Chapter 3
Functional Safety and Cybersecurity Analysis and Management in Smart Manufacturing Systems

Kazimierz T. Kosmowski

Abstract This chapter addresses some of the issues of the integrated functional safety and cybersecurity analysis and management with regard to selected references and the functional safety standards: IEC 61508, IEC 61511, ISO 13849-1 and IEC 62061, and a cybersecurity standard IEC 62443 that concerns the industrial automation and control systems. The objective is to mitigate the vulnerability of industrial systems that include the information technology (IT) and operational technology (OT) to reduce relevant risks. An approach is proposed for verifying the performance level (PL) or the safety integrity level (SIL) of defined safety function, and then to check the level obtained taking into account the security assurance level (SAL) of particular domain, for example, a safety-related control system (SRCS), in which the given safety function is to be implemented. The SAL is determined based on a vector of fundamental requirements (FRs). The method uses defined risk graphs for the individual and/or the societal risk, and relevant risk criteria, for determining the performance level required PL_r or the safety integrity level claimed SIL CL, and probabilistic models to verify PL/SIL achievable for the architecture of the SRCS considered.

Keywords Smart manufacturing systems · Industry 4.0 · Information technology · Operational technology · Safety-related control systems · Functional safety · Cybersecurity

3.1 Introduction

Nowadays, manufacturers face ever-increasing variability demands for innovative products, greater customization, smaller lot sizes and viable in practice supply-chain changes. However, disruptions also occur causing production delays and manufacturing losses. In many industrial sectors various hazards and threats are present or

K. T. Kosmowski (✉)
Faculty of Electrical and Control Engineering, Gdansk University of Technology, Gdansk, Poland
e-mail: k.kosmowski@upcpoczta.pl

K. B. Misra (ed.), *Handbook of Advanced Performability Engineering*,
https://doi.org/10.1007/978-3-030-55732-4_3

emerge that contribute significantly to the business and insurance risks [1]. Manufacturers to be successful have to choose and incorporate technologies that help them quickly adapt to dynamic changes in business environment while maintaining high product quality and optimizing the use of energy and resources to limit environmental emissions and pollutions. Such technologies form the core of emerging, information-centric, and the so-called smart manufacturing systems (SMSs) that should be designed and operated to maximize the business potential, in particular the use, flow and re-use of data throughout the enterprise and between cooperating companies [2].

The SMS design and operation principles, and business expectations, are similar to those that stand behind the Industry 4.0 technological concept being in dynamic development [3]. These concepts include new interesting ideas, models, solutions and tools, related to the information technology (IT) and the operational technology (OT), ranging from innovative software supporting business planning and management, using the artificial intelligence (AI) and big data (BD) applications, and the cloud technology (CT), to innovative production and maintenance supporting software tools, and advanced automation solutions, for example, AutomationML concept based on mechatronic metamodels [4]. More and more important functions are to be assigned to the distributed industrial control systems (ICS), operating often in sophisticated computer networks, to be designed using the wire and wireless technologies for communications.

The CT is a relatively new technology of increasing interest that has significant potential to support the effectiveness of the SMSs operating in changing business environment. This technology in principle supports the implementation of advanced internet technologies, currently in dynamic development and use, known as the internet of things (IoT) and the industrial internet of things (IIoT) [5]. Nowadays, the factory automation and process control systems, networks and protocols within the OT are increasingly merged with those of IT. Requirements formulated for the OT and IT are in principle different, but the networks and protocols for communication in the SMS must allow for effective and safe convergence of the IT and OT systems [6], especially when a concept of machine-to-machine (M2M) communication techniques is applied in the industrial interconnected systems.

Therefore, the questions may be raised concerning the security issues of such technical solutions in the context of the reliability and safety requirements. Lately, considerable efforts have been undertaken by the research community to identify existing and emerging problem areas [7, 8], point out more important issues that require further research to support the development and implementation in industrial practice of advanced safety and cybersecurity requirements and technologies [9]. These aspects are considered in some publications from the point of view of technology resilience, in particular, a cyber resilience that should be carefully reviewed in the computer systems and networks to be designed or modernized [10].

The expectations of the industry are high and some institutions have been involved in practically oriented research to propose new solutions for implementation in the industrial hazardous plants [11–13]. Proposing integrated safety and security analysis methodology to support managing of hazardous systems is undoubtedly challenging.

It concerns especially the systems to be designed to achieve possibly high functional safety and cybersecurity goals of relevant domains to be managed in life cycle [14]. It depends on decisions and actions undertaken by responsible management and engineering staff in given industrial company and is influenced significantly by awareness of the safety and security culture to be carefully shaped in time [15].

The complexity of industrial systems and networks, sometimes without clear hierarchy in information flow for controlling various processes, operating in changing internal and external environment, emerging of new hazards and threats, can make some additional challenges to reach, in practice, high level of system reliability and safety [16, 17]. No less important in such systems are the security-related issues, especially those influencing potentially the risk of high consequence losses [18, 19]. An important issue in industrial practice is the business continuity management (BCM) [20] that requires careful consideration of various aspects within an integrated RAMS&S (reliability, availability, maintainability, safety and security) framework. In such analyses the risk evaluation and management in life cycle is of special interest for both the industry and insurance companies [21]. Such issues are of significant interest also in the domain of performability engineering that have been stimulated by Misra for years [22].

In this chapter an approach is proposed for integrated functional safety and cybersecurity analysis and management in the SMSs and hazardous plants in the context of the design and operation of the industrial automation and control systems (IACSs) [14, 23]. The idea of the SMSs assumes the openness of markets and flexible cooperation of companies worldwide. It could not be effective without relevant international standardization. However, some problems have been encountered in industrial practice due to too many existing standards that have been published by various international organizations. Unfortunately, the contents of some related standards were not fully coordinated or require updating. It concerns, in particular, the IT and OT design principles in relation to the IACS functionality and architecture requirements with regard to the safety and security aspects [2, 6].

The main objective of this chapter is to outline a conceptual framework for integrated analyses of the functional safety solutions according to generic functional safety standard IEC 61508 (7 parts) [24], and the IACS cybersecurity, outlined in IEC 62443 (14 parts) [23]. For reducing vulnerability of the IT and OT systems and reduce risks of hazardous events, especially of high consequences, a set of seven fundamental requirements (FRs), defined in the IEC 62443-1 standard, is taken into account to determine the SAL of the domain considered.

The method proposed uses the individual and/or societal risk graphs for determining the performance level required (PL_r) [25], the safety integrity level required (SIL_r) [24, 26] or the safety integrity level claimed (SIL CL) [27] of consecutive safety functions to be defined in the analyses. These levels are then verified to indicate the PL or SIL to be achieved in designed SRCS of architecture proposed, in which particular safety function is to be implemented. For that purpose, relevant probabilistic model of SRCS is developed with regard to potential common cause failures (CCFs), when the redundancy of hardware is proposed. Then, the verified SIL is validated with regard to determined SAL of relevant domain, for example,

the domain of SRCS in which particular safety function is implemented, including internal and external communications.

In the analyses and assessments to be carried out, both quantitative and qualitative information available is used, including expert opinions. The analyses and assessments are based on classes defined or categories distinguished. For related evaluations some performance indicators are of interest, in particular the so-called key performance indicators (KPIs) defined, for example, in the standard [28] and numerous publications [e.g. 1].

3.2 Architectures and Conceptual Models of Complex Manufacturing Systems

3.2.1 Manufacturing System General Architecture

Opinions are expressed, based on evidence from industrial systems and networks, that the SMSs are driving unprecedented gains in production agility, quality, and efficiency across manufacturers present on local and global markets, improving both short-term and long-term competitiveness. Specifically, the SMSs use the information and communication technologies along with advanced software applications to achieve the following main goals [2]:

- support intelligent marketing for better production planning,
- develop innovative technologies and products,
- optimize the use of labour, material, and energy to produce customized, high-quality products for the long-term or just-in-time delivery,
- quickly respond to the market demands and supply chains with support of advanced logistics system.

Various categories of computer applications are used in industrial practice for supporting in achieving these goals including [2, 14]: ERP (enterprise resource planning), CRM (customer relationship management), SCM (supply chain management), MES (manufacturing execution system), CMM (computerized maintenance management), PLM (product lifecycle management) and so on.

The ability of potentially disparate systems to gather and exchange the production and business data rests critically on information technology and related standards that enable communication and services for running, supervising and coordinating effectively various processes in normal, transient and abnormal conditions. It becomes evident that a manufacturer's sustainable competitiveness depends on its capabilities with respect to cost, delivery, flexibility and quality, but also the reliability, safety and security of processes and assets.

The SMS's technical and organizational solutions should maximize those capabilities and profits by using advanced technologies that promote rapid flow and widespread use of digital information within and between manufacturing systems [2].

However, it is necessary to consider and assess various risks during the SMS design and its operation to reduce significant risks of potential major losses. It should be supported by the insurer having experience and knowledge gathered from industrial practice [1].

An example of the complex system consisting of the OT, IT and CT networks illustrating generally their functional and architectural issues of convergence is shown in Fig. 3.1. The OT is in the process of adopting the same network technologies as defined in the IT system at an increasing rate, so these two systems begin to merge together. It is expected that the use of the CT in favour of IT and OT will make additional business models and automation structures possible and profitable. Combining these domains is often referred to as the internet of things (IoT) or industrial internet of things (IIoT) [6]. However, such merging can cause some cybersecurity-related problems in relevant domains that require special treatment in the design and in the operation of the IT and OT systems, especially when using the CT network is to be considered [6].

An approach is proposed below for integrated functional safety and cybersecurity evaluation aimed at indicating rational solutions in the context of reducing relevant risks. In the functional safety approach the safety functions [12, 16] are defined to be implemented within the SRCSs, for example, the basic process control system (BPCS) [24], the safety instrumented system (SIS) in process industry [26] or in the machinery sector using, for example, the safety programmable logic controller (PLC) or the relay logic solutions [25, 27] (see the OT part in Fig. 3.1). Adoption of the same networks within the OT and IT systems may be justified regarding costs, but requirements concerning the functional safety and cybersecurity in the domains

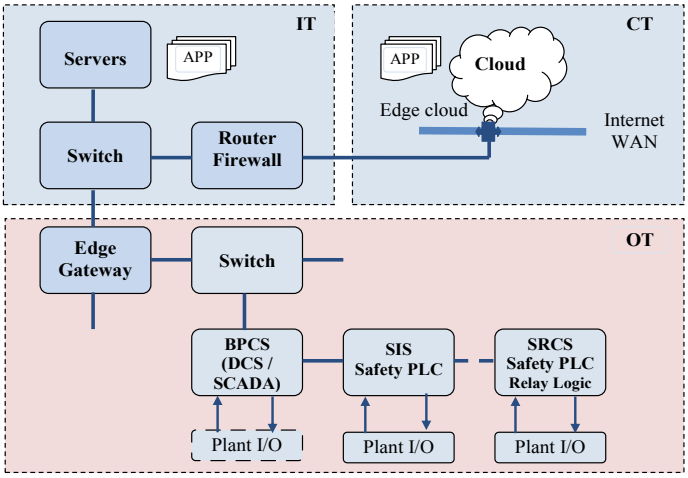

Fig. 3.1 Architectural relations of basic networks consisting of the operational technology (OT), information technology (IT), and cloud technology (CT) (based on [6])

of OT and IT are usually different, which might lead to new challenges in bridging these different technological worlds [6].

3.2.2 *Traditional Reference Model of the Manufacturing System*

A traditional reference model is based on the ISA99 series of standards derived from the generic model of ANSI/ISA-95.00.01 (Enterprise-Control System Integration), and represents the manufacturing system as the connection of following functional and logical levels (Fig. 3.2):

Level 0—Manufacturing processes: It includes the physical processes and basic process equipment, sensors and actuators, equipment under control (EUC) [24] that are the elements of safety-related system (SRS) for implementing the safety function (SF); these devices are periodically tested and subjected to the preventive maintenance (PM);
Level 1—Basic control: This level includes: local area network (LAN) controller, input/output (I/O) devices, communication conduits, and the PLCs; the devices of this level contribute to the continuous control, discrete/sequence control, or batch control;
Level 2—Area control: This level allows to implement functions for monitoring and controlling the physical process; it consists of LAN and local elements of the control and protection systems, human–machine interface (HMI) on local equipment panels;
Level 3—Site manufacturing and control: For example, the distributed control system (DCS)/supervisory control and data acquisition (SCADA) software that includes: a human–system interface (HSI), an alarm system (AS) and a decision support system (DSS) for the site control human operators; at this level the manufacturing execution system (MES) is placed;

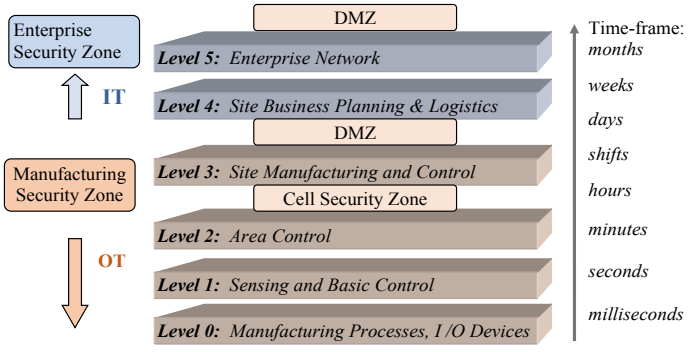

Fig. 3.2 Traditional reference model of the SMS based on ANSI/ISA95 standard

Level 4—Enterprise business planning and logistics: This level is characterized by the business planning and related activities, including logistics, using often the enterprise resource planning (ERP) system to manage and coordinate effectively business and enterprise resources required in manufacturing processes;
Level 5—Enterprise network: At this level additional external functions are to be realized, for example, business and logistics-related support by the CT applications.

Levels 0–3 are to be designed and operated with regard to relevant technical and functional requirements and specifications assigned to the OT network. The levels 4 and 5 are essential parts of the IT network. The purposeful and reliable system-oriented functional convergence of these networks has to include the functional safety and cybersecurity-related aspects. Nowadays, in case of the SMS, an intensive use of the cloud technology is of interest in industrial plants.

In such open manufacturing system, the safety and security aspects require special attention of the designers and operators [14, 29]. From the information security point of view an important role is to be assigned to the cell security zone (CSZ) and the demilitarized zone (DMZ) placed in Fig. 3.2. The safety and security issues, in particular the functional safety and cybersecurity solutions, obviously require careful treatment and management in life cycle.

Many internal and external influences, hazards and threats should be considered in the operation process of the OT and IT systems. Basic features of these system are illustrated in Fig. 3.3. Expected lifetime of the OT system is often to be evaluated in the range of 10–20 years, but only 3–5 years in the case of IT [30]. For characterizing of the OT an AIC (availability, integrity and confidentiality) triad is usually used to prioritize basic safety and security requirements, but a confidentiality, integrity, and availability (CIA) triad is to be assigned to the IT network.

The SMS's reliability, safety and security is influenced by external and internal factors, including human and organizational factors [15]. For high reliability and availability of the OT system an operational strategy should be carefully elaborated

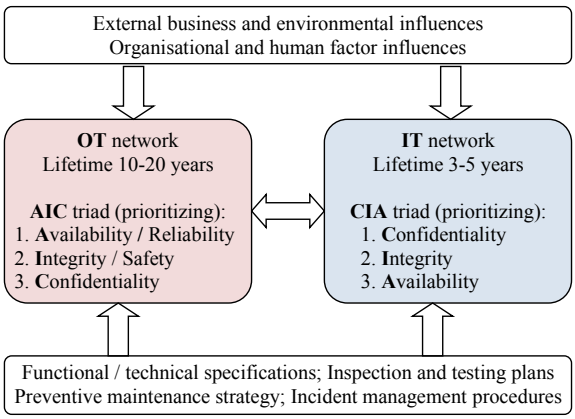

Fig. 3.3 Basic features concerning the OT and IT systems

that includes: inspection, testing, preventive maintenance plans and incident management procedures [21] to reduce the risk of major consequences due to potential hazardous events.

3.2.3 *RAMI 4.0 Reference Architecture Model*

Another recently published reference architecture model is the RAMI 4.0 (Reference Architectural Model for Industry 4.0), developed to support relevant business-oriented decision-making in practical applications [3, 31]. It seems to be also useful for the reliability, safety and security-related systemic analysis and management in the SMS [14]. This model describes the key elements of manufacturing system based upon the use of structured layers with distinguishing three axes:

- Architecture axis (see Fig. 3.4) of six different layers indicating the information depending view from the assets to business;
- Process axis (value stream) for including the various stages within the life of assets and the value-creation process based on IEC 62890;
- Hierarchy axis (hierarchy levels) for assigning the functional models to individual levels based on IEC 62264 and IEC 61512.

Some remarks concerning the security aspects are as follows:

- Layers—security-related aspects apply to all different levels; the risk evaluation has to be considered for the object/assets as a whole;
- Value stream—the owner of the object must consider security across its entire life-cycle;

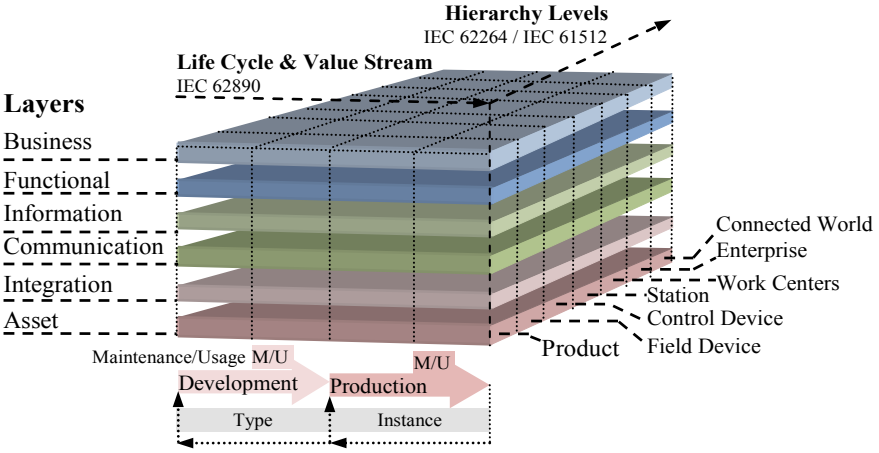

Fig. 3.4 The reference architecture model RAMI 4.0 for Industry 4.0 concept (based on [31])

– Hierarchy levels—all objects/assets are subjected to the security considerations (based on the risk evaluation) and need to possess or provide relevant security characteristics for fulfilling their tasks, thanks to applying appropriate protections.

Opinions are expressed that new opportunities are opened up by the Industry 4.0 idea, but also bring a host of challenges. Security by design, for instance, becomes an indispensable element in designing within Industry 4.0 concept. In some cases, security will be an enabler of new business models [31]. Security-related requirements can act in many cases as a skeleton that carries and holds together all of the structural elements within RAMI 4.0 model and, as a result, the design of the Industry 4.0 components and interrelated systems.

The security-related aspects can also play a role at relevant points of intersection between the various levels. This means that requirements shall be derived for some points of intersection by more specific analyses. The solutions have to be found for these requirements based on new capabilities of the Industry 4.0 components involved in the specific application in question. The manufacturers, integrators and asset owners should all be involved in implementing a holistic safety and security concept that brings the technical and organizational measures together [14, 31].

3.2.4 Knowledge and Standards Supporting the SMS Operational Analyses Including Functional Safety and Cybersecurity Aspects

Designing and operating of the SMS require a wide knowledge and considerable efforts. A rational way to deal with relevant issues is at least to consider existing standards. Examples of standards to be of interest in developing operational models of the SMS and the IACS are listed in Table 3.1. In Table 3.2, selected standards and publications useful for supporting the functional safety and cybersecurity analysis based on relevant risk analysis and management methods are collated.

Due to a considerable number of existing standards, the problem lays in purposeful selection of relevant standards, reports and publications, depending on the objectives of analyses. Some of these standards and publications, developed by various organizations to support the design and operation of the SMS or hazardous industrial plant, include mainly the functionality aspects of the IACS, and also some aspects to be included in related reliability, safety and security analyses. The objective is to improve functionality and to limit risks related to production goals with regard to criteria defined.

Nevertheless, a considerable research effort is still necessary to be undertaken directed towards development and successful implementation methods useful for the integration of existing methods and models. As it was mentioned, this chapter is directed towards integration of the functional safety and cybersecurity analyses of the SRCS as a part of the IACS.

Table 3.1 Selected standards useful for developing the operational models of the SMS and its IACS

Topic	Related standards	Remarks
Administration shell	IEC 62794 TR	Reference model for representation of production facilities (digital factory)
	IEC 62832	Industrial process measurement, control and automation—Digital factory framework
Life cycle and value stream	IEC 62890	Life cycle status
Hierarchy levels	IEC 62264/IEC 61512	
	ANSI/ISA 95	Enterprise control system levels
Configuration	IEC 6104 EEDL	Process control and electronic device description language (EDDL)
	IEC 6523 FDT	Information technology, Organization identification schemes
Engineering, data exchange	IEC 61360/ISO 13584 IEC 61987 IEC 62424 IEC 6214 ISO/IEC 20248	Standard data elements Data structures and elements Between P&ID tools and PCE-CAE tools For use in industrial automation systems Automatic identification and data capture
Communication	IEC 61784-2 IEC 61158 IEC 62351	Real-time ethernet (RTE) Industrial communications networks Power system information infrastructure
Condition monitoring	VDMA 24582	Fieldbus neutral reference architecture for condition monitoring in factory automation
OPC UA AutomationML	IEC 62541	Open platform communications unified architecture
	IEC 62714	The automation mark-up language

3.3 Functional Safety Analysis and Management in Life Cycle

3.3.1 Safety Functions for the Risk Reduction

The functional safety is defined as a part of general safety of an industrial hazardous plant installation or manufacturing machinery, which depends on a proper response of the SRCS during abnormal situation or accident to avoid or limit undesirable consequences. The functional safety methodology has been formulated in the generic standard IEC 61508 [24] and is appreciated in the design and operation of the electric/electronic/programmable electronic (E/E/PE) systems. Different names of the SRCS are used in various industrial sectors, for example, the safety instrumented systems (SIS) in case of the process industry sector [26], or the safety-related electrical control system (SRECS) for machinery [27]. Such systems are to be designed to

Table 3.2 Selected standards and publications useful for functional safety and cybersecurity analyses including the risk evaluation and management

Topic	Related standards and publications	Remarks
Risk management	ISO 31000 ISO 31010 ISO/IEC 27001	Risk management—guidelines Risk assessment techniques Information security management systems
	ISO/IEC 27005	Information security risk management
Functional Safety SIL—*safety integrity level* PL—*performance evel*	IEC 61508 ISO 13849-1 (PL) IEC 62061 IEC 61511	Generic standard FS of SRCS Machinery Production lines/systems Process industry
IACS cybersecurity SL—*security level* SAL—*security assurance level*	IEC 62443	Computer systems/networks security
	ISO 22100-4 DTR	Safety of machinery—security aspects
	VDI 2182	IT security for industrial automation
	IEC 63074 CD1	Security aspects of SRCS
	IEC 62351-12 TR	Security recommendation for power systems
Smart manufacturing/ Information security and risk management	NIST IR 8107	Standards for smart manufacturing systems
	NIST SP 800-30	Guide for risk assessments
	NIST SP 800-39	Managing information security risk
	NIST SP 800-53	Security and privacy control
	NIST SP 800-82	ICS security
	NIST SP 800-171	Protecting controlled information

perform specified safety functions to ensure that evaluated risk is reduced to the level specified for the particular industrial installation, and then maintained at a specified tolerable level during the life cycle of the system [16, 32].

Two different requirements are to be specified to ensure appropriate level of functional safety [24]:

– the requirements imposed on the performance of particular safety function being designed for the hazard identified,
– the safety integrity requirements, that is, 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 period of time. For the safety-related system, in which defined safety function is to be implemented, two probabilistic criteria are defined as presented in Table 3.3 for four categories of the SIL [24, 26], namely:

– the probability of failure on demand average (PFD_{avg}) of the SRCS in which particular safety function is to be implemented, operating in a low demand mode, or
– the probability of a dangerous failure per hour (PFH) of the SRCS operating in a high demand or continuous mode.

The SIL requirements for SRCS to be designed for implementing specified safety function stem from the results of the risk analysis and assessment to reduce sufficiently the risk of losses taking into account specified risk criteria, namely for the individual risk and/or the group or societal risk [24]. If the societal risk is of interest, the analyses can be generally oriented on three distinguished categories of losses, namely [16, 24]: Health (H), Environment (E) or Material (M) damage, then the safety integrity level required (SIL_r) for particular safety function is determined as follows:

$$SIL_r = \max\left(SIL_r^H,\ SIL_r^E,\ SIL_r^M\right) \tag{3.1}$$

In case of the machinery only the individual risk is to be considered, and then the performance level required (PL_r) [25] or the safety integrity level claimed (SIL CL) [27] is determined. The SRCS of machinery operates in a high demand or continuous mode, and therefore the PFH probabilistic measure (per hour) is to be evaluated and then assessed against relevant interval criteria.

Figure 3.5 illustrates these interval criteria of PFH in the context of risk graph for determining PL_r according to ISO 13849-1, and a method for determining SIL CL described in IEC 62061. The risk related to identified hazards is to be evaluated taking into account a measure of harm severity (S) that could result from that hazard, and the probability of occurrence of that harm. According to the ISO standard 12100 and ISO 22100 [33], the PFH is influenced by an exposure measure (F) of the person(s) to the hazard considered, the occurrence rate of hazardous event resulting, and the possibility (P) to avoid or limit the harm.

Thus, the PL_r for a safety function considered is determined according to the left side risk graph in Fig. 3.5, taking into account specific parameters to be evaluated

Table 3.3 Safety integrity levels and probabilistic criteria to be assigned to safety-related systems operating in a low demand mode or high/continuous mode

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	$[10^{-2}, 10^{-1})$	$[10^{-6}, 10^{-5})$

during the risk analysis [14, 25]. The PL_r categories, denoted from a to e, are related to required levels of the risk reduction, being highest in case of category e, which is equivalent to SIL CL 3 according to IEC 62061 [27].

Having the PL_r or SIL CL determined as described above, the relevant level has to be verified, whether it can be achieved by the SRCS of architecture proposed by the system designer, in which particular safety function will be implemented. The verification of the SRCS is based on the PFH probabilistic measure evaluated using appropriate probabilistic model. The result obtained is compared with the interval criteria presented in Fig. 3.5, and verified level PL or SIL is indicated that should be equal or higher than required.

For instance, if the PL (e.g. PL e) or SIL (e.g. SIL 3) obtained are equal or higher than the PL_r ($PL \geq PL_r$) or SIL CL ($SIL \geq SIL\ CL$), respectively, than the architecture proposed can be accepted. Otherwise, it is necessary to propose modified architecture and repeat the verification process as described above. It is worth to mention that the architecture includes the hardware, software and human component. The verification and validation procedure has to be carried out for each safety function considered to be implemented in the SRCS [25, 27].

3.3.2 Issues of the Safety Integrity Level Verification

As it was mentioned above, generally the SIL verification can be carried out for two categories of the operation mode, namely: (1) low operation mode, or (2) high or

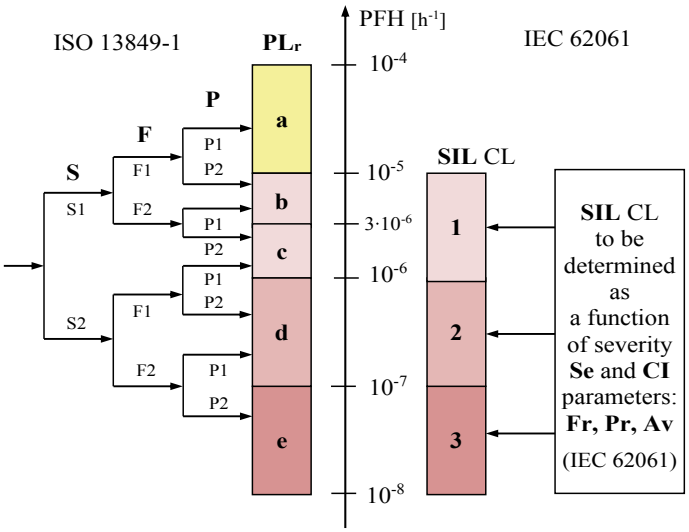

Fig. 3.5 Risk graphs for determining required performance level PL_r or safety integrity level claimed SIL CL (based on standards [25, 27])

continuous mode of operation [24, 34]. The former is characteristic for the process industry [26], and the latter is typical for the machinery [27] or the railway transportation systems, and also for monitoring and the real-time control of any installation using the DCS/SCADA technology.

Typical hardware architecture of an E/E/PE system [16], shown in Fig. 3.6, consists usually of three subsystems: (A) sensors and input devices (transducers, converters etc.), (B) logic device (e.g. safety PLC or safety relay modules) and (C) actuators, that is, the EUC and other output devices.

Such safety-related system constitutes a specific architecture of the hardware, software modules and communication conduits. The logic device comprises typically a safety PLC with its input and output modules. The subsystems shown in Fig. 3.6 can be generally of KooN configuration, for example, 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 [24]. The HFT (0, 1, 2) is an important parameter to be considered in final verification of the subsystem's SIL for the evaluated value of a safe failure fracture (S_{FF}).

Any redundant system, for example, the SRCS, is prone to a common cause failure (CCF) that can contribute significantly to decreasing its dependability due to potential failure mechanisms depending on the site-specific influence factors. The CCF is a failure resulting in one or more events, causing coincident failures of two or more channels in a multiple channel system, leading to the system failure. The multiple failures may occur simultaneously or over a period of time. Various probabilistic models are proposed to deal with CCF in safety-related systems, in particular the E/E/PE systems or SIS [24]. The CCF contribution in the PFD_{avg} or PFH is usually incorporated using the β-factor method [34].

If diagnostic tests run in each channel that can detect and reveal only a fraction of the failures, 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). The overall failure event probability per time unit of the subsystem is dangerous (D) failure due to potential failures including CCF is a function of several parameters [24, 34]

$$PF_D^{CCF} = f(\lambda_{Du}\beta, \lambda_{Dd}\beta_D, \ldots) \tag{3.2}$$

where:

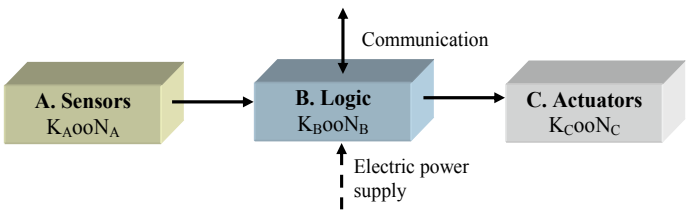

Fig. 3.6 General architecture of the E/E/PE system or SIS for implementing the safety function

Table 3.4 Proposal for evaluation values of β or β_D for subsystems [24]

Score for S or S_D	Values of β or β_D for the logic subsystem (%)	Values of β or β_D for the sensors or actuators (%)
≥120	0.5	1
[70, 120)	1	2
[45, 70)	2	5
<45	5	10

- λ_{Du} is the rate of danger (D) undetected (u) failure in a single channel, influencing the probability of failures that lie outside the coverage of the diagnostic tests; β is the common cause failure 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 danger (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 the common cause failure factor for detectable dangerous faults; as the repetition rate of the diagnostic testing is increased, the value of β_D falls increasingly below β.

In given subsystem probabilistic modelling of the value of β is determined for the score $S = X + Y$ to be evaluated for factors specified in the standard IEC 61508 and the value of β_D is evaluated for the score $S_D = X\ (Z + 1) + Y$ as it is presented in Table 3.4. These scores are evaluated respectively for the logic subsystem, and for the subsystems of sensors and actuators (final elements). In evaluating scores for X and Y, the following factors should be taken into consideration [24]:

(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.

Each of these factors is divided into several sub-attributes with specified sub-scores to be added to obtain final score, respectively for X and Y, and finally for S and S_D. The value of Z in calculating S_D depends on the diagnostic test interval and the diagnostic coverage (DC). For instance, in case of the subsystem of sensors or actuators, if DC ≥ 99% and the diagnostic test interval is between 2 h and 2 days, it is suggested: $Z = 1.5$. If the test interval is greater than 1 week, then $Z = 0$ [24].

Thus, the values of β and β_D parameters used in the probabilistic modelling of subsystems depend significantly on factors specified in IEC 61508 and the expert opinions collected during the functional safety analysis of the E/E/PE system or SIS. In publication [34] two examples are presented of the SIL verification of given SRCS

architecture using the probabilistic models of subsystems with regard to the CCF analysis. The architectural constrains with regard to the safe failure fraction (S_{FF}) for subsystems were also considered. It seems to be justified to assume that some categories of factors specified above are also relevant in case of the cybersecurity analysis.

3.4 Cybersecurity of the Safety-Related Control System

The security-related remote attacks are becoming increasingly important threats to the IT and OT systems, especially the IACS operating within industrial networks of hazardous plants [6, 8, 23] and the SMSs characterized in this chapter and publications [2, 3, 14]. The internal or external threats can initiate an IT or OT security-related incidents with the potential to adversely impact the SRCS and machinery operations. Vulnerability understood as a security-related weakness of the IT and/or OT networks that can be exploited by various threats to trigger hazardous events making losses. It is an important issue to be adequately treated in the BCM [20].

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 [19, 33]: database injection, spoofing and impersonation, phishing, malicious code, Denial of Service (DoS), escalation of privileges, physical destruction, etc. The analyses should be also carried out to identify the SRCS vulnerability that can be exploited by threats, potentially impacting the safety of entire manufacturing system.

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 [23]. Generally, the potential responses to the security risks should take following steps [33]:

(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.

The standard IEC 62443 [23] proposes an approach to deal systematically with the security aspects of the IACS. Four security levels (SLs) 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 [19] these levels are also proposed to deal with the SRCS security of machinery.

The SL is related to seven 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 proposed to apply a related vector of seven FRs specified above. Such vector is proposed for describing the security requirements for a zone, conduit, component or system. It may contain the integer numbers of SL from 1 to 4 or 0 to be assigned to consecutive FRs. A general format of the security assurance level (SAL) is defined as follows [23]:

$$\text{SL - ? ([FR], domain)} = \left[\text{IAC UC SI DC RDF TRE RA}\right] \tag{3.3}$$

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

For instance, according to the standard [23], it can be written as follows:

(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 the RA component is specified, instead of a seven-dimensional SAL vector SL-C.

Thus, three type of vectors describing SL_i for consecutive FR_i of particular domain are distinguished:

– SL-T (Target SAL)—the desired levels of security;
– SL-C (Capability SAL)—the security level that device can provide when properly configured;
– SL-A (Achieved SAL)—the actual level of security of a particular device.

The SL_i numbers provide a qualitative information addressing relevant protection scope of the domain or zone considered, for example, for the IACS or the SRCS as its part, as presented in Table 3.5.

Table 3.5 Security levels and protection description of the IACS domain [19, 23]

Security levels	Description
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

For instance, in the case of FR 1—identification and authentication control (IAC)—the security levels shall be interpreted in a following way "Identify and authenticate the SRCS users by mechanisms against" [19]:

- causal and coincidental access by unauthorized entities (SL 1),
- intentional unauthorized access by entities using simple means (SL 2),
- intentional unauthorized access by entities using sophisticated means (SL 3),
- intentional unauthorized access by entities using sophisticated means with extended resources (SL 4).

For improving the SRCS security it is suggested to elaborate guidance (the instruction handbook) for the end user that includes the following issues [19, 33, 35]:

(A) Restriction of logical/physical access to the IT systems with potential influence on safety, for example, 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 example, checking regularly means for detecting failed IT system components or unavailable service according to the specifications of the machine/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 example, using provided means for setting up and ending a remote access session according to the specifications of the machine/component manufacturer; using encryption means for initiating a remote service according to the specifications of the machine/component manufacturer; watching any remote access session with a restriction of duration for remote access, and so on.

Such topics should be included and carefully treated in a security information and event management (SIEM) to be developed and used proactively in practice according to requirements given in ISO/IEC 27001 [36], and supported by the information security risk management as suggested in ISO/IEC 27005 [37]. Its specific requirements to be formulated should include the target SAL (SL-T) and then verified as achieved SAL (SL-T) taking into account the capability SAL (SL-C) of technology applied. Defined system requirements (SRs) and specific requirement enhancements (REs) for consecutive FRs to be fulfilled at relevant SLs from 1 to 4 are specified in the IEC 62443 standard [23] and a recent publication [14].

3.5 Integrated Functional Safety and Cybersecurity Analysis and Management

The IEC 62443 [23] series of standards consists of 14 parts but some of them are still in development. The main objective of this series is to cover important topics of the IACS security entirely. In the second edition of the generic functional safety standard IEC 61508 [24] it is suggested to use the IEC 62443 standard to deal with the 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 have been rather loosely linked [29]. As it was mentioned, also in case of the SRCS of machinery there is a need to deal more systematically with security issues, as it has been lately emphasized [19, 33].

It is worth to mention that the SRCS security level to be achieved depends strongly on the quality of an information security management system (ISMS) established in industrial practice. The objective of the ISMS is to monitor, continuously control, maintain and, wherever justified, improve the IT and OT security. The IEC 62443 standard is based on general requirements and stipulations of the ISO/IEC 17799 and ISO/IEC 27000 series, especially as regards basic security requirements [36]. Due to complex and dynamic internal and external conditions making technical specifications related to the IT and OT security solutions for implementing in industrial practice is quite challenging.

An important task to be undertaken is the risk evaluation and management, as it is postulated both in ISO/IEC 27001 [36] and ISO/IEC 27005 [37]. It includes the consideration of all functional components of the information system including the hardware (HW) and software (SW), communication conduits and relevant human/organizational issues, especially those related to the IT and OT safety and security. Opinions are expressed that the quantitative risk evaluation is very difficult due to the complexity of the IT and OT system and many influencing factors involved. The credibility of such evaluation depends on a framework adapted and availability of data, and expert opinions concerning specific domain to be evaluated.

Opinions are also expressed that the CIA triad (confidentiality, integrity, availability) is a justified order of requirements in the IT security analysis (see Fig. 3.3), but in case of OT a reversed triad, namely AIC (availability, integrity, confidentiality) is more appropriate. As it was mentioned above the domain SAL defined in IEC 62443 is to be evaluated using the vector of seven FRs, as explained by the formula (3.3). So, there are some doubts how to match these two kinds of requirements in the security-related analyses. It seems to be reasonable that the fundamental requirements of IAC, UC, SI and TRE should be mapped to integrity (I), RA to availability (A), and DC, RDF to confidentiality (C) [14, 29].

Additional issue, worth to be explained in context of the cybersecurity evaluation, is related to the definition of seven evaluation assurance levels (EALs) in the so-called common criteria standard (IEC 15408) [38] that are to be applied in defining the IT security requirements. As explained above only four SLs are defined in IEC 62443. This issue was discussed in the publication [39] in the context of generic functional

Table 3.6 Proposed correlation between SIL and SAL [18]

Safety integrity level (SIL)	Security assurance level (SAL)	Explanation
SIL 1	SAL 1	SAL assignment is based on asset owner's assessment
SIL 2	SAL 2	
SIL 3 and SIL 4	SAL 3	Reserved for total system failure
	SAL 4	Reserved for loss of life

safety standard IEC 61508 [24], in which also four SILs are distinguished (see Table 3.3). So, the problem is encountered how to integrate these concepts in the integrated functional safety and cybersecurity analysis.

In the publication [18] the correlation between SIL and SAL is proposed as it is shown in Table 3.6. Similar correlation can be proposed for the SRCS of machinery; however, remembering that in the machinery sector the highest SIL to be evaluated is SIL 3 (see Fig. 3.5).

In view of the above we propose an approach for integrated functional safety and cybersecurity analysis based on a framework of existing concepts and accepted models suitable to apply the quantitative and qualitative information available, similarly as in the knowledge-based systems [14, 40]. We start from defining the safety functions with regard to hazards and threats identified and then evaluate required risk reduction regarding the risk criteria defined as it was described above in item 3.3.1. It allows to determine: the required safety integrity level SIL_r according to IEC 61508 according to the formula (3.1), or the safety integrity level claimed SIL CL (IEC 62061), or the required performance level PL_r (ISO 13849-1) as it is shown in Fig. 3.5.

As it is known, the levels: the safety integrity level required SIL_r (1, 2, 3 or 4) [24], SIL CL (1, 2 or 3) [27], or the performance level required PL_r (a, b, c, d or e) [25], are related to the required risk reduction with regard to relevant individual or social risk criteria [16]. For instance, the average probability of failure on demand PFD_{avg} (see Table 3.3) is related to the risk reduction measure as its reciprocal.

The PL_r or SIL_r or SIL CL determined for particular safety function has to be then be verified using probabilistic model of the SRCS of architecture proposed at the design stage (see the left site blocks for functional safety evaluation in Fig. 3.7). Such architecture includes generally the hardware configuration and requirements concerning software [24]. Parallelly, the security-related evaluation is to be carried out as it is shown in Fig. 7 (the right side) for cybersecurity evaluation. The integrated functional safety and cybersecurity analysis are repeated when justified to enable a rational management of the SRCS domain in life cycle.

Additional issue to be considered is associated with expressing SAL as a single number to be assigned to the security level achieved SL-A for given domain, as it is outlined in the formula (3.3), according to the standard IEC 62443. It would lead to sometimes disputable requirement that the security levels SL_i would be the same for each FR_i. For instance, confidentiality plays in some cases a minor role for

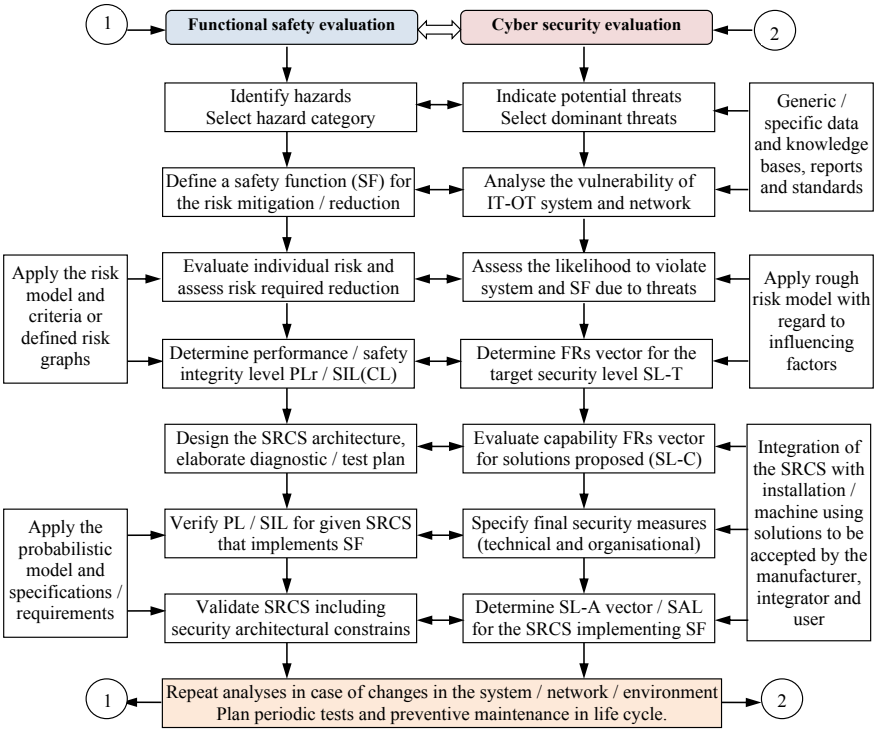

Fig. 3.7 Integrated functional safety and cybersecurity analysis for the SRCS domain

safety-related control system and encryption of all data might lead to complications in testing and the time response longer than required. So generally, different levels of SL_i may be assigned to seven consecutive elements of the FR vector.

This problem was noticed and discussed by Braband in the publication [29]. Only in simple cases of equal levels SL_i for consecutive FR_i (i from 1 to 7) determining SAL of domain of interest (e.g. the SRCS) is straightforward, for instance, SAL 1 = [1 1 1 1 1 1 1]. Generally, the SL_i can be different depending on the security technology applied or FR_i relevance for the domain considered. So, he suggests to use some security profiles, for example, for particular zones or conduits. However, it might also lead to a number of profiles, difficult for evaluation and security-related decision-making.

In our earlier publications [39] it was assumed that resulting SAL for the domain considered can be determined based on dominant FR_i and some common sense rules, in a similar way as in the methodology outlined in the IEC 15408 (common criteria) standard [38]. In this methodology seven evaluation assurance levels (EALs) are distinguished, related to classes of the security assurance requirements (SARs) and defined scope of fulfilling relevant requirements.

Table 3.7 Proposed correlation between security index SI^{Do} or SAL for the domain to be evaluated and final SIL to be attributed to the SRCS of hazardous installation

Security index	SIL verified according to IEC 61508[a]			
SI^{Do} and SAL	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

[a]verification includes the architectural constrains with regard to S_{FF} and HFT of subsystems

We propose below another method for determining the security level achieved SL-A (SAL) for the domain considered assuming that the weights w_i of security levels SL_i for consecutive (and relevant) FR_i are evaluated by experts. These weights can differ in general 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 to the domain considered. It is suggested in the IEC 62443, as explained in the formula (3.3). There can be cases that only one relevant FR_i is relevant [23].

Thus, instead of determination of SAL for given domain based on dominant FR_i we propose alternatively to evaluate a domain security index SI^{Do} and then to assign a number of SAL as described in first column of Tables 3.7 and 3.8. The importance I_i of FR_i is evaluated by experts for specific domain, for example, using integer number on the scale from 1 to 5 (or 1–10), and 0 if FR_i is not relevant, and then the weight w_i of given FR_i is calculated according to following formula

$$w_i = \frac{I_i}{\sum_{i=1}^{7} I_i} \tag{3.4}$$

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 relevant) for relevant (Re) fundamental requirements (FR_i) is evaluated as follows

$$SI^{Do} = \sum_{i \in Re} w_i SL_i \tag{3.5}$$

Four intervals of the domain security index SI^{Do} (from SI^{Do1} to SI^{Do4}) are proposed in the first column of Tables 3.7 and 3.8 for assigning the category number of SAL from SAL 1 to SAL 4. Such approach corresponds to 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 the SRCS in hazardous installation are presented in

Table 3.7. It was assumed that SIL has been verified according to IEC 61508 including such aspects as the common cause failures (CCFs) in probabilistic modelling, and the architectural constrains regarding the safe failure fraction (S_{FF}) and the hardware fault tolerance (HFT) of subsystems [24, 34].

Table 3.7 can be used to support the function safety and cybersecurity-related decision-making. For instance, if safety integrity level required, obtained from the risk assessment, is SIL_r 3, and it was positively verified according to IEC 61508 for the SRCS as SIL 3, we select the column with number 3. The SAL of the domain should be at least SAL 3 to attribute finally SIL 3 to the SRCS in which relevant safety function is implemented. If the SAL determined in the security analysis of domain considered would be lower (e.g. SAL 2), then the analyst should improve the system security (lowering its vulnerability) to increase SL_i of relevant FR_i to obtain at least SAL 3.

Other correlations are proposed in Table 3.8 for finally attributing the SIL or PL to the SRCS according to, respectively, IEC 62061 [27] or ISO 13849-1 [25]. Similarly, as it was explained above, if required performance level would be SIL CL 2 (or PL_r d), and such level were positively validated as SIL 2 (or PL d) the column 2 (d) of Table 3.8 is selected for the security validation. To obtain PL d the security assurance level should be at least SAL 2. If SAL would be lower (SAL 1) the security of SRCS should be improved to increase SL_i of relevant FR_i to obtain at least SAL 2, and finally validated safety integrity level SIL 2.

A case study was carried out concerning a modern end impregnation line used to treat yarns made of polyamide, polyester, viscose and other raw materials, so they are suitable for applications in tires [14]. A safety function of the pull roll section monitoring and door locking of the installation was analyzed. The performance level required PL_r was determined using a risk graph in Fig. 3.5 for following parameters indicated by a safety engineer for following path: S2, F1, and P2, leading to PL_r d.

The verification of the PL requires probabilistic modelling of the SRCS of known architecture. For HFT = 1, verified performance level obtained is PL e. Taking into

Table 3.8 Proposed correlation between security index SI^{Do} or SAL for the domain evaluated and final SIL (PL) to be attributed to the SRCS of machinery

Security index	SIL (PL) verified according to IEC 62061[a] (ISO 13849-1)			
SI^{Do} and SAL	(a)	1 (b/c)	2 (d)	3 (e)
$SI^{Do1} \in [1.0, 1.5)$/SAL 1	SIL—(PL a)	SIL 1 (PL b/c)	SIL 1 (PL b/c)	SIL 2 (PL d)
$SI^{Do2} \in [1.5, 2.5)$/SAL 2	SIL—(PL a)	SIL 1 (PL b/c)	SIL 2 (PL d)	SIL 2 (PL d)
$SI^{Do3} \in [2.5, 3.5)$/SAL 3	SIL—(PL a)	SIL 1 (PL b/c)	SIL 2 (PL d)	SIL 3 (PL e)
$SI^{Do4} \in [3.5, 4.0]$/SAL 4	SIL—(PL a)	SIL 1 (PL b/c)	SIL 2 (PL d)	SIL 3 (PL e)

[a]verification includes the architectural constrains with regard to S_{FF} and HFT of subsystems

account the domain of SRCS in which the safety function is implemented the vector of SL-A 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 Eq. (3.5), the result obtained is $SI^{Do} = 2.43$, that is, SAL 2. Looking at the column 3 (e) of Table 3.7 the final performance level validated with regard to the security requirements is PL d, the same as required performance level PL_r. For the case of hardware fault tolerance HFT = 0 (series configuration of the SRCS), the verified performance level obtained was PL c, lower than required performance level PL_r d. Thus, applying of the redundancy in the SRCS is necessary and the domain security assurance level SAL 2.

3.6 Conclusions

Unprecedented development of the smart manufacturing systems (SMSs) is observed that have the significant potential to make innovative production more profitable and improve business processes. Advanced technologies are under development in area of the internet of things (IoT) and industrial internet of things (IIoT) that offer new manufacturing possibilities, but require also effective monitoring and the control systems having sufficiently high reliability, safety, and security characteristics. These characteristics are especially important when hazardous installations of industrial plants are evaluated to elaborate effective management strategy in life cycle.

Traditionally, the industrial manufacturing system includes the information technology (IT) and the operational technology (OT). Lately, using the cloud technology (CT) is often considered as an external network being important for distributed manufacturing and coordinated management. Advanced automation and control systems are also in development based, for example, on OPC UA and AutomationML concepts that offer new manufacturing solutions and production flexibility. However, it causes also some problems to be solved that include the reliability, safety and security properties, crucial for the business continuity management (BCM) to mitigate the risks of abnormal situations and major accidents contributing to high losses.

Selected design and operational aspects of the OT and IT networks have been overviewed and discussed in this chapter in the context of functionality and architecture of the industrial automation and control systems (IACS). Emphasis was put on the functional safety and cybersecurity of the industrial control systems and networks. These issues are becoming crucial, because the IACS that includes the safety-related control system (SRCS) plays a key role in innovative high-quality manufacturing, especially in so-called smart manufacturing systems (SMSs) of Industry 4.0.

In this chapter a method is proposed for integrated functional safety and cybersecurity analysis, with regard to the concepts outlined in the generic functional safety standard IEC 61508 (7 parts) and the cybersecurity standard IEC 62443 (14 parts). To limit the vulnerability of the IT and OT systems and networks, and the SRCS to

be designed and operated to reduce relevant risks, a set of security-related fundamental requirements (FRs) defined in IEC 62443-1 is considered in the analyses and evaluations.

The method proposed uses the individual and/or societal risk graphs for determining the performance level required (PL_r) or the safety integrity level required (SIL_r) or the safety integrity level claimed (SIL CL) of consecutive safety functions defined in the analyses. These levels are then verified to indicate that the required PL or SIL is achievable in the designed SRCS of architecture proposed, in which particular safety function is to be implemented. For that purpose relevant probabilistic models of the SRCSs are developed with regard to potential common cause failures (CCFs), when a hardware redundancy is to be applied. Then, the verified SIL is validated with regard to determined SAL of the domain of interest, for example, the SRCS domain in which particular safety function is implemented, including internal and external communications.

The dependability of the SRCS performing the safety-related functions can be influenced both by technical factors, including requirements concerning hardware (HW) and software (SW), and also the human and organizational factors [1, 15, 17]. These aspects require further research, especially in the context of the design and operation of high complexity manufacturing systems, including the functional safety and cybersecurity aspects with regard to the defence in depths (D-in-D) concept and related strategy to be elaborated and applied in particular industrial plant or smart manufacturing system, characterized by the venture capital, production capacity, existing or emerging hazards and threats that influence various risks in changing environment.

References

1. Kosmowski, K. T., & Gołębiewski, D. (2019). Functional safety and cyber security analysis for life cycle management of industrial control systems in hazardous plants and oil port critical infrastructure including insurance. *Journal of Polish Safety and Reliability Association, 10*(1), 99–126.
2. Lu, Y., Morris, K. C., & Frechette, S. (2016). Current standards landscape for smart manufacturing systems. Systems Integration Division Engineering Laboratory, NISTIR 8107.
3. Li, S.W. et al. (2017). *Architecture alignment and interoperability, an industrial internet consortium and platform industrie 4.0.* IIC:WHT:IN3:V1.0:PB:20171205.
4. Vathoopan, M. Walzel, H., Eisenmenger, W., Zoitl, A., & Brandenbourger, B. (2018). AutomationML mechatronic models as enabler of automation systems engineering: Use-case and evaluation. In *Proceedings of the IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, IEEE 2018.
5. Kivelä, T., Golder, M., & Furmans, K. (2018). Towards an approach for assuring machinery safety in the IIoT-age. *Logistics Journal: Proceedings.*
6. Felser, M., Rentschler, M., & Kleinberg, O. (2019). Coexistence standardisation of operational technology and information technology. *Proceedings of the IEEE.*
7. MERgE. (2016). *Safety & security, recommendations for security and safety co-engineering.* Multi-Concerns Interactions System Engineering ITEA2 Project No. 11011.

8. SESAMO. (2014). *Integrated design and evaluation methodology. Security and safety modelling*. Artemis JU Grant Agr., No. 2295354.
9. EC. (2013). *Cybersecurity strategy of the European Union—An open, safe and secure cyberspace*. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, access: April 2020.
10. CISA. *Assessments: Cyber Resilience Review (CRR)*, us-cert.gov/resources/assessments, access: April 2020.
11. ENISA. (2016). *Communication network dependencies for ICS/SCADA Systems*. European Union Agency for Network and Information Security.
12. HSE-1. (2015). *Cyber Security for Industrial Automation and Control Systems (IACS)*, Health and Safety Executive (HSE) Interpretation of Current Standards on Industrial Communication Network and System Security, and Functional Safety.
13. HSE-2. (2016). *Cyber Security for Industrial Automation and Control Systems (IACS)*, Health and Safety Executive (HSE) Report for Chemical Explosives and Microbiological Hazard Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors.
14. Kosmowski, K. T., Śliwiński, M., & Piesik, J. (2019). Integrated functional safety and cybersecurity analysis method for smart manufacturing systems. *TASK Quarterly, 23*(2), 1–31.
15. Kosmowski, K. T., & Śliwiński, M. (2016). Organizational culture as prerequisite of proactive safety and security management in critical infrastructure systems including hazardous plants and ports. *Journal of Polish Safety and Reliability Association, 7*(1), 133–145.
16. Kosmowski, K. T. (2013). *Functional safety and reliability analysis methodology for hazardous industrial plants*. Gdansk University of Technology Publishers.
17. Nardello, M., Møller, C., & Gøtze, J. (2017). *Organizational learning supported by reference architecture models: industry 4.0 laboratory study*. Complex Systems Informatics and Modeling Quarterly (CSIMQ) Article 69, Issue 12.
18. Holstein, D. K., & Singer, B. (2010). *Quantitative security measures for cyber & safety security assurance*. ISA: Presented at ISA Safety & Security Symposium.
19. IEC 63074. (2017). *Security aspects related to functional safety of safety-related control systems*. International Electrotechnical Commission.
20. ISO 22301. (2012). *Societal security—Business continuity management—Requirements*. International Organisation for Standardisation.
21. Gołębiewski, D., & Kosmowski, K. T. (2017). Towards process based management system for oil port infrastructure in context of insurance. *Journal of Polish Safety and Reliability Association, 8*(1), 23–37.
22. Misra, K. B. (Ed.). (2008). *Handbook of performability engineering*. London: Springer.
23. IEC 62443. (2018). *Security for industrial automation and control systems*. Parts 1–14 (some parts in preparation). International Electrotechnical Commission.
24. IEC 61508. (2016). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, Parts 1–7. International Electrotechnical Commission.
25. ISO 13849-1. (2015). *Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design*. International Organisation for Standardisation.
26. IEC 61511. (2016). *Functional safety: Safety Instrumented Systems for the Process Industry Sector*. Parts 1–3. International Electrotechnical Commission.
27. IEC 62061. (2005). *Safety of machinery—Functional safety of safety-related electrical, electronic and programmable electronic control systems*. International Electrotechnical Commission.
28. ISO 22400. (2014). *Automation systems and integration—Key performance indicators (KPIs) for manufacturing operations management*, Parts 1 and 2. International Organisation for Standardisation.
29. Braband, J. (2016). *What's Security Level go to do with Safety Integrity Level?* 8th European Congress on Embedded Real Time Software and Systems (ERTS 2016), hal-01289437, Toulouse.
30. IS. (2019). *Industrial security*. Siemens, siemens.com/industrial-security. Access: July, 2019.

31. RAMI 4.0. (2016). *Reference architecture model Industrie 4.0*. DIN SPEC 91345.
32. Kosmowski, K. T. (2006). Functional safety concept for hazardous system and new challenges. *Journal of Loss Prevention in the Process Industries, 19*(1), 298–305.
33. ISO 22100-4. (2018). *Safety of machinery—Relationship with ISO 12100, Part 4: Guidance to machinery manufacturers for consideration of related IT-cyber security aspects*, International Organisation for Standardisation.
34. 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* (pp. 420–433). Springer International Publishing AG.
35. Malm, T., Ahonen, T., Välisalo, T. (2018). *Risk assessment of machinery system with respect to safety and cyber-security*. Research Report-VTT-R-01428-18.
36. ISO/IEC 27001. (2013). *Information technology—Security techniques—Information security management systems—Requirements.*
37. ISO/IEC 27005. (2018). *Information technology—Security techniques—Information security risk management*.
38. ISO/IEC 15408. (2009). *Information technology, Security techniques—Evaluation criteria for IT security*. Part 1–3.
39. Kosmowski, K. T., Śliwiński, M., Barnert, T. (2006). Functional safety and security assessment of the control and protection systems. *European Safety & Reliability Conference*, ESREL 2006, Estoril. Taylor & Francis Group, London.
40. Kosmowski, K. T., Śliwiński, M. (2015). Knowledge-based functional safety and security management in hazardous industrial plants with emphasis on human factors. In *Advanced systems for automation and diagnostics*, PWNT, Gdańsk.

Kazimierz T. Kosmowski is a Professor at the Gdansk University of Technology, Poland, Department of Electrical and Control Engineering. His scientific interest includes the reliability theory, and the safety and security in technical systems, in particular the functional safety and cybersecurity of industrial control systems. He is involved in teaching Masters courses and training courses for engieers from the industry within a state certification program of persons responsible for functional safety. He contributed to a number of international, state and university projects, and visited a number of universities and research institutes in Poland, Japan, Austria, Germany and Switzerland. He is the author of five books, seven book chapters and over two hundred peer reviewed papers on various aspects of reliability, safety and security in technical systems, including the human reliability aspects. He is a board member of the Polish Safety and Reliability Association.