Advances in Reliability, Safety and Security, Part 10 – Kołowrocki, Kosmowski (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, *ISBN 978-83-68136-22-7 (printed), ISBN 978-83-68136-09-8 (electronic)*

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Functional Safety And Cybersecurity Of Industrial Automation And Control Systems

Kazimierz T. Kosmowski

Polish Safety and Reliability Association, Gdańsk, Poland

Abstract

This article is aimed at explaining the state of knowledge and research that concern an integrated functional safety and cybersecurity analysis for safety and security management in life cycle regarding selected references, standards and reports pertaining to the industrial automation and control systems in critical infrastructure installations. The objective is to explain how to mitigate the vulnerability of industrial systems, in particular converged operational technology and information technology, to reduce risks during the operation of hazardous plants. The risk criteria considered include the individual risk and/or the societal risk. They are defined using relevant risk graphs. The verification of safety integrity level to be achieved, for designed safety related control system of proposed architecture, is based on a set of probabilistic models and reliability data of components. Dependent failures and common cause failures are also included in probabilistic modelling. So called architectural constrains and also considered in the design process. The security assurance for the domain of interest is determined regarding a vector of fundamental requirements. The approach proposed enables determining and verifying the safety integrity level of defined safety functions, and then to verify the level obtained regarding the security assurance level of particular domain, in which a safety related control system is to be implemented. The approach proposed can be applied for designing the safety-related control systems and then during the operation of hazardous industrial plant. In final part of the workshop some additional requirements concerning the functional safety and cybersecurity solutions will be formulated pertaining to new technologies to be presumably more widely applied in Industry 5.0, such as control and safety functions that include the machine learning and artificial intelligence algorithms. Such technologies might significantly influence the resilience of hazardous installations and critical infrastructure. The resilience issue requires further research due to its importance for reliable and safe system operation in uncertain conditions. In final part of the paper some research topics to undertake are proposed.

Keywords: functional safety, cyber security, industrial automation, safety related control systems, information technology, operational technology, risk evaluation, safety life cycle management

1. Introduction

The article addresses selected issues of the integrated functional safety and cybersecurity evaluation regarding the functionality and architecture of industrial automation and control systems (IACS) (IEC 62443, 2018; Kosmowski et al., 2019). Such systems play currently an important role in safe and secure operation of hazardous industrial installations and critical infrastructure systems to reduce rationally the risks, understood as the probability of potential abnormal events and their consequences. The methodology proposed is useful during the design and operation of hazardous plants, in particular for the safety and security management in life cycle. New emerging hazards and related risks should be periodically re-evaluated to support proactively the safety and security-related decisions depending on importance of given hazardous plant in changing conditions.

The research projects that have been carried out and finished, such as (SASEMO, 2014) and (MERgE, 2016), emphasized the importance of integrated safety and security analysis, but no satisfactory methodologies had been developed to apply them in industrial systems. Interesting proposals are related to the performability engineering (Misra, 2021; Kosmowski, 2021) that can be treated as an inspiration for systemic approach to deal systematically with safety and security issues in computerized industrial networks including control systems.

Some problems to be adequately considered are discussed in standard (ISO 22400, 2014) and publications (HSE, 2015; ENISA, 2016).

A framework is presented during the workshop for integrated analyses of the functional safety solutions regarding requirements of a generic functional safety standard IEC 61508, 7 parts (IEC 61508, 2010), and the IACS cyber security principles given in IEC 62443, 14 parts (IEC 62443, 2018). For limiting vulnerability of the information technology (IT) and converged operational technology (OT) to reduce risk of potential hazardous events, especially those of high consequences, a set of seven fundamental requirements (FRs), as defined in the IEC 62443-1 standard, is to be considered to determine the security assurance level (SAL) of domain of interest.

The method presented during workshop is based on the individual and/or societal risk graphs for determining the safety integrity level required (SIL_r) (IEC 61508, 2010; Kosmowski, 2013) of consecutive safety functions to be distinguished and defined in the analyses. Determined SIL_r of consecutive safety function - to be implemented in given safety related control system (SRCS) of architecture proposed by the designer - is then verified based on probabilistic models developed for subsystems to indicate achieved SIL, regarding relevant interval probabilistic criteria. In probabilistic models of subsystems the influence of potential common cause failure (CCF) are considered. The verified SIL is validated regarding the security assurance level (SAL) (IEC 62443, 2018; Kosmowski, 2020) determined for the domain of interest including internal and communications.

In final part of the article some additional requirements concerning the functional safety and cybersecurity solutions will be formulated pertaining to new technologies to be presumably used widely applied in Industry 5.0, such as control and safety functions that include the machine learning (ML) and artificial intelligence (AI) algorithms. Such technologies might significantly influence the resilience of hazardous installations and critical infrastructure. The resilience issue requires further research due to its importance for reliable and safe system operation in uncertain conditions. Some topics to undertake are shortly discussed.

2. Systems engineering perspective on functional safety evaluation

Systems engineering (SE) concept consists of two disciplines: the technical knowledge concerning domain in which this concept is to be applied and the systemic management in life cycle (SE, 2001). It includes an interdisciplinary engineering management process that evolves and verifies in time a balanced systemic oriented solutions that should satisfy needs of owners, producents and customers. Obviously, such solutions should include the reliability, productivity, safety and security aspects.

The SE process includes in particular (SE, 2001):

- requirements analysis (analyzing missions and environments, identifying functional requirements, defining/refining performance and design, and constraint requirements),
- functional analysis/allocation (decomposing to lower-level functions, allocating performance and other limiting requirements to all functional levels, defining/refining functional interfaces, both internal and external, defining/refining/integrating functional and physical architecture),
- synthesis (transforming architectures from functional to physical, defining alternative system concepts, configuring items and system elements, selecting preferred product and process solutions, defining/refining functional and physical interfaces, both internal and external, etc.

As it was mentioned, in the functional safety analysis and management in life cycle (IEC 61511, 2017; Kosmowski, 2006) a set of safety functions is defined in given critical installation considering the results of hazards identification. The safety integrity requirements result from evaluation of potential hazardous events and their consequences. Higher safety integrity levels impose more strict requirements on the safety-related system architecture consisting of subsystems, components, software and interfaces that enable human interventions according to predefined procedures (Kosmowski, 2018).

In order to deal systematically with all activities necessary to achieve required safety integrity for given safety function to be implemented in the E/E/PE system, the standard IEC 61508 adopts an overall framework for safety management in lifecycle. A simplified scheme of such framework is shown in Figure 1. It should include also the cyber security related issues, especially in steps 1, 3, 4, 5 of the analysis phase, and steps 7, 10, 13 in realization phase, and step 15 of the operation phase. According this standard the safety validation should be performed in terms of the overall safety function requirements and the overall safety integrity requirements, considering the safety requirements allocation for the E/E/PE safety-related system in the design phase.

A reference model for the system evaluation including OT and IT is based on the ISA99 series of standards derived from a general model of ANSI/ISA-95.00.01 (Enterprise-Control System Integration). It represents graphically a production system as the connection of several logical levels as described in publication (Kosmowski, 2020).

Below an approach is outlined for integrated functional safety and cybersecurity evaluation to mitigate risks regarding potential hazards and threats. In functional safety analysis in the process industry the safety functions (IEC 61508, 2010), IEC 62061, 2021) defined are implemented in the SRCS, for instance being a part of the basic process control system (BPCS) (IEC 61508, 2010) or as a safety instrumented system (SIS) (IEC 61511, 2017). These systems belong to the operational technology (OT) being linked, within industrial computer network, with the information technology (IT) system. Converged OT and IT systems can cause some security problems.

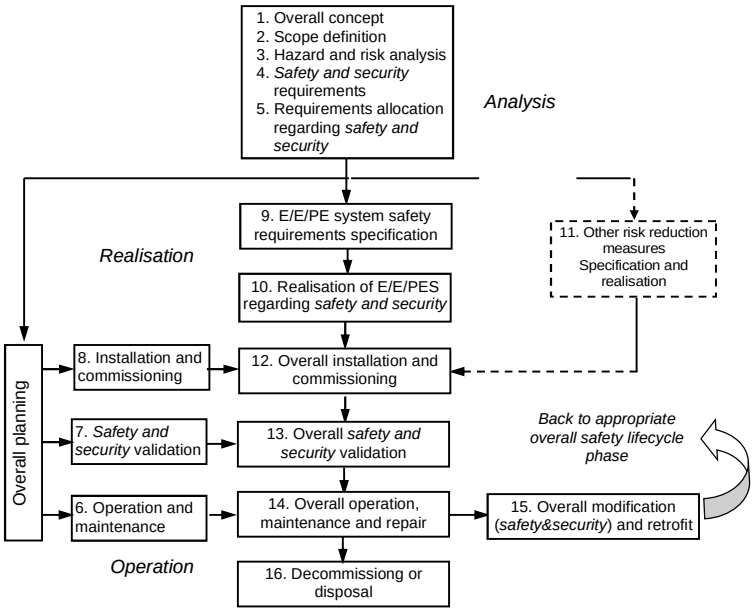

Fig. 1. Overall functional safety-related lifecycle (based on IEC 61508, 2010).

3. Verifying the safety integrity relevels of functions to be implemented for reducing risks

3.1. SIL determination and verification

Functional safety is defined as a part of general safety of the industrial plant critical installation or production line, which depends on a proper response of the SRCS during potential abnormal situation or accident to avoid or limit losses. The functional safety methodology has been formulated in the generic standard IEC 61508 and is appreciated in industrial practice in the process of design and then operation of the electric/ electronic/ programmable electronic (E/E/PE) safety-related system.

Different names of the SRCS are used in various industrial sectors, for example, a safety instrumented system (SIS) in case of the process industry sector (IEC 61511, 2017), or a safety-related electrical control system (SRECS) for machinery (IEC 62061, 2020). Such systems are designed to perform specified safety functions to ensure that the risk of interest is reduced to a level specified for given industrial installation, and then maintained at a tolerable level in life cycle of industrial plant (Kosmowski et al., 2019).

Two types of requirements are specified to ensure the functional safety (IEC 61508, 2010):

- the requirements imposed on performance of the safety function to be designed for hazards identified,
- the safety integrity requirements, i.e. the probability that the safety function will be performed in a satisfactory way when potential hazardous situation occurs.

The safety integrity is defined as the probability that a safety-related system, such as the E/E/PE system or SIS, will satisfactorily perform defined safety function under all stated conditions within given time period. For the safety-related control system (SRCS), in which defined safety function is to be implemented, two probabilistic criteria are defined as presented in Table 1 for four categories of SIL (IEC 61508, 2010), namely:

- average probability of failure on demand (PFD_{avg}) for SRCS operating in a low demand mode (LDM), or

- dangerous failure probability per hour (*PFH*) for SRCS operating in a high or continuous mode (HCM).

Table 1. Categories of SIL and probabilistic criteria to be assigned to the SRCS operating in LDM or HCM.

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})

The SIL requirements assigned for the SRCS to be designed for implementing specified safety function stem from the results of the risk evaluation to reduce sufficiently the risk of losses taking into account the risk criteria, namely for the individual risk and/or the group or societal risk. If the societal risk is of interest, the analyses are generally oriented on three categories of losses, namely (IEC 61508, 2010): health (H), environment (E) or material (M) damage, then SIL required (SIL_r) for particular safety function is determined as follows

$$\mathrm{SIL}_r = \max\left(\mathrm{SIL}_r^H, \mathrm{SIL}_r^E, \mathrm{SIL}_r^M\right) \tag{1}$$

As it was mentioned, generally the SIL verification can be carried out for one of two operation modes: LDM or HCM. The former is characteristic for the process industry (IEC 61508, 2010), and the latter is typical for the machinery (IEC 62061, 2020) or the railway transportation systems, and also for monitoring and real time controlling of industrial installation using such systems as DCS (distributed control system) and SCADA (supervisory control and data acquisition).

Typical hardware architecture of the E/E/PE system, shown in Figure 2 consisting of three subsystems [21]: (A) sensors and input devices (transducers, converters etc.), (B) logic device, e.g. safety programmable logic controller (PLC) or safety relay, and (C) actuators, i.e. equipment under control (EUC) or other output devices.

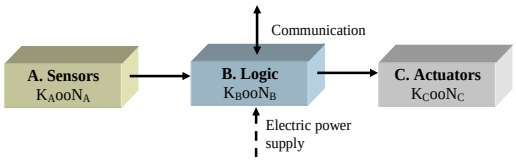

Fig. 2. Typical architecture of the E/E/PE system or SIS in which a safety function is implemented.

Such system constitutes a specific architecture of the hardware and software modules, and communication conduits. The logic device comprises typically a safety PLC with its input and output modules. The subsystems shown in Figure 2 can be generally of K out of N (KooN) configuration, for instance 1oo1, 1oo2 or 2oo3. Their hardware fault tolerance (HFT) is understood as ability of the subsystem to perform a required function in the presence of faults or errors. The HFT (0, 1, 2) is an important parameter to be considered in the final SIL verification of given subsystem regarding architectural constrains for determined value of a safe failure fracture (S_{FF}) (IEC 61508, 2010; Kosmowski, 2013).

Any redundant system, also redundant SRCS, is prone to a common cause failure (CCF) that contributes significantly to decreasing its dependability due to potential failure mechanisms regarding relevant site-specific influence factors. The CCF mechanism causes coincident failures of two or more channels in a redundant subsystem, leading to a failure of entire system. The multiple failures may occur simultaneously or over a period, shorter than testing time interval. Various probabilistic models are proposed to deal with CCF in safety-related systems, in particular the E/E/PE system or SIS. The CCF contribution in the PFD_{avg} or PFH is often incorporated using β-factor method in probabilistic modelling of redundant systems (Kosmowski, 2020, 2023).

If diagnostic tests run in each channel, they can detect and reveal only a fraction of failures. Therefore, it is justified to divide all failures into two categories: (1) those that lie outside the coverage of the diagnostic tests (cannot be detected) and (2) those that lie within the coverage (detected by the diagnostic tests). Overall probability per time unit of subsystem's dangerous failure (including CCF), is a function of parameters specified in formula below (Kosmowski, 2018)

$$PF_D^{CCF} = f\left(\lambda_{Du}, \beta, \lambda_{Dd}, \beta_D, \ldots\right) \tag{2}$$

where:

- λ_{Du} is a rate of dangerous (D) undetected (u) failure in a single channel, influencing the probability of failures that lie outside the coverage of the diagnostic tests; β is CCF factor for undetectable dangerous faults, which is equal to the overall β-factor that would be applicable in the absence of diagnostic testing;
- λ_{Dd} is the rate of a dangerous (D) detected (d) failure in a single channel, influencing the probability of failures that lie within the coverage of the diagnostic tests, β_D is CCF factor for detectable dangerous faults; as the repetition rate of the diagnostic testing is increased, the value of β_D falls below β.

In evaluation of β and β_D it is suggested to consider following factors (IEC 61508, 2010):

(1) Separation / segregation,
(2) Diversity / redundancy,
(3) Complexity / design / application / maturity / experience,
(4) Assessment / analysis and feedback of data,
(5) Procedures / human interface,
(6) Competence / training / safety culture,
(7) Environmental control,
(8) Environmental testing.

3.2. Case study of SIL verification

An example of the reliability block diagram of E/E/PE safety-related system will be considered for the hardware architecture as shown in Figure 3. It consists of three subsystems of following configurations: (A) 2oo3 for sensors, (B) 1oo1 of logic device, and (C) 1oo2 for actuators. The potential common cause failures (CCF) are included in probabilistic modelling of subsystems: A and C for low demand mode of operation.

It was assumed that channels of j-th subsystem are periodically tested with an interval T_{Ij}. The average probability of failure on demand PFD_{avg} for subsystems are evaluated according to the formulas that include relevant β and β_D factors (Kosmowski 2020).

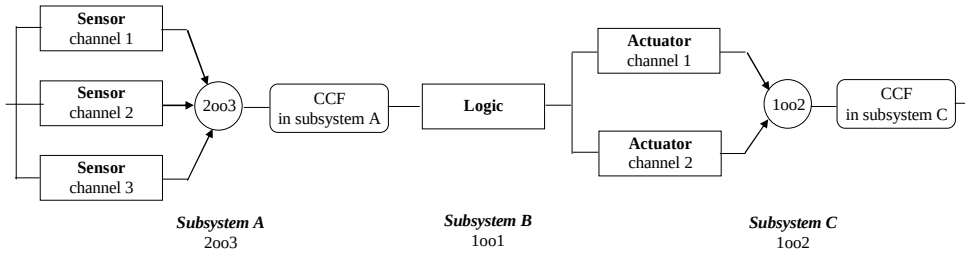

Fig. 3. Hardware architecture of safety-related system used for verifying the safety integrity level

The probabilistic measures of the system shown in Figure 3 have been calculated according to formulas (3) and (4) respectively for low and continuous mode of operation (Kosmowski, 2018):

$$PFD_{avg}^{Sys} \cong PFD_{avg}^{A,2oo3} + PFD_{avg}^{B,1oo1} + PFD_{avg}^{C,1oo2} \tag{3}$$

$$PFH^{Sys} \cong PFH^{A,2oo3} + PFH^{B,1oo1} + PFH^{C,1oo2} . \tag{4}$$

The component reliability data and other parameters for calculations of probabilistic measures according to formulas as above for determining the safety integrity levels (SIL) are in given in publication (Kosmowski, 2020). The results of calculations for subsystems A, B, C and the entire system are presented in Table 2 for low demand mode (LDM) of the system operation.

The results obtained indicate that the safety integrity level for the system under consideration is SIL 3 and the subsystem A contribute more significantly to PFD_{avg}^{Sys} (48,5%). The system can be considered as accepted if required SIL obtained from the risk evaluation is no higher than 3 (SIL_r 3 or lower). If required SIL would be higher (SIL_r 4) then redesigning of the safety-related system must be considered or applying additional layer of protection (IEC 61511, 2017).

Table 2. Results of SIL verification for the LDM of system operation.

System / *Subsystem* / Channel	KooN	PFD_{avg}^{Sys}	SIL	[%] of PFD_{avg}^{Sys}
Sys	**–**	**$13.6 \cdot 10^{-5}$**	**3**	**100**
A	***2oo3***	***$6.6 \cdot 10^{-5}$***	***4/3[a]***	***48.5***
1	–	$2.2 \cdot 10^{-3}$	2	–
2	–	$2.2 \cdot 10^{-3}$	2	–
3	–	$2.2 \cdot 10^{-3}$	2	–
B	***1oo1***	***$2.6 \cdot 10^{-5}$***	***4/3[b]***	***19.1***
C	***1oo2***	***$4.4 \cdot 10^{-5}$***	***4/3[a]***	***32.4***
1	–	$4.4 \cdot 10^{-3}$	2	–
2	–	$4.4 \cdot 10^{-3}$	2	–

[a] SIL reduced due to architectural constrains (S_{FF} = 90%, HFT 1)
[b] SIL reduced due to architectural constrains (S_{FF} = 99%, HFT 0)

The testing interval T_I assumed contributes also significantly on the results obtained. In determining of this interval, it is necessary to consider experience of the users of E/E/PE system and restrictions regarding the operation of given industrial installation. In case of the subsystem C, the partial tests of actuators can be proposed to be performed more frequently than overall tests. Thus, the parameters of the model proposed should be carefully evaluated in the modelling process, considering verified sources of information.

4. Cybersecurity of safety related control systems

The security related attacks are becoming increasingly important threats for converged IT and OT systems, particularly for the industrial automation and control system (IACS) in industrial networks of hazardous plants (IEC 62443, 2018; IEC 63074, 2018). External threats can initiate security-related incidents impacting adversely the critical installation causing losses. Their vulnerability of converged IT and/or OT systems is understood as a security related weakness of given industrial network that can be exploited by an attacker to trigger hazardous events causing losses (IEC 63074, 2018; Kosmowski, 2013). The cyber resilience of such systems and networks (CISA, 2020) is an important issue to be adequately shaped, also for the business continuity management (BCM) (ISO 22301, 2012).

A threat may be either passive or active. In case of the passive threat the agents usually gather information by casual communications with employees and contractors. Examples of active threats are as follows (IEC 63074, 2018): database injection, spoofing and impersonation, phishing, malicious code, Denial of Service (DoS), escalation of privileges, physical destruction, etc. The security-related analyses should be carefully carried out to identify the SRCS vulnerability that could be exploited by various threats impacting the reliability and safety of the entire production installations.

The IT security risks shall be mitigated through the combined efforts of component suppliers, the machinery manufacturer, the system integrator, and the machinery end user (IEC 62443, 2018; Kosmowski et al., 2019). Generally, the responses to the security risks should take following steps (IEC 63074, 2018):

(a) eliminate the security risk by design (avoiding vulnerabilities).
(b) mitigate the security risk by risk reduction measures (limiting vulnerabilities),
(c) provide information about the residual security risk and the measures to be adapted by the user.

Standard IEC 62443 proposes an approach to deal systematically with the security-related issues of the IACS. Four security levels (SL) are defined that are understood as a confidence measure that the IACS is free from vulnerabilities and it functions in an intended manner. In the standard IEC 63074 these levels are also adopted to deal with the SRCS security of manufacturing systems.

The security level can be related to following foundational requirements (FRs):

FR 1 ─ identification and authentication control (IAC),
FR 2 ─ use control (UC),
FR 3 ─ system integrity (SI),

FR 4 ─ data confidentiality (DC),
FR 5 ─ restricted data flow (RDF),
FR 6 ─ timely response to events (TRE), and
FR 7 ─ resource availability (RA).

Thus, instead to express the SL as a single number, it is suggested to apply a vector consisting of from one to seven FRs specified above. Such vector is proposed for describing the security requirements for a zone, conduit, component, or system. This vector may contain the integer numbers of SL from 1 to 4 or 0 (if not relevant) assigned to specified FR. A general format of a security assurance level (SAL) to be determined for given domain is as follows (IEC 62443, 2018):

SL-? ([FR,] domain) = [IAC UC SI DC RDF TRE RA] (5)

where: SL-? = (required) SL type - possible formats are: SL-T = target SAL, SL-A = achieved SAL, and SL-C = capabilities SAL; [FR,] = (optional) field indicating the FR that SL value applies; domain = (required) is domain to be evaluated - this may be procedure, system or component; when assigning SL to a system; it may be for instance: Zone A, Machinery B, Engineering Workstation, etc.

For instance, it can be written as follows (IEC 62443, 2018):

(a) SL-T (Control System Zone) = [2 2 0 1 3 1 3],
(b) SL-C (Engineering Workstation) = [3 3 2 3 0 0 1],
(c) SL-C (RA, Safety PLC) = 3; in this example only RA requirement is specified, instead of a 7-dimension SAL vector for description of SL-C.

Thus, three type of vectors that consist security levels (the integer number 1, 2, 3, 4 or 0) for given domain are can be evaluated:

- SL-T (target SAL) - the desired levels of security,
- SL-C (capability SAL) - the security level that particular device or system can provide when properly configured,
- SL-A (achieved SAL) - the actual level of security of a particular device or system.

For improving the security of SRCS it is suggested to elaborate guidance (the instruction handbook) for the end user that includes the following issues (IEC 63074, 2017):

(A) Restriction of logical/physical access to the IT systems with potential influence on safety, for instance using internal IT systems with risk reduction measures, such as firewalls, antivirus tools, etc., providing authentication and access control mechanisms, such as card readers, physical locks, according to specifications of manufacturer or integrator; disabling all unused external ports/interfaces and services, etc.,

(B) Detection and reaction on IT-security incidents with potential influence on safety, for instance checking regularly means for detecting failed IT system components or unavailable service according to the specifications of the machine or component manufacturer; being responsive for vulnerabilities resulting from a new IT security threat and potential attack;

(C) In case of remote maintenance and service, for instance using provided means for setting up and ending a remote access session according to the specifications of the component manufacturer; using encryption means for initiating a remote service according to specifications of the machine/component manufacturer; watching any remote access session with a restriction of duration for remote access, etc.

Such topics should be included and carefully treated in a security information and event management (SIEM) to be developed and proactively used in practice according to requirements given in ISO/IEC 27001 (2013), or supported by the information security risk management as suggested in standard ISO/IEC 27005 (2018). Its specific requirements to be formulated should include the target SAL (SL-T) to be then verified regarding achieved SAL (SL-A) knowing the capability SAL (SL-C) of solutions applied. Defined system requirements (SRs) and specific requirement enhancements (REs) for consecutive FRs to be fulfilled at given SL from 1 to 4 are specified in the IEC 62443 standard and a recent publication (Kosmowski, 2023).

5. Integrating of the functional safety and cybersecurity analysis

As it was mentioned, IEC 62443 standard consists of 14 parts. Some of them are still in the process of verification or updating. The main objective of this series is to cover more important topics of the IACS security entirely. In a second edition of generic functional safety standard IEC 61508 it was suggested to use the IEC 62443 standard to deal with cybersecurity issues at the design stage and operation of the programmable safety-related control systems. Up to now, though, the IEC 61508 and IEC 62443 standards are rather loosely linked (Braband, 2016; Felser et al., 2019). Also in case of the SRCS of machinery and manufacturing lines there is a need to deal more systematically with security issues, as it has been lately emphasized (IEC 63074, 2017).

It is worth to mention that achieved security assurance level (SL-A) of SRCS achieved depends strongly on the quality of the information security management system (ISMS), if it has been implemented in industrial plant. The objective of ISMS is to monitor, control, maintain and improve the security of converged IT and OT systems.

An important task to be undertaken is the risk evaluation and management of the IT system, as it is postulated in standards ISO/IEC 27001 and ISO/IEC 27005. It includes the consideration of all functional components of the information system including hardware (HW) and software (SW), communication conduits and relevant human/organizational factors, especially those related to the IT and OT reliability, safety and security. Opinions are expressed that the CIA triad (confidentiality, integrity, availability) is justified to specify basic requirements for the IT network, but in case of the OT system a reversed triad, namely AIC (availability, integrity, confidentiality) is more appropriate. The issues should be included in shaping resilience of IACS (Kosmowski, 2023).

As it was discussed above four SL categories have been are distinguished and defined in IEC 62443. They have been discussed in publications (Kosmowski, 2021,) in the context of functional safety standard IEC 61508, in which also four SILs are distinguished. So, the problem is encountered how to treat these issues in an integrated way in functional safety analysis including cybersecurity aspects of the industrial computer network. The correlation between SIL and SAL is proposed as it is shown in Table 3 (Kosmowski, 2021, 2023). Similar correlation can be proposed for the SRCS of manufacturing systems, however remembering that in the machinery sector the highest SIL to be assigned to the safety-related systems is SIL 3 (IEC 62061, 2020).

The method proposed for determining the security level achieved SL-A (SAL) for a computer network domain is based the weights w_i of security levels SL_i for relevant FR_i to be evaluated by experts who use available sources of information concerning the security solutions applied. These weights generally differ due to diversified importance of FR_i for the domain considered. The method includes cases in which not all fundamental requirements FR_i are relevant in given situation.

Thus, instead of determination of SAL for given domain based on dominant FR_i it has been proposed alternatively to evaluate a domain security index SI^{Do} and then to assign an integer number (1, 2, 3, or 4) to the SAL as it is proposed in first column of Table 3. The importance I_i of FR_i is evaluated by experts for specific domain, for instance indicating an integer number on the scale from 1 to 5 (or 1 to 10), and 0 if FR_i is not relevant. Then, the weight w_i of given FR_i is calculated according to formula

$$w_i = \frac{I_i}{\sum_{i=1}^{7} I_i} \tag{6}$$

The security index SI^{Do} for the domain (Do) and determined security level SL_i (the integer number from 1 to 4, or 0 if FR_i is not considered) for relevant (Re) fundamental requirements FR_i (i – selected integer values from 1 to 7) is calculated as follows

$$SI^{Do} = \sum_{i \in \mathrm{Re}} w_i SL_i \tag{7}$$

Four intervals of the domain security index SI^{Do} (from SI^{Do1} to SI^{Do4}) are proposed in first column of Table 3 for assigning the category number of SAL (SL-A) from 1 to 4. Such approach corresponds with attributing SAL for the domain in our earlier publications, based on dominant SL_i for relevant fundamental requirements FR_i.

Proposed correlations between security index to be assigned to the domain SI^{Do} or SAL and final SIL attributing to given SRCS in hazardous installation are presented in Table 3. It was assumed that SIL has been verified according to IEC 61508 based on results of probabilistic modelling as described above, regarding CCFs and human factors and the architectural constrains for evaluated S_{FF} and HFT of consecutive subsystems.

Table 3. Proposed correlation between SI^{Do} or SAL for evaluated domain and final SIL to be attributed to the SRCS of safety critical installation

Security index SI^{Do} / SAL	SIL verified according to IEC 61508*			
	1	2	3	4
$SI^{Do1} \in [1.0, 1.5)$ / SAL 1	SIL 1	SIL 1	SIL 1	SIL 1
$SI^{Do2} \in [1.5, 2.5)$ / SAL 2	SIL 1	SIL 2	SIL 2	SIL 2
$SI^{Do3} \in [2.5, 3.5)$ / SAL 3	SIL 1	SIL 2	SIL 3	SIL 3
$SI^{Do4} \in [3.5, 4.0]$ / SAL 4	SIL 1	SIL 2	SIL 3	SIL 4

* verification includes the architectural constrains regarding S_{FF} and HFT of subsystems

Thus, the SIL verification (in relation to required SIL_r determined from risk evaluation) is based on results obtain from probabilistic modelling of the SRCS of proposed architecture regarding S_{FF} and HFT of subsystems. In the case study as above (see results in Table 2), the safety integrity level SIL 3 was obtained. Considering the domain of SRCS in which the safety function is implemented including the communication conduits, the SL-A vector was evaluated as follows: [3 2 3 2 2 3 2].

Assuming that weights of all SL_i are equal (w_i = 1/7) and using the equation (7) the result is SI^{Do} = 2.43, i.e. belong to the interval SI^{Do2} and is interpreted as SAL 2. Looking at the column 3 of Table 3 the final safety integrity level, validated regarding the security requirements, is SIL 2, lower than required SIL_r 3.

Therefore, the security of the domain should be improved (its vulnerability decreased). For instance, in case of the SL-A vector [3 3 3 3 2 3 2], SI^{Do} = 2.71 (belong to interval SI^{Do3}) and SAL can be indicated as SAL 3. In this case validated SIL is SIL 3, and an iterative process of the SRCS design can be stopped, because determined was SIL_r 3.

6. Conclusion

Selected design, operational, safety and security issues of the OT and IT networks have been overviewed and discussed. The context of functionality and architectures of the industrial automation and control system (IACS) will be considered that should be designed and operated in life cycle. Emphasis was put on the functional safety and cybersecurity of the industrial control systems and networks. These issues are becoming crucial, because IACS includes the safety related control system (SRCS) that plays a key role in innovative high-quality manufacturing, especially in modern industrial plants of Industry 4.0/5.0, and hazardous industrial installations of critical infrastructure. This system contribute significantly to reducing risks to be reevaluated periodically in life cycle of the system.

The method to be presented uses the individual and/or societal risk graphs for determining the safety integrity level required (SIL_r) of consecutive safety functions distinguished and defined according to functional safety requirements. These levels are then verified to indicate that the required SIL is achieved or not for the architecture of SRCS considered during the design. The design process of SRCS is in practice iterative. If verified SIL for assumptions made is not achieved (is lower than required), some changes in the design of SRCS are considered how to achieve required SIL. This process will be explained on diagrams that include safety and security aspects.

The dependability of SRCS in which the safety functions are implemented is influenced both by various factors, including quality of hardware (HW) and software (SW) solutions as well as human factors and organizational culture (Kosmowski et al., 2022; Kosmowski, 2023). These aspects will be presented during next workshop devoted to cognitive aspects of human operator activities in context of properties of operational technology and alarm system considering also the defense in depths (D-in-D) concept and operational procedures that include ML and AI algorithms.

References

Braband, J. 2016. What's Security Level go to do with Safety Integrity Level? 8th European Congress on Embedded Real Time Software and Systems, hal-01289437, Toulouse.

CISA, 2020. Assessments: Cyber Resilience Review, us-cert.gov/resources/assessments.

ENISA, 2016. Communication network dependencies for ICS/SCADA Systems, European Union Agency for Network, and Information Security.

Felser, M., Rentschler, M., Kleinberg, O. 2019. Coexistence Standardisation of Operational Technology and Information Technology, Proceedings of the IEEE.

HSE, 2015. Cyber Security for Industrial Automation and Control Systems, Health and Safety Executive (HSE) Interpretation of Current Standards on Industrial Communication Network and System Security, and Functional Safety.

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

IEC 61511, 2017. Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1-3. International Electrotechnical Commission, Geneva.

IEC 62061, 2021. Safety of machinery – Functional safety of safety-related electrical, electronic, and programmable electronic control systems. International Electrotechnical Commission, Geneva.

IEC 62443, 2018. Security for industrial automation and control systems. Parts 1-14 (some parts in preparation). International Electrotechnical Commission, Geneva.

IEC 63074, 2017. Security aspects related to functional safety of safety-related control systems. International Electrotechnical Commission, Geneva.

ISO 22301, 2012. Societal security - Business continuity management - Requirements. International Organisation for Standardisation, Geneva.
ISO 22400, 2014. Automation systems and integration - Key performance indicators (KPIs) for manufacturing operations management, Parts 1 and 2. International Organisation for Standardisation, Geneva.
ISO/IEC 27001, 2013. Information technology - Security techniques - Information security management systems – Requirements, Geneva.
ISO/IEC 27005, 2018. Information technology - Security techniques - Information security risk management, Geneva.
Kosmowski, K.T. 2006. Functional Safety Concept for Hazardous System and New Challenges. Journal of Loss Prevention in the Process Industries, Vol. 19, No. 1, 298-305.
Kosmowski, K.T. 2013. Functional safety and reliability analysis methodology for hazardous industrial plants. Gdansk University of Technology Publishers.
Kosmowski, K.T. 2018. Safety Integrity Verification Issues of the Control Systems for Industrial Power Plants. In: Advanced Solutions in Diagnostics and Fault Tolerant Control. Springer Int. Publishing AG, 420-433.
Kosmowski, K.T., Śliwiński, M., Piesik, J. 2019. Integrated Functional Safety and Cybersecurity Analysis Method for Smart Manufacturing Systems. TASK Quarterly, Vol. 23, No. 2, 1–31.
Kosmowski, K.T. 2020. Systems Engineering Approach to Functional Safety and Cyber Security of Industrial Critical Installations. In Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar, 135-151.
Kosmowski, K.T. 2021. Functional Safety and Cybersecurity Analysis and Management in Smart Manufacturing Systems. In: Handbook of Advanced Performability Engineering (Ed. K.B. Misra), Chapter 3. Springer Nature Switzerland AG.
Kosmowski, K.T., Piesik, E., Piesik, J. & Śliwiński, M. 2022. Integrated functional safety and cybersecurity evaluation in a framework for the business continuity management. Energies 15, 3610–3631.
Kosmowski, K.T. 2023. Operational resilience regarding safety and security aspects of industrial automation and control systems. In Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar, 99-116.
MERgE, 2016. Safety & Security, Recommendations for Security and Safety Co-engineering, Multi-Concerns Interactions System Engineering ITEA2 Project No. 11011.
Misra, K.B. (Ed.) 2021. Handbook of Advanced Performability Engineering. Springer Nature Switzerland AG.
SE, 2001. Systems Engineering Fundamentals. defense acquisition university press, Fort Belvoir, Virginia 22060-5565.
SESAMO, 2014. Integrated Design and Evaluation Methodology. Security and Safety Modelling. Artemis JU Grant Agr., No. 2295354.