & q_{\mathrm{PS1}}(t) \cdot q_{\mathrm{PS2}}(t) + q_{\mathrm{PS1}}(t) \cdot q_{\mathrm{PS3}}(t) + q_{\mathrm{PS2}}(t) \cdot q_{\mathrm{PS3}}(t) + \\ & + q_{\mathrm{TS1}}(t) \cdot q_{\mathrm{TS2}}(t) + q_{\mathrm{TS1}}(t) \cdot q_{\mathrm{TS3}}(t) + q_{\mathrm{TS2}}(t) \cdot q_{\mathrm{TS3}}(t) + \\ & + q_{\mathrm{DI1}}(t) \cdot q_{\mathrm{DI2}}(t) + q_{\mathrm{CPU}}(t) + q_{\mathrm{DO}}(t) + q_{\mathrm{V1}}(t) \cdot q_{\mathrm{V2}}(t) \end{aligned} \quad (26)$$

where: *q*—the probability of failure on single elements in subsystem structure.

If the individual subsystems consist of the same elements, then the probability of *PFD*(*t*) is represented by the following relationship:

$$PFD(t) \cong 3 \cdot q_{\mathrm{PS}}(t)^2 + 3 \cdot q_{\mathrm{TS}}(t)^2 + q_{\mathrm{DI}}(t)^2 + q_{\mathrm{CPU}}(t) + q_{\mathrm{DO}}(t) + q_{\mathrm{V}}(t)^2 \quad (27)$$

Thus, for the example system in Figure 20, the average probability of failure PFD_{avg} to perform the safety-related function on demand is:

$$\begin{aligned} & PFD_{\mathrm{avg}} \cong 3\left((1-\beta_{\mathrm{PS}})\lambda_{\mathrm{D}^{\mathrm{PS}}}\right)^2\left(\tfrac{T_{\mathrm{I}}^2}{3} + T_{\mathrm{I}} \cdot MTTR_{\mathrm{PS}} + MTTR_{\mathrm{PS}}^2\right) + \\ & + \beta_{\mathrm{PS}} \cdot \lambda_{\mathrm{DU}^{\mathrm{PS}}}\left(\tfrac{T_{\mathrm{I}}}{2} + MTTR_{\mathrm{PS}}\right) + 3\left((1-\beta_{\mathrm{TS}})\lambda_{\mathrm{D}^{\mathrm{TS}}}\right)^2\left(\tfrac{T_{\mathrm{I}}^2}{3} + T_{\mathrm{I}} \cdot MTTR_{\mathrm{TS}} + MTTR_{\mathrm{TS}}^2\right) + \\ & + \beta_{\mathrm{TS}} \cdot \lambda_{\mathrm{DU}^{\mathrm{TS}}}\left(\tfrac{T_{\mathrm{I}}}{2} + MTTR_{\mathrm{TS}}\right) + \left((1-\beta_{\mathrm{DI}})\lambda_{\mathrm{D}^{\mathrm{DI}}}\right)^2\left(\tfrac{T_{\mathrm{I}}^2}{3} + T_{\mathrm{I}} \cdot MTTR_{\mathrm{DI}} + MTTR_{\mathrm{DI}}^2\right) + \\ & + \beta_{\mathrm{DI}} \cdot \lambda_{\mathrm{DU}^{\mathrm{DI}}}\left(\tfrac{T_{\mathrm{I}}}{2} + MTTR_{\mathrm{DI}}\right) + \lambda_{\mathrm{DU}^{\mathrm{CPU}}}\tfrac{T_{\mathrm{I}}}{2} + \lambda_{\mathrm{D}^{\mathrm{CPU}}} \cdot MTTR_{\mathrm{CPU}} + \lambda_{\mathrm{DU}^{\mathrm{DO}}}\tfrac{T_{\mathrm{I}}}{2} + \\ & + \lambda_{\mathrm{D}^{\mathrm{DO}}} \cdot MTTR_{\mathrm{DO}} + \left((1-\beta_{\mathrm{V}})\lambda_{\mathrm{D}^{\mathrm{V}}}\right)^2\left(\tfrac{T_{\mathrm{I}}^2}{3} + T_{\mathrm{I}} \cdot MTTR_{\mathrm{V}} + MTTR_{\mathrm{V}}^2\right) + \\ & + \beta_{\mathrm{V}} \cdot \lambda_{\mathrm{DU}^{\mathrm{V}}}\left(\tfrac{T_{\mathrm{I}}}{2} + MTTR_{\mathrm{V}}\right) \end{aligned} \quad (28)$$

The average frequency *PFH* dangerous failures for safety-related system continuous mode operation is described by the formula:

$$\begin{aligned} PFH \cong\ & 6\left(\left(1-\beta_{\mathrm{PS}}\right)\lambda_{\mathrm{D}^{\mathrm{PS}}}\right)^2\left(\tfrac{T_{\mathrm{I}}}{2}+MTTR_{\mathrm{PS}}\right)+\beta_{\mathrm{PS}}\cdot\lambda_{\mathrm{DU}^{\mathrm{PS}}}+\\ & +6\left(\left(1-\beta_{\mathrm{TS}}\right)\lambda_{\mathrm{D}^{\mathrm{TS}}}\right)^2\left(\tfrac{T_{\mathrm{I}}}{2}+MTTR_{\mathrm{TS}}\right)+\beta_{\mathrm{TS}}\cdot\lambda_{\mathrm{DU}^{\mathrm{TS}}}+\\ & +2\left(\left(1-\beta_{\mathrm{DI}}\right)\lambda_{\mathrm{D}^{\mathrm{DI}}}\right)^2\left(\tfrac{T_{\mathrm{I}}}{2}+MTTR_{\mathrm{DI}}\right)+\beta_{\mathrm{DI}}\cdot\lambda_{\mathrm{DU}^{\mathrm{DI}}}+\\ & +\lambda_{\mathrm{DU}^{\mathrm{CPU}}}+\lambda_{\mathrm{DU}^{\mathrm{DO}}}+2\left(\left(1-\beta_{\mathrm{V}}\right)\lambda_{\mathrm{D}^{\mathrm{V}}}\right)^2\left(\tfrac{T_{\mathrm{I}}}{2}+MTTR_{\mathrm{V}}\right)+\beta_{\mathrm{V}}\cdot\lambda_{\mathrm{DU}^{\mathrm{V}}} \end{aligned} \tag{29}$$

Similarly, as for structure I, the probability relationships for systems II and III were determined. Structure II consists of digital input modules DI with redundancy (1oo2), the processors CPU (2oo3), and the digital output module DO (2oo3).

Structure III consists of digital input modules DI with redundancy (1oo2), the processors CPU (1oo2), and the digital output module DO (1oo2). PFD_{avg} value for this E/E/PE safety-related system was calculated using the reliability data from Table 10 based on PDS Data Handbook. SINTEF [41].

Table 11 shows the results for different architectures of subsystems of the E/E/PE safety-related system considered.

Table 11. Result for different E/E/PE architectures.

	PS	TS	DI	CPU	DO	V
$PFD_{\mathbf{avg1oo1}}$	8.78×10^{-3}	4.39×10^{-3}	2.39×10^{-3}	4.57×10^{-3}	1.36×10^{-3}	2.85×10^{-3}
$PFD_{\mathbf{avg\ 1oo2}}$	2.76×10^{-4}	1.13×10^{-4}	$\mathbf{5.53 \times 10^{-5}}$	1.19×10^{-4}	2.96×10^{-5}	$\mathbf{6.76 \times 10^{-5}}$
$PFD_{\mathbf{avg\ 2oo3}}$	$\mathbf{4.77 \times 10^{-4}}$	$\mathbf{1.63 \times 10^{-4}}$	7.03×10^{-5}	$\mathbf{1.73 \times 10^{-4}}$	$\mathbf{3.45 \times 10^{-5}}$	8.88×10^{-5}
SIL$_{\mathbf{elem}}$	3	3	4	3	4	4
$PFD_{\mathbf{avgSYS}}$			$\mathbf{9.7 \times 10^{-4}}$			
SIL$_{\mathbf{SYS}}$			**3**			

The analyst can assess results (Table 11) PFD_{avgSYS} for various architectures of subsystems. However, special attention was paid to results relevant to the system structures in Figures 20, 22 and 23. The assessment of results obtained shows that for the structure on Figure 20 this value is equal to 2.41×10^{-3}, fulfilling the requirement of SIL2. For structure on Figure 21, the results for subsystems are shown in Table 11 in bold, and the resulting value for the system is 9.7×10^{-4}, fulfilling the requirement of SIL3. However, for the structure on Figure 22, this value is equal to 1.52×10^{-3}, fulfilling the requirement only of SIL2.

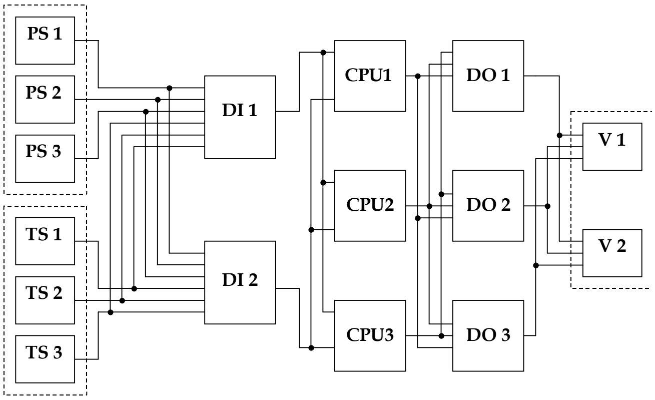

Figure 22. Structure II of E/E/PE safety-related system.

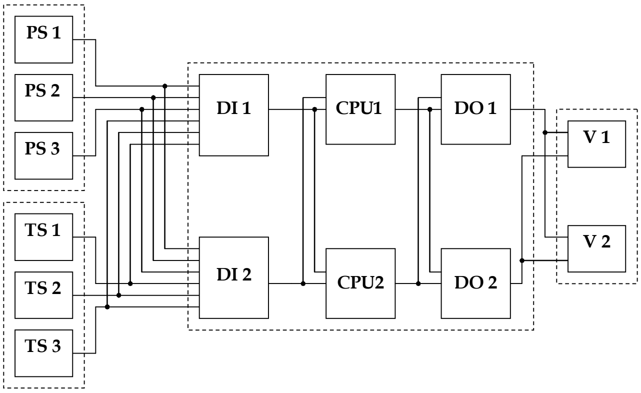

Figure 23. Structure III of E/E/PE safety-related system.

In PFD_{avg} calculation of the E/E/PE safety-related system, the point value near the upper/lower limit of the ranges (probabilistic criteria for SIL levels) can be obtained. For instance, for the structure in Figure 21 PFD_{avg} is equal to 9.7×10^{-4}, fulfilling formally the requirement of SIL3, but this value is near probabilistic criterion for SIL2. Similarly, for structure in Figure 22 PFD_{avg} is equal to 1.52×10^{-3} (SIL2), but the resulting value is near the probabilistic criterion for SIL3.

The PFD_{avg} for the safety-related system was calculated as a point value. In Figure 24 the PFD_{avg} point value was compared with SIL3 $[10^{-4}, 10^{-3})$ interval criterion. A lower factor $\mu_{\mathrm{SIL}}{}^{l}$ for SIL3 is equal to 0.2, but the upper factor $\mathrm{\mu_{SIL}}{}^{u}$ for SIL3 level is equal to 0.8.

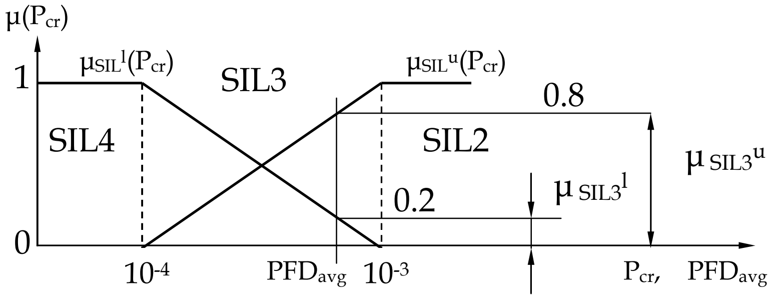

Figure 24. PFD_{avg} evaluation with membership function for SIL3 $[10^{-4}, 10^{-3})$ probabilistic criterion.

The result ($\mathrm{\mu_{SIL3}}{}^{l}$ = 0.2 and $\mathrm{\mu_{SIL3}}{}^{u}$ = 0.8) for the given PFD_{avg} value is useful for making an easier decision in regards to the SIL classification for the E/E/PE safety-related system considered.

5. Conclusions

Functional safety is an important element of 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 the 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 electrical and programmable electronic systems according to the requirements of the IEC 61508 and the IEC 61511 for safety instrumented systems (SIS).

In this paper, the concept of integrated functional safety and cybersecurity analysis is outlined with an emphasis on uncertainty factors. System safety depends on the quality of the industrial installation, which 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. The main task of cybersecurity is to protect the system against potential threats (internal and external) that compromise its assets and the environment. 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 impact safety, it is necessary to address them jointly.

Dealing in an integrated and comprehensive way with the functional safety and cybersecurity analysis in critical installations is extremely important 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 the 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 approach proposed is illustrated on an example of a critical installation. Comprehensive integration of the functional safety and cybersecurity analysis in installations critical infrastructures is very important and it is currently a challenging issue. There is also a challenge to include cybersecurity aspects in designing distributed industrial control systems (ICS).

Future works will focus on designed computer-aided functional safety and cybersecurity integrated analysis software. and there is a chance to include the human reliability analysis in the functional safety and cybersecurity integrity approach. The limitation, in that case, would be limited time for diagnosis and action (time-window) for human reaction to protect the systems. For that reason, layers of protection for safety and cybersecurity are implemented in the industrial installation.

Author Contributions: Conceptualization, M.Ś and E.P.; methodology, M.Ś.; validation, M.Ś.; formal analysis, E.P and M.Ś.; investigation, E.P.; resources, M.Ś.; writing—original draft preparation, M.Ś. and E.P.; writing—review and editing, E.P and M.Ś; visualization, E.P and M.Ś.; supervision, M.Ś. and E.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Gdańsk University of Technology.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kosmowski, K.T. *Functional Safety and Reliability Analysis Methodology for Hazardous Industrial Plants*; Gdansk University of Technology: Gdansk, Poland, 2013.
2. Śliwiński, M. *Functional Safety and Information Security in the Critical Infrastructure Systems and Objects*; Monographs 171; Gdansk University of Technology: Gdansk, Poland, 2018.
3. *Security for Industrial Automation and Control Systems*; IEC 62443; International Electrotechnical Commission: Geneva, Switzerland, 2013.
4. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*; IEC 61508; International Electrotechnical Commission: Geneva, Switzerland, 2010.
5. *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*; IEC 61511; International Electrotechnical Commission: Geneva, Switzerland, 2015.
6. *LOPA: Layer of Protection Analysis, Simplified Process Risk Assessment*; Center for Chemical Process Safety, American Institute of Chemical Engineers: New York, NY, USA, 2001.
7. Torres-Echeverria, A.C. On the use of LOPA and risk graphs for SIL determination. *J. Loss Prev. Process Ind.* **2016**, *41*, 333–343. [CrossRef]
8. Subramanian, N.; Zalewski, J. Quantitative Assessment of Safety and Security of System Architectures for Cyberphysical Systems Using NFR Approach. *IEEE Syst. J.* **2016**, *10*, 397–409. [CrossRef]
9. Śliwiński, M. Verification of safety integrity level for safety-related functions enhanced with security aspects. *Process Saf. Environ. Prot.* **2018**, *118*, 79–92. [CrossRef]

10. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. Approaches combining safety and security for industrial control systems. *Reliab. Eng. Syst. Saf.* **2015**, *139*, 156–178. [CrossRef]
11. Piesik, E.; Śliwiński, M.; Barnert, T. Determining the safety integrity level of systems with security aspects. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 259–272. [CrossRef]
12. Gabriel, A.; Ozansoy, C.; Shi, J. Developments in SIL determination and calculation. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 148–161. [CrossRef]
13. Śliwiński, M.; Piesik, E. Integrated functional safety and cybersecurity analysis. *IFAC Pap. OnLine* **2018**, *51*, 1263–1270. [CrossRef]
14. Saleh, J.H.; Cummings, A.M. Safety in the mining industry and the unfinished legacy of mining accidents. *Saf. Sci.* **2011**, *49*, 764–777. [CrossRef]
15. Subramanian, N.; Zalewski, J. Use of the NFR Approach to Safety and Security Analysis of Control Chains in SCADA. *IFAC Pap. OnLine* **2018**, *51*, 214–219. [CrossRef]
16. 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: Sophia Antipolis, France, 2017.
17. Kosmowski, K.T.; Śliwiński, M. Knowledge-based functional safety and security management in hazardous industrial plants with emphasis on human factors. In *Advanced Control and Diagnostic Systems*; PWNT: Gdańsk, Poland, 2015.
18. *Information Technology Security Techniques—Evaluation Criteria for IT Security*; ISO/IEC 15408; ISO: Geneva, Switzerland, 2009.
19. *Safety of Machinery—Guidance to Machinery Manufacturers for Consideration of Related IT Security (Cyber Security) Aspects*; ISO/DTR 22100; ISO: Geneva, Switzerland, 2018.
20. *Safety of Machinery—Security Aspects to Functional Safety of Safety-Related—Control Systems*; IEC TR 63074; International Electrotechnical Commission: Geneva, Switzerland, 2019.
21. *Information Technology—Information Security Management Systems—Overview and Vocabulary*; ISO/IEC 27000; ISO: Geneva, Switzerland, 2018.
22. *Information Technology, Security Techniques, Information Security Management Systems*; ISO/IEC 27001; ISO: Geneva, Switzerland, 2007.
23. *Information Technology, Security Techniques, Information Security Risk Management*; ISO/IEC 27005; ISO: Geneva, Switzerland, 2011.
24. Białas, A. *Semiformal Common Criteria Compliant IT Security Development Framework, Studia Informatica*; Silesian University of Technology Press: Gliwice, Poland, 2008.
25. *Risk Management—Guidelines*; ISO 31000; International Organization for Standardization: Geneva, Switzerland, 2018.
26. Braband, J. What's Security Level got to do with Safety Integrity Level? In Proceedings of the ERTS 2016, Toulouse, France, 27–29 January 2016.
27. Aven, T. A Framework for Risk Analysis Covering both Safety and Security. *Reliab. Eng. Syst. Saf.* **2007**, *92*, 745–754. [CrossRef]
28. Kanamaru, H. Bridging Functional Safety and Cyber Security of SIS/SCS. In Proceedings of the SICE Annual Conference 2017, Kanazawa University, Kanazawa, Japan, 19–22 September 2017.
29. Chockalingam, S.; Hadžiosmanović, D.; Pieters, W.; Teixeira, A.; van Gelder, P. A Survey of Integrated Safety and Security Risk Assessment Methods. In Proceedings of the CRITIS 2016, Paris, France, 10–12 October 2016; pp. 50–62.
30. Abdo, H.; Kaouk, M.; Flaus, J.M.; Masse, F. Safety and Security Risk Analysis Approach to Industrial Control Systems. *Comput. Secur.* **2018**, *72*, 175–195. [CrossRef]
31. *Guide for Conducting Risk Assessments*; Report NIST SP 800-30 Rev. 1; NIST: Gaithersburg, MD, USA, 2012.
32. Goble, W.; Cheddie, H. *Safety Instrumented Systems Verification: Practical Probabilistic Calculations*; ISA: Pittsburgh, PA, USA, 2015.
33. Smith, D.J. Reliability. In *Practical Methods for Maintainability and Risk*, 9th ed.; Elsevier: London, UK, 2017.
34. Subramanian, N.; Zalewski, J. Safety and Security Integrated SIL Evaluation Using the NFR Approach. In *Integrating Research and Practice in Software Engineering*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 53–68.
35. Kościelny, J.M.; Syfert, M.; Fajdek, B. Modern Measures of Risk Reduction in Industrial Processes. *J. Autom. Mob. Robot. Intell. Syst.* **2019**, *13*, 20–29. [CrossRef]
36. Hoyland, A.; Rausand, M. System Reliability Theory. In *Models and Statistical Methods*, 2nd ed.; John Wiley & Sons, Inc: Hoboken, NJ, USA, 2004.
37. Kumamoto, H. *Satisfying Safety Goals by Probabilistic Risk Assessment*; Springer Series in Reliability Engineering; Springer: London, UK, 2007.
38. Hokstad, P. A generalisation of the beta factor model. In Proceedings of the European Safety & Reliability Conference, Berlin, Germany, 14–18 June 2004.
39. Grøtan, T.O.; Jaatun, M.G.; Øien, K.; Onshus, T. *The SeSa Method for Assessing Secure Access to Safety Instrumented Systems*; Report SINTEF A1626; SINTEF: Trondheim, Norway, 2007.
40. SESAMO. *Security and Safety Modelling*; Artemis JU Grant Agreement 295354, April 2014; European Commission: Brussels, Belgium, 2014.
41. SINTEF. *Reliability Data for Safety Instrumented Systems*; PDS Data Handbook; SINTEF: Trondheim, Norway, 2010.