Cybersecurity in Industrial Automation Lab Design for EE 435

Presented By
Jules Hajjar
Emily Zhou

Project Advisor
Dr. Jason Poon

Senior Project
Electrical Engineering Department
California Polytechnic State University San Luis Obispo

June 2023

Table of Contents

List of Figures

List of Tables

Abstract

This project involves the creation of an instructional laboratory aimed at teaching cybersecurity for industrial automation applications. Specifically tailored for Electrical Engineering students at Cal Poly, the experiment focuses on configuring the Modicon M580, a PLC from Schneider Electric, and serves to introduce students to relevant cybersecurity protocols and techniques. This project will be implemented into the EE435 (Industrial Power Control and Automation) course curriculum upon Cal Poly's transition to the semester system.

Acknowledgements

We are grateful towards Darrick Baker, Professor Taufik, and Professor Poon for allowing this senior project to happen. This project wouldn’t have succeeded without their generous help and donations. We would also like to thank our friends and family for the support they provided throughout this project.

Chapter 1. Introduction

Since 2015, the Electrical Engineering Department at Cal Poly devised plans for increasing the number of courses related to power and control. Following the acquisition of six Modicon PACs from Schneider Electric in 2018, the department began developing a new, one unit laboratory known as EE435 (Industrial Power and Automation). This course features weekly PLC projects, with one week designated towards cybersecurity in industrial automation. Throughout the course of this experiment, students gain an understanding of security configurations in the Modicon PAC by modifying the architecture of its networks.

Cybersecurity is a field of technology that has experienced exponential growth since the rise of the internet. With an ever-increasing amount of automated systems responsible for numerous aspects of our lives, these systems are vulnerable to the actions of malicious attackers and can yield catastrophic results if left unchecked. Most notably, the industrial automation sector is increasingly at risk of cyberattacks. Given the deadly consequences of hacking into facilities such as power plants, dams, oil refineries, or similarly weaponizable sites, there exists a pressing need to raise cyber awareness within future engineers. Our senior project seeks to address this issue through a laboratory centered on cybersecurity.

This laboratory involves the usage of lab room 150 in Building 20 of Cal Poly. The room contains clusters of M580 modules, in which each cluster is connected to computers running the programming software required for the experiments. A multitude of sensors can be connected or simulated depending on the experiment run. This project aims for a three-hour long lab activity that explores cybersecurity through use of PLC, ethernet cables, and other devices supplied in the room.

Chapter 2. Background

Unlike instruction through online videos and manuals, the primary goal is to engage prospective engineers with hands-on work. The practical experience acquired through working with PAC devices offers engineers greater confidence in their ability to operate in industrial settings. By designing an experiment around cybersecurity, students can expand their comprehension on the necessary protocols. As noted by Fortune.com, the cybersecurity industry is a rapidly growing market, estimated to surpass a net value of 400 billion dollars by 2027. This reality highlights the importance of expertise in this field, with an increase in demand for knowledgeable individuals within the hiring process. Currently, there are over 300,000 cybersecurity positions available in the United States, a 75% increase compared to the past five years [1].

Despite this project's introductory nature, it is important to familiarize students with cybersecurity protocols given the increase in cyberattacks resulting from the growth in accessible internet and technology. According to the ICS Cyber Emergency Response Team, instances of cyber incidents increased by 112% between 2012 and 2013 [2]. In conjunction with this spike, studies show that a cyber attack occurs every 39 seconds on average. Despite this surge, only 38% of global organizations are prepared to face a major cybersecurity incident [1]. Furthermore, a 2018 survey conducted by Cisco of 320 companies revealed that only 23% met the minimum industry requirements and regulations concerning cyber protection. Follow-up research after the COVID-19 pandemic suggested that 14% of these 320 companies modified their security protocols as a result of the increase in remote work [3].

Implementing cybersecurity protocols within industrial control systems prevent economic and environmental disasters. In 2000, the Shire of Maroochy in Australia experienced issues with faulty pumps and radio communications with wastewater stations [4]. Over the span of three months, over one million gallons of untreated sewage water flowed through rivers and into parks. Upon examination, engineers discovered an unauthorized individual who had infiltrated the plant and interfered with the wastewater system, resulting in major environmental destruction to surrounding habitats. In April 2001, police arrested 49 year-old Vitek Boden and seized his laptop and SCADA (Supervisory Control and Data Acquisition) equipment from his vehicle. These devices were later identified to control the sewage system infrastructure. Unlike most cyber incidents, the Maroochy Water Incident was one of the rare moments an attacker was apprehended. This occurrence emphasized the vulnerability of SCADA systems to cyber attacks. As a result, a civil engineer from the Maroochy Water Services necessitated the implementation of protective measures within control systems, including logging user access and commands executed in SCADA systems [4].

Following the Maroochy Water Incident, a virus known nowadays as Stuxnet infected Iranian power stations in 2010 [5]. Believed to be orchestrated by nations targeting Iran's nuclear facilities, the virus contaminated over 12,000 staff computers and 30,000 IP addresses, inflicting multiple setbacks to essential processes. The worm's objective was to limit the plant's ability to enrich radioactive material by spoofing the machine statuses. Bypassing the Windows security mechanisms, Stuxnet reprogrammed PLC software and altered variables controlling the uranium centrifuge's frequencies. While Stuxnet gradually destroyed the equipment, the process was running as expected on the outside. Researchers soon discovered traces of Stuxnet within the computers and monitored its spread to prevent further catastrophes in other industrial processes, thereby successfully containing the virus. Though Electrical Engineering students may not be directly involved in cybersecurity measures in the field, Stuxnet and the Maroochy Water Incident serve as examples about the importance of learning preventative measures.

This project impacts the Electrical Engineering department, its students, and the course instructors. The broader academic community may moreover adopt the lab procedures, further extending the impact of the project. Given that this project aims to develop meaningful experiments, it is responsible for teaching students sufficient knowledge about cybersecurity. The benefits of this instruction extend beyond the classroom and into industry work, furthermore spreading the impact of this work to the cybersecurity sector. Hackers and other bad actors may also be considered stakeholders that benefit negatively due to the familiarization of security features and procedures within future cybersecurity employees.

The present options available to learn about cybersecurity for Electrical Engineering students are limited. The table below reveals Honeywell [6] and Schneider Electric [7] as major companies that provide training and equipment at expensive rates, with prior employment or training as requirements for the course. Most Cal Poly courses centered on cybersecurity are largely tailored towards Computer Engineering students, furthermore limiting opportunities for Electrical Engineering students due to their lack of prerequisites and software experience. In order to enhance knowledge in this field, it is essential to dedicate one week of the EE435 course curriculum for a basic understanding of cybersecurity.

TABLE I
BENCHMARKING WITH COMPETITORS

Parameter	Honeywell	Schneider Electric	CPE422, 464, 465	Our Target
Cost of equipment	Estimated > $200,000	$150,000	Low	Low to None
Accessibility	Open for Employees	Expensive	Affordable and available for CPE students	Affordable and available for EE students
Effectiveness	Caters to already trained individuals	Caters to already trained individuals	Caters to students learning about network security	Caters to students at an introductory level
Duration	3+ Months (per project)	3+ Months (per project)	1 Quarter	1 Week

Chapter 3. Design Requirements

In the development of a cybersecurity experiment for Electrical Engineering students, it is important to consider a variety of factors. A successful experiment must be short, relevant, inexpensive, and cover an adequate amount of topics within a three-hour time frame. If more time than expected is dedicated to the assignment, students may be unable to work on it outside of class hours, as the classroom contains the only supply of Modicon PAC Controllers. In addition to a three-hour course limit, the laboratory experiment must cover parts of the ISA99 cybersecurity standards. ISA99 [8] and IEC62443 [9] standards reflect the latest required cybersecurity measures, allowing students to translate their lab skills into an industrial setting. Moreover, the cost of equipment outside of the lab benches and M580s should be close to or equal to zero. Since this project entails software configurations over hardware specifications, there is little need for more electronic equipment. Lastly, an effective curriculum is one where most students achieve a grade of at least 70%, as a lower grade may indicate lack of clarity in the instruction of cybersecurity issues and protocols.

Since this project aims to cover the fundamentals of cybersecurity, it requires approval from Professor Taufik, Professor Poon, and the Electrical Engineering department. Despite its need for approval, the resulting project carries low risks. As it focuses more on software configuration than hardware manipulation, the risks of electrocution and other hazards are low.

Customer Requirements

TABLE II
CUSTOMER REQUIREMENTS

Customer Requirement	Justification
a) Short	The lab needs to fit in the time frame of a class session.
b) Relevant	The lab should be up to date with the latest cybersecurity standards.
c) Inexpensive	Aside from the provided equipment, the lab should not require extra external materials.
d) Effective	Students take away knowledge about present issues in the industry.

Engineering Specifications

TABLE III
ENGINEERING SPECIFICATIONS

Customer Requirement	Engineering Specification	Justification
a)	Lab must be completed in three hours.	Cal Poly labs are all three hours long and the material should fit this model [10].
b)	Lab must cover ISA99 cybersecurity standards.	ISA99 & IEC62443 reflect the latest required cybersecurity measures [8,9].
c)	The cost of equipment outside of benches and M580s is close to or equal to 0.	The budget of this project is limited to what the school has already provided. [11]
d)	The student shall receive a passing grade above 70% to be considered knowledgeable about the subject.	Getting a grade lower than 70% shows that the lab experiment was not effective at explaining cybersecurity issues. [12]

Analysis of Requirements

TABLE IV
DEVELOPING CUSTOMER REQUIREMENTS

Parameter	Target	Tolerance (Min/Max)	Risk (H, M, L)	Compliance (A, T, S, I)	Test Equipment Needed
Duration	3 hours	Max	M	T,S	Building 20, Room 150
Complexity Prior knowledge needed	3rd year EE student with prerequisites	Min	M	I,S	N/A
Outcomes	Grade C-	Min	L	I,A	N/A
Price	$50	Max	H	T,S,A	N/A

Chapter 4. Design

This laboratory experiment requires the use of on-campus computers supplied with Control Expert software and PLC equipment. Therefore, there remains an inability to modify settings within Windows itself without administrative privileges, rendering many cybersecurity features listed within the Schneider Electric Cybersecurity manual unusable. Furthermore, the three-hour long lab duration imposes limitations on the amount of information the project can contain. In order to establish a comprehensive lab experiment, the final design emphasizes three fundamental aspects of cybersecurity: event logging, PLC communication, and memory protection. These features are separated into three distinct tasks that students procedurally work through according to the lab report.

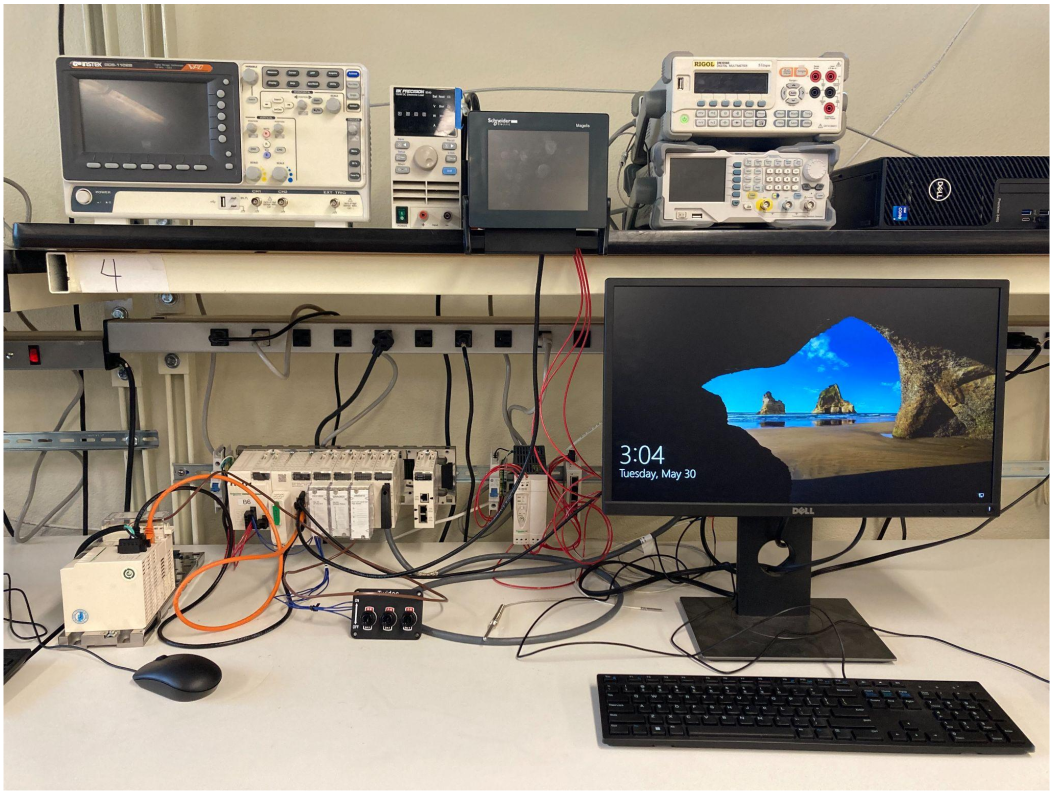


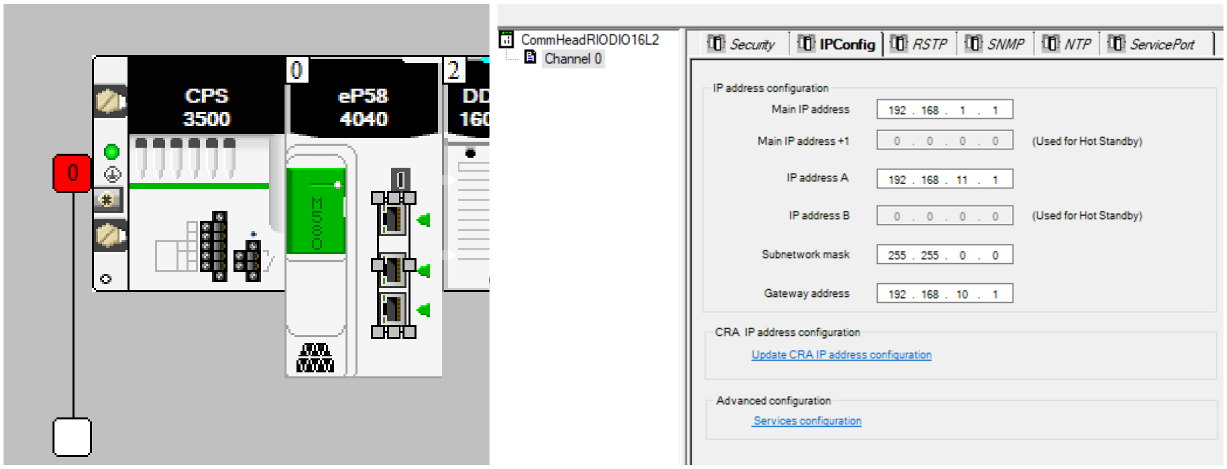
Figure 3-1: One of the eight workbenches equipped with a PLC in Room 150

Event Logging

Event logging is done through Syslog, a protocol programmed through an external device. After some research, we decided to implement a section covering Syslog, as it seems to be an incredibly valuable tool when it comes to logging events. The system is able to log both physical and software events and thus provides the engineers with valuable data in the case of a breach.

To implement this section of the lab, benches are connected to a Linux mini PC running an instance of a simple Syslog server with a web UI. Once the communication is set up, students are able to access the list of messages sent from their bench. The full list of messages that can be triggered are described in Appendix D.

To configure IP addresses, students access the ethernet port settings within the PLC bus' CPU module. Within the "IPConfig" section, the Main IP address and IP address A are changed according to the lab bench number. Going by standard IP address procedures, the Main IP address is called 192.168.1.# and the IP address A is named 192.168.#1.1, in which the "#" sign is replaced with the lab bench number.



IP address configuration

Main IP address 192 . 168 . 1 . 1

Main IP address +1 0 . 0 . 0 . 0 (Used for Hot Standby)

IP address A 192 . 168 . 11 . 1

IP address B 0 . 0 . 0 . 0 (Used for Hot Standby)

Subnetwork mask 255 . 255 . 0 . 0

Gateway address 192 . 168 . 10 . 1

Figure 3-2: Example of the ethernet port settings inside of Control Expert

With six benches in total, there will be six unique IP addresses reporting to the logging server, networked as described below.

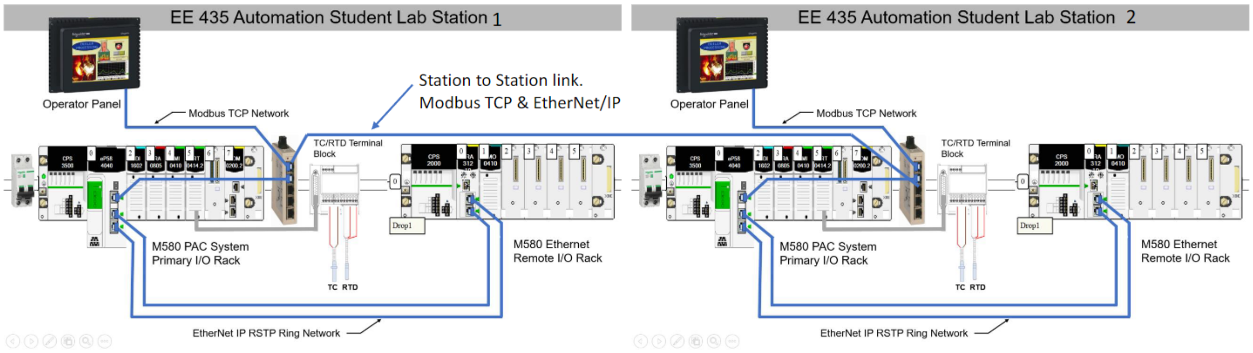
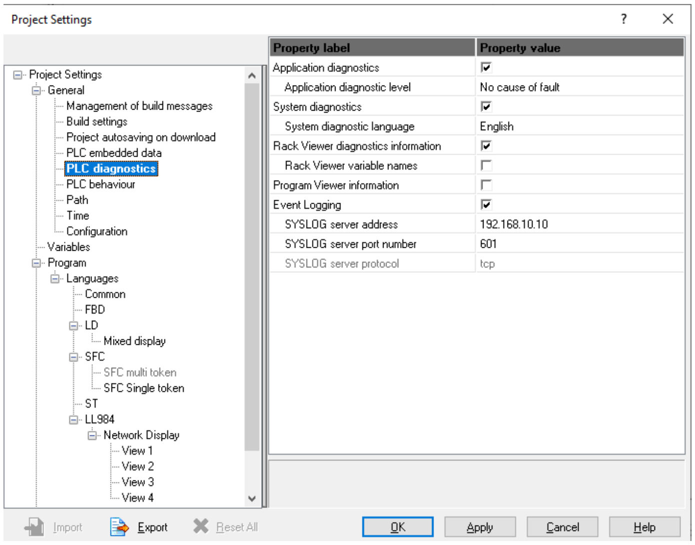

EE 435 Automation Student Lab Station 1
EE 435 Automation Student Lab Station 2
Operator Panel
Modbus TCP Network
Station to Station link.
Modbus TCP & EtherNet/IP
TC/RTD Terminal Block
Drop1
M580 PAC System Primary I/O Rack
M580 Ethernet Remote I/O Rack
TC RTD
EtherNet IP RSTP Ring Network
Operator Panel
Modbus TCP Network
TC/RTD Terminal Block
Drop1
M580 PAC System Primary I/O Rack
M580 Ethernet Remote I/O Rack
TC RTD
EtherNet IP RSTP Ring Network

Figure 3-3: Wiring schematic of the network for both Syslog and EthernetIP communications.

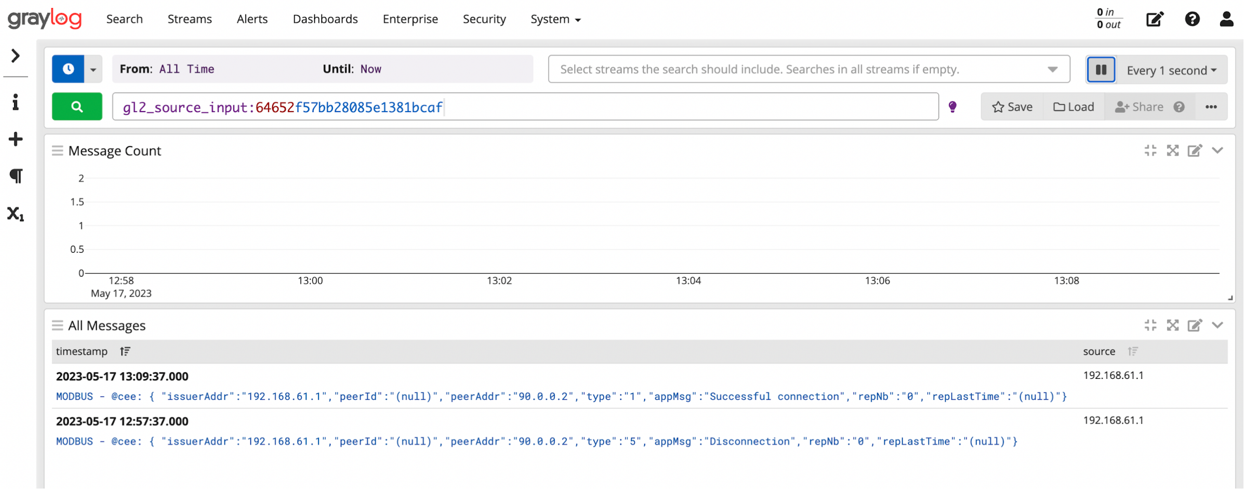
Logging also needs to be enabled in the Project Settings configuration, and the address of the server needs to be filled in.



Property label	Property value
Application diagnostics	☑
Application diagnostic level	No cause of fault
System diagnostics	☑
System diagnostic language	English
Rack Viewer diagnostics information	☑
Rack Viewer variable names	□
Program Viewer information	□
Event Logging	☑
SYSLOG server address	192.168.10.10
SYSLOG server port number	601
SYSLOG server protocol	tcp

Figure 3-4: Example of the Syslog configuration inside of Control Expert

Instructions for installing the Syslog server on a Linux machine will be included as part of the instructor manual in case the configuration has to be modified. The system uses the official Graylog Docker deployment system [13]. The machine used for this project is a low power mini PC running Ubuntu. To allow the students to connect to the interface, a WRT54GL Wi-Fi router was used. This allows for a simple procedure and saves both cabling and setup time overall. This network is air gapped from the school's network as well as the internet to prevent intrusion.



From: All Time Until: Now

```
gl2_source_input:64652f57bb28085e1381bcaf
```

```
timestamp                                                                                                        source
2023-05-17 13:09:37.000                                                                                          192.168.61.1
MODBUS - @cee: { "issuerAddr":"192.168.61.1","peerId":"(null)","peerAddr":"90.0.0.2","type":"1","appMsg":"Successful connection","repNb":"0","repLastTime":"(null)"}
2023-05-17 12:57:37.000                                                                                          192.168.61.1
MODBUS - @cee: { "issuerAddr":"192.168.61.1","peerId":"(null)","peerAddr":"90.0.0.2","type":"5","appMsg":"Disconnection","repNb":"0","repLastTime":"(null)"}
```

Figure 3-5: Sample output of the web UI of the Syslog server

PLC Communication

PLC communication is an essential process among industrial control systems. In order for one PLC to properly extract information and perform necessary computations, it must interact with other PLCs using read/write procedures. This segment demonstrates one method of implementing PLC communication using Modbus, IP addressing, and ethernet wiring. The procedures are heavily inspired by Darrick Baker’s week 4 lab experiment [14].

In order to establish proper communication from one PLC to another, ethernet cables are used to connect a local module to a remote module as detailed in Figure 3-3. This connection allows the PLC to read or send information from their system to a remote PLC with the correct IP address.

Each computer contains a Control Expert .stu file with the appropriate settings configured for communications. Students are responsible for designing a new function block diagram within the program’s logic section. In this file, students utilize three function blocks, ADDM, READ_VAR, and WRITE_VAR to interact with another PLC. The primary objective in this task is to operate three relays on the remote PLC using the local PLC’s breaker switches.

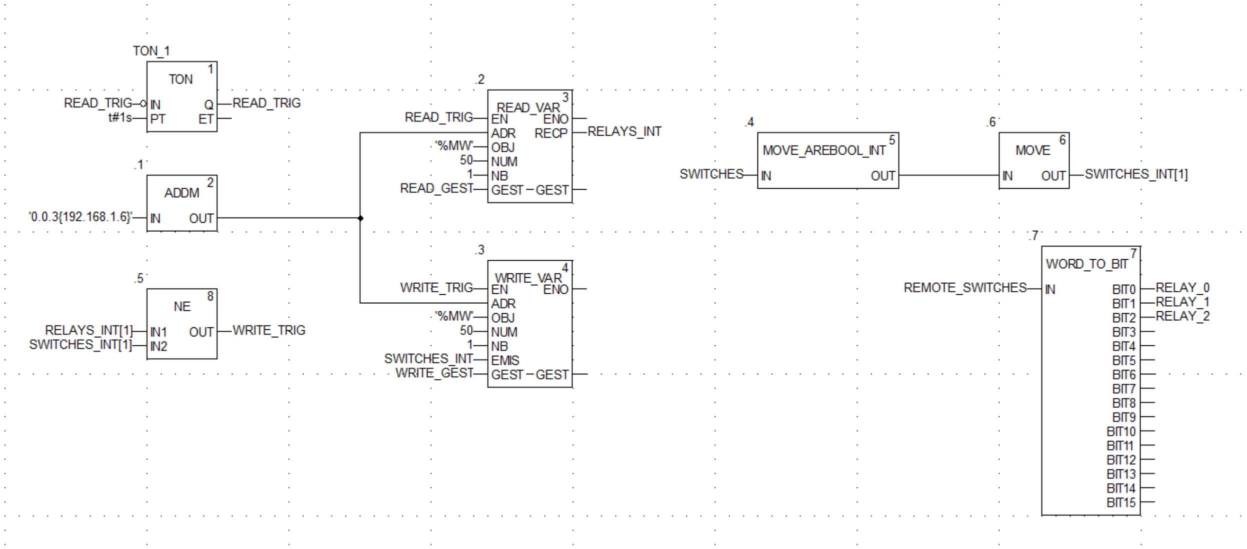


Figure 3-6: Logic section for Read/Write Operations

Figure 3-6 illustrates the blocks and variables required for communication. This file is also available under Appendix D for instructional use and debugging.

The ADDM module allows students to call the remote PLC's IP address. Both READ_VAR and WRITE_VAR blocks utilize the ADDM output for their ADR inputs. With the correct IP address called, READ_VAR operations begin with identifying the remote PLC's variables. In particular, information from the variable with Modbus address '%MW50' is stored in RELAYS_INT. This variable processes the remote relays that are currently on in the system. The NE (Not Equal) block compares this variable to another that processes the status of the local switches. If true, this condition triggers WRITE_VAR operations. WRITE_VAR converts the switch status to the same remote variable with '%MW50,' ensuring the NE block remains false. When successful, students are able to enable the remote PLC's relay lights with their three switches. Note that the WORD_TO_BIT block is optional and only serves as a monitoring tool to verify that the switches are being detected.

Memory Protection

The designed system reveals vulnerabilities to unwanted read/write commands, allowing attackers to surreptitiously connect to the device and modify variables. Once students establish PLC communication between both PLCs, the final task involves administering memory protection protocols. This section discusses upper-level CPU modifications to prevent reading or writing to Modbus addresses.

Within the CPU, students enter a range of Modbus addresses to protect from read/write operations. In particular, students firstly input the number 50 into the Modbus address range. This prevents the remote PLC from reading and writing to Modbus addresses assigned to 50 and above. Rerunning through the PLC communication logic, students should discover that the remote relays fail to update in accordance with the switches. Once students input a value in a register over address 50, however, the PLC operates as intended. By listing a range of Modbus addresses to block from remote communications, students learn to assign Modbus addresses according to the information they want protected, and information they want communicated.

Chapter 5. Test and Results

The primary concerns for this project include the experiment duration and overall complexity. As this lab experiment occurs further into the course, students are expected to have a basic understanding of Control Expert, including creating new logic sections, declaring variables, and adding function blocks. If students are able to work through this experiment in two or three hours, this verifies that students understand the relevant function blocks required for operation.

The test involved timing ourselves while following the lab procedures, with the goal of emulating a student's performance. The estimated time of completion should fall anywhere between 2:15 and 2:45 hours. Additionally, we performed individual tests on each bench setup to ensure proper functionality of every necessary equipment.

TABLE V
REQUIREMENTS ANALYSIS

Requirement	Met?	Notes
Procedure takes under 3 hours to complete	Yes	After test driving the procedure, we completed all the tasks in 2 hours and 10 minutes.
Coverage of industry standard safety measures	Yes	The procedure goes over three of the main precautions that can be taken.
Cost is under $50	Yes	The only purchase that was necessary was the Wi-Fi router and a low power computer.

We also tested the equipment numerous times, such as the PLC systems, software, and cables to make sure nothing was misconfigured or creating errors in the process. In case a problem were to arise in the future, we have posted the necessary resources under Appendix D. The resources include the necessary Control Expert project files, the installation procedure and files for the Syslog server, as well as an annotated lab manual for the instructor.

Chapter 6. Conclusion

The aftermath of the Maroochy Water Incident and Stuxnet present deep concerns over the safety of future industrial automation systems. With an increasing number of industries utilizing control systems as primary methods of system management and manufacturing production, PLC systems can be heavily compromised from the actions of one sole hacker, costing companies and other related sectors millions in reparations. This cybersecurity lab experiment aims to familiarize Electrical Engineering students with protective PLC measures, including requirements in duration, complexity, and effectiveness in mind. Covering major topics such as event logging, PLC communication, and memory protection offer a comprehensive overview on cybersecurity that, hopefully, students can apply in their future careers.

Project Results Summary

The three sections included in this lab design are an essential basis when it comes to cybersecurity. By going over these concepts, this lab activity effectively demonstrates three key aspects of cybersecurity to students. Early detection of issues and communication security are the most important processes when it comes to preventing intrusion and cyber attacks. While three hours is a very restrictive timeframe, this project will without a doubt give students a comprehensive overview of what the industry standards are, and how they function. The hands-on nature of the project pushes the participants to experiment, and try novel ideas if time permits.

Cost Breakdown

We were thankful to have almost all the equipment donated to the school. The total cost of designing and building the project thus only accounts for the purchase of a $21.50 router and $21.89 mini PC. The true cost of the project is detailed under Appendix A below.

Project Challenges

Throughout the course of this project, we were faced with many obstacles. In particular, the familiarization of PLC software and implementation of Syslog servers were especially challenging.

The majority of the project's first quarter involved learning about the Control Expert software in general. Although Darrick Baker was beyond helpful, many of the other lessons and activities were self-guided. The PLC environment required time to understand, as the Electrical Engineering degree curriculum did not contain courses specifically on PLCs and their related software. This meant that research on cybersecurity procedures were stalled until we understood the basic mechanisms. In addition to the late start, the location of the PLCs also brought challenges. Control Expert software was only available on room 150 computers, therefore barring opportunities for remote work or research. Additionally, since help guides were centralized within the software, there was a lack of online libraries to help resolve errors or answer questions regarding function blocks. Help from Darrick Baker progressed this project immensely, as his workshops, meetings, and lab experiments finalized decisions about the lab procedures.

Furthermore, implementing a working Syslog server using open source or free software took time, as the PLC only allowed for TCP messages. Most logging systems only allow for UDP messages to be received. With some modifications of existing configuration information, we were able to get the server to receive such messages. Another hurdle was the IP addressing of the system. The PLC CPUs are not compatible with DHCP, and that feature thus had to be disabled both on the router and on the machine running the server. After trying different configurations we settled on a working system where students could still benefit from DHCP, and thus save time on the procedure, while the rest of the network still functions with fixed IP addresses. This was done by connecting the whole system on the WAN port of the router, disabling the firewall, and enabling DHCP for Wi-Fi clients.

Recommendations for Future Work

Upon designing this laboratory activity, some difficulties were encountered throughout the process. Recommendations can be made if a similar project were to be started in the future. For example, we would suggest that the researchers make full use of the available documentation inside of Control Expert to learn more about different ways of implementing a given process. This can be done by accessing the help menu, which contains numerous sections about every functional block and software settings.

The use of software like Wireshark or other packet sniffers is also something that could be done for future projects. We decided to not go that route for this laboratory design as it would have taken too much setup time on the student's end. Being able to look at ethernet traffic was however helpful for the initial research phase as well as troubleshooting issues that arose throughout the research.

References

[1] UNG, “Cybersecurity: A global priority and career opportunity,” University of North Georgia, 2019. [Online]. Available: https://ung.edu/continuing-education/news-and-media /cybersecurity.php. [Accessed: 18-Oct-2022].

[2] P. Combs, “How Test Labs Reduce Cyber Security Threats to Industrial Control Systems,” Schneider Electric, 5-May-2014. [Online]. Available: https://www.se.com/ww/en/download/document/998-2095-05-05-14AR0_EN/ [Accessed: 18-Oct-2022].

[3] Matteo Iaiani, Alessandro Tugnoli, Sarah Bonvincini, and Valerio Cozzani, “Analysis of cybersecurity-related incidents in the process industry,” Reliability Engineering & System Safety, 19-Jan-2021. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S095183202100051X. [Accessed: 02-Dec-2022].

[4] K. E. Hemsley and D. R. E. Fisher, “History of industrial control system cyber incidents,” History of Industrial Control System Cyber Incidents (Technical Report) | OSTI.GOV, 31-Dec-2018. [Online]. Available: https://www.osti.gov/biblio/1505628. [Accessed: 02-Dec-2022].

[5] J. Fildes, “Stuxnet virus targets and spread revealed,” BBC News, 15-Feb-2011. [Online]. Available: https://www.bbc.com/news/technology-12465688. [Accessed: 02-Dec-2022].

[6] H. Processing, “Honeywell opens US Cyber Security Research Lab,” Hydrocarbon Processing - Refining, Petrochemical, Gas Processing and LNG Magazine, Data and Information, 31-Mar-2015. [Online]. Available: https://www.hydrocarbonprocessing.com/ news/2015/03/honeywell-opens-us-cyber-security-research-lab. [Accessed: 18-Oct-2022].

[7] D. Greenfield, “Industrial Cybersecurity Research Lab Opens,” Automation World, 05-May-2022. [Online]. Available: https://www.automationworld.com/home/blog/13313416/ industrial-cybersecurity-research-lab-opens. [Accessed: 18-Oct-2022].

[8] ISA, “ISA99, Industrial Automation & Control SYS security- ISA,” isa.org, Jan-2007. [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/ isa-standards-committees/isa99. [Accessed: 18-Oct-2022].

[9] ISA, “New standard specifies capability for control systems - ISA,” isa.org, 2018. [Online]. Available: https://www.isa.org/intech-home/2018/september-october/departments/ new-standard-specifies-security-capabilities-for-c. [Accessed: 18-Oct-2022].

[10] Cal Poly, “About the catalog,” *About the Catalog < California Polytechnic State University*. [Online]. Available: https://catalog.calpoly.edu/aboutthecatalog/. [Accessed: 19-Oct-2022].

[11] V. Prodanov, “EE460 - Introduction,” in *Project, Systems, EE460/1/2 Constraints*. [Accessed: 19-Oct-2022].

[12] Cal Poly, “Grading,” *Grading < California Polytechnic State University*. [Online]. Available: https://catalog.calpoly.edu/academicstandardsandpolicies/grading/. [Accessed: 19-Oct-2022].

[13] Graylog, “Docker”, graylog.org, 2023. [Online]. Available: https://go2docs.graylog.org/5-0/downloading_and_installing_graylog/docker_installation.htm [Accessed: 23-May-2023]

[14]D. Baker, “Ethernet Remote I/O & Peer to Peer Communications Lab,” in Cal Poly EE435 Automation Lab Week 4 Ethernet Peer to Peer Communications SP2023. [Accessed: 27-Apr-2023].

Appendices

Appendix A. Cost Estimate

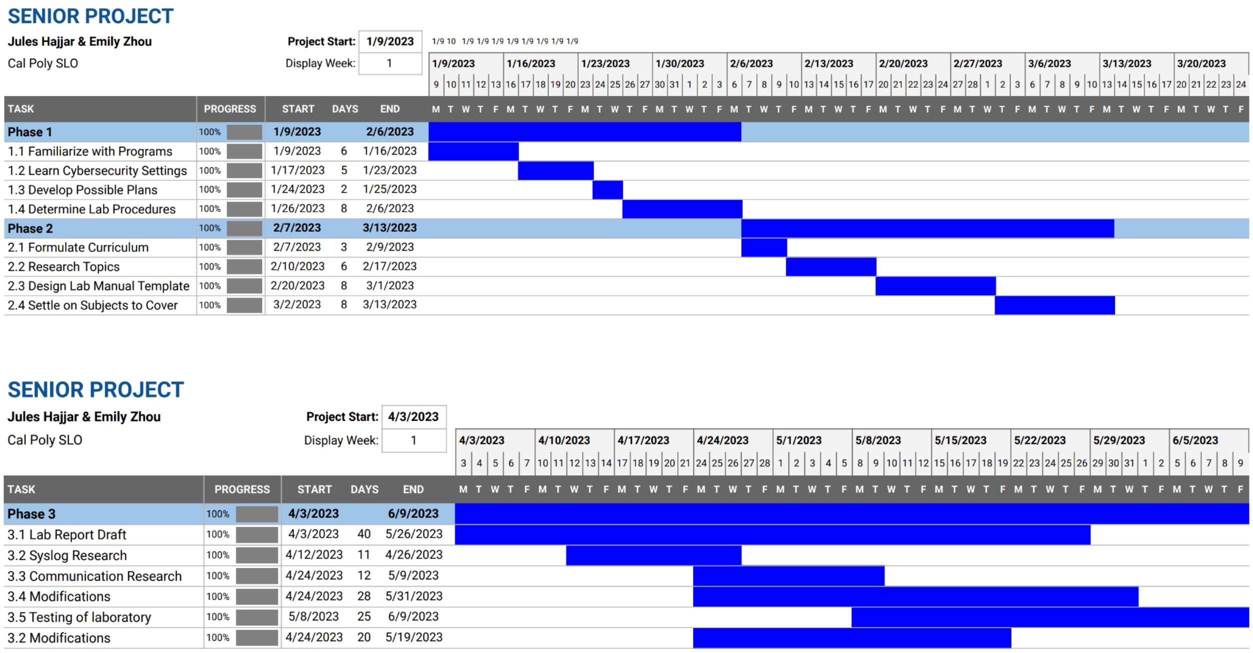
TABLE VI
COST ESTIMATE OF PROJECT DEVELOPMENT

Task/Item	Time Estimate (Hours)	Time Actual (Hours)	Cost Estimate	Cost Actual (To Date)
Project Plan				
Abstract	1	3	$30	$90
Requirements and Specifications	3	2	$90	$60
Literature Research	5	4	$150	$120
Gantt Charts	2	3	$60	$90
Cost Estimates	1	2	$30	$60
ABET Analysis	8	8	$240	$240
Report V1	12	8	$360	$240
Development	18	N/A	$540	N/A
Reading Documentation & Training	7	N/A	$210	N/A
Design of Experiment	54	N/A	$1,620	N/A
Formal Procedure Drafting	10	N/A	$300	N/A
Test and Modifications	48	N/A	$1,440	N/A
Finalized Report	24	N/A	$720	N/A
Parts Acquisition	2	N/A	$60	N/A
Totals	195	30	$5,850	$900

TABLE VII
COST ESTIMATE OF PARTS

Parts	Cost Estimate	Cost Actual
BMEP581020 (M580 Controller)	$5,828.00	$0.00
BMENOC0301 (M580 Communication Module)	$2,419.00	$0.00
EcoStruxure License	$2,279.00	$0.00
Desktop Computer	$800.00	$0.00
Ethernet Cables	$50.00	$0.00
Syslog Server	$100.00	$0.00
Wi-Fi Router	$21.50	$21.50
Mini PC	$21.89	$21.89
	$11,519.39.50	$43.39

Appendix B. Gantt Charts



SENIOR PROJECT
Jules Hajjar & Emily Zhou
Cal Poly SLO

Project Start: 1/9/2023
Display Week: 1

TASK	PROGRESS	START	DAYS	END
Phase 1	100%	**1/9/2023**		**2/6/2023**
1.1 Familiarize with Programs	100%	1/9/2023	6	1/16/2023
1.2 Learn Cybersecurity Settings	100%	1/17/2023	5	1/23/2023
1.3 Develop Possible Plans	100%	1/24/2023	2	1/25/2023
1.4 Determine Lab Procedures	100%	1/26/2023	8	2/6/2023
Phase 2	100%	**2/7/2023**		**3/13/2023**
2.1 Formulate Curriculum	100%	2/7/2023	3	2/9/2023
2.2 Research Topics	100%	2/10/2023	6	2/17/2023
2.3 Design Lab Manual Template	100%	2/20/2023	8	3/1/2023
2.4 Settle on Subjects to Cover	100%	3/2/2023	8	3/13/2023

SENIOR PROJECT
Jules Hajjar & Emily Zhou
Cal Poly SLO

Project Start: 4/3/2023
Display Week: 1

TASK	PROGRESS	START	DAYS	END
Phase 3	100%	**4/3/2023**		**6/9/2023**
3.1 Lab Report Draft	100%	4/3/2023	40	5/26/2023
3.2 Syslog Research	100%	4/12/2023	11	4/26/2023
3.3 Communication Research	100%	4/24/2023	12	5/9/2023
3.4 Modifications	100%	4/24/2023	28	5/31/2023
3.5 Testing of laboratory	100%	5/8/2023	25	6/9/2023
3.2 Modifications	100%	4/24/2023	20	5/19/2023

Figure 7-1: Gantt Charts for Winter and Spring Quarter

Appendix C. Analysis of Senior Project Design

1. **Summary of Functional Requirements**

   The laboratory about cybersecurity in industrial automation is part of the upcoming Spring 2023 EE435 class. This project aims to teach new students about the latest cybersecurity measures that need to be taken in the field to protect vital infrastructure and large scale automated processes. The end goal of the project is to be teaching new concepts effectively to a group of individuals with little to no experience in the field, and prepare them for future projects that could require these newly acquired skills. Moreover, even though the laboratory will be conducted using PAC controllers donated by Schneider Electric, most of the concepts will be applicable to other brands of PLCs since cybersecurity principles can be applied to other systems that rely on similar architectures.

2. **Primary Constraints**

   This laboratory complements the EE435 class and thus must develop within the scope of the class. Depending on which week the experiment will be conducted dictates the familiarity the students will have with the software and hardware required. Besides the teaching constraints, the project also faces temporal constraints. The laboratory activity needing to be achievable in the time of a lab session dictates how in-depth the concepts discussed can go. The other temporal constraint is the time allotted to complete the design phase. Since this laboratory will take place during Spring 2023, we will only have one quarter to plan and design the procedure. However revisions and modifications could be implemented before June 2023.

3. **Economics**

   The Cybersecurity in Industrial automation laboratory requires an estimated 195 hours of labor to produce. Most of the time is spent designing the experiment and writing a formal lab procedure. The project also requires a significant financial capital to acquire the devices needed. However, the equipment and software has already been donated by Schneider Electric, and the classroom is fully equipped with computers, driving the cost down significantly. Including the donations, the total cost of the project can still be estimated at 11,500$ per bench for an overall cost of 69,000$ for the whole classroom.

The costs of this laboratory are front loaded, since the equipment is required to start planning and designing the project. Occasionally, a modification may need to be implemented as students begin to experiment and failure points become prominent. However such measures should not drive the costs upwards.

The main stakeholders for this project are Cal Poly, the students enrolled in the class, and future employers that value knowledge in this specific field. Future engineers benefit from the project by developing professional skills needed in modern industrial automation positions, the EE department at Cal Poly benefits from an increase of classes in its catalog as well as an increase in reputation in the industry.

4. If Manufactured on a Commercial Basis

The training of electrical engineering students in industrial automation is the main purpose for this project. As the project is educational, no effort is put into the commercialization of the experiment.

If we intended for the project to be commercialized, the customer demographic would solely consist of other universities offering electrical or industrial engineering degrees interested in adding a new class about cybersecurity or industrial automation to their catalog. It would thus be possible to license the experiment.

5. Environmental

The project has an innately minimal detrimental impact on the environment. Since it does not contain any manufacturing. However, conducting the experiment does require hardware and software which require energy to run, estimated to be around 1kWh/bench/lab session. Using recycled PLCs could be a viable option to increase the sustainability of the overall project. The PLCs currently in our possession are brand new but could be replaced with used units that do not pass the requirements of Schneider Electric’s clients. Doing so would allow for a longer lifespan of the devices and thus a better use of their embodied energy. Besides implementing recycling, using a zero-emission electricity source to run the equipment would be the next step to improve the sustainability of the project.

While direct impacts on the environment are minimal, indirect impacts exist. This is because the project can have an impact on the future of the industry and can allow future professionals of the field to put their newly acquired skills to good use. Preventing cybersecurity attacks can greatly affect the environment by reducing downtime of vital infrastructure.

6. Manufacturability

Since the project does not entail any physical manufacturing, this outcome does not apply to the project. However if we were to implement the laboratory activity for another brand of PLCs, part of the procedure would have to be modified to fit the software associated with it. Thus the manufacturability would only entail a rewrite of the procedure for other systems, and no physical devices would have to be manufactured on our end.

7. Sustainability

As stated in section 5, the project does not generate any byproducts and thus has no direct impact on the environment besides energy consumption. If the electricity used is free of emissions, then the project can be considered environmentally sustainable.

When it comes to economic sustainability, the setup cost of the project consists of a one time purchase of the required equipment (computer and PLC system). No running costs are present and the project can be modified to discuss new cybersecurity standards. Thus, the project can be considered economically sustainable because the cost is fixed.

In terms of social sustainability, this lab aims to educate college students and thus cannot provide equal access for all individuals to advance in society. Not all members of society have access to a college education. To remediate this ethical shortcoming, it could be preferable to publish the lab procedure online to allow for more individuals to be educated about the subject.

8. Ethical

This project and cybersecurity generally present important problematics regarding ethics. With an ever increasing danger as more devices get connected to the internet, a growing need for cybersecurity arises in all fields. More specifically in our case, cybersecurity in the industrial automation space is a crucial point of upcoming infrastructure.

While our project itself is part of a “sandboxed” environment, the skills that students will take away can play an important role ethically speaking when it comes to preventing future cyberattacks. This laboratory strives to educate on the dangers of unsecured industrial automation systems and thus has an indirect ethical role in the greater scope of cybersecurity.

9. Health and Safety

This project has a minimal immediate safety risk, as the direct experience with the PLC system in the classroom takes place through a computer and low voltage interfaces. The risks involved are thus the same as using a computer, ethernet cables, and USB cables. The lab classroom policy of closed toed shoes and no drinking or eating should still be enforced to prevent risks in the eventuality of an equipment failure.

Another safety aspect of the project could entail its misuse. In the unlikely event that bad actors got access to the laboratory procedure, they could try to attack existing infrastructures and possibly break into PLC networks by testing for vulnerabilities discussed in our project.

10. Social and Political

As described in the ethical drawbacks, this project could be put to nefarious usage. However this edge case is easily outweighed by the benefits of teaching a larger group of individuals on how to deal with cybersecurity in industrial automation. If implemented correctly, this project could help save companies from cyber attacks and reduce the likelihood of employees being laid off as a result of diminished profits. While doing so seems to only benefit a few individuals working in the field, the future consequences apply to society as a whole by reducing the risk of service and supply chain disruptions on a large scale.

On the political side, this project has no adverse effect since it aims to improve the awareness of future professionals regarding cybersecurity matters. Doing so would allow for less political tensions because less attacks would take place.

11. Development

The development of this project requires us to learn how to use ecoStruxure, the software used to change the settings of the PLC and its network interfaces. We also need to learn more about network security measures and how to apply them to a networked PLC. Most of the guidelines we will follow are contained in the supervisory control and data acquisition (SCADA) standards for safety. To design the laboratory procedure, we will also need to review what has been done in the past regarding similar subjects and decide what structure we want the experiment to follow.

Appendix D. Syslog Messages List, Project Files, and Configuration Instructions

The resources are hosted at this address :
https://drive.google.com/drive/folders/11KV-F_bE5fW5xKDUyEji57xvNcGxR64c?usp=share_link

Appendix E. Laboratory Report

The report is appended on the following pages.

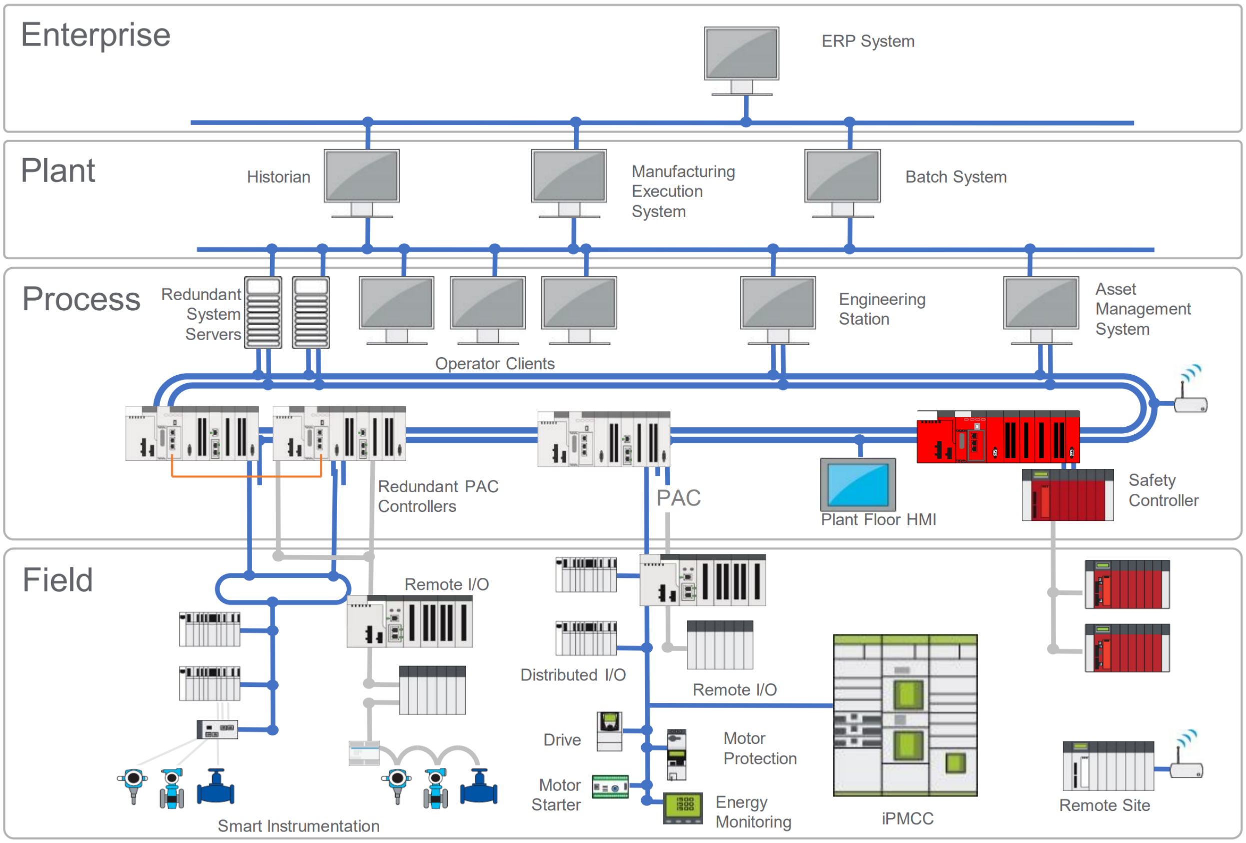
OBJECTIVES

This experiment introduces cybersecurity protocols for the PLC. These measures include event logging using Syslog, communication between neighboring PLCs, and memory protection to prevent unwanted data changes anywhere in the 0-8000 address range.

BACKGROUND

The cybersecurity field has experienced exponential growth since the advent of technology. With an ever-increasing amount of automated systems responsible for numerous aspects of our lives, these systems grow increasingly vulnerable to the actions of malicious hackers and can yield catastrophic results if left unchecked. Most notably, the industrial automation sector has encountered major cyberattacks, some in the form of near-nuclear shutdowns and massive sewage spills. Given the deadly consequences of hacking into facilities such as power plants, dams, oil refineries, and other weaponizable sites, this experiment seeks to give an overview of the possible cybersecurity procedures that can be taken preemptively.

To remediate cybersecurity issues, rules can be put in place on PLCs as well as on the network they are connected to. During this activity, we will explore some of (but not all) the steps that can be taken when setting up a PLC network.

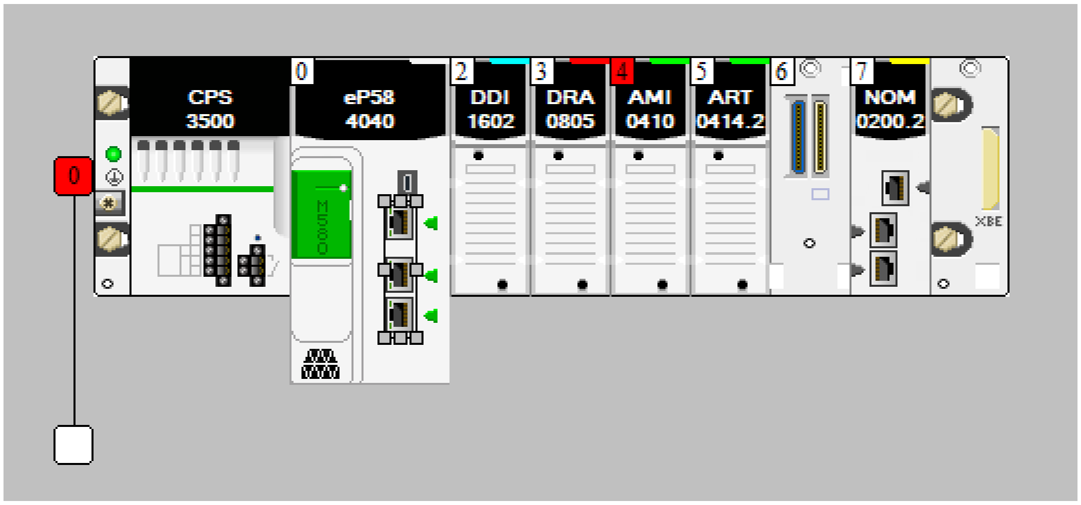


PROCEDURE

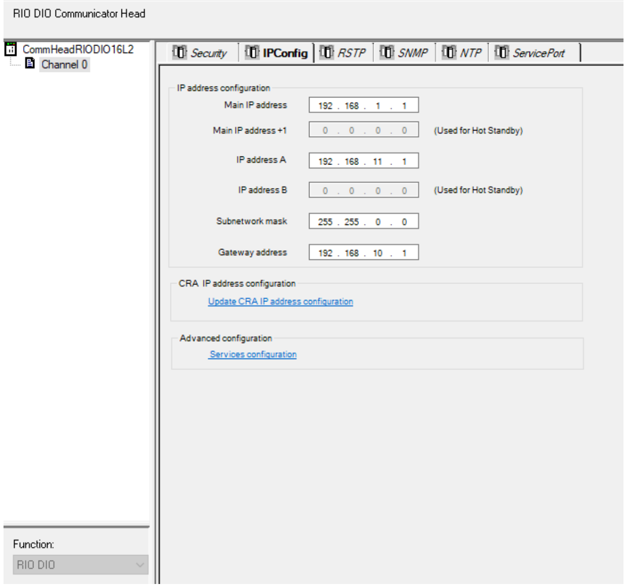
Task 0: PLC IP Setup

1. Open the file `cybersecurity.stu` from Canvas in Control Expert.

2. In the PLC Bus, double click the eP584040 CPU ethernet ports.



3. In the IPConfig tab, set the Main IP address as "192.168.1.#" and IP address A as "192.168.#.1," where "#" denotes your lab bench number.



RIO DIO Communicator Head

CommHeadRIODIO16L2
Channel 0

IP address configuration

Main IP address 192 . 168 . 1 . 1

Main IP address +1 0 . 0 . 0 . 0 (Used for Hot Standby)

IP address A 192 . 168 . 11 . 1

IP address B 0 . 0 . 0 . 0 (Used for Hot Standby)

Subnetwork mask 255 . 255 . 0 . 0

Gateway address 192 . 168 . 10 . 1

CRA IP address configuration

Update CRA IP address configuration

Advanced configuration

Services configuration

Function: RIO DIO

4. Apply settings by switching to another tab (Security for example).

5. Rebuild all project, connect PLC and upload program.

Task 1: Syslog Event Logging

Hardware Setup:

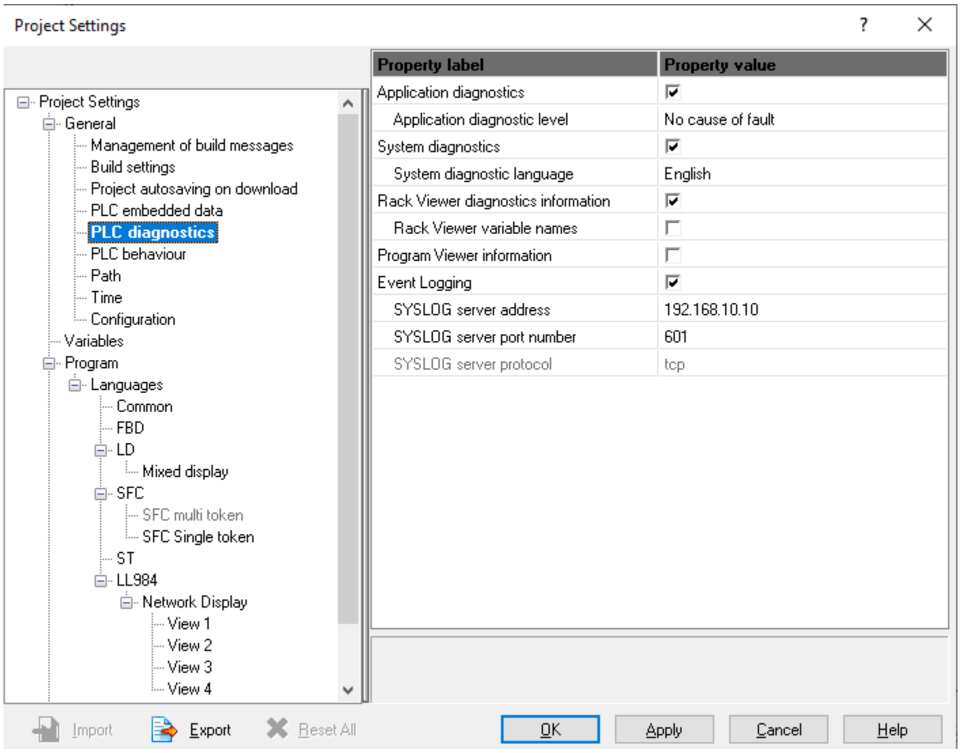
1. Connect one short ethernet cable from the PLC Service Port located on the eP584040 Module to your 1x5 Ethernet switch.

2. Connect one long ethernet cable from your 1x5 Ethernet switch to the neighboring bench's 1x5 Ethernet switch.

Activating Syslog:

3. Disconnect Control Expert from the PLC, then go under Tools > Project Settings > PLC Diagnostics.

4. Enable event logging and enter 192.168.10.10 in the SYSLOG Server address field.



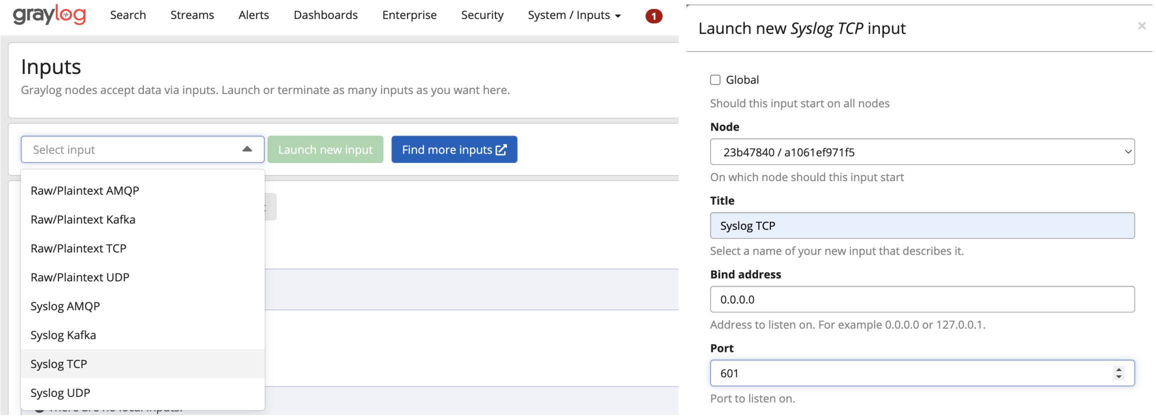
Property label	Property value
Application diagnostics	☑
Application diagnostic level	No cause of fault
System diagnostics	☑
System diagnostic language	English
Rack Viewer diagnostics information	☑
Rack Viewer variable names	☐
Program Viewer information	☐
Event Logging	☑
SYSLOG server address	192.168.10.10
SYSLOG server port number	601
SYSLOG server protocol	tcp

5. Using your laptop or other device, connect to the PLC_LAB wifi network.
Note: Due to security reasons, this network cannot access the internet.

6. Once connected, navigate to 192.168.10.10 and log in with the following credentials:
Username: `admin` Password: `admin`

7. In the top navigation menu, go to System > Inputs.

8. Select "View messages" under the Syslog TCP Input.
    a. If the Input is not present, create it as follows (Only ONE group should do this for everyone):
        i. Browse for Syslog TCP.
        ii. Launch new input.
        iii. Give it a name and specify port 601.
        iv. Scroll down and save.



Launch new *Syslog TCP* input

☐ Global
Should this input start on all nodes

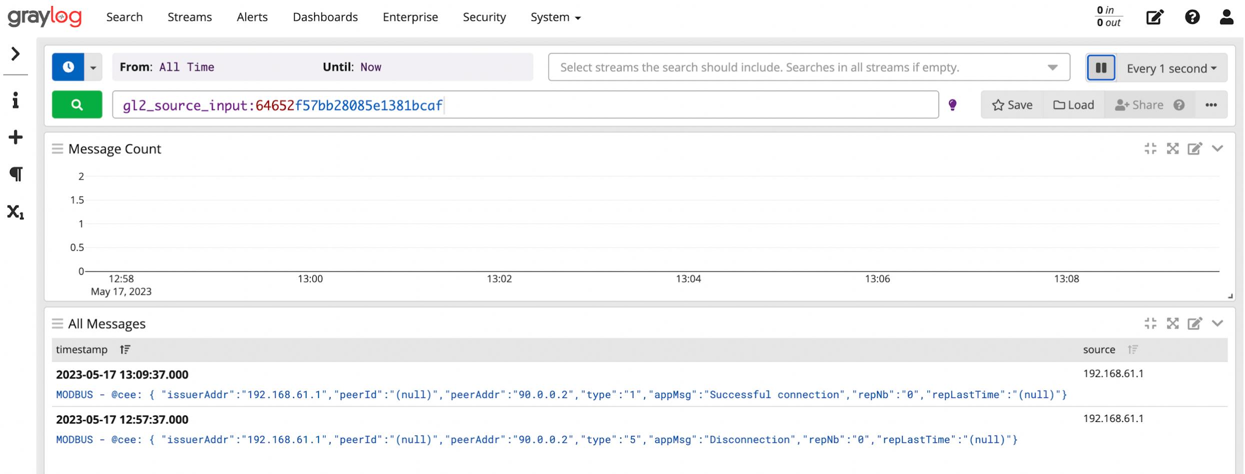
Node
23b47840 / a1061ef971f5
On which node should this input start

Title
Syslog TCP
Select a name of your new input that describes it.

Bind address
0.0.0.0
Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port
601
Port to listen on.

9. In Control Expert, connect to PLC and transfer the project to PLC.
    a. After doing so, you should start seeing Syslog messages from other benches as well as from your own PLC. Feel free to run, stop, or try other actions on Control Expert to see their effect on the Syslog output.
    Note: Pay attention to the IP address of your bench. Try generating messages by interacting with the PLC. Possible messages are listed in one of the PDF files on Canvas.



From: All Time Until: Now

```
gl2_source_input:64652f57bb28085e1381bcaf
```

timestamp	source
2023-05-17 13:09:37.000 MODBUS - @cee: { "issuerAddr":"192.168.61.1","peerId":"(null)","peerAddr":"90.0.0.2","type":"1","appMsg":"Successful connection","repNb":"0","repLastTime":"(null)"}	192.168.61.1
2023-05-17 12:57:37.000 MODBUS - @cee: { "issuerAddr":"192.168.61.1","peerId":"(null)","peerAddr":"90.0.0.2","type":"5","appMsg":"Disconnection","repNb":"0","repLastTime":"(null)"}	192.168.61.1

Throughout the remainder of the lab, feel free to log back in the Syslog server and witness the logging of new events.

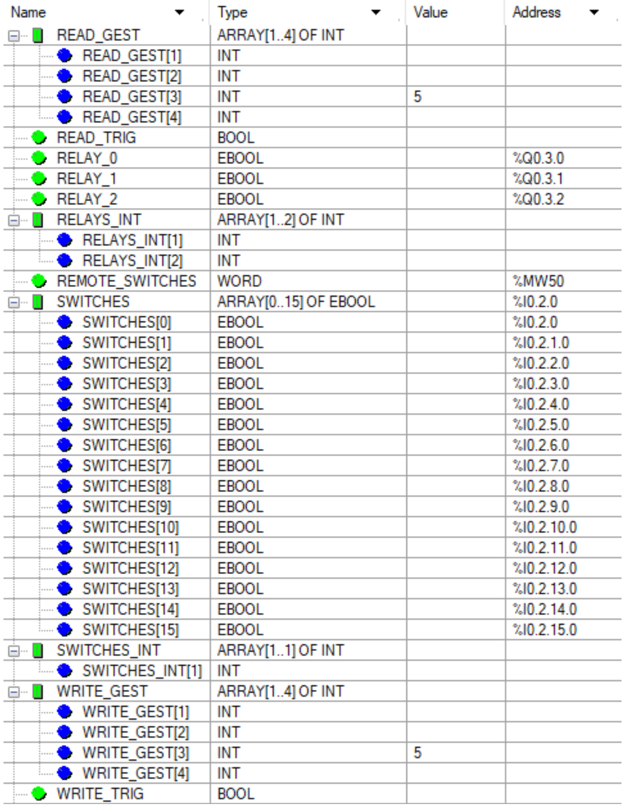
Task 2: PLC Communication

Neighborhood Communication:

1. Add a new FBD in the logic section and give it a name.

2. Add the function blocks TON, ADDM, NE, READ_VAR, WRITE_VAR, MOVE_AREBOOL_INT, MOVE, and WORD_TO_BIT into the FBD.

3. In the data editor, implement the following data variables.

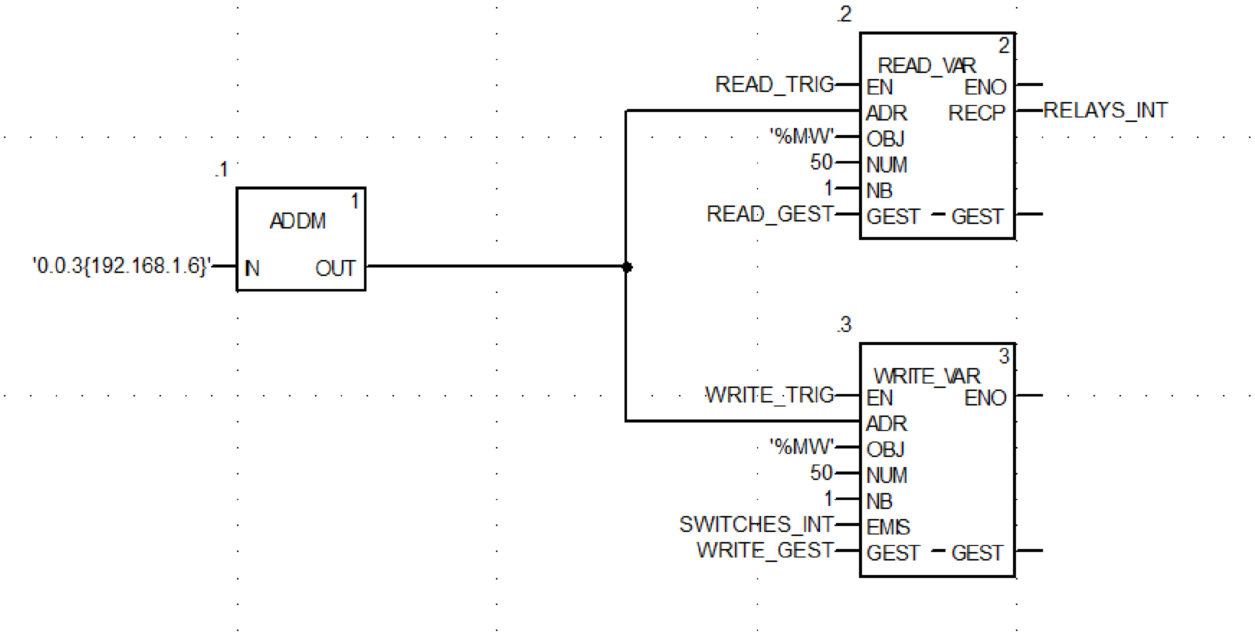


Name	Type	Value	Address
READ_GEST	ARRAY[1..4] OF INT		
READ_GEST[1]	INT		
READ_GEST[2]	INT		
READ_GEST[3]	INT	5	
READ_GEST[4]	INT		
READ_TRIG	BOOL		
RELAY_0	EBOOL		%Q0.3.0
RELAY_1	EBOOL		%Q0.3.1
RELAY_2	EBOOL		%Q0.3.2
RELAYS_INT	ARRAY[1..2] OF INT		
RELAYS_INT[1]	INT		
RELAYS_INT[2]	INT		
REMOTE_SWITCHES	WORD		%MW50
SWITCHES	ARRAY[0..15] OF EBOOL		%I0.2.0
SWITCHES[0]	EBOOL		%I0.2.0
SWITCHES[1]	EBOOL		%I0.2.1.0
SWITCHES[2]	EBOOL		%I0.2.2.0
SWITCHES[3]	EBOOL		%I0.2.3.0
SWITCHES[4]	EBOOL		%I0.2.4.0
SWITCHES[5]	EBOOL		%I0.2.5.0
SWITCHES[6]	EBOOL		%I0.2.6.0
SWITCHES[7]	EBOOL		%I0.2.7.0
SWITCHES[8]	EBOOL		%I0.2.8.0
SWITCHES[9]	EBOOL		%I0.2.9.0
SWITCHES[10]	EBOOL		%I0.2.10.0
SWITCHES[11]	EBOOL		%I0.2.11.0
SWITCHES[12]	EBOOL		%I0.2.12.0
SWITCHES[13]	EBOOL		%I0.2.13.0
SWITCHES[14]	EBOOL		%I0.2.14.0
SWITCHES[15]	EBOOL		%I0.2.15.0
SWITCHES_INT	ARRAY[1..1] OF INT		
SWITCHES_INT[1]	INT		
WRITE_GEST	ARRAY[1..4] OF INT		
WRITE_GEST[1]	INT		
WRITE_GEST[2]	INT		
WRITE_GEST[3]	INT	5	
WRITE_GEST[4]	INT		
WRITE_TRIG	BOOL		

4. In TON, set READ_TRIG to trigger on and off every second.

6. Set the input for ADDM as the string “0.0.3{192.168.1.#}” in which the # is the neighboring lab bench number. The ADDM output goes into both READ_VAR and WRITE_VAR “ADR” inputs. *Note: Form pairs between benches (1-2 3-4 5-6).*

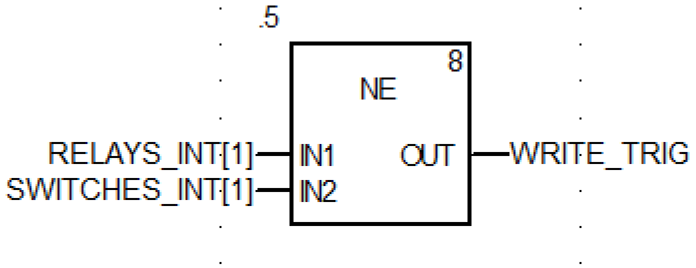
7. Set the READ_VAR and WRITE_VAR blocks as depicted below.

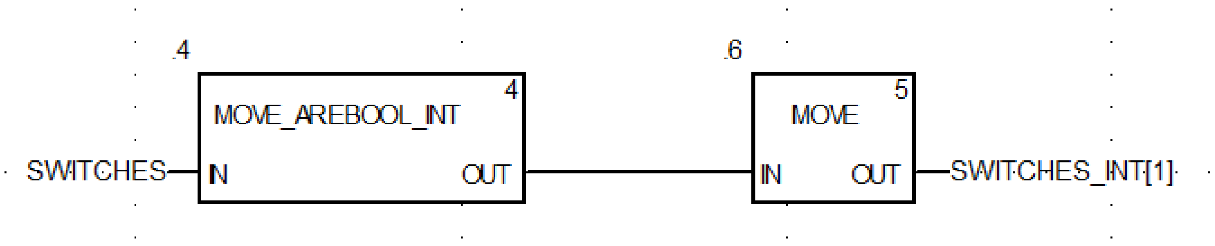


In both READ_VAR and WRITE_VAR blocks, the OBJ input requires a string. The string is typically the beginning of an address, such as “%M” or “%MW.” Since we desire the remote PLC to process words, the necessary address is “%MW,” or “Memory Word.” The number 50 in NUM denotes the particular address we want to access. We read the variable REMOTE_SWITCHES, stored in the address %MW50, and input this information into RELAYS_INT. Observe that “1” is in NB. This is because READ_VAR and WRITE_VAR reads and writes to array-type variables. If we want to access two consecutive elements in an array, NB changes to two.

Note: It is important that the GEST variables have “5” assigned in the third element of the array. This number sets the speed of read/write commands.

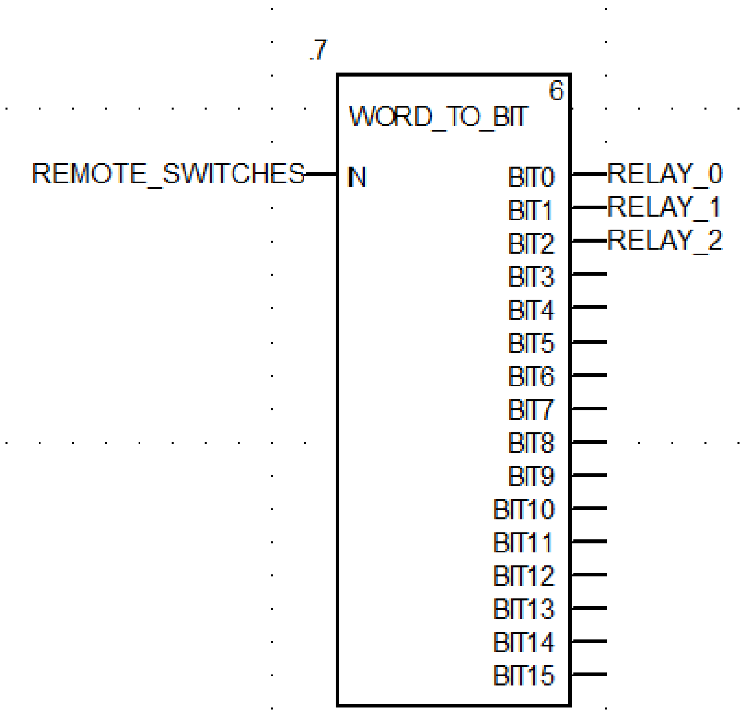
8. Allow WRITE_VAR to only operate when there is a mismatch between your local switches and the neighboring relays. This is done to prevent constant switching of the relays by only updating them when necessary. This is accomplished with a NE block, in which the first elements of the arrays RELAYS_INT and SWITCHES_INT are compared to detect a mismatch.





Since the NE block requires INT data types, MOVE blocks are necessary to complete the operation.

9. For the ability to observe which remote switches are enabled, a WORD_TO_BIT block allows you to observe which relays are on.

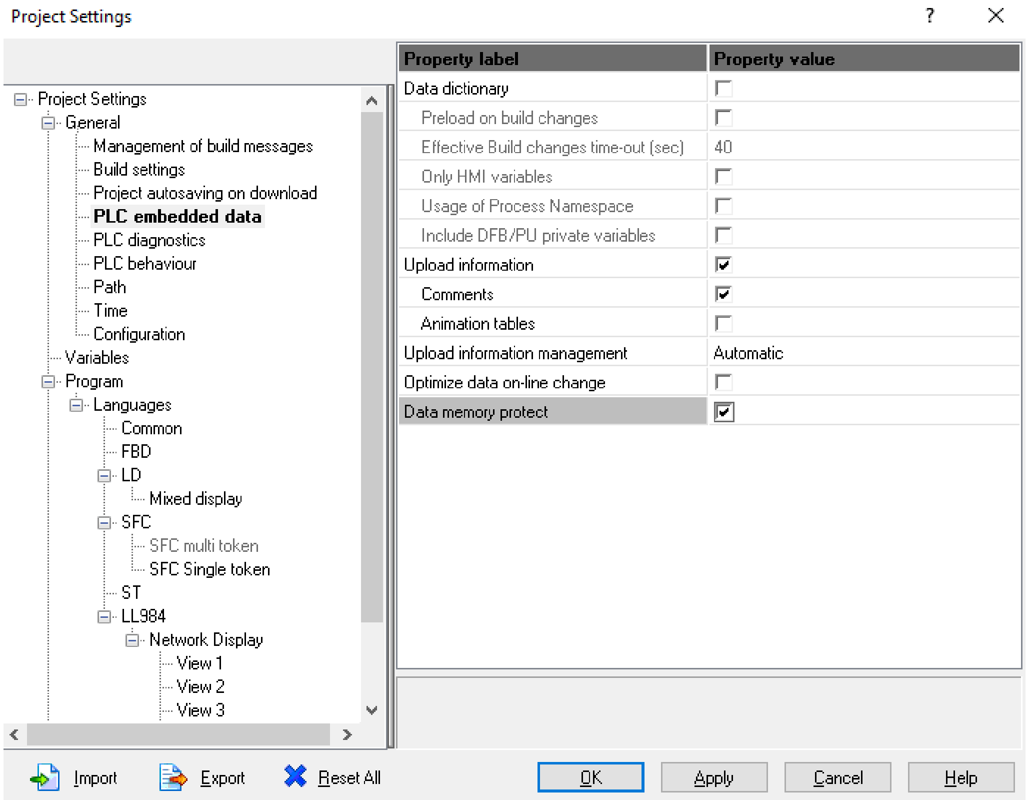


10. Transfer the project to the PLC and communicate with the neighboring PLC. This may require both PLCs to have working FBDs first.

Task 3: Memory Protection

1. After establishing communications, disconnect the PLC.

2. Under Tools > Project Settings > PLC embedded data, enable “Data memory protect”.



Property label	Property value
Data dictionary	□
Preload on build changes	□
Effective Build changes time-out (sec)	40
Only HMI variables	□
Usage of Process Namespace	□
Include DFB/PU private variables	□
Upload information	☑
Comments	☑
Animation tables	□
Upload information management	Automatic
Optimize data on-line change	□
Data memory protect	☑

3. Double click the eP584040 CPU. Under the Data Protection tab, change the value in “%MW Protect” to 50. Variables assigned to addresses over %MW50 should be protected from outside interference.

4. Connect to the PLC again, and rebuild the project. Then observe if there are any changes to the communication. You should not be able to make changes to the neighboring PLC anymore.