INTEGRATED FUNCIONAL SAFETY AND CYBERSECURITY. ANALYSIS METHOD FOR SMART MANUFACTURING SYSTEMS

KAZIMIERZ T. KOSMOWSKI[1], MARCIN ŚLIWIŃSKI[1] AND JAN PIESIK[2]

[1] *Faculty of Electrical and Control Engineering*
Gdansk University of Technology
Narutowicza 11/12, 80–233 Gdansk, Poland

[2] *Michelin Polska S. A.*
Leonharda 9, 10–454 Olsztyn, Poland

(received: 18 January 2019; revised: 4 February 2019;
accepted: 8 February 2019; published online: 25 February 2019)

Abstract: This article addresses integrated functional safety and cybersecurity analysis with regard to: the generic functional safety standard IEC 61508 and the cyber security standard IEC 62443 concerning an industrial automation and control system (IACS). The objective is to mitigate the vulnerability of information technology (IT) and operational technology (OT) systems, and reduce relevant risks taking into account a set of fundamental requirements (FRs). A method is proposed for determining and verifying the performance level (PL) or the safety integrity level (SIL) of defined safety functions, and then validating these levels depending on the security level (SL) of a particular domain, *e.g.* a safety related control system (SRCS). The method is general in the sense that it is based on risk graphs prepared for individual risk and/or societal/group risk with regard to the criteria defined.

Keywords: smart manufacturing systems, Industry 4.0, information technology, operational technology, industrial automation and control system, functional safety, cybersecurity, risk evaluation

DOI: https://doi.org/10.17466/tq2019/23.2/c

Acronyms

AIC availability, integrity, confidentiality
ALARP as low as reasonably practicable
AS alarm system
BC batch control

BCM business continuity management
BPCS basic process control system
CBA cost-benefit analysis
CC continuous control
CFAT cybersecurity factory acceptance
CI class index
CIA confidentiality, integrity, availability
CIS critical infrastructure
CME current maintenance execution
CMM computerized maintenance management
CRM customer relationship management
CS cybersecurity
CSAT cybersecurity site acceptance test
CT cloud technology
DC discrete / sequence control
DCS distributed control system
DoS denial of service
DSS decision support system
EAL evaluation assurance level
EM environmental management
ERP enterprise resource planning
EUC equipment under control
FRs fundamental requirements
FS functional safety
HFT hardware fault tolerance
HMI human machine interface
HSI human system interface
HW hardware
IACS industrial automation and control system
ICS industrial control system
IEC International Electrical Commission
IIoT industrial internet of things
IoT internet of things
I/O input / output
IS international standard
ISMS information security management system
ISO International Standard Organization
IT information technology
KPIs key performance indicators
MES manufacturing execution system
MOM manufacturing operation monitoring
OEE overall equipment effectiveness
OPC UA open platform communications, unified architecture
OT operational technology
OTMS operational technology maintenance system
PFH danger failure rate per hour
PL performance level
PLr performance level required
PLC programmable logic controller
PLM product lifecycle management
PM preventive maintenance

QM quality management
RAMI 4.0 reference architectural model for Industry 4.0
RAMSS reliability, availability, maintainability, safety and security
RM risk management
SAL security assurance level
SARs security assurance requirements
SCADA supervisory control and data acquisition
SCM supply chain management
SF safety function
SI^{Do} security index for the domain
SIL safety integrity level
SIL CL safety integrity level claimed
SIS safety instrumented system
SL security level
SMS smart manufacturing system
SRCS safety related control system
SRS safety-related system
SW software
TS technical specification
TSN time sensitive networking
WAN wide area network

1. Introduction

Nowadays manufacturers face ever-increasing variability demands for products, greater customization, smaller lot sizes and supply-chain changes that would be possible in practice, but unfortunately also disruptions occur that can cause manufacturing losses. In some industrial sectors various hazards and risks are encountered causing relatively high business and insurance risks [1]. Wishing to be successful, manufacturers have to choose and incorporate technologies that help them quickly adapt to the rapid changes in the 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 an emerging, information-centric, so-called *Smart Manufacturing System* (SMS) that maximizes the use, flow and re-use of data throughout the enterprise and cooperating industrial companies [2]. The SMS design and operation principles as well as the business expectations are similar to those that stand behind the idea of Industry 4.0 [3].

The ability of potentially disparate systems to gather and exchange the production and business data rests critically on information related standards that enable communication and services to effectively run, supervise and coordinate 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 [1]. The technical and organizational solutions of an SMS should maximize those capabilities by using advanced technologies that

promote rapid flow and widespread use of digital information within and between manufacturing systems [2].

There are opinions, based on evidence from industrial systems and networks that 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, SMSs use information and communication technologies along with intelligent software applications to achieve the following major goals [2]:

(1) support intelligent marketing for better production planning;
(2) develop innovative technologies and products;
(3) optimize the use of labor, material, and energy to produce customized, high quality products for on-time delivery;
(4) quickly respond to the market demands and supply chains with support of advanced logistics system.

Some computer applications are to be used in industrial practice to support achieving these goals including [2]: ERP (*enterprise resource planning*), CRM (*customer relationship management*), SCM (*supply chain management*), MES (*manufacturing execution system*), and PLM (*product lifecycle management*).

Traditionally, two kinds of technologies are often distinguished within a manufacturing system, namely: *operational technology* (OT) and *information technology* (IT). Lately, a relatively new technology, named the *cloud technology* (CT), has been also used in practice, which is of special interest in the case of SMSs. This technology in principle supports the implementation of advanced Internet technologies, currently being under rapid development, known as: *Internet of Things* (IoT) and *Industrial Internet of Things* (IIoT) [4]. Nowadays the factory automation and process control systems, networks and protocols of OT are increasingly merged with those of IT. Although the requirements formulated for OT and IT are in principle different, the networks and protocols for communication in the factory automation and process control systems must allow for coexistence and convergence between IT and OT systems [5].

The idea of SMSs assumes openness of markets and flexible worldwide cooperation of interested companies. It could not be effective without coordinated international standardization. However, some problems have been encountered in the industrial practice due to the necessity of designers and operators to use many existing standards that have been published by various international organizations, even those still under development. It concerns in particular the IT and OT design principles in relation to the expected functionality and architecture of the IACS including safety and security aspects [2].

Historically, the standards concerning OT were developed by the International Electrical Commission (IEC). IT, on the other hand, is rather a domain of the International Telecommunication Union (ITU) and the International Standardization Organization (ISO), which takes over most of the standards in the communication field from the IEEE 802 Standards group. A key technology for

real-time applications in the factory installations is merging OT and IT, *e.g.*, on an Ethernet network, with *time sensitive networking* (TSN). The adoption of an industrial protocol concept OPC UA (*open platform communications*, *unified architecture*) can provide connections from factory automation and control systems to the cloud infrastructure. These issues are related to the AutomationML concept [5].

However, questions may be raised concerning security issues of such connections in relation to safety principles and requirements. Considerable effort has been expended by the research community to identify these problems [6, 7], point out more important issues that require further research and help in the development and implementation of advanced safety and security technologies. The expectations of the industry are high and some institutions are involved in practically oriented research to propose some solutions for implementation in industrial practice in a relatively short time [8–10].

The dependability of automation and control systems [11] performing safety functions is to be influenced by both technical factors, *e.g.* requirements concerning *hardware* (HW) and *software* (SW) of the IACS, and organizational factors [1, 12]. The functional safety and cybersecurity related KPIs (*key performance indicators*) [11] and relevant factors should be carefully evaluated and assessed in the verification and validation process of the IACS, especially the safety-related control system (SRCS) of the manufacturing system at the design stage, and then after its modernizing or introducing organizational changes [13, 14].

In this paper selected design aspects of the *operational technology* (OT) and the *information technology* (IT) are overviewed and discussed in the context of the *industrial automation and control system* (IACS) functionality and architecture, especially those related to the safety and security aspects of computer systems and industrial networks. The design issues of *functional safety* (FS) and *cybersecurity* (CS) are of special interest [15] as IACS and computer networks play nowadays a key role in advanced manufacturing systems, especially SMSs operating in accordance with the Industry 4.0 idea and principles. *Business continuity management* (BCM) [16] in an SMS requires careful consideration of various aspects within an integrated RAMSS (*reliability, availability, maintainability, safety* and *security*) framework. In such analyses the risk evaluation and management in a life cycle is of special interest for both industrial and insurance companies [17].

The main objective of this article is to propose a method and conceptual framework for integrated analyses of *functional safety* (FS), described in the generic functional safety standard IEC 61508-x (7 parts) [13], and *cybersecurity* (CS) of *industrial automation and control systems* (IACS), outlined in IEC 62443-y (14 parts) [18]. To limit the vulnerability of IT and OT, and reduce the risks of potential hazardous events of large losses, a set of seven *fundamental requirements* (FRs) described in IEC 62443-1 is taken into account.

2. Reference model of IT and OT technologies including IACS

The following advanced systems are to be designed, operated and managed in a life cycle for effective execution of manufacturing processes in an SMS:

A. *Operational technology maintenance system (*OTMS*)* for preventive maintenance planning to achieve the required quality of products and high reliability/availability of manufacturing subsystems and an entire manufacturing system, characterized, *e.g.*, by *overall equipment effectiveness* (OEE); the OEE should be periodically evaluated in industrial practice to support the *business continuity management* (BCM) as it represents a measure of synthetic effectiveness of a specific manufacturing system.

B. *Industrial automation and control system* (IACS) that should assure the required functionality and reliability to limit manufacturing system outages to effectively achieve the production goals, and to adequately reduce the safety and security related risks; the IACS design includes high quality and reliability hardware (HW) and software (SW) to be carefully verified and validated as regards functionality and security aspects, and user friendly interfaces: *human system interface* (HSI) and *human machine interface* (HMI).

A reference model shown in Figure 1, based on the ISA99 series of standards derived from a general model of ANSI/ISA-95.00.01 (*Enterprise-Control System Integration*), represents a manufacturing system as a connection of logical levels:

Level 0 – *Production / manufacturing processes*; it includes the physical processes and basic equipment: process equipment, sensors and actuators, *equipment under control* (EUC) [13] that are components of *safety-related systems* (SRS) for implementing *safety functions* (SFs); these devices are periodically tested (T) and subjected to *preventive maintenance* (PM);

Level 1 – *Sensing and controlling / manipulating*; this level includes: *input / output* (I/O) devices, communication conduits, *programmable logic controllers* (PLCs), components of control and protection systems, and devices of the *human machine interface* (HMI), also on local equipment panels; the devices of this level contribute to *continuous control* (CC), *discrete / sequence control* (DC), and *batch control* (BC);

Level 2 – *Monitoring, control and supervising*; this level allows implementing functions for monitoring and controlling the physical process using a *distributed control system* (DCS) and *supervisory control and data acquisition* (SCADA) software; this level includes: a complex *human-system interface* (HSI), an *alarm system* (AS), and a *decision support system* (DSS) for human operators of the OT; this level includes also some subsystems that diagnose processes and devices alerting operators in case of impending unsafe conditions to undertake actions according to prescribed procedures using HSI and/or HMI;

Level 3 – *Manufacturing operations management and monitoring*; this level includes engineering aspects of the operation using *e.g.* a *manufacturing execution systemMES*).

Level 4 – *Enterprise business planning and logistics*; this level is characterized by business planning and related activities, including logistics, using for instance an *enterprise resource planning* (ERP) *system to manage and effectively coordinate business and enterprise resources required in manufacturing processes.*

On the right side of Figure 1 the time frame categories for typical information processing to be carried out at the distinguished levels of the reference model are presented. The time windows range from milliseconds at levels 0 and 1 (*e.g.* controlling / protecting signals) to weeks and months at level 4 (*e.g.* periodical big data analysis for supporting long-term decision making within the ERP and logistics). In case of very dynamic processes at levels 0, 1 and 2 it causes difficulties in designing reliable control systems and communication conduits for safety and security-related protections due to a short reaction time required.

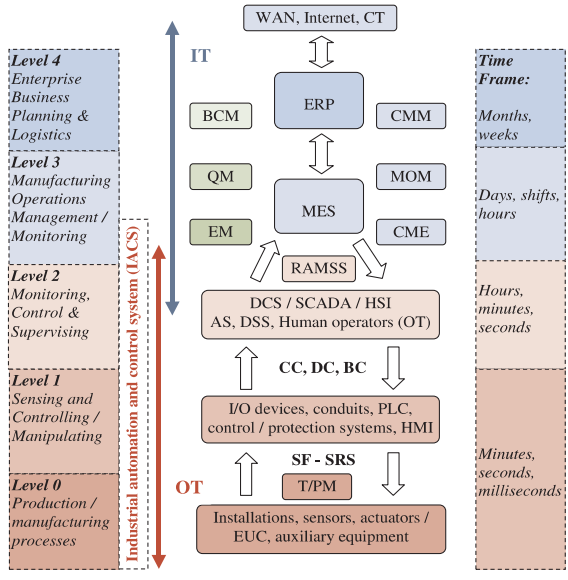

Figure 1. Reference model for operational management and control in a manufacturing system

The operational technology (OT) in this reference model includes levels 0, 1, and 2, whereas the information technology (IT) levels 3 and 4. As is shown in Figure 1 some activities can be distinguished at levels 3 and 4 that can include: BCM (*business continuity management*), QM (*quality management*), EM (*environmental management*), and CMM (*computerized maintenance management*), MOM (*manufacturing operation monitoring*), and CME (*current maintenance execution*), and other supporting activities and management systems depending on the industrial sector and the specific technological processes. Some of these activities may require considerable computer resources and services to be available through network conduits using relevant advanced solutions of the *wide area network* (WAN), *Internet*, and the *cloud technology* (CT). However, such exter-

nal communications can cause cybersecurity problems to IT and OT systems, in particular to safety related control systems (SRCSs) designed according to the *functional safety* (FS) concept [13, 14].

An example of simplified architectures of OT, IT, and CT systems and networks for their architectural and functional convergence is illustrated in Figure 2. The OT is in the process of adopting the same network technologies as defined in the IT world at an increasing rate, so these two worlds begin to merge together. It is also expected that the use of CT in favor of IT and OT will make additional business models and automation structures possible and profitable. Combining these domains is often referred to as the *Industrial Internet of Things* (IIoT) [4]. However, this merging can cause some cybersecurity related problems that require special treatment in the design and operation of IT and OT systems and networks [5].

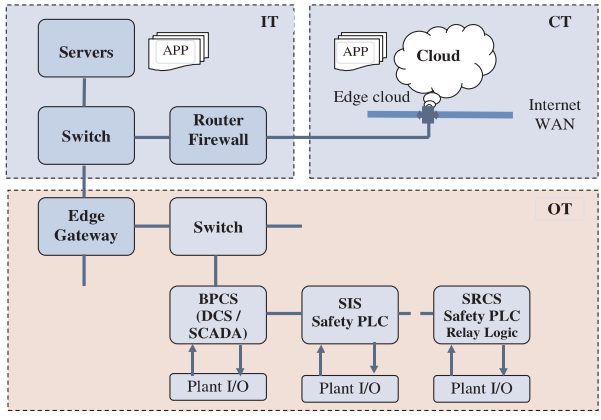

Figure 2. Architectural relations of IIoT domains consisting of operational technology (OT), information technology (IT), and cloud technology (CT) (based on [5])

Below an approach is proposed for integrated functional safety and cybersecurity analysis for reducing relevant risks. In the functional safety approach the safety functions [8] are to be defined and then implemented in SRCSs, *e.g.* the *basic process control system* (BPCS) [13], the *safety instrumented system* (SIS) in process industry [14] or in case of manufacturing machinery using safety PLCs or *relay logic* solutions [19–21] (see OT part in Figure 2). Adoption of the same networks in OT and IT systems may be of interest regarding costs, but the requirements for applications in the field of OT and IT are quite different, which might lead to new types of challenges in bridging these different technological worlds [5].

These issues become more visible taking into account some characteristics of OT and IT systems and networks, such as the expected lifetime of OT in the range of about 10–20 years, but only of 3–5 years for IT [22] (see Figure 3).

An AIC (*availability, integrity*, and *confidentiality*) triad is usually used in OT for prioritizing basic safety and security requirements, as opposed to a different CIA (*confidentiality, integrity*, and *availability*) triad for IT. Figure 3 illustrates

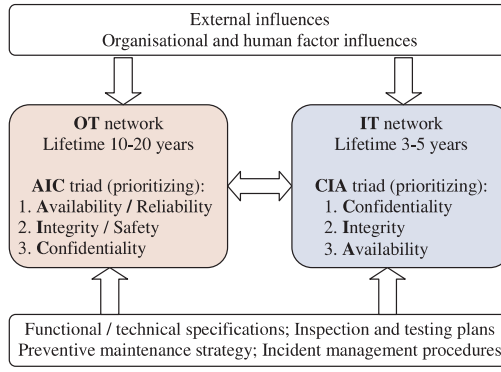

Figure 3. Basic characteristics and design requirement triads for OT and IT networks

that the reliability, safety and security of an SMS are influenced by external factors and human / organizational factors. An operational strategy including: inspection, testing, preventive maintenance plans and incident management procedures should be carefully formulated for high reliability and availability of the IT network, and the OT system, in particular [17].

3. Reference architecture model RAMI 4.0 and security analysis issues

The RAMI 4.0 (*Reference Architectural Model for Industry* 4.0) model describes the key components of a manufacturing system based upon the use of structured layers, distinguishing three axes [23]:

- Architecture axis (*layers* in Figure 4) of six different layers indicating the view depending on information, from assets to business;
- Process axis (*value stream*) for including various stages within the life of an asset and the value creation process based on IEC 62890;
- Hierarchy axis (*hierarchy levels*) for assigning functional models to individual levels based on IEC 62264 and IEC 61512.

Below some general remarks are specified as follows:

- *Layers* – security related aspects apply to all of the different levels; the risk evaluation has to be considered for the object/asset as a whole;
- *Value stream* – the owner of the object must consider security across its entire life-cycle;
- *Hierarchy levels* – all objects/assets are subjected to security considerations (risk analysis) and need to possess or provide relevant security characteristics for fulfilling their tasks applying appropriate protections.

Opinions are expressed that some new opportunities are opened up by the *Industry 4.0* idea, but also bring a host of different challenges. *Security by design*, for instance, becomes an indispensable element in designing within the *Industry 4.0* concept. In some cases, security will be an enabler of new business models [23]. Security related requirements can act in many cases as a skeleton that carries and

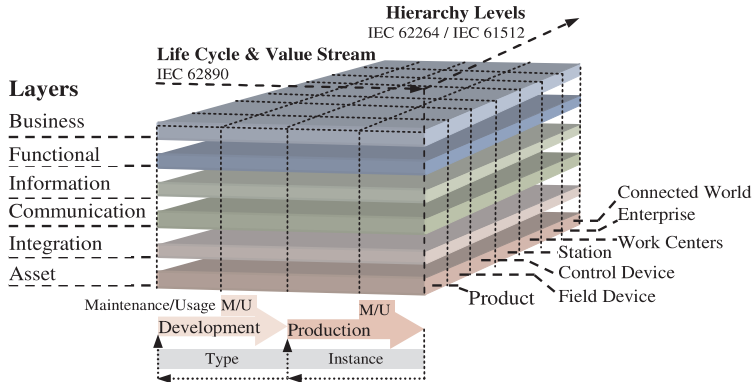

Figure 4. Reference architecture model RAMI 4.0 (Industry 4.0) [23]

holds together all the structural components within the RAMI4.0 model and, as a result, the design of the *Industry 4.0* components and systems.

Security can play a role at the relevant points of intersection between various levels. This means that the requirements will be derived for some intersection points by specific analyses. The solutions have to be found for these requirements based on the relevant 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 [23].

Examples of standards more often considered in developing operational models of the SMS and its IACS are listed in Table 1. In Table 2 selected standards and publications useful for the functional safety and cybersecurity analyses based on relevant risk evaluation methods are collated.

Thus, the problem lays in purposeful selection of standards, reports and relevant publications, depending on the objectives of analyses. These standards and publications have been developed by various organizations to support the design and operation of SMSs with regard to the reliability, safety and security requirements to limit risks to be evaluated with regard to the criteria proposed. It still requires a considerable research effort directed towards the development and successful implementation of advanced technical and effective organizational solutions.

4. Manufacturing control system functional safety evaluation based on risk assessment

Today many institutions and industrial companies face problems due to internal and external influences that make them uncertain about achieving business and technical goals. Some goals may be more or less precisely described, especially those concerning business and operating objectives in a changing and uncertain environment. It concerns also modern industrial companies, interested to follow the principles and challenges of the Industry 4.0 idea mentioned

Table 1. Examples of standards useful for developing operational models of SMS and its IACS

Topic	Related standards	Remarks
Administration Shell	IEC 62794 TR IEC 62832	Reference model for representation of production facilities (digital factory) Industrial process measurement, control and automation – Digital factory framework
Life Cycle & Value Stream	IEC 62890	Life cycle status
Hierarchy Levels	IEC 62264 / IEC 61512 ANSI/ISA 95	Enterprise Control System Levels
Configuration	IEC 61804 EEDL IEC 6523 FDT	Process control and electronic device description language (EDDL) Information technology, Organization identification schemes
Engineering, Data Exchange	IEC 61360/ISO 13584 IEC 61987 IEC 62424 IEC 62714 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 IEC 62714	Open Platform Communications Unified Architecture The Automation Mark-up Language

above. Each industrial plant operates in a specific surrounding area and is dependent on the availability of energy sources, materials and services to be provided by operators of the *technical infrastructure*, in particular, the *critical infrastructure* (CIS), *e.g.*, the electric power grid, the transport infrastructure, telecommunication and computer networks, *etc.* [1, 24].

In the ISO 31000 standard [25] *risk* is generally defined as an effect of uncertainty on the organization's objectives. Such effect can be, *e.g.*, a deviation from something expected that can be positive, negative or neutral. It addresses opportunities in the context of hazards and threats. *Risk management* (RM) is understood as a process of activities coordinated in time in order to direct and control a specific organization with regard to risks to be evaluated. *Risk* can be expressed in terms of *risk sources* with regard to possible hazards and/or threats that can potentially result in serious consequences with a probability measure. Such definition of risk differs from other more specific definitions of risk, *e.g.*, proposed in functional safety standards [13]. In the second edition of the ISO 31000 standard a general risk management methodology is outlined that includes: *principles*, *framework*, and *process*, as shown in Figure 5.

Table 2. Examples of standards and publications useful for functional safety and cybersecurity analyses supported by risk evaluation and management

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

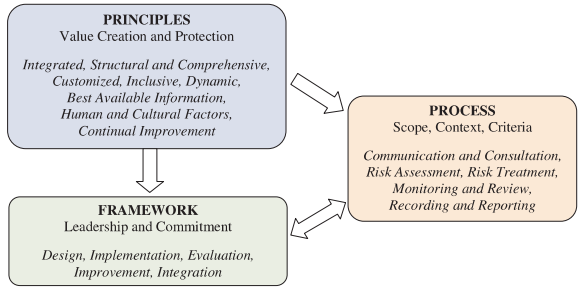

Figure 5. Relations between principles, framework and process in risk management (based on [25])

The *risk management process* (see Figure 6) involves systematic application of polices, processes, procedures, and practices related to activities of communication and consultation in a relevant context, as well as monitoring and recording performances to be useful in evaluating some *key performance indicators* (KPIs) relevant to the risk evaluation and treatment.

Below a risk analysis method is outlined, proposed for the design a *safety-related system* (SRS), *e.g.*, a protection system of implementation in an SMS, for implementing a safety function of high reliability with regard to the individual risk criterion. It is assumed that the individual risk R^I per year $[a^{-1}]$ should be reduced in case of workers, as shown in Figure 7, to the level below $R^I < 10^{-3}a^{-1}$ (preferably close to the threshold line 10^{-5}).

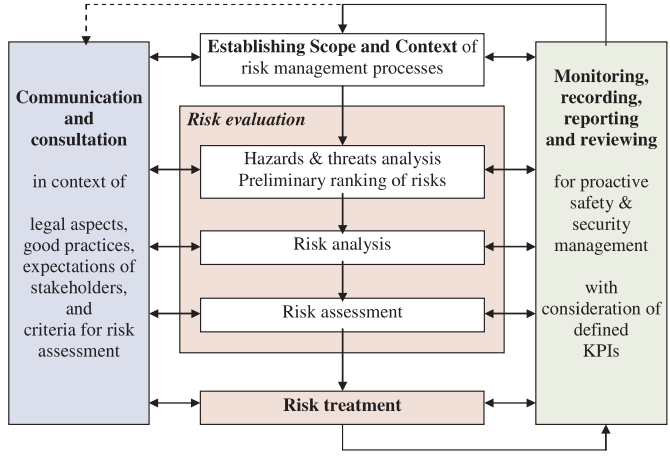

Figure 6. Risk management process (based on [25])

The ALARP (*as low as reasonably practicable*) principle is to be used in practice to evaluate and reduce a risk measure of interest to the level which involves balancing the risk reduction against the time available, the technical problems and the related cost of achieving it, *e.g.*, applying the *cost-benefit analysis* (CBA) [26]. Below this level, the cost of further risk reduction could become too high, unreasonably disproportionate to the benefit obtained due to the decreased risk.

Typical individual risk thresholds for workers and other persons exposed to danger are presented in Figure 7. It is shown that the individual risk threshold values proposed in publications for workers / employees are an order of magnitude higher than for other persons (*e.g.* visitors) [1]. Three individual risk ranges are indicated in this figure: the intolerable range – I, the conditionally tolerable range – II and the tolerable range – III, for workers (w) and other persons (o), respectively.

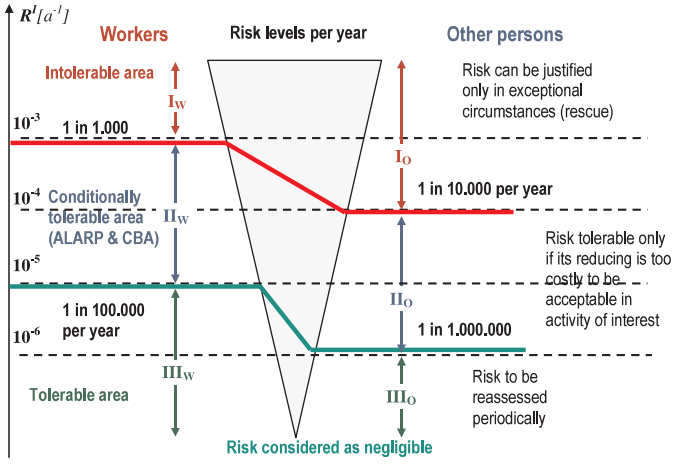

Figure 7. Individual risk criteria in the context of ALARP principle [1]

The individual risk R^I can be roughly defined as a function of the occurrence rate of a hazardous event W per year and probability of a danger failure of the *safety related control system* (SRCS) Q_a in which specific *safety function* is implemented. Approximate values of Q_a are calculated in the middle column of Table 3 for two values of *danger failure rate per hour* PFH (10^{-8} and $10^{-7}\,\mathrm{h}^{-1}$) of the SRCS for the period of one year $T_a \approx 10^4\,rmh$) and three values of W assumed. It can be seen in the third column that the obtained values of R^I correspond to some threshold values in Figure 7, indicating the PFH levels to meet the relevant R^I criterion.

Table 3. Rough evaluation of individual risk as a function of the occurrence rate of a hazardous event and the danger failure probability of a protection system

Occurrence rate W of hazardous event [a^{-1}]	Probability of danger failure of SRCS in one year ($\approx 10^4$ h), $Q_a \cong \mathrm{PFH} \times T_a$ [—]	Rough evaluation of $R^I = W \cdot Q_a$ [a^{-1}]
0.1	$Q_a = 10^{-8} \times 10^4$	10^{-5}
1		10^{-4}
10		10^{-3}
0.1	$Q_a = 10^{-7} \times 10^4$	10^{-4}
1		10^{-3}
10		10^{-2}

The PFH related interval criteria proposed for designing a *safety-related control system* (SRCS) that implement the defined safety functions are specified in functional safety standards for *a high demand or continuous mode of operation* [13]. Figure 8 illustrates, in terms of a risk graph, these interval PFH criteria for determining the required *performance level* (PL_r) according to ISO 13849-1 [20], and *safety integrity level claimed* (SIL CL) given in IEC 62061 [21]. They correspond to the required individual risk reduction after implementation of the safety function in the designed SRCS of the architecture proposed, characterized *e.g.* by the *hardware fault tolerance* (HFT), *i.e.* hardware (HW) without redundancy (HFT = 0) or with single redundancy (HFT = 1), and the requirements concerning its quality including reliability of safety-related software (SW).

The risk related to the identified hazard is defined as a function of [20, 27]:

- *severity of harm* (S) that could result from that hazard; and
- *probability* of occurrence of that harm.

It is assumed in ISO 12100 that this probability is influenced by three factors:

- the exposure (F) of person(s) to the hazard;
- the occurrence rate of a hazardous event; and
- the possibility (P) to avoid or limit the harm.

The performance level required (PL_r) for a safety function considered is determined according to the left side of the risk graph in Figure 8 taking into account the parameters described in Table 4.

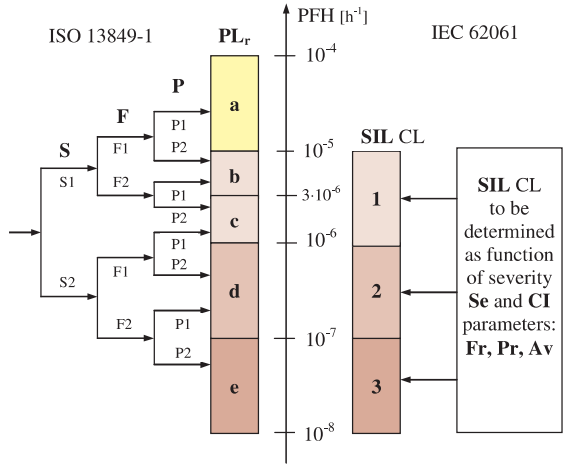

Figure 8. Risk graphs for determining required performance level PL_r or safety integrity level claimed SL CL (based on standards [20, 21])

Table 4. Risk graph parameters for determining required performance level PL_r of a safety function [20]

Severity of injury S		Frequency and/or exposure to hazard, F		Possibility of avoiding hazard or limiting harm, P	
Slight (reversible) injury	S1	Seldom, short exposure time	F1	Possible under specific conditions	P1
Serious (irreversible) injury or death	S2	Frequent to continuous	F2	Scarcely possible	P2

As shown in Figure 8 the risk evaluation methods proposed in ISO 13849-1 and IEC 62061, for determining PL_r and SIL CL, respectively, for the safety function considered for reducing individual risk, differ significantly. The safety integrity level claimed (SIL CL) for a safety function considered is determined in a different way (see the right side of Figure 8). The SIL CL is determined according to Table 4 for the *severity level* (Se) selected and the *class index* (CI) evaluated. The CI is a sum of the integer numbers for the three parameters presented in Table 6. For instance, if Fr = 5, Pr = 4, Av = 3, then CI = 12 and for the selected severity level Se = 3 from Table 4 SIL CL = 2 is determined for the safety function considered. For specific cases the determining of SIL CL is not required if other safety measures (OM) are available.

Then, for the determined PL_r or SIL CL a relevant level has to be verified and validated whether it is achieved by the designed SRCS of the architecture considered for implementing the safety function of interest. The verification of the SRCS hardware configuration is based on PFH evaluation using a relevant probabilistic model to be compared with the interval criteria for PFH_r (Figure 8) for indicating specific PL (*e.g.* PL e) or SIL (*e.g.* SIL 3). The verification procedure is to be carried out for each safety function defined. Then, the PL or SIL validation has to be performed for some additional requirements, *e.g.* concerning the software

Table 5. Determining the safety integrity level claimed (SIL CL) of a safety function for severity level Se of consequence and class index CI [21]

Consequences	Severity (Se)	Class Index (CI = Fr + Pr + Av)				
		3–4	5–7	8–10	11–13	14–15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		(OM)	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			(OM)	SIL 1	SIL 2
Reversible, first aid	1				(OM)	SIL 1

Table 6. Parameters for determining class index CI [21]

Frequency and duration, Fr		Probability index of hazardous event, Pr		Avoidance, Av	
$\leq$ 1 hour	5	Very high	5		
$>$ 1 hour $\leq$ day	5	Likely	4		
$>$ 1 day $\leq$ 2 weeks	4	Possible	3	Impossible	5
$>$ 2 weeks $\leq$ 1 year	3	Rarely	2	Possible	3
$>$ 1 year	3	Negligible	1	Likely	1

quality and reliability, for the SRCS designed for a specific site (industrial installation). Details are given in standards [20, 21] and publications [28, 29].

5. Cybersecurity of industrial automation and control system (IACS) and safety related control system (SRCS) of machinery

IT security remote attacks are increasingly becoming an important threat to the safety of machinery. Safety of machinery might be affected by IT security attacks related to the direct or remote access to, and manipulation of, a SRCS by persons for intentional abuse. General characterization and principle objectives of the machinery safety including the SRCS functional safety versus IT-security are presented in Table 7. Intentional abuse events were not considered in the risk assessment process according to ISO 12100, however, it is without doubt reasonable for machinery manufacturers to consider such threats in the way discussed in the standard ISO 22100 [27].

A threat can initiate an IT security-related incident with the potential to adversely impact the SRCS and machinery operations. Vulnerability is a weakness in the security of IT and/or OT networks that can be exploited or triggered by a threat. Threats may be either passive or active. In case of a *passive threat* agents usually gather passive information by casual communications with employees and contractors. Examples of *active threats* are as follows [27, 30]:

- *Communication*: the intent of a communication attack is to disrupt communications for control systems;

Table 7. Principle objectives of machinery safety and cyber security (based on [27])

Aspect of interest	Safety of machinery / manufacturing system	IT cybersecurity
Objectives in the context of hazards / threats	Prevention of injury / accident, avoidance of harm	To reach high availability, integrity, confidentiality levels
Conditions (risks, methods, measures)	Transparent (not confidential)	Confidential (not shared with machinery designer / user)
Dynamics	Rather a static field (intended use, reasonably foreseeable misuse)	Dynamic field, moving target (intentional manipulation, criminal intent)
Risk reduction (mitigation measures)	Mainly by machine manufacturer at a dedicated time (when providing the machine for the first use)	By various actors (machine manufacturer, system integrator, service provider, machine user) at any time along the overall life cycle

- *Database injection*: injection attacks are used to steal information from a database;
- *Replay*: signals may be captured from control system communications paths and replayed later to provide access to secured systems or to falsify data in a control system;
- *Social engineering*: threat agents attempt to obtain the secure data by tricking an individual into revealing secure information;
- *Spoofing and impersonation*: it is the act of disguising a communication from an unknown source as being from a known, trusted source in networking; a variety of ways are distinguished in which hardware and software can be fooled;
- *Phishing*: is a fraudulent attempt to obtain *sensitive information* such as usernames and password details by disguising oneself as a trustworthy entity in *communication*;
- *Malicious code*: such attacks can take the form of viruses, worms, automated exploits, or Trojan Horses;
- *Denial of service* (DoS): those attacks affect the availability of a network, operating system, or application resources;
- *Escalation of privileges*: due to increased privileges the attacker can take actions that would otherwise be prevented;
- *Physical destruction*: such attacks are aimed at destroying or incapacitating physical components (*i.e.* hardware, software storage devices, conduits sensors, and controllers) that are part of the control system network.

A vulnerability assessment will be carried out to identify vulnerabilities of the SRCS that can be exploited by threats within its intended use and the potential influence to safety.

IT security risks will be mitigated through the combined efforts of component suppliers, the machinery manufacturer, the system integrator, and the

machinery end user. In general, the potential responses to security risks should apply the following hierarchy based on ISO 22100 [27]:

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

The IEC 62443 standard [18] is widely indicated to deal systematically with key security aspects of the IACS, especially the safety-related control system (SRCS). The security level (SL) is defined as a measure of confidence that the SRCS is free from vulnerabilities and it functions in the intended manner. In the standard IEC 63074 the use of term the *security level* (SL) is limited to the SRCS of machinery.

As it is known the assessment of the *security level* (SL) is based on 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).

Instead of compressing the SL down to a single number, it is proposed to apply a SL vector that uses the seven FRs specified above. Such a vector allows definable separations between the SL and different FRs. Thus, a vector is used to describe the security requirements for a *zone, conduit, component, or system* instead of a single number. This vector may contain either a specific SL requirement or a zero value for consecutive foundational requirements. A general format of the *security assurance level* (SAL) vector description is as follows [18]:

$$\text{SL-?}\,([\text{FR,}]\ \textit{domain}) = [\text{IAC UC SI DC RDF TRE RA}] \tag{1}$$

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*) a field indicating the FR that the SL value applies; the *FRs* can be written out in abbreviated form instead of numerical form for better readability;

domain = (*required*) is the applicable domain that the SL applies; in the standards development process, this may be a *procedure*, *system* or *component* – when applying the SL to a system, it may be for instance: *Zone A*, *Machinery B*, *Engineering Workstation*, *etc.*

For instance, according to the standard [18] 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, of a 7 dimension SAL vector SL-C.

For relevant FR_i concerning a particular domain the SL type vectors describe:

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

The SL number provides a qualitative information addressing the protection scope of the domain / zone, *e.g.* for the IACS (see Table 8) or the SRCS as its part.

Table 8. Security levels and protection description of IACS domain [18, 30]

Security level	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 AC case the security levels will be interpreted in the following way "Identify and authenticate IACS / SRCS users by mechanisms against" [30]:

- 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 vulnerability it is suggested to elaborate guidance (instruction handbook) for the end user that includes the following topics [27, 30]:

A. *Restriction of logical/physical access to IT systems with potential influence on safety*, *e.g.* – using internal IT systems with risk reduction measures, such as firewalls, antivirus tools, *etc.*; – using provided 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; and so on;
B. *Detection and reaction on IT-security incidents with potential influence on safety*, *e.g.* – checking regularly the provided means for detecting failed IT

system components or unavailable service according to the specifications of the machine/component manufacturer; – being responsive and reactive for new vulnerabilities resulting from an IT security threat / attack;

C. *In case of remote maintenance and service*, *e.g.* – using the provided means for setting up and ending a remote access session according to the specifications of the machine/component manufacturer; – using means of encryption for initiating a remote maintenance/remote service according to the specifications of the machine/component manufacturer; – watching any remote access session (restriction of duration for remote access; and so on.

Such topics will be included in an *information security management system* (ISMS) to be developed and used in practice according the requirements given in ISO/IEC 27001 [31]. The specific requirements to be formulated will depend on *Target* SAL (SL-T).

The *system requirements* (SRs) and some *requirement enhancements* (REs) are specified in Table 9 for selected *fundamental requirements* (FRs) to be fulfilled at relevant *security levels* (SLs) from 1 to 4.

6. Integrated functional safety and cybersecurity analysis of safety-related control system

The IEC 62443 [18] series of standards consists now in principle of 14 parts, but some of them are still under development or proposed (see Figure 9). The objective is to cover the topics of the IACS security entirely and independently. This series of standards is suggested to be used to add security-related topics to IEC 61508 [13] that is a generic functional safety standard for the design and operation of programmable control systems. Up to now, though, the IEC 61508 and IEC 62443 standards have been only loosely linked [32]. The safety-related programmable systems include the IACSs and SRCSs discussed above in the context of functional safety and cybersecurity of machinery [27, 30].

Four categories of IEC 62443-c addressing different security aspects are distinguished (see Figure 9), namely: *General* ($c = 1$), *Policies and procedures* (2), *System* (3) and *Component* (4). A small number of parts only, such as IEC 62443-3-3, have been issued as an *International Standard* (IS) or a *Technical Specification* (TS) [32]. Due to the novelty of the IEC 62443 standard series some essential concepts will be explained briefly below for better understanding of the adaptation of security aspects into the SRCS design for machinery (*e.g.* within the SMS) in compliance with a holistic approach proposed.

Thus, this standard proposes an approach to the IACS security management activities that are distributed regarding sites and time in the design, verification and validation of the hardware (HW) and software (SW). Figure 10 shows the actors involved and basic activities of the *product supplier* that is responsible, *inter alia*, to carry out successful CFAT, the *system integrator* for successful CSAT, as well as a key role and responsibility of the *service provider* and *asset owner*. All

of them should follow the guidelines specified in relevant parts of IEC 62443 as shown in Figure 10.

It should be emphasized that the security of the SRCS will depend strongly on the quality of the *information security management system* (ISMS) to be established in the SMS. The aim of the ISMS is to continuously control, monitor, maintain and, wherever necessary, improve the IT and OT security. The IEC 62443 standard is based on the general requirements and stipulations of the ISO/IEC 17799 and ISO/IEC 27000 series, especially as regards basic security requirements [31].

It details these general standards by adding specific aspects for safety-related control systems. If the ISMS has been already established, it will remain in use. However, the essential principles from IEC 62443 should be included and respectively integrated. In case of such integration into the existing ISMS, the relevant technical and organizational aspects of the SMS should be carefully considered. It is worth mentioning that in reality they strongly depend on the existing safety culture and the security culture within the organization [12].

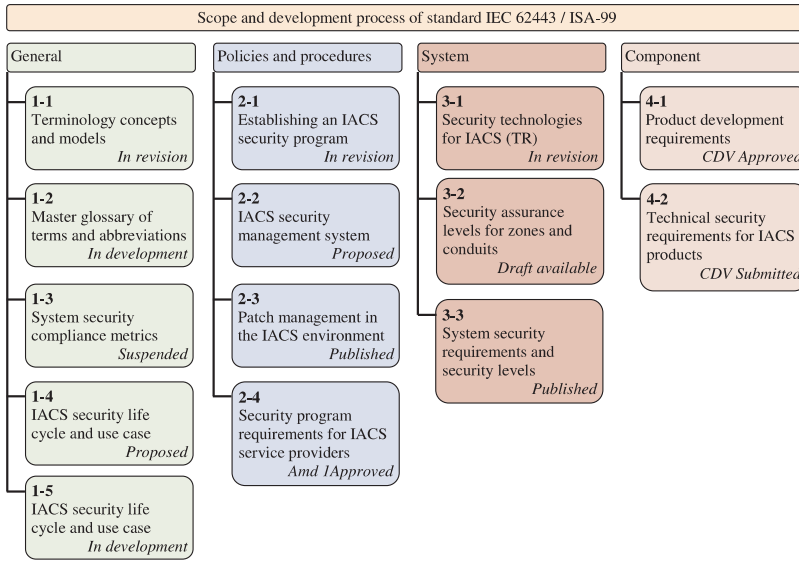

Figure 9. Scope and development process of IEC 62443 standard

Due to specific conditions the adoption of stipulations related to IT and OT security for implementing in industrial practice can cause problems. An important task to be undertaken in the ISMS is risk management, as postulated in ISO/IEC 27001 [31] and ISO/IEC 27005 [33]. It includes the consideration of all functional components of the system including *hardware* (HW) and *software* (SW), *communication conduits* and relevant *human/organizational factors* together with those that are specific to the IT and OT security as described above. Opinions are expressed that the quantitative risk evaluation is very difficult due to the

Table 9. System requirements (SRs) and requirement enhancements (REs) for selected fundamental requirements (FRs) to be fulfilled at relevant security levels (SLs) (based on [18, 22])

System requirements (SRs) and requirement enhancements (REs)	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentification control				
SR 1.1 – Human user identification and authentification	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentification		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentification for untrusted networks			✓	✓
SR 1.1 RE 3 – Multifactor authentification for all networks				✓
SR 1.2 – Software process and device identification and authentification		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentification			✓	✓
…				
SR 1.8 – Public key infrastructure certificates		✓	✓	✓
…				
FR 3 – System integrity				
SR 3.1 – Communication integrity	✓	✓	✓	✓
SR 3.1 RE 1 – Cryptographic integrity protection			✓	✓
SR 3.2 – Malicious code protection	✓	✓	✓	✓
SR 3.2 RE 1 – Malicious code protection on entry and exit points		✓	✓	✓
SR 3.2 RE 2 – Central reporting for malicious code protection			✓	✓
SR 3.3 – Security functionality verification	✓	✓	✓	✓
SR 3.3 RE 1 – Automated mechanisms for security vulnerability verif.			✓	✓
SR 3.3 RE 2 – Safety functionality verification during normal operation				✓
SR 3.4 – Software and information integrity		✓	✓	✓
SR 3.4 RE 1 – Automated notification about integrity violations			✓	✓
…				
FR 5 – Restricted data flow				
SR 5.1 – Network segmentation	✓	✓	✓	✓
SR 5.1 RE 1 – Physical network segmentation		✓	✓	✓
SR 5.1 RE 2 – Independence from non-control system networks			✓	✓
SR 5.1 RE 3 – Logical and physical isolation of critical networks				✓
SR 5.2 – Zone boundary protection	✓	✓	✓	✓
SR 5.2 RE 1 – Deny by default, allow by exception		✓	✓	✓
SR 5.2 RE 2 – Island mode			✓	✓
SR 5.2 RE 3 – Fail close			✓	✓
…				
FR 6 – Timely response to events				
SR 6.1 – Audit log accessibility	✓	✓	✓	✓
SR 6.1 RE 1 – Programmatic access to audit logs			✓	✓
SR 6.2 – Continuous monitoring		✓	✓	✓
FR 7 – Resource availability				
SR 7.1 – Denial of service protection	✓	✓	✓	✓
SR 7.1 RE 1 – Manage communication loads		✓	✓	✓
SR 7.1 RE 2 – Limit DoS effects to other systems or networks			✓	✓
SR 7.2 – Resource management	✓	✓	✓	✓
SR 7.3 – Control system backup	✓	✓	✓	✓
SR 7.3 RE 1 – Backup verification		✓	✓	✓
SR 7.3 RE 2 – Backup automation			✓	✓
SR 7.4 – Control system recovery and reconstruction	✓	✓	✓	✓
…				

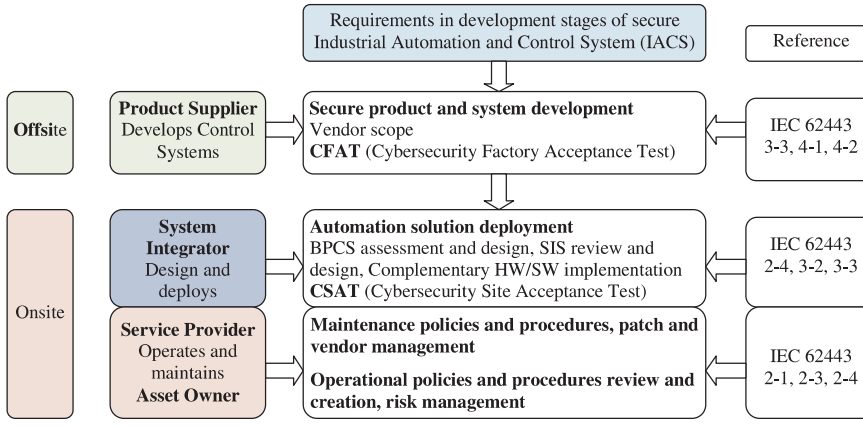

Figure 10. Holistic approach to IACS security management in life cycle using indicated parts of IEC 62443 (based on [22])

complexity of the IT system and many factors involved. The credibility of such evaluation depends on the theoretical framework adapted and the availability of credible expert opinions concerning the specific domain.

Therefore, we propose an approach for integrated functional safety and cybersecurity analysis starting from defining the safety functions for hazards identified and evaluation of risk reduction required regarding the criteria adopted to determine the required *performance level* (PLr) or the *safety integrity level* claimed (SIL) as described above for the SRCS of machinery in the SMS (see the left side of Figure 11). Then, the architectural constrains [21] of the SRCS in which a specific safety function is implemented are taken into account to include the security aspects (see the right side of Figure 11) as described below in the method proposed.

Normally, it is only the issues of *integrity*, *availability* and *data confidentiality* that are considered in IT security (see Figure 3). However, the *fundamental requirements* (FRs in IEC 62443) IAC, UC, SI and TRE can be mapped to integrity, RA to availability and DC and RDF to confidentiality. Instead of defining seven EALs (*Evaluation Assurance Level*s) as in the Common Criteria (IEC 15408) [34, 35] applied to the IT security requirements, four *security levels* (SLs) are defined in IEC 62443. An explanation might be that most functional safety standards, *e.g.* IEC 61508 [13], define four *safety integrity levels* (SILs).

Nevertheless, it would sometimes lead to unnecessary requirements, if the security level (SL) were the same for each of the FRs. For example, confidentiality often plays a minor role for safety systems and encryption of all data might lead to complications in testing or maintenance of these systems. Hence, different levels may be assigned for each of the seven FRs. The SL values for all the seven basic areas are then combined in a vector, *e.g.* the SL-A vector. As was noticed by Brand [32], this would lead theoretically to 16384 possible different SLs. It is only in simple cases of equal levels SL_i for each FR_i (i from 1 to 7)

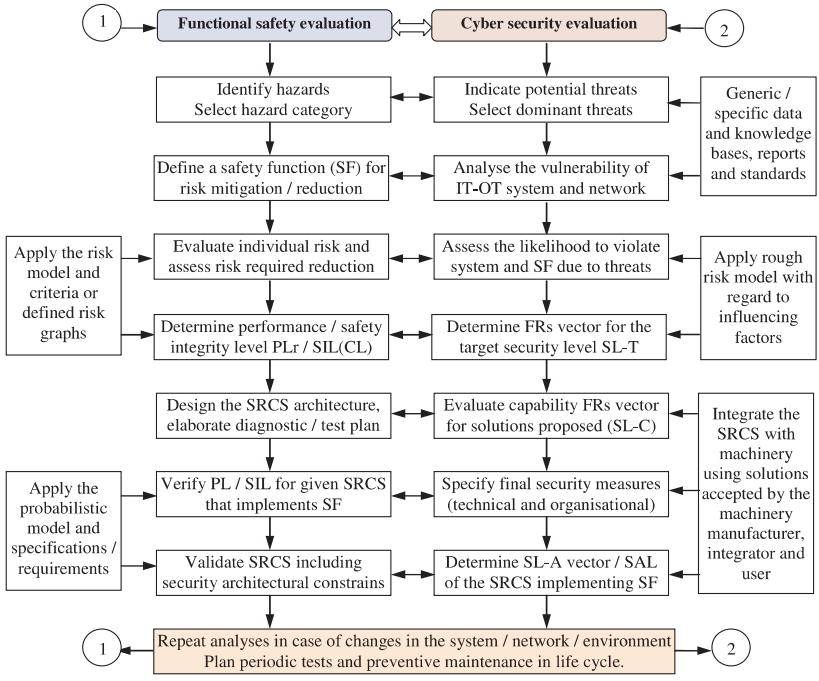

Figure 11. Integrated functional safety and cybersecurity evaluation for life cycle management of the safety related control system

determining SAL of the domain of interest (*e.g.* the SRCS) is straightforward [32], *e.g.*, SAL 1 = [1 1 1 1 1 1 1].

This, in order to come up with a manageable number of SL vectors, Brand proposes [32] as a first simplification and short hand notation set SL 1 as the default for all FRs that are not directly security-related. He proposes to work under the assumption that in the first approach all other FRs may have the same importance. This would lead to four generic SL profiles: [1 1 1 1 1 1 1], [2 2 2 1 1 2 1], [3 3 3 1 1 3 1] and [4 4 4 1 1 4 1]. He admits that additional SL profiles are necessary for specific zones or conduits. For example, a zone containing a key management centre will deserve more demanding confidentiality requirements leading to another profile. However, the challenge would be to cope with 5 to 10 profiles instead of 16384 possible combinations [32].

In our earlier publications [15, 24] it was assumed that the resulting SAL for the domain of interest could be roughly determined based on the dominant FR_i and the evaluated SL_i in a similar way as in the methodology developed in IEC 15408 (common criteria) [34] for the seven distinguished *evaluation assurance levels* (EALs) for defined classes of the *security assurance requirements* (SARs) and the scope of fulfilling the relevant requirements.

We propose below another method for determining SL-A, *i.e.* SAL, achieved, for the domain of interest assuming that the weights w_i of SL_i (security levels: 1, 2, 3 or 4) for consecutive (and relevant) FR_i are known (these weights can dif-

fer in general due to diversified importance of FR_i for the domain of interest). The method should include cases that not all FR_i are determined, because as explained below in the Formula (1), it is permitted in IEC 62443 to determine in a simplest case SL_i for only one i^{th} FR_i (i from 1 to 7). Instead of determining the SAL for the domain of interest based on dominant FR_i we propose alternatively to calculate a security index SI^{Do} for assigning the SAL as described below.

The weight w_i related to the importance I_i of FR_i evaluated by experts for a given specific domain (*e.g.* an integer number on the scale from 1 to 10, and 0 if FR_i is not relevant) is calculated from the formula

$$w_i = \frac{I_i}{\sum_{i=1}^{7} I_i} \tag{2}$$

and the security index (SI^{Do}) for the domain (Do) of interest based on known SL_i (integer number from 1 to 4, or 0 if FR_i is not relevant) for consecutive and relevant (Re) FR_i is evaluated as follows

$$SI^{Do} = \sum_{i \in Re} w_i SL_i \tag{3}$$

Four ranges of the security index SI^{Do} are proposed in Table 10 for assigning SAL from SI^{Do1} to SI^{Do4}. They correspond to the relevant SAL evaluated for the domain of interest in earlier publications based on a set of dominants SL_i. The SIL (or PL) of the SRCS to be verified and validated as regards functional safety and cybersecurity aspects cannot exceed the levels specified in Table 10 for the relevant *hardware fault tolerance* (HFT), even if the results of probabilistic modeling with regard to the PFH criteria defined (see Figure 8) indicate a higher SIL (or PL). Thus, lower security can decrease the validated SIL (or PL) and in some cases and it will be necessary to improve security to achieve SIL CL (or PL_r) determined for the required risk reduction.

Table 10. Architectural constrains imposed on systems of different fault tolerance HFT of SRCS depending on security index SI of the domain.

Security index (domain)	HFT (*hardware fault tolerance*) N		
SI^{Do} / SAL	0	1	2*
$SI^{Do1} \in [1.0, 1.5)$ / SAL 1	— (Pl a)	SIL 1 (Pl b/c)	SIL 2
$SI^{Do2} \in [1.5, 2.5)$ / SAL 2	SIL 1 (Pl b/c)	SIL 2 (Pl d)	SIL 3
$SI^{Do3} \in [2.5, 3.5)$ / SAL 3	SIL 2 (Pl d)	SIL 3 (Pl e)	SIL 3
$SI^{Do4} \in [3.5, 4.0]$ / SAL 4	SIL 3 (Pl e)	SIL 3 (Pl e)	SIL 3 / 4**
HFT of N means that $N+1$ faults could cause a loss of the safety function. * HFT 2 in case of IEC 62061. ** SIL 4 is not considered in IEC 62061 (see IEC 61508)			

7. Case study

The object chosen for the case study is a modern single end impregnation line used to treat yarns made of polyamide, polyester, viscose and other raw

Figure 12. Single end cord production line and the pull roll section of this line [36]

materials so that they are suitable for applications in tires. The pull roll section shown in Figure 12 is a part of the line analyzed in this case study.

The case study is based on a pull roll section with the safety function of door locking and monitoring. The *performance level required* (PL_r) is determined using a risk graph (Figure 8) for the following parameters indicated by a safety engineer: S2, F1, and P2, leading to $PL_r = d$. The safety-related control system (SRCS) in which this function is implemented should be designed to reach at least the performance level $PL_r = d$. The verification of PL requires probabilistic modeling for the SRCS of the architecture shown in Figure 13.

This safety function ensures that the hazardous movement is stopped, and that safety output power has been removed, before the gate is unlocked upon request, it also monitors the lock and the door, and it drops the output power if they unexpectedly change their state. In case that any fault occurs, such as loss of communication, the output power to the safety actuators is put down. While the door is open, its status is monitored to prevent unexpected startup of machinery. As the door is closed and locked, there is a hazardous motion and the power to the motor does not resume until a secondary action (reset button depressed).

In this example, an unlock is requested by pressing the *unlock request button*. The unlock request is sent over a safety conduit to the safety controller. The safety controller (Figure 13) drops out the redundant contactors, and the hazard coasts to a stop. The safety contactors (K1 and K2) are connected to a pair of safety outputs on a safety output module. The I/O module is connected via the Ethernet network to the *safety controller*. After the hazard stops, the safety controller commands to unlock the door, which allows entry to the hazard zone. Once the operator has completed the routine and repetitive maintenance, the operator closes the door and extends the bolt via the handle. If the door is closed and the bolt is extended, a lock button can be used to send a signal to the safety controller to lock the door by de-energizing the lock solenoid.

The safety controller safety code monitors the status of the door by using the pre-certified safety instruction, *Dual Channel Input Stop* with *Test and Lock*. The door lock provides a status bit that indicates that the door is closed, the bolt is extended, and the bolt is locked. The data for evalution of the *dangerous failure probability* per hour PFH of component given by manufacturers are presented in Table 11.

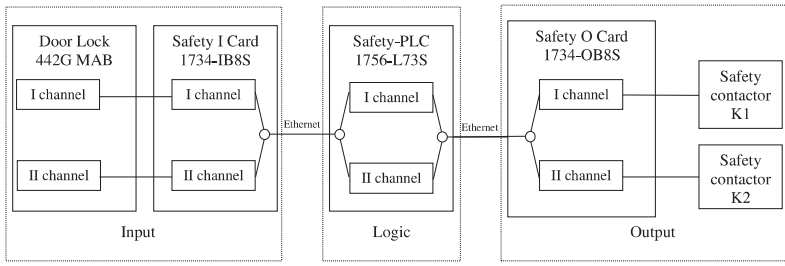

Figure 13. Door locking with monitoring safety function

Table 11. Reliability data for SRCS components for implementing the safety function

Subsystem	PL	PFH [h^{-1}]
A. Input subsystem Door Lock (DL) Safety Input Card (SIC)	e	$5.4 \cdot 10^{-9}$
B. Logic subsystem Safety PLC (SPLC)	e	$1.2 \cdot 10^{-9}$
C. Output subsystem Safety Output Card (SOC) Safety Contactors (SC)	e	$2.5 \cdot 10^{-8}$

The PFH of the safety function (PFH_{SF}) is roughly evaluated for the sum of PFH_X (as for a series configuration of subsystems) in which the safety function is implemented:

$$PFH_{SF} \cong PFH_A + PFH_B + PFH_C = 3.2 \cdot 10^{-8}\ [h^{-1}] \tag{4}$$

The performance level of this safety function is PL = e (see the PFH axis in Figure 8), and the SRCS subsystems are designed for *hardware fault tolerance* HFT = 1 (one failure does not disable the given subsystem). Thus, based on a formal evaluation using probabilistic modelling it can be said that the achieved performance level is higher than the required performance level determined above ($PL_r = d$).

The next stage of this case study is the validation of the verified performance level in relation to specific cyber security threats [18]. The security levels SL_i evaluated for successive fundamental requirements FR_i are presented in Table 12.

The analysis of the examined domain from the point of view of security levels was performed with validation of seven FRs into a vector as described above. The first one is IAC (see Table 12) and its SL was evaluated at Level 3 which corresponds to identifying and authenticating users by mechanisms that protect against intentional unauthorized access by entities using sophisticated means. The SL for UC was validated at Level 2. The SL of SI was also validated at Level 3, which corresponds to the restricted use of the system / assets according to specified privileges to protect against circumvention by entities using sophisticated means. The SL of DC was evaluated at Level 2, and the SL of RDF was assessed at Level 2 (see Table 9 showing the relevant requirements). The SL of TRE is evaluated at

Table 12. Achieved security levels for foundational requirements evaluation score

Foundational requirements		SL_i
FR 1	Identification and authentication control (IAC)	3
FR 2	Use control (UC)	2
FR 3	System integrity (SI)	3
FR 4	Data confidentiality (DC)	2
FR 5	Restricted data flow (RDF)	2
FR 6	Timely response to event (TRE)	3
FR 7	Resource availability (RA)	2

Level 3 (corresponding to prevent the intended circumvention of zone and conduit segmentation systems by entities using sophisticated means). The SL of RA was estimated at Level 2.

Assuming three FRs: DC, RDF and RA as dominant, the resulting SL-A for the domain, treated as the security assurance level (SAL) is SAL 2. Due to HFT = 1 in subsystems only PL = d was achieved (see Table 10) equal to the required level $PL_r = d$. From probabilistic modeling higher PL = e was obtained for PFH_{SF} looking at the interval criteria shown in Figure 8.

If SI^{Do} is calculated assuming that the weights are equal for all $SL_i (w_i = 1/7)$ from the Formula (3) we obtain $SI^{Do} = 2.43$, hence, the analysis result will be as above. Should the weights be different, or should some FR_i be not relevant, then the analysis based on the Formulas (2) and (3) seems to be more justified.

The example presented above confirms the importance of dealing with cybersecurity aspects in the functional safety analysis in a consistent way because any cyber attack concerns the IT and/or OT system that includes the IACS and in particular the SRCS in which the safety functions of the required SIL are implemented to adequately reduce non-tolerable risks.

8. Conclusions

Selected design aspects of OT and IT have been overviewed and discussed here in the context of the IACS functionality and architecture, especially related to the safety and security of the computer technology and networks applied in industrial companies. The design issues of *functional safety* (FS) and *cybersecurity* (CS) are usually of special interest because the IACS and computer networks play a key role in advanced manufacturing systems, especially SMSs operating in accordance with the idea and principles of Industry 4.0.

Unprecedented development of *smart manufacturing systems* (SMSs) increasingly affects technologically advanced industrial companies. At the same time, it can be the reason why *information technology* (IT) and also *operational technology* (OT) will become increasingly opened to be connected to external networks and *cloud technology* (CT) solutions. Understandably, the objective is to reach manufacturing flexibility and functionality in conditions of high product quality

required to be accessible on time, as well as the necessity to reduce resources and energy, and protect the environment.

Advanced *industrial automation and control systems* (IACS) are also under development, based, *e.g.*, on the OPC UA and AutomationML concepts (see Table 1) that offer new manufacturing possibilities including architectural flexibility. However, due to their complexity and dynamic changes of manufacturing goals some challenges arise to be solved including the reliability, safety and security aspects, crucial for *business continuity management* (BCM) to mitigate identified risks.

A method is described for integrated *functional safety* (FS) and *cybersecurity* (CS) analysis, with regard to the methodology and requirements of the generic functional safety standard IEC 61508-x (7 parts) and the cyber security standard IEC 62443-y (14 parts), respectively. A set of *fundamental requirements* (FRs) described in IEC 62443-1 was considered to limit the vulnerability of the IT and OT systems and reduce relevant risks.

The method is based on using risk graphs to determine and verify the *performance level* (PL) or the *safety integrity level* (SIL) of defined safety functions. The next step is to validate these levels depending on the security level (SL) of the FRs in the context of a specific domain. The method is general in the sense that it is based on these graphs defined for cases of individual risk and/or societal/group risk.

The dependability of safety-related control systems performing safety and security-related functions can be influenced both by technical factors, including requirements concerning hardware (HW) and software (SW), and also organizational factors [1, 12, 37, 38]. These aspects require further research, especially in the context of the design and operation of high complexity manufacturing systems. The role of human factors and potential errors of operators supervising the technological processes using advanced interfaces (HMI and HSI) is another important topic for research to treat the safety and security incidents consistently. It is known that human and organizational factors, if not shaped adequately, can influence adversely the likelihood of abnormal and hazardous events, and risks of high losses. Therefore, the technical and organizational factors should be carefully considered in *business continuity management* (BCM) in the life cycle of a specific manufacturing system.

References

[1] Kosmowski K T and 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*, Interreg Baltic Sea Region, HAZARD Report

[2] Lu Y, Morris K C and 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] Kivelä T, Golder M and Furmans K 2018 *Towards an approach for assuring machinery safety in the IIoT-age*, *Logistics Journal: Proceedings*
[5] Felser M, Rentschler M and Kleinberg O 2019 *Proceedings of the IEEE*
[6] SESAMO 2014 *Integrated Design and Evaluation Methodology. Security and Safety modelling*, Artemis JU Grant Agr. no. 2295354
[7] MERgE 2016 Safety & Security, *Recommendations for Security and Safety Co-engineering*, Multi-Concerns Interactions System Engineering ITEA2 Project #1 101 1
[8] HSE 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
[9] HSE 2016 *Cyber Security for Industrial Automation and Control Systems (IACS)*, HSE report for Chemical Explosives and Microbiological Hazard Division (CEMHD) and Energy Division, Electrical Control and Instrumentation (EC&I) Specialist Inspectors
[10] ENISA 2016 *Communication network dependencies for ICS/SCADA Systems*, European Union Agency for Network and Information Security
[11] ISO 22400 2014 *Automation systems and integration – Key performance indicators (KPIs) for manufacturing operations management. Parts 1 and 2*, International Organisation for Standardisation
[12] Kosmowski K T and Śliwiński M 2016 *Journal of Polish Safety and Reliability Association* **7** (1) 133
[13] IEC 61508 2005–2016 *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Parts 1–7*, International Electrotechnical Commission, Geneva
[14] IEC 61511 2015 *Functional safety: Safety Instrumented Systems for the Process Industry Sector. Parts 1–3*, International Electrotechnical Commission, Geneva
[15] Kosmowski K T, Śliwiński M and Barnert T 2006 *Proc. European Safety & Reliability Conference – ESREL, Estoril*, Taylor & Francis Group, London
[16] ISO 22301 2012 *Societal security – Business continuity management – Requirements*, The International Organisation for Standardisation
[17] Gołębiewski D and Kosmowski K T 2017 *Journal of Polish Safety and Reliability Association* **8** (1) 23
[18] IEC 62443-x 2011–2018 *Security for industrial automation and control systems. Parts 1–13*, International Electrotechnical Commission (undergoing development)
[19] Malm T, Ahonen T and Välisalo T 2018 *Risk assessment of machinery system with respect to safety and cyber-security*, Research Report-VTT-R-01428-18
[20] ISO 13849-1 2015 *Safety of machinery – Safety-related parts of control systems. Part 1: General principles for design*
[21] IEC 62061 2005 *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*
[22] Siemens *Industrial security* [online] `siemens.com/industrial-security` [accessed: 10-Jul-2019]
[23] DIN SPEC 91345 *Reference architecture model Industrie 4.0 (RAMI4.0)*
[24] Śliwinski M, Piesik E and Piesik J 2018 *Integrated functional safety and cyber security analysis*, *IFAC Papers OnLine* **51** 1263
[25] ISO 31000 2018 *Risk management – Principles and guidelines*, International Organization for Standardization, Geneva
[26] Kosmowski K T 2013 *Functional safety and reliability analysis methodology for hazardous industrial plants*, Gdańsk University of Technology Publishers
[27] ISO 22100-4 2018 *Safety of machinery – Relationship with ISO 12100. Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects*
[28] Kosmowski K T *et al.* 2015 *Basics of functional safety*, Gdańsk University of Technology Publishers (in Polish)

[29] Kosmowski K T 2017 *Safety Integrity Verification Issues of the Control Systems for Industrial Power Plants*, *Advanced Solutions in Diagnostics and Fault Tolerant Control*, Springer International Publishing AG 420
[30] IEC 63074 2017 *Security aspects related to functional safety of safety-related control systems*
[31] ISO/IEC 27001 2013 *Information technology – Security techniques – Information security management systems – Requirements*
[32] Braband J 2016 *8th European Congress onEmbedded Real Time Software and Systems (ERTS 2016), Toulouse*
[33] ISO/IEC 27005 2018 *Information technology – Security techniques – Information security risk management*
[34] ISO/IEC 15408 2009 *Information technology, Security techniques – Evaluation criteria for IT security. Part 1–3*
[35] Białas A 2008 *Semiformal Common Criteria compliant IT security development framework*, *Studia Informatica*, Silesian University of Technology Press, Gliwice
[36] Benninger Z 2019 [online] `http:/www.benningergroup.com/tire-cord/overview#products` [accessed: 17-Jul-2019]
[37] Gabriel A, Shi J and Ozansoy C 2017 *A proposed Alignment of the National Institute of Standards and Technology framework with the Funnel Risk Graph Method*, *IEEE Access* **5**
[38] Nardello M, Møller C and Gøtze J 2017 *Organizational Learning Supported by Reference Architecture Models: Industry 4.0 Laboratory Study*, *Complex Systems Informatics and Modeling Quarterly (CSIMQ)*, **12**