Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 191 (2021) 33–40

Procedia Computer Science

www.elsevier.com/locate/procedia

The 18th International Conference on Mobile Systems and Pervasive Computing (MobiSPC)
August 9-12, 2021, Leuven, Belgium

Vulnerability and security risk assessment in a IIoT environment in compliance with standard IEC 62443

Hicham Lalaoui Hassani[a,b,*], Ayoub Bahnasse[c,d], Eric Martin[a], Christian Roland[a], Omar Bouattane[c], Mohammed El Mehdi Diouri[b]

[a] *University Bretagne Sud, Lab-STICC (Laboratoire des Sciences et Techniques de l'Information de la Communication et de la Connaissance), Lorient, France*
[b] *LREA, Institut Supérieur du Génie Appliqué IGA, Casablanca, Morocco*
[c] *Lab SSDIA, ENSET Mohammedia, Hassan II University of Casablanca, Morocco*
[d] *ENSAM Casablanca, Hassan II University of Casablanca, Morocco*

Abstract

Industrial networks based on the Internet of Things (IoT) have become the backbone of Industry 4.0. Indeed, these connected objects increase the efficiency, flexibility and autonomy of machines, thus improving the productivity and profitability of factories. However, the opening up of digitization technologies, especially in environments where failure is hardly tolerable, creates new challenges related to security. The number of vulnerabilities in industrial facilities is constantly increasing [1]. To implement a cyber defense framework for industrial systems, the cybersecurity standard IEC 62443 has been proposed. This standard mainly provides a set of instructions and measures to be put in place to ensure not only the security of the industrial system, but also operational safety. In this paper, we propose a new approach based on the standards IEC 62443-3-2 and IEC 62443-4-2 allowing us to verify, through an in-depth risk assessment, the conformity of the objects with the main security requirements.

Keywords: Assessment method; IEC 62433; IIoT; Industry 4.0; risks; vulnerabilities.

1. Introduction

Industry 4.0 is based on the integration of digital technologies with production techniques to make tasks autonomous, programmable and efficient. Among these technologies, we mainly cite the Industrial Internet of Things (IIoT). The IoT refers to all physical objects connected and communicating via the Internet. The IIoT allows all the

[*] Corresponding author. Tel.: +212-663-514-791.
E-mail address: hicham.lalaoui@iga.ac.ma

10.1016/j.procs.2021.07.008

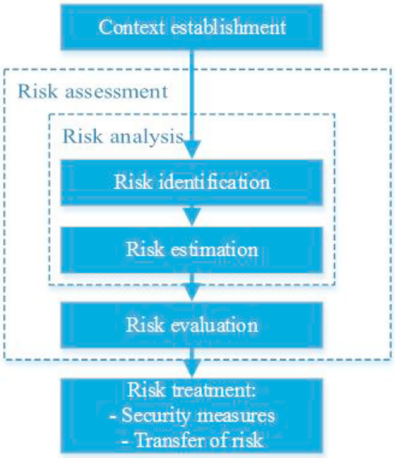

Fig. 1. General approach of a risk analysis.

actors of the industrial chain to communicate from the machines to the customers. The opening on digital technologies and the benefits of Industry 4.0, gave rise to new challenges, mainly in relation to cybersecurity and the standardization of communications between objects. Indeed, the situation exposes industrial systems to conventional threats such as unavailability, identity theft, alteration and disclosure of confidential data. To better assimilate these risks and build a more resilient system, the IEC 62443 [2] standard has been proposed. This standard, which is specific to the cyber security of industrial installations, is interposed between the two standards ISO 27000 and IEC 61508, which relate to the security of information systems and operational safety respectively [3]. Several risk analysis methods (EBIOS, MEHARI, etc.), following the recommendations of the ISO 27005 standard, have been designed for the needs of information systems [4]. These methods converge in a number of points and follow more or less the approach described in Figure 1.

IEC 62433 is aimed at the various players in Industrial Control Systems (ICS): owners and operators, system integrators, product or service providers, government agencies and regulatory bodies. This standard covers ICS: automated systems, supervision systems (SCADA) for industrial processes, and also control systems for transport or energy networks, as well as installations including IIoT equipment. In the following section, we present a collection of work on the subject carried out by some researchers.

2. Related works

Several contributions related to the IEC 62443 standard have been made to secure industrial environments. Rekik et al [5] deal with the cyber security issues to which railway systems are exposed affecting overall performance. They start by analyzing the characteristics of threats to railway systems. Then, they examine the direct impacts of the identified potential threats and their consequences on the overall system. The authors assess, according to IEC 62443, the risks based on the analysis of impact and likelihood of the threat on system functionality, namely the control of external doors. A set of countermeasures has been proposed to reinforce the security of the system against the identified potential threats. The effectiveness of the countermeasures was demonstrated with several iterations of the risk assessment process. Shaaban [6] reused the IEC 62443 standard by breaking down the IACS system components into zones and ducts according to the required security levels. To improve safety at the component level, the author takes up this idea on a small scale to show how the same concept can be used to define zones and ducts between mixed criticality components. The MORETO tool, capable of automatically recognizing and identifying the zones and ducts of a given ’Purdue’ diagram, implements the safety risk analysis process. Chai Jiwen [7] presents a comprehensive vulnerability assessment platform for evaluating cyber security devices and networks in intelligent substation automation systems. His paper refers to IEC 62443-3-3, Fundamental Requirements (FR) and Security

Requirements (SR). In [8], Juárez cited three essential recommendations for the development of an IoT-type system in industrial environments that meet the necessary security requirements [9]. Some articles [10, 11] have addressed the vulnerabilities that can potentially affect an IoT device, as well as potential protection methods [11]. To ensure compliance of their IIoT device with the IEC 62443 standard before its integration in the industrial environment, their approach proposes a pentesting evaluation model to detect surfaces and etching vectors with the aim to reduce them.

3. Research Motivation

We propose to evaluate the risks to which the IIoT objects are exposed in order to validate them or to apply corrective measures in a second step before integrating them into the industrial system.

3.1. Proposed Evaluation Model

Using a qualitative approach, based on the IEC 62443 Part 3-2 [12], the authors recommend following a three-step approach (described by the majority of IS security risk control methods):

- Identification of critical information systems.
- Detailed risk analysis for these information systems.
- Definition of the security measures applicable to these systems.

First, a network map of the site or plant should be available to identify which CSIs can be partitioned. A brief risk analysis is then performed for each of the identified systems. Two parameters are evaluated:

- The probability or likelihood of the attack on the system.
- The severity or impact on essential assets.

’Likelihood’ identifies the likelihood that a specific threat will be realized, while ’Impact’ determines the magnitude of destruction that the threat may cause. Tables 1 and 2 below define possible values for each of these variables. The likelihood rate is inferred from a count of the occurrences of attacks on the platform over a given period of time.

Table 1. Likelihood of a threat.

Element of occurrence	Probability of occurrence	Score
Never occurred	Improbable	1.5
Occurred only once a week	Unlikely	3
Occurred several times a week	Moderate	5
Occurred once a day	Probable	7
Occurred several times a day	Certain	9

On the other hand, to evaluate the impact rate of these threats, we looked at the three properties of security; namely, availability, integrity and confidentiality. Indeed, an insignificant level of impact, for example, corresponds to a few minutes of unavailability, to some altered but correctable data or to some data disclosed internally but of little importance. Table 2 below gives details of the different impact rates with a description of their consequences.

Referring to AMDEC method [13], this process identifies the risk level of each threat applicable to the system based on the equation:

$$Risk = Likelihood \times Impact. \tag{1}$$

From this, we can deduce the levels of risk detailed in Table 3. In this case, a risk classified as Category 1 corresponds to a estimated rate of less than 4 - which is insignificant - and therefore requires no action. On the other hand,

Table 2. Impact score.

Level	Availability	Integrity	Confidentiality	Score
Insignificant	Less than a few minutes	Some correctable altered data	Some data exposed in-house	0,5
Minor	Less than a few hours	Several correctable altered data	Several data exposed in-house	2
Medium	Less than a few days	Some unrecoverable altered data	All data exposed in-house	4
Important	Less than a week	Several unrecoverable transaction data	Some externally exposed data	7
Severe	More than a week	All unrecoverable altered data	Several data exposed externally	12

a class 4 risk is qualified as ”Very Important” and requires immediate action even if it leads to a temporary cessation of activity.

Table 3. Risk level.

Risk Class	Level	Score	Action required
1	Insignificant	< 4	Risk accepted
2	Medium	>= 4 et < 18	Risk accepted and monitored
3	Important	>= 18 et < 37	Action required and planned
4	Very important	>= 37	Immediate action required

ICS are rated in a likelihood-impact matrix to classify them according to the risks involved. In their case, four classes are proposed. The matrix below (Table 4), which is based on the IEC 62443-3-2 guide, classifies systems according to the impact and likelihood of their attack.

Table 4. Impact/likelihood Matrix.

		Impact				
		Insignificant	Minor	Medium	Important	Severe
Likelihood	Improbable	0.75	3	6	10.5	18
	Unlikely	1.5	6	12	21	36
	Moderated	2.5	10	20	35	60
	Probable	3.5	14	28	49	84
	Certain	4.5	18	36	63	108

Ultimately, the aim of controlling the cybersecurity of industrial systems is to reduce risks that could lead to a disruption in the activity carried out by these facilities. More or less restrictive countermeasures may be applied, depending on the risk class.

3.2. Testbed

As a starting point, the standard proposes to clearly identify the system under consideration (SuC), which consists of all the objects involved in this by the analysis. In their case, the test model (Figure 2) represents a functional description of a metal construction plant that performs sorting, assembly and control functions for parts. Its architecture is composed of several elements: a Siemens S7-300 PLC, an Industrial Control Bench (ICB), a Raspberry PI 2, an Arduino Mega 2560, an HMI station, a wireless access point, a mobile terminal to supervise the Raspberry Pi2 controller, three non-configurable switches, three firewalls and an Internet access gateway.

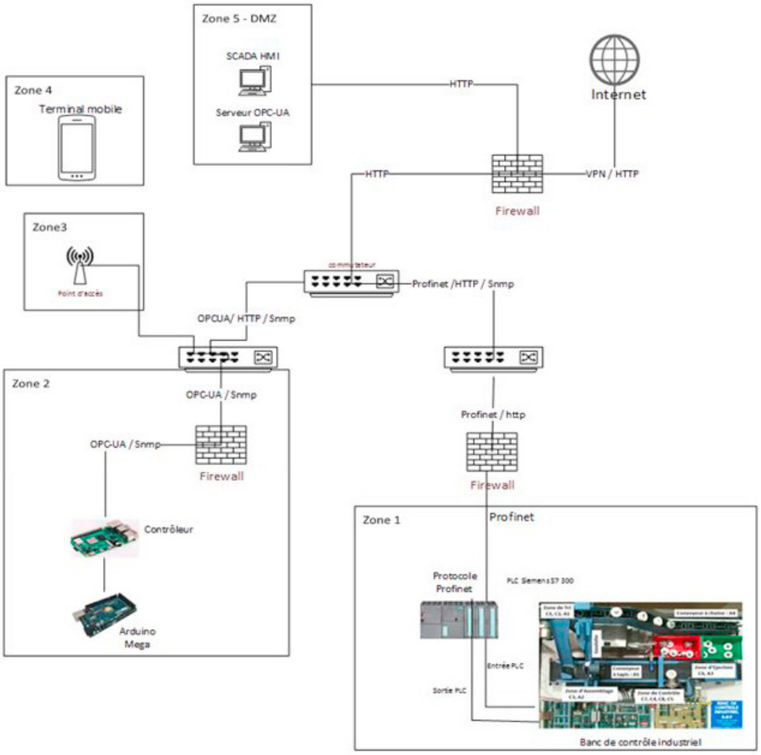

Fig. 2. Testbed broken down into zones and conduits.

Once the SuC is identified, the evaluation phase, begins which initiates the asset allocation phase to zones and conduits in order to prepare the detailed analysis. The aim is to achieve a given level of security per zone in compliance with the rules imposed by the IEC 62443 standard. In fact, according to the IEC 62443 standard, system security requirements are grouped into seven Fundamental Requirements (FRs): Identification and Authentication Control (IAC), Use Control (UC), System Integrity (SI), Data Confidentiality (DC), Restricted Data Flow (RDF), Timely Response to Events (TRE) and Resource Availability (RA). The importance of this assignment is that each specific scenario has different levels of security associated with the tolerable risk for each organization. In our model, partitioned into zones and conduits as shown in Figure 2, we are interested in studying the IAC security requirement by zone according to the following distribution:

- Zone 1: control and command, consisting of an industrial control bench controlled by a programmable logic controller. The BCI is composed of two conveyors, 7 detectors and 3 actuators that allow the sorting of the parts produced according to their nature as well as their conformity with the desired product. In this area there is no identification required to access the programming of the PLC, i.e. there is no user or administrator account required. In this case, the likelihood of unauthorized access to zone 1 is ”probable”.
- Zone 2: measurements of physical quantities, consisting of a Raspberry controller and an Arduino acquisition board connected to two sensors (temperature and humidity). The access interface of the Raspbian OS uses a default login and password and no access control policy is in place. In addition, the Node-Red programming interface is not secure. Remote access to the Raspberry is however prohibited. The likelihood in this area is ”moderate”.
- Zone 3: Wireless access point, consisting of a Wi-Fi terminal. It is secured with a WPA2 encryption key only. No authentication protocols are implemented such as TACACS+ and Radius. The likelihood in this zone is ”moderate”.

Table 5. Risk level for unauthorized access thread by zone.

Zones	likelihood	Impact	Level of risk
Zone 1	Probable	Important	Very Important (risk = 49)
Zone 2	Moderated	Important	Important (risk = 35)
Zone 3	Moderated	Medium	Important (risk = 20)
Zone 4	Unlikely	Minor	Medium (risk = 6)
Zone 5	Improbable	Minor	Insignificant(risk = 3)

- Zone 4: Temporary mobile equipment, consisting of a mobile monitoring terminal. The access to the supervision interface is done by a hardened authentication on an Android application through the Wi-Fi terminal. The likelihood in this zone is ”unlikely”.
- Zone 5: DMZ, access to the supervision servers via the Internet by a regularly reviewed and modified. The likelihood of the vulnerability in this zone is ”unlikely”.

Conduits are defined as network services (HTTP, SNMP and OPC-UA) allowing communication or passage of the information flow between two areas. However, this communication is not encrypted. This means that logins and passwords are transmitted in clear text and may be the target of a sniffing attack. However, zone 2 is linked to the rest of the network by a conduit implementing the OPC-UA IIoT communication protocol, which can be reinforced by an authentication (login and password/digital certificate), an encryption algorithm or a digital signature [14].

3.3. Risk assessment applied to their testbed

The practical evaluation of their approach took place over two weeks at a rate of 5 hours per day in order to truly quantify the occurrences of the threats materialized within the laboratory. To do this, they have made available to the Pentesters tools for exploiting attacks on the Siemens S7-300 PLC, a frame analysis tool that supports all communication protocols in order to attempt, for example, to gain unauthorized access to connected objects. This approach allowed them to assess the level of risk faced by the model, by zone. Based on the impact and likelihood levels mentioned above in the metrics, they evaluate authentication in the different zones in this study. Here are few sources of plausible threats or vulnerabilities:

Unauthorized access : due to the non-existence of an authentication phase refers to the illegal use of infrastructure assets such as program changes at the PLC or Arduino level. Usually, these attacks target both IAC and SI requirements. Their impact is described according to the areas in Table 5. As an example, an intrusion in zone 5 does not present any danger to the smooth running of the production and therefore the impact is assumed to be ”Minor”. Whereas in zone 2 the impact would be ”Important” as it would allow an attacker to change the control program in such a way as to disrupt the production process. Whereas in zone 2 the impact would be ”Important” since it would allow an attacker to change the PLC control program in such a way as to disrupt the production process (e.g. select metal parts that do not meet the technical specification instead of those that do).

Non-secure software services Web applications and OSs can be compromised by malware. In their case, the non-existence of the https protocol for web access to the Node-Red programming interface as well as the fact that the default password of the Raspberry OS is not changed can lead to such threats. This type of attack can affect all three security requirements, namely SI, IAC and RA.

Rootkit a backdoor installed in an information system providing uninterrupted and secret access with administrator privileges. This type of malware is primarily aimed at compromising the integrity and authenticity of systems.

Spyware It can be executed at the support and application layer and targets the confidentiality of the IIoT system (e.g. keylogging).

Table 5 provides a summary of the estimated risk levels per area regarding the threat of unauthorized access to the system.

4. Evaluation

In their risk assessment approach, they have used the recommendations of standard IEC 62443 related to the Fundamental Requirements (FRs) and more specifically FR1: Identification and Authentication Control (IAC). These recommendations were applied to an industrial facility represented by their test model. They were able to implement a detailed risk assessment method by zone, which allowed them to detect the vulnerabilities that generate a high level of risk on the model. The interest of this first analysis is to assess the likelihood of threats while taking into consideration the degree of impact. This also allowed them to deduce the level of risk, wich gives a clear idea of the most harmful vulnerabilities. The threats identified exploit the fact that the security level of the FR under study (IAC) is limited to SL0. The impact assessment takes the following factors into consideration:

- The mission of the system or the business processes involved.
- The criticality of the system, derived from the value of the data to the organization.
- The sensitivity of the system and its data.

The data required for an impact assessment can be retrieved from organizational documentation. A business impact analysis uses quantitative or qualitative means to determine the impact of damage or harm to the organization's business assets. The ultimate objective is to apply countermeasures to each area of the model according to the security properties to be ensured. They have noted, for example, that the threat linked to authenticity can generate a set of risks on the model. Indeed, by exploiting tools offered on the Internet [15], the attacker can repeatedly send commands to the PLC such as the STOP function. However, countermeasures must be applied to the cyber security requirements by zone, e.g. such as protecting inter-zone communications with secure protocols. In addition, they propose countermeasures that can be applied at the time of implementation, such as:

- The prohibition of extracting of the .hex file from the Arduino circuit.
- The application of authentication using a login and password for programming of the IIoT object.
- The modification of the Raspberry default password.
- Adding authentication on the PLC before importing the Ladder program.

5. Conclusion

The model studied in this paper aims to estimate in the most accurate way the risks incurred by an industrial installation in view of the detected vulnerabilities. The impact rate is a very important parameter. Therefore, additional aspects have to be included in the impact analysis such as:

- The number of annual occurrences of threats exploiting a vulnerability
- The approximate cost of the attacks perpetrated

The simultaneous management of several objects is a tedious task especially when security policies are subject to continuous changes, or when the objects to be connected have specific vulnerabilities to be checked. From this point of view, the Software-Defined Network (SDN) paradigm represents an important improvement to ensure centralized control and automatic countermeasures in an industrial installation of several network nodes. This last point is part of their perspectives. On the other hand, their evaluation model requires further development. Indeed, the evaluation method proposed in this article does not take into account the other security requirements listed above. In this sense, it is necessary to list the threats related to these different FRs and their respective impacts; and in order to avoid a number of false positives, it would be interesting to distinguish between cyber security-related events and the usual technical failures that physical objects undergo.

References

[1] I. Kaspersky, Threat landscape for industrial automation systems, Tech. rep. (2019).

[2] IEC, Quick start guide: An overview of isa/iec 62443 standards, isa global cybersecurity alliance.

[3] P. Kahn, Cybersecurite et securite fonctionnelle pour systeme embarque: Quel (s) referentiel (s)?, in: Congrès Lambda Mu 21,Maîtrise des risques et transformation numérique: opportunités et menaces, 2018.

[4] M. Romdhane, Comment adapter une méthodologie d'analyse de risque cybersécurité d'un contexte aéronautique au ferroviaire?, in: Congrès Lambda Mu 21 Maîtrise des risques et transformation numérique: opportunités et menaces, 2018.

[5] M. Rekik, C. Gransart, M. Berbineau, Cyber-physical security risk assessment for train control and monitoring systems, in: 2018 IEEE Conference on Communications and Network Security (CNS), IEEE, 2018, pp. 1–9.

[6] A. M. Shaaban, E. Kristen, C. Schmittner, Application of iec 62443 for iot components, in: International Conference on Computer Safety, Reliability, and Security, Springer, 2018, pp. 214–223.

[7] C. Jiwen, L. Shanmei, Cyber security vulnerability assessment for smart substations, in: 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), IEEE, 2016, pp. 1368–1373.

[8] F. A. B. Juárez, Cybersecurity in an industrial internet of things environment (iiot) challenges for standards systems and evaluation models, in: 2019 8th International Conference On Software Process Improvement (CIMPS), IEEE, 2019, pp. 1–6.

[9] L. G. Whitepaper, Overcoming the hurdle of iot security, Tech. rep. (2019).

[10] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things, in: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), IEEE, 2015, pp. 1–6.

[11] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, Y. Jin, Security analysis on consumer and industrial iot devices, in: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE, 2016, pp. 519–524.

[12] IEC, security for industrial automation and control systems - iec 62443-3-2 part 3-2: Security risk assessment for system design, Tech. rep. (June 2020).

[13] V. Ozouf, Comment conserver un niveau de risques acceptable dans un contexte de conception/industrialisation de plus en plus rapide d'un produit de plus en plus complexe?, Ph.D. thesis, Université de Savoie (2009).

[14] IEC, 62541-2 OPC Unified Architecture – Part 2: Security Model, November 2020.

[15] Dark-lbp, Industrial control system exploitation framework, https://github.com/dark-lbp/isf (2020).