**Advancement of Control System Education and Its Application to Security Education**

W. Yamanouchi a, K. Yajima b and J. Sato \*,a

a NIT, Numazu College, Dept. of Electronics and Control Engineering, Numazu, Japan

b NIT, Sendai College, Dept. of General Engineering, Sendai, Japan

c NIT, Tsuruoka College, Dept. of Creative Engineering, Tsuruoka, Japan

\* jun@tsuruoka-nct.ac.jp

**Abstract**

**This paper introduces examples of advanced control system exercises using OMRON PLCs, which have been introduced in many KOSENs. Specifically, this paper presents a model and configuration of connecting PLCs via fieldbus and Ethernet to realize network compatibility of the system. Next, examples of IIoT (Industrial IoT) support and cyber security training environment and educational materials for ICS (Industrial Control System) will be introduced.**

**Keywords:** *Control System Education, Industrial Control System, Cybersecurity*

**Introduction**

In the manufacturing industry, the trend toward digitalization is progressing rapidly. As a result, information and manufacturing systems are being integrated to realize Industry 4.0 and DX (Digital Transformation). However, in the midst of this trend, damage caused by cyber-attacks has become more apparent, and cyber-attacks are on the rise. As a result, there is an increasing need for cybersecurity measures and education in the manufacturing industry and factories. The Purdue model used for modelling industrial control systems represents the system hierarchically as follows:

1. ERP (Enterprise Resource Program): Management level [L4]

2. MES (Manufacturing Execution System): Planning level [L3]

3. SCADA (Supervisory Control and Data Acquisition): Supervisory level [L2]

4. PLC (Programmable Logic Controller)/DCS (Distributed Control System): Control level [L1]

5. Production Process: Field level [L0]

From the information technology perspective in operation, levels Two to Four can be classified as IT (Information Technology) and levels Zero to Two as OT (Operational Technology). The current production system is in the direction of being networked vertically and horizontally. In particular, the realization of Industry 4.0 and the utilization of IIoT (Industrial Internet of Things) require communication across hierarchical levels. Many technical colleges use stand-alone PLCs (not networked) for exercises. Unfortunately, this situation is also insufficient for pre-Industry 4.0 production systems. Therefore, we will introduce a case study of upgrading control system exercises using Omron PLCs, which have been introduced in many cases at KOSEN. Specifically, examples and configurations of PLCs connected by Fieldbus (RS485, RS232C) and Ethernet will be presented to realize system network support. Next, we will offer a case study of IIoT support by connecting Node-Red to a controller. Finally, a cyber security exercise environment and educational materials for ICS will be developed by taking advantage of Omron PLC's features that allow multiple industrial protocols (Modbus, FINS, OPC UA) to be used.



Figure 1 Automation Pyramid (Hierarchy of Automation) According to IEC 62264-3

**Industrial Ethernet and Fieldbus**

Industrial Ethernet refers to the use of Ethernet in an industrial environment, with a deterministic approach for real-time control over processes. Traditional Ethernet was not designed for real-time control but industrial variants of Ethernet like PROFINET, EtherNet/IP, EtherCAT, Modbus/TCP, POWERLINK, CC-Link IE, OPC UA, etc., have been adapted to better suit the needs of industrial control systems. Fieldbus refers to a family of industrial computer network protocols used for real-time distributed control for highly reliable systems. Examples of Fieldbus protocols include PROFIBUS, Modbus/RTU, CC-Link, DeviceNet, CANopen, etc. The following outlines the industrial protocols supported by the OMRON PLC.

Ethernet/IP (Ethernet Industrial Protocol) is an open industrial Ethernet network protocol developed by Rockwell Automation and maintained by the Open DeviceNet Vendors Association (ODVA). EtherNet/IP is built upon the Common Industrial Protocol (CIP), a technology also used by DeviceNet and ControlNet, which allows EtherNet/IP to be easily integrated with these networks. Features of EtherNet/IP are as follows,

1. Transport and Network Layers: EtherNet/IP uses standard Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/Internet Protocol (UDP/IP) for its transport and network layers.
2. Real-time Data Transfer: EtherNet/IP uses both standard Ethernet and Industrial Ethernet switches and supports real-time I/O messaging and explicit messaging.
3. Objects: It uses objects to represent data on a network. Each device on a network is represented as a collection of objects.
4. Integration: EtherNet/IP makes it possible to integrate safety, synchronization, motion, and configuration, as well as information and standard control onto one network.
5. Interoperability: The use of CIP allows for high interoperability among devices from different vendors.
6. Common Industrial Protocol (CIP): CIP provides a consistent approach to data exchange in manufacturing automation. It is application-layer protocol that encompasses a comprehensive suite of messages and services for industrial automation applications, including control, safety, synchronization, motion, configuration, and information.

FINS (Factory Interface Network Service) is a network protocol developed by OMRON Corporation for communications within industrial automation systems. This protocol allows OMRON PLC (Programmable Logic Controller) and other automation devices to exchange data and commands. FINS is used to establish communication between OMRON automation devices like PLCs, HMIs, temperature controllers, and others. It allows devices to read and write data, run and stop programs, change PLC modes, and perform other automation tasks. Key features of FINS are as follows,

1. Network Layers: FINS can be used over various network services including Ethernet, Controller Link, SYSMAC LINK, SYSMAC BUS, and serial communications (RS-232C/422/485).
2. Communication Types: FINS supports both cyclic and non-cyclic communications. Cyclic communication is used for continuous data exchange between devices, while non-cyclic communication is used for occasional data exchanges or for system configuration.
3. Message Structure: FINS messages consist of a header and data. The header includes fields for the command, the error code, the client node, the server node, and the client and service node addresses. The data contains the payload of the message, which depends on the command.
4. Command Structure: FINS commands are divided into multiple categories like memory area commands, data block commands, program commands, system commands, and others.

Modbus is a simple and robust serial communication protocol used in industrial automation and other applications. It was developed in 1979 for use with Programmable Logic Controllers (PLCs), and despite the development of more complex protocols, Modbus remains a common choice due to its simplicity and ease of deployment. Key features of Modbus are as follows,

1. Master-Slave Structure: Modbus uses a master/slave model for communication. The master device issues commands and the slave devices respond by providing the requested data or performing the action.
2. Modbus RTU and Modbus ASCII: Modbus can operate in two modes - RTU (Remote Terminal Unit) and ASCII. Modbus RTU is a compact, binary representation of the data while Modbus ASCII is human-readable. Modbus RTU is the most commonly used variant.
3. Modbus TCP/IP: In addition to the original serial versions, Modbus can also be used on Ethernet-based networks, in which case it's referred to as Modbus TCP/IP.
4. Function Codes: Modbus messages include function codes to indicate the type of action to be performed, such as reading from or writing to registers, reading device identification, etc.
5. Data Model: Modbus uses a simple data model that includes discrete inputs, coils, input registers, and holding registers.

OPC UA (OPC Unified Architecture) is an industrial M2M (machine to machine) communication protocol for interoperability developed by the OPC Foundation. It combines the functionality of the OPC Classic specifications into one extensible framework, enabling secure, reliable and vendor-neutral transport of raw and preprocessed data from sensors to enterprise software. Key features of OPC UA are as follows,

1. Platform-Independent: OPC UA is platform-independent and can be used on different operating systems and hardware platforms.
2. Security: OPC UA has integrated security models that ensure data integrity and confidentiality. It includes features like authentication, authorization, encryption and auditability.
3. Data Modeling: OPC UA allows for the abstract description of data, which can then be shared consistently across all levels of an organization. This helps with the integration of data from different systems.
4. Scalability: OPC UA scales from small devices and embedded systems up to large enterprise applications.
5. Protocol Flexibility: OPC UA can use various protocols for the transport of data, including HTTP, HTTPS, and various forms of TCP.

EtherCAT (Ethernet for Control Automation Technology) is an open real-time Ethernet Master/Slave network developed by Beckhoff Automation. It is suitable for hard and soft real-time requirements in automation technology, in test and measurement, and many other applications. EtherCAT is widely used in a range of industries where real-time control is necessary, such as industrial automation, robotics, semiconductors, and test and measurement applications. It allows for fast control and data acquisition, making it useful in complex automation tasks. Key features of EtherCAT are as follows,

1. Efficiency: EtherCAT is designed to process on the fly: the Ethernet frame is processed by each slave device while it is being received, and the corresponding result is already on its way when the frame is sent. This makes EtherCAT communication highly efficient.
2. Real-time Performance: EtherCAT meets real-time requirements with jitter times down to the microsecond range.
3. Topology Flexibility: The network does not necessarily need to be configured; rather, it recognizes its configuration on its own, supporting a variety of topologies including line, tree, star, or any combination thereof.
4. Hardware Independence: EtherCAT slave devices can operate on any Ethernet hardware.
5. High Precision: EtherCAT provides highly accurate synchronization, which is essential for control and measurement applications.

**Results and Discussion**

Figure 2 shows the series of PLCs widely used at KOSEN. CP1L is donated by Omron to each technical college, and the control kit and controller are used for various exercises. Node-Red (Fugure 3) can be used as a unit corresponding to SCADA to construct an environment for analyzing various protocols and security exercises. Node-Red can also support Ethernet and Serial communication. However, most Omron PLCs support RS232C or USB communication as standard, but few support RS485. However, for the CP1L and NX1P2 mentioned above, it is easy to support RS485 by adding a front module. Therefore, it is easy to construct a security practice environment that supports communication methods widely used in industry in addition to Ethernet.



1. CP1L



1. NX1P2



1. NX1

Figure 2 Omron PLCs



Figure 3 Node-Red Dashboard

By using Node-red, sniffing of most protocols (except EtherCAT) can be performed using WireShark or similar. An example of a packet caputure is shown in Figure 4.



Figure 4 Packet Capture Sample by Wireshark

 By using Node-red, sniffing of most protocols (except EtherCAT) can be performed using WireShark, etc. An example of packet caputure is shown in Figure 4.

In addition to sniffing, Ethernet can be supported by Arp Spoofing, etc. Serial communication (Modbus, FINS) can be supported by the inexpensive devices shown in Figure 5.



Figure 5 Devices supporting RS485

**Conclusions**

Previously, it was thought that only Ethernet-capable PLCs would be able to handle security exercises. However, Fieldbus based on Serial communication has a market share of over 30% in the industry. Therefore, we have shown that a practical industrial security exercise environment can be realized by inexpensively modifying PLCs that were previously used as stand-alone units..

**References**

Popp, K. (2010). Industrial communication with PROFINET. Publicis.

Durrani, Z. (2008). A detailed study of Ethernet/IP. Instrumentation & Measurement Magazine, IEEE.

Hägglund, J. (2007). Real-Time Characteristics of Ethernet for Control Automation Technology (EtherCAT).

Palizban, O., & Zamani, M. (2013). Modbus communications in embedded systems: a case study for an industrial controller. Journal of Electrical Engineering, **63**(7-S), 116-123.

Colombo, A. W., & Schoessler, M. (2009). An introduction to IEC 61131-3 and Ethernet POWERLINK in automation and industrial systems.

Takaya, S., & Itaya, M. (2007). Introduction to the CC-Link IE industrial ethernet. IEEE International Symposium on Industrial Electronics (ISIE 2007).

Hopkins, M., & National Instruments. (2012). Understanding DeviceNet.

Lohr, F. (2001). CAN System Engineering: From Theory to Practical Applications.

Omron. FINS Commands Reference Manual.

https://www.ia.omron.com/support/manuals/index.html.