Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 16 (2021) pp. 073-084
© MIR Labs, www.mirlabs.net/jias/index.html

Interactions between cyber security and safety in the ICS context

Omar El Idrissi[1], Abdellatif Mezrioui[2] and Abdelhamid Belmekki[3]

[1, 2, 3] STRS Lab, RAISS Team, INPT, Rabat, Morocco
[1] elidrissi.omar@inpt.ac.ma, [2] mezrioui@inpt.ac.ma, [3] belmekki@inpt.ac.ma

***Abstract*: In this paper, we discuss the inadequacy of the application of classical IT cyber security approaches to the industrial control systems (ICSs) domain and we show the interaction that exists between cyber security and safety in the ICSs context. Indeed, we show for instance that the application of IT risk analysis methods is not adapted to the ICSs context and that some characteristics of ICSs must be taken into account. Furthermore, we show that when implementing IT security measures some aspects of safety (especially the real-time aspect which is very important in ICSs) are impacted as well as the Safety Integrity Level (SIL). We therefore propose a new way to calculate the SIL while taking into account cyber security and we also propose a global process of risks analysis and management which integrates both the cyber security and the safety.**

Keywords: Industrial Control System, Critical infrastructure, SCADA, Cyber security, Safety, Risk management.

I. Introduction

Industrial Control Systems (ICS) are commonly used to monitor and control industrial infrastructures providing vital services like electricity, water, transportation, manufacturing, etc. Initially, ICS were designed to operate in isolated and autonomous mode. They were designed without any security requirements in mind, while safety and physical security have been considered as the most crucial concern in ICS. As the industry opens up to the outside world, with increased connectivity of external systems, industrial cyber security is becoming one of the most complex and delicate topics in industrial environments. Indeed, the convergence of IT and Operational Technology (OT) in recent years makes ICS a prime target for hackers and cybercriminals [1] [2]. The number of cyber incidents targeting ICS systems has increased dramatically in recent years, and the same goes for the number of ICS vulnerabilities which in turn has increased considerably [3] [4]. While, the cyber security threats can lead to the same dangerous and disastrous phenomenon as a safety incident [5] [6], we note on the other hand, some limitations of management methods, untrained and unskilled developers in business management and organizational areas, various classifications and non-unique taxonomies of vulnerabilities [7]. 77% of industrial organizations are concerned about cyber security incidents, but half have no appropriate response program [8]. Contributing to this challenge is that the methodologies and approaches available today to handle cyber risk in operating industrial environments have been developed for traditional IT domains, and when applied to engineering environments, they are unfit for this purpose because factors such as exposure, threats, and consequences are different [9] [10]. In this regard, implementing IT security solutions and tools (proxies, Firewalls, IDS ...) has a negative impact on the performance of the ICS, including real-time requirements and system availability which can lead to communication latency between the different industrial instruments [11] [12], therefore and to maintain system availability, IT security solutions are rarely applied to protect ICS from cyber risks [13]. To face this problem, a significant number of research works have been published in the field of cyber security risk management related to the ICS with two different perspectives. Some researchers and industrials [5] [14] try to develop new methodologies exclusive to industrial environments, for example IEC-62443 which is a series of standards including technical reports to secure Industrial Automation and Control Systems (IACS), and it provides a systematic and pragmatic approach to industrial systems cyber security. Every stage and aspect of industrial cyber security is covered, from risk assessment to operations, while others prefer not to reinvent the wheel and work to adapt available IT approaches to be applicable in the ICS domains. In Park and Lee (2014) [15], the authors discuss the need to update and adapt international security standards such as NIST SP 800-53 and ISO 27001 in order to consider and address the specifics of the ICS. For that, in this paper, we will analyze and study the second perspective and verify whether we can adapt IT approaches and find a way to make them useful to the industrial context. The challenge to do this is more difficult than we can imagine, due to the complex interferences and mutual interactions between the areas of cyber security and safety [16]. Indeed, these interferences can take many forms, which may affect the efficiency and effectiveness of the preventive barriers associated with both areas. Numerous cyber security attacks targeting security systems to disrupt them and affect their performance to achieve their goals to ensure the safety of the industrial facility [17] [18]. So regardless of cyber security controls, safety functions must be designed to respond to these kinds of risks in the event of failure or absence of cyber security controls including zero day attack to prevent catastrophic situations. In this regard, the analysis of the safety integrity level (SIL) including cyber security threats is essential to gain a global view of the industrial platform protection [19]. We therefore propose a new way to calculate the SIL while taking into account cyber security and we also propose a global process of risks analysis and management which integrates both the cyber security and the safety.

This paper is structured as follows: We clarify in the next section, the meanings of the terms safety and security used in the context of this paper. In section 3, we provide an overview of the ICS architecture and we introduce the concepts of safety requirements for ICS. In section 4, we present some constraints related to ICSs cyber security management. In section 5, we highlight the global idea behind this study and we undertake an ICS cyber security management analysis. In section 6, we will make a depth analysis of cyber Security and Safety interferences. In Section 7, we will study the impact of cyber security on safety aspect, and we will propose a new formula and a new process to redefine the new safety indicator level. In section 8, we will suggest a new process for managing ICS cyber security using IT mechanisms. Finally, the paper overview and perspectives are summarized in section 9.

II. Terminology

The definitions of the terms safety and security vary widely in different contexts and technical communities [20]. According to [21] [22], security is defined as the state of being away from hazards caused by deliberate intention of human to cause harm, the source of hazard is posed by human deliberately. While safety is defined as the state of being away from hazards caused by natural forces or human errors randomly, the source of hazard is formed by natural forces and/or human errors. In our context, the definitions of "safety" and "cyber security" will be considered as stated below.

Safety: the goal of safety is to protect against accidental nature hazards such as natural disasters, environmental failure, mechanical failure and unintended actions of an authorized user [23].

Cyber security: the goal of cyber security is to protect or defend the use of cyberspace from cyber-attacks [24].

III. Background of ICSs

A. *Industrial control systems operations and types*

ICSs are designed to support industrial processes. It aims to monitor and to control in real time a large number of processes and operations of complex infrastructures. ICS are used in different domain such as gas and electricity distribution (conventional and nuclear), water treatment, oil refining and rail transportation etc. They consist of numerous control loops, human-machine interfaces, diagnostic and maintenance tools that communicate with each other across an industrial network. The figure below (Figure.1) illustrates the operation of the ICSs.

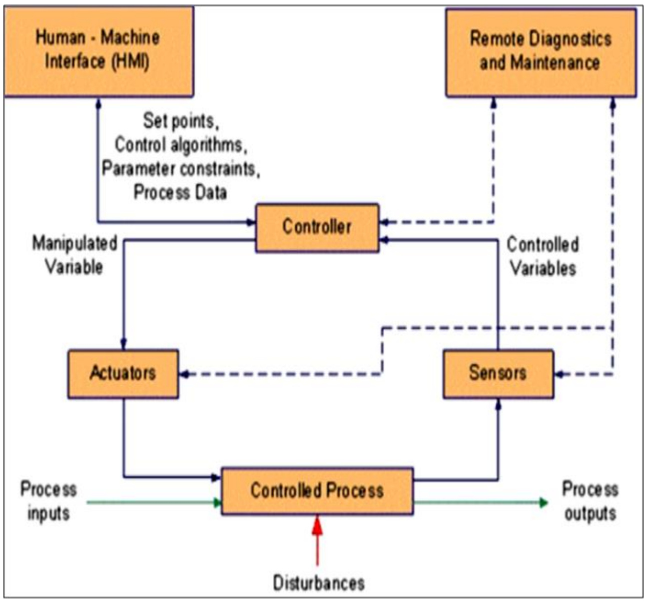
Human - Machine Interface (HMI)
Remote Diagnostics and Maintenance
Set points, Control algorithms, Parameter constraints, Process Data
Controller
Manipulated Variable
Controlled Variables
Actuators
Sensors
Process inputs
Controlled Process
Process outputs
Disturbances

Figure 1. ICS Operation [25]

There are different types of ICS:

SCADA Systems (Supervisory Control and Data Acquisition): SCADA systems are used to control geographically dispersed assets. These systems are used in distribution systems such as water and wastewater systems, oil and gas pipelines, electricity grid, rail and other transportation systems.

DCS system (Distributed Control Systems): A DCS is a control system of industrial processes located geographically in the same area, such as oil refineries, water and wastewater treatment, power plants, power plants manufacture of chemicals, etc.

PLC (Programmable Logic Controller): PLCs are used as a primary controller in smaller control system configurations to provide operational control of processes.

SIS (Safety Instrumented Systems): SISs are designed to bring the process to a safe state when process conditions that threaten safety are detected. SIS is used to perform safety functions. For example it can quickly shutdown a process and isolate it completely to prevent dangerous situations from occurring or getting worse. It may order a shutdown of the entire factory, unit or equipment if necessary.

B. *Typical architecture of ICS*

The Purdue Enterprise Reference Architecture (PERA) provides a reference model for computer integrated manufacturing [26] that divides the enterprise architecture into different layers based on organizational hierarchy. The basic ICS architecture is classified into six distinct levels that are presented bellow and also by Figure.2 [5]:

- **Level 0** - field instruments: the lowest level of the control hierarchy which includes sensors, pumps, actuators, etc. which are directly connected to the plant. This level generates the data that will be used by the other levels to supervise and control the process [27].

- **Level 1** - control level using Programmable Logic Controller (PLC): PLC is an industrial digital computer that controls manufacturing processes. It is linked to field instruments and SCADA host software via an industrial communication network.
- **Level 2** - SCADA: monitors, supervises, maintains and engineers the processes and instruments.
- **Level 3** - MES: this level is responsible for process planning, handling, maintenance, inventory, etc.
- **Level 4** - ERP: the highest level of industrial automation that manages the entire control and automation system. This level deals with business activities including production planning, customer and market analysis, etc.
- **Level 5 –** this level of the architecture describes the corporate network with internet access; it's managed within the layer where the centralized IT systems and functions are located, along with business-to-business (B2B) and business-to-customer (B2C) services.

Levels 4 and 5 constitute the corporate network in (Fig.2), the services, systems and applications in these levels are normally managed and operated by the IT teams [28]. Industrial communication networks are most prominent in ICS which represents the link that relays data from one level to the other in order to provide continuous flow of information.

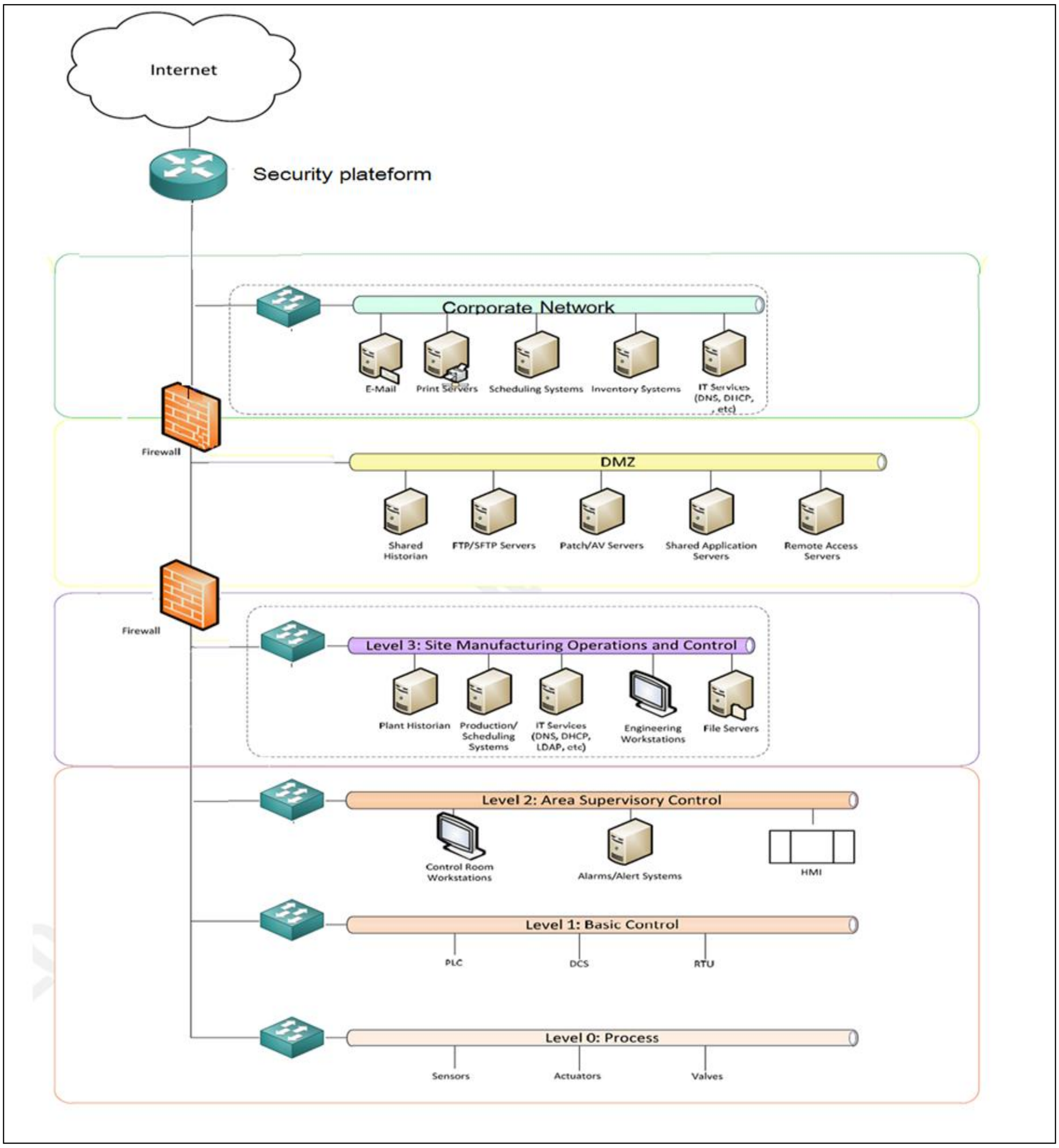

Figure2. Typical layered architecture of ICS

C. *Safety requirements for ICSs*

Physical safety is the most crucial and the main requirement in industrial control [1]. It is a prime concern of industrial activities that directly affect the engineering and operational decisions of an ICS. Indeed, ICS systems are designed according to IEC 61508 and IEC 61511 to ensure certain prerequisites and requirements related to the safety of the industrial infrastructure. IEC 61508 is a generic and complete standard that covers the complete safety lifecycle including the analysis, realization and operation phases, these phases are common to several industries, from which different industries derived their own standards (e.g., IEC 61513 for the nuclear industry, IEC 61511 for industrial processes, and ISO 26262 for the automotive industry) [29]. The safety requirements of IEC 61511 (see Table 1) are composed of 15 domains and the total number of controls is 215 pieces, divided into five safety parts that consist of development, allocation, design, installation, commissioning, validation, operation, modification, and decommissioning for an ICS [30].

IEC 61511 (Requirements)
Management of functional safety
Safety life-cycle requirements
Verification
Process hazard and risk analysis
Allocation of safety functions to protection layers
SIS safety requirements specification
SIS design and engineering
Requirements for application software including selectio criteria for utility software
Factory acceptance testing
SIS installation and commissioning
SIS safety validation
SIS operation and maintenance
SIS modification
SIS decommissioning
Information and documentation requirements

Table 1. ICS safety requirements according to IEC 61511

Safety requirements are met partly by the safety-related technology other than safety instrumented systems (SIS), such as relief valves, alarms, and other specific-safety devices [31]. Therefore, any safety strategy must consider not only all the elements within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems [32]. The table 1 shows the safety requirements according to IEC 61511.

IV. ICSs cyber security management constraints and difficulties

In addition to its primary purpose of controlling and supervising the industrial process, ICS also aims to protect industrial infrastructure, users and environment from physical accidents in general. However, in recent years, ICS general safety concern may arise in particular from malicious cyber threat factors that attempt to disrupt an industrial process such as interfering with its specific operations (e.g. to create a power outage) or to negatively impact the environment and/or personal safety (e.g. exploding a fuel tank or destabilizing chemical process to free noxious gases) [33]. Unfortunately, facing this type of threat faces many limitations and obstacles, we provide some examples below.

A. *Insecure by design*

Initially, the ICS were designed to operate, with specific protocols and hardware, in isolated and autonomous mode. They were designed without any cyber security requirements in mind. Most components of ICSs (PLCs, protocol converters or data acquisition servers) lack even basic authentication and accept generally any properly formatted command [34]. On the other hand, the communication protocols used by ICS environments to control field devices are proprietary protocols that are designed to ensure efficiency, reliability and accuracy in real-time operation. This means that any other functions of the protocol have been omitted [35].

B. *Resources constraints*

ICS operating systems (OS) and applications may not have the computing resources to tolerate typical security practices including the upgrade of these systems with current security capabilities and desired features such as encryption capabilities, error logging and password protection [36].

C. *Interaction with physical environment*

ICS have been designed to meet high performance and reliability requirements; it has different priorities and involves risks that are much broader in scope and impact. Cyber security issues in ICS systems can disrupt system functionality and interfere with functional requirements that have a potential physical impact including significant risks to the safety of human lives and severe damage to the environment [18] [37].

D. *Management skills*

In addition to all constraints we have mentioned above, there is a very critical point that further complicates the situation, as the ICS management team generally consists of automation professionals and their knowledge of the norms and standards related to cyber security is often very limited. Unfortunately and despite the criticality of industrial cyber security, in the European Union, limited resources are dedicated specifically to this area and the most efforts in cyber security risk management are limited to the IT field [38].

V. Inadequacy of IT approaches for ICS cyber security

For a longtime, only accidental component failures and software errors were traditionally addressed in industrial environment. Today, cyber-attacks and security breaches can also compromise the safety of the system [22] and can lead to various risks affecting the critical infrastructure business continuity, including degradation of production and performance, unavailability of critical services, and violation of the regulation [39]. Therefore, great attention should be paid to cyber security issues and their potential impacts on critical infrastructure systems, but as we have seen in the previous section, securing ICS is a huge challenge due especially to the fact that most IT security approaches are inadequate and not suitable for ICS that have specific requirements. In this regard, we will identify the points of incompatibility and inadequacy that exist between traditional cyber security norms and industrial environments by studying and analyzing de gap between ICS cyber security objectives and ISO 27001 controls and requirements [18].

A. Cyber Security objectives for ICSs

We chose to work with the objectives instead of the requirements because working directly with the requirements of all ICS applications is very complicated due to the differences between processes and networks deployed across different industries. On the other hand, common cyber security objectives are sufficient for every ICS, regardless of the specific application. For that and to identify the cyber security objectives for ICSs, we will use the System Protection Profile for ICSs (SPP-ICS) document [33] produced by the working group PCSRF that initiated by NIST. The goal of PCSRF group is to assess vulnerabilities and to design and document a set of security specifications using the Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408 [32]. The table below (Table 2) shows the cyber security objectives for industrial control systems according to SPP-ICS document.

Cyber Security Objectives for ICS (SPP-ICS)	
O.1	Physical
O.2	Risk
O.3	Non_interference
O.4	Interconnectivity
O.5	Data_Backup
O.6	Data_authentication
O.7	Continuity
O.8	Management
O.9	Migration
O.10	Compliance
O.11	3Rdparty
O.12	Remote
O.13	Acess_control
O.14	Secure_comms
O.15	Data_integrity
O.16	Confidentiality
O.17	Availability
O.18	System_integrity
O.19	System_diagnostics
O.20	Monitoring
O.21	Audit
O.22	IDS

Table 2. Cyber Security Objectives for ICS (SPP-ICS) [33]

B. Cyber security controls and requirements for information technology

The main cyber security concern according to the Standard ISO 27001 is to protect information from harmful threats. For this purpose, it offers a set of measures to protect assets and reduce risk to an acceptable level. The table below (Table 3) shows the controls and requirements according to ISO 27001.

ISO 27001 (Requirements + Controls)	
R.4	Context of the organization
R.5	Leadership
R.6	Planning
R.7	Support
R.8	Operation
R.9	Performance evaluation
R.10	Improvement
A.5	Information security policies
A.6	Organization of information security
A.7	Human resources security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communications security
A.14	System acquisition, development and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance

Table 3. ISO 27001 controls and requirements

C. Mapping Cyber Security Objectives for ICS (SPP-ICS) with ISO 27001 controls

The purpose of this section is to extract the points of incompatibility and inadequacy that exists using traditional standards in industrial environments. For that we compare and analyze the cyber security objectives for ICS in accordance to SPP-ICS with ISO 27001 controls and requirements. Our comparison method is as follows: For each ICS cyber security objective identified in the System Protection Profile for Industrial Control Systems (SPP-ICS) document, we examine a similar security topic (requirements and controls) in ISO / IEC 27001.

Cyber Security Objectives for ICS	**ISO/IEC 27001 (Requirements & Controls)**

O.1	Physical	A.11
O.2	Risk	R.6, R.8, A.12
O.3	Non_interference	**None**
O.4	Interconnectivity	A.9
O.5	Data_Backup	A.12
O.6	Data_authentication	A.14, A.9, A.10, A.12
O.7	Continuity	A.17
O.8	Management	R.4, R.5, A.5, A.6
O.9	Migration	R.10, A.12,
O.10	Compliance	A.18
O.11	3Rdparty	A.7, A.9, A.14
O.12	Remote	A.6,
O.13	Acess_control	A.9
O.14	Secure_comms	R.9, A.10, A.13
O.15	Data_integrity	A.9, A.10, A.12
O.16	Confidentiality	A.9 A.10
O.17	Availability	A.17
O.18	System_integrity	R.9, A.9, A.11, A.12
O.19	System_diagnostics	R.9
O.20	Monitoring	R.9, A.12
O.21	Audit	A.12, A.16, A.18
O.22	Ids	A.12, A.14, A.18

Table 4. Mapping Cyber Security Objectives for ICS (SPP-ICS) with ISO 27001 controls

In Table 4, we note that the Cyber Security Objective: O.3 “Non_interference” is not covered by ISO 27001.

D. ICS risk management requirements

Ensure that security functions are implemented in a noninterfering manner with safety functions is an important and necessary goal in industrial fields [33]. Through our mapping analysis, we conclude that there is no ISO 27001 requirement or control to meet this end. Therefore, based solely on the CIA triad (confidentiality, integrity, and availability) it is not sufficient to properly manage ICS cyber security, but a new component must be added in order to deal with IT and functional safety interferences [15]. For that we associate the objective “O.3 NON_INTERFERENCE ", with a new principle that called: “Cyber-Safety”. This new principle “Cyber-Safety” consists of verifying the effect of each security control or measure on safety requirements before it is implemented, based on the analysis of the interferences between cyber security and operational safety.

VI. Analyzing of Cyber Security and Safety interferences/ interactions in ICS context

A. Introduction

ICS systems are exposed to potential cyber security risks of different natures and patterns that could have a serious impact on the health, safety of human lives and serious damage to the environment [40] [25] and vice versa, security threat can lead to the same dangerous phenomenon as a safety incident [5]. In addition, the requirements and objectives related to security and safety domains converge and can interact with each other. Unfortunately, this aspect has not found the necessary importance by researchers, and therefore it is still to the time ambiguous. For that, the purpose of this section is to study the impact of cyber security on safety part by evaluating how cyber security risks can affect the safety integrity level. In addition, we will propose a new formula and new process to redefine the safety integrity levels taking into account cyber security risks.

B. Cyber security impact on safety part

Our methodology to analyze the impact safety requirements due to the implementation of IT approaches in the context of ICS consist to segment the system into several levels with the components that constitute each one of them. Next, for each level, we assess the impact on the ICS performance of implementing certain IT cyber security measures such as cryptography based on the performance of equipment of the same level. Below is a list of the main components that make up industrial control systems [35].

Control server: the control server is the software responsible for configuring the controllers (PLC); it hosts all the control logic applications and the device network configuration. In addition, it hosts real-time monitoring services. The control server is connected directly to the control devices via a control network.

SCADA Server: Known in academic literature as MTU (Master Terminal Unit); which is the central device of the SCADA architecture to host all supervision, control and data object functions for process assets.

Remote Terminal Unit (RTU): are field devices typically used in telemetry implementations of SCADA systems. By telemetry we mean a highly automated communication process where measurement and data acquisition is done remotely in inaccessible areas where wired connections are not available. RTUs interface objects in industrial facilities with a SCADA or DCS system by transmitting acquired telemetry data and executing control logic for basic control for the connected objects.

Programmable Logic Controller (PLC): NIST [25] defines the first version of PLCs that appeared in mid-60’s, as "a small industrial computer originally used to perform the logic functions executed by electrical hardware”. Currently, PLCs are able to control complex processes in DCS and SCADA systems and are able to solve complex logic to control the process functions and communications that are generated by the control server. In some situations, PLCs are connected to lower level devices such as sensors and actuators.

Intelligent Electronic Devices (IED): are industrial devices (sensors, actuators) smart enough to collect data and transmit it to PLCs, RTUs and monitoring services. The IEDs are interfacing with the field part of the process where analog communication capabilities are required for IEDs in both, data acquisition and local control.

Human Machine Interface (HMI): is software hosted in computers or in specific hardware used to monitor the process, change control parameters and manually override control operations. The HMIs can be SCADA server clients or directly connected to the control network.

Data Historian: is a centralized database connected to one or more MTUs and which stores all process logs and events. Part of the information hosted by Historian is analyzed by certain Big Data services and communicated at the company level.

Input/output (I/O) Server: The IO server is a software component responsible for collecting, buffering and providing access to process information from control devices to be transmitted to Control and SCADA servers.

Communication Protocols: The communication protocols used in industry are often simple and proprietary protocols (modbus, Fieldbus..) designed by different manufacturers of industrial equipment without any security in mind. These protocols do not support the majority of security mechanisms recommended by IT approaches [41].

Actuators/Sensors: We must not ignore the fact that the field equipment (sensors, actuators) of latest generation is intelligent equipment that is accessible via other communication mechanisms, namely WIFI and the HART protocol. The attacker can modify the configuration of the field equipment's, changing the threshold values to allow readings that should be out of range, and which can put the systems and installation in risk [3].

According to the ICS segmentation discussed earlier, we will provide in the table below (Table.5), a set of information regarding the technologies and components used at each level of the ICS architecture. For Level 4 and 5, we state that they are outside the scope of our study because the systems, services and protocols deployed in these levels are conforms to standard IT approaches and as a result, managing cyber security at these areas using standard security mechanisms should be adequate [42]. Regarding the requirements for functional safety, we consider only the real time requirement because it constitutes the major constraint for applying IT approaches in ICS [25].To elaborate the table below (Table 5) we are based on the result presented by Macaulay et al, in [36] and on the list of security topics that must be supported by the system without impacting real time requirement presented by [43]. The table below recapitulates the impact of cryptography measure applied to all components used in industrial control systems.

The performance of level0 equipment consists of the accuracy of the measurement, the performance in the "CPU: RAM" calculation is optional. Latency is defined as the time interval between a message being sent to a device and a corresponding event occurring [12].

According to the table 5, the components used in levels 2 and 3 are the same technologies used in traditional information systems with the same performance which can guarantee real-time requirements despite the implementation of all the IT security issues mentioned above. Therefore, we can confirm that we can apply the IT approaches to manage cyber security at Levels 2 and 3, but with more attention to level 2, because the safety requirements are more stringent. Whereas the application of security controls at the levels 0 and 1 can have serious impact on the real time requirement and on the functioning of the industrial system and this is mainly due to two factors, the limitation of the computing resources of ICS equipment and the slowness of speeds on existing networks [25].

Table 5. The impact of cryptography measure applied to all components used in industrial control systems.

LEVEL	**Components/ Applications**	**Operating system**	**Protocol**	**CPU / MEMORY**	**Real time Requirements** [36]	**Impact of cryptography ON real time requirements**
LEVEL3	Plant historian Engineering Workstations IT services (DNS, DHCP..)	Stadard OS	TCP/IP	IT perfomance	Minutes TO Hours	OK
LEVEL2	Control Room Workstations HMI Alarms/ Alerts Systems	Stadard OS	TCP/IP	IT performance	Seconds TO Minutes	OK
LEVEL1	DCS/ PLC/RTU	Stadard OS Proprietary OS	TCP/IP Proprietary Protocol (modbus…), HART, WIFI	22 ns/inst 64 MB RAM, 128 MB Flash	MilliseConds TO Seconds	causes latency
LEVEL0	Sensors/ Actuators/ Valves	Proprietary OS	Proprietary Protocol (0-4mA, Fieldbus…), HART, WIFI	[44] Limited resources – Calcul (4 MHz) – Memory (512 Kbytes to Mbytes)	Continuous	Not applicable

C. Degree of Security and safety consideration in ICS systems architecture

Through our analysis, we can conclude that the difficulty of implementing IT approaches in industrial environments lies mainly in the lowest levels 0 and 1 where the functional safety requirements are very high, while we can use the IT approaches with little adjustment to manage cyber security in levels 2 and 3. The table below (Table. 6) illustrates the need for cyber security and safety for industrial control systems (0: corresponds minimum need; 3: corresponds maximum need).

Target Level	**Cyber Security Need**	**Safety Need**
Level 3	Security (+++)	Safety(+)
Level2	Security (++)	Safety (++)
Level 1	Security (++)	Safety (+++)
Level 0	Security (+)	Safety (+++)

Table 6. Safety and cyber security need for ICS per level.

VII. Cyber security impact on safety aspect (Safety integrity level concept)

Safety Integrity Level (SIL) is widely used as safety performance indicator for safety instrumented functions to satisfy the safety integrity requirements. Standard IEC 61508 defines 4 performance levels for the safety functions. For each level, two parameters are specified, one (PFDavg) for safety-related systems operating in a low demand mode of operation and one (PFH) for safety-related systems operating in a high demand or continuous mode of operation. The safety integrity level 1 (SIL1) is the lowest one, while the safety integrity level 4 is the highest level [32].

Safety integrity level (SIL)	**PFDavg interval criteria for systems operating in a low demand mode**	**PFH interval criteria for systems operating in a high demand or continuous mode**
SIL4	[10-5 , 10-4)	[10-9 , 10-8)
SIL3	[10-4 , 10-3)	[10-8 , 10-7)
SIL2	[10-3 , 10-2)	[10-7 , 10-6)
SIL1	[10-2 , 10-1)	[10-6 , 10-5)

Table 7. Safety integrity levels and interval probabilistic criteria for safety-related systems.

International safety standards functional IEC 61508 and IEC 61511 suggests different methods of determining the safety integrity levels required for an instrumented function of security, ranging from fully quantitative methods to fully qualitative methods [45], including Layers of Protection Analysis (LOPA), risk graphs and hazardous event severity matrix but none is preferred. In this section, we will analyze the impact of cyber security threats on the functional safety performance designated by "SIL: Safety integrity level" and how we can use the safety barriers as a cyber security controls.

A. New value of SIL determining

Safety Integrity Level “SIL” as an indicator of the level of reliability required in its classical form i.e. without regard to the risks associated to cyber security does not reflect the effective level required to protect an industrial infrastructure. Taking into account the cyber security aspect of industrial risk analysis, it is certain that the required level of safety integrity should be redefined, but this is not sufficient, it is also necessary to review the structure and design of the system. The process of SIL determination is described in the standard IEC 61508 and it is based on the risk assessment. In this case the risk is understood as a combination of probability or frequency of dangerous event occurrence and its severity [46].Therefore, to determine the new SIL, we have to calculate the probability and impact relating to global risks including cyber security risks and then apply one of the methods proposed by IEC 61508 (part5).

In the context of ICS, the definition of risk should cover both safety risks and cyber security risks. The safety risk is described as a set of undesirable events scenarios with their related likelihoods and impacts; while the cyber security risk is described as a set of scenarios that consist of threats exploiting vulnerabilities with the attached likelihoods and impacts. Risks related to cyber security can be classified into two categories, risks that do not have an impact on the safety part, and risks that can lead to operational risks. In our study, we are interested only in category 2. The figure below (Fig. 3) illustrates the scenario of industrial physical damage caused by safety and cyber security risks.

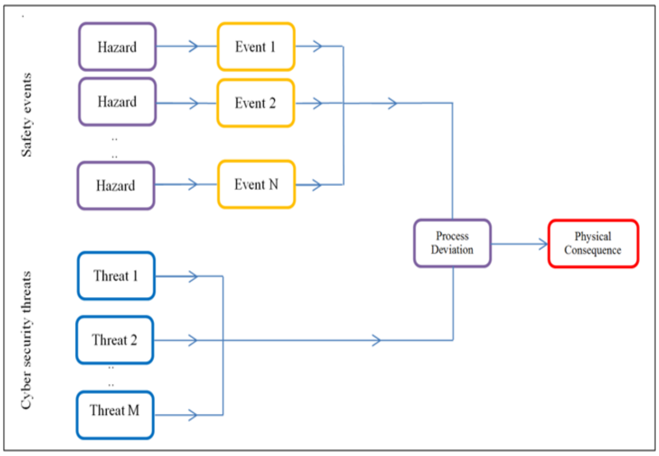

Figure 3. Global physical damage scenarios

The safety and security risks are defined as follows:

R (safety) = {(Sai, Psai, Csai); i=1,2,……,N }; Set of events scenario that can lead to undesirable safety accidents result the same process deviation (*), that can lead to physical damage.
R (cyber security) = {(Sej, Psej, Csej); j=1, 2 …, M}; Set of cyber security scenario leading to the same process deviation (*).

Where:

- P – likelihood of occurrence of S;
- C – impact of consequences of S;
- N – is the number of undesirable events that can cause damages;
- M – is the number of possible cyber security risk scenarios that can cause process deviation.

For the items related to R (safety) are already calculated as part of the functional risk analysis. We still have to define the parameters related to R (cyber security) especially Pse and Csej.

To determine Pse, ANSSI [47] has proposed the following formula to calculate the likelihood Pse: L= E+ [A+U-2 /2]; Where L is the likelihood, E is the exposure, U is the users and A is the level of the attacker. The mathematical operator [:] means to round up to an integer.

For Cse: Each cyber Security scenarios that can lead to the dangerous safety incident, initially causes a deviation in the functioning of the industrial process. This deviation is imperatively taken into account by the analysis of the operational risks (exist event k that can cause this deviation), therefore the consequences of these scenarios (Sei, Sak) are the same (Csai= Csk= C), it suffices to find the corresponding safety scenario related to event k.

B. Process for determining Safety Integrity Level (SIL) by including cyber security risk

The ultimate goal of attacker consists of causing a failure or deviation of industrial process that lead to physical undesirable events consequently must be handled according to safety risk process. As we have proven, the occurrence of safety related events, security related events or both can lead to the same undesirable accidents; the safety barriers used to prevent safety issue could be also used against cyber security attacks. In addition to the negative impact of the IT control on the safety part as we have seen previously, there is reinforcement between the two sides. All these points make it necessary and efficient to have a holistic and global approach for safety and security, integrating two approaches one for safety and other for security. Below, we will illustrate the process of determining the SIL safety integrity level, taking into account both the risks related to functional safety and the risks related to cyber security.

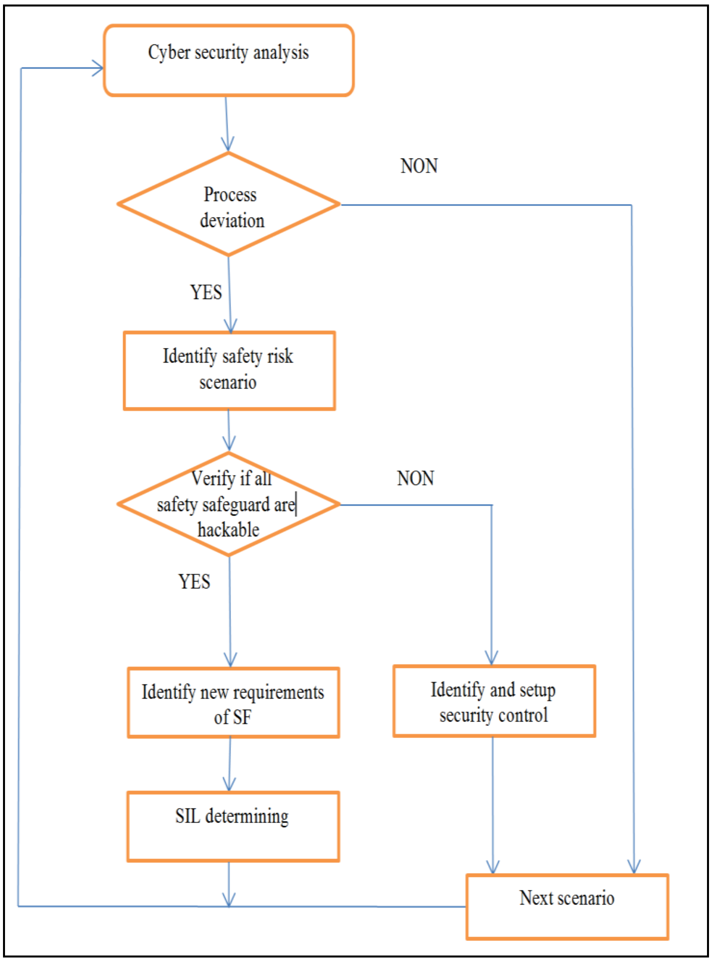
Cyber security analysis
Process deviation
NON
YES
Identify safety risk scenario
Verify if all safety safeguard are hackable
NON
YES
Identify new requirements of SF
Identify and setup security control
SIL determining
Next scenario

Figure 4. Process to determine Safety Integrity Level (SIL) including cyber security risk.

VIII. A new ICS cyber security risk management process

The application of security controls in the industrial control system can have an impact on the safety and the functioning of the industrial system, as we have seen in the above section, it is necessary to integrate the principle “Cyber-safety” in the process of risk management to evaluate and verify the impact after the implementation of a security measure (for example a firewall blocks or delays the sending of alarms) on the functional safety. Below, we will propose a new process to manage cyber security risk in ICS environment that integrate the “Cyber-Safety” principle as recommended in section 5.4. This process allows also, enriching safety requirements by redefining the safety integrity levels “SIL”, in order to take into account cyber security threats.

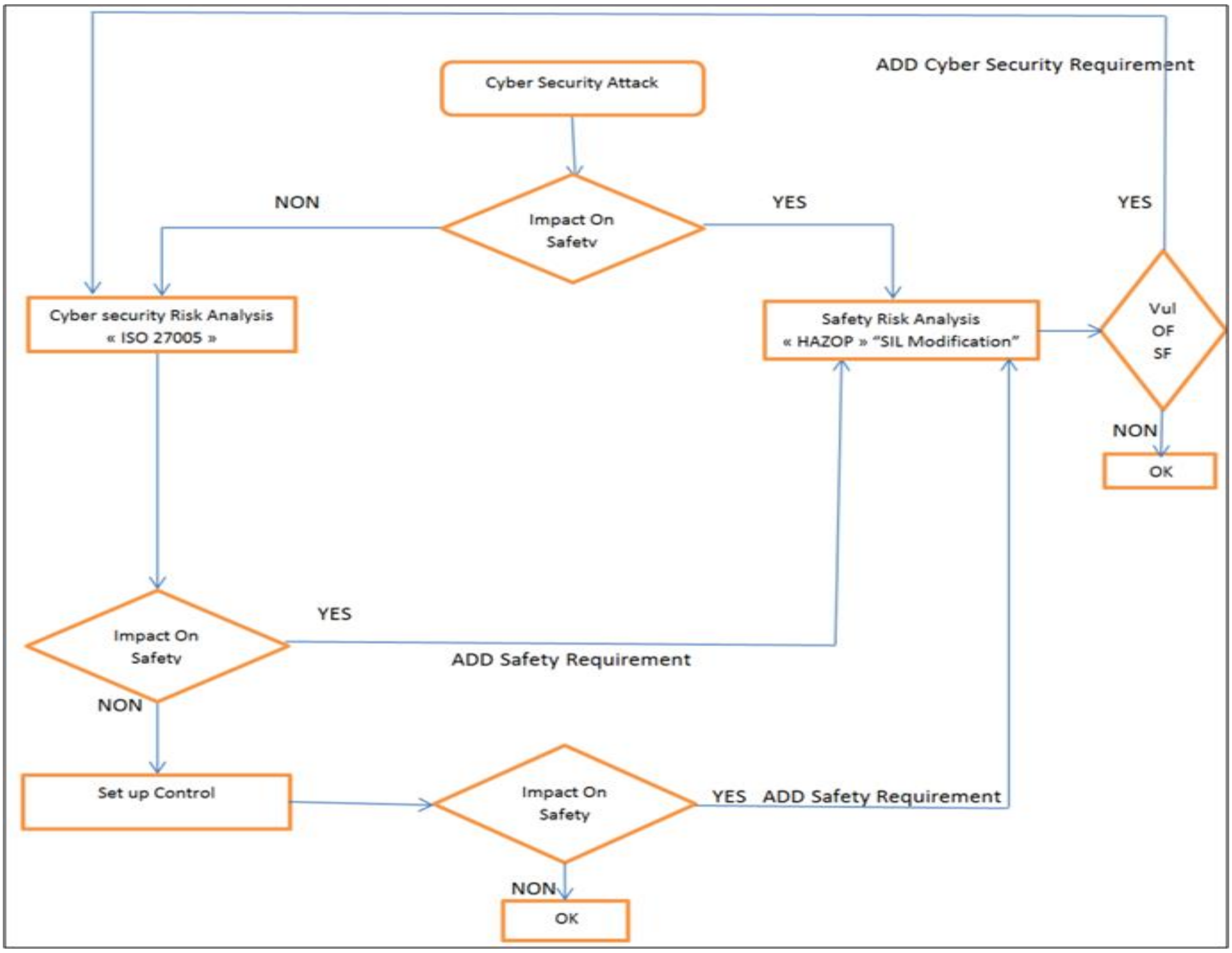
Cyber Security Attack
Impact On Safetv
NON
YES
ADD Cyber Security Requirement
YES
Cyber security Risk Analysis « ISO 27005 »
Safety Risk Analysis « HAZOP » "SIL Modification"
Vul OF SF
NON
OK
Impact On Safetv
YES
ADD Safety Requirement
NON
Set up Control
Impact On Safety
YES ADD Safety Requirement
NON
OK

Figure 5. ICS cyber security risk management process

IX. Conclusion and perspectives

Industrial control systems are exposed to potential cyber security risks of different natures and patterns that could have a serious impact to the health, safety of human lives and serious damage to the environment [25] and can lead to the same dangerous phenomenon as a safety incident [5]. On the other hand, the simple implementation of some standard security measures and controls also may compromise the functional safety requirements and affect negatively the proper functioning of the system; we have cited some scenarios to illustrate these kinds of situations. Through our mapping analysis, we concluded that “non_interference” objective is mandatory to manage cyber security in ICS in order to evaluate and avoid negative impact on industrial safety aspect. Indeed, the requirements and objectives related to security and safety domains converge and can interact with each other, the introduction of cyber security risks in the industrial environment makes the risk analysis related to functional safety already undertaken not credible and requires redoing it from the beginning because it does not consider cyber security risks. Therefore, ICS cyber security risk management system must be designed in a coherent manner that takes into account the cyber security and functional safety requirements (IEC 61508 and derived standards) at the same time.

For that, we carefully studied the interferences and interactions between cyber security and industrial safety and then suggested an easy and efficient way to recalculate the Safety integrity levels “SIL” of systems exposed to cyber security attacks that could harm the functional safety part. And then, we have proposed a preliminary process which meets the Cyber-safety requirements. On the other hand, safety and cyber security are two very rich areas in terms of risk management methodologies and approaches, as cyber security and safety engineering has a long history of good practices, standards and tools, which have reached a high degree of maturity. Using IT approaches or safety approaches separately are unfit to manage cyber security in ICS context and it does not cover all relevant aspects [48]. Therefore, an appropriate approach for managing the cyber security of industrial control systems should be consistent with both aspects of information systems security and functional safety; it must be designed in a coherent manner that takes into account the cyber security and functional safety requirements (IEC 61508 and derived standards) at the same time. For this purpose, we believe that the best way to design a cyber security risk management approach is to consider the security and the functional safety in the same process, based on the integration and combination between cyber security approaches for information systems and safety approaches for industrial systems. For that the relationship and interdependencies between safety and cyber security must be analyzed with careful detail. Also developing new methods to manage the modeling of safety and security interdependencies and responding to the possible conflict between safety requirements and good security practice.

References

[1] X.Xu et al. “Global and initiative safety mechanism in industrial control system”, International Journal of Computational Science and Engineering, 9(1–2), pp.139–146, 2014.

[2] I.N. Fovino. “SCADA system cyber security”, in: Secure Smart Embedded Devices, Platforms and Applications, pp. 451–471, M.Konstantinos, M.Keith. London, 2014.

[3] ENISA. “Communication network dependencies for ICS/SCADA Systems”. European Union Agency For Network And Information Security, 2016.

[4] M.Humayun, et al. "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study”. Arabian Journal for Science and Engineering, 45, pp. 3171–3189, 2020.

[5] H.Abd, M. Kaouk, J.-M. Flaus, F. Masse. “A safety/security risk analysis approach of industrial control systems: a cyber bowtie - combining new version of attack tree with bowtie analysis”, Computers & Security, 72, pp. 175–195, 2017.

[6] T.Alladi, V.Chamola, S.Zeadally. "Industrial Control Systems: Cyberattack trends and countermeasures", Computer Communications, Volume 155, pp.1-8, 2020.

[7] M.Hentea. “Improving security for SCADA control systems”, Interdisciplinary Journal of Information Knowledge and Management, 3, 2008.

[8] W.Schwab, M.Poujol.“The State of Industrial Cybersecurity 2018”. Kaspersky lab, 2018.

[9] R.Mohr. “Evaluating cyber risk in engineering environments: a proposed framework and methodology”. SANS Institute, 2016.

[10] D.Bhamare, M. Zolanvari,A. Erbad, R. Jain,K. Khan, N. Meskin. “Cybersecurity for Industrial Control Systems: A Survey”, Computers & Security, volume 89, 2020.

[11] K.Stouffer, et al. “Roadmap for Measurement of Security Technology Impacts for Industrial Control Systems”. National Institute of Standards and Technology, 2014.

[12] J.Falco, J. Gilsinn, J,K.Stouffer. “IT security for industrial control systems: requirements specification and performance testing”. National Institute of Standards and Technology, 2004.

[13] Y.Hashimoto et al. “Safety securing approach against cyber-attacks for process control system”. Computers & Chemical Engineering, 57, pp. 181–186, 2013.

[14] IEC. “Industrial communication networks – Network and system security Part 2-1: Establishing an industrial automation and control system security program”, IEC 62443-2-1, 2010.

[15] S.Park, K. Lee. “Advanced approach to information security management system model for industrial control system”, The Scientific World Journal, 13 pages, 2014.

[16] J.Martinez , J. Godot, A.Ruiz, A.Balbis, R.R. Nolasco. “Safety and Security Interference Analysis in the Design Stage”, in Computer Safety, Reliability, and Security Casimiro A., Ortmeier F., Schoitsch E., Bitsch F., Ferreira P. (eds). SAFECOMP 2020 Workshops, Lecture Notes in Computer Science, vol 12235. Springer, Cham, 2020.

[17] J.Jang-Jaccard, S.Nepal. “A survey of emerging threats in cybersecurity,Journal of Computer and System Sciences”, 80, pp. 973-993, 2014.

[18] O.El Idrissi, A. Mezrioui, A. Belmekki. “A lightweight risk analysis of a critical infra-structure based ICSs”, in: 2019 1st International Conference on Smart Systems and Data Science (ICSSD), Rabat, Morocco, pp. 1–8, 2019.

[19] M.Śliwiński, E.Piesik. “Designing Control and Protection Systems with Regard to Integrated Functional Safety and Cybersecurity Aspects”, Energies, 14, 2021.

[20] A.Burns, J. McDermid, J.Dobson. “On the meaning of safety and security”. The Computer Journal, 35, pp. 3–15, 1992.

[21] S.Nas. “The Definitions of Safety and Security”, Journal of ETA Maritime Science 3(2), pp.53-54, 2015.

[22] S.Kriaa, L.Pietre-Cambacedes, M.Bouissou, Y. Halgand. “A survey of approaches combining safety and security for industrial control systems”, Reliability Engineering & System Safety, 139, pp.156–178, 2015.

[23] L.Piètre-Cambacédès. “Des relations entre sûreté et sécurité. Cryptographie et sécurité [cs.CR] ”, Télécom ParisTech, 2010.

[24] R.Kissel. “Glossary of key information security terms”. NIST Interagency/Internal Report (NISTIR) - 7298 Rev. 3, National Institute of Standards and Technology, 2013.

[25] K.Stouffer, et al. “Guide to Industrial Control Systems (ICS) Security”, NIST Special Publication 800-82 R2, National Institute of Standards and Technology, 2014.

[26] T.J.Williams. “A Reference Model for Computer Integrated Manufacturing from the Viewpoint of Industrial Automation”, IFAC Proceedings Volumes, Volume 23, Issue 8, Part 5, pp. 281-291, 1990.

[27] J. Weiss. “Industrial control system cyber security and the critical infrastructures”. International Council on Systems Engineering, 19, pp. 33-36, 2016.

[28] O.Luciana. “Secure Architecture for Industrial Control Systems”. SANS Institute, 2015.

[29] S.Kriaa. “Joint safety and security modeling for risk assessment in cyber physical systems”, Other. Université Paris Saclay (COmUE), 2016.

[30] IEC. “Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements”, International Electrotechnical Commission, IEC 61511-1, 2003.

[31] S.Marcin, P.Emilian. “Integrated approach for functional safety and cyber security management in maritime critical infrastructures”, Journal of Polish Safety and Reliability Association, Summer Safety and Reliability Seminars, 10, pp.137-148, 2019.

[32] IEC. “Functional safety of electrical/electronic/programmable electronic safety related systems”, International Electrotechnical Commission, IEC 61508, 2010.

[33] K.Stouffer. “System Protection Profile--Industrial Control Systems Version 1.0”. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, 2004.

[34] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. “Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program”, 2008.

[35] Z.Drias, A. Serhrouchni, O.Vogel. “Analysis of cyber security for industrial control systems”. In International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, pp. 1–8, 2015.

[36] T.Macaulay, B.Singer. “Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS”. Auerbach Publications, 2011.

[37] X.Lyu, Y.Ding, S.Yang. “Safety and security risk assessment in cyber-physical systems”. IET Cyber-Physical Systems: Theory &amp; Applications, 4, (3), p. 221-232, 2019.

[38] ENISA: “Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors”. European Union Agency For Network And Information Security, 2015.

[39] H.I.Kure, S.Islam, M.A. Razzaque. “An integrated cyber security risk management approach for a cyber-physical system”. Applied Sciences 8(6), 898, 2018.

[40] M.Śliwiński, E.Piesik, J. Piesik. “Integrated functional safety and cyber security analysis”. IFAC-PapersOnLine, Volume 51, Issue 24, pp. 1263-1270, 2018.

[41] O.El Idrissi, A. Mezrioui, A.Belmekki. “Cyber Security challenges and Issues of Indus-trial Control Systems–Some Security Recommendations”, in 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, pp. 330-335, 2019.

[42] A.Cook et al. “An assessment of the application of IT security mechanisms to industrial control systems”, International Journal of Internet Technology and Secured Transactions Vol. 7, No. 2, 2017.

[43] U.S. Department of Homeland Security. “Recommended Practice- Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies”, 2016.

[44] H.Karl, A. Willig. “Protocols and architectures for wireless sensor networks”. Wiley. Wiley–Blackwell, 2005.

[45] A.C.Torres-Echeverria. “On the use of LOPA and risk graphs for SIL determination”, Journal of Loss Prevention in the Process Industries, Volume 41, pp. 333-343, 2016.

[46] E.Piesik, M.Śliwiński, T.Barnert. “Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects”, Reliability Engineering & System Safety, Volume 152, pp. 259-272, 2016.

[47] ANSSI. “Cybersecurity for Industrial Control Systems – Classification Method and Key Measures”. Agence nationale de la sécurité des systèmes d’information, 2014.

[48] O.El Idrissi, A.Mezrioui, A.Belmekki. “Inadequacy of IT Approaches to Manage Cyber Security in ICS Context”, in Proceedings of the 12th Inter-national Conference on Soft Computing and Pattern Recognition (SoCPaR 2020), Abraham A. et al. (eds). SoCPaR 2020. Advances in Intelligent Systems and Computing, vol 1383. Springer, Cham, 2020.

Author Biographies

Omar El Idrissi is currently a PhD student at the the Moroccan Telecommunications Graduate Institution (INPT), Rabat, Morocco. He was born in El Jadida, Morocco, in 1975. He obtained a master’s degree in Network Service Mobility from Henri Poincaré University, Nancy 2 France in 2008 and a master’s degree in cyber security from INPT in 2017. He is the Information Security Manager of Morocco’s Samir refinery since 2004. His research interests include information security, in particular cyber security for industrial control systems and IOT.

Abdellatif Mezrioui received his PhD in the field of software engineering from the University of Nancy 1 France in 1993. He is a Full Professor at the Moroccan Telecommunications Graduate Institution (INPT) since 1995. He has served as the head of the Mathematics, Computer Science and Networks Department on several times. He was responsible of the research team RAISS at INPT (2013-2018). He was also the coordinator of the cyber security master at INPT (2015-2020). His actual research interests are related to cyber security of Cloud Computing, IoT and ICS infrastructures.

Abdelhamid Belmekki received the PhD thesis in Computer Science from the Hassan II University, Mohammadia, Morocco in 2010, and Bachelor in Mathematics from the Mohamed V University in Rabat, Morocco in 1998. Currently, since 2010, he is a Professor in the National Institute of Posts and Telecommunications (INPT) in Rabat, Morocco. He is member of RAISS (Network, Architectures, Service Engineering and Security) research team of the 2TI laboratory in INPT, Rabat. his research topics include Cybersecurity, privacy, computer security.