Industrial and Automation Control System Cyber Range Prototype for Offensive Capability Development

Austris Uljāns[1] and Bernhards Blumbergs[2] [a]

[1]*Vidzeme University of Applied Sciences, Cesu Str. 4, Valmiera LV - 4200, Latvia*
[2]*IMCS UL, CERT.LV, Raina Blvd. 29, Riga, LV-1459, Latvia*
austris.uljans@va.lv, bernhards.blumbergs@lumii.lv

Keywords: Industrial Automation, Cyber Range, Offensive Cyberoperations.

Abstract: Industrial and automation control systems (IACS) are broadly utilized in sectors, such as manufacturing processes control and energy transmission. Attacks on these systems may have devastating effects. Moreover, current IACS systems are interconnected with conventional IT infrastructures thus increasing potential adversary access to industrial systems. This research describes and offers a prototype for a realistic and easily reproducible IACS cyber range for offensive exercise development. An extensive study of various technical aspects and scenarios of existing IACS cyber ranges is conducted to create the knowledgebase for such range development. Created IACS cyber range use is validated by conducting practical offensive capability development training for a target audience. This work concludes, that IACS cyber ranges are a viable tool for understanding and developing offensive tactics and techniques used to gain access to the IACS network and damage physical processes.

1 INTRODUCTION

The digital world nowadays is rapidly expanding with having significant impact on human society. This also applies to IACS systems, which provide efficient automation and operation of critical infrastructures (CI), such as, electrical grids, gas distribution grids, water treatment, transportation, and heating plants. IACS systems are typically characterized by proprietary protocols, isolated networks, and purpose-specific hardware, which have started to close the gap between traditional IT systems with related elements, networks, and ideologies. This has made IACS a target to various adversaries, especially due to rapid expansion towards industrial IoT devices, which further increase the attack surface. IACS receive an increasing number of sophisticated and debilitating attacks (CISA, 2021; Geng et al., 2019; Kaspersky Lab, 2021a) from organized crime and nation-state affiliated actors (FireEye, 2021; MITRE, 2021).

There is little reported information about actual attacks on industrial infrastructure or scenarios executed by adversaries, despite the growing awareness of IACS cybersecurity (Zhu et al., 2011). To increase understanding and discover vulnerabilities in

IT infrastructure, researchers create testbeds and cyber ranges (CR) to test the attack and defense mechanisms in a controlled environment. Publication (Krishnan and Wei, 2019) indicates that there is a lack of existing research on IACS cyber ranges, therefore making them less accessible to the broader community to gain more experience in the defense and offense of related components. Offensive capabilities are deliberate invasions into opponent systems to cause destruction, disruption, or damage. Research (Lewis, 2015) draws attention to how the lack of an utter offensive cyber capability affects NATO's ability to deter and defend. Therefore, offensive capabilities need to be developed as adversaries cannot be refuted by pure defense. In the author's opinion, the point is valid for any national state entity. However, national state's cybersecurity exercises are focused on defense, where immediate attention is to train blue team's defense response on red team's attacks. Thus, exercises improving the readiness of red team's offensive capabilities are limited in scope and mostly not public. This signifies the need for an open and well-documented CR to allow a better understanding and wider development of offensive capabilities.

This paper addresses the problem in the field of cyber red team's offensive capability development. Only some of the NATO nations have publicly ex-

---

[a] https://orcid.org/0000-0001-9679-6282

pressed limited information on possessing offensive capabilities (Gold, 2020; Muller, 2019; UK Government, 2016). Such capability development might be as a response to a steadily growing cyber attacks attributed to nation-state actors (Kaspersky Lab, 2021b). Thereby the problem addressed in this paper is that *red team offensive capabilities in the IACS field are yet to be closely studied to gain a deeper insight into how IACS elements can be attacked and defended.* Current studies mainly focus on defensive capability development in the IACS field, due to development of blue team defenses to counter adversary attacks as presented in section 2. Additionally, offensive capabilities may be used to respond to aggressors with proportional measures. Offensive capability development is necessary both for private and public entities operating or depending on IACS, as they need to know how to test and protect their infrastructure.

The main objective and novelty of this research is aimed towards development of the IACS CR, where the red team can practice developing offensive capabilities, encompassing the following key aspects: 1) realistic, 2) easily reproducible, 3) with publicly available documentation, and 4) supporting multi-stage attack scenarios. The created CR prototype may be used to develop exercises for evolving red team offensive capabilities within IACS field, thereby improving understanding of related tactics and techniques, and utilizing CR for exercises to develop both defensive and offensive capabilities by any suitable means.

This research addresses identified gaps within current IACS CR approaches and use-cases (section 2.1). Moreover, the created CR encompasses the minimal investments of resources, ease of replication, open-source paradigm, publicly available documentation, and complexity to perform realistic offensive multi-stage attack scenarios. The main contributions of this research are:

1. Comprehensive literature analysis of current relevant IACS testbeds;
2. Core concepts and approaches for IACS CR prototype design and implementation.

This paper prototypes an IACS cyber range for practical offensive cyber capability development, Section 2 provides literature analysis of related work and summarizes the outcomes; Section 3 identifies and presents cyber range development and training scenario requirements; Section 5 offers the results of cyber range training use case; and Section 6 provides conclusions and future work directions.

2 RELATED WORK AND CYBER RANGE REVIEW

To identify related work, the following keywords and their combinations were used: *IACS, ICS, SCADA, testbed, cyber range, training, offensive cyber operations*. As the IACS field develops quickly, a primary period of the last five years was chosen as an optimal time frame for relevant literature identification. Searches were conducted in Google Scholar, Scopus, IEEE scientific databases and indexes, and public search engines. Research eligibility criteria was based on the direction towards CR creation or review of industrial CRs.

IACS elements are distributed in operational technology (OT) network with a difference between conventional information technology (IT) systems being minimal delays for time-critical processes. Research (Zhou et al., 2018) mentions that the key difference between IT and OT is that OT includes multiple embedded operating systems, which use field-specific proprietary protocols. OT networks rely on real-time data round-trips and interruption in these communications can cause operational, financial, and physical losses. Research (Holm et al., 2015) points out that due to the high availability requirements of IACS, security tests are strongly not advised to be performed on a live system. For this reason, researchers, corporations, and military institutions turn to cyber ranges that mimic real IACS.

The core control elements in a cyber-physical system include at least a programmable logic controller (PLC), human-machine interface (HMI), and supervisory control and data acquisition (SCADA). A PLC being a programmable device performs logical operations for a physical process based on received external inputs. To visualize the control process a multi-purpose HMI or SCADA is used to allow an operator to supervise and interact with a physical process. All of these systems are either managed or installed from a general-purpose computer or server, which increase the attack surface (Larrucea and Molinuevo, 2020).

2.1 Overview of Current IACS Cyber Ranges

Publication reviewing the development in IACS attacks (Larrucea and Molinuevo, 2020) states that developing cyber-security competencies through the use of CR and their use for research topics is of increasing interest. Also, CRs are a vital tool for exploring and modeling vulnerabilities, and producing viable data sets that enable testing security solutions as novel architectures, intrusion detection systems, and attacks
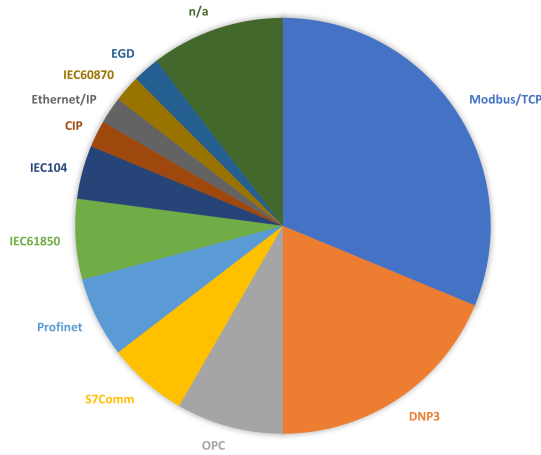
Figure 1: Overview of industrial protocols used in CR testbeds listed in table 1.

against infrastructure. While performing the literature review, 28 created testbeds were identified in the relatively new research. These testbeds are indicated in table 1.

Table 1 shows that half of the CR testbeds are created in the USA, with the rest being scattered across Europe and Asia. However, in recent years, the number of CRs and testbeds is increasing in Europe and Asia. Such increase may be explained by the rise of overall governmental and industry interest due to the emergence of global cyber-powers and accelerating integration and merger of OT and IT systems with the raise of industry 4.0. Based on the assessment, IACS CR typical applications include electrical generation plants, the chemical and oil industry, water and wastewater management, nuclear power stations, and the manufacturing industry. The primary industry created in CRs is energy transmission and generation. This may be reasoned, that the energy sector is one of the most obvious targets for adversaries due to the nation's critical dependency on the electrical power supply. Additionally, research using an electrical grid can more easily emphasize the gravity of cyberattacks. It may be observed, that one of the most common vendors used in physical IACS cyber ranges across multiple studies are Siemens and Allen-Bradley, which may be explained due to these vendors being present in worldwide markets and across a huge share of industries.

Furthermore, very few of the physical cyber ranges in table 1 publicly share a detailed documentation of the system, making it hard to validate or replicate the research. Publication (Green et al., 2017) note that making the testbed more open for researchers extends its usability, and it should be taken into account when designing such testbeds.

Important part of the IACS system lies within ensuring effective and interoperable communications between the control elements. To achieve this, TCP/IP-based communication protocol usage is becoming more prevalent, which also broadens the overall attack surface of IACS. Figure 1 provides the overview of the used protocols within the assessed CR testbeds. It is shown that one of the most used protocols in cyber ranges across multiple fields of IACS is Modbus/TCP, followed by DNP3, OPC, and s7comm. Modbus/TCP has been adapted worldwide due to its open specification, available documentation, and community support. DNP3 is an open and public protocol standard primarily used in electric and water utilities in the USA. S7comm is a Siemens proprietary protocol used in communication between PLCs of the Siemens S7-300/400/1200/1500 family. OPC is a series of standards and specifications maintained by and made available to OPC Foundation members, mainly used for industrial telecommunication in higher-level management systems, such as, manufacturing, building automation, oil and gas, and renewable energy.

Testbeds and CRs may be divided by type, purpose, and applicable sector. Sector-wise test-beds may be divided into academic, military, or commercial. From the perspective of their purpose, CRs may cover a very wide range of applicability, such as, cyber training, capture the flag events, research and development, testing, assessment, and recruitment. Research works, such as (Reaves and Morris, 2012; Geng et al., 2019), categorize CRs into physical, virtual, and hybrid architectures. Many testbeds hybridize the physical and virtual components to make a trade-off between fidelity and economy. The majority of assessed research is being done on virtualized testbeds as they do not require huge investments, are relatively easy to implement, and re-purpose.

2.1.1 Physical Testbed

Physical testbeds rely on physical hardware and actual software running on that hardware. Some of the physical CRs, such as (Adepu et al., 2019; Mathur and Tippenhauer, 2016) are used to control the actual physical process containing actuators and sensors. Despite the advantages, most physical CRs use the hardware-in-the-loop physical system simulation method, which uses mathematical models to represent physical processes. There is a lack of exact mathematical models for representing the behavior of sensors and actuators used in monitoring and controlling the physical devices, however when designing CRs fulfilling such requirements is not mandatory (Green et al., 2017).

For example, a physical SWAT CR testbed (Mathur and Tippenhauer, 2016) consists of a six-

Table 1: Cyber range overview (Chemical plant - C, Smart Grid - SG, Nuclear plant - N, General - G, Electrical Grid - G, Transportation - T, Manufacturing - M, Water Treatment - W, V - Virtual CR, P - physical CR, H - hybrid CR, Unspecified - information not provided by the research, N/A - hardware does not apply to virtual testbeds).

Nr.	Name	Country	Year	Field	Type	Hardware vendor	Ref.
1	Unspecified	USA	2012	G	V	N/A	(Reaves and Morris, 2012)
2	Unspecified	USA	2017	EG	V	N/A	(Koganti et al., 2017)
3	Unspecified	USA	2016	EG	P	Unspecified	(Korkmaz et al., 2016)
4	VTET	China	2018	C	H	Siemens	(Xie et al., 2018)
5	Unspecified	Quatar	2021	C	H	Siemens	(Noorizadeh et al., 2021)
6	Unspecified	USA	2019	N, T	P	Koyo, RaspberryPi	(Stranahan et al., 2019)
7	Unspecified	USA	2017	G	P	Siemens	(Su et al., 2017)
8	MSICST	China	2019	G	P	Siemens, Rockwell, GE, Schneider	(Tao et al., 2019)
9	Unspecified	Portugal	2017	EG	V	N/A	(Rosa et al., 2017)
10	Unspecified	USA	2019	C	P	Koyo, Eaton	(Krishnan and Wei, 2019)
11	IOSB	Germany	2017	M	H	Siemens	(Pfrang et al., 2017)
12	EPIC	Singapore	2019	SG	P	Pcvue, Wago, Siemens, SMA, Hirschmann	(Adepu et al., 2019)
13	Unspecified	France	2017	EG	P	RaspberryPi	(Rubio-Hernan et al., 2017)
14	Unspecified	Netherlands	2018	EG	V	N/A	(Chromik et al., 1 06)
15	Unspecified	Switzerland	2018	T	V	N/A	(Urdaneta et al., 2018)
16	Unspecified	USA	2021	HVAC	V	N/A	(Werth and Morris, 2021)
17	RICS-el	Sweeden	2019	EG	V	N/A	(Almgren et al., 2019)
18	Unspecified	USA	2018	G	V	N/A	(Alves et al., 2018)
19	SWAT	Singapore	2016	W	P	Allan-Bradley's	(Mathur and Tippenhauer, 2016)
20	PowerCyber	USA	2010	EG	V	N/A	(Hahn et al., 2010)
21	GRFICS	USA	2018	C	V	N/A	(Formby et al., 2018)
22	Unspecified	Italy	2010	EG	H	ABB, OpenPLC	(Fovino et al., 2010)
23	VCSE	USA	2011	EG	V	N/A	(Stamp et al., 2011)
24	Unspecified	USA	2011	G	P	GE, PXI, Rockwell's	(Morris et al., 2011)
25	VPST	USA	2009	EG	V	N/A	(Bergman et al., 2009)
26	TASSCS	USA	2011	EG	V	N/A	(Mallouhi et al., 2011)
27	ICSrange	Italy	2019	G	V	N/A	(Giuliano and Formicola, 2019)
28	SoftGrid	Singapore	2016	EG	V	N/A	(Gunathilaka et al., 2016)

stage water treatment process, where each stage is autonomously controlled by a local physical PLC. Physical CRs have two main drawbacks: 1) difficulty to reconfigure and maintain real hardware and software in a testbed, especially given the presence of firmware exploits that have the potential to damage elements, 2) is a financial aspect as physical components used in CRs may be expensive, hence researchers tend to use a small amount of core physical components and augment it with virtualized components. Key advantages of physical CRs include several aspects: 1) provision of realistic system and environment reaction on attacks, which would be present in an actual process control system, 2) realistic communication patterns and latency, and 3) physical devices with susceptible to software, firmware, and hardware vulnerabilities, which are hard, if not possible, to replicate within a virtual testbed.

2.1.2 Virtualized Testbed

Research (Xie et al., 2018) mentions, that virtualization is a straightforward approach to overcome the disadvantages of physical testbeds. Although the virtual testbed would lose some fidelity, it is more suitable for preliminary IACS security research in the laboratory environment. For example, one of such virtualized testbeds is GRFIACS framework (Formby et al., 2018) based on OpenPLC (Alves et al., 2014) research, which permits the GRFIACS to virtualize the entire IACS network and related physical processes. Main advantages mentioned in (Reaves and Morris, 2012) are: 1) virtual testbeds are easy to duplicate and reproduce, and 2) virtualization provides a common framework for conducting research, and sharing the results and the code to the research community for reproduction and validation.

2.1.3 Hybrid Testbed

Researches, aiming for low cost and maintaining some fidelity of IACS cyber range, include both physical and virtual components, thus designing hybrid testbeds. Such testbeds try to combine the best of both worlds – virtual and physical, and may employ physical components, such as, PLCs, HMIs, and other physical systems, which are hard or practically impossible to virtualize or simulate. On the other hand, system elements like SCADA workstations, data historians, and network infrastructure may be virtualized. An element, such as, SCADA commonly resides on a MS Windows-based operating system, which may run in a virtual environment like VMware or VirtualBox. For example, related work (Pfrang et al., 2017) presents a CR by dividing it into physical and virtual parts as follows: 1) virtual environment - virtual network components, virtual machines (VMs) for programming PLCs, VM SCADA servers, attack detection tools, and 2) physical environment - physical PLCs, industrial actuators, HMIs, and RTUs.

3 CYBER RANGE DEVELOPMENT CONSIDERATIONS

CR criteria may change based on objectives, for example, research (Formby et al., 2018) has created GRFIACS testbed framework, which is intended to help beginners in IACS security to overcome barriers created by the exclusive use of expensive and proprietary hardware and software used in IACS. Therefore, this research offers a novelty through the following main considerations: 1) modular design permitting to swap virtual elements with physical ones, 2) low initial cost, and 3) simple communication protocols for students to reduce the learning curve. Other related works (Fovino et al., 2010; Koganti et al., 2017) have created electrical grid hybrid IACS cyber rages, with the main objective being to explore the cascading effects in case of IACS failure with realistic attack scenarios and to test novel cyber-attacks. Testbeds like these require sophisticated simulation of the electrical grid to understand the impact of the attacks, whilst having a minor emphasis on control system complexity.

This research prototypes a CR with the following key considerations:

1. Repeatability: an inherent possibility for other researchers to replicate the testbed and build upon it;
2. Fidelity: the CR requires to reproduce the real system as accurately as possible, CR has to present interaction with real IACS components using real IACS tools, as well as, providing conditions for performing realistic attacks;
3. Physical process interaction: the different IACS processes may interact with each other not only through data link but by a physical process, such as, temperature, vibration, or mechanical motion;
4. Common communication protocols: research (Green et al., 2017) suggests to choose industrial protocols in accordance with the IACS field, and country or region represented within the CR. Common protocols in the industry are Modbus/TCP, Profinet, DNP3, IEC61850, OPC/OPC-UA, S7comm, and IEC60870-5-104 (IEC104) (Fig. 1);

5. Network segmentation: from the perspective of the CR topology, the research (Green et al., 2017) indicates that IACS need to be separated in zones to mimic realistic IACS system, such as, a manufacturing zone, demilitarized zone, and enterprise zone. The same ideology is applied in research by (Almgren et al., 2019), where a more realistic environment is created by attaching other IT networks to IACS network segments, such as, office or enterprise networks;

6. Adaptability and flexibility: a capability for reconfiguring the whole testbed by exchanging components through standardized interfaces mechanically, electrically, and from networking infrastructure perspective. For this purpose, CR encompasses common industrial communication protocols and widely used hardware vendors;

7. CR element selection by market share: components are chosen based on common automation component vendors in the Baltic state region.

In this research, the emulated primary physical process in the CR prototype is the district heating plant, which supplies heating to the city. The secondary control process is the heating plant's warehouse management system controlling alarms and lights. The warehouse is an integral part of the heating plant support infrastructure. The heating plant and warehouse are collocated (Fig. 2) and are interconnected in a single communication network. The authors have chosen the heating plant since it may be considered as a part of the city's critical infrastructure and may be valid targets for adversaries. Moreover, the heating process is relatively easy to implement, comprehend by the training audience, and understand the possible negative impact to civilians caused by the disruption of different physical processes.

4 PRACTICAL IMPLEMENTATION

The CR prototype network topology is shown in figure 2. The system consists of two PLCs (3) and (4), SCADA (2) and WEB-SCADA (1). This is divided into supervisory and control systems containing SCADAs, and execution systems containing PLCs. The following subsections introduce the detailed working principles of each implemented elements and their communication specifics. The CR prototype component choices have been based on the following criteria: 1) supported common industrial protocols (Fig. 1), 2) vendor popularity (Tab. 1), and 3) estimated average price in Euros (Tab. 2).4

4.1 Heating Process

The heating plant's SCADA HMI visualization is shown in figure 3. The virtualized heating plant consists of circulation pump (A1), transmission line valve (A3), gas flow valve (A2), tank temperature and burning temperature sensors (S3, S2), pressure sensor (S4), and flow speed sensor (S1).

The heating process in the CR prototype is divided into two phases – 1) the heating of the heat transfer liquid (HTF), and 2) HTF transmission to the city districts:

1. HTF is heated by burning gas in the furnace, which is then distributed to the rural area. Gas flow is related to the burning temperature, which is controlled by gas flow valve A2 (see Fig. 3). To automate the burning process, an operator sets a setpoint with the desired fluid temperature level. The S7-1200 PLC (4) compares setpoint temperature with the actual heat transfer fluid temperature at sensor S4. Based on that, S7-1200 PLC controls the gas-burning temperature (S2) by adjusting gas flow controller (A2). This system has been designed with limits for maximum temperature and pressure, exceeding these values inflict damage to the heating plant. If temperature or pressure values reach a set threshold, S7-1200 automation logic protects the physical system by stopping the gas flow to safeguard against the damage;

2. The HTF transmission depends on the heating process. When the temperature of the HTF reaches 60°C in the transmission line, the circulation pump A1 switches on and heating valve A3 opens. In this phase, heating system is fully operational and heat is delivered to the city districts. However, this part of the system may be damaged irreversibly if the circulation pump operates with the heating liquid valve (A3) closed. It has to be noted, that the concept of damage in these phases relates to logical damage from the attack scenario perspective and no actual damage is inflicted on the CR elements.

Heating process control logic is handled by Siemens Simatic PLC S7-1200 (see Fig. 2). CR prototype is built to be easily reproducible with no additional hardware, sensors, or actuators attached to S7-1200. Instead, the physical process is simulated using the hardware-in-the-loop (HIL) method, which is based on a simplified model of the heating process. HIL includes and controls nominal values of the physical process so that it may be damaged if these values are exceeded, therefore both the control and HIL programs run on the same physical device. These programs are separated so that control logic may only
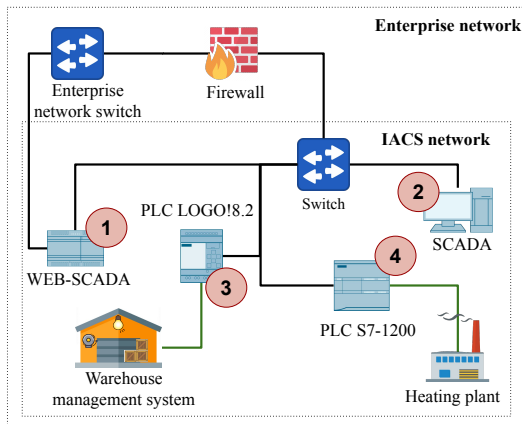
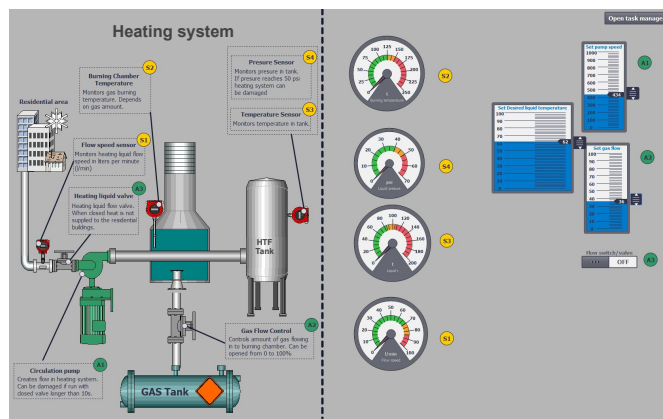Figure 2: The created CR prototype network topology.

Figure 3: Designed SCADA visualization screen.

Table 2: List of elements and their system description used in CR.

Nr.	Element	System description	MLFB order code	Approx. price, EUR
1	WEB-SCADA	NodeRed V1.0.0	n/a	0,00
		Yocta Linux V2.6	n/a	0,00
		IOT2040	6ES7647-0AA00-1YA2	210,00
2	SCADA	Siemens, SIMATIC WinCC Advanced V15.1	6AV2102-0AA05-0AA5	Available as trial
		Windows 7 enterprise, SP1, Build 7601	n/a	0,00
		VirtualBox V6.0	n/a	0,00
3	PLC LOGO!	Siemens, LOGO! 8.2, Full versions: 1.82.02	6ED1052-1FB08-0BA0	100,00
4	PLC s7-1200	Siemens, SIMATIC S7-1200, CPU 1215C	6ES7215-1AG40-0XB0	700,00

interact with heating process simulation as if through sensors and actuators (Fig. 3). For this reason, part of the controller responsible for physical system simulation is off-limits for the CR participants. PLC program is structured in two parts. The first contains control functions that monitor temperature pressure and flow speed from sensors and ensure that setpoint temperature is reached and maintained. The second has physical simulation functions which simulate how the temperature pressure and flow speed are changing and interacting with each other to mimic physical processes in a heating system. Siemens TIAportal project files, including PLC configuration, used in this CR prototype have been made publicly available on GitHub repository frostyICS [1].

4.2 Warehouse Management

Warehouse management in this CR prototype is used to control alarms and lights, which is a much simpler

process than the heating plant. The control is provided by Siemens LOGO! 8.2 PLC since it is meant for simple applications. LOGO! can have different configurations depending on added functional modules. In this CR, LOGO! 8.2 basic module (Tab. 3) is used with built-in I/O and communication interface. Created program logic implements Modbus/TCP and S7comm protocol communications to control the physical digital outputs, however, these outputs are not connected to any physical actuators and the actions are being simulated.

4.3 Supervision and Control of Systems

SADA permits an operator to visualize and interact with the process, and this supervisory control system in the CR prototype is handled two SCADA devices (see Fig. 2): 1) SCADA used to control and monitor the heating plant, and 2) WEB-SCADA for monitoring and controlling the warehouse management system and displaying a simple indication of the heat plant state.

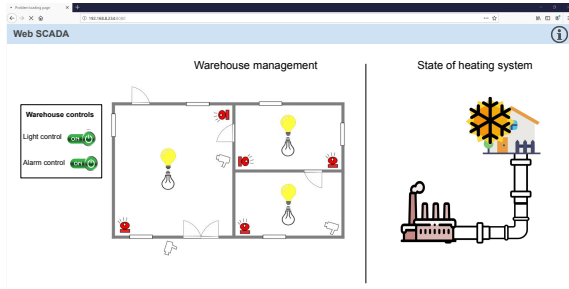[1] frostyICS - https://github.com/austrisu/frostyICS

Figure 4: Created warehouse management system visualization.

Heating plant SCADA is visualized using WinCC advanced V15.1 run-time (Fig. 3), which is the run-time of the HMI and SCADA system for use on MS Windows systems. WinCC software communicates with an automation system, reads a data block, displays process visualization, and allows an operator to interact with the automation system. WinCC runtime resides on virtualized Windows 7 workstation (Fig. 2 (2)).

Warehouse management WEB-SCADA is different from conventional SCADA as it utilizes web technologies for visualization and usually can be accessible as a web page. In this CR prototype, the authors utilize NodeRed to create WEB-SCADA interface, which is a common solution for low-budget projects. NodeRed is a low-code platform, where programming is similar to functional block diagram (FBD). NodeRed is suitable for simple custom system solutions sometimes encountered in IACS. Additionally, NodeRed is used in RevolutionPI, which is a RaspberryPi based PLC for prototyping industrial automation projects. The created NodeRed application communicates with LOGO! 8.2 to display and control warehouse lights and alarms. Additionally, WEB-SCADA collects and visualizes data from LOGO! regarding the heating plant state (Fig. 4).

The WEB-SCADA application resides on the Siemens IOT2040 hardware (Fig. 2 (1)), a budget industrial computer designed to withstand industrial environments. IOT2040 has two network interfaces which are used to introduce an intentional misconfiguration by connecting one interface directly to the enterprise network, bypassing the IACS firewall (Fig. 2). This misconfiguration of the CR prototype network represents an intentional or incorrect network configuration bypassing the intended security mechanisms. The authors believe that such security vulnerabilities may arise in an IACS segment, where automation engineers sometimes neglect IT safety procedures.

4.4 Communication Layout

Communication scheme is presented in figure 2 and table 3 summarizes the communication services used on IACS elements. To represent a realistic industrial communication network, the CR prototype utilizes two main industrial protocols – Modbus/TCP and S7comm, which are commonly seen in different IACS networks. S7comm usage is bound to Siemens equipment as most of the Siemens components can communicate using this protocol.

Modbus/TCP is an open-source protocol initially used to work with serial communication, but with TCP/IP protocol stack introduction in the IACS field, Modbus was adopted to work with this protocol stack. Modbus/TCP has become as one of the widely adopted industry standards for transferring digital and analog input/output (I/O) information. Detailed information about this protocol is described in technical specifications (Modbus, 2021; Dube and Camerini, 2002).

S7comm protocol is a Siemens proprietary protocol and does not have a publicly available detailed official documentation. However, due to its popularity, it has been reverse-engineered and thoroughly described in different documents and publications (Wireshark, 2021; Miru, 2016a; Miru, 2016b; Biham et al., 2019; Snap7, 2021).

5 VERIFICATION

Created CR prototype was used to conduct an offensive cybersecurity exercise for a treining audience, to validate its functionality and applicability to knowledge and practical skill development. This section describes the validation exercise attack scenario, possible attack vectors, and execution steps.

5.1 Threat Scenario

Based on performed literature review identified outcomes, training audience, within a defined attack scenario (Section 5.3), conducts attacks through a broad variety of routes, such as, the Internet, business or enterprise networks, and at the level of field devices target the IACS systems. After gaining initial foothold into the target network, attackers may traverse the network until access to the IACS systems is obtained. Authors in the research (Zhu et al., 2011) state that common attack vectors are backdoors, rootkits, holes in network perimeter, vulnerabilities in standard protocols, communications hijacking, and man-in-the-middle attacks. These considerations are taken into

Table 3: Communication partners and services running on IACS elements.

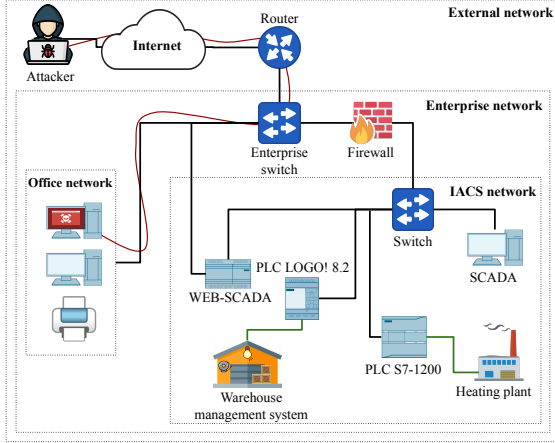| Nr.	Component	Interaction partner	Protocol support
1	SCADA	WEB-SCADA	S7comm, FTP
2	WEB-SCADA	PLC S7-1200, Office workstations	Modbus/TCP, HTTP, SSH
3	PLC LOGO! 8.2	PLC S7-1200, WEB-SCADA	S7comm, Modbus/TCP
4	PLC S7-1200	SCADA, WEB-SCADA	S7comm, Modbus/TCP

Figure 5: Created IACS CR prototype threat scenario topology.

account when deciding the initial position of the attacker within the exercise threat scenario. Within this exercise scenario, it is assumed that the attacker has already gained persistent access to the enterprise network and has established an internal pivot point inside the office network. Gaining this initial position is assumed within the threat scenario to be already reached by the attacker and is out of scope for this research as it does not contribute towards IACS specific attack execution. The initial state of the scenario is shown in figure 5. In this scenario enterprise network is divided into two segments – one is the office network, where the attacker has gained initial access and has established a command and control channel, and second is the IACS network including the heating plant and warehouse management systems.

In this scenario, the exercise participant plays as a member of the cyber red team, which has two main objectives: 1) switch off warehouse lights and alarm preventing system recovery, and 2) damage heating plant preventing system recovery.

5.2 Attack Structure

The MITRE ATT&CK (MITRE ATT&CK®, 2021) TTPs knowledge-base is used to provide structure to preformed attacks within threat scenario. This knowledge-base is used to describe adversary's actions to gain further access, compromise, and operate

within the target network. MITRE ATT&CK framework provides consistent considerations to classify the attacker's goals, tasks, and steps, therefore being applicable for modelling attack steps needed to reach the specified objectives within the scenario.

A summary for the applicable tactics derived from MITRE ATT&CK framework and used in the prototype exercise scenario are divided among each network segment:

Tactics in the office network:
1. Discovery: searching for available devices in the office network;
2. Lateral movement: exploiting and spreading to other devices;
3. Persistence: gaining stable access to the devices;
4. Command and control: use of techniques to establish the communication with the compromised system.

Tactics in the IACS network:
1. Discovery: searching for available devices in the IACS network, and discovering open ports and IACS processes controlled by the IACS network;
2. Collection: extracting detailed information about IACS elements and their purpose;
3. Impact: actions on objectives.

5.3 Attack Execution Scenario

For the attacker to disrupt the operation of the warehouse and heating plant controls, the following staged attack execution scenario was designed and implemented in the CR prototype:
1. Discovery in office network: This is the initial phase with the attacker's starting position in the office network (Fig. 5). Based on the MITRE ATT&CK knowledge-base, the attacker may perform network scanning and enumeration to identify services running on remote hosts. During this step the main target is WEB-SCADA (IOT2040) device;
2. Lateral movement: During this phase, the attacker exploits a common misconfiguration of NodeRed application to gain a foothold on the WEB-SCADA (IOT2040) device and change the position in the network (Fig. 5);
3. Persistence: The attacker establishes persistent

administrative access by exploiting misconfigured user rights on WEB-SCADA (IOT2040), from where the attacker has the possibility to propagate further to the IACS network;

4. Command and control: In this step, the attacker exploits misconfigured network topology where WEB-SCADA has two network interfaces and one of them is directly connected to the IACS network bypassing the firewall. Attacker configures WEB-SCADA (IOT2040) to redirect traffic from the attacker to the target IACS network bypassing firewall;

5. Discovery in IACS network: In this stage, the attacker tries to enumerate devices in the IACS environment and learn about the internal network;

6. Objective Nr.1 - the attack on the warehouse: The attacker attempts to get information about the target warehouse management system controlled by LOGO! 8.2. Afterwards, the attacker attempts to manipulate, disrupt, or impair IACS systems and controlled physical processes by sending crafted raw Modbus/TCP commands to LOGO! 8.2. Furthermore, attacker performs a denial of service attack against LOGO! 8.2 by exploiting buffer overflow vulnerability in PLC web server;

7. Objective Nr.2 - the attack on heat plant: During this stage, the attacker tries to get information about the target heating plant system controlled by S7-1200 PLC (Fig. 5). The attacker exploits a lack of authentication for PLC, hence using rough TIAportal downloads configuration from PLC. Gained configuration facilitates attacker to obtain contextual feedback and how the physical system operates. During the impact stage, the attacker attempts to manipulate, disrupt or impair IACS systems and controlled physical processes. The main vulnerabilities of S7-1200 are bound to the S7comm protocol and to exploit these vulnerabilities, the attacker needs to understand the control logic program structure, which was gathered during the collection phase. From the downloaded S7-1200 program, the attacker may determine which defined tags are responsible for specific physical function control. The attacker may send crafted S7comm requests to the PLC by using a Python script using Snap7 library bindings[2]. This attack exploits the lack of authentication of the s7comm protocol. Python script example for this scenario is located in GitHub[3]. This attack process may be divided into two steps

[2]PyPi Python-Snap7 - https://pypi.org/project/python-snap7/

[3]S7comm attack proof-of-concept scripts. - https://github.com/austrisu/ICS_poc
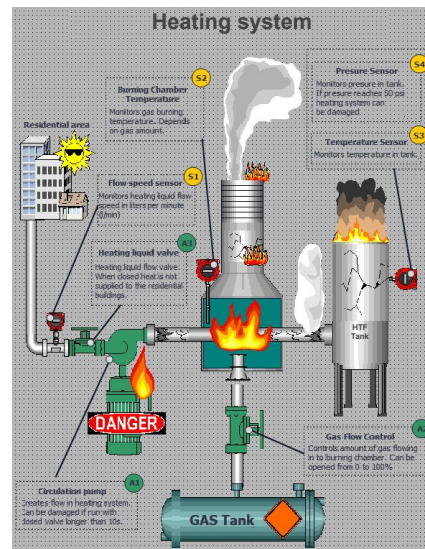
Figure 6: Heating system state seen in the SCADA after attack to S7-1200 PLC created by the author.

- the first one focusing on inflicting damage to the circulation pump (Fig. 3 A1), and the second aiming to damage the whole heating system. After a successful execution of the attack, the SCADA screen should visualize a damaged simulated heating plant (Fig. 6). Successful execution of these attacks results in impairment of the physical process and recovery, from a scenario perspective, may be made only by a physical repair. However, as the physical process is simulated then no damage is done to actual CR physical devices and they may be easily restored to the initial configuration.

The goal of the created IACS CR was to provide an environment, where participants may practice offensive capabilities, in a game-based exercise, against IACS elements and observe their impact. After the two-day training and exercise, the participants in the collected feedback indicated that the created CR prototype environment is a perfect testbed for experimentation and development of offensive capabilities in the IACS field. Furthermore, the participants clearly indicated that their confidence and knowledge had increased after the two-day training session.

This work was recognized as a high importance by representatives from national energy operators, national mobile telecommunication operator, national cert, national armed forces, and universities.

6 CONCLUSION AND FUTURE WORK

This paper reviews the newest publicly available IACS testbeds and based on identified gaps and requirements derived the criteria for the CR testbed prototype. Based on this, an actual novel prototype of a cyber range was designed and created for red team offensive capability development in game-based exercise in the IACS field, thereby improving understanding of IACS red team tactics and techniques. This understanding of red team capabilities also provided knowledge and practical capabilities on how to defend IACS. The authors intend that individuals and private or government entities may utilize this CR for offensive exercises development by any suitable means. The created CR prototype has been successfully validated by the authors by the developing and conducting an offensive cyber red team validation exercise for a dedicated training audience. The future work would include pursuing the directions of automated threat scenario creation and generated configuration deployment on IACS CR elements to allow customizable training experience and variety of possible scenario variations based on the same testbed elements.

ACKNOWLEDGEMENT

REFERENCES

Adepu, S., Kandasamy, N. K., and Mathur, A. (2019). EPIC: An electric power testbed for research and training in cyber physical systems security. In Katsikas, S. K., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Antón, A., Gritzalis, S., Mylopoulos, J., and Kalloniatis, C., editors, *Computer Security*, pages 37–52. Springer International Publishing.

Almgren, M., Andersson, P., Björkman, G., Ekstedt, M., Hallberg, J., Nadjm-Tehrani, S., and Westring, E. (2019). RICS-el: Building a national testbed for research and training on SCADA security (short paper). In Luiijf, E., Žutautait{\textbackslash}.e, I., and Hämmerli, B. M., editors, *Critical Information Infrastructures Security*, pages 219–225. Springer International Publishing.

Alves, T., Das, R., Werth, A., and Morris, T. (2018). Virtualization of SCADA testbeds for cybersecurity research: A modular approach. *Computers & Security*, 77:531 – 546.

Alves, T. R., Buratto, M., de Souza, F. M., and Rodrigues, T. V. (2014). Openplc: An open source alternative to automation. In *IEEE Global Humanitarian Technology Conference (GHTC 2014)*, pages 585–589.

Bergman, D. C., Jin, D., Nicol, D. M., and Yardley, T. (2009). The virtual power system testbed and inter-testbed integration. In *Proceedings of the 2nd Conference on Cyber Security Experimentation and Test*, CSET'09, page 5, USA. USENIX Association.

Biham, E., Bitan, S., Carmel, A., Dankner, A., and Malin, U. (2019). Rogue7: Rogue engineering-station attacks on s7 simatic plcs. *BlackHat*.

Chromik, J. J., Remke, A., and Haverkort, B. R. (2018-11-06). An integrated testbed for locally monitoring SCADA systems in smart grids. *Energy Informatics*, 1(1):56.

CISA (2021). Compromise of u.s. water treatment facility. https://us-cert.cisa.gov/ncas/alerts/aa21-042a. Accessed: 13.03.2021.

Dube, D. and Camerini, J. (2002). Modbus application protocol. https://datatracker.ietf.org/doc/html/draft-dube-modbus-applproto-00. Accessed:15.05.2021.

FireEye (2021). Advanced persistent threat groups. https://www.fireeye.com/current-threats/apt-groups.html. Accessed: 13/03/2021.

Formby, D., Rad, M., and Beyah, R. (2018). Lowering the barriers to industrial control system security with GRFICS. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*, Baltimore, MD. USENIX Association.

Fovino, I. N., Masera, M., Guidi, L., and Carpi, G. (2010). An experimental platform for assessing scada vulnerabilities and countermeasures in power plants. In *3rd International Conference on Human System Interaction*, pages 679–686.

Geng, Y., Wang, Y., Liu, W., Wei, Q., Liu, K., and Wu, H. (2019). A survey of industrial control system testbeds. *IOP Conference Series: Materials Science and Engineering*, 569:042030. Publisher: IOP Publishing.

Giuliano, V. and Formicola, V. (2019). Icsrange: A simulation-based cyber range platform for industrial control systems. *CoRR*, abs/1909.01910.

Gold, J. (2020). The five eyes and offensive cyber capabilities: Building a 'cyber deterrence initiative'. Technical report, NATO CCDCOE.

Green, B., Lee, A., Antrobus, R., Roedig, U., Hutchison, D., and Rashid, A. (2017). Pains, gains and plcs: Ten lessons from building an industrial control systems testbed for security research. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*, Vancouver, BC. USENIX Association.

Gunathilaka, P., Mashima, D., and Chen, B. (2016). Softgrid: A software-based smart grid testbed for evaluating substation cybersecurity solutions. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, CPS-SPC '16, page 113–124,

New York, NY, USA. Association for Computing Machinery.

Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S., and Higdon, M. (2010). Development of the powercyber scada security testbed. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*.

Holm, H., Karresand, M., Vidström, A., and Westring, E. (2015). A survey of industrial control system testbeds. In Buchegger, S. and Dam, M., editors, *Secure IT Systems*, pages 11–26. Springer International Publishing.

Kaspersky Lab (2021a). Apt attacks on industrial companies in 2020. Technical report, AO KASPERSKY LAB.

Kaspersky Lab (2021b). Threat landscape for industrial automation systems. Technical report, AO KASPERSKY LAB.

Koganti, V. S., Ashrafuzzaman, M., Jillepalli, A. A., and Sheldon, F. T. (2017). A virtual testbed for security management of industrial control systems. In *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*, pages 85–90.

Korkmaz, E., Dolgikh, A., Davis, M., and Skormin, V. (2016). Industrial control systems security testbed. In *11th Annual Symposium on Information Assurance*.

Krishnan, S. and Wei, M. (2019). SCADA testbed for vulnerability assessments, penetration testing and incident forensics. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6.

Larrucea, X. and Molinuevo, A. (2020). An ICS based scenario generator for cyber ranges. In Yilmaz, M., Niemann, J., Clarke, P., and Messnarz, R., editors, *Systems, Software and Services Process Improvement*, pages 543–554. Springer International Publishing.

Lewis, J. A. (2015). The role of offensive cyber operations in nato's collective defence. *The tallin papers*.

Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., and Hariri, S. (2011). A testbed for analyzing security of scada control systems (tasscs). In *ISGT 2011*, pages 1–7.

Mathur, A. P. and Tippenhauer, N. O. (2016). Swat: a water treatment testbed for research and training on ics security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, pages 31–36.

Miru, G. (2016a). The siemens s7 communication - part 1 general structure. http://gmiru.com/article/s7comm/. Accessed: 27.04.2021.

Miru, G. (2016b). The siemens s7 communication - part 2. http://gmiru.com/article/s7comm-part2/. Accessed:15.05.2021.

MITRE (2021). Apt groups. https://attack.mitre.org/groups/. Accessed: 13/03/2021.

MITRE ATT&CK® (2021). Mitre att&ck®. https://attack.mitre.org/. Accessed: 01.04.2021.

Modbus (2021). Modbus official technical resources. https://www.modbus.org/tech.php. Accessed:15.05.2021.

Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., and Reddi, R. (2011). A control system testbed

to validate critical infrastructure protection concepts. *International Journal of Critical Infrastructure Protection*, 4(2):88 – 103.

Muller, L. P. (2019). Military offensive cyber-capabilities:small-state perspectives. Technical report, Netherlands.

Noorizadeh, M., Shakerpour, M., Meskin, N., Unal, D., and Khorasani, K. (2021). A cyber-security methodology for a cyber-physical industrial control system testbed. *IEEE Access*, 9:16239–16253.

Pfrang, S., Kippe, J., Meier, D., and Haas, C. (2017). Design and architecture of an industrial IT security lab. In Guo, S., Wei, G., Xiang, Y., Lin, X., and Lorenz, P., editors, *Testbeds and Research Infrastructures for the Development of Networks and Communities*, pages 114–123. Springer International Publishing.

Reaves, B. and Morris, T. (2012). An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11.

Rosa, L., Cruz, T., Simões, P., Monteiro, E., and Lev, L. (2017). Attacking SCADA systems: A practical perspective. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, pages 741–746.

Rubio-Hernan, J., Rodolfo-Mejias, J., and Garcia-Alfaro, J. (2017). Security of cyber-physical systems. In Cuppens-Boulahia, N., Lambrinoudakis, C., Cuppens, F., and Katsikas, S., editors, *Security of Industrial Control Systems and Cyber-Physical Systems*, pages 3–18. Springer International Publishing.

Snap7 (2021). Step7 open source ethernet communication suite. http://snap7.sourceforge.net/. Accessed:15.05.2021.

Stamp, J., Urias, V., and Richardson, B. (2011). Cyber security analysis for the power grid using the virtual control systems environment. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–4.

Stranahan, J., Soni, T., and Heydari, V. (2019). Supervisory control and data acquisition testbed for research and education. In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0085–0089.

Su, W., Antoniou, A., and Eagle, C. (2017). Cyber security of industrial communication protocols. In *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–4.

Tao, Y., Xu, W., Li, H., and Ji, S. (2019). Experience and lessons in building an ICS security testbed. In *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, pages 1–6.

UK Government (2016). National cyber security strategy 2016-2021. Technical report, UK.

Urdaneta, M., Lemay, A., Saunier, N., and Fernandez, J. (2018). A cyber-physical testbed for measuring the impacts of cyber attacks on urban road networks. In Staggs, J. and Shenoi, S., editors, *Critical Infrastructure Protection XII*, pages 177–196. Springer International Publishing.

Werth, A. W. and Morris, T. H. (2021). Prototyping PLCs and IoT devices in an HVAC virtual testbed to study

impacts of cyberattacks. In Yang, X.-S., Sherratt, R. S., Dey, N., and Joshi, A., editors, *Proceedings of Fifth International Congress on Information and Communication Technology*, pages 612–623. Springer Singapore.

Wireshark (2021). S7 communication (s7comm). https://wiki.wireshark.org/S7comm. Accessed: 27.04.2021.

Xie, Y., Wang, W., Wang, F., and Chang, R. (2018). VTET: A virtual industrial control system testbed for cyber security research. In *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–7.

Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C., and Zhang, W. (2018). Kill chain for industrial control system. *MATEC Web Conf.*

Zhu, B., Joseph, A., and Sastry, S. (2011). A taxonomy of cyber attacks on scada systems. In *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, pages 380–388.