**DEVELOPMENT OF CYBER RANGE FOR OPERATIONAL TECHNOLOGY USING OPEN SOURCE SOFTWARE**

S.Yamada \*,a, M. Matsunokia , T. Kanmachia , M. Yamaguchia ,

S. Nakayamab , S. Ueta c and J. Sato d

a Department of Electrical Engineering, National Institute of Technology, Ishikawa College, Ishikawa, Japan

b Department of Social Design Engineering, National Institute of Technology, Kochi College, Kochi, Japan

c Education and Research Support Center, National Institute of Technology, Kochi College, Kochi, Japan

d Course of Information Systems Engineering, National Institute of Technology, Tsuruoka College, Tsuruoka, Japan

\*E-Mail: satoru@ishikawa-nct.ac.jp

**Industrial control systems such as factories, power plants, and transportation systems are used in various social infrastructures. Networked control systems offer benefits such as remote monitoring and operation of control systems and intelligent systemization. However, most communication protocols for ICS were designed without cybersecurity in mind. A cyber attack on an ICS, instead of an attack on an information system alone, can directly affect the physical object. Incidents can shut down processes controlled by the ICS and services provided by the ICS or deliver products that do not meet product requirements. Incidents can also result in lost opportunities by disrupting the production or shipment of products containing hazardous materials. Therefore, operational technology (OT) cybersecurity is critical in protecting the industrial environment and infrastructure.**

**OT cybersecurity training requires the creation of a test environment that closely resembles a real-world environment, including PLCs and control devices. However, vendor-supplied PLCs are subject to restrictions such as disclosure and confidentiality.**

**In this study, we developed cybersecurity training materials using OpenPLC, an open source system without such restrictions. The human-machine interface (HMI) was developed using the open source software Node-RED.**

**The developed system allows students to learn about cyber-attacks and dangers on ICSs, such as information theft through man-in-the-middle attacks and malfunctions caused by cyber-attacks on vulnerable protocols.**

**Keywords:** *cyber range, OpenPLC, cyber security education, operational technology, open source software, Node-Red*

**Introduction**

Until now, cyber-attacks have mainly targeted information systems such as web services, e-mail systems, and corporate business systems. Cyber-attacks were mainly aimed at stealing companies' corporate intellectual property and personal information, as well as system downtime and tampering. Recently, however, social infrastructures such as factories, power plants, and transportation systems have begun to be targeted, and there is a concern that systems that provide social services and maintain safety may be attacked. Industrial control systems have been considered relatively safe from network attacks, but in recent years, the number of cyber-attacks has increased.

In 2010, malware called Stuxnet infected the industrial control system of a nuclear facility in Iran, causing it to malfunction. In 2015, a cyber attack caused a massive power outage in Ukraine, profoundly impacting people's lives. Cyber attacks on industrial control systems have continued to increase since then, and there is a shortage of security personnel in industrial control systems, making training such personnel an urgent task. However, security education for industrial control systems has been conducted infrequently, and there needs to be teaching materials for security education, in contrast to security personnel training for information systems.

As part of efforts to develop human security resources, some higher education institutions are conducting training in the form of practical exercises. Exercises are conducted using specialized experiential learning tools, and exercises are conducted using a cyber range that enables training based on actual security incidents. Exercises using the Cyber Range can be conducted in a virtual environment that simulates an existing system, and assuming actual incidents, it is possible to conduct highly realistic and practical exercises. While recognizing the necessity of a training system, the introduction of Cyber Range has not progressed due to the high introduction cost. There are confidentiality obligations regarding high cost and vulnerability. Therefore, there is almost no cyber range for industrial control.

In this research, We created exercise materials using OpenPLC, open software not subject to such restrictions. In this teaching material, you can learn about network attacks related to PLC. In this paper, we report the outline of this teaching material and the result of education.

**System Overview**

1. Software system

Figure 1 shows the architecture of a typical industrial control system. The system consists of field devices, PLCs that control them, and a Human Machine Interface(HMI), Supervisory Control, and Data Acquisition (SCADA).



**Figure 1 Typical Industrial Control System**

The developed system consists of OpenPLC runtime, field devices, signal input interface, and SCADA. Node-RED can be used as SCADA to link with external databases and control network devices flexibly.

OpenPLC, an open source project, was used for the PLC part. The OpenPLC consists of the OpenPLC Editor for PLC program development, the runtime for executing the program, and the HMI Builder for providing SCADA and HMI environments.



**Figure 2 OpenPLC Editor**

The software architecture of the OpenPLC Editor was developed by IEC 61131-3, the international standard for PLC programming languages, and includes the following development languages: Ladder Diagram (LD language), Function Block Diagram (FBD language), Structured Text (ST language), and Function Block Diagram (ST language). Structured Text (ST language), Instruction List (IL language), and Sequential Function Chart (SFC language) are available as development languages, providing a global standard development environment.



**Figure 3 Human Machine Interface**

The OpenPLC runtime supports the Raspberry Pi and FreeWave ZumLink 900 series embedded system platforms and software runtimes running on Windows and Linux. Furthermore, by connecting an Arduino as a slave device, it can function as I/O for the software PLC, and I/O points of the embedded system platform can be extended.

HMI and SCADA were built using Node-RED. Figure 3 shows the operation screen of the developed HMI system, which consists of a display of digital signals input to the PLC runtime, control status of external devices, analog signals from sensor devices, and operation/stop buttons for control devices. Figure 4 shows an overview of the cyber range developed.



**Figure 4 Cyber Range Overview**

The communication between OpenPLC Runtime and SCADA uses Modbus/TCP. This open protocol uses the TCP/IP application layer to communicate, so there are no restrictions on the physical layer, allowing the system to operate in remote locations far from the experiment.

The system uses a polling cycle of 100 ms, and the SCADA system display is updated every 100 ms.

1. Hardware System

Figure 5 shows the overall configuration of the developed PLC experiment device. The control program developed by Open PLC is sent to the Raspberry Pi and executed. Using Arduino Uno as a remote I/O device provides the following advantages.



**Figure 5 Overview of Hardware System using OpenPLC**



**Figure 6 Overall Structure of the Control Circuit**

The Arduino Uno's analog input terminal can handle analog signals, such as signals from sensors.

The digital input terminal can be used to input 5V signals, commonly used in education. The number of analog output terminals can be increased. The electromagnetic relay used for control is a 24 V drive relay commonly used in control panels. Figure 6 shows the overall structure of the control circuit.

An isolated drive circuit was fabricated to drive the electromagnetic relay. Figure 7 shows the configuration of the drive circuit. A photocoupler is used to convert the Arduino Uno's output voltage to the electromagnetic relay's voltage.



**Figure 7 Drive Circuit**

The interface circuit consists of an analog signal input section, a digital signal input section, and an isolated relay drive circuit. Elements necessary for control, such as sensors and switches, can be easily connected via connectors. Pull-up resistors required when using switches are mounted on the board, and a footed pin socket is used for connection to the Arduino Uno, which can be easily connected by inserting pins into the Arduino Uno's pin socket.

**Training Scenarios**

1. Reconnaissance

Network reconnaissance is an essential part of the early stages of a cyberattack. Detailed information about a target's network can provide insight into the target's infrastructure and potential attack vectors and exploits that lead to vulnerabilities. Attackers can use passive and active reconnaissance tools and techniques to retain large amounts of information while reducing the likelihood of detection.

In this scenario, the network analysis commands reveal the PCs on which the PLC and HMI are running and their communication protocols. Figure 8 shows the port scan results on a PC running the OpenPLC runtime. The results show that the PC has open ssh and Modbus/TCP ports.



**Figure 8 Port Scan Result**

1. Man-In-The-Middle attack

A man-in-the-middle attack is a cyber attack in which a malicious attacker intrudes into a conversation between two parties, impersonating both parties and gaining access to information that the two parties intended to share. Figure 11 shows man in the middle attack model. The malicious attacker intercepts and transmits data intended for the other party or never intended to be transmitted without the outside party being aware of it until it is too late. The attacker launches a man-in-the-middle attack between the PLC and the HMI, intercepting communications between the PLC and the HMI and acquiring PLC control commands and sensor data without the operator being aware.



**Figure 9 Man in the Middle Attack Model**

1. Modbus/TCP attack

Modbus packets have a function code that specifies the type of operation requested. All Modbus devices have a register map of functions used to monitor, configure, and control the input/output of the module. The Modbus/TCP protocol is an extension of Modbus Serial to TCP/IP communication, with features such as encryption and authentication. It does not have encryption and authentication. Figure 10 shows a packet-captured Modbus communication.

Therefore, ICSs controlled by the Modbus/TCP protocol are vulnerable to cyber-attacks. The ICS is hijacked from intercepted Modbus/TCP communications in this scenario.



**Figure 10 Part of Packet Capture by Wireshark**

**Practicing** **the developed materials**

A lecture using the developed teaching materials was conducted in the Robotics Systems Control Engineering course at the National Institute of Technology, Kochi College. The students who attended this lecture were electrical, electronic, and mechanical students who did not specialize in information engineering. The lecture included network reconnaissance and an attack using a vulnerability in the Modbus protocol.



**Figure 11 Lecture using developed teaching materials**

The following are some comments from the students who attended the lecture.

I could understand the advantages and dangers of connecting ICS to an open network.

I understood the necessity for electrical and mechanical engineers to know the terms related to networking.

This lecture was presented at the K-SEC public lecture event.

**Conclusions**

This paper reports constructing a cyber range in an industrial control system using OpenPLC, an open source software. This system can connect field devices used, and students can learn about the threat of cyber-attacks in real space.

The advantage of this material is that it is composed entirely of open source software, making it vendor-independent and inexpensive. On the other hand, frequent version upgrades of OpenPLC and Node-RED require revision of the Cyber Range Construction Manual.

We want to expand the Cyber Range by using this material in technical colleges and referring to their feedback.

**Acknowledgments**

This work was supported by JSPS KAKENHI Grant Number 20K03241.

**References**

Ayesha Rahman, Ghulam Mustafa, Abdul Qayyum Khan, Muhammad Abid, Muhammad Hanif Durad. (2022). *Launch of denial of service attacks on the modbus/TCP protocol and development of its protection mechanisms*. International Journal of Critical Infrastructure Protection, Volume 39, 100568

E. Korkmaz, A. Dolgikh, M. Davis and V. Skormin. (2016). *ICS security testbed with delay attack case study*. MILCOM 2016 - 2016 IEEE Military Communications Conference, 2016, pp. 283-288

François Karch. (2016). *Stuxnet Recruits the Proteasome to Take Down Polycomb.* Developmental Cell,Volume 37, Issue 6, pp. 485-486

Jean-Paul A. Yaacoub, Ola Salman, Hassan N. Noura, Nesrine Kaaniche, Ali Chehab, Mohamad Malli. (2020). *Cyber-physical systems security: Limitations, issues and future trends*. Microprocessors and Microsystems, Volume 77

Jeff Morgan, Mark Halton, Yuansong Qiao, John G. Breslin. (2021). *Industry 4.0 smart reconfigurable manufacturing machines*. Journal of Manufacturing Systems,Volume 59,2021, pp. 481-506

Juan Du, Junzheng Zhang, Tao He, Yajuan Li, Ying Su, Feng Tie, Min Liu, Peter J. Harte, Alan Jian Zhu. (2016). *Stuxnet Facilitates the Degradation of Polycomb Protein during Development*. Developmental Cell,Volume 37, Issue 6,Pages 507-519

Muhammad M. Roomi, Wen Shei Ong, Daisuke Mashima, Suhail S.M. Hussain. (2022). *OpenPLC61850: An IEC 61850 MMS compatible open source PLC for smart grid research*. SoftwareX, Volume 17,100917

R. Nakata and A. Otsuka. (2021). *CyExec\*: A High-Performance Container-Based Cyber Range With Scenario Randomization.* in *IEEE Access*, vol. 9, pp. 109095-109114

S. Karnouskos. (2011). *Stuxnet worm impact on industrial cyber-physical system security*. IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, VIC, Australia, pp. 4490-4494

S. Shin, Y. Seto. (2020) . *CyExec - Training Platform for Cybersecurity Education Based on a Virtual Environment*. International Journal of Learning Technologies and Learning Environments International Institute of Applied Informatics, Vol. 3, No. 1, 1 – 20

Thiago Alves, Rishabh Das, Aaron Werth, Thomas Morris. (2018). *Virtualization of SCADA testbeds for cybersecurity research: A modular approach*. Computers & Security, Volume 77, pp. 531-546

Thiago Alves, Thomas Morris. (2018). *OpenPLC: An IEC 61,131–3 compliant open source industrial controller for cyber security research*. Computers & Security, Volume 78, pp. 364-379