Obtaining High Preventive and Resilience Capacities infraestructure by industrial automation cells.

Date: 2020-03-06

Santiago G. González [a,*], S. Dormido Canto [b], José Sánchez Moreno [b].

[a] National Centre for the Protection of Infrastructures and Cybersecurity, Secretary of State for Security, Ministry of Interior Spain, CETSE, El Pardo, Madrid,28048, Spain

[b] Department of Computer Science and Automatic Control, Universidad Nacional Educación a Distancia (UNED), Madrid, 28040, Spain

Keywords:

Cybersecurity

Industrial Control System

Critical Infrastructure

National Security

Cyber Resilience

Abstract

The advances in Information Technologies (ITs) are providing Industrial Control Systems (ICS) with a great capacity for interconnection and adaptability. However, the use of communication networks makes ICS highly vulnerable. Consequently, it is essential to develop methodologies for the identification and subsequent classification of the ICS that intervene in critical infrastructure assets with any level of complexity, scalability and heterogeneity. The System and Infrastructure of Knowledge for Real Experimentation by means of Cells of Industrial Automation (SIKRECIA), described in this work, provides new capabilities for research, development, simulation and testing of the functioning of these systems, and the ability to foresee the behavior of a specific system in industrial production. The scenarios recreated through SIKRECIA have the ability to anticipate new threats that affect the ICS of critical infrastructures. Using SIKRECIA, a specific vulnerability of a PLC has been verified through the engineering programmed for the management of a traffic light control system. The results obtained demonstrate the high dependence between IT and OT (Operation Technologies) systems and therefore the importance of being able to recreate those environments before entering into operation. As SIKRECIA is an open system, it can

* Corresponding author. Tel.: +34 696 400 360; fax: +34 913987690

Email addresses: Santiago.gonzalez@invi.uned.es - sgg@interior.es (S. G.-González), sebas@dia.uned.es (S.Dormido-Canto), jsanchez@dia.uned.es (J. Sánchez-Moreno)

use components from different industrial manufacturers to cover the existing architectures in the process industry.

1 Introduction

The research presented in this contribution is the result of the work developed in the area of cybersecurity in ICS environments [1, 2, 3]. To obtain a real result adapted to the specific needs of the so called "evaluation of prior risks" in an industrial production system, it is necessary to use real scenarios. At the same time, it provides the ability to perform forensic analyses of non-allowed interventions and analyses of behavior patterns through different tools present in the SIEM (Security Information and Event Management).

Academic institutions must take the initiative in the provision of scenarios for simulation testing and tests of real components of the industry, as well as the architectures deployed for this purpose. The importance of virtualized environments should be relegated to the background, since industrial systems require real contexts with complete operational readiness. These actions are intended to generate confidence in the world of operation technologies (OT).

One of the main issues that motivated the work presented here was the analysis of what was proposed in the technical report "Introduction to the Framework Certification of Cybersecurity Components (ICCF)" [4] , published by the Joint Research Centre (JRC), the science and knowledge service of the European Commission, which pursues a scientific dispensation provision for the European policy-making process. This report aims to propose an initial set of common and comprehensive European requirements to promote IACS cybersecurity certification in Europe, to the point where suppliers are stimulating new demands by responding with innovation in its products to devise the cybersecurity certification of IACS components and play a key role in protecting critical infrastructures, and as a result of improving the resilience of systems and, therefore, both , a greater sense of security for citizens.

The IACS Components Cybersecurity Certification Framework (ICCF) aims to provide sufficient help to make certification in cybersecurity fluid and easy, always at a controlled cost and with recognition within and outside European borders. In this way, the possible inclusion of the SIKRECIA system as one more architecture collaborating in IACS is feasible, having a place by its very nature within the role of ICCF identified as laboratory, and complying with consistent evaluation pathways in evaluation, assessment, testing and certification. With the

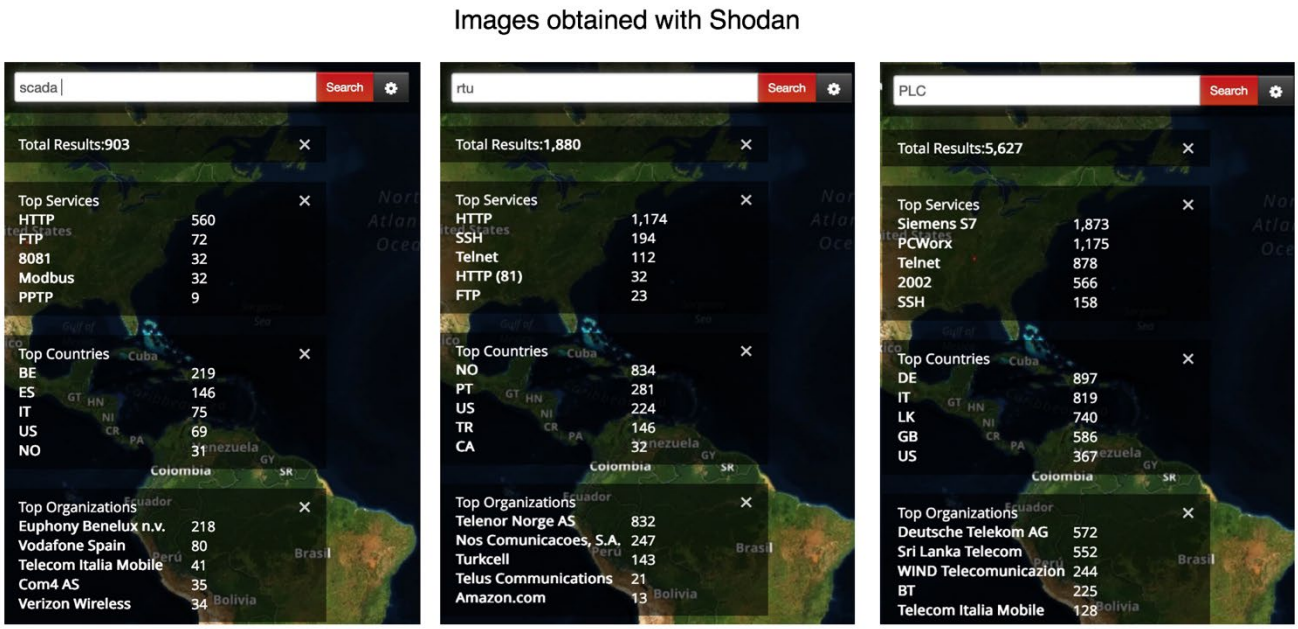
Industrial Automation Cell (IAC 1) [5,6] developed as the basic tool for this study using an architecture of the manufacturer SIEMENS, it has been possible to implement at an atomic level each one of the most common processes existing in any industrial environment. The industrial elements incorporated into the IAC 1 provide various capacities that are carried out in industrial processes:

- The SIEMENS S7 1200 PLC, used through an OPC server (Ole for Process Control) [7], can be connected with MATLAB and Simulink [8]. In this way we can obtain patterns of behavior in different industrial environments.
- Simulation of uninterrupted processes over time and in a completely automatic way (continuous and discrete signals).
- Simulation of discrete processes, depending on the data provided by external agents (analog and digital sensors remote terminals etc.)
- Design of autonomous control of PID1 processes (control mechanisms by feedback) typical of PLC.
- Analysis of graphic patterns obtained from the processes.
- Local and remote connectivity under multiplatform architectures, granting the ability to analyze vulnerabilities associated with ICS, operating systems and, what is more important, the combination of both.
- Deployment of SIEM [9,10,11] systems not only assigned to IT but also to OT.

In summary, what this research tries to determine is the effectiveness of the prediction by knowing the preventive measures taken and, as a direct consequence of this, learning how to improve them [12,13]. That is, the resilience capabilities in cybersecurity [14,15,16] in the convergence of the IT and OT worlds, as a simple demonstration of the exposure levels of industrial instrumentation, using the Shodan tool, [17] which is a search engine developed so that, through a variety of filters, there are equipment (routers, servers, plc, etc.) connected to Internet.

A significant example of the level of exposure to the Internet of ICS systems, are the results obtained (see Figure 1).

1 A proportional–integral–derivative controller (PID controller or three term controller) is a control loop feedback mechanism widely used in industrial control systems and a variety of other applications requiring continuously modulated control.



(a) key word: SCADA (b) key word: RTU (c) key word: PLC

Figure 1. Images obtained after a simple search with Shodan: Time stamp 20190613

This level of exposure of Industrial Control Systems makes it easier for today to be a reality of concern to the governments of different nations. So, for example we get the following news :

- 2019-October: *"54 Percent in Utility Sector Expect Cyber Attack on Critical Infrastructure in Next Year."*
- 2020 February: *"CISA: Cyberattack Resulted in Two-Day Shutdown of Natural Gas Pipeline."* (https://www.hstoday.us/subject-matter-areas/infrastructure-security/54-percent-in-utility-sector-expect-cyber-attack-on-critical-infrastructure-in-next-year/)
- *2019 April : "Cyber-attacks 'damage' national infrastructure."*
  "CISA: Cyberattack Resulted in Two-Day Shutdown of Natural Gas Pipeline"
- *2019 May: "Cyberattacks are the newest frontier of war and can strike harder than a natural disaster…"*
  https://www.businessinsider.com/cyber-attack-us-struggle-taken-offline-power-grid-2019-4?IR=T.
- July 2019: *"An estimated two million cyber-attacks in 2018 resulted in more than $45 billion in losses worldwide as local governments struggled to cope with ransomware and other malicious incidents."*
  https://www.securitymagazine.com/articles/90493-cyber-attacks-cost-45-billion-in-2018.
- May 2019. *"Experts assess damage after first cyberattack on U.S. grid."*

https://www.eenews.net/stories/1060281821.

Governments have long worried about the potential for a cyberattack on their country's critical national infrastructure, and the researchers have attempted to calculate just how much such an event would cost the economy.

An attack on the UK's power distribution network could cost the country's economy between £12bn and £85bn. The report by University of Cambridge researchers models the economic impact of a coordinated and sustained cyberattack on the UK's power distribution networks. It concludes that a widespread cyberattack on a piece of the UK's critical national infrastructure could cost the country tens of billions of pounds. The paper was written by academics from Cambridge Centre for Risk Studies, part of the University of Cambridge Judge Business School, and sponsored by Lockheed Martin [18].

This article focuses on the development of SIKRECIA. This will allow a great flexibility of creation and evaluation of real OT environments. The objectives of the SIKRECIA system are broad and ambitious, since it is designed from the beginning to address the world of IT and OT in an equitable way, given the emerging great co-dependence in the ICS world.

The convergence between IT and OT makes it necessary to create a new definition in the field of cybersecurity of industrial environments: Convergence of Information Technology and Operation (henceforth, CITO). This definition should encompass the technological field and the purest definition of the mechanical and electronic processes supported under the intercommunication thereof.

As a consequence of this situation, the objectives established in the work have been:

Evaluate the effectiveness of a specific IT OT architecture implemented to evaluation, based on the actual production of the network and the operational architectures.

Develop different behavior patterns under the creation of modeling and evaluation systems with the capacity to be incorporated in SIEM systems.

Portability of the automation cell for fast connectivity outside the scope of remote and virtual laboratories.

Implement the high cohesion capacity with technologies from different manufacturers through communication protocols (PROFINET PROFIBUS,S7)[2], as possible future lines of implementation. .

Grant real and remote access to the IAC programming environment.

2 Proprietary communication protocol of SIEMENS.

Provide the ability to deploy any operating system whose mission is to interact with the laboratory. Thanks to the availability of a virtual machine server, a high number of options will be granted, giving complete autonomy to the system user.

Provide the ability to analyze the real time behavior of vulnerabilities in the operating systems (OS) or in an industrial control system and, most interestingly, of both at the same time.

Facilitate and inform in a legal and convenient way of the discovery of some type of IT OT vulnerability from "0 Day" type found during the deployments.

The notification protocol would require a previous confidentiality agreement between the university and the manufacturer of the industrial device to be tested, which would be renewed biannually or when the conditions that originated this agreement change. (https://www.incibe.es/protege-tu-empresa/blog/importancia-proteger-informacion-mediante-acuerdos-confidencialidad)

Obtain patterns of behavior from different sources:

- Patterns of behaviors obtained from the SIEM system of Alien Vault OSSIM.
- Databases displayed in the SCADA (Supervisory Control and Data Acquisition) system.
- Graphic patterns generated from different industrial variables.

Generate knowledge extrapolated to the academic world from the Spanish and European critical infrastructures and manufacturers of industrial devices.

Regarding the structure of the document, Section 2 highlights the importance of the ICS and the tools that are used today as test bed for these environments, while at the same time describing the objectives established in the present investigation. Section 3 is devoted to methodology, materials and analysis through the use and creation of an Industrial Automation Cell (IAC) with SIEMENS technology and different simulations of industrial processes related to SARLAB. Section 4, explains and describes the degree of innovation contributed to the world of industry and research with the creation of the system developed. Section 5 reports the results obtained from SIKRECIA; in this section, the IAC 1 and the human machine interface created for remote system administration are shown. A final discussion with the perspectives of new research is the main content of Section 6.

2 Background

Table 1 - Glosary of terms	
Acronyms	**Definition**
AWL	Programming language with list of instructions
CERT	Computer Emergency Response Team
CI	Critical Infraestructure
CIPR	Critical Infraestructure Protection Regulation
CPU	Central Processing Unit
CTOI Concept	Components in the Technologiers of Operation in Indus
CVSS	Common Vulnerability Scoring System
FUP	Programming language is a graphical S7
HMI	Human Machine Interface
IAC	Industrial Automation Cells
ICS	Idustrial Control System
ICT	Information and communication technologies
IP	Internet Protocol
ISC	Infraestructure-Strategic-Criticality
IT	Information Technology
KOP	Programming language with outline of contacts
LAN	Local Area Network
LPCI	Law Protection of Critical Infraestructure
LPCI	Law for the Protection of Critical Infrastructures
NCSS	National Cyber Security Strategy
NNIL	National Network of Industrial Laboratories
NSS	National Security Strategy
OPC	OLE for Process Control
OpenVAS	Open Vulnerability Analysis
OS	Operating System
OT	Operational Technology
PARL	Practical Access to Remote Laboratory
PID	Proportional Integral Derivative controller
PLC	Programmable Logic Controller
PROFIBUS	Process Field Bus
PROFINET	Process Field Network
S7	SIEMENS proprietary protocol
SARLAB	Remote Access System to Laboratories
SCADA	Supervisory Control and Data Acquisition,
SCI	Strategic Critical Infraestructure
SIEM	Security Information and Event Management
SIKERCIA	System of Knowledge by Real Experimentation
TCP	Transmission Control Protocol
TIA Portal	Totally Integrated Automation Portal
VPN	Virtual Private Network
WAN	Wide Area Network

Table 2. Glossary of terms

Table 1 (a) - Word Definition	
Words	**Definition**
Adaptability	The quality of being able to adjust to new conditions.
Exposure	The exposure of any weakness (vulnerabilities/misconfigurations) in an organisation's public facing infrastructure that poses the risk of a breach or a compromise is termed as cyber exposure.
Preventive	The quality of being preventive means being designed to prevent something undesirable from happening (in this case, a cyberattack).
Resilience or Cyber resilience	Cyber resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events.
Risk	Is the probability of exposure or loss resulting from a cyber attack or data breach on your organization.
Vulnerability	Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack.

Table 1(a). Word Definitions

As reported in the introduction, this research has been carried out in a very specific area, namely industrial cybersecurity. Specifically, it provides a differentiating value in the field of essential services [19,20]. These essential services are provided by what are currently referred to as Strategic and/or Critical Infrastructures (henceforth, SCI) [21,22,23]. These infrastructures have adopted a relevant position in the management of risks and crises of any country. Therefore, cybersecurity related to SCI is key to the normal functioning of the social order of a country. Although definitions of critical infrastructure vary from country to country, virtually all countries identify the types of infrastructure based on the services they provide [24,25]. Specifically, these are power plants and networks, communications and information technologies, finance, health, food, water, transportation, production, storage and transport of dangerous goods.

In Spain, the Law for the Protection of Critical Infrastructures (LPCI) [26] was enacted and all its points have been implemented in the Critical Infrastructure Protection Regulation (CIPR) [27].

The origin of this national regulation comes from the European Directive, Directive 2008/114 / EC - Identification and designation of 41European critical infrastructures and assessment of the need to improve their protection [28].

In Spain, twelve strategic sectors directly involved in the LPCI have been defined and divided into sub sectors: administration, space, nuclear industry, chemical industry, research facilities, water, energy, health, information and communication technologies, transportation, food, and financial and tax system. In turn, the National Security Strategy (NSS) of 2011 [29,30] lists cyber threats and cyber-attacks among the main risks to national security. An improved NSS was approved in 2013. This upgraded strategy helped to define new strategic scenarios and to involve civil society more actively in

national security. In its fourth chapter, which is dedicated to key action lines, the NSS identifies the cybersecurity as one of the twelve priority work areas. The cybersecurity challenge is equated with traditional threats, such as terrorism. The National Cyber Security Strategy[3] (NCSS) was adopted in December 2013 and it is the fundamental document for cyber security in Spain. As a result of the concerns articulated in the NSS 2013, the NCSS developed a policy framework and executive structure to prompt cybersecurity to the top priorities of the national security.

As noted, and given the relevance of the processes carried out in the industry and more specifically those classified as CI, it is not possible to expose this infrastructure to an experimental process. As an aid to this process transition, the concept of virtual and remote laboratories arises from the area of university research to help in this task. Currently the idea of distance education is firmly and globally established in this field. The staging of different technological advances, with virtualization as its main component, has helped in this consolidation. [31,32,33]

There is a lot of scientific literature on the design and development of remote laboratories in different areas of research and teaching [34]. Remote and virtual laboratories are experimental systems based on a communication architecture where the user and the devices to be controlled (simulated or real) are geographically separated, with ICTs being in charge of allowing those users to access to the experimental equipment [35,36,37,38]. These virtual spaces allow users to perform practices in real time, visualizing the executed actions by means of webcams. These architectures support the development of SIKRECIA, using as a starting point the access to IAC through spatially distributed locations. The aim is to solve the three fundamental aspects of teaching, learning, communications and experimentation [37]. In turn, the model must be applicable to any area of knowledge regardless of the nature of the solution, which used to be the limiting factor. To this end, SARLAB (System Access to Remote Laboratories) [39] is taken as tool for the intercommunication of SIKRECIA. In turn, the complexity of what has been discussed has made its use necessary. SARLAB is an implementation, that is used between local area networks (LAN) and wide area networks (WAN) , in the field of TCP/IP protocols of the system in charge of the management of communications. It controls communications among the data of the connected users and the IAC. At the same time, SARLAB is responsible for managing the concurrency allowed to each

3 Estrategia Nacional de Ciberseguridad, published in 2013 by the government of Spain.
(http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional.

type of programming hardware and for software, granting the capacity for collaborative access.

To complete this system, we will make use of the learning management systems, which are software tools for creating web applications oriented to the administration, documentation, monitoring and reporting of learning programs in the network or digital learning [40,41,42]. While virtual laboratories are based on mathematical models, remote laboratories use real equipment and, therefore, the experiments are actually carried out.

Another technology that complements the learning and as a result adds value to the ability to prevent cybernetic threats in industrial environments are the so-called honeypots [43,44]. This type of computer security tool, although not the object of study of this work, is considered very useful as a possible evolution to be implemented in future development lines of SIKRECIA.

The concept of honeypot technology is over fifteen years old, although the technology applied in a formal way in OT is more modern in terms of service. The Honeynet Project is a leading international non-profit security research organization founded in 1999. The Honeynet Project has contributed to fighting malware, hacking and malicious attacks. In fact, its motto says: "To learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned.” The main tool is the Honeypot system. A honeypot is a tool specially designed to serve as a trap against possible attackers and is very useful in the confluence of IT and OT [45].

The types of classification of honeypots is illustrated in Figure 2., and the types of interaction of honeypots is shown in Table 2. Sometimes, real devices are used as honeypots to save time in the development stage. Honeypots with the characteristics of an IT environment are the most common, but given the increasing number of attacks experienced by industrial control systems, some experts believe it would be useful to incorporate them

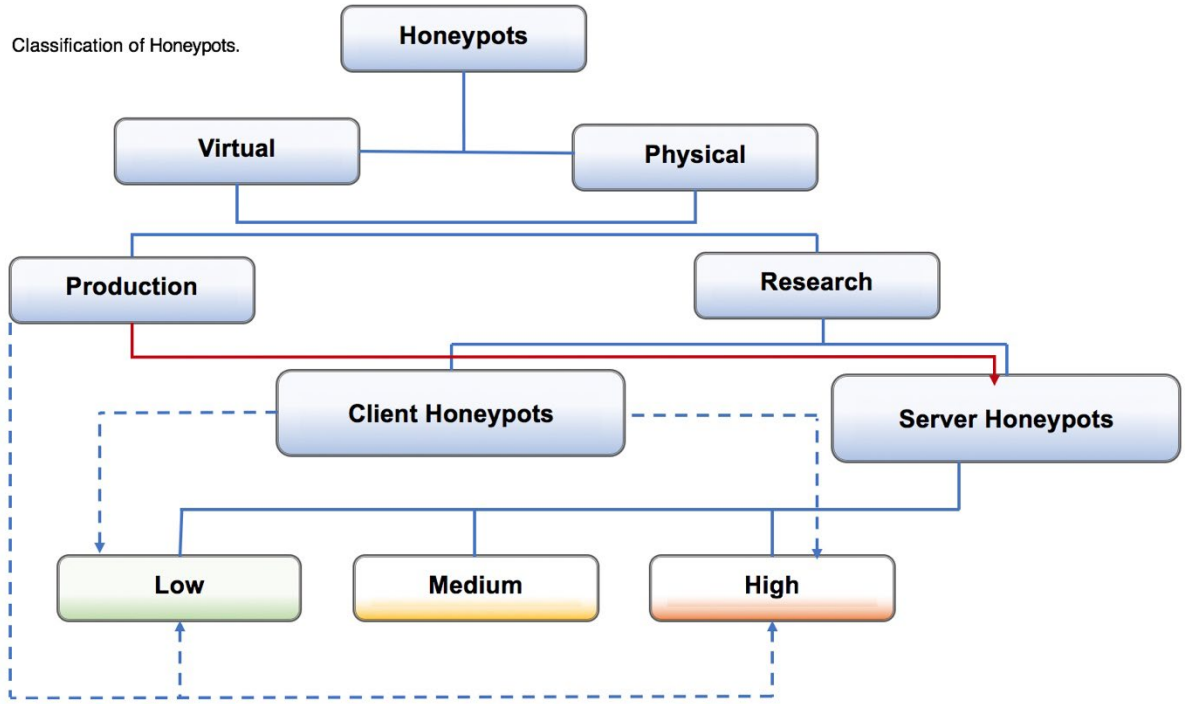


Figure 2. Classification of Honeypots

into these environments to detect attack vectors [46,47]. As already noted, some time ago in countries such as Ukraine, the anticipation and detection of attacks on industrial systems can prevent major problems, such as those caused by Black Energy [48], Stuxnet [49] or PLC Blaster [4] [50].

Table 2- Classification of type interaction of Honeypots		
	High Interaction	Low interaction
Simulation	They simulate real services, applications or devices. Identifying them is usually comlex.	They simulate operating systems or services. Tey are likely to be easily detected as traps.
Threats	Discovering new attacks or abnormal behaviours not detected previously.	Discovering automated tools or vulnerabilities alredy known in specific servies.
Information	They collect large amounts of information of great value because they sometimes contain registrations of unknown attacks. Their implementation	The amount of resources collected is limited. Not recommended if an in-depth analysis of system is required.

Table 3. Classification of type interaction of Honeypots

The cost of a large scale of specific test banks can reach prices completely outside of the reach of 90% of the institutions, research centers and even the developers themselves. In fact, full scale systems are

4 BlackEnergy: Trojan used to attack Ukraine, its objective being to sabotage the control systems of public infrastructures.
Stuxnet: Malware that infected the Natanz nuclear power plant, in Iran, affecting the uranium centrifuges.
PLC Blaster: malware running on a PLC.

extremely unusual and their use is limited to experimentation and controlled research for the remaining 10% of the institutions. Despite significant attention and much progress over the past 15 years, threats continue to evolve about as fast as preventive solutions.

Therefore, and after reviewing the state of the art in cyber security risk assessment of SCADA systems, [51,52] there should be an increase in empirical and theoretical research into the technical aspects of cybersecurity based on the volumes of incidents related to errors in bad configurations, and in order to establish paths in which the current cybersecurity practice can benefit. One of the main goals of modern security solutions would be to develop novel methods that could detect and disrupt the activities of system attackers.

SIKRECIA is critical to increasing resilience capabilities in infrastructure environments. It is important to note that, these environments in industrial control systems belonging to CI, do not have sufficient accessibility to perform, test, behave analysis in the face of system upgrades, or simply stops often programmed, by the nature of the systems, hence the importance of creating a System capable of granting these capabilities in anticipating possible facts. Particular attention should be paid to the implementation of new strategies that can detect, prevent and mitigate attacks.

To help in such task, SIKRECIA provides the advantages of heterogeneity, availability, expansion, and cost reduction, allowing experimentation within controlled environments as well as with real processes.

3 Methodology, Materials and Analysis

The architecture developed as well as the steps carried out to meet with the objectives established in this project has been developed in a modular way and in different stages. As detailed in the description of the objectives of this investigation, it was necessary to consider, from a global point of view, the union of the IT and OT worlds, granting the same operational importance to both.

As a result of the CITO concept, a new way of experimenting in the field of industrial cybersecurity is explored, creating a controlled and highly configurable system for the requirements of the tests to be executed [53,54].

3.1 Architecture

The Fig. 3, shows the environment recreated to provide the capacities to the industrial systems testbed with SIKRECIA. The recreated architecture consists of several subsystems.

The whole system known as SIKRECIA provides, through its different components, a remote and secure access to the production environment. It manages the access through SARLAB to a server of virtual machines that are available to users and can be set up in accordance with the objectives planned to achieve them and simulate them. This provides real access to the various existing industrial automation cells, allowing their management through the use of a human-machine interface. This architecture includes all the CITO components created in this work. It allows the development and evaluation of the different architectures remotely proposed by the user community. It provides access in a controlled and orderly manner to the community that uses the system, while the knowledge generated by the various combinations of instrumentation can be extrapolated to the academic world, as well as to Spanish and European critical infrastructures and manufacturers of industrial devices.

3.1.1 Sub-System SARLAB

SARLAB is a modular and scalable system that constitutes a complete ecosystem of solutions for IoT. It offers a way to easily implement cloud services for managing the configuration and access to sensors, actuators and controllers. The access to any device or equipment managed through SARLAB is Secure, Controlled, Organized and Collaborative (SCOC). An institution using SARLAB provides SCOC access by Internet to any of its physical systems (production lines, pilot plants, laboratory equipment, etc.) These institutions may use a private server for this purpose or establish itself as an IaaS (Infrastructure as a Service) provider [55,56,57]. SARLAB is also responsible for managing the concurrency allowed for each type of access to SIKRECIA, providing it with the capacity of collaborative access.

3.1.2 Server of Virtual Machines

Based on the needs raised by the users of SIKRECIA, the server provides the power to make use of a certain number of virtual machines. It allows the possibility of acting with different OS. The OS are classified into three categories according to the functionality they offer within of SIKRECIA:

1. *Pentesting,*
2. *Production systems,*
3. *Programming systems and acquisition knowledge.*

Within the functionality of pentesting the OS available are: OpenVAS system which facilitates the creation of evaluation scripts and search of vulnerabilities of industrial devices; a Kali Linux, having several network audit tools; and a specific auditing system for industrial environments, SamuraiSTFU. For production systems there are several versions of Windows operating systems (Windows 7, 10), which support a wide range of possibilities related to the operation of systems according to the systems programming of industrial environments (WinCC[5]) as well as the simulation of corporate networks as an integral part of industrial networks in production. It also extends to production systems in DMZ[6], analyzing the possible security failures resulting from OS vulnerabilities, network architectures or PLC programming systems. There is also a SCADA system created with a WinCC flexible V8, which collects the data produced in the industrial network recreated. At the same time, there is an engineering station with the TIAPortal (Totally Integrated Automation Portal) software, whose mission is to provide the capacity of the PLC programs and other instrumentation used in OT.

5 SIMATIC WinCC is a supervisory control and data acquisition (SCADA) and human machine interface (HMI) system from Siemens. SCADA systems are used to monitor and control physical processes involved in industry and infrastructure on a large scale and over long distances.

6 In computer networks, a DMZ (demilitarized zone) is a physical or logical sub network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet.

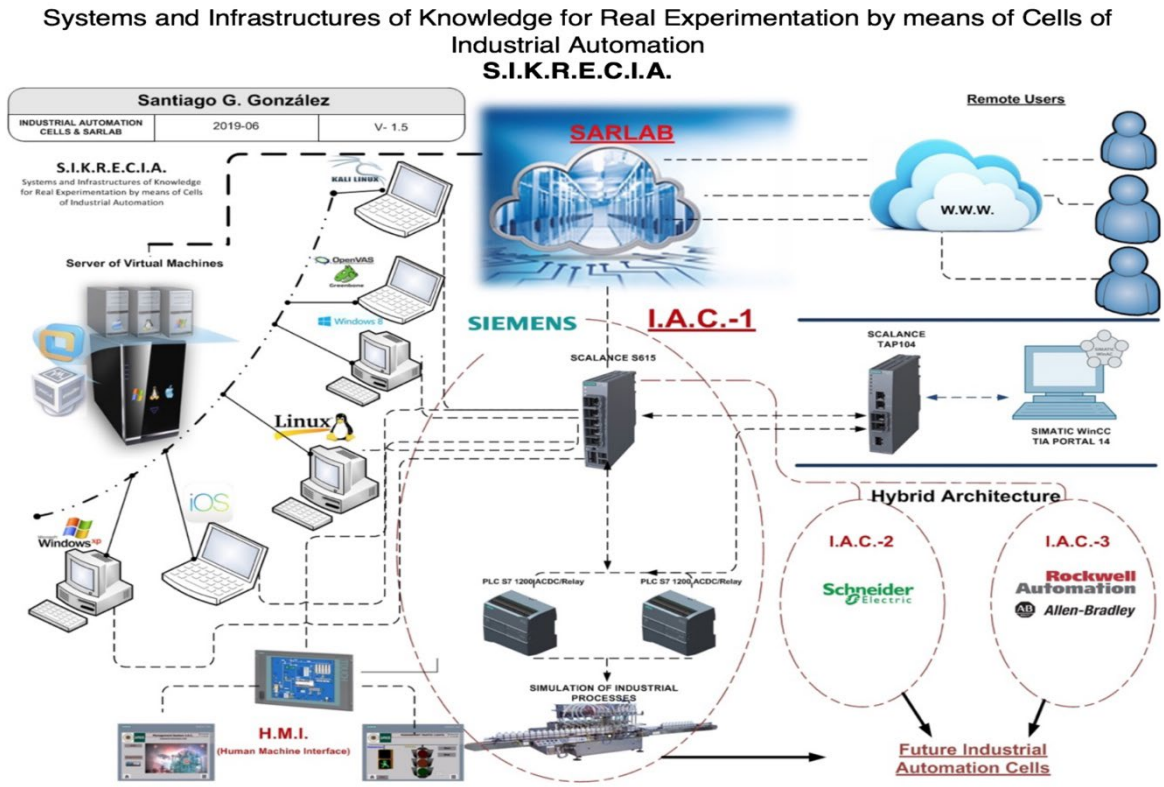


Figure 3. Network scheme and testbed created for Testing Industrial Systems.

3.1.3 IAC Industrial Automation Cells

In the first instance, a unique IAC with SIEMENS element was considered. The components of the IAC 1 (see Figure 3.), and the industrial test bed designed, can be seen in Figure 4. This cell consists of a PLC S7 1200, 1214 AC / DC Relay. This PLC has a built-in trigger plate which is capable of acting directly on the PLC circuitry providing manual access to its digital inputs.

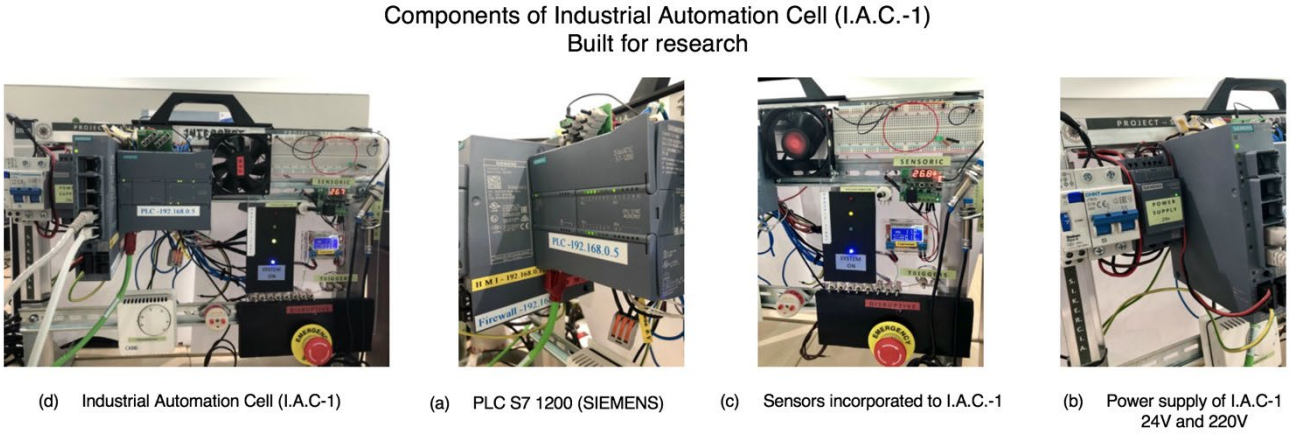


Figure 4. Pictures of testbed, CAI-1 with components PLC, firewall SCALANCE 615 and sensorics elements. (a)PLC S7 1200 1214-ACDCRelay; (b)Power supply of IAC ; (c) Sensors incorporated to IAC; (d) General view of IC

A SCALANCE S615 industrial firewall has been incorporated. The SCALANCE S615 security module has five Ethernet ports that offer protection for various network topologies

via firewall or virtual private network VPN (IPsec and OpenVPN) and enable flexible implementation of security concepts. Users can configure up to four variable security zones with individual firewall rules. With the auto configuration interface, the device can be easily integrated and parameterized with the Sinema Remote Connect (SRC) management platform. This device allows the creation of several VLANs so that in accordance with the permissions granted to the different virtual machines, bidirectional access is allowed between the PLC to HMI, PLC to Programming System with TIA Portal (Totally Integrated Automation Portal), and PLC to SCADA.

3.1.4 HMI (Human-Machine Interface)

In order to carry out remote control of the actions implemented in the programmable automaton of the IAC 1, a HMI has been created through a simulated touch panel and all this has been developed through the TIA Portal. These panels offer the appropriate interface for each application programmed in the PLCs and the OT field. The remote-control panel has several navigation screens, which offers management possibilities. Figure 5. shows pictures of RJ 45 port control systems and associated HMI. In Figure 5.(a), it can be appreciated the user administration or access to the core of the industrial management system.

After the appropriate verification of credentials in the screen previously shown, we can see the possibilities of administration of the processes created in IAC 1(Figure 5.(b)). This image shows the ability to manage the rights of the different types of users allowed to interact with IAC 1. This management user panel, Figure 5. (c), is of vital importance from the point of view of the cybersecurity of the systems, because the core of the industrial functionality can be accessed remotely.

At the same time, a PID controller has been implemented for the management control of processes; it can be tuned manually and automatically with predefined parameters (Figure 5. (e)). Figures 5. (f, g, h) are part of the HMI and show the functionality of the traffic light system implemented.

Different screens of Human Machine Interface for Industrial Automation Cell (I.A.C.-1) Designed for research

Figure 5. Pictures of Human Machine Interface (HMI) connected to CAI-1. The HMI has created several control screens;

(a) Sensoric; (b) Management users; (c) Management System; (d) Principal Screen Human Machine Interface; (e)Integral Derivate Controller PID; (f, g h) Management Traffic Lights.

3.2 Development

The TIA Portal is the innovative engineering system that allows an intuitive and efficient configuration of all planning and production processes. It offers a unified engineering environment for all control, visualization and management tasks. The TIA Portal incorporates the latest versions of the SIMATIC STEP 7, WinCC and Startdrive Engineering Software for the planning, programming and diagnostics of all SIMATIC controllers, display screens and latest generation of SINAMICS drives. The automation cell in turn consists of a sensor panel which provides discrete signals over time provided by metal detection sensors and temperature probes, being interpreted by the PLC and programmed for this purpose in the HMI created in the system. In the same way, a light indicator is created emulating a traffic light whose implementation is recreated with a TIA Portal simulating a continuous process. The signals and times are programmed in the PLC, which in turn is designed so that in the event of a logical or physical disruption of the system (cyberattack or unauthorized physical intrusion); it is reset and continues functioning. These environments have been programmed to perform simulations of direct cyber-attacks to the PLC, trying to violate the industrial firewall, attacking the web server enabled in the PLC or testing the combination of the OS after having made changes in the firmware versions of the industrial automations and updates of the industrial programming machines.

The programming languages supported by the TIA Portal platform, and with which the functionalities of SIEMENS I.A.C have been designed, are FUP, KOP and AWL.[7]

FUP is a graphical Step7 language that uses Boolean algebra blocks to represent logic. It also allows representing complex functions (e.g. mathematical functions) by means of logical tables. It has the advantage of showing the different logics grouped by blocks and having complex blocks.

KOP is a scheme of contacts ladder. It is a Step 7 graphic language and probably the most widespread in all PLC programming languages, and therefore the most similar to others. It is probably the easiest one to understand by people from the electrical industry and electrical technicians. In short, it is the representation that would have to be wired if you wanted to carry out the same program as with the PLC.

AWL is a textual programming machine-oriented language. In a program created in AWL, the instructions are largely equivalent to the steps with which the CPU executes the program. To facilitate programming, AWL has been extended with high level language structures (such as structured access to data and block parameters). It is the most complete and the most visually complex to follow.

4 Level of Contributed Innovation

As we have described in previous sections, this paper shows the work carried out in which an Industrial Automation Cell has been created with different components from the OT world and which is, in turn, part of a System with other testbed capabilities mainly from the IT world, allowing the System to face the cyber-security of the OT, IT to research, for the improvement of cyber-resilience. The System and Infrastructure of Knowledge for Real Experimentation by means of Cells of Industrial Automation (SIKRECIA), described in this work, provides new capabilities for research, development, simulation and testing of the functioning of these systems, and the ability to foresee the behavior of a specific system in industrial production.

7 Programming languages according to IEC standard (International Electro technical Commission)

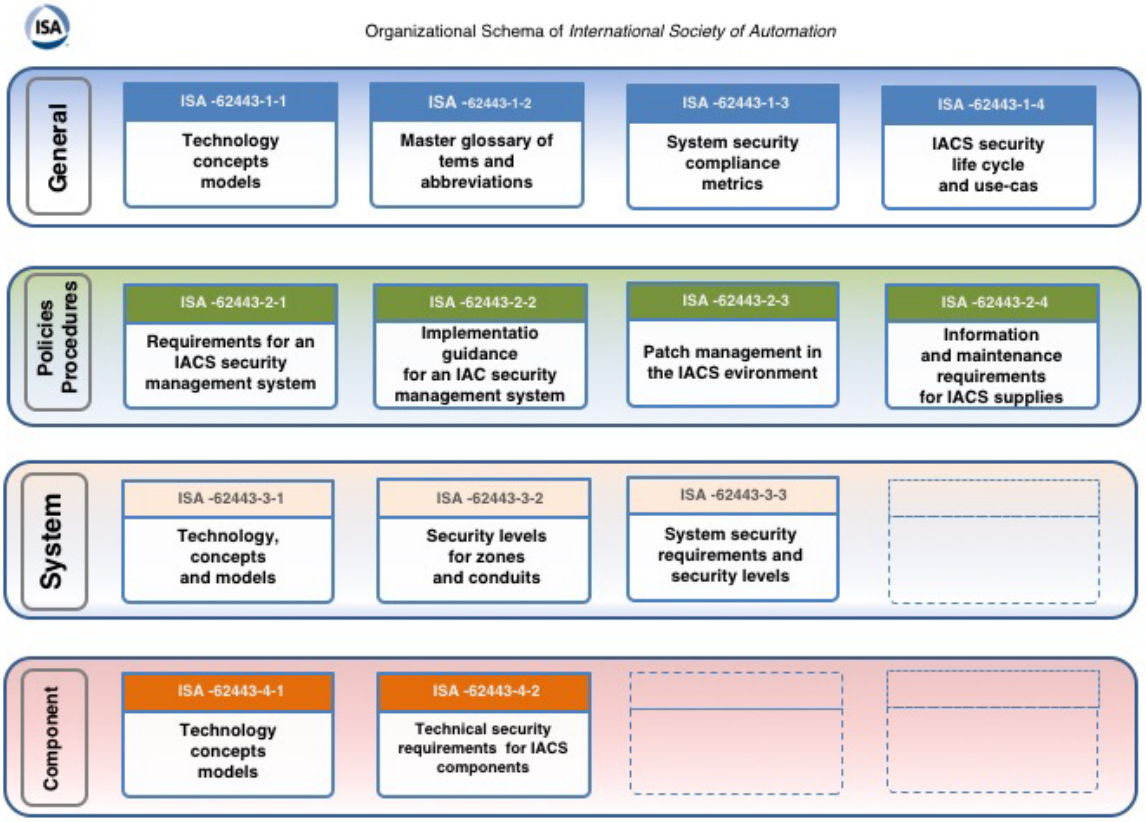


Figure 6. Organizational Schema of International Society of Automation (ISA)

As a point of reference for the analysis and development of this work, the ISA99 / IEC62443 standard has been taken into account (Figure 7). This is the main international frame of reference for application in the cybersecurity of industrial systems, where it is of vital importance in their processes to maintain availability and integrity. These factors have been taken into account fundamentally for the adoption of protection measures against cyber threats, but also to reduce unintentional technological incidents. This is based on IEC 62443 and specifically on the sections detailed in Figure 7.

The work presented here represents an advance in the field of ICSS risk analysis. The IT and OT elements that support an ICSS architecture are now incorporated in a safe and real way. The real-world combination of these software and hardware components would be impossible to simulate through the classic concept of a virtual remote access laboratory, as discussed in the introduction.

Thus, a step forward has been taken in the correct treatment of two very different areas, which require the convergence of industrial control and information technologies. Until now, these two technologies had followed parallel paths, as the industrial and technological advances had dictated.

The paper introduces a new concept that enriches the level of maturity in cybersecurity that can be considered an in-depth defense, namely, "knowledge through real experimentation" [56,57]. This new concept contains insights that differentiate it from those traditionally assumed through the use of remote access and/or virtual laboratories.
True remote access laboratories are not always available for the needs that can arise. This fact is obvious and difficult to resolve, since there are no platforms that facilitate all these possibilities of architectures deployed in the world of industrial production.

The ability to load these configurations in SIKRECIA through the server of the virtual machine allows infinite functional combinations without having to look for similar configurations in remote laboratories with virtual or real access that have implemented it specifically, which changes the static concept of the architectures from another test bed.
In this way, it helps to dismiss the fear surrounding the industry's operating systems in relation to their suitability in the field of cybersecurity. Also, it offers the possibility of experimenting in a controlled environment on complex devices given their functionality, providing answers to questions such as:

- What would happen if the operating system were updated from the operating environment?
- How much time is available to make a scheduled stop to download security updates? Will everything remain the same?
- Is an emergency update possible in industrial systems in production?
- Are you really aware of the potential threats to your industrial control systems?

4.1 Transferability

As reported in previous sections, SIKRECIA is critical to increasing resilience in infrastructure environments. It is important to note that, these environments in the industrial control systems belonging to CI, do not have sufficient accessibility to perform, test, behave analysis before system upgrades. These characteristics are directly related by the levels of criticality of their actions, hence the importance of creating a system capable of providing these capabilities in anticipation of possible events. Similarly, the European Community, in its directive "Introduction to the Certification Framework for Cybersecurity Components (ICCF)" [4] , published by the Joint Research Centre (JRC), the European Commission's science and knowledge service, proposes a certification system to increase cyber-resilience in CIs. As a consequence, it would be appropriate to take into account SIKRECIA as an element to be

included like a testbed in the existing critical systems in the 12 Strategic Sectors defined by the Spanish Law [26,27].

5 Results

The results obtained for the cohesion and design capabilities of specific environments met the established expectations and the objectives pursued in this work.

Several tasks have been developed through the programming software of SIEMENS TIA Portal, This Engineering Software, used to program several families of controllers of SIEMENS, promotes a perfect integration of TIA Portal, as an engineering tool that “increases the availability of applications and plants up to 99%, and at the same time leads to savings in maintenance costs of up to 15%”.[58].

The tasks implemented by the TIA Portal are:

- **Simulation of repetitive and continuous processes** represented by a traffic light control system of vehicles and pedestrians. We decided to program this type of simulation, because of the importance and concern that currently has the control of signals for the improvement of resilience in the transport sector, sector that has the rating of critic [59,60,61,]
- **Simulation of discrete processes**. Data obtained by temperature and proximity sensors.
- **Simulation of a PID control**. It allows to control the flow of a liquid tank. In this case, the PLC CPU is used.
- **Management of the security** of the own automaton, its web server and program modules. This action shows the first step of the defense line of the industrial system, a key process.
- **Development of an HMI** which provides the necessary interface for transmitting locally and remotely the operating orders from the different actors of the system. This directly addresses network connectivity (LAN, WAN, etc.)

Before its physical construction, the IAC 1 was built in a virtual way through the TIA Portal v13 (today migrated to v15.1), although it has been upgraded to higher versions depending on the network electronics and versions incorporated in the project.

Table 6 - Glosary of terms, metrics value and parameters.	
Metric Value	**Parameters**
Attack Vector (AV)	Network(N), Adjacent (A), Local(L),Physical (P)
Attack Complexity (AC)	Low (L), High (H),
Privileges Required (PR)	None (N), Low (L), High (H)
User Interaction (UI)	None (N), Required (R.)
Scope (SC)	Unchanged (U), Changed (C.)
Confidentiality Impact (CI)	High (H), Low (L), None (N)
Integrity Impact (II)	High (H), Low (L), None (N)
Availability Impact (AI)	High (H), Low (L), None (N)
Exploit Code Maturity (ECM)	Not Defined (X), High (H), Functional (F), Proof-of-Concept (P), Unproven (U)
Remediation Level (RL)	Not Defined (X), Unavailable (U), Workaround (W), Temporary Fix (T), Official Fix (O)
Report Confidence (RC)	Not Defined (X), Confirmed (C.), Reasonable (R.), Unknown (U)
Security Requirements	Not Defined (X), High (H), Medium (M), Low (L)

Table 6. Glossary of terms, metrics, values an parameters used in CVSS

The starting scheme of the SIKRECIA architecture is endowed with several differentiated components that provide a high degree of independence and cohesion with other entities (remote laboratories, research centers, incorporation of new industrial automation cells from other manufacturers, etc.).

5.1 Common Vulnerability Scoring System V3.0 (CVSS) as a tool for improving cyber resilience.

The Common Vulnerability Scoring System (CVSS), is an open framework for communicating the characteristics and severity of software and hardware vulnerabilities [62,63].

To complete the tools and to improve the resilience in SIKRECIA, after a detailed literature review of the most relevant ICT infrastructure and cybersecurity collection tools, we have deployed a system with OpenVAS in our study. The OpenVAS scanner shows the results of the vulnerabilities and highlights them according to the impact on the systems (low, medium or high) indicating the number of vulnerabilities found in each category. OpenVAS is an official OVAL Adopter and it is registered as a Systems Characteristics Producer. In order to quantify the risk of the systems deployed in SIKRECIA by the different users, the CVSS was applied (see Table 6. to understand de terms used in CVSS). Throughout this paper the following metrics are used:

- **Vulnerability:** Corresponds to a weakness or failure of an information system. This failure puts security at risk, allowing the commitment of integrity, availability or confidentiality. It is necessary to find and eliminate them as soon as possible. The elapsed time from when they are discovered until these failures are solved is called the "exposure time".

- **Threat:** It is an action that takes advantage of a vulnerability attacking an information system. Therefore, vulnerabilities are the conditions and characteristics that make a system susceptible to threats.
- **Risk:** The risk is the likelihood of a security incident. That is, the materialization of a threat, causing damage or loss.

Being able to detect software, hardware and firmware vulnerabilities in industrial control system environments is paramount since this risk is critical for any organization that operates an IOT system. The identification of these risks can be difficult, as well as their categorization and mitigation. The CVSS provides a way to discover the main vulnerability characteristics , providing a quantitative and qualitative classification (critical, high, medium and low) that reflects their severity.

In summary, the CVSS provides three important benefits:

1. Provides standardized vulnerability ratings. When an organization uses a common algorithm to rate vulnerabilities on all IT platforms, it can take advantage of a single vulnerability management policy that defines the maximum time allowed to validate and remedy a given vulnerability.
2. Provides an open frame of reference. Users may get confused when a vulnerability is assigned an arbitrary score by a third party. With CVSS, the individual characteristics used to obtain a score are transparent.
3. CVSS allows prioritizing risks. When the environmental score is computed, the vulnerability becomes contextual for each organization, and helps to provide a better understanding of the risk posed by this vulnerability to the organization [62,64]

CVSS has three types of metrics groups to evaluate the risks: Base, Temporal and Environmental (see Figure 6.):

- Base represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time,
- Temporal represents the characteristics of a vulnerability that change over the time but not among user environments and,

- Environmental represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

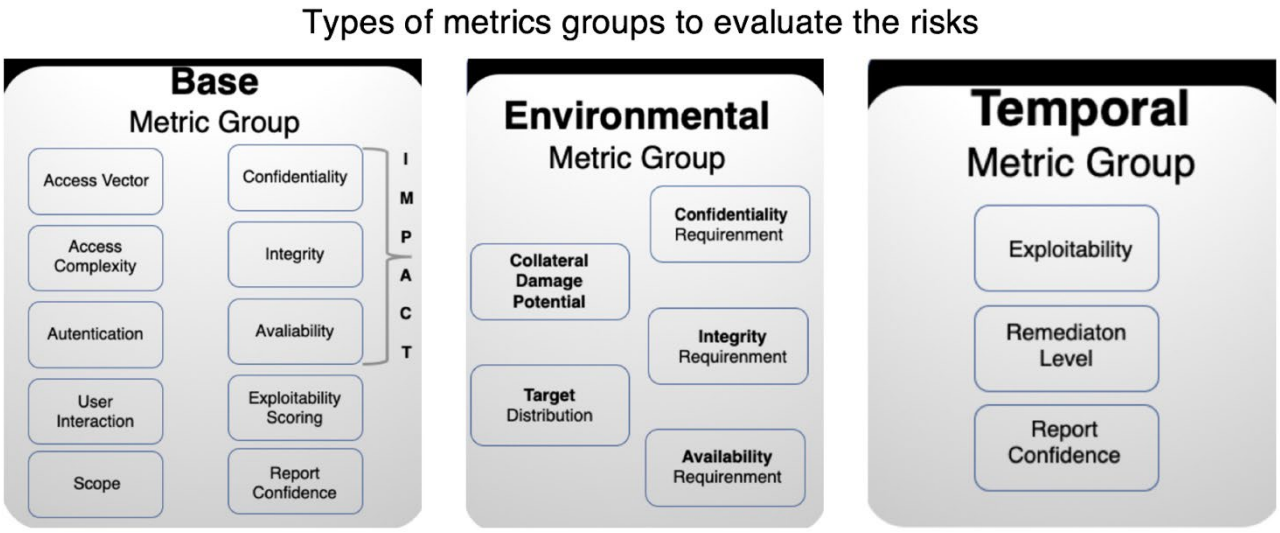


Figure 7. Metrics groups to evaluate the risks; Base, Temporal and Environmental

The interrelation and subsequent mathematical analysis of the data offered by these three metrics result in an operating system score.

The purpose of this cataloguing is to define and specify the fundamental characteristics of a vulnerability. This provides users with a clear and intuitive representation of vulnerability and a common taxonomy for the description. The users may or may not invoke the temporal and environmental groups, thus providing contextual information that more accurately reflects the risk to the environment under consideration.

When the metrics catalogued and defined in the previous paragraph contain values, the base equation calculates a score in a range from 0 to 10 and creates a vector, as shown in Table 3. The vector, which is a string of text that contains the values assigned to each metric, facilitates the "open" nature of the framework. It is used to communicate exactly how the score is derived for each vulnerability, so that anyone can understand how the score was obtained and, if desired, confirm the validity of each metric. Therefore, the vector must always be shown with the vulnerability score. The values of these vectors are shown in Table 4.

Table 3 - Examples of vectors associated with the metric groups.	
Metric Group	**Vector**
Base	AV: [L,A,N,P]/AC: [H,M,L]/Au: [M,S,N]/C: [N,P,C]/I: [N,P,C]/A: [N,P,C]
Temporal	E: [U,POC,F,H,ND]/RL: [OF,TF,W,U,ND]/RC: [UC,UR,C,ND]
Envorimental	CDP: [N,L,LM,MH,H,ND]/TD: [N,L,M,H,ND]/CR: [L,M,H,ND]/ IR: [L,M,H,ND]/AR: [L,M,H,ND]

Table 4. Examples of vectors associated with the metric groups

Table 4 - Rating of the characteristics and impact of IT vulnerabilities (metrics value and numerical value)		
Metric	**Metric Value**	**Numerical Value**
Attack Vector / Modified Attack Vector	Network	0.85
	Adjacent Network	0.62
	Local	0.55
	Physical	0.2
Attack Vector / Modified Attack Vector	Low	0.77
	High	0.44
Privilege Required / Modified Privilege Required	None	0.85
	Low	0.62 (0.68 if Scope / Modified Scope is Changed)
	High	0.27 (0.50 if Scope / Modified Scope is Changed)
User Interaction / Modified User Interaction	None	0.85
	Required	0.62
Confidentiality, Integrity, Availability Impact / Modified Imp	High	0.56
	Low	0.22
	None	0
Exploit Code Maturity	Not Defined	1
	High	1
	Functional	0.97
	Proof of Concept	0.94
	Unproven	0.91
Remediation Level	Not Defined	1
	Unavailable	1
	Workaround	0.97
	Temporary Fix	0.96
	Official Fix	0.95
Report Confidence	Not Defined	1
	Confirmed	1
	Reasonable	0.96
	Unknown	0.92
Security Requirements – Confidentiality, Integrity, Availabi	Not Defined	1
	High	1.5
	Medium	1
	Low	0.5

Table 5. Rating of the characteristics and impact of IT vulnerabilities (metrics value and numerical value)

Each metric in the vector consists of the abbreviated metric name, followed by a ":" (colon), then the abbreviated metric value. The vector lists these metrics in a predetermined order, using the "/" (slash) character to separate the metrics. If a temporal or environmental metric is not used, it is given a value of "ND" (not defined).

Applying the parameters and values of the concrete metrics of the standard C [65], allows obtaining a specific numerical value according to the scale of values specified in the Table 5.

The intervening parameters for obtaining the rating of the characteristics and impact of IT vulnerabilities correspond to those detailed in Table 4. The value of the metric must be chosen according to the intrinsic characteristics of each OT system to examine. This implies that not all variables must necessarily appear.

5.2 *Equations*

To perform the calculations described in previous sections, three equations are used.[66]

- Base Equation: the equations that define and compose the so-called base equation are shown in Table 7.

Table 7 - Definition of Base Equation
Definition of Base Sco
If (Impact sub score < = 0 else, 0) Scope Unchanged Roundup (Minimum [(Impact+Exploitability),10]) Scope Changed Roundup (Minimum[1.08×(Impact+Exploitability),10])
Impact sub score (ISC
Scope Unchanged 6.42×ISCBase Scope Changed 7.52× [ISCBase−0.029] −3.25× [ISCBase−0.02]15 Where, ISCBase=1−[(1−ImpactConf) × (1−ImpactInteg) × (1−ImpactAvail)] Scope Unchanged Roundup (Minimum [(Impact+Exploitability),10]) Scope Changed Roundup (Minimum[1.08×(Impact+Exploitability),10])
Exploitability sub scor
8.22 × AttackVector x AttackComplexity × PrivilegeRequired × UserInteraction

Table 7. Definition of Base Equation

Table 8 - Definition of Temporal Equation
Temporal Score
Roundup (BaseScore × ExploitCodeMaturity × RemediationLevel × ReportConfidence)

Table 8. Definition of Temporal Equation

Table 9 - Definition of Environmental Equation
Definition of Environmental Score
If (Modified Impact 0 else, Sub score <= 0 If Modified Scope is Unchanged Roundup (Roundup (Minimum [× (M.Impact + M.Exploitability),10]) × Exploit Code Maturity × Remediation Level × Report Confidence) If Modified Scope is Changed Roundup (Roundup (Minimum [1.08 × (M.Impact + Exploitability),10]) × Exploit Code Maturity × Remediation Level × Report Confidence)
The modified Impact sub score
If Modified Scope is Unchanged 6.42×[ISCModified] If Modified Scope is Changed 7.52 ×[ISCModified−0.029]-3.25×[ISCModified−0.02]15 Where, ISCModified = Minimum [[1−(1−M.IConf × CR)×(1−M.IInteg × IR)×(1−M.IAvail × AR)],0.915]
The Modified Exploitability sub score
8.22 × M.AttackVector × M.AttackComplexity × M.PrivilegeRequired × M.UserInteraction

Table 9. Definition of Environmental Equation

Temporal Equation: the complete definition of this equation is shown in Table 8.

- Environmental Equation: the complete composition corresponding to the environmental equation is defined by three components:
- Definition of environmental score
- The modified impact sub score
- The modified exploitability sub score.

The metrics value and parameters are defined in Table 9.

5.3 *Case Study and Analysis*

The main objective of this research paper presented, is to provide a conceptual and practical model of how cybersecurity of information technology should be incorporated in the world of operation and research, facilitating experimentation in such industrial environments. complex, being able to anticipate a problem that would directly impact the infrastructure to be evaluated. This prior examination capacity, will grant a very high capacity for prior identification of the vulnerability in the deployed system, and consequently, the ability to solve it. Below is a specific case study that has been raised in the laboratory where SIKRECIA is implemented using CVSS metrics. In this case study, a real and specific vulnerability corresponding to the SIEMENS SIMATIC S7 1200 PLC has been considered as a reference. The objective of the use of this vulnerability (documented and analyzed) corresponds to a case adapted from it. In this case of SIKRECIA study, after using the result obtained through

the CVSS metrics, it should be taken into account that the parameters of the study carried out have been adapted to a case produced for verification in the SIKRECIA system, not being the objective the analysis of a vulnerability, if not its use as a practical example.
This vulnerability has been previously reported and published in:

- **CVE 2016, 2846** (Common Vulnerabilities and Exposures) [67].
- **Advisory (ICSA 16 075 01),** industrial control system, US CERT, Department of Homeland Security [68].
- **SSA 833048**, SIEMENS security advisory by SIEMENS Product CERT [69]. SIEMENS is aware of the protection mechanism failure vulnerability in old firmware versions of SIMATIC S7 1200. Currently, SIEMENS provides the SIMATIC S7 1200 CPU product, V4.0 or later to mitigate this vulnerability and recommends maintaining the firmware up to date. This vulnerability could be exploited remotely.
- SIMATIC S7 1200 CPU family: all firmware versions prior to V4.0.

As a general security measure, SIEMENS strongly recommends protecting network access to the web interface of the S7 1200 CPU with the appropriate mechanisms. At the same time, it can be configured in accordance with the manufacturer's operating rules in order to run the devices in a protected IT environment.
The results obtained from the analysis are:

- Impact scores: 9.8
- Base score: 7.35
- Overall score: 8.575 (High)

Base vector: **(AV:N/AC:L/Au:N/UI:N/S:CC:P/I:P/A:N/E:POC/RL:OF/RC:C)**

The score obtained corresponds to the arithmetic mean between the values contributed by the impact and the base values. This vulnerability corresponds to a rating of 8.75, and in accordance with the criticality scale of CVSS Score (Table 5) is **high.**

According to this example (see operational calculations in Tables 10, 11 and 12) and taking the base vector as an initial vector , the parts that have been taken into account for the exercise are:

- The first parameter, the attack vector (AV), that is, the origin of the access, occurs throughout the network; a vulnerability exploitable with network access means that the vulnerable software is bound to the network stack and the attacker does not require local network access or local access. Such vulnerability is often termed “remotely exploitable”.

- The complexity of access (AC) has been considered low. Specialized access conditions or extenuating circumstances do not exist.
- The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted.

Table 10. Base-Exploitability-Environmental equations.		
BASE METRIC	**EVALUATION**	**SCORE**
Access Vector	[Network]	(0.85)
Access Complexity	[Low]	(0.77)
Authentication	[None]	(0.85)
User Interaction	[None]	(0.85)
Scope	[Changed]	-------
Confidentiality Impact	[Partial]	(0.34)
Integrity Impact	[Partial]	(0.34)
Availability Impact	[None]	(0.00)
Exploitability Scoring	[POC]	(0.94)
Remediation Level	[Official Fix]	(0.95)
Report Confidence	[Confirmed]	(1.00)

Table 10. Base Exploitability Environmental equations (Base Metric)

Table 11. Base-Exploitability-Environmental equations.	
FORMULA BASE	**SCORE**
Impact 10.41 x (1-(1-ConfImpact) x (1- IntegrImpact	== 5.80
BaseScore (((0.6 x Impact) + (0.4 x Exploitability) - 1.5) x f (impact)	== 7.04
F (impact)	== 1.17
ISCBase = 1- [(1-0.34) x (1-0.34) x (1-0)]	== 0.56
Impact Sub Score= 7.52 x [ISCBase – 0.029] -3.25 x [ISCBase – 0.02]15	== 0.74
Exploitability = 20 x [(Access Vector) x (Access Complexity) x (Authentication)]	== 10.0
Exploitability Sub Score = 8.22 x AccesVector x AccessCplex x UserInteract	== 4.57

Table 11. Base-Exploitability Environmental equations (Formula Base)

Table 12. Base-Exploitability-Environmental equations.		
TEMPORAL METRIC	**ENVALUATION**	**SCORE**
Exploitability	= 10.41 x (1-(1-0.66 x 1) x (1-0.66 x 1) x (1-0.0 x 0.5))	== 9.80
AdjustedBase	= ((0.6 x 9.8)+(0.4 x 0.94)–1.5) x 1.176	== 7.35
AdjustedTemporal	= (7.35 x 0.9 x 0.87 x 1.0)	== 5.75
EnviroScore	= round ((5.75 + (10-5.75) x 0.5) x 0.25)	== (0.0 - 2.0)

Table 12. Base-Exploitability Environmental equations (Temporal Metric)

- The attack can be performed manually and requires little skill or additional information gathering. It lacks authentication level because it is not required to access the exploitability of the vulnerability.
- The exploited vulnerability can affect resources beyond the authorization privileges provided by the vulnerable component. In fact, this capacity would be materialized in the administration of HMI's connected to the PLC, the vulnerable component and the implicated component being different, the cataloguing of the level of confidentiality involved has been considered partial because there is considerable informative disclosure.
- Access to some system files is possible, but the attacker has no control over what is obtained, or the extent of the loss is restricted.

The evaluation of exploitability is considered simply as a proof of concept, since the attack does not work in all situations and may require substantial modifications by an expert attacker.

- The vendor solution completely mitigates the vulnerability and is available, drastically reducing the exposure time. The manufacturer has issued an official patch and an update is available.
- The last parameter to be considered within the vector is the metric corresponding to the credibility between what is considered as the vulnerability itself and the credibility of it having been recognized by the PLC manufacturer.

  Tables 10, 11 and 12 show the mathematical calculations made for the resolution of the case study taken as example and in accordance with the base vector previously discussed.

6 Conclusions and Future Works

The development of a new concept of simulation of processes in industrial environments through learning by real experimentation has been presented in this work, taking advantage of the advances in the IT world. At present, with the increase of the presence of IT in the area of industrial control, industrial systems are exposed to a large number of new cyber threats. In view of the important role played by these infrastructures and essential services for the normal development and coexistence of society, we must consider that current and future lines of cyber-attacks will result from attempts to violate these infrastructures [70]. We must discard the idea that "security through ignorance" is a valid method for protection against these types of attacks. For this reason, it is very important to be prepared for possible eventualities through "practice and testing" [71], thus obtaining a high degree of resilience [72,73] and, at the same time, a high level of maturity in view of the new vectors that will give access to cyber-attacks in industrial control systems. The best defense against these new challenges is training. In turn, the implementation of theoretical knowledge without the risk involved in putting into practice these analyses in production plants favors experimentation and broadening the views.

These practical capacities are granted by the SIKRECIA system, since it allows us to choose how to design the real environment to be simulated, including each one of the components involved in the control systems:

- Operating systems (on the side of the control and administration network).
- Specific programming software for industrial components (PLC, network electronics, SCADA system).

- Connection to the Industrial Automation Cell (IAC 1) available.
- Network traffic analysis system.
- Vulnerability monitoring and analysis tools (open source vulnerability analysis OpenVAS[8]).

The true versatility of the system is granted by the high adaptability for the incorporation of as many IAC as there are existing manufacturers of industrial control systems and automatisms. In turn, providing all the software involved in these networks allows for increased quality in the vulnerability analysis. Consequently, the main contribution of this research, materialized in SIKRECIA, is the provision of a secure framework that will help us to obtain analyses that demonstrate the true state of maturity of an industrial architecture that users will deploy according to their research needs.

Future lines of research are to incorporate new IAC from different manufacturers as well as connections to more complex and heterogeneous organizations, such as the National Network of Industrial Laboratories (NNIL[9]) and others existing in other universities. Likewise, it is considered of great importance to incorporate CAT (Cyber Attack Taxonomy) [74] as a model of analysis and representation of cyberattacks to be recreated by SIKRECIA. The strategic model of CAT will assist in the simplification of the understanding and design of the cyberattacks, will standardize the interpretation of the way the actors operate, will allow to faithfully reproduce the actions carried out by the attackers, and will throw out solutions such as countermeasures. Thus, its functionality fits perfectly with the fundamental basis for the creation of SIKRECIA, which is to recreate and verify the systems in ICS leaving duly documented each and every phase of layer seven of the Model Detection Maturity Level (DML) [75], in line with the recommendations of the European Commission and following the guidelines set out in the introduction to this article, IACS Components Cybersecurity Certification Framework.

8 OpenVAS is an Open Source vulnerability scanner, which provides several services and tools, providing a comprehensive and powerful solution for vulnerability analysis and management.
9 The National Network of Industrial Laboratories (NNIL) is an information search platform for industrial laboratories with the capacity to experiment and research solutions that increase the security levels of national industrial infrastructures.

7 Bibliography & References

1. A. Cendoya, National Cyber Security Organization: Spain. CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence Tallinn (Estonia), 2016.
2. Resilience team, ENISA (European Union Agency for Network and Information Security), Communication network dependencies for ICSS/SCADA Systems, 2016.
3. Resilience team, ENISA (European Union Agency for Network and Information Security), Cyber Insurance: Recent Advances, Good Practices and Challenges, 2016.
4. European Commission, Introduction to the European IACS Components Cybersecurity Certification Framework (ICCF), Feasibility study and initial recommendations for the European Commission and professional users, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC102550/jrc102550.pdf , 2016.
5. M. Marcos, U. Gangoiti, D. Orive, E. Estévez, S. Calvo, J. Barandiarán, Design and Validation of Industrial Distributed Control System,, 43rd IEEE Conference on Decision and Control, decembre 14-17, 2004.
6. A. Wortmann, O. Barais, B. Combemale, M. Wimmer, Modeling languages in Industry 4.0: an extended systematic mapping study, DOI, https://doi.org/10.1007/s10270-019-00757-6, 2019.
7. SINEMA REMOTE CONNECT (https://w3.siemens.com/mcms/industrial-communication/es/industrial-remote-communication/remote-networks/pages/sinema-remote-connect-access-service.aspx), 2020.
8. MathWorks, Simulation and model based design, (https://es.mathworks.com/products/simulink.html), 2020.
9. C. Sarno, A. Garofalo, I. Matteucci, M. Vallini, A novel security information and event management system for enhancing cyber security in a hydroelectric dam, International Journal of Critical Infrastructure Protection 13, 2016.
10. R. James, Damon Frezza, Burhan Necioglu, L. Michael Cohen, Kebbeth Hoffman, Kristine Rosfjord, Interdependent Critical Infrastructure Model (ICIM): An agent-based model of power and water infrastructure, 2019.
11. R. Setola, V. Rosato, E. Kyriakides, E. Rome, Managing the Complexity of Critical Infrastructures a Modelling and Simulation Approach, Studies in Systems, Decision and Control, Volume 90, 2016.

12. M. Abdelghafar, Elhady ,M. Hazem, El-bakry, Ahmed Abou Elfetouh, Comprehensive Risk Identification Model for SCADA HindawiSecurity and Communication NetworksVolume 2019, Article ID 3914283, 24 pageshttps://doi.org/10.1155/2019/3914283, 2019.
13. D. Upadhyay, S. Sampalli, SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations, Computer and Security Journal,DOI https://doi.org/10.1016/j.cose.2019.101666, 2020.
14. Resilience Team, ENISA (European Union Agency for Network and Information Security), Communication network dependencies for ICSS/SCADA Systems, 2016.
15. Resilience team, ENISA (European Union Agency for Network and Information Security), Cyber Insurance: Recent Advances, Good Practices and Challenges, 2016.
16. R. Setola, V. Rosato, E. Kyriakides, Managing the Complexity of Critical Infrastructures, a Modelling and Simulation Approach, Studies in Systems, Decision and Control Volume 90 2016.
17. R. Neil, N. Thuy, K. Marian, R. Zaky, H. Dhae, Creating Convincing Industrial-Control-System Honeypots, http://hdl.handle.net/10125/63967, 2020.
18. E.J. Oughton, D. Ralp, R. Pant, E.Leverett, J. Copic, S.Thacker, R. Dada, S. Ruffle, M. Tuveson, J. W. Hall, Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks, DOI; https://doi.org/10.1111/risa.13291, 2019
19. S. Anna, Secure Infrastructure & Services Unit, ENISA (European Union Agency for Network and Information Security), Stocktaking, Analysis and Recommendations on the Protection of CIIs, 2016.
20. S. Wang, an analytical model for benchmarking the development of national infrastructure items against those in similar countries, International Journal of Critical Infrastructure Protection 13, 2016.
21. European Commission, Green Paper on a European Program for Critical Infrastructure Protection, com (2005) 0576 final, Brussels, Belgium, 2005.
22. Council Directive 2008/114/EC of 8 december 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008.
23. Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016.

24. Directive 2008/114/EC — Identification and Designation of European Critical Infrastructures and assessment of the need to improve their protection, 2008.
25. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016- 2019.
26. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas, BOE núm. 102, 2011.
27. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas, BOE núm. 120, 2011.
28 Critical Infrastructures and assessment of the need to improve their protection, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0013&from=EN, 2016.
29. Real Decreto 385/2013, de 31 de mayo, de modificación del Real Decreto 1886/2011, de 30 de diciembre, por el que se establecen las Comisiones Delegadas del Gobierno, BOE núm. 131, 2013.
30. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, BOE núm. 25, 2010.
31. S. Dormido, Control learning: present and future, Annual Reviews in Control, Vol 28 (1), pp. 115 136, 2004.
32. J. Sánchez, F. Morilla, S. Dormido, J. Aranda, P. Ruipérez, “Virtual and remote control lab using Java: A qualitative approach” IEEE Control System Magazine (ISSN: 0272 1708), vol. 22, no. 2, 2002, pp. 8 20. DOI: 10.1109/37.993309.
33. M. Zhang, Y. Li, Students’ Continuance Intention to Experience Virtual and Remote Labs in Engineering and Scientific Education, International Journal Emerging Technologies in Learning, 2019.
34. J. Chacón, H. Vargas, G. Farias, J. Sánchez, S. Dormido, JJS, JIL Server, and LabVIEW: An Architecture for Rapid Development of Remote labs, IEEE Transactions on learning Technologies, Vol. 8, No. 4, 2015.
35. F. Cerezo, F. Sastrón, Laboratorios Virtuales y Docencia de la Automática en la Formación Tecnológica de Base de Alumnos Preuniversitarios, Revista Iberoamericana de Automática e Informática industrial 12 (2015) 419 431, 2015.
36. C. J. Del Canto, M. A. Prada, J. J. Fuertes, S. Alonso, M. Domínguez, Remote Laboratory for Cybersecurity of Industrial Control System, IFAC PapersOnLine 48,29 (2015) 013 018, 2015.

37. L. de la Torre, J. Sánchez, S. Dormido, what remote labs can do for you? Physics today, 2016.
38. J. Saenz, L. de la Torre, J. Chacón, S. Dormido, A new architecture for the design of virtual/remote labs: The coupled drives system as a case of study, 2019.
39. M.A. Márquez Sánchez, Un modelo general de referencia para el acceso remoto a laboratorios docentes y de investigación, Universidad de Huelva, Departamento de Ingeniería Electrónica, de Sistemas Informáticos y Automática, 2015.
40. L. de la Torre, J. Sánchez, T. Andrade, M.T. Restivo, Easy Creation and Deployment of JavaScript Remote Labs with EjsS and Moodle, International Journal of Engineering Education, Vol. 27 No.3, pp. 528 534, 2011.
41. L. de la Torre, T. Faustino Andrade, P. Sousa, J. Sanchez, M.T. Restivo, Assisted Creation and Deployment of JavaScript Remote Experiments, International Journal of online Engineering, 2016.
42. F. Esquembre, F.J. García Clemente, R. Chicón, L. Wee, L. Leong Tze Kwang, D. Tan, Easy Java/JavaScript Simulations as a tool for Learning Analytics, Cornell University, 2019.
43. N. Dutta, N. Jadav, N. Dutiya, D. Joshi, Using Honeypots for ICS Threats Evaluation, Part of the Studies in Systems, Decision and Control book series (SSDC, volume 255) Octo-2019.
44. The Honeynet Project. 2001. Know Your Enemy. Addison Wesley: Boston, MA. (https://www.honeynet.org/about).
45. M. Winn, M. Rice, S. Dunlap, J. Lopez, B. Mullins, Constructing cost effective and targetable industrial control system honeypots for production networks, International Journal of Critical Infrastructure Protection 10, 2015.
46. N. Kambow, L. Kaur Passi, Honeypots: The Need of Network Security, International Journal of Computer Science and Information Technologies, 2014.
47. M. L. Bringer, C.A. Chelmecki, H. Fujinoki, A Survey: Recent Advances and Future Trends in Honeypot Research, I.J. Computer Network and Information Security, 2012.
48. ICS Cert USA, Homeland Security, Alert (IR ALERT H 16 056 01) Cyber Attack Against Ukrainian Critical Infrastructure (BlackEnergy), 2016.
49. ICS Cert USA, Homeland Security, Advisory (ICSA 10 272 01) Primary Stuxnet Advisory Original release date: September 29, 2010. Last revised: January 21, 2014.
50. R. Spenneberg, M. Brüggemann, H. Schwartke, PLC Blaster: A Worm Living Solely in the PLC, BlackHat Asia, 2016.

51. J. Graham , J.Effrey Hieb , J. Naber, Improving cybersecurity for Industrial Control Systems, IEEE 25th International Symposium on Industrial Electronics (ISIE), 2016.
52. Leandros A. Maglarasa,d,, Ki-Hyung Kimb, Helge Janickea, Mohamed Amine Ferragc,Stylianos Rallisd, Pavlina Fragkoue, Athanasios Maglarasf, Tiago J. Cruz Cyber security of critical infrastructures, ScienceDirect, 2018.
53. R. ROSS, M. McEvilley, J. Carrier Oren, Systems Security Engineering Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST (National Institute of Standards Technology) Special Publication 800 160, 2016.
54. G. Roldán Molina, M. Almache Cueva, C. Silva Rabadao, I. Yevseyeva, V. Basto Fernandes, A Comparison of Cybersecurity Risk Analysis Tools, Procedia Computer Science, 2017.
55. R. Sanchez Herrera, A. Mejías, M.A. Márquez, J.M. Andújar, A fully integrated open solution for the remote operation of pilot plants, IEEE transactions on Industrial Informatics, (2019) DOI 10.1109/TII.2018.2889135, 2019.
56. M. Márquez, R.S. Herrera, A. Mejías, F. Esquembre, J.M. Andújar, Controlled and Secure Access to Promote the Industrial Internet of Things, accepted IEEE Access 6.1 (2018) 48289 48299, 2018.
57. Mejías, R.S. Herrera, M.A. Márquez, A.J. Calderón, I. González and J.M. Andújar, Easy Handling of Sensors and Actuators over TCP/IP Networks by Open Source Hardware/Software, Sensors 17.1, 1 to 23, 2017.
58. SIEMENS, Advance The magazine for Totally Integrated Automation, Núm 1 April 2014,https://assets.new.siemens.com/siemens/assets/api/uuid:7414ea58057a1731bb917c22b4ebffd1956ef3b0/version:1542790198/advance-2014-1-en.pdf, 2014.
59. S.-Wen Chiou, A resilience-based signal control for a time-dependent road network with hazmat transportation, Reability Engineering & System Safety, DOI; https://doi.org/10.1016/j.ress.2019.106570, 2020.
60. X. (Joyce) Lyang, S. Ilgin Guler, Vikash V. Gayah, An equitable traffic signal control scheme at isolated signalized intersections using Connected Vehicle technology, Transportation Research Part C: Emerging Technologies, DOI: https://doi.org/10.1016/j.trc.2019.11.005, pages 81-97, 2020.
61. Alexander Skabardonis, Chapter 11 - Traffic management strategies for urban networks: smart city mobility technologies, Transportation, Land Use, and Environmental Planning, DOI: https://doi.org/10.1016/B978-0-12-815167-9.00011-6, pages 207-216, 2020.

62. Common Vulnerability Scoring System SIG, https://www.first.org/cvss/, 2020.
63. Peter M., Karen S., Sasha R., The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems, NIST Interagency Report 7435 Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899 8930, 2007.
64. E. LeMay, K. Scarfone, P. Mell, The Common Misuse Scoring System (CMSS): Metrics for Software Feature Misuse Vulnerabilities, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, 2012.
65. FIRST Improving Security Together, Standard, Common Vulnerability Scoring System (CVSS), Common Vulnerability Scoring System v3.0 Specification Document (v1.8), 2018.
66. FIRST, CVSS v3 Equations, https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator/equations, 2020.
67. CVE Common Vulnerabilities Exposures, list of common identifiers for publicly known cybersecurity vulnerabilities, 2018.
68. United States Computer Emergency Readiness (US CERT), National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security, 2016.
69. SIEMENS Security Advisory, Computer Emergency Response Team CERT, SSA 833048: Vulnerability in SIMATIC S7 1200 CPU´s prior to v4, 2016.
70. B. Genge, I. Kiss, P. Haller, a system dynamics approach for assessing the impact of cyber-attacks on critical infrastructures, International Journal of Critical Infrastructure Protection 10, 2015.
71. G. Stergiopoulss, P. Kotzanikolaou, M. Theocharidou, G. Lykou, D. Gritzalis, Time based critical infrastructure dependency analysis for large scale and cross sectorial failures, International Journal of Critical Infrastructure Protection 12, 2015.
72. G. Roldán Molina, M. Almache Cueva, C. Silva Rabadão, I. Yevseyeva, V. Basto Fernandes, A Comparison of Cybersecurity Risk Analysis Tools, International Conference on Project Management / HCist International Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2017, 8 to 10 November 2017.
73. A. Chaves, M. Rice, S. Dunlap, J. Pecarina, Improving the cyber resilience of industrial control systems, International Journal of Critical Infrastructure Protection 17, 2017.

74. Intelligence-Led Cyber Attack Taxonomy (C@T), posted in https://github.com/fdeandres/CAT , 2019.
75. V. Mavroeidis, S Bromander, Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence, European Intelligence and Security Informatics Conference (EISIC), 2017.