VALMIERA UNIVERSITY OF APPLIED SCIENCES

ENGINEERING FACULTY

INDUSTRIAL AND AUTOMATION CONTROL SYSTEM CYBER RANGE FOR OFFENSIVE CAPABILITY DEVELOPMENT

MASTER THESIS

Author: Austris Uljāns

Student number: KI19006

Supervisor: Dr.comp.sc. Bernhards Blumbergs

VALMIERA 2021

CONTENTS

ANOTĀCIJA (LV)

Autors: Austris Uljāns, Studenta numurs: KI19006,
Vadītājs: Dr.comp.sc. Bernhards Blumbergs,
Darba nosaukums: Industriālās un automātikas kontroles sistēmas kiberdrošības testēšanas laboratorija uzbrukuma spēju attīstīšanai.

Šis maģistra darbs ir rakstīts angļu valodā un kopā satur 96 lapaspuses, septiņas nodaļas, 12 tabulas un 16 attēlus un četrus pielikumus.

Industriālās un automatizācijas kontroles sistēmas (IAKS) vada un pārrauga dažādas sistēmas sākot no ražošanas procesiem līdz pat enerģijas pārvades tīkliem. Tādēļ, ka IAKS vada kritiskus procesus mūsu sabiedrībā, kiber uzbrukumiem, mērķētiem uz IAKS sistēmām, var būt katastrofālas sekas. Risku palielina arī tas, ka IAKS sistēmas attīstās un tiek integrētas ar tradicionālajām IT sistēmām, kas padara tās ar vien sasniedzamākas uzbrucējiem.

Pētījuma mērķis ir izveidot reālistisku un viegli atkārtojamu IAKS kiberdrošības poligonu, kas palīdz attīstīt uzbrukuma spējas.

Lai radītu pamatu jaunas kiberdrošības laboratorijas izveidei, darba teorētiskajā daļā tiek apskatīti līdz šim izveidoto IAKS kiberdrošības laboratoriju tendences, arhitektūra un scenāriji. Praktiskajā daļā autors izveido IAKS kiberdrošības testēšanas poligonu, ko arī izmanto mācībās. Autora galvenais secinājums ir tāds, ka IAKS kiberdrošības poligons ir vērtīgs rīks, lai izprastu un izmēģinātu uzbrukuma veidus, ko uzbrucēji var izmantot IAKS tīklos, lai nodarītu kaitējumu industriālajiem procesiem.

ANNOTATION (ENG)

Author: Austris Uljāns, Student number: KI19006,
Supervisor: Dr.comp.sc. Bernhards Blumbergs,
Thesis title: Industrial and automation control system cyber range for offensive capability development.

This thesis is written in the English language and has 96 pages, includes seven chapters, 12 tables, 16 figures and four annexes.

Industrial and automation control systems (IACS) are utilized, starting from manufacturing processes to energy transmission. As IACS controls critical infrastructures, attacks on these systems can have devastating effects. Moreover, IACS systems are evolving by creating connections to conventional IT infrastructures what increase adversary access to industrial systems.

The research objective is to develop a realistic and easily reproducible IACS cyber range for offensive exercise development.

The theoretical part of the work studies the concepts, trends, architecture, and scenarios of previously created IACS cyber ranges to create the basis for cyber range development. The author creates IACS cyber range in the practical part and uses it to conduct offensive capability development training. From the gathered information, the author's main conclusion is that IACS cyber ranges are a viable tool for understanding and trying tactics and techniques attackers may use to gain access to the IACS network and damage physical processes.

Аннотация (RU)

Автор: Austris Uljāns, Номер студента: KI19006,
Руководитель: Dr.comp.sc. Bernhards Blumbergs,
Название диссертации: Промышленная и автоматизированная система управления кибернетическим диапазоном для развития наступательного потенциала.

Эта диссертация написана на английском языке и имеет страницы 96 включает семь глав, 12 таблиц, 16 рисунков и четыре приложения.

Используются промышленные и автоматизированные системы управления (СУПА), начиная с производственных процессов и заканчивая передачей энергии. Поскольку IAKS контролирует критические инфраструктуры, атаки на эти системы могут иметь разрушительные последствия. Кроме того, системы СУПА развиваются за счет создания соединений с обычными ИТ-инфраструктурами, что увеличивает доступ противника к промышленным системам.

Целью исследования является разработка реалистичного и легко воспроизводимого кибер-диапазона СУПА для разработки наступательных упражнений.

Теоретическая часть работы посвящена изучению концепций, тенденций, архитектуры и сценариев ранее созданных кибердиапазонов СУПА для создания основы для разработки кибердиапазонов. Автор создает кибер-полигон СУПА в практической части и использует его для проведения тренировок по развитию наступательного потенциала. Исходя из собранной информации, основной вывод авторов заключается в том, что кибер-диапазоны СУПА являются жизнеспособным инструментом для понимания и проверки тактики и методов, которые злоумышленники могут использовать для получения доступа к сети СУПА и повреждения физических процессов.

ACKNOWLEDGMENTS

I, the author, would especially like to thank:

- to my supervisor Dr.comp.sc. Bernhards Blumbergs, whose experience and support was invaluable while creating this research;
- to Vidzeme University of Applied Sciences for giving the chance to accomplish this thesis;
- to Siemens OY Latvian Branch and Riga Technical University for the lab equipment;
- to all of the organizations which showed interest in my research;
- to my colleagues and coursemates from mutual support and cooperation.

Very special thanks to my wife Baiba Uljāne, for her support and assistance in every step of my thesis. I also would like to thank my daughter, who joined us while writing my research, for giving me unlimited happiness and pleasure.

ACRONYMS

APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
BT	Blue Team
CNO	Computer Network Operation
CPS	Cyber Physical Systems
CR	Cyber Range
CVE	Common Vulnerabilities and Exposure
DB	Data Block
DNP3	Distributed Network Protocol 3
DoS	Denial of Service
EW	Electronic Warfare
FB	Function Block
FBD	Function Block Diagram
FC	Function
FTP	File Transfer Protocol
GrT	Gray Team
GT	Green Team
HIL	Hardware in the Loop
HMI	Human-Machine Interface
HTF	Heat transfer fluid
HTTP	HyperText Transfer Protocol
IACS	Industrial and Automation Control Systems
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IL	Instruction List

IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
LAD	Ladder logic
OB	Organization Block
OPC	Open Platform Communications
OT	Operational Technology
PDU	Protocol Data Unit
PLC	Programmable Logic Controller
PT	Purple Team
RQ	Research Questions
RT	Red Team
RTU	Remote Terminal Unit
S7comm	S7 Communication
SCADA	Supervisory Control and Data Acquisition
SCL	Structured Control Language
SFC	Sequential Function Charts
SSH	Secure Shell Protocol
SWaT	Secure Water Treatment
TTPs	Techniques, Tools and Procedures
WT	White Team
YT	Yellow Team

1. INTRODUCTION

The digital world nowadays is expanding with unprecedented speed. All fields of our lives are controlled and influenced by digital industries shaping them. This also applies to Industrial and Automation Control Systems (IACS) or also called ICS/SCADA. IACS are devices that operate Critical Infrastructures (CI), such as, electrical grids, gas distribution grids, nuclear power plants, water treatment, transportation, heating plants, and many more. In general, these systems enable efficient automation of the physical processes that businesses, industries, and countries relay. For that reason, IACS is also called Cyber Physical Systems (CPS) as they operate on physical structures. Typical characteristics of IACS systems are propitiatory protocols, isolated networks, and purpose-specific hardware. These systems have started to close the gap between traditional Information Technology (IT) systems by introducing IT elements, networks, and ideologies. Therefore nowadays, most IACS components cannot exist without communication with different parts of the system. This development has made IACS a target to various adversaries. Moreover, some industrial and automation control systems include characteristics of Internet of Things (IoT) devices that increase the attack surface even more.

Each year IACS receives an increasing number of sophisticated and debilitating attacks, one of such attacks happened recently on February 5th, 2021, where actors gained access and seized control of drinking water treatment facilities in the USA (CISA, 2021). Many similar incidents are widespread, and the most popular of them are Stuxnet, Duqu, Flame, BlackEnergy, Triton, Lazarus, and MuddyWater (Geng et al., 2019; Kaspersky Lab, 2021a). Furthermore, an indicator that cyber-attacks and warfare are escalating in all fields is an increase in identified actors (FireEye, 2021; MITRE, 2021). The review “APT attacks on industrial companies in 2020” (Kaspersky Lab, 2021a) shows an increase in Advanced Persistent Threat (APT) activity in the year 2020 targeted to IACS infrastructure and lists various attacks like Sofacy, PoetRAT, Mikroceen, Lazarus, SolarWinds, MuddyWater as few of the important ones. Kaspersky Labs report (Kaspersky Lab, 2021c) also confirmed a 62% increase of attacks on IACS in the past year. The same report suggests that threats belonging to more than 5 thousand malware families

were blocked on IACS workstations.

Based on current trends, report "ICS threat predictions for 2021" (Goncharov, 2021) speculates that cybercriminals will increase unconventional attack scenarios and create new ways to monetize the attacks. As most upfront global danger for IACS is the end of support for widely used MS Windows 7 and MS Windows Server 2008, and also recently leaked Windows XP source code. Huq et al. (Huq et al., 2018) has used search engine Shodan [1] to discover that in IACS MS Windows 7/8 is used in 51.56% and Windows XP is used in 8.75% of total workstations used in IACS. Hence, confirming the high usage of these OS. Goncharov (Goncharov, 2021) also mentions that an increase in ransomware attacks, cyber espionage, APT operation, and Covid19 consequences are on the rise.

There is still 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 or cyber ranges to test attack and defense mechanisms in a controlled environment. IACS cyber ranges and testbed numbers are increasing as the trend of IACS security progresses. Krishnan and Wei (Krishnan & Wei, 2019) indicate that a literature vacuum exists around IACS cyber ranges, making them inaccessible for the broader community to gain more experience in the defense and offense of IACS components.

Offensive capabilities are deliberate invasions into opponent systems to cause destruction, disruption, or damage. Lewis (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 states' 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 the development of offensive capabilities.

1.1. Problem statement and objective

This master thesis addresses the problem in the field of cyber red team's offensive capability development. Only some of the nations as the UK, Netherlands, USA, Canada, and Australia have

[1] Shodan - https://www.shodan.io/

publicly expressed having offensive capabilities (Gold, 2020; Muller, 2019; UK Government, 2016). However, the disclosed information is not detailed enough, making it impossible to understand their potential. Nonetheless, it is well known that in the past decade number of attacks by nation-state actors has steadily been on the rise (Kaspersky Lab, 2021c). Thereby the problem addressed in the author's research is that *red team offensive capabilities in the IACS field are yet to be closely studied to gain more insights into how IACS elements can be attacked and defended.* Current studies mainly focus on defensive capability development in the IACS field, which is understandable, considering that blue team defenses need to be up-to-date and on full alert to counter adversary attacks. However, research and reports point out that national states should maintain offensive capabilities as a political tool to deter any tensions directed at themselves or allayed countries. If necessary, offensive capabilities can be used to respond to aggressors with destructive power. Additionally, report "The role of offensive cyber operations in NATO's collective defence" (Lewis, 2015) mentions that modern warfare cannot exist without Electronic Warfare (EW) support. In addition from governments, offensive capabilities are necessary for companies utilizing IACS, as they need to know how to test and protect their infrastructure.

Based on the problem, the objective of the master thesis is to develop the IACS Cyber Range (CR), where the red team can practice developing offensive capabilities. CR need to encompass the following key aspects:

- realistic;
- easy reproducible;
- with publicly available documentation;
- supporting multi-stage attack scenarios.

The created CR can be used to create exercises for red team offensive capability development in the IACS field, thereby improving understanding of IACS red team tactics and techniques. Understanding red team's capabilities also provides knowledge on how to defend IACS. The author intends that private or government entities can utilize this CR for exercises to develop offensive capabilities by any means is suitable for them.

1.2. Research questions

In this thesis following Research Questions (RQ) are addressed:

1. What are the main objectives IACS cyber ranges and testbeds are created for?
2. What are the IACS cyber range development criteria?
3. How IACS cyber rages are built to resemble realistic systems?

The answers to these three RQ's are used to propose tentative means of constructing a high fidelity, easily reproducible IACS CR meant for red team offensive capability development.

1.3. Research scope

The scope of the research includes:

1. Review of previous IACS CR and testbed research;
2. Development of the IACS CR based on thesis objective;
3. Created IACS CR usage in exercises for red team offensive capability development.

1.4. Road map

Work will be structured as follows:

- Background and related work - explains the essential background of IACS system cybersecurity and studies related work done in IACS CR and testbed fields. This chapter also describes cyber operations with emphasis on offensive operations;
- IACS CR design - describes the development of IACS CR, used components, and operating principles. Design of CR are also available publicly in GitHub[2];
- Attack design - describes conducted offensive cybersecurity exercise utilizing IACS CR. This chapter describes attack scenario, possible attack vectors, and exercise execution steps;
- Economic justification - explains potential markets where the solution can be used together with an approximate cost of the CR.

[2]frostyICS - IACS CR for offensive capability development (https://github.com/austrisu/frostyICS)

2. BACKGROUND AND RELATED WORK

This chapter focuses on background and related work from academic and non-academic sources. Gaps of current studies are identified, and at the end of the chapter, contributions of the author's work are proposed.

2.1. IACS overview

IACS elements are distributed in so-called Operational Technology (OT) network. OT networks are distinguished between conventional IT systems as OT systems run a time-critical process where the smallest delay can cause system disruption. Research (Zhou et al., 2018) has summarized differences as displayed in the table 2.

2 Table: Difference between traditional IT system and IACS (Zhou et al., 2018).

Item	**IT System**	**IACS**
Operating Systems (OS)	General purpose OS (MS Windows, Linux, Unix)	Embedded OS (VxWorks, uClinux etc.), General purpose OS with reduced functionality.
Data exchange protocols	TCP / IP protocol stack	Field-specific proprietary and open-source protocols (DPN3, Modbus, OPC etc.) are used as an application layer of the TCP / IP stack or via the serial communication bus.
Real-time requirements	Low requirements for real-time data roundtrips	High requirements for real-time data round-trips, delays, or disruptions can be damaging.
System fault response	Response level dependent on IT system requirements	Interruption can cause financial and physical loss.

Item	IT System	IACS
System upgrades	Almost all the systems are relatively easy to upgrade.	Due to poor hardware compatibility, upgrades usually are not advised.

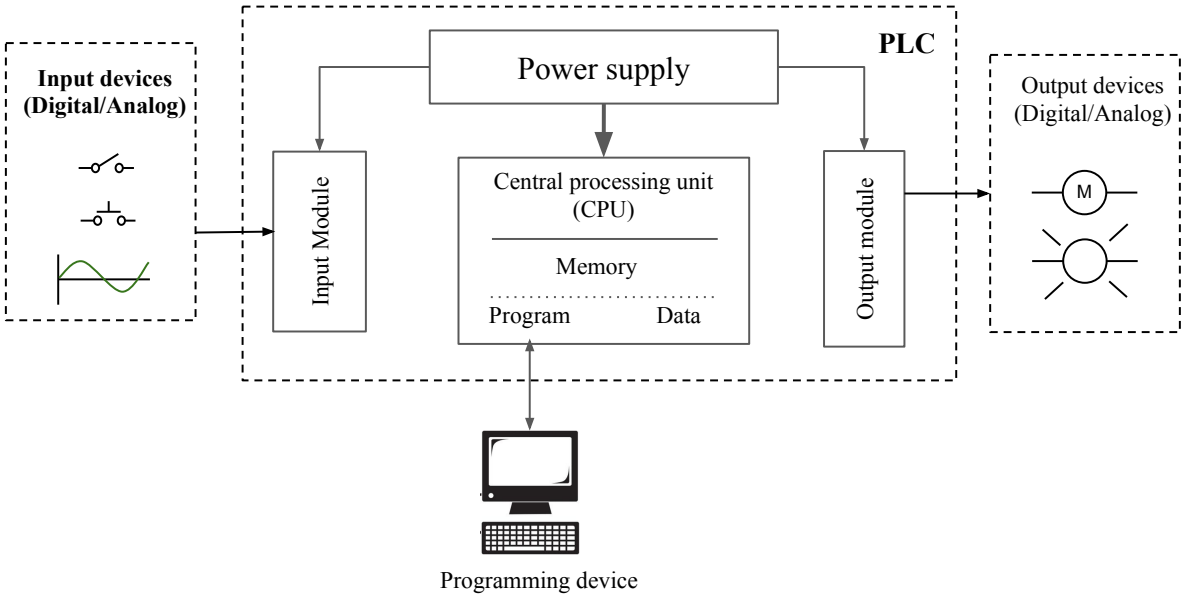
The common components making up an IACS system are as follows (Ukwandu et al., 2020):

- Programmable Logic Controller (PLC);
- Human-Machine Interface (HMI);
- Supervisory Control and Data Acquisition (SCADA) workstations;
- Intelligent Electronic Device (IED);
- Remote Terminal Unit (RTU);
- Data historians.

The main control elements in a cyber-physical system are usually PLC, which receives external inputs, performs a logic operation, and acts on outputs accordingly. The high-level process of PLC is shown in figure 1.

PLC is a programmable device. Nowadays, the programming of PLC is performed by general purpose PC, which runs programming software. Programs usually can be created in five standardized IEC61131-3 languages (RealPars, 2021):

- Ladder logic (LAD) - graphical language, which imitates the behavior of electromechanical relay contacts. It was common in early automation designs. LAD can also perform more sophisticated operators as implementing timers, counters, cooperators, mathematical functions, moving operations of memory segments, signal conversions, etc.;
- Function Block Diagram (FBD) - graphical language, where chained function blocks visualize the logic decision flow from one block to another;
- Structured Control Language (SCL) - text-based programming language which is derived from pascal;
- Sequential Function Charts (SFC) - graphical block diagram-based language where the program is structured as a flowchart;
- Instruction List (IL) - text-based programming language which closely resembles assembler. It is mostly used for compact and time-critical programs.



1 Figure: High level overview of PLC operation (Siemens, 2007).

Program for PLC is compiled for the actual hardware of the PLC that will control the physical process. Thus, the control layer is mapped to the cyber-layer, and it exists in actuality as a compiled program in binary machine code. It resides in the memory of the PLCs hardware and is processed by the CPU of the hardware. In the real system, the PLC is connected to actuators and sensors that operate a physical process (RealPars, 2020). This can be seen in figure 1.

Visualization in IACS is done by a HMI or SCADA. HMI is usually a purpose-built physical PC with a built-in display to visualize the physical process and allows for the operator to interact with the process. SCADA typically is computer software installed on a general-purpose PC or server that allows the operator to oversee the physical process and interact with it. SCADA also can be used to collect and visualize the data from geographically distributed control systems.

It is worth mentioning that the term SCADA is often used misleading as SCADA is usually computer software installed on a workstation, allowing the operator to monitor and interact with the system. SCADA workstations can be installed locally or in a wide area like an electrical grid. Wide-area SCADA has more components to allow connections to remote sites, including RTUs, which serve as information gateways between end devices and SCADA workstations. Thus, when research usually mentions SCADA, it means SCADA networks with vastly interconnected field devices which send data to the central control center.

According to research (Giuliano & Formicola, 2019) IACS security is a significant challenge. Firstly, the complexity and diversity of devices involved in the IACS increase the attack surface. For example, an attacker might strike the cyber-part, the physical part, or both parts of the IACS.

As indicated by Larrucea and Molinuevo (Larrucea & Molinuevo, 2020) until 2020, 60% of manufacturing companies have been subject to cyberattacks, and almost a third of them suffered financial loss and, as a result, disruption of the business.

Giuliano and Formicola (Giuliano & Formicola, 2019) express a point of view that the issues in IACS security results from the interdisciplinary nature of the problem. It is challenging to bring together experts from different fields, such as information security, information technologies, and automation engineering.

2.2. Literature review

This section will look at the overall research done on IACS testbeds, and afterwards, describe CRs with regards to architecture, objectives, purpose, and design considerations.

The systematic literature review aims to identify and evaluate the existing literature of scientific research regarding a particular research question or topic.

The objective of this literature review is to study the concepts, trends, architecture, and scenarios of previous research to determine shortcomings in the field of IACS CRs.

For the search of scientific articles, the author has used the following keywords: *IACS/ICS testbeds, IACS/ICS testbed reviews, SCADA cybersecurity testbed, IACS cyber range* . The author used IEEE and Scopus scientific databases and Google Scholar search engines to search for literature. As the IACS field develops quickly, five year period was chosen as an optimal time frame for literature review. Found papers were reviewed, and approximately 40 relevant articles and ten cited in these articles were deemed relevant and read through thoroughly.

2.2.1. Overview of current IACS cyber ranges

IACS systems usually are critical systems that cannot be offline or face failures during their operation. Thereby, Holm et al. (Holm et al., 2015) points out that the high availability requirements on IACS do not allow performing security tests on a live system. Craggs et al. (Craggs et al., 2019) presents a point that there is a lack of knowledge about the attack surfaces of overlapping OT/IoT/IT systems, possible vulnerabilities, and defense mechanisms that may mitigate risks of attacks to such overlapping systems. For this reason, researchers, corporations, and military institutions turn to cyber ranges that mimic real IACS.

Larrucea and Molinuevo (Larrucea & Molinuevo, 2020) state that developing cyber-security competencies through the use of CR and their use for research topics is of increasing interest.

In addition, CR is a tool that can help improve the stability, security, and performance strength of IT/OT systems. 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 against infrastructure.

According to the literature review, 28 created testbeds were found in the relatively new research. These testbeds are indicated in table 3.

3 Table: Cyber range overview (Chemical plant - C, Smart Grid - SG, Nuclear plant - N, General - G, Electrical Grid - G, Transportation - T, Manufacturing - M, Water Treatment - W).

Nr.	Name	Country	Year	Field	Type	Ref.
1	n/a	USA	2012	G	V	Reaves and Morris, 2012
2	n/a	USA	2017	EG	V	Koganti et al., 2017
3	n/a	USA	2016	EG	P	Korkmaz et al., 2016
4	VTET	China	2018	C	H	Xie et al., 2018
5	n/a	Qatar	2021	C	H	Noorizadeh et al., 2021
6	n/a	USA	2019	N, T	P	Stranahan et al., 2019
7	n/a	USA	2017	G	P	Su et al., 2017
8	MSICST	China	2019	G	P	Tao et al., 2019
9	n/a	Portugal	2017	EG	V	Rosa et al., 2017
10	n/a	USA	2019	C	P	Krishnan and Wei, 2019
11	IOSB	Germany	2017	M	H	Pfrang et al., 2017
12	EPIC	Singapore	2019	SG	P	Adepu et al., 2019
13	n/a	France	2017	EG	P	Rubio-Hernan et al., 2017
14	n/a	Netherlands	2018	EG	V	Chromik et al., 2018
15	n/a	Switzerland	2018	T	V	Urdaneta et al., 2018
16	n/a	USA	2021	HVAC	V	Werth and Morris, 2021
17	RICS-el	Sweden	2019	EG	V	Almgren et al., 2019
18	n/a	USA	2018	G	V	T. Alves et al., 2018
19	SWAT	Singapore	2016	W	P	Mathur and Tippenhauer, 2016
20	PowerCyber	USA	2010	EG	n/a	Hahn et al., 2010
21	GRFICS	USA	2018	C	V	Formby et al., 2018

Nr.	Name	Country	Year	Field	Type	Ref.
22	n/a	Italy	2010	EG	H	Fovino et al., 2010
23	VCSE	USA	2011	EG	V	Stamp et al., 2011
24	n/a	USA	2011	G	P	Morris et al., 2011
25	VPST	USA	2009	EG	V	Bergman et al., 2009
26	TASSCS	USA	2011	EG	V	Mallouhi et al., 2011
27	ICSrange	Italy	2019	G	V	Giuliano and Formicola, 2019
28	SoftGrid	Singapore	2016	EG	V	Gunathilaka et al., 2016

Table 3 shows that half of the testbeds are created in the USA, and the rest are scattered across Europe and Asia. However, in recent years, the number of CRs and testbeds is increasing in Europe and Asia. In the author's opinion, the increase of IACS CR research topics is explained by developments in the IACS field where OT systems merge with IT networks.

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. In author's opinion, the energy sector is one of the most obvious targets for adversaries as nowadays everything relies on electricity. Secondly, research using an electrical grid can more easily emphasize the gravity of cyberattacks.

Krishnan and Wei (Krishnan & Wei, 2019) shows that a literature vacuum exists about detailed cyber range documentation, focusing on cyber-security readiness, penetration testing, IACS protocols analysis, vulnerability assessments, defensive and offensive security, risk analysis, and IACS incident forensics.

CRs use different vendor elements and protocols in their systems. All of this data is collected in table 4. One of the most common vendors used in physical IACS cyber ranges across multiple studies are Siemens and Allen-Bradley. In author's opinion popularity of these vendors can be justified by vendor presence in worldwide markets and across virtually all industries.

4 Table: IACS testbed overview by vendors and protocols.

Nr.	Name	Vendors	Protocols	Ref.
1	n/a	n/a	n/a	Reaves and Morris, 2012
2	n/a	n/a	Modbus/TCP	Koganti et al., 2017
3	n/a	n/a	n/a	Korkmaz et al., 2016
4	VTET	Siemens	OPC, Modbus/TCP, S7comm	Xie et al., 2018
5	n/a	Siemens	Profinet	Noorizadeh et al., 2021
6	n/a	n/a	Modbus/TCP	Stranahan et al., 2019
7	n/a	Siemens	Profinet	Su et al., 2017
8	MSICST	Siemens, Rockwell, GE, Schneider	S7comm, EDG, Modbus/TCP	Tao et al., 2019
9	n/a	n/a	Modbus/TCP	Rosa et al., 2017
10	n/a	Multiple	Modbus/TCP, OPC, ARTI, DNP3, KOYO, IEC 60870-5-104	Krishnan and Wei, 2019
11	IOSB	Siemens	S7comm, OPC, Profinet	Pfrang et al., 2017
12	EPIC	Multiple	IEC-61850, Modbus/TCP	Adepu et al., 2019
13	n/a	Multiple	Modbus/TCP, DNP3	Rubio-Hernan et al., 2017
14	n/a	n/a	Modbus/TCP	Chromik et al., 2018
15	n/a	n/a	Modbus/TCP	Urdaneta et al., 2018
16	n/a	OpenPLC	n/a	Werth and Morris, 2021
17	RICS-el	n/a	IEC 60870-5-104	Almgren et al., 2019
18	n/a	n/a	Modbus/TCP, DNP3	T. Alves et al., 2018

Nr.	Name	Vendors	Protocols	Ref.
19	SWAT	Allan-Bradley's	EtherNet/IP, CIP	Mathur and Tippenhauer, 2016
20	PowerCyber	n/a	DNP3, IEC 61850	Hahn et al., 2010
21	GRFICS	n/a	n/a	Formby et al., 2018
22	n/a	ABB, OpenPLC	Modbus/TCP, DNP3	Fovino et al., 2010
23	VCSE	n/a	n/a	Stamp et al., 2011
24	n/a	Multiple	Modbus/TCP, DNP3	Morris et al., 2011
25	VPST	n/a	DNP3	Bergman et al., 2009
26	TASSCS	n/a	DNP3, Modbus/TCP	Mallouhi et al., 2011
27	ICSrange	n/a	Multiple	Giuliano and Formicola, 2019
28	SoftGrid	n/a	IEC 60870, IEC61850	Gunathilaka et al., 2016

As the crucial part of the IACS system lies in the communication between control elements, TCP/IP communication protocols are used, which is also one of the broad attack surfaces of IACS. In table 4 used protocols are listed, and one of the most used protocols in cyber ranges across multiple fields of IACS is Modbus. It is widely used because the protocol is open-source with vastly available documentation and relatively easily exploitable vulnerabilities. Another protocol of interest is Distributed Network Protocol 3 (DNP3), which is mainly utilized in electric and water utilities mainly in the USA. S7 Communication (S7comm) is a Siemens proprietary protocol used in communication between PLCs of the Siemens S7-300/400/1200/1500 family. Open Platform Communications (OPC) is a series of standards and specifications for industrial telecommunication, mainly used in higher-level management systems.

Testbeds and CRs can be divided by type, purpose, and supporting sector. Sectors are academic, military, or commercial. Most of the reviewed research is about CRs in the academic sector. Regarding purpose, CRs are divided into flowing parts: team building, cyber training, capture the flag events, research and development, testing, assessment, and recruitment. The broad spectrum of purposes requires an extensible and configurable IACS platform. Multiple researches (Geng et al., 2019; Reaves & Morris, 2012) divide CRs by physical, virtual, and hybrid architecture. Many testbeds hybridize the physical and virtual components to make a trade-off between fidelity and economy, which is also confirmed by table 3. Most research is

done on virtualized testbeds as they are cheap and relatively easy to implement and re-purpose. Further, these three CR architectures are described in detail.

2.2.1.1. Physical testbed

This type of testbeds uses physical hardware and actual software running on hardware. Some of the physical CRs as (Adepu et al., 2019; Mathur & 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 (HIL) physical system simulation method, which uses mathematical models to represent the physical process. There is a lack of exact mathematical models for representing the behaviors of sensors and actuators used in monitoring and controlling the physical devices. Green et al. (Green et al., 2017) points out HIL is not that necessary as these mathematical models cannot reproduce the exact physical model. Hence simple physical stimulation can be enough.

One of such physical CR is Secure Water Treatment (SWaT) (Mathur & Tippenhauer, 2016). SWaT consists of a six stage water treatment process, each stage is autonomously controlled by a local PLC. As indicated by Geng et al. (Geng et al., 2019) this testbed framework is widely used in many research papers, for instance, “An Investigation into the Response of a Water Treatment System to Cyber Attacks” (Adepu & Mathur, 2016), “HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems” (Ghaeini & Tippenhauer, 2016).

Most of the reviewed research agrees that physical CRs closely represent real-life system, suggesting that it has the highest fidelity. It can contain hardware, firmware, and software vulnerabilities, thus exposing a broader attack surface to exploit. In this way, it allows to understand attacker incentives better.

Possible drawbacks of such physical CRs are:

- 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;
- Difficulty for researchers to build large-scale CRs due to cost limitations. Therefore, researchers usually use a small amount of necessary core physical components to build a minimal IACS test environment and surround it with virtualized components.

However, Reaves and Morris (Reaves & Morris, 2012) imply that physical testbeds have

several advantages compared to virtual systems:

- Data reflect realistic measurement variations that would be present in an actual process control system;
- Communication patterns and latency is entirely accurate and not vulnerable to inaccuracies in simulated variables like OS scheduling load;
- IACS elements can hold software, firmware, and hardware vulnerabilities which is not possible for virtual testbeds. These attacks can be provided in addition to protocol-based attacks.

2.2.1.2. Virtualized testbed

Xie et al. (Xie et al., 2018) mentions that virtualization of the testbed is a straightforward approach to overcome the disadvantages mentioned in section 2.2.1.1. Although the virtual testbed would lose some fidelity, it is more suitable for preliminary IACS security research in the laboratory environment.

Geng et al. (Geng et al., 2019) illustrates that the virtualized testbed enables researchers to conduct low-cost, reusable security studies in a real IACS configuration environment with an IT architecture. However, virtualized complex physical processes involve a large amount of computation. Therefore the hardware requirements of the computer are high. As an advantage, virtual CRs have high scalability and generally operate on either a single or a small number of servers. Additionally, virtualization can only support open-source PLCs and related software in virtual machines. On the downside, mainstream PLCs, such as, Schneider, Omron, and Siemens are closed-source industrial devices. Commercial vendors have limited information on hardware and firmware, making it difficult to virtualize these PLCs. So one of the biggest obstacles to virtualize high-fidelity IACS testbeds is the lack of open-source virtualized PLCs. For virtualization purposes, the OpenPLC controller is used (T. R. Alves et al., 2014). OpenPLC supports five programming languages based on IEC61131-3 (RealPars, 2021) and commonly used IACS protocols - Modbus TCP, DNP3 and others. Therefore OpenPLC is easy to deploy and relatively cheap to install and maintain. However, several academic papers question whether test results from a simulation reflect reality.

One of such virtualized testbed is GRFIACS framework (Formby et al., 2018) based on OpenPLC (T. R. Alves et al., 2014) research. The framework was created relatively recently in the year 2018. GRFIACS virtualized the entire IACS network and physical processes. The

GRFIACS testbed can be used to practice common methods of IACS attacks and exploits while observing the impact of network attacks on physical processes.

Advantages mentioned by Reaves and Morris (Reaves & Morris, 2012) are:

- Virtual testbeds are easy to duplicate and reproduce. Virtual testbed platform reduces duplication of effort as research groups do not have to develop testbeds from scratch. An open platform enables researchers to update existing virtual testbeds;
- Virtual testbed platform provides a common ground for research enabling research groups to share code and enabling published results to be duplicated and compared.

2.2.1.3. Hybrid testbed

Hybrid testbeds try to combine the best of both worlds, virtual and physical. Testbed by this approach can be created using physical components, such as, PLCs, HMIs, and other physical systems that are hard or close to impossible to virtualize or simulate. On the other hand, system elements like SCADA workstations, historians, and network infrastructure can be virtualized. For example, SCADA commonly resides on MS Windows type of operating system that can be run in a virtual environment like VMware or VirtualBox.

One of such CR was created by Rosa et al. (Rosa et al., 2017). The study created an electrical grid CR where SCADA and the network ran in a virtual environment, but elements controlling circuit breakers and disconnectors were physical devices. Rosa et al. mentions that this setup provides more information about less evident events in the SCADA system during attacks.

Pfrang et al. (Pfrang et al., 2017) has created a CR by dividing in physical and virtual parts as follows:

- Virtualization environment - virtual switches, VM PLC programming stations, VM SCADA servers, attack detection tools;
- Physical environment - PLCs, industrial actuators, HMIs, RTUs.

2.2.2. Objectives, purpose, and requirements of IACS cyber ranges

Researches (Tao et al., 2019; Tippenhauer, 2019) mention that the testbed and cyber ranges can be built for a multitude of purposes such as vulnerability analysis, education and training, tests of defense mechanisms, control system tests, performance analysis, honeypot, impact analysis,

threat analysis, and creation of standards. However, review by Davis (Davis, 2013) argues that CRs are predominantly used for training. The training varies in complexity going from computer security fundamentals to advanced Techniques, Tools and Procedures (TTPs) for Computer Network Operation (CNO). As described in NIST Glossary (NIST, 2021) TTPs are adversary behaviors where tactics are high-level actions and techniques are behaviors attacker performs in the context of the specific technique. Term CNO encapsulates defense and offense computer operations.

Diversity in the range of IACS elements, software, and protocols, is essential to replicate real-world scenarios in cyber ranges. Green et al. (Green et al., 2017) points out that diversity comes at a cost, not only in financial terms but also with regards to scalability and complexity of the experimental infrastructure.

Researches are aiming for low cost and still keeping some fidelity of IACS cyber range to develop CRs with physical and virtual components, making them hybrid testbeds. Physical elements are the ones increasing the fidelity of the system. One such CR was created by Xie et al. (Xie et al., 2018) it is Virtual Tennessee-Eastman Testbed (VTET) which consists of virtual and physical elements. Tippenhauer (Tippenhauer, 2019) mentions that it is essential to understand which components are required to be real and which should be virtual. This is undoubtedly one of the most important decisions when designing a testbed for security research. Several trade-offs have to be considered depending on the individual project scope, domain, and intended research.

CR requirements change based on objectives. For example, Formby et al. in research (Formby et al., 2018) has created GRFIACS testbed framework, which is intended to help beginners in IACS security to overcome barrier created by the exclusive use of expensive, proprietary hardware and software used in IACS. CR is designed for students to create an attack that causes significant physical damage to the simulated system. Therefore, Formby et al. as main requirements mention modular design to allow swapping virtual elements with physical ones, low initial cost, and simple communication protocols for students to reduce the learning curve. Other researches as (Fovino et al., 2010; Koganti et al., 2017) have created electrical grid hybrid IACS cyber rages. In this case, the main objective of the research was to understand the cascading effects of failures in IACS with realistic attack scenarios and to test novel cyber-attacks. These testbeds require sophisticated simulation of the electrical grid to understand the impact of attacks. Thus, minor emphasis is placed on control system complexity.

From reviewed research flowing objectives are summarized:

- Assessing the effectiveness of methods for cyberattacks and defense against them;
- To generate real-time data-sets for real-time attack detection systems;
- To help beginners in IACS security overcome barrier created by the exclusive use of expensive, proprietary hardware and software used in IACS;
- To improve the way the IACS networks are created;
- To find new exploits and attacks in IACS field;
- Evaluate IACS in terms of the probability and availability of cyber-attack likelihood on the electrical grid systems;
- Learn cyberattack impact on electrical grids;
- Evaluate effectiveness of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS);
- Providing training of penetration skills for red teams, professional hackers employed by organizations to challenge their defensive capabilities;
- Improving defensive methods and practices for blue teams.

Multiple researches (T. Alves et al., 2018; Bergman et al., 2009; Craggs et al., 2019; Geng et al., 2019; Giuliano & Formicola, 2019; Green et al., 2017; Holm et al., 2015; Pfrang et al., 2017; Tao et al., 2019; Tippenhauer, 2019) indicate that cyber ranges need to consider flowing key points:

- Repeatability - precisely repeating the experimental conditions and reproducing entire or partial results;
- Fidelity - the experimental CR needs to reproduce the real system of the research object as accurately as possible, CR has to present interaction with real IACS components using real IACS tools including providing grounds for realistic attacks and countermeasures;
- Measurement accuracy - monitoring testbed process and reactions cannot interfere with experimental results;
- Safe Execution - testbed should be isolated and does not have a devastating effect on the physical system and personal safety;
- Diverse physical processes interacting with each other - meaning that different IACS process can interact with each other not only through data link but by a physical process,

like temperature, vibration, mechanical motion;

- Legacy and non-legacy IACS software platforms and devices - testbed should support and include old and contemporary IACS elements;
- Support for communication protocols - testbed infrastructure must support typical IACS communication protocols, such as, Modbus TCP, Ethernet/IP, DNP3, and OPC DA. By its very inclusion, the diversity of communication protocols will introduce several vulnerabilities and real-world scenarios;
- Ease of deployment of local and remote experiments - CR should be accessible for parties outside of testbed network;
- Adaptability and flexibility - reconfiguring the whole laboratory set up by exchanging components through standardized interfaces mechanically, electrically, and the networking infrastructure. Cyber-Physical testbeds that contain real devices and real processes will require more effort to reconfigure and adapt to different settings. Fully simulated processes can likely be changed more quickly by updating the process topology. Real PLC will have to be reprogrammed with new control logic;
- Real-world interoperability - is highly desirable if the testbed can be used to assess products or prototype solutions that are meant for actual deployment;
- CR element selection by market share - selection of control devices, protocols, and software should be based on market share and combined with the characteristics of the target market. This allows to create realistic testbed that mimics target systems;
- Choose physical process according to industry - IACS in different industries have significant differences, and it is not easy to have an IACS testbed that can represent process scenarios in all industries. Therefore, the IACS testbed usually selects one or several process scenarios to simulate.

2.2.3. Design overview and considerations

Literature review shows that IACS cyber ranges and testbeds should consist of both real hardware components and virtualized components to gain flexibility and reduce costs. Davis (Davis, 2013) Control software like SCADA runs on general PC software like windows which can be virtualized. Also, for some vendors, SCADA software is available as a trial. Hence, this also reduces costs by using this free software.

Whether the testbed is physical, virtual, or hybrid, the selection of IACS elements, protocols, and software should be based on protocol or device popularity in a specific target region. This allows to create of a realistic system that mimics targeted systems. “Pains, Gains and PLCs: Ten Lessons from Building an Industrial Control Systems Testbed for Security Research” (Green et al., 2017) research stipulates that IACS cyber range should be built for specific field. IACS fields are led by device vendors and integrators and are not as standardized as IT systems. IACS in various industries and countries are substantially diverse, their architecture, elements, and protocols are different. Establishing a reference model is the primary means of addressing these variations. This is also recognized by observing different cyber ranges, they are created to represent a specific industry that uses various protocols, IACS elements, etc. The author has chosen Europe as the focus region of this study, as it is more familiar.

IACS systems control physical field-level devices. One way to create a physical industrial process is to use actual hardware that is costly but close to real life. A second approach, and it is the most common method, uses mathematical models to simulate a physical process HIL. Green et al. (Green et al., 2017) argues that there is a lack of exact mathematical models for representing the behaviors of sensors and actuators used in monitoring and controlling the physical devices. However, precise HIL is not that necessary as these mathematical models cannot reproduce the exact physical process. Thus simple simulation can be enough.

IACS cyber ranges have oversimplified assumptions about the IACS systems. Green et al. (Green et al., 2017) stipulates that oversimplification mainly is observed in virtual testbeds.

It is worth mentioning that almost none of the cyber ranges in table 3 share a detailed documentation of the system. Primarily it refers to physical IACS testbeds, making it hard to replicate similar cyber ranges. Green et al. (Green et al., 2017) notes that making the testbed more open for researchers extends its usability, and it should be taken into account when designing testbeds.

2.2.3.1. Topologies

Green et al. (Green et al., 2017) indicates that IACS need to be separated in zones to mimic realistic IACS system - manufacturing zone, demilitarized zone and enterprise zone. The same ideology is applied in research by Almgren et al. (Almgren et al., 2019), where a more realistic environment is created by attaching other IT networks to IACS segments like office or enterprise networks.

2.2.3.2. Protocols

Industrial control systems are getting more interconnected and have started to utilize standardized IT interfaces for communication. Hence communication protocols are responsible for a wide attack surface. As Green et al. (Green et al., 2017) mentioned, protocols as IACS elements and architecture should be chosen according to the IACS field, and country/region CR represents.

Common protocols in the industry are Modbus/TCP, Profinet, DNP3, Goose IEC61850, OPC-UA, S7comm, and IEC60870-5-104 (IEC104), also seen through different CRs in table 4. These protocols usually have a specific purpose and are used in specific fields. General description of these protocols is listed as follows:

- Modbus - one of the most used protocols across multiple fields of IACS. Initially, it has been used in serial communication, but with the introduction of TCP/IP in the IACS field Modbus used by encapsulated in the TCP application layer. Wide usage can be explained by it being around for more than 20 years (Modbus, 2021). It is an open-source protocol with a vastly available documentation and has relatively easy exploitable vulnerabilities. Also, virtual testbeds usually use Modbus as there are multiple open-source libraries in different programming languages. This protocol is also known to be vulnerable, but it is still widely utilized. By author's opinion and experience, it is due to its widely available support and ease of implementation. Modbus/TCP had an updated version called Modbus/TCP Security, which includes security mechanisms like authentication and encryption (Modbus, 2021).

- S7comm - Siemens proprietary protocol also called Step7. It runs between Siemens S7 PLCs and between Siemens HMIs and SCADAs. This protocol field of usage is broad and depends more on the S7 PLC configuration. S7comm comes without any security implemented. However, newer Siemens S7 PLCs support the S7commPlus protocol, where security mechanisms can be enabled if configured correctly, and both communication devices support the S7commPlus protocol. S7comm should be considered if Siemens elements are used. In author's opinion, the S7Comm protocol is prevalent in regions where Siemens are highly utilized.

- DNP3 - are used since the year 1990 when GE Harris developed it. This protocol is mainly used for communication between SCADA and geographically distributed stations. Initially, DNP3 was built to work with serial communication, but with the introduction of TCP/IP in the IACS field, DNP3 were encapsulated inside TCP/IP. DNP3 is more common in North

America but is used in some IACS sectors also in Europe. In the author's opinion, DNP3 is more prevalent in America as the company GE originated there. In recent years DNP has been evolving to include different security mechanisms. More detailed information about this protocol can be found in (DNP, 2021).

- OPC-UA - stands for Open Platform Communications-Unified. Initially, it was intended to be used for communication between shop floor devices like PLCs, but it can also be used for communication between SCADA and geographically distributed stations. OPC-UA integrates authentication by using certificates. Research (Polge et al., 2019) mentions that there is a lack of studies about OPC-UA security. This protocol is mainly used in manufacturing industries.

- Profinet - is based on ethernet and replaces Profibus, which is based on serial communication. Profinet is created for high-speed applications where response time is less than one millisecond. This protocol is used mainly by Siemens PLCs (Profinet and Profibus, 2014). Profinet has integrated security mechanisms which can be broken (Müller et al., 2018).

- GOOSE - stands for Generic Object Oriented Substation Events. This protocol is defined by IEC61850 (Communication networks and systems in substation) standard. It is used to transmit high-speed status information to multiple control devices. GOOSE is mainly used in the energy sector. This protocol has security mechanisms implemented, however as indicated by (Sidhu & Yin, 2007) it contains security vulnerabilities.

- IEC104 - is the protocol used in the energy sector. This protocol is used similarly to DNP3 to establish communication between SCADA and geographically distributed stations (Radoglou-Grammatikis et al., 2019). However, the IEC104 protocol does not implement any security mechanisms. Consequently, this protocol can be exploited to perform attacks on IACS elements (Blumbergs, 2019).

2.2.4. Exercise scenarios

Adversaries perform attacks on IACS with a specific objective. Tippenhauer (Tippenhauer, 2019) argues that usually attacks on IACS systems are intended to achieve physical damage as impact. Urdaneta et al. (Urdaneta et al., 2018) states that launching a successful attack on a cyber-physical system involves five fundamental steps, also called ICS kill chain:

1. Gain access to the system;
2. Discover the system;

3. Take control of the system;

4. Cause damage or disruption to the physical process;

5. Clean up all the evidence pointing to the cyberattack.

CR research rarely addresses the way how attackers gain access to IACS networks. Giuliano and Formicola (Giuliano & Formicola, 2019) states that for the CR to be effective and lifelike, it should provide multi-staged attack scenarios where the attacker breaches the network and performs lateral movements also observed in APT attacks. Pfrang et al. (Pfrang et al., 2017) indicates an important point regarding how the attacker gains access to an IACS network in the first place. Many infections of production networks arise via the enterprise network through infected email attachments, malicious code on websites, phishing attacks, or infected USB drives, as human personnel is susceptible to social engineering attacks. Inadequate separation of networks then allows an attacker to spread within the network. Attacker spreading to IACS network is discussed by NSTB (NSTB, 2008), an intruder can use several proven techniques, such as, piggybacking, on a connection or exploiting a service allowed through the firewall, discovering an auto-answer modem or connection circumventing the firewall, or gaining access through a trusted peer site. IACS attack trees and taxonomies can be used to create a complete attack chain from the office network to the IACS segment.

Kaspersky has created report “Threat landscape for industrial automation systems” (Kaspersky Lab, 2021c) where they mention that the three primary threat sources for the IACS network are access from the Internet, removable media, and email clients.

Rosa et al. (Rosa et al., 2017) express that during cyber range development, it is essential to grasp the attacker’s perspective, including the challenges he faces to implement a successful attack. This will help to create realistic scenarios.

As an example, a successful cyberattack against a power system will likely target power flow operations. In order to determine critical assets and provide a basis for establishing attack goals Hahn et al. (Hahn et al., 2010) have proposed various impact scenarios. These scenarios address high-level attack objectives that will either directly or indirectly affect power production. This can be one way how to create high-level attack objectives.

IACS systems are different from mainstream IT systems. The main difference is that an attacker performing attacks needs to determine the physical system’s state to execute malicious action. Research (NSTB, 2008) points out that attacker must find information about the target

control system and discover details about the process under its control before he can create an attack against it. If the adversary aims to shut down the process, very little analysis of the system is needed. However, if the attacker aims for a specific attack on process manipulation, details are necessary. Giuliano and Formicola (Giuliano & Formicola, 2019) explains that the easiest way to determine systems status is by observing information on HMI or SCADA screen or PLC embedded web page. Hence, in CRs, HMI and SCADA can serve two purposes. The first is for the attacker to determine the process state. The second is for an attacker to have a reference to determine whether the attack has been successful.

2.2.5. Offensive operations

Term cyber operation describes entities' capabilities to affect cyber-domain by using capabilities, such as, resource, knowledge, skill, and tactics. Furthermore, offensive operations utilize cyber capabilities to fulfill objectives in the cyber domain (Gold, 2020).

All governments are developing and using defensive cyber capabilities to some degree. Unfortunately, when it comes to cyber offensive capabilities, information is sparse. Only some of the nations, such as, the United Kingdom, Netherlands, USA, Canada, and Australia have expressed having offensive capabilities (Gold, 2020; Muller, 2019; UK Government, 2016). However, disclosed information is not detailed enough to understand their true potential (Ottis, 2009). Offensive cyber operations seek to disrupt data and services, computer machinery, sow confusion, and damage networks. They are directed towards all digital assets in the military, government, critical infrastructure in the opponent homeland.

Cybersecurity professionals have terminology used by the military during training. Mentioned by Ukwandu et al. (Ukwandu et al., 2020) teams are divided as follows:

- Red Team (RT) - defensive operations;
- Blue Team (BT) - offensive operations;
- White Team (WT) - administrative management;
- Yellow Team (YT) - motivator during exercise;
- Green Team (GT) - maintains exercise infrastructure;
- Purple Team (PT) - sets objectives for offensive and defensive strategies;
- Gray Team (GrT) - conducts non-malicious activity.

RT offensive capabilities are an intrusion into the opponent's IT infrastructure to cause damage, disruption, or gather sensitive data. Report "The role of offensive cyber operations in NATO's collective defence" (Lewis, 2015) mentions NATO's considerable efforts to integrate cyber capabilities. Nevertheless, additional effort and strategies need to be created. Currently, NATO has an emphasis on defensive operations. However, the lack of an articulated offensive cyber capability affects NATO's ability to deter or defend. In the military, offensive force in the form of kinetic weapons, ground, troops, or airstrikes is common and part of any military toolset. These offensive physical domain operations can be executed using clear rules of engagement. However, in the cyber domain, offensive actions are difficult to justify and disclose.

By performing additional literature review on national offensive capabilities, the author concludes that there is a lack of verified knowledge of official strategic documents in cyber offensive capability development, the execution of various cyber operations, and the design of such operations, execution, management, and governance. At the strategic level, governments desire to have a degree of plausible deniability. This is also confirmed by Schab (Schab, 2021).

Nations are not well known to publicly announce offensive capabilities in the cyber field, and this is particularly displayed with USA actions " [...] The US has always been overly secretive about its offensive cyber capabilities, even after a flood of media leaks have made the most sensitive doctrine publicly available. This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests [...] " (Lewis, 2015).

Reasons why offensive capabilities are needed according to Gold (Gold, 2020) is that governments can use this capability as a political tool to deter any tensions directed to themselves or allayed countries. If necessary, it can be used to respond to aggressors with destructive power. Moreover, report "The role of offensive cyber operations in NATO's collective defence" (Lewis, 2015) mentions that modern warfare like air force will not enter into combat without electronic warfare (EW) support. It is also true for other military domains.

Offensive capabilities are necessary not just for governments but also for the private segment, for example, to perform penetration assessment of IACS fields. This requires experts with offensive capabilities in this field.

2.3. Identified gaps

Related work analysis shows that work has been done in the area of IACS cyber ranges and testbeds. However, multiple drawbacks are identified, and the solution proposed by this work is subject to the following security gaps:

1. Small number of IACS cyber ranges and testbeds are aimed for cyber red team technical offensive exercise development;
2. IACS cyber ranges with multistage attacks are not explored fully;
3. Physical testbeds lack detailed documentation and are not portable enough, making them hard to reproduce;
4. Only virtual testbeds are considered easy to reproduce, and to the author's knowledge, no research is found with a focus on physical testbed repeatability;
5. Lack of open-source physical PLCs to increase testbed fidelity;
6. Most similar research has created CRs that rely on simple attack scenarios where the physical process does not play an important role. As a result, these CRs show things that do not correspond to the actual situation in the IACS field;
7. Related work CRs are primarily virtual. More extensive research needs to be done by creating physical CRs because there are many undisclosed vulnerabilities in the hardware and software of the IACS elements.

2.4. Novelty and contribution

The master thesis research can be considered novel as it has been built upon identified gaps listed in 2.3. Moreover, the created CR is relatively unique as it tries to encompass ease of replication, available documentation, and complexity to perform realistic offensive attack scenarios. Created CR key aspects are listed below:

1. Tackle the issue of too expensive testbeds with a proposal on how to hybridize physical testbed by introducing virtual components;
2. CR will be aimed for technical offensive capability development as these capabilities 2.2.5. is necessary for both government and private sectors;
3. Have standard communication protocols for convenient integration in other CRs. For

example, that allows the attachment of additional IACS or IT networks to the CR;

4. Open-source extensive step by step documentation and system programs/configuration available for the public for easy reproduction;
5. Focus on multistage attacks mimicking realistic lateral movements of the attacker through network.

Contributions of this master theses are as follows:

- Summary of available relevant IACS testbeds across different studies. That gives future researchers summarized information about previous testbeds and CR. Can be seen in tables 3 and 4;
- Summarized concepts and approaches regarding IACS testbed design considerations 2.2.3., objectives 2.2.2., scenarios 2.2.4. and architectures 2.2.1.2., 2.2.1.3., and 2.2.1.1.;
- Author has created a realistic IACS cyber range prototype for red team offensive exercise development. In addition, detailed and publicly available documentation under MIT license author has made available in GitHub [3] repository frostyICS for ease of reproduction.

[3] frostyICS - IACS cyber range for offensive capability development https://github.com/austrisu/frostyICS

3. IACS CYBER RANGE DESIGN

This chapter concentrates on the design of CR for use in offensive capability development exercises and, in a structured manner, introduces and explores various aspects of IACS CR development and design considerations.

3.1. Overview

The author has designed the IACS CR taking into account identified gaps from section 2.3., additional literature reviews about IACS vulnerabilities, and the author's personal practical experience in the IACS field as he has done testing, implementation, and configuration of various IACS components in the past.

This master thesis objective is to create the CR by utilizing key aspects from the literature review (see Sec. 2.4.). Developed IACS cyber range encompasses the following characteristics:

- realistic;
- easily reproducible;
- with publicly available documentation;
- supporting multistage attack scenarios;
- oriented to use in offensive exercises (see Sec. 2.2.5.).

Since most of the population nowadays is concentrated around the cities, it is crucial to sustain this population by providing water, electricity, heating, transportation, communication, and several other services. Most infrastructures are controlled and automated by the IACS, and any interruption or loss of these services is likely to have a devastating effect.

For this CR, as a primary physical process, the district heating plant is used. The district heating plant supplies heat to the city. A secondary control process is a warehouse management system controlling alarms and lights. The warehouse is part of the heating plant and is used to store materials, spare parts, and other goods necessary to ensure continuity of heating plant

operation. The heating plant and warehouse are collocated, and as seen in figure 2 they are connected in one communication network. The author has chosen the heating plant as it is part of the critical infrastructure for the cities, and they can be valuable targets for adversaries. The second reason is that the heating process is relatively easy to comprehend and understand the causality of different physical mechanics.

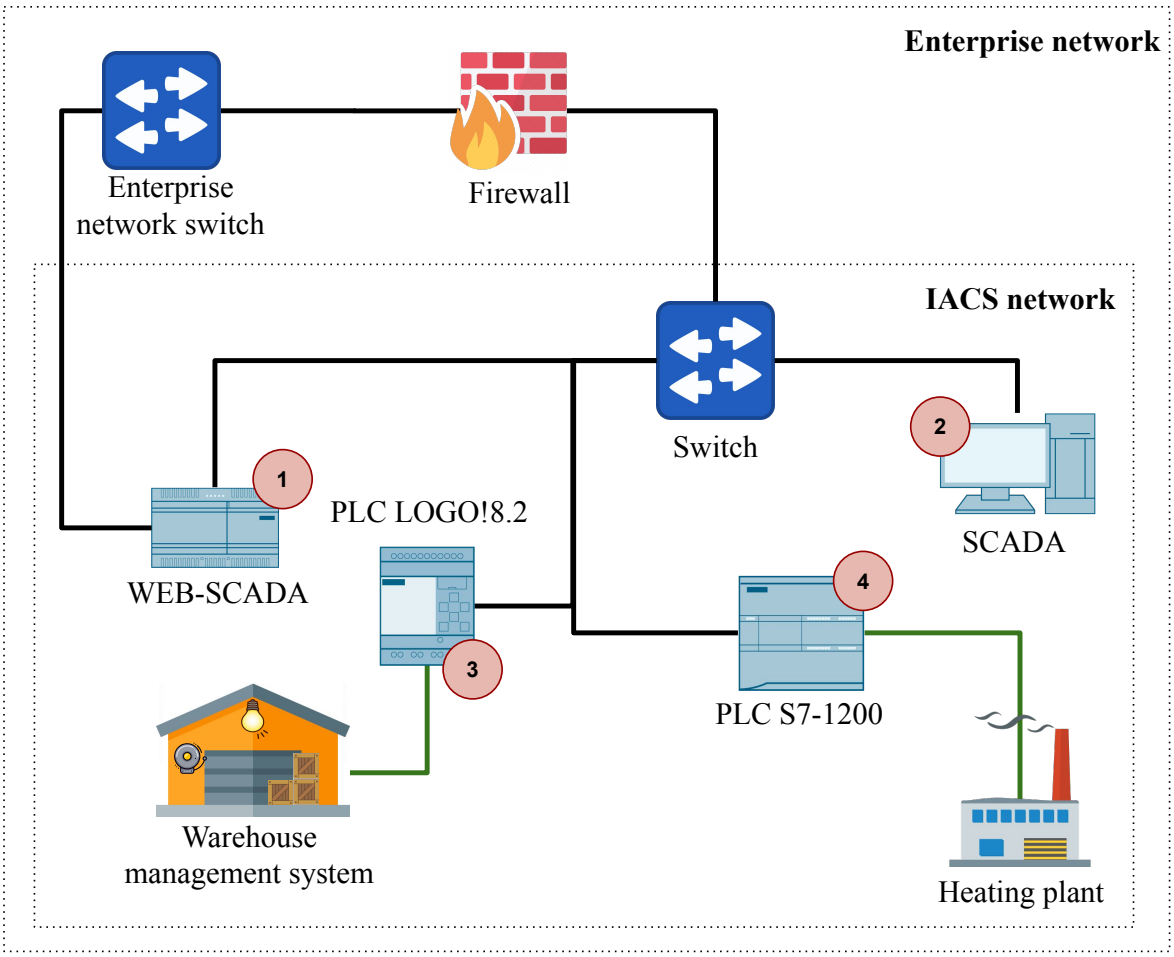
The CR network topology is shown in figure 2. The system consists of two PLCs (3) and (4), SCADA (2) and WEB-SCADA (1). So CR can be divided into supervisory and control systems containing SCADAs, and execution systems containing PLCs. Further, each of the elements, working principles, communication, and simulated physical systems are described in detail.

Author's choice of elements was motivated by two reasons. Firstly, as indicated in the literature review, CR should encompass elements used in the target region. Europe is the target region for this master thesis. In Europe, Siemens is one of the vendors widely used across various IACS industries. Moreover, as the cost of physical devices is not negligible and the master thesis was performed without any budget, the author used Siemens equipment already accessible from other projects. Table 5 describes the hardware and software of each element, used versions, and Siemens reference code for respective devices. In further sections, each of these elements, purpose, and communication partners are described in detail.

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

Nr.	Element	System description	Siemens reference
1	SCADA	Siemens, Simatic WinCC Advanced V15.1	6AV2102-0AA05-0AA5
		MS Windows 7 enterprise, SP1, Build 7601	n/a
		VirtualBox V6.0	n/a
2	WEB-SCADA	NodeRed V1.0.0 [4]	n/a
		Yocta Linux V2.6	n/a
		IOT2040	6ES7647-0AA00-1YA2
2	PLC LOGO!	Siemens, LOGO! 8.2, Full versions: 1.82.02	6ED1052-1FB08-0BA0
3	PLC S7-1200	Siemens, Simatic S7-1200, CPU 1215C	6ES7215-1AG40-0XB0

[4]NodeRed - (https://nodered.org/)



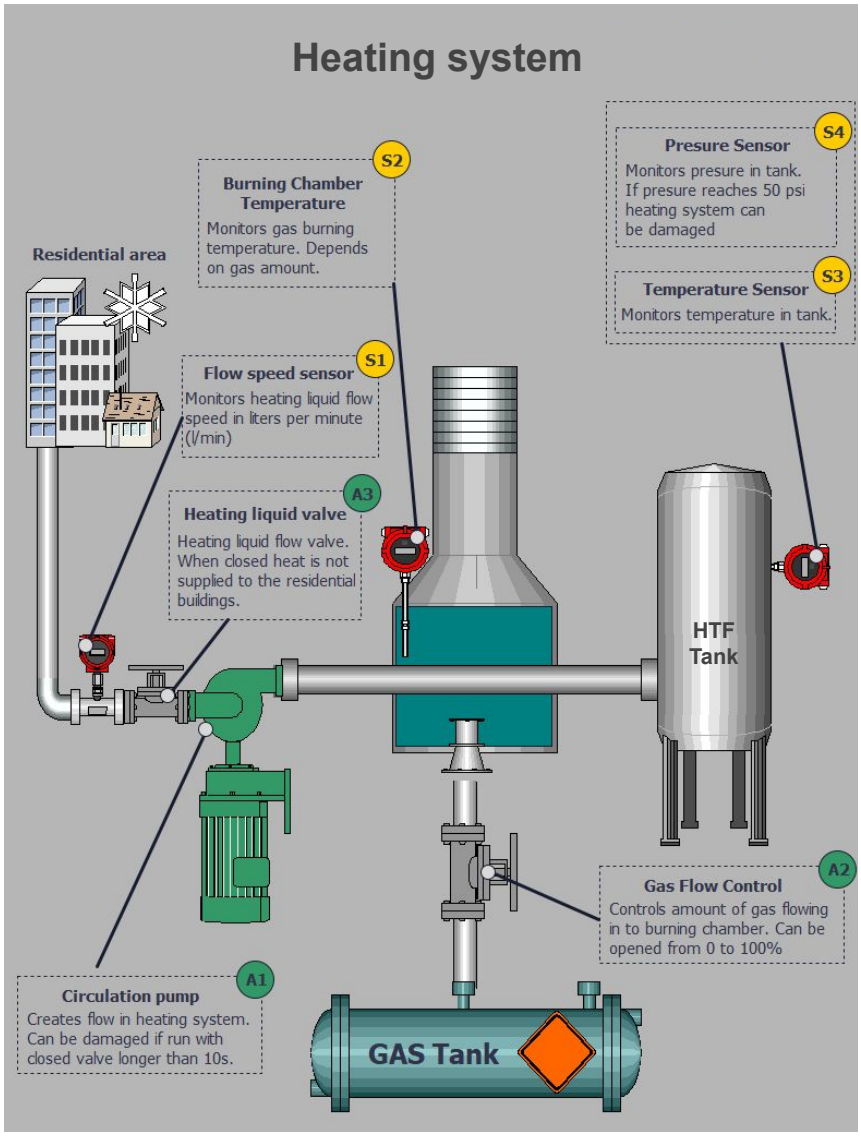
2 Figure: The CR network topology created by the author.

3.2. Heating process

SCADA HMI visualization of the heating plant is shown in figure 3. The heating plant consists of:

- Heating transmission line - transports Heat transfer fluid (HTF) to the city;
- Circulation pump (A1) - forces the HTF flow to the city;
- Transmission line valve (A3) - required to be open for the HTF to circulate;
- Gas flow valve (A2) - control the burning temperature of the gas in the burning chamber;
- Temperature and pressure sensors (S3, S4) - to monitor and give feedback to the control system about temperature and pressure in HTF tank;
- Flow speed sensor (S1) - To monitor and give feedback to the control system about the state of the HTF flow speed.

The heating process can be divided into two phases. One of the phases is the heating of



3 Figure: The heating plant visualization created by the author.

HTF, and the second is HTF transmission to the city districts:

1. HTF is heated by burning gas in the furnace. Then the heated fluid is distributed to the rural area. Gas flow is related to the burning temperature. Burning temperature 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. S7-1200 PLC (see Fig. 2) compares setpoint temperature with the actual heat transfer fluid temperature S4. Based on that, S7-1200 PLC controls gas-burning temperature S2 by adjusting gas flow controller A2. This system has embedded physical limits, such as, maximum temperature and maximum pressure. After exceeding maximum values, the heating plant gets damaged. If temperature or pressure values reach a set threshold, S7-1200 automation protects the physical system by stopping the gas flow to safeguard against the damage;

2. The HTF transmission process depends on the heating process. When HTF in the transmission line reaches temperature 60° C, then 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 can be damaged irreversibly if the circulation pump runs with the heating liquid valve (A3) closed.

Heating process control logic is in PLC S7-1200 (see Fig. 2). The author has built CR to be easily reproducible with no additional hardware, sensors, or actuators attached to S7-1200. Instead, the physical process is simulated using the HIL method. HIL consists of a simplified mathematical model of the heating process. HIL includes and controls nominal values of the physical process so that it can be damaged if these values exceed, which means that both the control program and HIL program runs on the same device. Both programs are separated so that control logic can only interact with heating process simulation as if through sensors and actuators seen in figure 3. For this reason, part of the controller responsible for physical system simulation is off-limits for the CR participants.

S7-1200 is Siemens Simatic PLC, which is widely utilized in different industrial fields. This PLC can have multiple configurations by adding expansion blocks like additional I/O ports, additional communication interfaces, and process-specific extensions. In this CR, basic S7-1200 module is used with built-in I/O and communication ports (see Tab. 7).

S7-1200 was configured and programmed utilizing Siemens software TIA Portal advanced V15.1 [5]. The TIA Portal is a multipurpose platform that allows the programming and configuration of Simatic PLC and other peripheral devices like networking components, HMIs, and SCADAs. TIA Portal also allows access to the devices in online mode and diagnoses them during commissioning. TIA Portal supports all programming IEC61131-3 (RealPars, 2021) standardized languages. Author uses LAD and SCL for this project as these languages are best suited for this program. There is no difference in using one or another language according to the author's knowledge and researched literature from the point of vulnerabilities.

Figure 4 displays overall structure of S7-1200 program. For Siemens PLC most fundamental programming construct is Organization Block (OB). OBs are the highest-level constructs that are executed cyclically or by some trigger event. Research (Su et al., 2017) states that OBs are similar to function calls in the C programming language or system calls in Unix OS. OB is always present in Simatic PLC programs and is identified as OB1. OB1 is also seen in the

[5]TIAportal - https://new.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal.html

author's program structure in figure 4. There the OB1 is used as a program's entry point where all other program functions are called. OB1 is executed cyclically as PLC's inputs and outputs (I/O) must always be updated. During the cycle, OB1 checks I/O, makes function calls and manages memory. Additionally, Simatic PLCs has a construct called Data Block (DB). DB contains global retentive variables which can be used in OB, Function (FC), or Function Block (FB).

The program is structured in two parts. The first contains control functions, and the second has physical simulation functions. Information transfer between these two program parts is done by using functions *actuator_translation[FC14] and sensor_translation[FC13]*. These two functions during each cycle copies simulated physical state:

- Sensor data - from *physical_DB[DB1]* to *sensor_inputs[DB8]*;
- Actuator data - from *actuator_output[DB9]* to *physical_DB[DB1]*.

TIAportal project files used in this CR are publicly available in the author's GitHub repository frostyICS [6].

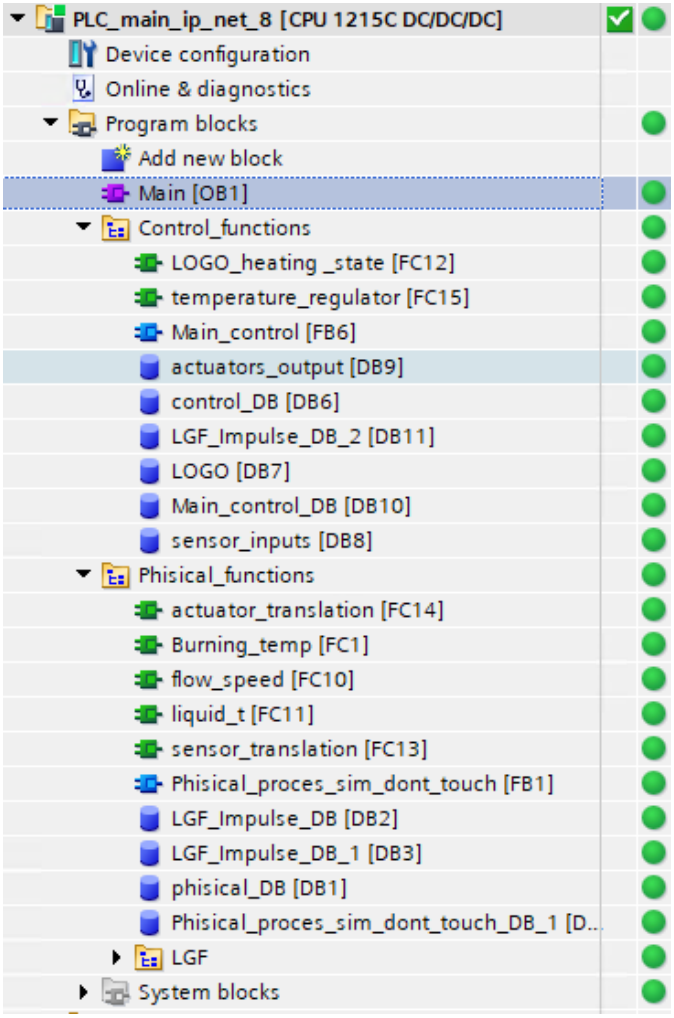
3.3. Warehouse management

Warehouse management in this CR is used to control alarms and lights. This process is much simpler than the heating plant. Siemens LOGO! 8.2 PLC is used to control it as it is meant for simple applications. LOGO! can have different configurations depending on added functional modules. In this CR LOGO! 8.2 basic module (see Tab. 7) is used with built-in I/O and communication interface.

Siemens LOGO! supports two programming languages FBD and LAD. For this CR author uses FBD as this programing language is easier to comprehend. Used LOGO! program is shown in figure 5. FBD program is executed from left to right. Each block represents some function that is built-in or user-defined. For example, some built-in functions are boolean operators, timers, comparators, memory write and read functions, math functions. Functions has inputs and outputs which can be connected and chained to other functions making logic instructions. For the program in LOGO! only built-in functions are used. Used functions in the program (see Fig. 5) are as follows:

- NI - network input is used to read values from local LOGO! memory or to read values

[6] frostyICS - IACS cyber range for offensive capability development (https://github.com/austrisu/frostyICS)



4 Figure: S7-1200 program structure created by the author.

from other devices in the network supporting S7comm protocol;

- NQ - network output is used to write values to local LOGO! memory or to write values to other devices on a network supporting S7comm protocol;
- Q - output is used to control LOGO! physical digital inputs and outputs (I/O);
- hi - keeps function output always in high state;
- B001 - display function is used to configure what information is displayed on LOGO! built-in screen.

LOGO! stores variables in several address types. Each address type is used for a specific purpose listed in table 6. In this program, Q and V address types are used. V address type is used so that Modbus can interact with the LOGO! program. Q is used so that the program can control LOGO! 8.2 physical outputs.

6 Table: LOGO! 8.2 used address types (R- read, W-write).

Address Type	Range	Direction	Unit
Inputs (I)	1 – 24	R	bit
Outputs (Q)	1 – 20	R/W	bit
Marker bit (M)	1 – 64	R/W	bit
Data block 1 (V)	0.0 – 850.7	R/W	bit
Data block 1 (VW)	0 – 850	R/W	16 bits
Analog Input (AI)	1 – 8	R	16 bits
Analog output (AQ)	1 – 8	R/W	16 bits
Analog marker bytes (AM)	1 – 64	R/W	16 bits

Siemens LOGO! program (see Fig. 5) is divided into four parts: 1) light control, 2) alarm control, 3) state of heating plant, and 4) the part which enables LOGO! hardware display. For example, light control flow works as follows:

- NI1 function each cycle reads value (true or false) from bit memory space V10.1;
- Value from NI1 is transferred to the input of function NQ1 and Q1;
- NQ1 function writes value from input to memory space V33.0;
- Q1 function writes value from function input to LOGO! physical output, setting voltage to high or low.

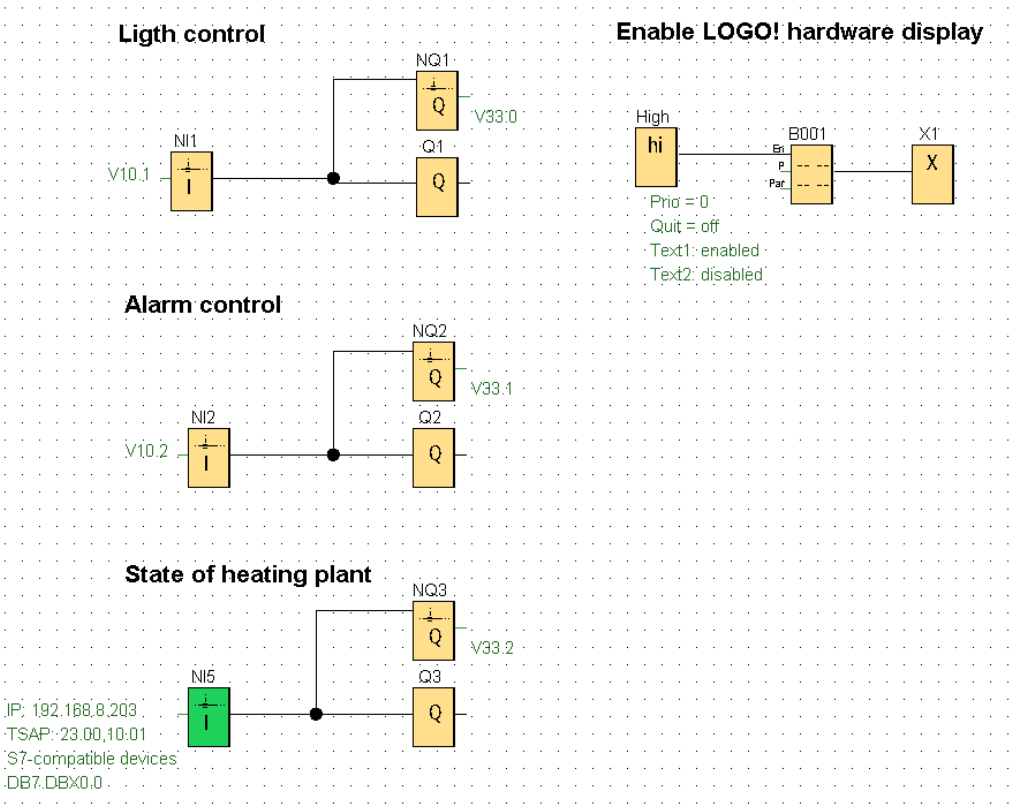
Siemens LOGO! is programmed utilizing Siemens LOGO! Soft Comfort [7] software. LOGO! Soft Comfort is a programming tool specifically for Siemens LOGO!. This software has a user interface that allows creating and uploading software. LOGO! Soft Comfort project files used for this CR are publicly available in the author's GitHub repository frostyICS [8].

3.4. Supervision and control of systems

Supervision and control system in the CR contains two SCADA devices (see Fig. 2): 1) WEB-SCADA is to monitor and control the warehouse management system and display a simple indication of heat plant state, and 2) SCADA is used to control and monitor the heating plant. The following sections describe both SCADAs.

[7] Siemens LOGO! Soft Comfort - https://new.siemens.com/global/en/products/automation/systems/industrial/plc/logo/logo-software.html

[8] frostyICS - IACS cyber range for offensive capability development (https://github.com/austrisu/frostyICS)

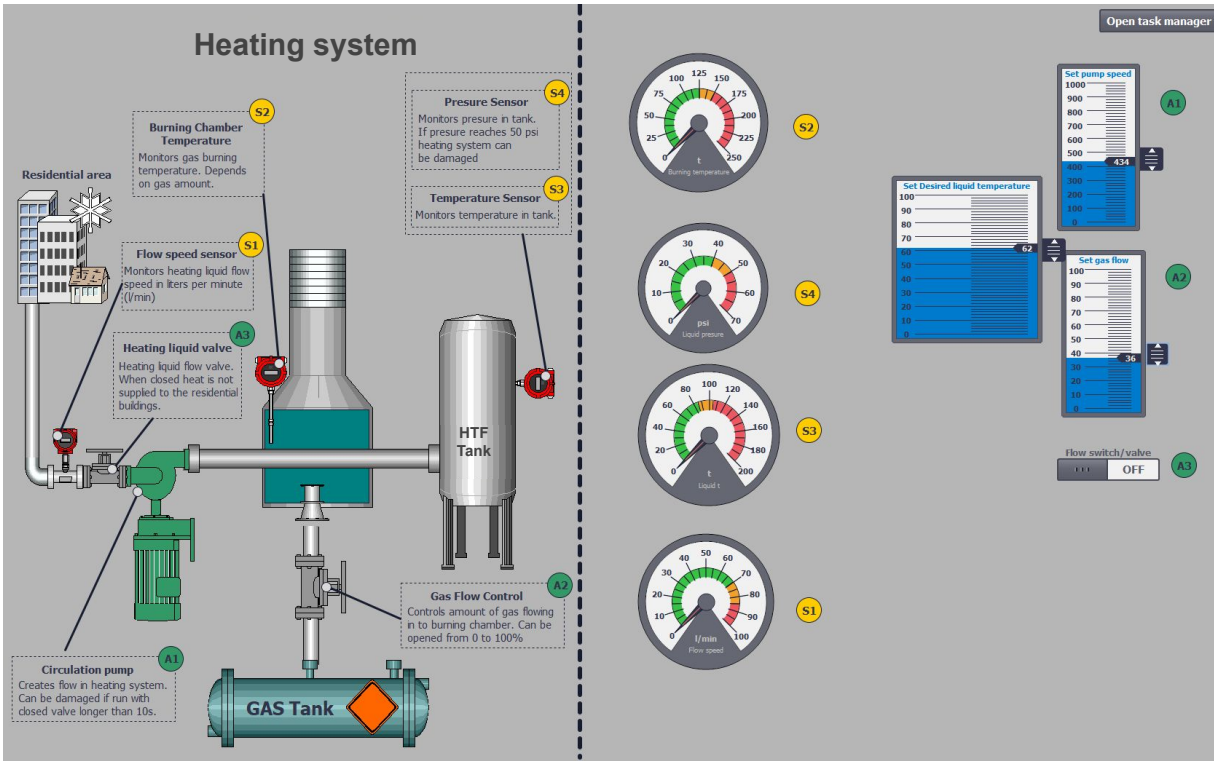


5 Figure: Siemens LOGO! program created by the author.

3.4.1. Heating plant SCADA

For the operator to visualize and interact with the process, SCADAs are used in this case. In this CR, SCADA can be used for an attacker to understand the state and purpose of the system. Heating plant is visualized using WinCC advanced V15.1 run-time (see Fig. 6). WinCC is the run-time of the HMI and SCADA system for use on MS Windows OS. WinCC software communicates with an automation system, reads a data block, displays process visualization, and allows an operator to interact with the automation system.

TIA portal advanced V15.1 is used to create the WinCC application. For this CR, both S7-1200 and WinCC applications are created under the same TIA portal project because this way, communication between two applications is established. Project structure is displayed in figure 7. Main parts of the application is located in folders *Screens* and *HMI tags*. *Screens* are where visualization of heating system is created. *HMI tags* are where mapping of S7-1200 and WinCC application variables, also called tags, is done. Therefore, making them available for both applications across the network.



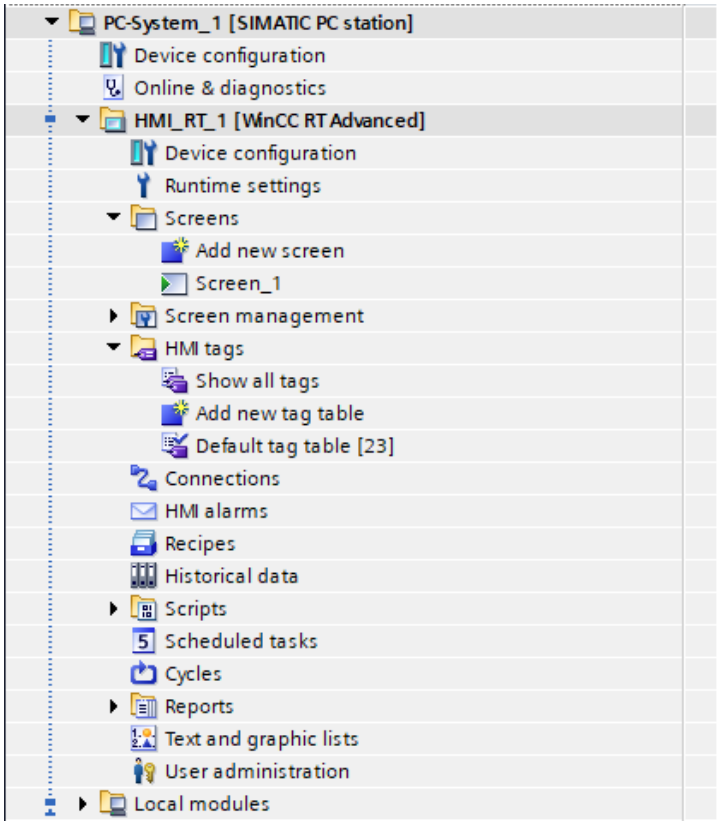
6 Figure: SCADA visualization screen created by the author.

3.4.2. Warehouse management WEB-SCADA

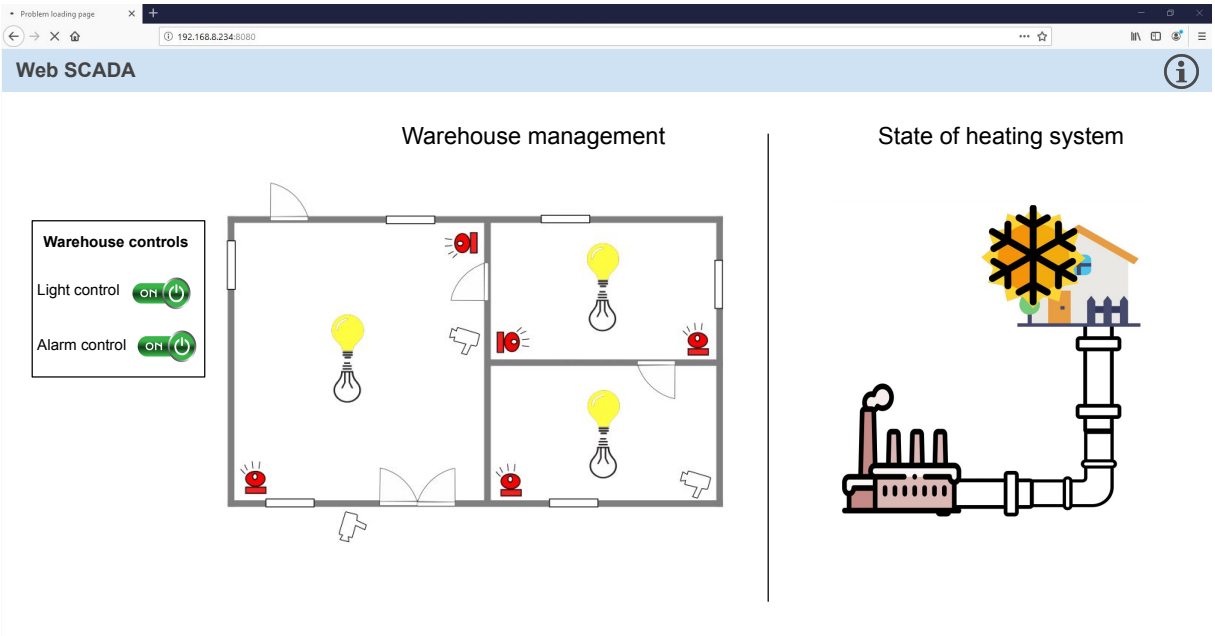
WEB-SCADA is different from conventional SCADA as it utilizes web technologies for visualization and usually can be accessible as a web page. For this CR, author utilizes web technologies such as NodeRed to create WEB-SCADA. Based on author's opinion and experience, some organizations cut corners and create simple web interfaces to control assets located in the field. Sometimes, due to a lack of budget, they create these solutions by themselves, possibly creating even more security risks.

Previously mentioned security gaps are the reason why for developing WEB-SCADA author chose NodeRed [9] which is a low-code platform where programming is similar to FBD. NodeRed is suitable for simple DIY system solutions sometimes encountered in IACS. Additionally, NodeRed is used in RevolutionPI [10], which is on RaspberryPi based PLC for industrial DIY projects. Overall, 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! about heating plant state. Visualization can be seen in figure 8.

[9] NodeRed - https://nodered.org/
[10] RevolutionPI - https://revolution.kunbus.com/



7 Figure: WinCC SCADA application structure created by the author.



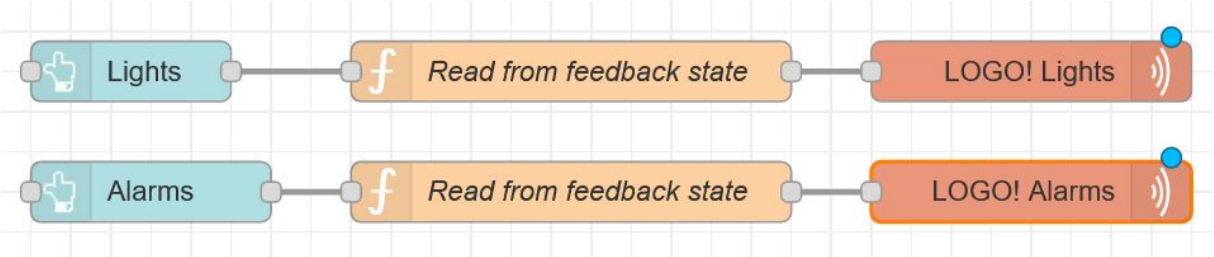
8 Figure: Warehouse management system visualization created by the author.

The WEB-SCADA application resides on the Siemens IOT2040 hardware, a budget industrial PC designed to withstand industrial environments. IOT2040 has two network interfaces. Hence, misconfiguration is introduced by connecting one interface directly to the enterprise network bypassing the IACS firewall (see Fig. 2). The misconfiguration of the CR network

represents an intentional or incorrect network configuration that bypasses the intended security mechanisms. The author believes these security vulnerabilities are common in the IACS segment, where automation engineers sometimes neglect IT safety procedures.

NodeRed application configuration is done using a web browser. Part of the authors created the WEB-SCADA application example is shown in figure 9. Application logic is executed from left to right, similar to in FBD programming language. Each of the blocks performs some functionality, and each block has input and output. A particular example in figure 9 shows how the control inputs from the user interface are sent to LOGO! using Modbus protocol:

1. Blocks with names *Lights* and *Alarms* receive input from the user interface shown in figure 8;
2. Blocks with the name *Read from feedback state* are custom functions that receive input from *Lights* and *Alarms*, compares previous light and alarm state, and inverts it;
3. Inverted state is sent to *LOGO! Lights* and *LOGO! Alarms* blocks which send this state over Modbus protocol to LOGO! 8.2.



9 Figure: Example of WEB-SCADA application created by the author.

3.5. Communication layout

Overall CR layout is presented in figure 2 and table 7. CR utilizes two main industrial protocols Modbus and S7comm. The author uses Modbus as it is commonly seen in different IACS networks. Thus, Modbus is applied to represent a realistic communication network. S7comm usage is bound to Siemens equipment as most of the Siemens components can communicate using S7comm protocol. Further, both of these protocols are described in detail.

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

Nr.	Component	Interaction partner	Protocol support	Running processes
1	SCADA	WEB-SCADA	S7comm, FTP	WinCC advanced V15.1, TIAportal advanced 15.1, FTP server
2	WEB-SCADA	PLC S7-1200, office workstations	Modbus, HTTP, SSH	Web server, NodeRed, SSH client
3	PLC LOGO! 8.2	PLC S7-1200, WEB-SCADA	S7comm, Modbus	Warehouse light and alarm control logic and I/O control
4	PLC S7-1200	SCADA, WEB-SCADA	S7comm, Modbus	Heating plant automation, heating plant HIL simulation

3.5.1. Modbus protocol

All of the detailed and official technical information about Modbus protocol is described in documents (Dube & Camerini, 2002; Modbus, 2021). Further, the author highlights particular Modbus technical aspects relevant for this CR, as well as conducted attacks in section 4.4.

						Application data	
General frame structure	Transaction Identifier	Protocol Identifier	Length in Bytes	Unit ID	Function Code	Data	
Size of frame sections	2 Bytes	2 Bytes	2 Bytes	1 Byte	1 Byte	Varies	
						Reference number	Bit count
Master read coil request	00 36	00	00 06	01	01	01 08	00 08
						Byte count	Values of requested coils
Slave response	00 36	00	00 04	01	01	01	00

10 Figure: Modbus general frame with examples for master and slave communication frames (Dube & Camerini, 2002; Modbus, 2021). Example frames are displayed in hexadecimal.

Documentation (Dube & Camerini, 2002; Modbus, 2021) mentions that Modbus is an open-source protocol developed in the year 1979 for serial communication. Initially, Modbus was used to work with serial communication, but with TCP/IP introduction in the IACS field, Modbus was adopted to work in the TCP/IP stack. Modbus/TCP has become the industry standard for transferring digital and analog I/O information. The protocol's simple implementation made it highly utilized in the IACS environment. Protocol communicates using master (client) and slave (server) architecture. The slave is usually a field-level device like PLC, RTU, or similar device controlling physical processes. Modbus/ TCP embeds a serial Modbus data frame into a TCP/IP frame. A typical master message will consist of function code, determining what action is required from the slave, and required data that depends on the function. Successful slave response includes function code and corresponding data. Function code contains a function number that is standardized but also can be created by a user. Almost all of the devices support six function codes shown in table 8. Examples of Modbus frames in successful communication between devices are displayed in figure 10. If function code is to write or read data from a device, then the data section frame includes memory address or range of addresses. Modbus addresses are mapped to the device memory.

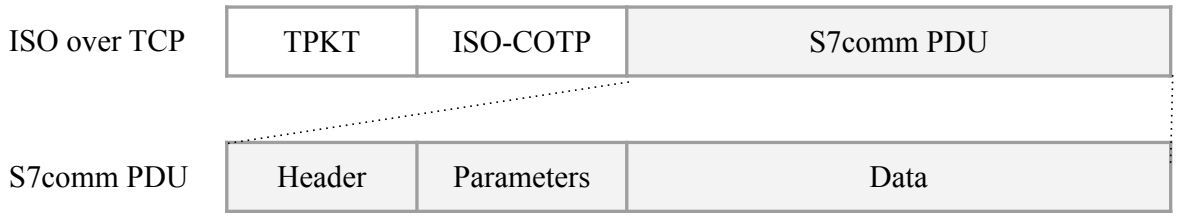
Modbus protocol contains various vulnerabilities such as lack of confidentiality, integrity, and authentication. Relevant vulnerabilities are described in the next chapter 4.

8 Table: Some of the standard Modbus function codes (Dube & Camerini, 2002).

Code in hex	**Function name**	**Description**
0x01	Read coil status	Reads 1 bit from memory space of the device. used for reading digital output state of the PLC
0x03	Read holding registers	Reads 2 bytes from memory space of the device. Used for retrieving analog inputs of the PLC
0x04	Reading input registers	Reads 1 bit from the device. Used to retrieve data about input state of PLC
0x05	Force single coil	Writes 1 bit to the memory of slave.
0x0F	Force multiple coils	Writes multiple 1bit values to the slave memory.

3.5.2. S7comm protocol

S7comm protocol is Siemens proprietary protocol, meaning it does not have detailed official documentation. However, as it is popular, it has been reverse-engineered and thoroughly



11 Figure: S7comm protocol frame (Miru, 2016a, 2016b).

described in different documents and researches (Biham et al., 2019; Miru, 2016a, 2016b; Snap7, 2021; Wireshark, 2021a). Further, the author highlights particular S7comm technical aspects relevant for this CR, as well as conducted attacks in section 4.4.

Summarizing relevant information from (Biham et al., 2019; Miru, 2016a, 2016b; Snap7, 2021; Wireshark, 2021a), S7comm protocol or also called Step7, is an industrial protocol created by Siemens based on ISO 8073 (Wireshark, 2021b) protocol. S7comm protocol is a standard for communicating and programming all Siemens S7 PLCs. This protocol is also utilized for Siemens HMI and SCADA communication. The S7comm is based on TCP/IP, but lacks encryption and authorization. Therefore, it is relatively easy to inject rogue commands into the target. Like Modbus, this protocol works using the master-slave model. This protocol is function-oriented, where master transmission consists of requests. S7comm Protocol Data Unit (PDU) is encapsulated in TPKT and ISO 8073 (Wireshark, 2021b) protocols and is presented in figure 11. To exploit the protocol, PDU is the part attacker manipulates. The header contains length information, PDU reference, and message type. Parameters contain function code and function code related information. Data is an optional field required by some function codes. Step7 closely relies upon the PLC program architecture. The protocol requires to specify DB or FB and tags to modify them. For some PLCs, S7comm can update not just only tag values but also the whole PLC program. For an attacker to exploit this protocol library, Snap7 (Snap7, 2021) is used since the most important protocol functionality is included in this library.

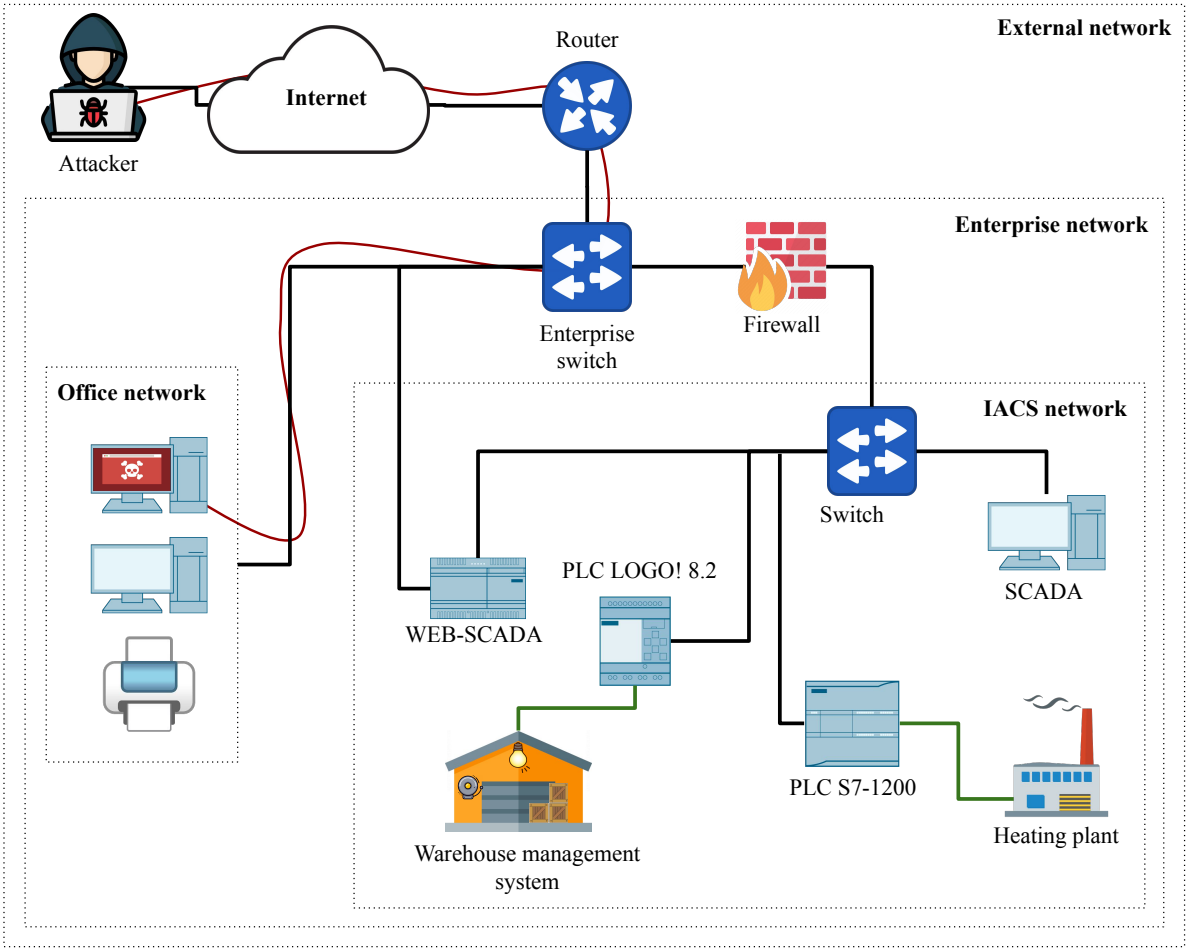
This protocol has a updated version called S7commPlus, which encrypts the data, increasing security. Research (Lei et al., 2017) describes that the S7commPlus encryption can be broken. However, S7commPlus protocol is not in the scope of this research as IACS elements used in this CR cannot fully support this protocol (Beresford, 2011; Miru, 2016a; Wireshark, 2021a).

4. ATTACK DESIGN

Created CR was used to conduct offensive cybersecurity exercise. This chapter describes the exercise attack scenario, possible attack vectors, and execution steps. Section 4.1. describes an environment scenario where the attacker needs to fulfill objectives. Section 4.2. describes attack frameworks and approaches and chooses one which can be used to describe attacker actions and decisions for the scenario. Section 4.3. offers attack vectors which participants can use during the exercise. Section 4.4. describes executed attacks on CR to achieve the objectives. Section 4.5. explains practical workshop execution steps.

4.1. Threat scenario

Based on information in literature review 2.2., attackers use routes through the Internet, business, or enterprise networks and down the level of field devices to attack IACS systems. Then, gaining a foothold into the enterprise network, attackers can traverse the network till finding access to the IACS systems. Zhu et al. (Zhu et al., 2011) states that common attack vectors are backdoors, rootkits, holes in network perimeter, vulnerabilities in standard protocols, communications hijacking, and man-in-the-middle attacks. This is considered when deciding the initial position of the attacker for this threat scenario. Hence, in this scenario, the attacker has gained persistent access to the enterprise network and has established an internal proxy inside the office network. The establishment of this initial position is out of scope for this research and will not be discussed. The initial state of the scenario is shown in figure 12. 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. Second is the IACS network containing heating plant and warehouse management system described in chapter 3.. In this case office network does not contain any devices as it is out of scope for this exercise and is not required to complete attacks in the IACS network. The displayed structure has informative nature for participants to facilitate the overall idea of the scenario. Therefore, only the IACS network contains actual devices.



12 Figure: IACS CR threat scenario topology created by the author.

With participants in this exercise, the author understands cybersecurity experts with knowledge in IACS systems. In this scenario, the participant plays as the red team and has two main objectives, which can be achieved by any tools possible, but mainly self-created Python scripts are encouraged:

1. Switch off warehouse lights and alarm, and prevent system recovery;
2. Damage heating plant and prevent system recovery.

4.2. Attack structure

Adversary attacks usually consist of multiple steps to achieve the objectives. Each of these steps includes TTPs. As described in NIST Glossary (NIST, 2021), TTPs are adversary behavior where tactics are high-level procedures and techniques are specific actions the attacker makes in the context of the specific technique. The chain of these steps is called the kill chain. In other words, the cyberattack kill chain is steps that trace stages of a cyberattack from the initial reconnaissance stage to the final actions (Zhou et al., 2018). The author has found three different

kill chain approaches - Lockheed-Martin Kill Chain, ICS kill chain, and MITRE ATT&CK TTPs knowledge base. It worth mentioning that the cyber kill chain is a concept used for defense to understand and predict attacker TTPs. For this research purposes kill chain is not used for defense but for attack scenario structure development.

Term kill chain was first used by Lockheed-Martin (Lockheed-Martin, 2018). Lockheed-Martin Kill chain is used to understand and counter adversary's actions in each step of attack - reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives.

Research Zhou et al. (Zhou et al., 2018) has adapted Lockheed-Martin (Lockheed-Martin, 2018) kill chain for use in IACS field. The author proposed to nest kill chains in 3 stages. The external kill chain is meant to breach the enterprise network perimeter. The internal kill chain is to gain access to the IACS network, and ICS kill chain is used to implement the final attack on IACS processes. Each of the processes iterates through Lockheed-Martin (Lockheed-Martin, 2018) kill chain.

Both approaches (Lockheed-Martin, 2018; Zhou et al., 2018) look at attacker actions from the perspective of defense operations. Hence, the author concludes that this attack structure is not suitable for this scenario. Moreover, it lacks depth in attacker actions.

Yet another approach to attack classification is MITRE ATT&CK (MITRE ATT&CK®, 2021). This framework focuses more on attacks from the attacker's viewpoint. MITRE ATT&CK TTPs knowledge base describes an adversary's actions to gain access, compromise, and operate within the target network. This TTPs knowledge base gives a deeper level of granularity in describing what can occur during an intrusion. In addition, attackers and defenders can utilize MITRE ATT&CK TTPs to describe attacks using them in any order since threat actor's approaches are often creative and not standardized. MITRE ATT&CK seeks to classify the attacker's goals, tasks, and steps. Thus, it is a much more comprehensive approach for attack modeling. MITRE ATT&CK uses tactics to describe the adversary's goals for specific attack stages and techniques to describe how attackers can reach the goal. It is worth mentioning that these TTPs can deviate according to the actual target situation during the attack. Therefore an attacker can also skip some of the tactics.

Tactics are summarized as follows (MITRE ATT&CK®, 2021):

- Reconnaissance - preparing for the attack by gathering information about target;

- Resource development - gathering resources to support operations;
- Initial access - obtaining an initial foothold into target system;
- Execution - trying to run malicious payload code on target systems;
- Persistence - retain access to systems across restarts and other target system interruptions;
- Privilege escalation - obtain higher-level permissions on a system;
- Defense evasion - an adversary attempts to avoid the detection;
- Credential access - stealing accounts names and passwords;
- Discovery - gain information about internal networks and systems;
- Lateral movement - exploring the network by moving through the environment;
- Collection - collecting data of importance to the adversary objective;
- Command and control - establishing communication channels with compromised systems to control them;
- Exfiltration - stealing data of interest;
- Impact - interrupt, manipulate or destroy systems and data.

The author considers MITRE ATT&CK TTPs knowledge base as most suitable for this research for two reasons. Firstly, this framework views attack from the attacker's perspective and encompasses broad attack techniques, and secondly, MITRE ATT&CK tactics can be shaped and rearranged to match specific needs.

A complete list of MITRE ATT&CK tactics is unnecessary for this threat scenario, as the attacker has already gained stable access to the office network. Therefore, the author proposes to use only the following tactics for each network segment:

1. Tactics in office network:

   Discovery - looking for available devices in the office network;

   Lateral movement - attacker spreading to other devices;

   Persistence - attacker gains stable access network devices to gains access to IACS network;

Command and control - attacker uses techniques to establish communication with the compromised system.

2. Tactics in IACS network:

   Discovery - Looking for available devices in the IACS network, discovering open ports, and discovering IACS processes controlled by the IACS network;

   Collection - Extracting detailed information about IACS elements and their purpose;

   Impact - actions on objectives.

4.3. Attack vectors

Across literature there is multiple definitions of attack vector (Kaspersky Lab, 2021b; PCMag, 2021; Shacklett, 2021). The author in this work interprets the term attack vector as one or more vulnerabilities, permitting attack against the target system. Attack vectors used in this threat scenario (see Section 4.1.) is listed in table 9. Author has included listed vulnerabilities for the CR has based on two considerations. The first one is based on hardware and software capabilities, and the second is based on common vulnerabilities listed in reports (Andreeva et al., 2016; MITRE, 2020).

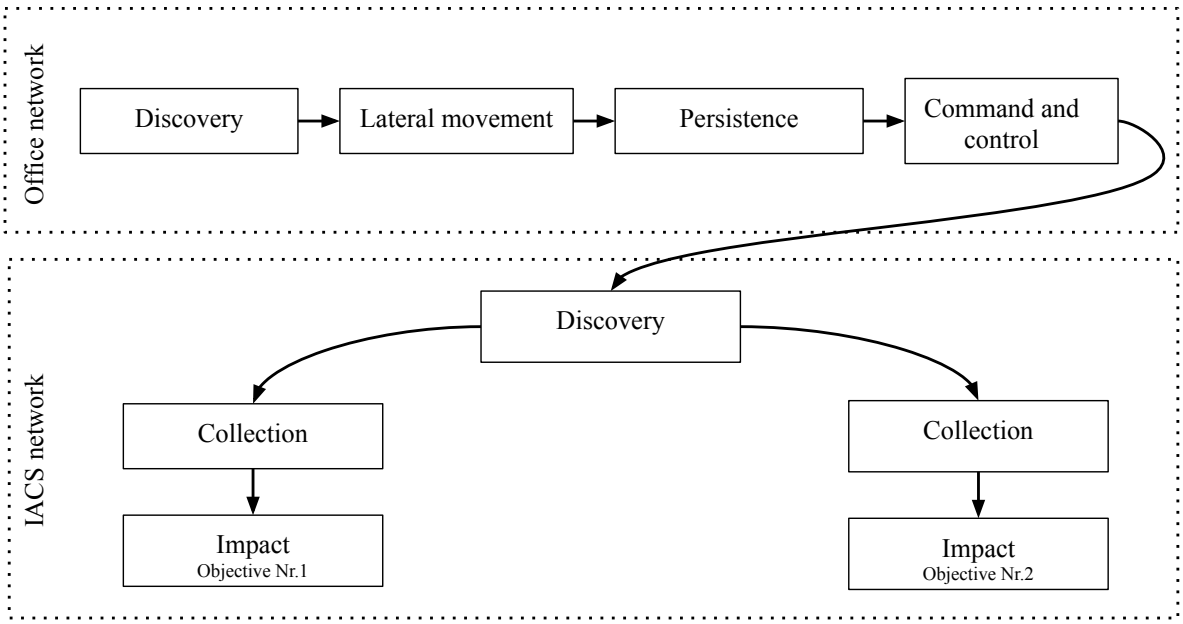
9 Table: Implemented security flaws by the author.

Nr.	**Name**	**System element**	**Description**
1	Lack of network segmentation	Network	Lack of segmentation between warehouse and heating plant systems
2	Topology misconfiguration	Network	web-SCADA has two interfaces, where one interface is connected directly to the office network bypassing IACS firewall and security
3	Weak credentials	WEB-SCADA	Credentials of NodeRed configuration are too week
4	Lack of user privilege separation	WEB-SCADA	NodeRed is run by only user on system which has root privileges
5	Modbus are not limited to specific master device	LOGO! 8.2	LOGO! Can receive Modbus requests from any device in the network

6	Modbus built in vulnerability	LOGO! 8.2	Modbus communication protocol vulnerabilities as lacks authentication and encryption
7	Buffer overflow	LOGO! 8.2	LOGO!8.2 version suffers from web-server buffer overflow vulnerability CVE-2020-7593 (Perez-Palma & McDaniel, 2020)
8	Lack of security in PLC configuration	S7-1200	S7comm protocol PUT GET commands allows attacker to execute various read and write attacks.
9	TIAportal project lacks protection	S7-1200	S7-1200 project can be downloaded, viewed, and updated
10	FTP server with anonymous access	SCADA	MS Windows 7 workstation FTP server allows anonymous authentication

4.4. Attack execution

Overview of attack execution structured by segments and objectives is displayed in figure 13. In the following subsections, each attack phase is described in detail. Used vulnerabilities in flowing scenario are designed and created by the author.



13 Figure: Attack execution graph divided by network segment and objectives, based on MITRE ATT&CK knowledge base.

4.4.1. Discovery in office network

This is the initial phase, so the network wise the attacker is in initial position in office network (see Fig. 12). Based on MITRE ATT&CK knowledge base, the attacker can perform network scanning and enumeration to identify services running on remote hosts. Attacker may use Nmap [11] to discover remote hosts. The scan reveals 22/tcp, 80/tcp, 8080/tcp open ports on the IOT2040 device.

The attacker can then use a web browser to access the webpage running on port 80/tcp and determine it is WEB-SCADA, which controls the warehouse management system. Therefore, this device is connected to the IACS network. Next, the attacker performs a thorough check of services running on the WEB-SCADA and discovers NodeRed running on this device. Thus, NodeRed is the attack vector in the lateral movement phase.

4.4.2. Lateral movement

During this phase, the attacker performs actions to gain a foothold to the WEB-SCADA device and change network position (see Fig. 12).

One of the possible ways to gain access to the WEB-SCADA attacker is to perform remote code execution by modifying the NodeRed application running on IOT2040. The attacker can adjust the NodeRed application by introducing a function block named *exec* which executes shell commands directly on the target machine. Hence attacker can execute any command on the target device by injecting it to the *exec* as shown in 14. The executed command is reverse shell:

```
bash -i >& /dev/tcp/{Attacker IP}/4445 0>&1
```

Reverse shell command connects to attackers machine listening on port 4445/tcp using NetCat listener command:

```
nc -lvp 4445
```

Now the attacker have gained access to WEB-SCADA shell. As the NodeRed service runs with root privileges, the attacker gains root shell access. From here, the attacker may discover that the IOT2040 has two network interfaces, one connected to the office network and the second one to the IACS network. Also, now the attacker discover that the IACS network is responsible for controlling warehouse management and heat plant systems.

[11] Nmap - https://nmap.org/https://nmap.org/

14 Figure: Example of NodeRed application modification for reverse shell execution.

4.4.3. Persistence

To gain persistent access to the newly captured device attacker can utilize gained root shell to WEB-SCADA. Attacker performs account manipulation by modifying the SSH */.ssh/authorized_keys* file. Attacker inserts his generated SSH public key into the file. The *authorized_keys* file in SSH identifies the SSH keys used to log in to the user account. After this step attacker can connect to the IOT2040 by using a standard SSH connection. That allows for the attacker to maintain access to the machine even if the device restarts.

4.4.4. Command and control

Through this step, the attacker configures IOT2040 to work as an internal proxy to redirect traffic from the attacker to the target network, in this case, IACS. In addition, proxying also reduces numerous connections to external systems, hence concealing the adversary's actions.

The attacker can use numerous tools and techniques to create the proxy. However, as every tool and technique cannot be described here, the author must limit choice between the two techniques. Each of them has some drawbacks and advantages. One is using proxychains, and the second is to configure Linux to work as a router:

Proxychains are created utilizing ssh local port forwarding. The attacker executes command:

```
ssh -i key.private -L 4040 localhost:5050 iot2040@{IOT2040 IP}
```

This command create SSH tunnel from attacker machine to IOT2040. This tunnel forwards all traffic from the attacker's local port 4040/tcp to remote device port 5050/tcp. Now the attacker can pipe the traffic from the attacker machine through the tunnel to the IACS network using Linux command *proxychains*. First, the attacker needs to configure proxy chains by adding SOCKS4 proxy to */etc/proxychains.conf*. For example, for the attacker to scan devices on the IACS network, he can append *proxychains* before the command, like so

```
proxychains nmap -n -Pn -sT -T2 {target IP range}
```

.

The drawback of this technique is the limitation of network scans, as a proxy cannot support ICMP, SYN stealth scans, and OS detection. In this case, the attacker is limited to simple TCP connections.

Routing is a convenient way to send traffic to and from the attacker. To set the IOT2040 Linux machine to work as a router attacker needs to enable IP forwarding by executing:

```
sysctl net.ipv4.ip_forward=1
```

, set NAT rule with

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

, and accept traffic from eth0 interface:

```
iptables -A INPUT -i eth0 -j ACCEPT
```

Using this method, all traffic sent on one IOT2040 network interface is routed to the second interface. The drawback of this method is the lack of traffic obfuscation to reduce attacker detection.

4.4.5. Discovery in IACS network

In this stage, the attacker tries to enumerate devices in the IACS environment and learn about the internal network. To do so, the attacker scans the network using Nmap or other noninvasive network enumeration techniques. Nmap scan in IACS network should be limited in speed and complexity of the scan as PLCs have limited computing capacity and can be overwhelmed with too many requests. Research (Ljøsne, 2019) has done extensive investigation on Nmap scans against different PLCs and suggests limiting Nmap to SYN or ARP scan with reduced speed setting of -T2 (0.4s).

Through this step, the attacker can locate three other devices in the network, where two of them are PLCs with open ports 102/tcp and 502/tcp. Port 102/tcp is standard for S7comm communication, and 502/tcp is typical for Modbus. The third device is SCADA (see Fig. 12). From this position, the attacker can act on PLCs, as they directly control physical processes.

4.4.6. Objective Nr.1 - warehouse attack

The first objective for the attacker is to *switch off warehouse lights and alarm and prevent system recovery*. This objective is focused on the warehouse management system. Next are the steps attacker takes to acquire this objective.

4.4.6.1. Collection

During the collection stage, the attacker attempts to get information about the target system, in this case, the warehouse management system controlled by LOGO! 8.2 . Techniques used in this stage facilitate attacker to obtain contextual feedback and how the physical system operates.

For the attacker to gain more insights, he can download the PLC configuration file from the memory of the LOGO! 8.2. It can be done by utilizing Siemens LOGO! Soft Comfort configuration software described in section 3.3. From the captured PLC program attacker can determine memory locations that should be targeted using Modbus protocol vulnerabilities. LOGO! 8.2 application with used address are presented in figure 5.

4.4.6.2. Impact

During the impact stage, the attacker tries to manipulate, disrupt or impair IACS systems and controlled physical processes. In this particular case, the attacker performs manipulation of control by sending rough Modbus commands to LOGO! 8.2. Furthermore, he performs a denial of control attack.

10 Table: LOGO! 8.2 address type and Modbus mapping.

Address Type	**Range**	**Mapped Modbus address**
Inputs (I)	1 – 24	Digital inputs 1 – 24
Outputs (Q)	1 – 20	Coil – 8193 – 8212
Data block 1 (V)	0.0 – 850.7	Coil 1 – 6808

To perform control manipulation, the attacker uses information gathered from the collection phase. For the attacker to switch off the lights and alarms, he needs to control a specific LOGO! 8.2 variables *V10.1* and *V10.2*. Derived from LOGO! 8.2 user documentation are Modbus address mapping shown in figure 10. Using this information attacker sends Modbus commands, changing the state of addresses 82 and 83 from true to false. Function code for writing to memory is *0x05* (see Tab. 8). An example of a crafted Modbus packet in hexadecimal is displayed in figure 15. Created Modbus frame is encapsulated in TCP/IP packet and sent to the destination. Python script example created by the author for this scenario can be seen in GitHub [12].

To impair the functionality and availability of the warehouse management system, the attacker can perform two types of attack. First is the Denial of Service (DoS) attack exploiting

[12]Modbus proof of concept scripts created by the author. - (https://github.com/austrisu/ICS_poc)

General frame structure	Transaction Identifier	Protocol Identifier	Length in Bytes	Unit ID	Function Code	Reference number	Bit state
Master read coil request	00 3C	00	00 06	01	05	00 52	00 00

15 Figure: Attacker constructed Modbus frame example.

LOGO! 8.2 firmware vulnerability. The second is to modify the LOGO! 8.2 application so that it does not respond to any requests.

DoS attack exploits a buffer overflow in LOGO! 8.2 firmware. To perform this attack participant sends an HTTP request to LOGO! 8.2 built-in web server with too long path. As the web page does not check for the length of supplied string, it results in overriding memory outside the allowed memory space causing LOGO! 8.2 to crash and restart. This vulnerability is described in CVE-2020-7593 (Perez-Palma & McDaniel, 2020). In practice, DoS can be achieved by cyclically running the command:

```
curl http://{LOGO! IP}/`python -c 'print("A"*100)'`/
```

The second way to impair warehouse management is to update LOGO! 8.2 program. That can be done by using Siemens LOGO! Soft Comfort described in section 3.3.

4.4.7. Objective Nr.2 - heat plant attack

The next objective is to disable and damage the heating of the city and prevent system recovery. Following are the tactics attacker takes to acquire this objective.

4.4.7.1. Collection

During this stage, the attacker tries to get information about the target system, in this case, the heating plant controlled by S7-1200 PLC (see Fig. 12). Techniques used in this stage facilitate attacker to obtain contextual feedback and how the physical system operates.

S7-1200 program includes two parts: control logic and HIL simulation of the heating process. Hence, the part responsible for physical system simulation is off-limits for the CR participants. Therefore, attacks are directed only to the control logic part.

The attacker can gather additional information about the state of the heating plant by getting access to the PLC program. As PLC program download is password protected, for that reason, the attacker cannot gain access to it. However, a copy of this program is located in the SCADA

workstations FTP server. The FTP server runs with anonymous access. Therefore, the attacker can download the program and examine it with TIAportal described in section 3.2..

4.4.7.2. Impact

During the impact stage, the attacker tries to manipulate, disrupt or impair IACS systems and controlled physical processes. The main vulnerabilities of S7-1200 are bound to the S7comm protocol. For the attacker to exploit protocol vulnerabilities, he needs to understand the program structure gathered during collection phase.

From the downloaded S7-1200 program, the attacker can determine what tags are responsible for specific physical function control. These tags are shown in table 11. Each tag name has assigned the data block number and memory offset within that data block. These are the parameters necessary to send the S7comm control request to the PLC.

11 Table: S7-1200 tags, relevant for the attack.

Tag name	**Data type**	**Memory offset**	**Data block**
temperature_setpoint	int	0.0	DB6
max_pressure	int	2.0	DB6
pump_speed	int	0.0	DB9
valve_state	bool	2.0	DB9

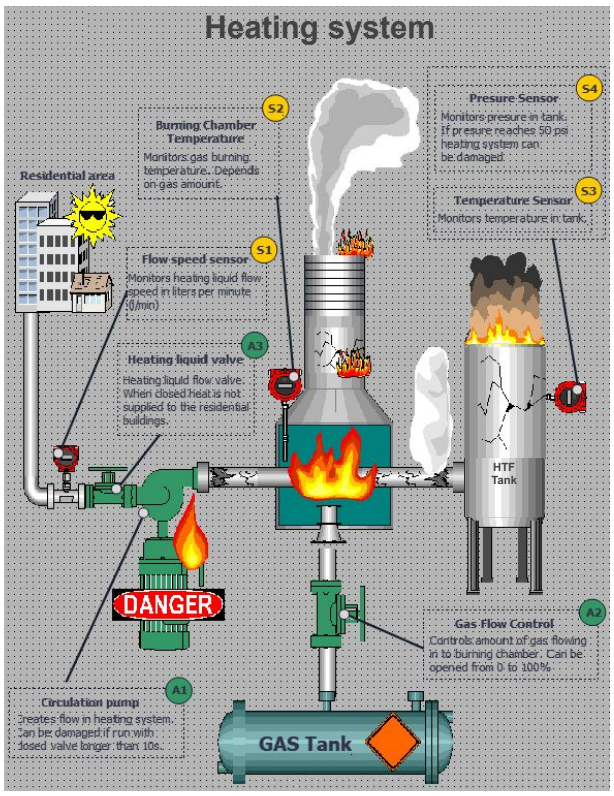
The attacker can send crafted S7comm requests to PLC using Python script with S7comm library called Snap7 [13]. Before using the Snap7 library, it should be compiled from the source, and the high-level Python wrapper can use the Snap7 library. The author created a Python script example for this scenario is located in GitHub [14].

This attack process can be divided into two steps. The first one is to damage the circulation pump (see Fig. 6 A1), and the second is to damage the whole heating system:

1. To damage the circulation pump, the attacker needs to close the valve A3 (see Fig. 3) controlling HTF flow to the city districts and keep the circulation pump A1 (see Fig. 3) running. Hence, the attacker sets *pump_speed* to nominal value and *valve_state* to false, thus, closing the valve A3. Physical system limitations allow the pump to operate under such conditions for 10 seconds after that pump gets damaged and cannot be controlled

[13] Snap7 - http://snap7.sourceforge.net/

[14] S7comm proof of concept scripts created by the author. - https://github.com/austrisu/ICS_poc



16 Figure: Heating system state seen in the SCADA after attack to S7-1200 PLC created by the author.

anymore.

2. To damage the heating plant, the attacker needs to overheat and overpressurize the system by setting a tag *temperature_setpoint* above 100 °C. This will increase gas flow to the burning chamber and raise the HTF temperature. However, the PLC program has safeguards. When the system's temperature and pressure reach the maximum value, PLC protects the process by extinguishing the furnace and alarms the operator. Therefore, before adjusting the setpoint, the attacker needs to increase *max_presure* tag value above 60 psi to remove implemented safeguards.

After the successful execution of the attack, the SCADA screen shows a damaged simulated heating plant, seen in figure 16. After these attacks, the physical process is impaired, and recovery can be made only by physical repair. However, as the physical process is simulated then no damage is done to actual CR physical devices.

4.5. Training conclusion

One of the main goals for creating IACS CR was to provide an environment for practicing offensive capabilities where participants can try attacks on IACS elements and observe their impact. For that reason author developed an exercise using the scenario described in section 4.

This exercise was conducted for five participants who are experts in the cybersecurity field and some of them had a background in IACS. Each participant had dedicated CR, thereby, for this exercise, five sets of CR were used.

As the exercise aimed to develop an offensive skillset in the IACS field for the participants, the author also created a supporting presentation to guide the participants. Author's created presentation can be found in GitHub repository [15].

The successful completion of the course was determined by the fact, whether the participants reached the objectives (see Sec. 4.1.). The exercise took a little less than two days during which all participants attained scenario objectives for both physical systems. After the exercise, participants were asked to fill the feedback form. Summary of the feedback form questions in respective order are:

1. Were the tasks and achievable results understandable?
2. Does this exercise help to understand industrial control systems better?
3. Did this cyber range increase knowledge about cybersecurity risks in IACS systems?
4. Is the knowledge provided useful?

Detailed examination of the feedback data is in chapter 6.. The summary of the feedback form is listed in Appendix II.

[15] frostyICS - IACS cyber range for offensive capability development (https://github.com/austrisu/frostyICS)

5. ECONOMIC JUSTIFICATION AND ANALYSIS OF SOCIO-TECHNICAL FACTORS

The project is created to be open-source under MIT license and is not meant to be monetizing. As this system are available openly to organizations, companies or individuals will have the opportunity to replicate the project and train offensive IACS capabilities. This project can be found in GitHub repository frostyICS [16]. Time to create the research is estimated for 800 hours.

To calculate implementation cost, prices are acquired from publicly available sources. These prices could vary based on country. Price calculation is shown in table 12 and the total hardware and software cost of one set is around 1 100 EUR.

12 Table: Price calculation of one set of CR.

Nr	Name	Unit price, EUR
1	SIMATIC S7-1200 Starter-Kit: CPU 1212C, STEP 7 Basic V16	700.00
2	IOT2040	210.00
3	LOGO! starter kit: LOGO! V8.3, LOGO! Soft Comfort, WinCC , power supply	100.00
4	MS Windows 7 enterprise trial	0.00
5	NodeRed, open-source software	0.00
		1010.00

From a financial point of view, it is difficult to compare other created cyber ranges as there is a lack of such financial information in the research. Although IACS courses that claim to encompass cyber ranges can be found, and price ranges for them vary from a couple of thousands per person (SANS, 2021) to a couple of hundreds per year (DiTechSolutions, 2021). However, it is hard to determine the exact training scope and what type of cyber ranges are used. Based on that and the author concludes that the CR is somewhere in the middle of the price range.

[16] frostyICS - IACS cyber range for offensive capability development (https://github.com/austrisu/frostyICS)

Hence, the price is reasonable considering the system's complexity. Moreover, from the author's experience, similar physical system automation usually costs more than ten times the CR cost.

Theoretical market volume can be estimated by looking at the need for offensive capability development exercise. As mentioned in section 2.2.5., offensive capabilities are necessary for both private and government sectors. As IACS is getting more interconnected and more interesting for adversaries, governments will need to defend their critical infrastructure using offensive operations. Likewise, the private sector will need to conduct penetration tests on critical infrastructure to protect IACS from future threats. Thus, CR has the potential to be used by companies and government structures worldwide and, more specifically, in countries where Siemens products are strongly utilized.

Created CR has the potential for a positive influence on cybersecurity improvements in the IACS field. It will allow for offensive operation training and exercise. In that way, it is increasing understanding and awareness of adversary capabilities in the IACS segment. This CR being open source gives groups and individuals to increase skill sets. It also can shape the cybersecurity community by providing a chance to contribute to this project and improve it.

6. CONCLUSION

The general direction of the master thesis is to create the mobile IACS cyber range prototype where the red team can practice developing offensive capabilities. Cyber range should encompass the following key aspects:

- realistic;
- easily reproducible;
- with publicly available documentation;
- supporting multi-stage attack scenarios.

The created cyber range can be used in red team offensive capability development exercises in the IACS field, thereby improving understanding of IACS red team tactics and techniques. Understanding red team capabilities also provides knowledge on how to defend IACS. The author intends that individuals and private or government entities can utilize this CR for offensive exercises development by any suitable means. Using created CR, the author has developed and conducted a red team offensive exercise, which was described in chapter 4.

Based on the literature review, IACS testbed and CR development will continue to be essential in cybersecurity research, as CRs can facilitate research about attack surfaces in the IACS segment. However, despite numerous studies in this area, there is a lack of openly documented CR projects, especially in physical testbed areas. This affects the academic, business, and government sectors.

6.1. Answering research questions

RQ1: What are the main objectives IACS cyber ranges and testbeds are created for? Based on literature review (see Sec. 2.2.), CR objectives are intrusion detection system evaluation and testing, assessment of attack impact on physical systems, training to help beginners to overcome the barrier of proprietary IACS systems, test new security mechanisms, offensive and defensive

operation training, and for use in CTF events. The author has chosen to build IACS cyber range to support offensive capability development in the IACS field as the topic of offensive capabilities is gaining popularity. Already some countries have openly stated that they have offensive capabilities. Furthermore, as the IACS infrastructure includes more general-purpose and standardized elements, protocols, and topologies, adversary interest in IACS is growing. Hence, public and private entities will need to have offensive capabilities to perform responsive operations against adversaries. Also, the private segment needs to create offensive capabilities to test their IACS systems to prevent future attacks. This RQ is observed in section 2.2.2.

RQ2: What are the IACS cyber range development criteria for CR to be used in offensive exercises? The main development criteria for testbeds and CR is repeatability, fidelity, safe execution, diverse physical process, legacy device incorporation, support of standard protocols, ease of deployment. This master thesis CR emphasizes on fidelity, repeatability, support of standard protocols, and ease of deployment. This RQ is viewed in section 2.2.2.

RQ3: How to build IACS cyber rages to resemble realistic systems? Identified characteristics to build a realistic CR include hardware IACS components from different vendors and controlled physical processes, which should create complex scenarios where physical processes influence one another. Most of the current research limits testbeds and cyber ranges with communication-based vulnerabilities and does not focus on the controlled physical system. Considering this research limitation, the author has tried to encompass the following aspects into the CR to increase real system resemblance:

- CR encompasses both physical and virtual components, where physical components increase systems fidelity and virtualized elements allow for the testbed to be easy to recreate, as well as reduce cost;
- The controlled physical process includes two physical systems, where the heating plant has interdependent physical processes.

This RQ is observed in chapter 3.

6.2. Evaluation of cyber range

The author divides the evaluation of the created CR into three parts: 1) support by companies and organizations, 2) cyber range feedback from exerciser participants, 3) covered identified gaps. In the study, the author interprets evaluation as system analysis without specific criteria based on collected feedback described in section 4.5. and personal experience.

6.2.1. Support of companies and organizations

In the author's opinion, one way to measure the relevance of the conducted research is by asking principal acknowledgment in the form of a support letter from the industry. Therefore, the author has asked multiple Latvian organizations and institutions involved with critical infrastructures and the IACS field for conceptual acknowledgment. Following is the list of companies and organizations that recognize the research topic as important and justify the work's practical significance. Support letters are included in Appendix I:

- Vidzemes University of Applied Sciences;
- Riga Technical University;
- National Guard Cyber Defense Unit;
- SIA "Latvijas Mobīlai Telefons";
- Siemens OY Latvian branch;
- CERT.LV;
- AS "Latvenergo";
- AS "Gaso".

6.2.2. CR feedback from exerciser participants

One of the main goals for creating IACS CR was to provide an environment for practicing offensive capabilities where participants can attempt to attacks on IACS elements and observe their impact. For that reason, the author has developed an exercise using the scenario described in section 4.. After the exercise, participants were asked to give feedback in the form of pull about the usefulness and usability of the developed CR. The summary of pull is showed in Appendix II.

The exercise was conducted once, and during the executed scenario, five participants took part and performed attacks to achieve intended attack objectives. In the author's opinion, a number of participants for this research was sufficient as they should be from a specific target audience with particular knowledge and skillsets about cybersecurity and IACS.

Feedback polls are shown in Appendix II. A feedback poll consists of four questions that can be graded on a scale from one to five, where 1 - very bad, 2 - bad, 3 - satisfactorily, 4 - good, 5 - very good.

Feedback form questions and their description in respective order is:

1. Were the tasks and achievable results understandable? - to understand whether the attack scenario was clear and understandable;
2. Does this exercise help to understand industrial control systems better? - to understand whether participants have new insights into attack scenarios in IACS networks;
3. Did this cyber range increase knowledge about cybersecurity risks in IACS systems? - to understand how much information participants learned;
4. Is the knowledge provided useful? - to understand whether participants can apply gained knowledge in the future.

Based on the participant's feedback grade exercise grade was 4.6. Thus, the author can conclude that created CR is a good environment where participants can experiment and practice developing offensive capabilities in the IACS field.

6.2.3. Covered identified gaps

Identified gaps during the literature review and the author's personal opinions are used for the final evaluation how the created IACS CR covers them.

One identified gap was the lack of detailed documentation providing the means to reproduce physical IACS CR easily. In the author's opinion, this research fulfills this statement as this master thesis LaTeXsource code, complete documentation together with PLCs and SCADAs configurations is available publicly in GitHub [17] [18] to replicate the CR.

The second identified gap was the lack of CRs meant for offensive exercise development. This research not just creates CR for single-use. The author has created and published documentation, configuration files, exercise material, and this master thesis itself to be accessible for everyone publicly, hence increasing possibility to develop upon this research. In the author's opinion, these actions cover the identified gap as well as possible.

The last identified gap was portability, meaning IACS CR should be easily to move from one place to another and relatively easy to assemble and disassemble. During the exercise time to set up five sets of CRs took around three hours. In the author's opinion, this time is reasonable to consider created CR portable.

[17] frostyICS - IACS cyber range for offensive capability development (https://github.com/austrisu/frostyICS)
[18] Master thesis LaTeXsource code - (https://github.com/austrisu/master_thesis)

6.3. Future work

In a final summary, based on the conducted research, the author suggests directions for future research:

- CR for offensive capability development should also include security elements, such as, honeypots, intrusion detection systems, and similar elements, in order to increase the difficulty and create even more realistic scenarios;
- CR should include even more modern and up-to-date protocols;
- Increasing the size of the IACS CR by introducing additional virtualized components will keep the low cost of the testbed and increase complexity. Hence, allowing for a wider vulnerability surface. The possible solution is to add virtualized IACS testbed like GRFICS (Formby et al., 2018) to the author's created CR;
- Test MitM attack against SCADA and WEB-SCADA;

The author's plans for this research are to rewrite this thesis for conference publication within the year and propose introducing this CR into the university's study curriculum.

LIST OF FIGURES

LIST OF TABLES

BIBLIOGRAPHY

Adepu, S., & Mathur, A. (2016). An investigation into the response of a water treatment system to cyber attacks. *2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE)*, 141–148. https://doi.org/10.1109/HASE.2016.14

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

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

Alves, T. R., Buratto, M., de Souza, F. M., & Rodrigues, T. V. (2014). Openplc: An open source alternative to automation. *IEEE Global Humanitarian Technology Conference (GHTC 2014)*, 585–589. https://doi.org/10.1109/GHTC.2014.6970342

Alves, T., Das, R., Werth, A., & Morris, T. (2018). Virtualization of SCADA testbeds for cybersecurity research: A modular approach. *Computers & Security*, *77*, 531–546. https://doi.org/https://doi.org/10.1016/j.cose.2018.05.002

Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. I., & Timorin, A. A. (2016). Industrial control systems vulnerabilities statistics. *Kasperky Lab*.

Beresford, D. (2011). Exploiting siemens simatic s7 plcs. https://paper.bobylive.com/Meeting_Papers/BlackHat/USA-2011/BH_US11_Beresford_S7_PLCs_WP.pdf

Bergman, D. C., Jin, D., Nicol, D. M., & Yardley, T. (2009). The virtual power system testbed and inter-testbed integration. *Proceedings of the 2nd Conference on Cyber Security Experimentation and Test*, 5.

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

Blumbergs, B. Remote exploit development for cyber red team computer network operations targeting industrial control systems. In: *Proceedings of the 5th international conference on information systems security and privacy - icissp,* INSTICC. SciTePress, 2019, 88–99. ISBN: 978-989-758-359-9. https://doi.org/10.5220/0007310300880099.

Chromik, J. J., Remke, A., & Haverkort, B. R. (2018). An integrated testbed for locally monitoring SCADA systems in smart grids. *Energy Informatics*, *1*(1), 56. https://doi.org/10.1186/s42162-018-0058-7

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

Craggs, B., Rashid, A., Hankin, C., Antrobus, R., Şerban, O., & Thapen, N. (2019). A reference architecture for IIoT and industrial control systems testbeds. *Living in the Internet of Things (IoT 2019)*, 1–8. https://doi.org/10.1049/cp.2019.0169

Davis, S., Jon Magrath. (2013). A survey of cyber ranges and testbeds. *DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION EDINBURGH (AUSTRALIA) CYBER AND ELECTRONIC WARFARE DIV*, *38*.

DiTechSolutions. (2021). Learn ics/scada security fundamentals [Accessed:22.05.2021]. https://ditechsolutions.com/pages/ics-scada-cybersecurity-training

DNP. (2021). Distributed network protocol [Accessed:15.05.2021]. https://www.dnp.org/

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

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

Formby, D., Rad, M., & Beyah, R. (2018). Lowering the barriers to industrial control system security with GRFICS. *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. https://www.usenix.org/conference/ase18/presentation/formby

Fovino, I. N., Masera, M., Guidi, L., & Carpi, G. (2010). An experimental platform for assessing scada vulnerabilities and countermeasures in power plants. *3rd International Conference on Human System Interaction*, 679–686. https://doi.org/10.1109/HSI.2010.5514494

Geng, Y., Wang, Y., Liu, W., Wei, Q., Liu, K., & Wu, H. (2019). A survey of industrial control system testbeds [Publisher: IOP Publishing]. *IOP Conference Series: Materials Science and Engineering*, *569*, 042030. https://doi.org/10.1088/1757-899x/569/4/042030

Ghaeini, H. R., & Tippenhauer, N. O. (2016). Hamids: Hierarchical monitoring intrusion detection system for industrial control systems. *Proceedings of the 2nd ACM Workshop on*

Cyber-Physical Systems Security and Privacy, 103–111. https://doi.org/10.1145/2994487.2994492

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

Gold, J. (2020). The five eyes and offensive cyber capabilities: Building a 'cyber deterrence initiative'. https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf

Goncharov, E. (2021). Ics threat predictions for 2021. https://ics-cert.kaspersky.com/reports/2020/12/02/ics-threat-predictions-for-2021/

Green, B., Lee, A., Antrobus, R., Roedig, U., Hutchison, D., & Rashid, A. (2017). Pains, gains and plcs: Ten lessons from building an industrial control systems testbed for security research. *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*. https://www.usenix.org/conference/cset17/workshop-program/presentation/green

Gunathilaka, P., Mashima, D., & Chen, B. (2016). Softgrid: A software-based smart grid testbed for evaluating substation cybersecurity solutions. *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 113–124. https://doi.org/10.1145/2994487.2994494

Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S., & Higdon, M. (2010). Development of the powercyber scada security testbed. *Proceedings of the sixth annual workshop on cyber security and information intelligence research*. Association for Computing Machinery. https://doi.org/10.1145/1852666.1852690

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

Huq, N., Hilt, S., & Hellberg, N. (2018). Us cities exposed:industries and ics. https://documents.trendmicro.com/assets/wp/wp-us-cities-exposed-industries-and-ics.pdf

Kaspersky Lab. (2021a). Apt attacks on industrial companies in 2020. https://ics-cert.kaspersky.com/reports/2021/03/29/apt-attacks-on-industrial-companies-in-2020/

Kaspersky Lab. (2021b). Encyclopedia: Attack vector [Accessed:15.05.2021]. https://encyclopedia.kaspersky.com/glossary/attack-vector/

Kaspersky Lab. (2021c). Threat landscape for industrial automation systems. https://ics-cert.kaspersky.com/reports/2021/03/25/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/

Koganti, V. S., Ashrafuzzaman, M., Jillepalli, A. A., & Sheldon, F. T. (2017). A virtual testbed for security management of industrial control systems. *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*, 85–90. https://doi.org/10.1109/MALWARE.2017.8323960

Korkmaz, E., Dolgikh, A., Davis, M., & Skormin, V. (2016). Industrial control systems security testbed.

Krishnan, S., & Wei, M. (2019). SCADA testbed for vulnerability assessments, penetration testing and incident forensics. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 1–6. https://doi.org/10.1109/ISDFS.2019.8757543

Larrucea, X., & Molinuevo, A. (2020). An ICS based scenario generator for cyber ranges. In M. Yilmaz, J. Niemann, P. Clarke, & R. Messnarz (Eds.), *Systems, software and services process improvement* (pp. 543–554). Springer International Publishing.

Lei, C., Donghong, L., & Liang, M. (2017). The spear to break the security wall of s7commplus. *Blackhat USA*.

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

Ljøsne, M. J. (2019). *Network scanning industrial control systems* (Master's thesis) [URN:NBN:no-73983]. University of Oslo. https://doi.org/http://hdl.handle.net/10852/70862

Lockheed-Martin. (2018). *Gaining the advantage: Applying cyber kill chain methodology to network defense* (tech. rep.). Lockheed-Martin.

Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., & Hariri, S. (2011). A testbed for analyzing security of scada control systems (tasscs). *ISGT 2011*, 1–7. https://doi.org/10.1109/ISGT.2011.5759169

Mathur, A. P., & Tippenhauer, N. O. (2016). Swat: A water treatment testbed for research and training on ics security. *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, 31–36. https://doi.org/10.1109/CySWater.2016.7469060

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

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

MITRE. (2020). 2020 cwe top 25 most dangerous software weaknesses [Accesed: 09.05.2020]. https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

MITRE. (2021). Apt groups [Accessed: 13/03/2021].

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

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

Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., & Reddi, R. (2011). A control system testbed to validate critical infrastructure protection concepts. *International Journal of Critical Infrastructure Protection*, *4*(2), 88–103. https://doi.org/https://doi.org/10.1016/j.ijcip.2011.06.005

Muller, L. P. (2019). Military offensive cyber-capabilities:small-state perspectives. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2583385/NUPI_Policy_Brief_1_2019_Muller.pdf?sequence=1&isAllowed=y

Müller, T., Walz, A., Kiefer, M., Dermot, D. H., & Sikora, A. (2018). Challenges and prospects of communication security in real-time ethernet automation systems. *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, 1–9. https://doi.org/10.1109/WFCS.2018.8402338

NIST. (2021). Nist computer security resource cente glosaryr [Accessed: 06.05.2021]. https://csrc.nist.gov/glossary

Noorizadeh, M., Shakerpour, M., Meskin, N., Unal, D., & Khorasani, K. (2021). A cyber-security methodology for a cyber-physical industrial control system testbed. *IEEE Access*, *9*, 16239–16253. https://doi.org/10.1109/ACCESS.2021.3053135

NSTB. (2008). Common cyber securityvulnerabilities observed incontrol system assessments bythe inl nstb program. https://energy.gov/oe/downloads/common-cyber-security-vulnerabilities-observed-control-system-assessments-inl-nstb

Ottis, R. (2009). Theoretical model for creating a nation-state level offensive cyber capability. https://www.ccdcoe.org/uploads/2018/10/Ottis2009_TheoreticalModelForCreatingANation-StateLevelOffensiveCyberCapability.pdf

PCMag. (2021). Encyclopedia: Attack vector [Accessed:15.05.2021]. https://www.pcmag.com/encyclopedia/term/attack-vector

Perez-Palma, A., & McDaniel, D. (2020). Siemens logo! web server code execution vulnerability [Accessed: 18.04.2021; CVE-2020-7593].

Pfrang, S., Kippe, J., Meier, D., & Haas, C. (2017). Design and architecture of an industrial IT security lab. In S. Guo, G. Wei, Y. Xiang, X. Lin, & P. Lorenz (Eds.), *Testbeds and research infrastructures for the development of networks and communities* (pp. 114–123). Springer International Publishing.

Polge, J., Robert, J., & Traon, Y. L. (2019). Assessing the impact of attacks on opc-ua applications in the industry 4.0 era. *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 1–6. https://doi.org/10.1109/CCNC.2019.8651671

Profinet and Profibus. (2014). *Profinet system description technology and application*.

Radoglou-Grammatikis, P., Sarigiannidis, P., Giannoulakis, I., Kafetzakis, E., & Panaousis, E. (2019). Attacking iec-60870-5-104 scada systems. *2019 IEEE World Congress on Services (SERVICES)*, *2642-939X*, 41–46. https://doi.org/10.1109/SERVICES.2019.00022

RealPars. (2020). What are the major plc manufacturers? [Accesed: 18.03.21]. https://realpars.com/plc-manufacturers/

RealPars. (2021). What are the most popular plc programming languages? [Accessed: 06.05.2021]. https://realpars.com/plc-programming-languages/

Reaves, B., & Morris, T. (2012). An open virtual testbed for industrial control system security research. *International Journal of Information Security*, *11*. https://doi.org/10.1007/s10207-012-0164-7

Rosa, L., Cruz, T., Simões, P., Monteiro, E., & Lev, L. (2017). Attacking SCADA systems: A practical perspective. *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 741–746. https://doi.org/10.23919/INM.2017.7987369

Rubio-Hernan, J., Rodolfo-Mejias, J., & Garcia-Alfaro, J. (2017). Security of cyber-physical systems. In N. Cuppens-Boulahia, C. Lambrinoudakis, F. Cuppens, & S. Katsikas (Eds.), *Security of industrial control systems and cyber-physical systems* (pp. 3–18). Springer International Publishing.

SANS. (2021). Ics410: Ics/scada security essentials [Accessed:22.05.2021]. https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/

Schab, J. (2021). Tackling dod cyber red team deficiencies through systems engineering.

Shacklett, M. E. (2021). What is an attack vector? [Accessed:15.05.2021]. https://searchsecurity.techtarget.com/definition/attack-vector

Sidhu, T. S., & Yin, Y. (2007). Modelling and simulation for performance evaluation of iec61850-based substation communication systems. *IEEE Transactions on Power Delivery*, *22*(3), 1482–1489. https://doi.org/10.1109/TPWRD.2006.886788

Siemens. (2007). *Step 2000 basics of plcs*. Siemens. http://diagramas.diagramasde.com/otros/Siemens%20Basics%20Of%20Plc.pdf

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

Stamp, J., Urias, V., & Richardson, B. (2011). Cyber security analysis for the power grid using the virtual control systems environment. *2011 IEEE Power and Energy Society General Meeting*, 1–4. https://doi.org/10.1109/PES.2011.6039786

Stranahan, J., Soni, T., & Heydari, V. (2019). Supervisory control and data acquisition testbed for research and education. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0085–0089. https://doi.org/10.1109/CCWC.2019.8666482

Su, W., Antoniou, A., & Eagle, C. (2017). Cyber security of industrial communication protocols. *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1–4. https://doi.org/10.1109/ETFA.2017.8247769

Tao, Y., Xu, W., Li, H., & Ji, S. (2019). Experience and lessons in building an ICS security testbed. *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, 1–6. https://doi.org/10.1109/ICIAI.2019.8850804

Tippenhauer, N. O. (2019). Design and realization of testbeds for security research in the industrial internet of things. In C. Alcaraz (Ed.), *Security and privacy trends in the industrial internet of things* (pp. 287–310). Springer International Publishing. https://doi.org/10.1007/978-3-030-12330-7_14

UK Government. (2016). National cyber security strategy 2016-2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, *20*(24). https://doi.org/10.3390/s20247148

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

Werth, A. W., & Morris, T. H. (2021). Prototyping PLCs and IoT devices in an HVAC virtual testbed to study impacts of cyberattacks. In X.-S. Yang, R. S. Sherratt, N. Dey, & A. Joshi (Eds.), *Proceedings of fifth international congress on information and communication technology* (pp. 612–623). Springer Singapore.

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

Wireshark. (2021b). S7 communication (s7comm) [Accessed:14.05.2021]. https://wiki.wireshark.org/S7comm

Xie, Y., Wang, W., Wang, F., & Chang, R. (2018). VTET: A virtual industrial control system testbed for cyber security research. *2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 1–7. https://doi.org/10.1109/SSIC.2018.8556732

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

Zhu, B., Joseph, A., & Sastry, S. (2011). A taxonomy of cyber attacks on scada systems. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 380–388. https://doi.org/10.1109/iThings/CPSCom.2011.34

APPENDIX I. LETTERS OF SUPPORT

SIEMENS

Siemens Osakeyhtio Latvijas filiāle, Zemintāna iela 78, Rīga, LV-2167, Latvija

Name Gints Skroderis
Division **Industry division**

Telephone +371 6701-5549
Fax +371 6701-5511

E-mail Gints.skroderis@siemens.com
Internet www.siemens.lv

Date April 19, 2021

Recepient

To whom it may concern

Letter of support

This letter is to confirm that the concepts and main goals of the master thesis research created by Austris Uljāns and entitled “Industrial control system cyber range laboratory for offensive capability development”, is supported by Industry division at Siemens Osakeyhtioe Latvian Branch Office.

The main goal of the master thesis research is to provide an realistic, easy reproducible, scalable, physical industrial control system (ICS) cyber range platform where the participants can practice developing offensive capabilities in the ICS field thereby improving understanding of ICS adversary capabilities. Such ICS cyber range will improve understanding of possible attack surfaces and scenarios used in attacking ICS and in future could allow building more secure ICS infrastructure.

Our company is interested in the master thesis research study.

Kind regards,

Industry division at Siemens Osakeyhtioe Latvian Branch
Division manager

_____
Gints Skroderis

VIDZEME UNIVERSITY
OF APPLIED SCIENCES

Cēsu iela 4,
Valmiera, LV-4200
T.: +371 64207230,
F: +371 64207229
info@va.lv, www.va.lv

LV90001342592
Valsts Kase
LV38TREL9150130000000
TRELLV22

Valmiera

_____ No._____

To whom it may concern

Letter of support

This is to confirm that the concepts and main goals of the master thesis research created by Austris Uljāns and entitled “Industrial control system cyber range laboratory for offensive capability development”, is supported by Vidzeme University of Applied Sciences.

The main goal of the master thesis research is to provide a realistic, easy reproducible, scalable, physical industrial control system (ICS) cyber range platform where the participants can practice developing offensive capabilities in the ICS field thereby improving understanding of ICS adversary capabilities. Such ICS cyber range will improve understanding of possible attack surfaces and scenarios used in attacking ICS and in future could allow building more secure ICS infrastructure.

Kind regards,

Dr.sc. ing. Alvis Sokolovs

Dean of the Faculty of Engineering
Acting Head of Information Technologies studies

Rīgas Tehniskā universitāte
MODELĒŠANAS UN IMITĀCIJAS KATEDRA
Kaļķu iela 1
LV-1658 Rīga
Tālr. 67089514
Fakss 67089513
E-pasts: andrejs.romanovs@rtu.lv

Riga Technical University
DEPARTMENT OF MODELLING AND SIMULATION
1, Kalku Street
LV-1658 Riga, Latvia
Phone +371-67089514
Fax +371-67089513
E-mail: andrejs.romanovs@rtu.lv

TO WHOM IT MAY CONCERN

LETTER OF SUPPORT

This letter is to confirm that the concepts and main goals of the Master Thesis research created by Austris Uljāns and entitled "Industrial control system cyber range laboratory for offensive capability development", is supported by the Department of Modelling and Simulation of Riga Technical University.
The main objective of the Master Thesis research is to provide the realistic, easy reproducible, scalable, physical industrial control system (ICS) cyber range platform where the participants can practice developing offensive capabilities in the ICS field thereby improving understanding of ICS adversary capabilities. Such ICS cyber range will improve understanding of possible attack surfaces and scenarios used in attacking ICS and in future could allow building more secure ICS infrastructure.
Our department is interested in the Master Thesis research study.

2021, April 19th

Sincerely,
Associate Professor, Dr.sc.ing. Andrejs Romanovs
Head of the RTU Department of Modelling and Simulation
Director of the RTU Master Study Program "Cybersecurity Engineering"
Riga Technical University, Riga, Latvia
Mobile Phone: +371-29637251, E-mail: Andrejs.Romanovs@rtu.lv

"Latvijas Mobilais Telefons" SIA
Reģistrācijas Nr. 50003050931

Ropažu iela 6, Rīga, LV - 1039, Latvija
Tālrunis: +371 29340000, e-pasts: info@lmt.lv, www.lmt.lv

Vidzemes Augstskola

Cēsu iela 4, Valmiera

LV – 4200

21st April 2021,

Nr. 576/DI

Letter of support

To whom it may concern

This letter is to confirm that the concepts and main goal of the master thesis research "Industrial control system cyber range laboratory for offensive capability development" written by Austris Uljāns, is supported by SIA "Latvijas Mobilais Telefons".

The main objective of the master thesis research is to provide a realistic, easy reproducible, scalable, physical industrial control system (ICS) cyber range platform where the participants can practice developing offensive capabilities in the ICS field thereby improving understanding of ICS adversary capabilities. Such ICS cyber range will improve understanding of possible attack surfaces and scenarios used in attacking ICS and in future could allow building more secure ICS infrastructure.

Our company is interested in this master thesis research study.

Sincerely,

Head of Cybersecurity Division

Mārtiņš Kaļķis

SIA "Latvijas Mobilais Telefons"

CERT.LV
Information Technologies
Security Incident
Response Institution

To whom it may concern

Letter of support

This letter is to acknowledge that the concepts and main goals of the master thesis by Vidzemes Augstskola student Austris Uljāns entitled “Industrial automation and control system cyber range laboratory for offensive capability development”, is being recognized by CERT.LV as an important research topic.

The main objective of the master thesis research is to provide a realistic, easy to reproduce, scalable, and physical industrial automation and control system (IACS) cyber range platform. In this environment, participants may practice developing offensive capabilities in the IACS field, thereby improving their understanding of IACS adversary capabilities. Such IACS cyber range will develop the concepts of possible attack surfaces and scenarios used in attacking IACS and could allow building a more secure infrastructure.

Our institution is interested in the results of the master thesis research study.

Kind regards,

General Manager

Baiba Kaškina

CERT.LV

Nacionālie bruņotie spēki

LATVIJAS REPUBLIKAS ZEMESSARDZES KIBERAIZSARDZĪBAS VIENĪBA

Maiznīcas iela 5, Rīga, LV-1001, tālr. 67335970, 67335971,fakss 67371150, e-pasts: kibersargs@mil.lv

Rīgā

2021.gada 25.maijā Nr. 2/3.23/18

Vidzeme Univeraity of Applied Sciences

Letter of support

This letter is to confirm that the concepts and main goals of the master thesis research created by Austris Uljāns and entitled "Industrial control system cyber range laboratory for offensive capability development", is supported by Latvian National Guard Cyber Defence Unit.

The main goal of the master thesis research is to provide a realistic, easy reproducible, scalable, physical industrial control system (ICS) cyber range platform where the participants can practice developing offensive capabilities in the ICS field thereby improving understanding of ICS adversary capabilities. Such ICS cyber range will improve understanding of possible attack surfaces and scenarios used in attacking ICS and in future could allow building more secure ICS infrastructure.

Our organization is interested in the master thesis research study.

Kind regards,

NG CDU commander

Major Ronalds Mandelis

Akciju sabiedrība „Latvenergo”
Vien. reģ. Nr. 40003032949
Pulkveža Brieža iela 12, Rīga, LV-1230, Latvija
Tālr. (+371) 67728222,
www.latvenergo.lv, info@latvenergo.lv

Rīgā
#REG-DATE# Nr. #REG-NUMBER#

Vidzemes Augstskola
Cēsu iela 4, Valmiera,
LV-4201

Letter of support

This letter is to confirm that the concepts and main goals of the master thesis research “Industrial control system cyber range laboratory for offensive capability development” written by Austris Uljāns, is supported by AS "Latvenergo".

The main objective of the master thesis research is to provide a realistic, easy reproducible, scalable, physical industrial control system (ICS) cyber range platform where the participants can practice developing offensive capabilities in the ICS field thereby improving understanding of ICS adversary capabilities. Such ICS cyber range will improve understanding of possible attack surfaces and scenarios used in attacking ICS and in future could allow building more secure ICS infrastructure.

Our company is interested in the master thesis research study.

Šis dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu.

Chief Technology and Support Officer — Kaspars Cikmačs

Raitis Palms 67728658

Gmail **Austris Uljāns <austris.u@gmail.com>**

Par maģistra darbu

1 message

Juris Gailis <Juris.Gailis@gaso.lv> 11 May 2021 at 13:18
To: Austris Uljāns <austris.u@gmail.com>

Labdien

Viena no GASO prioritātēm ir drošas un pieejamas sadales sistēmas infrastruktūras nodrošināšana.

Vidēja un ilga termiņa perspektīvā, lai nodrošinātu turpmāku esošās dabasgāzes infrastruktūras izmantošanu un ES enerģētikas dekarbonizāciju, būs jāievieš viedie risinājumi un vienlaicīga AG un dabasgāzes izmantošana, pakāpeniski samazinot pēdējās procentuālo īpatsvaru. Savukārt, ņemot vērā to, ka sistēmas viedizācija būs aktuāla ne tikai dabasgāzes transportēšanai un uzglabāšanai, bet arī sadalei, dabasgāzes sadales jomu tuvākajās desmitgadēs sagaida nopietni tehnoloģiski un organizatoriski pārkārtojumi. Tas nozīmē, ka viedā dabasgāzes sadales ieviešanai būs nepieciešama visaptveroša plānošana, ietverot gan gāzesvadu drošības, optimālas risku un aktīvu pārvaldības, gan arī efektīvas klientu komunikācijas un datu apmaiņas faktorus. ES energoresursu uzskaites sistēmas un enerģijas lietotāju datu aizsardzības stratēģija ir balstīta uz pieņēmumu, ka SSO izmantotajam sakaru tīklam jābūt autonomam, lai nodrošinātu maksimālu sistēmas un enerģijas lietotāju datu drošību. ES 2016 gada regulā 2016/679 un Fizisko personu datu apstrādes likumā paredzēts, ka sadales sistēmas operatoram (SSO) kā datu pārzinim vai apstrādātājam ir jāgarantē viedās energoresursu uzskaites sistēmas un enerģijas lietotāju datu drošība.

Attīstoties Latvijas ekonomikai, arvien vairāk izjūtams dažādu jomu, sevišķi IKT, speciālistu trūkums, kas gan nav tikai Latvijas fenomens, bet izteikta situācija arī citviet pasaulē. Ņemot vērā situāciju, būtiska loma ir izglītībai un datorikas mācīšanai Latvijas skolās, kā arī IKT speciālistu sagatavošanai profesionālajās vidējās izglītības un augstākās izglītības iestādēs. Vienlaikus centieniem paaugstināt sabiedrības vispārējās zināšanas ir jāveicina jauno IT speciālistu izglītošana un izaugsme, kur būtiska nozīme ir iespējām piedalīties interešu izglītības pasākumos un sacensībās kiberdrošības jomā. Kā 23.03.21. biznesa tehnoloģiju platformas BiSMART rīkotajā tiešsaistes konferencē atzina IT atlases aģentūra LikeIT vadītāja Irina Točko – darba devējiem nozīmīga ir: 1) IT drošības vadītāju (u.c. IT drošības speciālistu) sertifikācija 2) praktiskā tehniskā pieredze.

Tamdēļ Vidzemes augstskolas students Austris Uljāns maģistra darba tēmu “Industriālās un automātikas kontroles sistēmas kiberdrošības testēšanas laboratorija uzbrukuma spēju attīstīšanai” izvēlējies atbilstoši mūsdienu kiberdrošības mērķim - spēt uzlabot industriālo kiberdrošības speciālistu tehnisko un praktisko pieredzi.

Juris Gailis

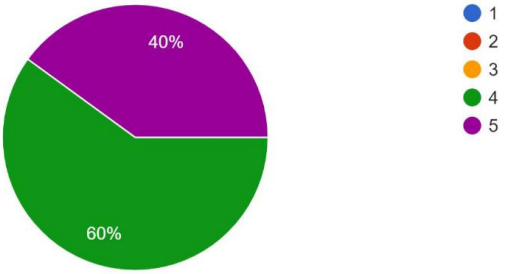
AS "Gaso"

IT departamenta IT uzturēšanas un drošības daļas IS drošības pārvaldnieks
Tālr. (+371) 67369187
e-pasts: juris.gailis@gaso.lv

APPENDIX II. FEEDBACK FORM SUMMARY

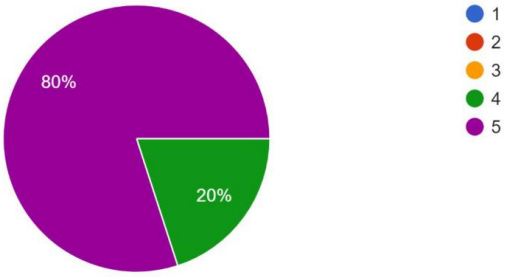
Vai uzdevumi un sasniedzamie rezultāti bija izprotami?

5 responses



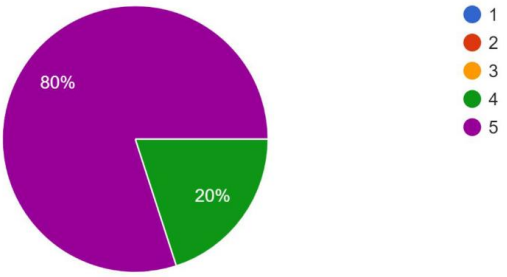
Vai šīs apmācības palīdz labāk izprast industriālās kontroles sistēmas?

5 responses



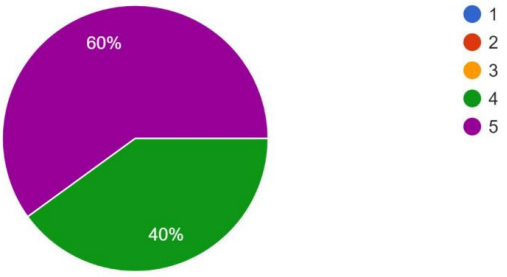
Vai šis mācību poligons veicināja izpratni par kiberdrošības riskiem ICS sistēmās?

5 responses



Vai sniegtās zināšanas ir noderīgas?

5 responses



APPENDIX III. DECLARATION OF TRANSFER OF AUTHOR'S PROPERTY RIGHTS

APLIECINĀJUMS

par autora mantisko tiesību nodošanu

Maģistra Darbs (turpmāk - Darbs)

„ Industriālās un automātikas kontroles sistēmas kiberdrošības testēšanas laboratorija uzbrukuma spēju attīstīšanai”

Pamatojoties uz Autortiesību likuma 15.pantā noteiktajām mantiskajām tiesībām, kuras darba autors var nodot trešajām personām, **piekrītu**, ka mans Darbs tiek padarīts sabiedrībai pieejams bez maksas pilnā apjomā:

Darba autors: Austris Uljāns *Dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu*

vārds un uzvārds *paraksts, datums*

APPENDIX IV. DECLARATION OF COMPLIANCE

APLIECINĀJUMS

par darba atbilstību

Maģistra darbs

„ Industriālās un automātikas kontroles sistēmas kiberdrošības testēšanas laboratorija uzbrukuma spēju attīstīšanai”

izstrādāts Vidzemes Augstskolas Inženierzinātņu fakultātē.

Ar savu parakstu apliecinu, ka darbs izstrādāts patstāvīgi un tajā ir atsauces uz visām izmantotajām citu autoru atziņām un datiem. Darbs izstrādāts saskaņā ar ViA ētikas pamatprincipiem, Studējošo akadēmiskās ētikas nolikumam un fakultātes metodiskajiem norādījumiem. Apzinos, ka plaģiāta konstatēšanas gadījumā darbs tiks noraidīts.

Iesniedzot darbu, uzņemos atbildību par jebkuras konfidenciālas informācijas, kas iegūta darba izstrādes gaitā, neizplatīšanu.

Darba autors: Austris Uljāns / *Dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu*

autora vārds un uzvārds *paraksts un datums*

Darbs iesniegts fakultātē: _____ / _____ / _____

fakultātes vecākā speciālista vārds un uzvārds *paraksts* *datums*

Rekomendēju darbu aizstāvēšanai:
Dr.comp.sc. Bernhards Blumbergs / *Dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu*

darba vadītāja zinātniskais grāds, vārds un uzvārds *paraksts un datums*

Darbs aizstāvēts 2021.gada_____. ____ar vērtējumu _____ _____(_____)

vērtējums vārdiem *vērtējums cipariem*

Valsts pārbaudījumu komisijas priekšsēdētājs *(bakalaura un maģistra darbam)*_____ / _____ / _____

vai studiju programmas direktors *(gada projektam)* *valsts pārbaudījumu komisijas priekšsēdētāja vai studiju programmas direktora vārds, uzvārds* *paraksts* *datums*