



## Article

# Design of Platforms for Experimentation in Industrial Cybersecurity

Manuel Domínguez \*, Juan J. Fuertes , Miguel A. Prada, Serafín Alonso , Antonio Morán and Daniel Pérez

Suppress Research Group, Escuela de Ingenierías, Universidad de León, Campus de Vegazana s/n, 24007 León, Spain; jj.fuertes@unileon.es (J.J.F.); mapram@unileon.es (M.A.P.); saloc@unileon.es (S.A.); a.moran@unileon.es (A.M.); dperl@unileon.es (D.P.)

\* Correspondence: manuel.dominguez@unileon.es

**Abstract:** The connectivity advances in industrial control systems have also increased the possibility of cyberattacks in industry. Thus, security becomes crucial in critical infrastructures, whose services are considered essential in fields such as manufacturing, energy or public health. Although theoretical and formal approaches are often proposed to advance in the field of industrial cybersecurity, more experimental efforts in realistic scenarios are needed to understand the impact of incidents, assess security technologies or provide training. In this paper, an approach for cybersecurity experimentation is proposed for several industrial areas. Aiming at a high degree of flexibility, the Critical Infrastructure Cybersecurity Laboratory (CICLab) is designed to integrate both real physical equipment with computing and networking infrastructure. It provides a platform for performing security experiments in control systems of diverse sectors such as industry, energy and building management. They allow researchers to perform security experimentation in realistic environments using a wide variety of technologies that are common in these control systems, as well as in the protection or security analysis of industrial networks. Furthermore, educational developments can be made to meet the growing demand of security-related professionals.



**Citation:** Domínguez, M.; Fuertes, J.J.; Prada, M.A.; Alonso, S.; Morán, A.; Pérez, D. Design of Platforms for Experimentation in Industrial Cybersecurity. *Appl. Sci.* **2022**, *12*, 6520. <https://doi.org/10.3390/app12136520>

Academic Editors: Howon Kim and Thi-Thu-Huong Le

Received: 23 May 2022

Accepted: 23 June 2022

Published: 27 June 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** industrial cybersecurity; SCADA; security tests; industrial control systems (ICS); industrial firewall; critical infrastructure cybersecurity

## 1. Introduction

The current digital transformation is changing industry in terms of flexibility, management or scalability. The growing connectivity leads to a progressive incorporation of information technologies (IT) into the field of operational technology (OT), whose elements used to be isolated. This IT/OT convergence exposes control systems to more threats that exploit both typical IT vulnerabilities and specific ones [1]. Nevertheless, industrial control systems usually have different requirements than other information systems. Unlike most information systems, availability of information in a control system is a more critical requirement than integrity and confidentiality for an effective operation. The direct use of traditional security solutions might cause production stops or larger response times that are not acceptable [2]. Moreover, long-term deployments use specific outdated technology that disregards the most essential security measures.

However, cybersecurity becomes essential for control processes included in critical infrastructures, where a disruption of their services can cause serious damages to environment, human lives, or economy. Given the importance of these services, critical infrastructures are strategical targets for cyber-attacks from several sources such as saboteurs or other nations, with a great level of sophistication. Furthermore, critical infrastructures often possess interdependence relationships between them [3], e.g., cyber-physical dependence (when one requires resources from other), geographical or logical. This interdependence could produce cascading effects as a result of an incident. For this reason, research efforts have been focused on critical infrastructure protection [4,5], joining efforts of several entities such as government and institutions to make them more resilient.

Indeed, the governments enact laws concerned about the security of these facilities, such as the directive 114/08/EC “on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection” of the European Commission. Efforts are made to propose effective security frameworks focused on ICS, such as those proposed by the National Institute of Standards and Technology. Standards such as ISA/IEC 62443 (formerly ISA99) provide useful guidelines for the secure implementation and operation industrial control systems (ICS). Furthermore, the Industrial Control System Cyber Emergency Response Teams from countries and/or manufacturers provide information about threats through different reports and training programs.

Although security practices developed in the IT field in the last few decades should be taken as a starting point for developing solutions, the particularities of control systems should be considered for its successful application [6]. That is why increasing efforts have been made lately to create industrial-oriented testbeds, where researchers can perform experiments safely and evaluate security-related experiments in similar scenarios to those ones found in critical infrastructures [7]. Furthermore, these environments are also necessary for industrial cybersecurity training in critical infrastructures because of a lack of professionals with the related skills [8]. However, there is not a methodology established for their design because of the difficulty for integrating realistically the cyber and physical aspects and their interconnections. This challenge requires further experimental work in realistic environments in order to achieve fidelity.

For mentioned reasons, in this paper, design guidelines for experimentation in cybersecurity of control systems are proposed. The approach is based on several principles such as network reconfigurability, modularity, and integration of virtualized computer systems with real equipment covering technologies used in different levels of automation. This resulted in the design of the Critical Infrastructure Cybersecurity Laboratory (CICLab), which includes four different systems: industry, buildings, energy and wireless sensors, as well as IT infrastructure virtualization and a flexible management system. Both the proposed structure and the heterogeneous equipment for these diverse sectors provide several possibilities for performing security experiments. This can help researchers to design security-oriented procedures and technologies in similar industrial environments. It will also be useful to obtain knowledge in the industrial security field, enabling the design of innovative educational platforms to address the skills required by future professionals in this area.

The contributions of this paper are the extensive description of the CICLab, firstly presented for training [9]; the enumeration of several objectives that a laboratory with these characteristics needs to accomplish; the evaluation of the main activities conducted in the laboratory in its first stages. The main novelty of the laboratory presented in this work is its diversity, since it is possible to apply a large set of technologies and protocols to emulate complex scenarios. The paper is structured as follows: in Section 2, testbeds for cybersecurity are reviewed focused on control systems are reviewed; in Section 3, the objectives and design criteria for the laboratory are presented; in Section 4, the description of the laboratory is detailed; in Section 5, main goals achieved are evaluated and, finally, in Section 6, conclusions are summarized and future directions are discussed.

## 2. Literature Review

Given the technical difficulty to perform a security assessment on a running system placed in a critical infrastructure, scientists have created testbeds where experimental research can be made safely [10,11]. A great number of alternatives have been proposed so far [7] with differences in the sector under study, the scale and coverage of their architecture, the usage objectives, the structural and functional characteristics or their evaluation process [12]. An especially active field for the application of testbeds is that of power system infrastructures and smart grids. A taxonomy of smart grid testbeds can be found in [13] for different research purposes, including cybersecurity. The scale and coverage of the testbed will depend greatly on the simulation approach. Nevertheless, even the approaches with

real physical systems often cover only a small set of communication protocols, up to three in most scenarios [7]. Among the thirty different ICS testbeds that have been analyzed in [14], the most common usage objectives identified are vulnerability analysis, education and test of defence mechanisms. With regard to their core characteristics, the testbeds in the literature usually aim at achieving fidelity, flexibility or cost-effectiveness. However, characteristics such as diversity, ability to monitor, reproducibility or isolation should not be disregarded. A comprehensive list of characteristics valuable to achieve credibility can be found in the study by Ani et al. [12].

Despite the variety of testbeds proposed, most of them are built on either simulated environments, where it is difficult to avoid a certain lack of fidelity with respect to real situations, or have a limited coverage of architectures and technologies. Previous works in the literature classify the approach to testbed construction into three different categories [15,16]. A first approach is the use of software-based simulations of the behaviours of industrial control networks. An opposite approach is the replication of real physical processes using the same components that can be found in an industrial facility. Finally, hybrid approaches can make use of a combination of physical components and emulation, which might include hardware-in-the-loop approaches.

Completely simulated testbeds are a low-cost solution to study cybersecurity in control systems, but they usually cannot model all interactions between control devices. These limitations can include delays and introduce inaccurate simulation results that could create an erroneous sense of security. Furthermore, research on vulnerabilities of specific technologies is generally beyond the reach of these testbeds.

Several works have implemented simulation frameworks in different environments to test the security of industrial control systems. For instance, a SCADA testbed architecture is provided in [17], where a simulation framework is implemented by means of Simulink subsystems, using discrete event and network simulation technology such as OMNET++ or Emulab in order to test three specific attacks scenarios. SCADASim [18] provides a modular and flexible framework to model SCADA simulations, also based on OMNET++ and built on a previous simulator [19], allowing for studying attacks on devices and simulated networks. In [20], a testbed is created using a PowerWorld server to simulate a power grid. In this case, the client visualizes and controls power system elements whereas a network emulator, using the RINSE tool, simulates the communication to show the vulnerability of the network client to a DDoS attack. On the other hand, C2WindTunnel is used in [21] to create an assessment environment and simulate a chemical plant and a controller connected through an Ethernet network, to estimate the effects of several attacks. To avoid some of the limitations caused by the use of traditional network simulation software, an approach based on the implementation of virtual devices is presented in [22]. Finally, the SCADA-SST [23] is generic enough to support different scenarios, lightweight and supports hybrid configurations such as simulated or physical components.

A hybrid approach usually involves the use of emulated processes, along with commercially available hardware and software. Sometimes, it can be framed as a hardware-in-the-loop emulation strategy. An example of this approach can be found in SCADA VT [24], which provides a SCADA testbed built on top of the CORE emulator that uses simulators of Modbus/TCP enabled equipment and I/O. A similar structure is proposed by [25]. Another simulated environment is described in [26], to provide extensible and adaptable assessment of the security of SCADA systems in associated infrastructures, using an OPC client and server, a SCADA protocol tester, SCADA Remote Terminal Units, sensors and actuators. An example in the domain of power systems is the cybersecurity testbed proposed by [27], which uses a power system simulator along with intelligent electronic devices, circuit breakers and interfaces with different specific communication protocols. The strategy of hardware-in-the-loop (HIL) provides benefits in terms of accuracy and feasibility [11], where sophisticated simulations can be comparable with real environments while providing advantages such as safety, modularity or repeatability. However, cyber-physical systems present challenging considerations in order to model correctly their behaviour, e.g., the interaction between different components such as

legacy and modern devices, or the IT configurations between them. The PowerCyber testbed of Iowa State University, introduced in [28], integrates cyber-physical components, virtualization, real time simulators, and emulation.

A more ambitious alternative is that of physical replication, i.e., the construction of a testbed for experimentation fully based on real equipment. This is difficult due to its high costs and complex implementation but provides higher similarity with respect to real setups found in industry. It might be more complicated to perform destructive tests without causing any damage to the real system. One large-scale facility was created in the U.S. National Idaho Laboratory (INL), whose research is related to security in critical infrastructures. In the context of the national security program, this laboratory includes electric power grid, wireless communications, and physical and cyber security protection and is aimed to improve resilience. In collaboration with other industrial, academic and governmental partners, such as Sandia National Laboratories, they have also created the National SCADA testbed (NSTB) [29] program, which offers research facilities to evaluate vulnerabilities, develop standards, promote best practices, test new industrial products and perform other secure-related activities.

Focused on the energy management infrastructure, the SCADA Security Laboratory and Power and Energy Research laboratory of the Mississippi State University have created another testbed aiming to cover several industrial control systems (such as those used in HVACs, petrochemical industry, gas pipelines, etc.). It uses commercially available software and hardware, a variety of routable and serial-based communication protocols and functional physical processes [30]. Their intended use is both pedagogical (for workforce development) and research-oriented, focused on the implications of vulnerabilities and the validation of their potential mitigations [31]. Some strategies for deploying a European SCADA security testbed are discussed in [32]. Moreover, the European CRUTIAL project has developed two complementary testbeds [33,34] to analyze their behaviour against attacks in several scenarios such as power station controllers on a real-time control network and power electronic controllers connected over an open communication network. In this case, elements from the industrial and information technologies are integrated to support research on architectures, dependencies and emergency management. The ENEL SPA and the Joint Research Centre of the European Commission have built an experimental facility [35] that recreates key elements of a power plant showing real scenarios.

The architecture proposed in this work stands out for the diversity of systems that can be emulated, an approach also followed by laboratories such as the Multiple-Scenario Industrial Control System Testbed (MSICST), the National Institute of Standards and Technology (NIST) testbed or the University of New Orleans SCADA system [7]. However, compared to these and other previous works, the proposed testbed covers a much larger set of technologies and protocols. The potential of reconfiguration among those technologies widens the scenarios that can be emulated.

### 3. Objectives and Design Criteria

Among the approaches listed in the previous section, the one presented in this paper can be framed as a physical replication approach for experimentation. The aim is to provide realistic environments for cybersecurity in critical infrastructures, based on the use of real equipment along with physical and virtualized computational resources. Virtualization should not be understood in this case as a simulation of those resources, since virtual machines are completely functional hosts and servers that run on top of a hypervisor instead of directly on the physical machine. Virtualization of hosts and network management allows a more efficient use of computational resources and makes it easier to deploy a machine to a certain subnetwork. The deployment of new hosts might be necessary in different scenarios.

The characteristics that are considered more important are fidelity, diversity, flexibility and ability to monitor:

- Fidelity or the ability to reflect the real nature of the system is a challenge that is addressed through the use of a physical replication approach. It is necessary to enable some of the proposed usage objectives.
- Diversity is addressed through a wide coverage of sectors but also of the specific technologies that are commonly found in each sector. In this sense, the proposed laboratory covers four different domains (industry, buildings, energy and wireless sensors), including their architectural and technological differences. Although control systems in different areas follow common principles, some of their elements are domain-specific and are interconnected using particular architectural patterns. For instance, ignoring non-routable serial protocols would hide the complexity of fieldbus networks, hampering a deep understanding of their vulnerabilities. The platform also covers the usual elements, software and communication protocols that are commonly used in the lower levels of the automation pyramid for each sector.
- Flexibility is needed to adapt to different usage scenarios. The use of virtualization makes reconfigurability possible, enabling the evaluation of different network architectures and the rapid deployment of elements needed for operation of the control system, security enforcement, information gathering or attack emulation. Regarding the control system, the arrangement of a certain subset of hosts can be used to create different automation schemas. These schemas can be designed from the perspective of complexity (e.g., monitoring a subprocess with a stand-alone SCADA or the whole process with a networked structure), security (in terms of network segmentation and host-based or perimeter security measures) or communication protocols (e.g., Ethernet/IP instead of Modbus TCP for communication in the control network).
- The ability to monitor the system operation involves the acquisition of security-related data (such as network traffic, logs or system artifacts) or process data (such as those recorded by the operational historian software). It allows the online monitoring or offline analysis of any research activity performed in a testbed. This characteristic is critical for experimentation since, in some cases, it is a key stage. That would be the case for the validation of proposed security mitigations, such as IDSs.

It is also necessary to define the main usage objectives for the laboratory:

- The development and assessment of demonstrations used for operator training, which address both the technical and pedagogical challenges to train professionals with different backgrounds in the interdisciplinary topic of industrial cybersecurity;
- Identification of vulnerabilities and experimental validation of the feasibility of threats that can affect control systems and their networks;
- Assessment of the efficacy of mitigations and countermeasures. It includes on one hand the evaluation of procedures for prevention, detection and response to incidents. On the other hand, it also includes the development or evaluation of technologies and configurations oriented to protect industrial control systems or critical infrastructures;
- Demonstrations of control systems. This implies the definition and construction of testbeds, especially in the industrial, electrical and building management fields, using elements with similar features to those included in real infrastructures.

Figure 1 shows the architectural concept on which the laboratory is based in order to achieve the proposed objectives. Through a mixed structure of specific hardware equipment (e.g., PLCs, sensors or actuators) and virtual machines with automation software (such as workstations, SCADAs, or historians) that are deployed where necessary, a replica of an automation pyramid is created with all the fundamental systems. This structure is interconnected by means of networks (Field, Control, Supervision and Management) recreating the connections that can be set in a control system. These links are configured by means of gateways, switches and routers (either physical or virtualized), which can be reconfigured remotely. This structure allows creating new network topologies to connect the different equipment.

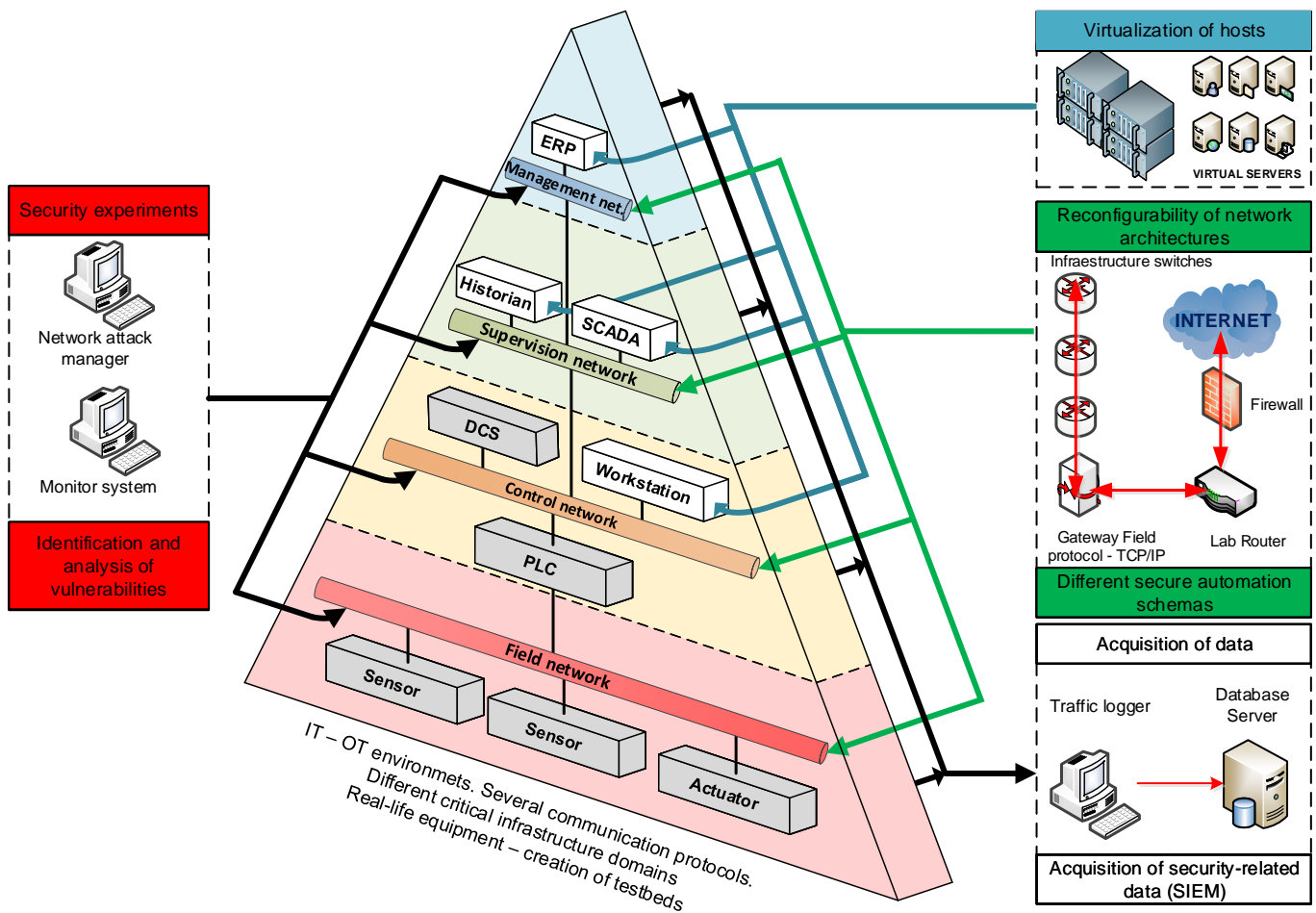


Figure 1. Laboratory architecture.

With this configurable architecture, it is also possible to acquire network traffic and monitor the involved equipment in order to collect information that can be studied afterwards. Several probes can be connected to collect the traffic and operating parameters of the equipment and store them in a database. Once the OT structure has been configured, the cybersecurity related tools that manage the attacks on the networks, analyze the possible vulnerabilities or apply countermeasures can be connected.

#### 4. Description of the Laboratory

To fulfill the requirements exposed previously, a laboratory for industrial cybersecurity in critical infrastructures has been developed at the University of León [9], the Critical Infrastructure Cybersecurity Laboratory (CICLab). In Figure 2, a photography of the laboratory is shown. This section provides an extensive description of the laboratory oriented to extract design guidelines that can be applicable by other researchers in similar environments.

CICLab includes four subsystems covering different areas: industrial control systems, building management systems, electric energy management systems and wireless sensor networks. The architecture was designed according to ISA95 automation pyramid, although connections with other elements can be established as required to perform possible experiments. Computing equipment consists of administration servers that are able to deploy virtual machines easily to perform particular tasks such as programming, monitoring, database management or collecting data.



**Figure 2.** Photography of the laboratory.

There is one virtual LAN (VLAN) for each system, which represents the first levels (0–1) of the ISA95 automation pyramid and includes several components such as instrumentation or PLCs. These networks are separated using firewalls, such as Tofino Xenon or Hirschmann Eagle, which allow for establishing specific rules for industrial communication protocols and, in some cases, deep packet inspection. Level 2 contains SCADA systems whose networks are segmented according to the requirements of experimentation. A demilitarized zone (DMZ) is created in level 3 between operational and business information systems using firewalls. The DMZ protects the network from unauthorized traffic in both directions and contains auxiliary services such as web servers. The business information systems are located in level 4, where several virtual machines run typical IT and management software.

From the point of view of computer hardware, CICI Lab is formed by a storage area network (SAN) with a storage capacity of 48TB, five servers with dual Intel Xeon processors of eight cores, 128 GB of RAM, and managed switches and routers. The first three servers allow for deploying configurations of heterogeneous machines in a simple way corresponding to the different levels of the ISA95. The fourth one deploys virtual machines for laboratory management and cybersecurity-oriented software. The last server is used as firewall, with a pfSense distribution and connected to 12 network interfaces. Finally, the managed switches are used to reconfigure the network architecture, with it being possible to adjust the segmentation strictness.

In Figure 3, a schema of the network architecture of the laboratory and the main virtual machines is shown. It can be seen that the second digit of the IP address indicates the subsystem (0: management, 1: industrial control, 2: building management, 3: electric energy management and 4: Wireless sensors). The third one indicates the ISA95 level and the last one the specific device or host. The right part of the figure shows the virtual machines with the software corresponding to the different levels of the pyramid, whereas the left part of the figure shows the virtual machines used to manage the laboratory and to perform the cybersecurity experiments. It should be noted that VLANs might be further segmented or interconnected to generate different training and research scenarios that are common in the industrial world.

Electric supply for the four systems is provided through four power lines (two single-phase of 16 A, another single-phase of 32 A and one three-phase of 32 A) that are duplicated to ensure safety for the elements of the laboratory, and managed by electric cabinets with devices that can be operated remotely.

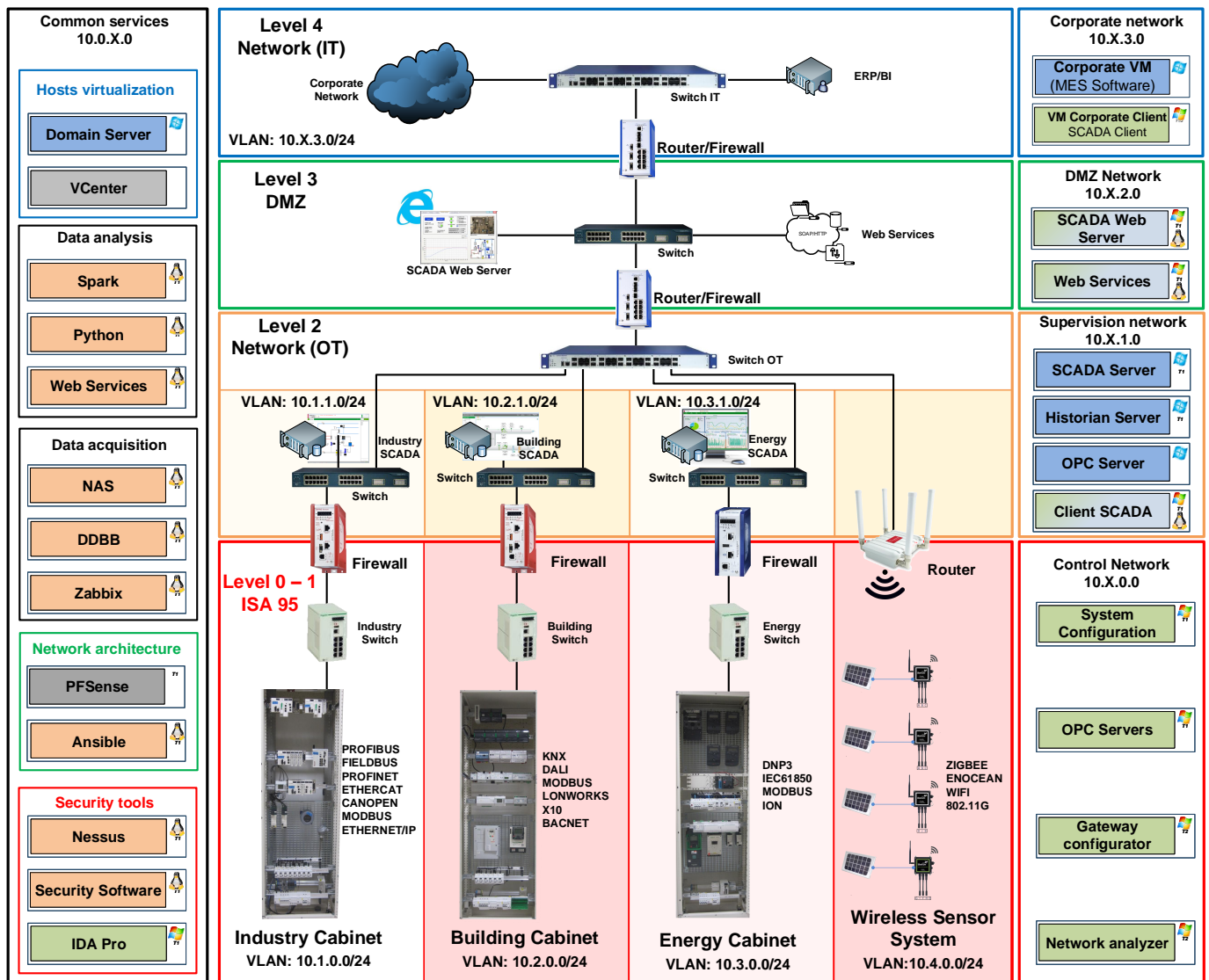


Figure 3. Network architecture of the laboratory.

#### 4.1. Industrial Control System

Typical devices for each level of automation pyramid are included, for instance, actuators and sensors of the process belong to the field level, programmable logic controllers (PLCs) and remote terminal unit (RTUs) are included in control level or human machine interface (HMI) in the supervision level, each level connected with a communication configuration.

The topology of this system consists of three industrial automation rings: a main ring and two secondary ones (Figure 4). The main ring has two PLCs with their corresponding input/output remote units that exchange information using Modbus TCP or Ethernet/IP protocols. These I/O cards manage field devices connected either directly or through field buses. In this case, two motor starters of 0.75 KW are connected to the I/O cards using AS-i and Modbus RTU, respectively. Other devices of the field level are a power electric meter, which communicates using Modbus RTU, and a temperature transmitter, using HART protocol.

The first secondary ring manages interconnection among several communication protocols. For that purpose, gateways link different types of networks that are used in industry, e.g., Modbus TCP–DeviceNet or Profinet–EtherCat. In the field level, the devices are variable frequency drives with communication cards for these protocols. The other secondary ring acts as an auxiliary, and its devices are mostly slaves of the two master



PLCs of the main ring. This ring is formed by a distributed I/O station, an Ethernet controller with protections and a variable frequency drive, connected using Modbus TCP. Other variable frequency drives are connected to this ring using CanOpen and Profibus DP protocols. An industrial switch establishes the connection between this ring and the main one.

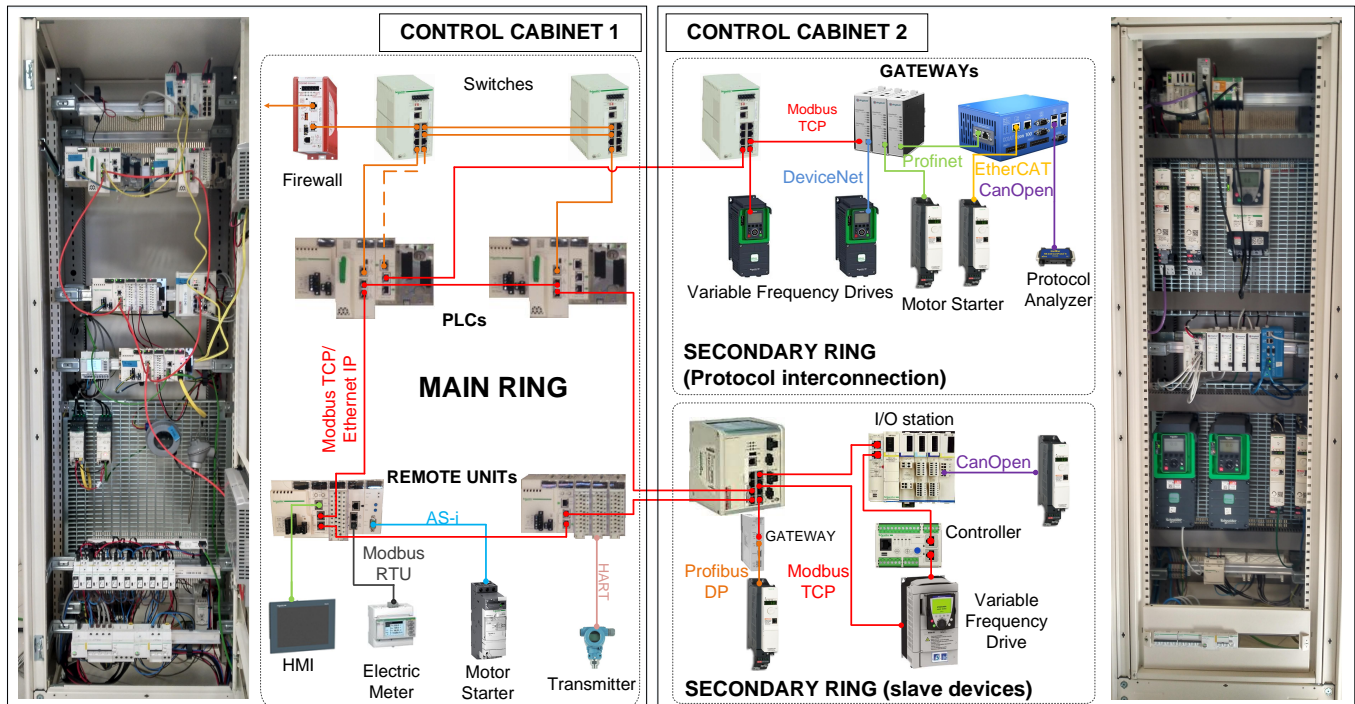


Figure 4. Schema for the industrial control system.

For the supervision level, a supervisory control and data acquisition (SCADA) system and historian server are included. Finally, a Tofino Xenon firewall can filter traffic between this level and control level. A specific feature of this firewall is that it can analyze some industrial protocols at the application layer of the OSI model.

#### 4.2. Building Management System

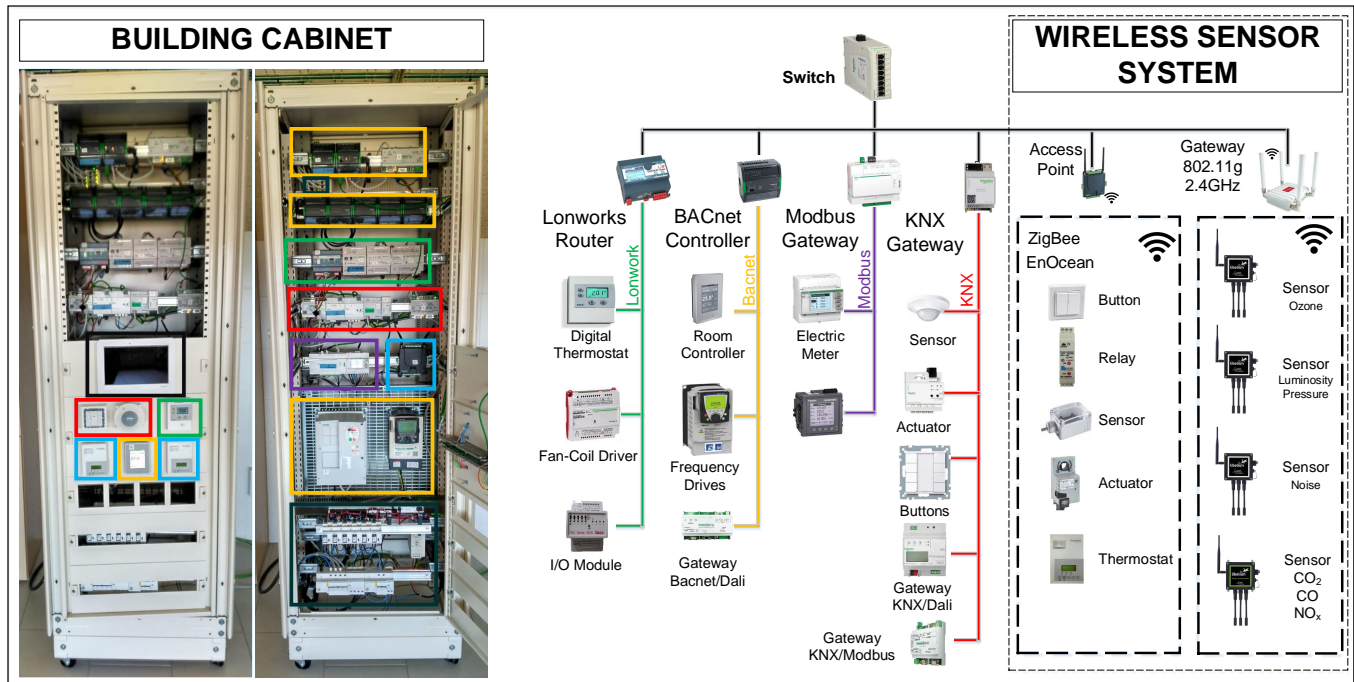
This system replicates the architecture of a building management system (BMS) used to control heating, ventilating and air conditioning systems (HVAC), lighting and other services of a building with the aim of increasing energy efficiency and comfort. The design of this system is made again to cover as many technologies as possible related to building automation (Figure 5).

For that reason, several controllers and routers are installed to manage field elements such as sensors or actuators in several typical building management networks: LonWorks, BACnet, KNX, Modbus, as well as wireless communications based on ZigBee and EnOcean. The elements installed for each network are the following:

- The Lonworks network is connected through a router and is composed of a digital thermostat, two fan coils drivers and an I/O module;
- In the BACnet network, there is a central controller and a room controller. Field devices are two digital thermostats and two variable frequency drives. In addition, a DALI gateway is designed for controlling lightning from this network;
- A Modbus gateway connects two electric meters communicated using Modbus RS485;
- An area implements basic elements for a KNX network such as power supply, a line coupler for extending the number of devices, and different sensors and actuators. A KNX/IP router allows an encrypted data transmission and several gateways are

available in order to convert KNX standard to other home automation protocols such as DALI and Modbus;

- Moreover, other sensors and actuators, e.g., presence or temperature sensors, exchange wireless information using EnOcean and Zigbee with a concentrator;
- Finally, the external access to this system is performed through a firewall.



**Figure 5.** Schema for building management system.

#### 4.3. Electric Management System

The electric system is designed to represent the supervision and control of an electric management system. For that purpose, the architectures used for this purpose in distribution substations and final clients have been replicated. This architecture of the substation includes most representative elements used in electricity distribution. The distribution substation includes a central unit, local HMI panels and intelligent electronic devices (IEDs) in charge of the protection, control and measurement in the electric positions. The communication network of this substation is defined in an optical fibre ring using the IEC 61850 standard where three positions have been defined. Each one has an electric network analyzer, a protection relay with a IEC 61850 communication card, a bay control unit and an industrial switch that links to the main ring (Figure 6).

Two transformer centres have been considered in the transformer station. One centre is assumed to be operated by an industrial company. It includes a unit to control a medium voltage substation remotely, with advanced meters and protection relays, connected using DNP3 protocol. The other centre is assumed to provide supply to end-use clients. It includes automatic circuit breakers, protection relays and measurement devices. The communication in this case uses Modbus TCP.

A set of loads emulate the end-use of electric energy. The loads available are two coupled induction motors of 5 kW with variable speed drives and starters. Moreover, this system includes electric panels for power supply and protection devices wired for a remote control using Modbus (TPC and serial) protocol. Finally, the electric energy is measured by smart meters communicating using PRIME protocol on Power-Line Communication (PLC), which sends data to a central hub.

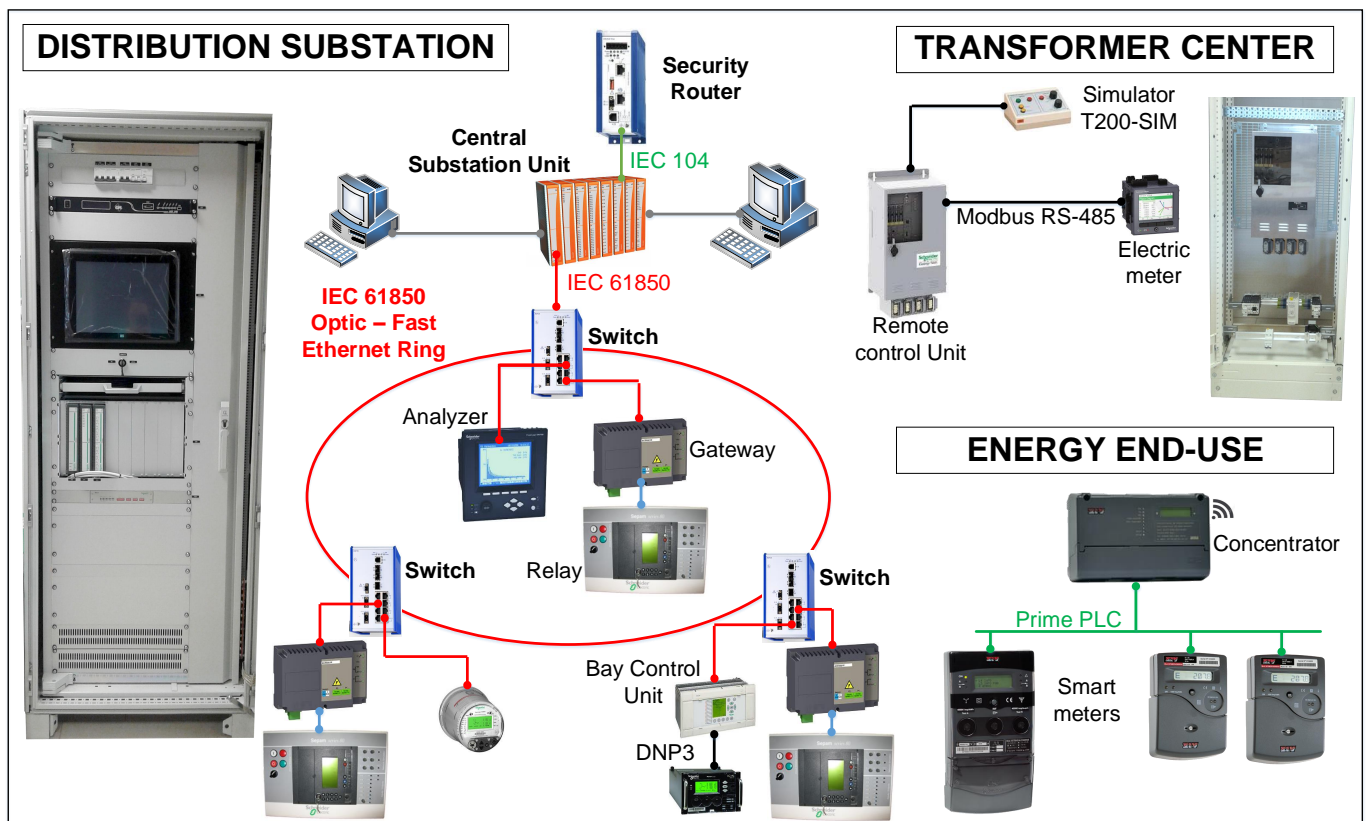


Figure 6. Schema for the electric management system.

#### 4.4. Wireless Sensor System

In this system, a set of wireless sensors are physically distributed in several points (indoor and outdoor) of the laboratory, connected each other to monitor atmospheric conditions. These interconnected devices allow collecting data, generating alarms and taking decisions without human interaction. They measure luminosity, atmospheric pressure, noise, ozone, dioxide of carbon, monoxide of carbon and nitrogen. Their batteries are charged by solar panels providing autonomy to the devices. The sensors are deployed in a 802.11 g/2.4 GHz network with a maximum velocity of 54 MBps. The measures are acquired each 5 min and sent to a central hub where they are stored in the internal memory. This hub manages communications and can be used to transfer data to a central database or cloud storage for posterior analysis. A schema of the wireless sensor system can be seen on the right side of Figure 5.

### 5. Fulfilment of the Usage Goals

This section explains the main activities that have been achieved in the CICLab during its first stages. Regarding the proposed usage objectives, they have been classified into four groups: cybersecurity training, vulnerability and threats identification, assessment of mitigation and countermeasures and development of testbeds or demonstration systems.

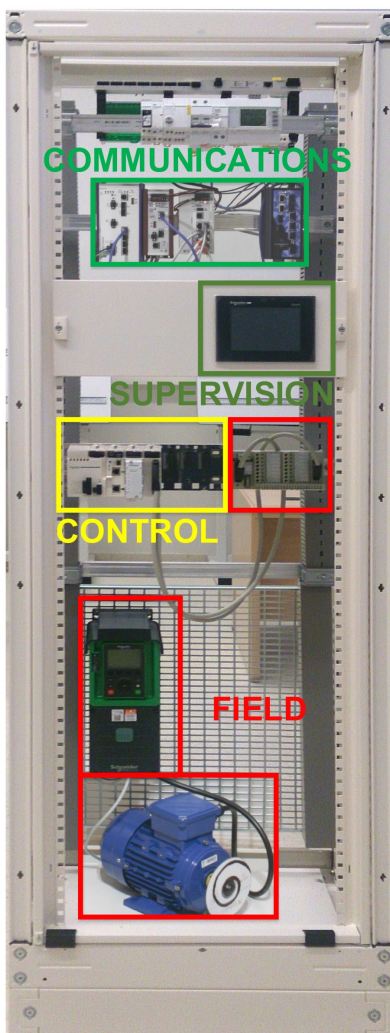
A relevant use of the laboratory at the university was focused on innovation for **cybersecurity training** using real control systems and networks [9]. In this sense, as a result of the lessons learnt from the design guidelines of the CICLab laboratory, while sacrificing coverage in exchange of cost-effectiveness and usability, a control cabinet was designed for educational purposes in industrial cybersecurity. This cabinet (See Figure 7a) implements a simple but complete automation system with field equipment, industrial and electric control and supervision, communication devices and the auxiliary supply equipment.

By combining the elements in each part, diverse configurations can be used for training in industrial cybersecurity. This system, which has given rise to a patent (number

ES 1197111 Y), has been used in several short courses developed for professionals and university students and focused on the following topics:

- Risk assessment in industrial environments—Security levels in an automated industrial environment;
- Secure configuration of ICS–SCADA—Integration, diagnosis, analysis and anomaly detection for ICS;
- Design and implementation of secure industrial networks—Segmentation and protection of industrial networks: switches, routers and industrial firewalls;
- Network vulnerability assessment and incident detection—Identification of vulnerabilities in industrial networks devices;
- Use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS);
- External access: virtual private network (VPN) configurations.

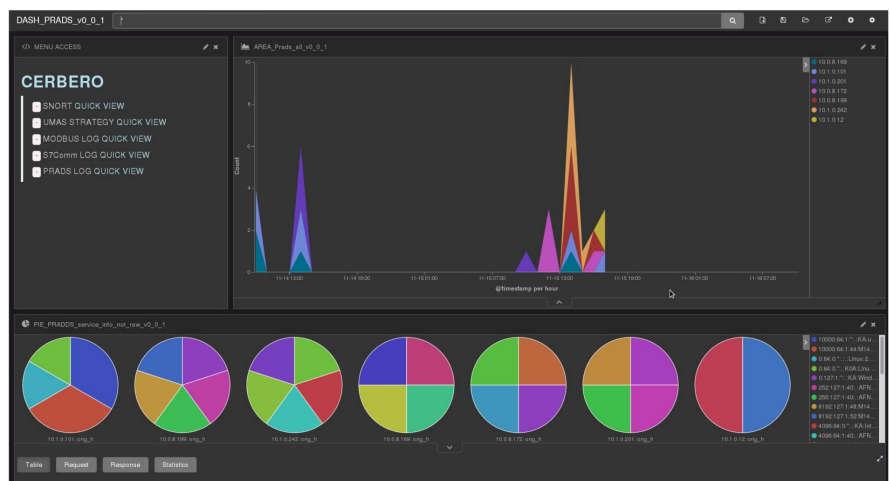
Feedback from the students by means of questionnaire has shown substantial acceptance and motivation on the topic.



(a)



(b)



(c)

**Figure 7.** Activities resulting from experimentation in the laboratory. (a) control cabinet ES 1197111 Y; (b) Industriwall; (c) NIDS user interface

Regarding a **vulnerability identification** in industrial equipment, a comparative analysis of the security in industrial control networks has been made through the study of

configuration protocols. Penetration testing scripts were developed to perform offensive actions against Schneider Electric and Siemens PLCs:

- Loading control strategies;
- Changing operation mode (stop/start);
- Extraction of device information through FTP, memory dumps and restoration back-ups;
- Sending of malicious packets for denial of services;
- Modification of system variables in the device and storage of small files in memory registers.

The results of these experiments revealed successful attacks on the devices which showed weaknesses of existing configurations [36]. Furthermore, a vulnerability in the M340 programmable logic controller was found that caused uncontrolled resource consumption, as documented in ICS-CERT Advisory ICSA-17-054-03.

With regard to the **assessment of countermeasures**, the laboratory was used for experimentation with a prototype for an industrial firewall, also developed by the research group. This firewall, shown in Figure 7b, is created as an adjustable low-cost device to filter and block undesirable traffic of industrial protocols at the network and application levels. The prototype is designed as an all-in-one built-in system with low-cost hardware and a robust protection box, embeddable in DIN Rail for industrial environments. It is oriented to be plug and play and to have an intuitive web-based interface for its intended use in small and medium-sized enterprises (SMEs) in the industrial sector, which usually have limited means and training for the basic network segmentation and protection of their processes. Although there are powerful solutions in the market, they generally have a higher cost, complicated configuration and monitoring or, sometimes, limited support of industrial protocol filtering. The experiments with this prototype were oriented to measure its performance under network conditions as the ones expected in small to medium-sized control systems. For that reason, the elements in the industrial control system were used to generate traffic. For that purpose, the prototype substituted the pre-existing firewall (see Figure 4) during the experiments. The results showed the feasibility of the prototype for operation under those circumstances, both with respect to its ability to filter traffic and the quality of user experience.

In the area of **demonstrations of control systems**, another result is the design and implementation of the testbed necessary for the development of a functional and scalable network intrusion detection system (NIDS) in a collaboration with the National Cybersecurity Institute of Spain (INCIBE). This NIDS captures security events and system information transparently, by means of custom filters and rules applied to well-known network monitoring software. It also includes a security information and event management (SIEM) system, for the storage and visualization of those events. As a result, it allows the generation of alerts and reports both during operation (for intrusion detection) and in the past (to support forensic analysis). This NIDS allowed to analyze and visualize security events that occurred in the industrial testbed. Although the configuration of the laboratory was centered in the generation of Modbus and UMAS (Schneider Electric configuration protocol) traffic in realistic conditions, it was an example of experimentation with a wide variety of technologies. Indeed, it involved the use of industrial-oriented software, such as an historian server, a SCADA server and client and an engineering workstation running the PLC programming platform, and the coordinated operation of control devices. These elements were located in different zones in the supervision and control networks, following a realistic network design, using network and filtering devices. For the experiment operation, it was also necessary to deploy services in the management subsystem of the laboratory, including several network probes, as well as hosts for intrusion detection, event processing, storage and visualization. The testbed was used to emulate several normal conditions but was also subject to a set of attacks. The results were positive, since the developers of the NIDS were able to run all their predefined tests and experiments. In Figure 7c, a screenshot of the NIDS use is shown. In this example, logs of two days were selected. The user interface shows IP addresses of the computers that accessed to the control system, along with times

and frequency. In the lower part of the screen, more information of the security event is displayed.

## 6. Conclusions

Given the need for industrial cybersecurity research and training of specialized personnel, the Critical Infrastructure Cybersecurity Laboratory (CICLab) is presented. The laboratory is extensively described, establishing the expected requirements to accomplish, showing the main activities that were conducted there and evaluating lessons learned from these experiences in its first stages. The approach proposed for the deployment of the CICLab provides a flexible framework to perform experimental activities related to security in critical infrastructures. Several subsystems replicate different types of environments that are found in critical infrastructures such as industrial control, building management, electric energy management or wireless sensors. These systems include a wide range of elements commonly used in each specific field, e.g., sensors, controllers and a large set of communication protocols, which allow users to work with diverse technologies present in real facilities. The design guidelines of the laboratory can be followed by other researchers to develop similar cybersecurity environments.

Several activities have been successfully performed in the laboratory; for example, the assessment of the prototype of an industrial firewall, a testbed for the development of a network intrusion detection system or the identification of vulnerabilities in industrial equipment. Moreover, the laboratory has been used for educational innovation to study how future professionals might be trained in cybersecurity of industrial systems.

A set of future developing activities are planned to be implemented in the laboratory including new research lines and pedagogical uses in cybersecurity courses. It is expected to exploit the laboratory capabilities to monitor and log the experiments to assess the use of visual data analysis techniques to improve interpretation of security events in monitoring systems.

**Author Contributions:** Conceptualization, M.D., J.J.F., S.A. and A.M.; methodology, J.J.F., M.A.P., A.M. and D.P.; software, M.A.P. and A.M.; validation, J.J.F. and S.A.; formal analysis, M.D.; investigation, J.J.F., M.A.P., A.M. and D.P.; resources, M.D.; data curation, J.J.F. and D.P.; writing—original draft preparation, D.P., M.A.P. and A.M.; writing—review and editing, D.P. and M.A.P.; visualization, A.M.; supervision, J.J.F.; project administration, M.D.; funding acquisition, M.D. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by MINECO (Grant UNLE13-3E-1578).

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Stouffer, V.; Lightman, S.; Hahn, A. *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*; NIST Special Publication 800-82 Revision 2. Initial Public Draft; National Institute of Standards and Technology (NIST), U.S. Department of Commerce: Washington, DC, USA, 2015.
2. Knowles, W.; Prince, D.; Hutchison, D.; Disso, J.F.P.; Jones, K. A survey of cyber security management in industrial control systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *9*, 52–80. [[CrossRef](#)]
3. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst.* **2001**, *21*, 11–25.
4. Yusta, J.M.; Correa, G.J.; Lacal-Arantequi, R. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy* **2011**, *39*, 6100–6119. [[CrossRef](#)]
5. Alcaraz, C.; Zeadally, S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* **2015**, *8*, 53–66. [[CrossRef](#)]
6. Hahn, A. Operational technology and information technology in industrial control systems. In *Cyber-Security of SCADA and Other Industrial Control Systems*; Springer: Cham, Switzerland, 2016; pp. 51–68.

7. Conti, M.; Donadel, D.; Turrin, F. A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2248–2294. [[CrossRef](#)]
8. Chowdhury, N.; Gkioulos, V. Key competencies for critical infrastructure cyber-security: A systematic literature review. *Inf. Comput. Secur.* **2021**, *29*, 697–723. [[CrossRef](#)]
9. Domínguez, M.; Prada, M.A.; Reguera, P.; Fuertes, J.J.; Alonso, S.; Morán, A. Cybersecurity training in control systems using real equipment. *IFAC Pap. Online* **2017**, *50*, 12179–12184. [[CrossRef](#)]
10. Giraldo, J.; Sarkar, E.; Cardenas, A.A.; Maniatakos, M.; Kantarcioglu, M. Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Des. Test* **2017**, *34*, 7–17. [[CrossRef](#)]
11. McLaughlin, S.; Konstantinou, C.; Wang, X.; Davi, L.; Sadeghi, A.R.; Maniatakos, M.; Karri, R. The cybersecurity landscape in industrial control systems. *Proc. IEEE* **2016**, *104*, 1039–1057. [[CrossRef](#)]
12. Ani, U.D.; Watson, J.M.; Green, B.; Craggs, B.; Nurse, J. Design Considerations for Building Credible Security Testbeds: A Systematic Study of Industrial Control System Use Cases. *arXiv* **2019**, arXiv:1911.01471.
13. Cintuglu, M.H.; Mohammed, O.A.; Akkaya, K.; Uluagac, A.S. A survey on smart grid cyber-physical system testbeds. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 446–464. [[CrossRef](#)]
14. Holm, H.; Karresand, M.; Vidström, A.; Westring, E. A survey of industrial control system testbeds. In *Secure IT Systems*; Springer: Cham, Switzerland, 2015; pp. 11–26.
15. Tippenhauer, N.O. Design and Realization of Testbeds for Security Research in the Industrial Internet of Things. In *Security and Privacy Trends in the Industrial Internet of Things*; Springer: Cham, Switzerland, 2019; pp. 287–310.
16. Furfaro, A.; Argento, L.; Parise, A.; Piccolo, A. Using virtual environments for the assessment of cybersecurity issues in IoT scenarios. *Simul. Model. Pract. Theory* **2017**, *73*, 43–54. [[CrossRef](#)]
17. Giani, A.; Karsai, G.; Roosta, T.; Shah, A.; Sinopoli, B.; Wiley, J. A testbed for secure and robust SCADA systems. In Proceedings of the 14th IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS 2008, St. Louis, MO, USA, 22–24 April 2008; Volume 5.
18. Queiroz, C.; Mahmood, A.; Tari, Z. SCADASim—A framework for building SCADA simulations. *IEEE Trans. Smart Grid* **2011**, *2*, 589–597. [[CrossRef](#)]
19. Queiroz, C.; Mahmood, A.; Hu, J.; Tari, Z.; Yu, X. Building a SCADA security testbed. In Proceedings of the 2009 Third International Conference on Network and System Security, Gold Coast, QLD, Australia, 19–21 October 2009; pp. 357–364.
20. Davis, C.; Tate, J.; Okhravi, H.; Grier, C.; Overbye, T.; Nicol, D. SCADA cyber security testbed development. In Proceedings of the 2006 38th North American Power Symposium, Carbondale, IL, USA, 17–19 September 2006; pp. 483–488.
21. Chabukswar, R.; Sinopoli, B.; Karsai, G.; Giani, A.; Neema, H.; Davis, A. Simulation of network attacks on SCADA systems. In Proceedings of the First Workshop on Secure Control Systems, Stockholm, Sweden, 12 April 2010.
22. Reaves, B.; Morris, T. An open virtual testbed for industrial control system security research. *Int. J. Inf. Secur.* **2012**, *11*, 215–229. [[CrossRef](#)]
23. Ghaleb, A.; Zhioua, S.; Almulhem, A. SCADA-SST: A SCADA security testbed. In Proceedings of the 2016 World Congress on Industrial Control Systems Security (WCICSS), London, UK, 12–14 December 2016; pp. 1–6.
24. Almalawi, A.; Tari, Z.; Khalil, I.; Fahad, A. SCADAVT-A framework for SCADA security testbed based on virtualization technology. In Proceedings of the 38th Annual IEEE Conference on Local Computer Networks, Sydney, NSW, Australia, 21–24 October 2013; pp. 639–646.
25. Mallouhi, M.; Al-Nashif, Y.; Cox, D.; Chadaga, T.; Hariri, S. A testbed for analyzing security of SCADA control systems (TASSCS). In Proceedings of the Innovative Smart Grid Technologies (ISGT), Anaheim, CA, USA, 17–19 January 2011; pp. 1–7.
26. Wang, C.; Fang, L.; Dai, Y. A simulation environment for SCADA security analysis and assessment. In Proceedings of the 2010 International Conference on Measuring Technology and Mechatronics Automation, Changsha, China, 13–14 March 2010; Volume 1, pp. 342–347.
27. Hong, J.; Wu, S.S.; Stefanov, A.; Fshosha, A.; Liu, C.C.; Gladyshev, P.; Govindarasu, M. An intrusion and defense testbed in a cyber-power system environment. In Proceedings of the 2011 IEEE Power and Energy Society General Meeting, Detroit, MI, USA, 24–28 July 2011; pp. 1–5.
28. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [[CrossRef](#)]
29. (INL), I.N.L. National SCADA Test Bed: Fact Sheet, 2007. Available online: [https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB\\_Fact\\_Sheet\\_FINAL\\_09-16-09.pdf](https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf) (accessed on 22 May 2022).
30. Morris, T.; Srivastava, A.; Reaves, B.; Gao, W.; Pavurapu, K.; Reddi, R. A control system testbed to validate critical infrastructure protection concepts. *Int. J. Crit. Infrastruct. Prot.* **2011**, *4*, 88–103. [[CrossRef](#)]
31. Morris, T.; Vaughn, R.; Dandass, Y.S. A testbed for SCADA control system cybersecurity research and pedagogy. In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA, 12–14 October 2011; p. 27.
32. Christiansson, H.; Luijff, E. Creating a european SCADA security testbed. In Proceedings of the International Conference on Critical Infrastructure Protection, Hanover, NH, USA, 18–21 March 2007; pp. 237–247.

33. Dondossola, G.; Deconinck, G.; Garrone, F.; Beitollahi, H. Testbeds for assessing critical scenarios in power control systems. In Proceedings of the International Workshop on Critical Information Infrastructures Security, Rome, Italy, 13–15 October 2008; pp. 223–234.
34. Dondossola, G.; Garrone, G.; Szanto, J.; Deconinck, G.; Loix, T.; Beitollahi, H. ICT resilience of power control systems: Experimental results from the CRUTIAL testbeds. In Proceedings of the 2009 IEEE/IFIP International Conference on Dependable Systems & Networks, Lisbon, Portugal, 29 June–2 July 2009; pp. 554–559.
35. Fovino, I.N.; Masera, M.; Guidi, L.; Carpi, G. An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants. In Proceedings of the 3rd International Conference on Human System Interaction, Rzeszow, Poland, 13–15 May 2010; pp. 679–686.
36. Martín-Liras, L.; Prada, M.A.; Fuertes, J.J.; Morán, A.; Alonso, S.; Domínguez, M. Comparative analysis of the security of configuration protocols for industrial control devices. *Int. J. Crit. Infrastruct. Prot.* **2017**, *19*, 4–15. [[CrossRef](#)]