IIoT SOC Service

Seiichi Koizumi [*1] *Tetsuo Shiozaki* [*1]

To help customers promote digital transformation (DX), Yokogawa has been providing Yokogawa Cloud, an Internet of Things (IoT) cloud service. We are also striving to make DX services secure; we leveraged the know-how obtained through the operation of Yokogawa's internal security system (Yokogawa Security Monitoring Center: Y-SOC) and developed IT/OT security monitoring services. This paper explains technological trends in IT/OT convergence and introduces application examples of Yokogawa's IT/OT integrated SOC service.

INTRODUCTION

Toward digital transformation (DX), cloud services are expanding and operational technology (OT) and information technology (IT) are being integrated (IT/OT convergence). Although the IT and OT domains were traditionally managed separately, their networks are becoming increasingly interconnected to effectively use OT data as a management information resource. Figure 1 shows the architecture of an integrated IT/OT network[1].

In addition, the scalability, data lake, and machine learning functions of cloud services are needed to efficiently manage and analyze vast amounts of OT data. Accordingly, an increasing number of OT networks are now connected directly to cloud systems, skipping IT networks.

Yokogawa Cloud, an IoT cloud service, comes with various security measures such as log and event monitoring, vulnerability diagnosis, access control, and data encryption. Meanwhile, on-premises OT networks face security threats because they connect to the Internet and use general-purpose OS products, both of which are vulnerable to cyberthreats.

*1 DXP Planning Department, DX Platform Center, Digital Solutions Headquarters

According to IDC Japan's "2021 Survey on IoT/OT Security Measures for Enterprises in Japan"[2], 36.4% of companies have experienced security incidents or accidents related to their plants and systems (34.4% in the previous year). Nearly half of the companies (47.7%) consider that their IIoT/OT security measures are not sufficient. This paper explains the trend of IT/OT convergence and introduces Yokogawa's OT security operation center (OT SOC) through examples of its services.

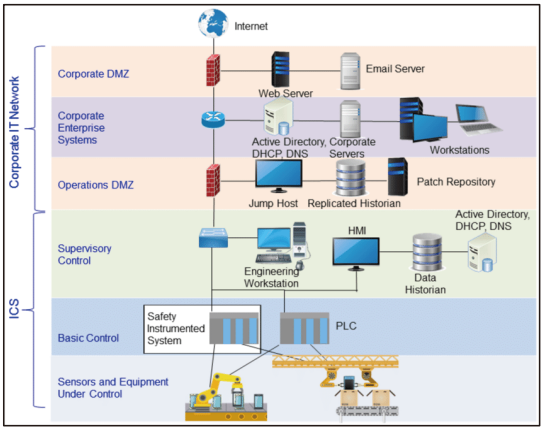

Figure 1 Architecture of an integrated IT/OT network

TRENDS OF IT/OT CONVERGENCE

Background

Due to the need to promote the Sustainable Development Goals (SDGs), the business environment in the process industry is undergoing major changes, including the shift to green energy and the introduction of carbon pricing. Merely improving either the IT domain or the OT domain is not sufficient to respond to these changes. Thus, IT/OT convergence, which transcends the boundaries of the two domains, is spreading. Previously, the layer of plant control equipment and that of IT systems such as enterprise resource planning (ERP) and customer relationship management (CRM) were separated from each other. Flexible IT technologies such as cloud computing and edge computing are used to store IT data and OT data in a data lake, making it possible to optimize plant operation tasks, which are difficult to handle by IT or OT control alone. This enables plants to automatically adapt to changes in the business environment, such as adjusting the manufacturing schedule in accordance with the CO_2 emission limit and optimizing utility control with digital twin technology that uses an energy consumption model.

Even with IT/OT convergence, some problems are beyond the capability of a single company, such as carbon pricing and CO_2 emission reduction in the entire value chain from raw materials to intermediate and final products. As a solution, one approach that is attracting attention is to flexibly create new business value through system of systems (SoS) collaboration beyond corporate boundaries[3]. Therefore, the application area of IT/OT convergence is expected to expand even further. Figure 2 shows Yokogawa's SoS concept[4].

Technologies Supporting IT/OT Convergence and Relevant Issues

ISA-95[5] and the Purdue Model[6] are often used for connecting OT controllers and IT systems. OT controllers include distributed control systems (DCS) and programmable logic controllers (PLC) while IT systems include ERP, supply chain management (SCM), and manufacturing execution systems (MES). These models satisfy functional and non-functional requirements in the OT domain such as standard support for industrial data, real-time performance, high availability, safety, and stability. Although these models assume on-premises IT systems, new IT/OT convergence models that incorporate cloud computing and edge computing[7] are also spreading.

This new IT/OT convergence approach offers various advantages to customers: visualization of the entire operations in the process industry and development of improvement measures by using the Industrial IoT (IIoT), AI, and digital twin technologies; flexible automatic control by using software defined everything (SDx) and virtual containers; and the provision of recurring services for manufacturing control through integration with the IT service management (ITSM) and operation support system/business support system (OSS/BSS). IT/OT convergence has become a driving force for DX in the manufacturing industry.

On the negative side, threats are emerging that cannot be covered by conventional IT- or OT-dedicated vulnerability countermeasures[8]. Specific technical issues to be solved are the increasing number of items requiring countermeasures due to cloud connection; inconsistent IT and OT management systems and coexistence of different security policies; limited performance of hierarchical network security; and difficulty in managing diverse devices and protocols.

DIFFERENCES BETWEEN IT SECURITY AND OT SECURITY

There are several differences between IT security and OT security; these must be considered when designing an OT SOC.

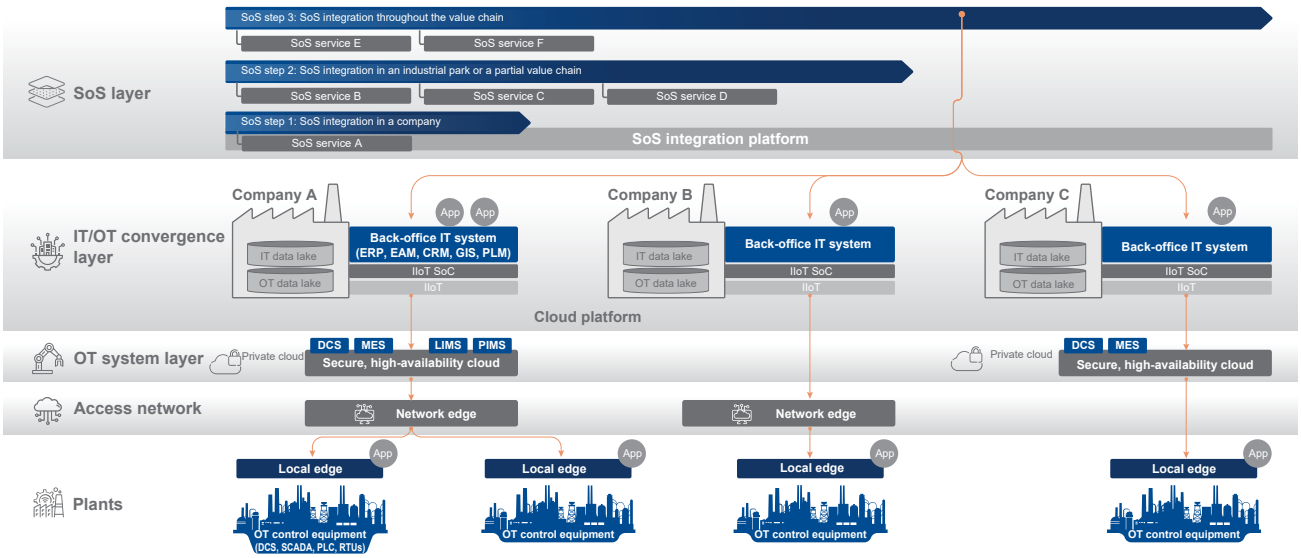

Figure 2 IT/OT convergence and system of systems

First, IT and OT differ in the priority of the three security elements: confidentiality, integrity, and availability.

In the IT domain, confidentiality is prioritized because the system must be defended from malware, phishing, data leaks, unauthorized access, and various other threats through the Internet. In the OT domain, the major threat is takeover of key process control equipment, safety systems, and production lines. Therefore, the highest priority in the OT domain is availability, and monitoring focuses on safety, reliability, and productivity. A monitoring infrastructure is needed that fully visualizes OT assets, logs, and event information and can investigate and track relevant events.

In industrial control systems for power, oil refining, and water treatment, complex physical processes are operated based on experience accumulated over the years. Therefore, unplanned shutdowns are likely to occur due to slight defects or abnormal patterns, even if they are not caused by malicious third parties. To identify and analyze the risks and prevent incidents, it is important to check for deviation in the process, suppress abnormal device behavior due to latent factors, and monitor new devices that may not be compatible with the existing system[9].

OT SOC needs to monitor the operating status of various devices and detect anomalies to ensure safety, as well as satisfy a higher service level agreement (SLA) in terms of the time from the occurrence of an event to the notification and its contents.

Second, security standards to be complied with are different. ISO27001, NIST, and PCI-DSS are for IT systems, and several other standards are applied to control systems (Figure 3). The North American Electric Reliability Corporation critical infrastructure protection (NERC CIP) requires detailed OT data. ISA/IEC 62443, an international standard for cybersecurity measures for industrial control systems, is referred to by many other standards. When monitoring for OT security, it is necessary to ensure consistency with these standards. Figure 4 shows the structure of the IEC 62443 series.

Figure 3 Standards for OT security

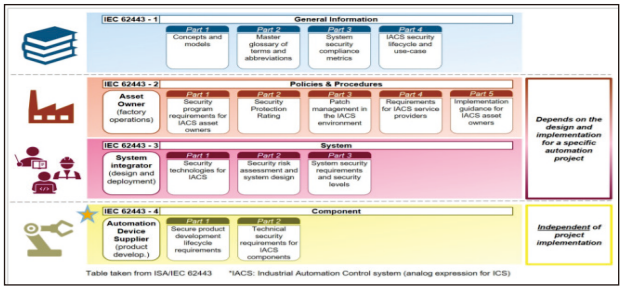

Figure 4 Structure of the IEC 62443 series[10]

Third, communication protocols differ. OT systems use various protocols (Modbus, MQTT, OPC UA) and industrial Ethernet (PROFINET Ethernet/IP) depending on the type of equipment, and some log formats are not disclosed. Therefore, the OT SOC comes with a different set of lenses (mechanisms for monitoring logs, events, networks, and event sequences) to collect, analyze, and visualize various data sets. In some cases, there is a need to negotiate with control device manufacturers on how to collect and interpret event data and logs.

Fourth, customer support is also different. IT systems are often managed by the information system department and there is a single point of contact. Meanwhile, OT SOC needs the help of OT engineers who are familiar with special process control equipment, safety systems, and production lines because OT systems are operated by local OT engineers, who directly access and analyze the data and identify the cause of a problem. For this reason, OT SOC security engineers are required to build relationships of trust with local OT engineers and be able to communicate in the local language.

YOKOGAWA'S APPROACH TO IT/OT SECURITY

Yokogawa's Efforts in Security Monitoring Services

Yokogawa set up Yokogawa Security Operation Center (Y-SOC) in 2019, which monitors various IT equipment in Yokogawa's 16 bases around the world. The monitoring targets include not only internal IT devices such as IDS, AD, PC, DHCP, and DNS but also cloud environments including the web application firewall (WAF) of Amazon Web Services and Microsoft Azure and collects logs of 500-600 million events/day for real-time analysis[11].

Y-SOC has a cloud-based security information and event management (SIEM) system, develops detection programs based on cyberthreat intelligence (CTI) and machine learning, integrates ServiceNow SecOps with SecOps connector, and automates operations from incident detection to defense (security orchestration, automation and response: SOAR). The monitoring targets have now expanded to cover the OT domain such as the IoT gateway, PLC, collaborative information server, and remote-FAT. Figure 5 shows the structure of Y-SOC, and Figure 6 shows the flow of the automated incident response. When Y-SOC detects an incident [1], ServiceNow SecOps automatically refers to cyber threat information [2] and blocks the attack [3], requests CSIRT to perform tasks [4], and reviews the incident [5].

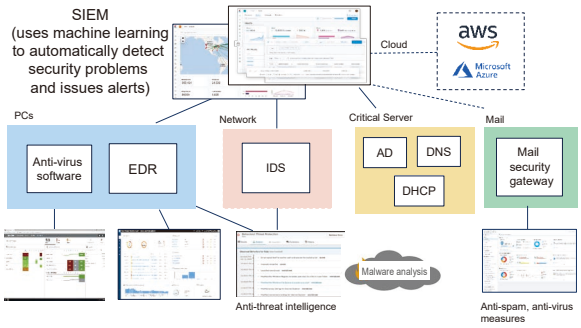

Figure 5 Structure of Y-SOC

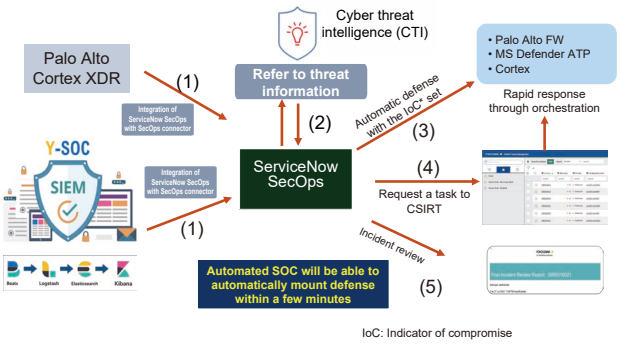

Figure 6 Workflow of incident response and automated protection

In addition, the center offers an OT SOC/network operations center (NOC) service, in which each monitoring center monitors the security status of customers. Unified threat management devices (e.g., FortiGate, NOZOMI Networks Guardian) and monitoring servers dedicated to communication analysis are installed at key locations in plant networks. When an incident occurs, the center reports the detection and communication status and provides advice on how to respond.

IT/OT-integrated SOC

Yokogawa has been expanding an SOC service that integrates Y-SOC's cybersecurity expertise with OT SOC operations at each regional office (Region).

This service combines the capabilities of Region SOC engineers to provide outstanding support to customers with the capabilities of Y-SOC to develop detection programs based on machine learning and analyze security, enabling security threats to be analyzed more efficiently.

Y-SOC's cloud collects various events and log information from customer OT systems, and its dashboard shows the information in an integrated manner. When any alert is detected by CTI and machine learning, an alert is automatically issued to Region SOC engineers, who then use various product consoles and tools to analyze the alert in detail. Incident workflows between Y-SOC and Region SOC as well as dashboard screens for customers are developed in Jira, an open-source program used for managing issues and projects. Region SOC engineers can make full use of Y-SOC's cybersecurity knowledge and offer meticulous service to local customers through working in closer cooperation with them. Figure 7 shows the collaboration between Y-SOC and Region SOC.

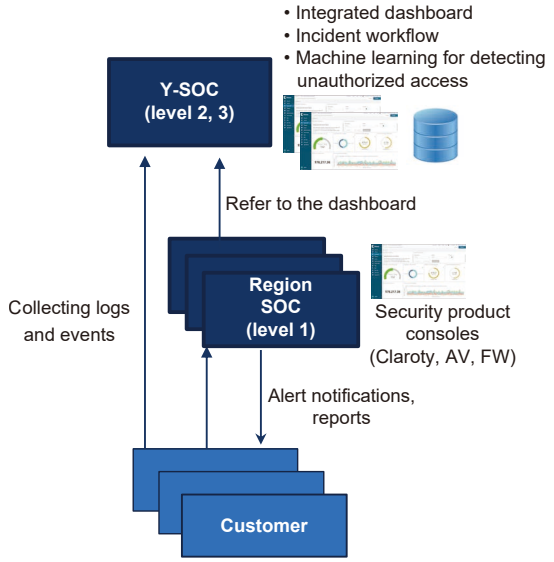

Figure 7 Collaboration between Y-SOC and Region SOC

Example of OT SOC Monitoring

An example of OT SOC monitoring is presented below. Figure 8 shows the configuration of the OT SOC monitoring network, and Figure 9 shows the architecture of OT SOC.

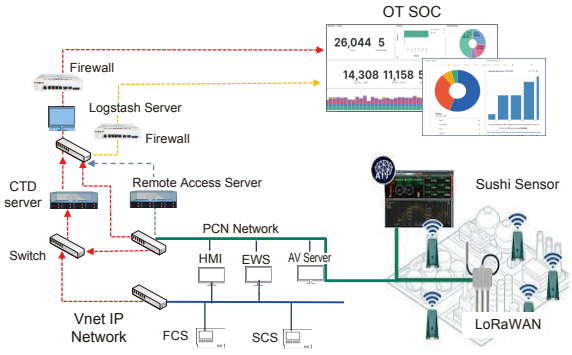

Figure 8 Configuration of the OT SOC monitoring network

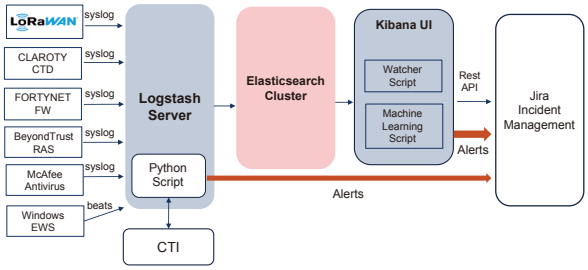

Figure 9 Architecture of OT SOC

Table 1 Relationships between OT SOC use cases and security standards

No.	Use case	Description	ICS/ISO standard	Security item
1	Monitoring IoT devices (Sushi sensor, etc.)	Monitors Modbus and other communications to detect unauthorized/unapproved devices. Collects LoRaWAN gateway logs and monitors the battery level of sensors.	ISO/IEC 19770-1, IEC 62443	Asset management
2	Monitoring the firewall policy	Monitors in-bound/out-bound packets, changes in the firewall policy and their validity, and the resulting configuration.	ISO/IEC 19770-1, IEC 62443	Compliance management
3	Monitoring downloads and configuration changes	Tracks changes in any node (EWS/FCS) and issues alerts.	ISO/IEC 19770-1, IEC 62443	Asset management
4	Detecting viruses	Monitors alert information about virus infection. Monitors unauthorized connection of USB flash drives.	IEC 80001-2-8: 2016, ISO/IEC 27035, ISO 27039	Risk management
5	Monitoring the remote access server	Monitors remote access performed for maintenance. Monitors for unauthorized access. Monitors downloading and uploading of maintenance data.	IEC 62827-3: 2016, ISO/IEC 18028-4:2005	Remote access security
6	Monitoring the OT protocol	Deploys continuous threat detection (CTD) for monitoring OT equipment. Monitors map generation in the OT network and the status of the OT protocol.	ISO/IEC 19770-1, IEC 62443	Asset management

System logs from various devices are sent to the Logstash server (Elastic NV's tool for collecting and managing logs). Windows events are also collected from Level 2 process network servers (e.g., EWS). With reference to cyberthreat information (CTI), a Python script automatically detects unauthorized access and abnormal communication. Then the data are managed by Elasticsearch Cluster with a Hot-Warm architecture, which satisfies both easy access and accumulation of time-series data. A Watcher script and a machine learning script process the accumulated data and then Kibana (a visualization tool) displays them on the dashboard. When an incident is detected, a ticket is automatically generated by Jira via API and forwarded to SOC engineers at SOC level 1. In this case, we prioritize the availability of the OT system, identify the possible risk cases (use cases), and set risk priorities and notification times as the service level objectives (SLO) for each use case. We also check their consistency with IEC/ISO standards. Table 1 shows an example of prioritized use cases and specific monitoring actions.

The analysis results of each case can be monitored centrally on the dashboard. This makes it possible to comprehensively visualize the behavior of each node in the OT network, the correlation between each device and events, and IT and OT security. Figure 10 shows examples of OT SOC dashboard screens using the Kibana UI.

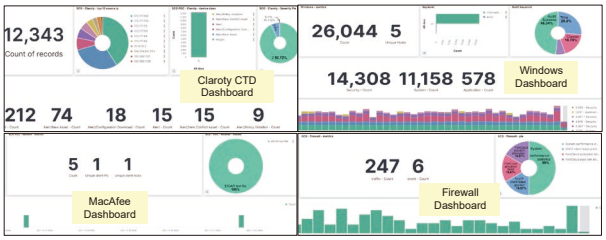

Figure 10 OT SOC dashboard screens

We have also sped up the workflow after the detection of an incident. An incident ticket is automatically generated by Jira and ServiceNow via API.

- Region SOC engineers at SOC Level 1 are responsible for security monitoring, equipment health checking, and customer contact. They also determine whether incident information falls under "true" or "false positive." True positive incidents are sent (escalated) to SOC Level 2.
- Engineers at SOC Level 2 analyze the incident for its threat potential based on relevant information and if they determine that it is necessary to issue an incident ticket, the incident information is escalated to Level 3.
- Engineers at SOC Level 3 compile a report on the incident about its handling, further investigation, and recovery measures.

A series of steps in the workflow are automatically processed by Jira, which is connected via API to the Elastic Cloud. Engineers at local Level 1 explain the results in detail to the customer by using the customer dashboard. The status of each incident ticket is visualized, and its SLA compliance is clearly shown. Figure 11 shows the OT SOC's engineer support system, and Figure 12 shows an example of an incident ticket and the relevant dashboard screen.

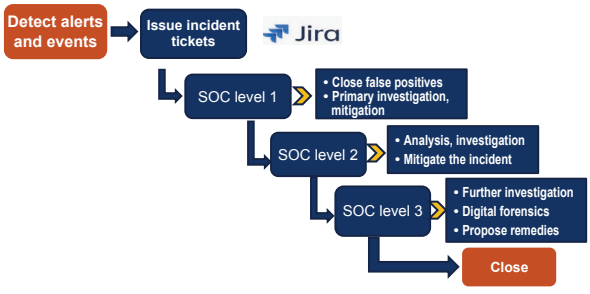

Figure 11 OT SOC's engineer support system

Figure 12 Example of an incident ticket and the relevant dashboard screen

FUTURE DEVELOPMENT

We are planning to strengthen the security-service capabilities of the Yokogawa Group. We will promote collaboration between Y-SOC and each Region SOC (Japan, Singapore, India, Romania, the Netherlands, and Thailand). By leveraging Y-SOC's cybersecurity analysis know-how, we will provide advanced IT/OT security services globally.

In addition to its own OT products, Yokogawa also aims to expand monitoring to other companies' OT products and develop cybersecurity intelligence for control systems including MITRE ATT&CK for Industrial Control Systems[12]. Figure 13 shows the organizational structure of the global security operation.

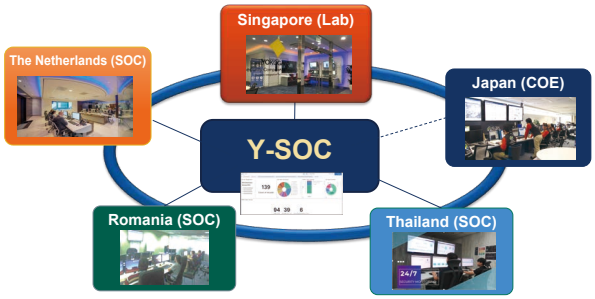

Figure 13 Structure of global security operation

CONCLUSION

This paper described Yokogawa's approach to security monitoring services in view of the ongoing convergence of IT and OT.

IT and OT are different from each other in terms of system availability and incident response. Based on interviews with customers about their IT/OT network environment, Yokogawa will propose how to collect log and event information according to the risk, develop a detection program using machine learning, and monitor customers' assets. Working with SOC engineers in each region, we also plan to develop DX security services tailored to customers, such as proposing incident response measures or workaround plans and providing incident response training.

REFERENCES

(1) Edward Colbert, Daniel T. Sullivan, Alexander Kott, "Cyber-Physical War Gaming," Journal of Information Warfare, Vol. 16, No. 3, 2017, pp. 119-133
(2) IDC Japan, "IDC Japan Releases Results of 2021 Survey on IoT/OT Security Measures for Enterprises in Japan," 2021 (in Japanese), https://www.idc.com/getdoc.jsp?containerId=prJPJ47631521 (accessed on June 1, 2022)
(3) Carlock, P.G., et al., "System of Systems (SoS) Enterprise Systems for Information-Intensive Organizations," Systems Engineering, Vol. 4, No. 4, pp. 242-261, 2001
(4) Yokogawa Electric Corporation, "Yokogawa Draws Up New Mid-term Business Plan, Accelerate Growth 2023," press release, 2021, https://www.yokogawa.com/news/press-releases/2021/2021-05-11/ (accessed on June 1, 2022)
(5) ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration
(6) Theodore J. Williams, "The Purdue enterprise reference architecture," Computers in Industry, Vol. 24, No. 2-3, 1994, pp. 141-158
(7) Wenbin Dai, Hiroaki Nishi, et al., "Industrial edge computing: Enabling embedded intelligence," IEEE Industrial Electronics Magazine, Vol. 13, No. 4, 2019, pp. 48-56
(8) Richard Paes, David C. Mazur, et al., "A guide to securing industrial control networks: Integrating IT and OT systems," IEEE Industry Applications Magazine, Vol. 26, No. 2, 2020, pp. 47-53
(9) VERVE, "What is an OT SIEM and how is it different from IT SIEM," 2020, https://verveindustrial.com/resources/blog/what-is-an-ot-siem-and-how-is-it-different-from-it-siem/ (accessed on June 1, 2022)
(10) Ease ISA/IEC 62443 compliance with EdgeLock™ SE05x (Rev. 1.1), 2020, https://www.nxp.com/docs/en/application-note/AN12660.pdf (accessed on June 1, 2022)
(11) Tetsuo Shiozaki, "Yokogawa's Approach to Cybersecurity in the IT/OT Convergence Environment," Yokogawa Technical Report English Edition, Vol. 64, No. 1, 2021, pp. 27-32, https://web-material3.yokogawa.com/1/31643/files/rd-te-r06401-005.pdf?_ga=2.133994635.485524645.1655879796-1121227122.1655879796 (accessed on June 1, 2022)
(12) MITRE, ATT&CK® for Industrial Control Systems, https://collaborate.mitre.org/attackics/index.php/Main_Page (accessed on June 1, 2022)