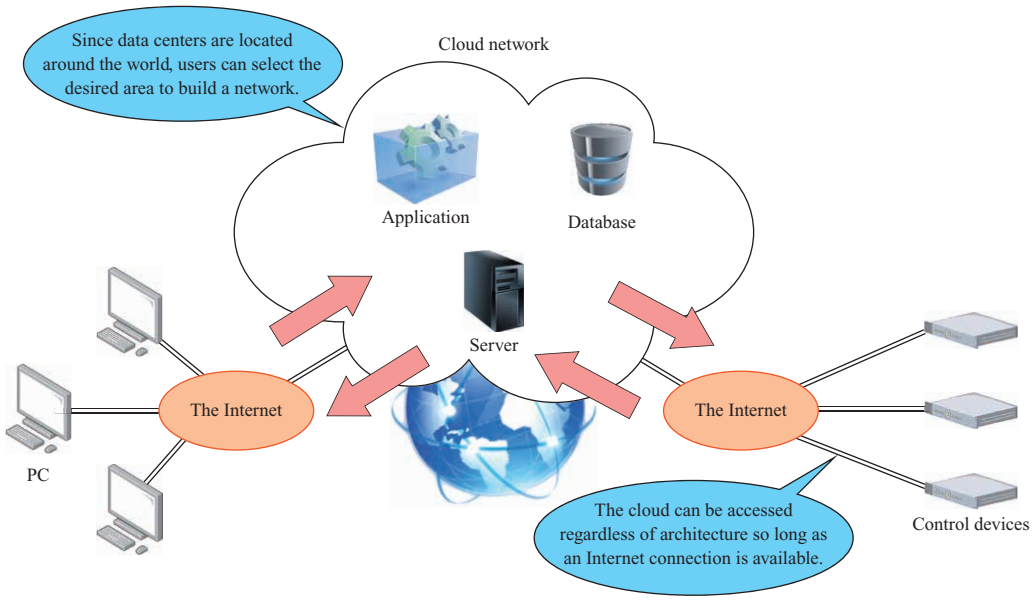
Development of Secure Remote Control Using the Cloud

Remote control technologies that meet needs for remote control while contributing to customers' safety and security

In the "New Normal" arising from the impacts of COVID-19, needs for remote control utilizing ICT are increasing in all industries. By making the most of a cloud platform, the IHI Group aims to realize both efficiency improvement and safety in remote control as well as in maintenance support of devices operating in factories.

HIRATA Keishiro
Advanced Control & Intelligent Sensing Group,
Technology Platform Center,
Technology & Intelligence Integration,
IHI Corporation



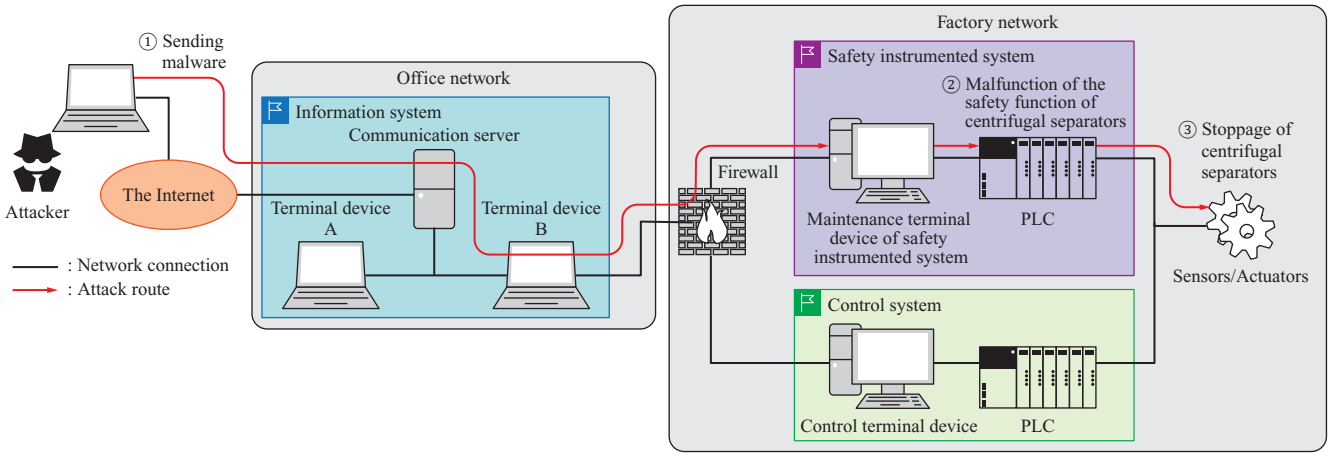
Conceptual diagram of a cloud

Current state of use of cloud services

Cloud services are a collective name for the services that provide computing resources via the Internet as shown in the figure above and are used for IT (Information Technology) services, a core of corporate operations and services. Cloud services are superior to systems in which devices are operated on the premises of a facility that users manage because cloud services do not require large initial investments associated with the introduction of hardware, nor do they require a large number of human resources for resource procurement, maintenance, and capacity use scheduling.

In Japan, because a principle that use of clouds should be considered first when building governmental information systems was established in 2018, use of clouds in the private sector has also started to advance.

The size of the cloud market continues to expand, and cloud platforms with major shares include Amazon Web



Example of the attack method with Stuxnet

Services (AWS), Microsoft Azure, and Google Cloud Platform. All of these platforms have data centers around the world, and users can use any of the servers located in the various areas. In particular, in the IaaS (Infrastructure as a Service) field, where computing resources, not services, are used via the Internet, AWS has a 45% market share and is the de facto standard for cloud platforms.

Trends in control system security

Conventional OT (Operational Technology) systems for controlling important infrastructure such as electricity and gas were designed and operated as independent systems without connection to the Internet or intranet information systems. Such systems made use of devices that featured non-standard OSs and network devices that communicated via non-standard communication protocols. However, technology standardization, such as the use of multi-purpose OSs and standard protocols, as well as open technologies have recently spread, and there is a trend of integrating IT networks and OT networks in order to build a network system with the aim of achieving effective use of data and resources. As a result, experts have pointed out an expansion in cyberattacks and increased exposure to vulnerabilities due to the use of general-purpose specifications.

In 2010, the first cyberattack against OT systems, which was conducted with the Stuxnet malware, was observed. When brought into a nuclear fuel facility in Iran, this malware tampered with the logic set for the PLC (Programmable Logic Controller), which controls the centrifugal separators, and carried out an attack, the flow of which is shown in the above figure. As a result, about 1 000 of the approximately 8 400 centrifugal separators were rendered inoperable, and the facility's operations were suspended. Since then, security incidents related to OT systems have been reported one after another. Recently, there was a case in which a petroleum pipeline in the U.S. was attacked by ransomware, which led to suspension of its operation, resulting in a gasoline supply shortage and other direct impacts on the lives of people.

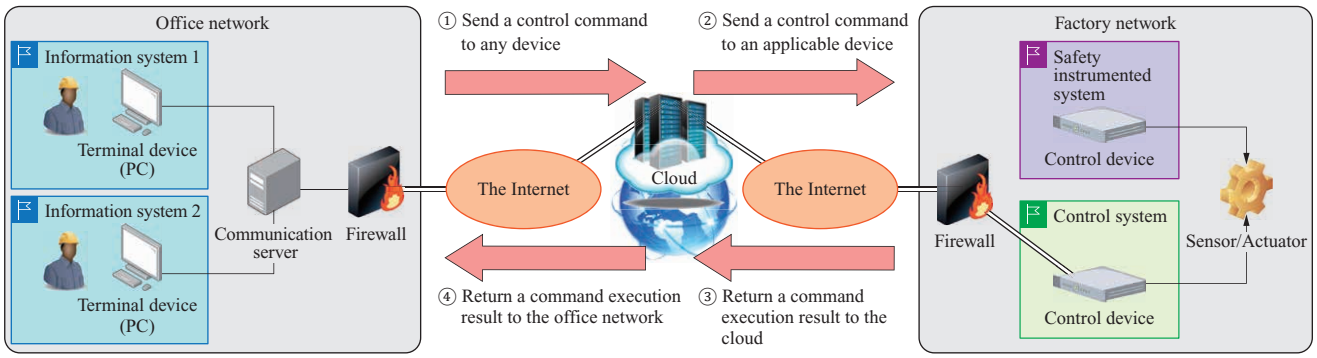
The IEC62443 standards, which are international standards on security function requirements, functional design, and technologies for OT systems, are referenced by many other standards, and standards for realizing both the safety and security of systems are being formulated. In addition, provision of a third-party certification system for IEC62443 has started, and the number of certificate issuance is increasing. In Japan, the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry are working to establish security laws. While keeping a close eye on these security trends, the IHI Group is also working on technological development to ensure safety and security.

Expectations for and issues with cloud-based remote control systems

The necessity of cloud usage is increasing for workstyle reforms using ICT, and the manufacturing field is no exception. Clouds are expected to be used for Smart Factories that obtain, analyze, and visualize floor data in the factory by using advanced analysis tools in the cloud as well as large-scale parallel computing that utilizes the wealth of computing resources available in the cloud. Furthermore, needs for remote control, in which control devices operating within a factory are controlled by physically remote offices for maintenance operations (refer to the figure on the next page), are increasing due to the COVID-19 pandemic. It is possible to build remote control systems for large numbers of bases and devices with a short lead time while reducing the initial investment by utilizing parallel computing in the cloud.

On the other hand, operation of cloud technologies for remote control systems has the following issues.

- Countermeasures against communication delays due to transmission via a cloud:
  Communication specification design to improve real-time bi-directional communications between the office and the factory.



Remote control system

- Security breach countermeasures against attacks via Internet communication:

  Prevent connection by unauthorized users or devices under the situation where connectivity with a network rises. Evaluate countermeasures for known vulnerabilities and communication robustness.

The following gives an overview of such countermeasure technologies.

(1) Countermeasures against communication delays

To prevent communication delays, transactions between a computer/device and the cloud must be reduced as much as possible. We have reduced communication delays by employing WebSocket, which allows bi-directional communication by a single connection only, for transactions between computers and the cloud. For transactions between devices and the cloud, we employ the MQTT (Message Queuing Telemetry Transport) communication method, which is lightweight and allows for point-to-multipoint communications. To relay these transactions, we built a server in the cloud. In addition, we prevented the response speed from falling when loads increase by activating multiple servers in the cloud based on the number of requests instead of having a single server receive all requests.

(2) Security breach countermeasures

To prevent unauthorized connections, we developed a function that controls requests by having the cloud monitor the communication connection with a device and command execution status of the device when the cloud receives a control command from a computer. When a computer or device communicates with the cloud individually, authorization is performed for each in order to prevent unauthorized connection. Computers authorize the operator by ID and password when a WebSocket communication connection starts, while devices use an individually issued certificate to perform authentication when an MQTT session starts. Both methods are encrypted by TLS (Transport Layer Security) to maintain a certain level of eavesdropping prevention.

Performance evaluation of the remote control system

Based on the aforementioned reviews, we will describe the communication response performance and security evaluations of the remote control system prototyped by the IHI Group. The control device used for the prototype system is a single-board computer having performance equivalent to that of general controllers.

(1) Communication response performance evaluation

We evaluated the communication response by using a cloud server which provided the nearest physical distance between a computer and a control device.

It took approximately 260 ms from when the computer sent a request to the cloud to when the cloud received a response indicating that the control device successfully received the request, and approximately 150 ms from when the cloud sent a control command to the control device to when the cloud received a response indicating that the control device successfully received the command. In the latter case, because the processing time of the program operating on the control device was 35 ms, the communication processing itself took approximately 115 ms.

All processing from when the computer sent the request to when it received the response indicating the control device worked was completed in approximately 400 ms in total, and it was confirmed that the remote control system could be operated with a standard response time as a web service.

(2) Security evaluation

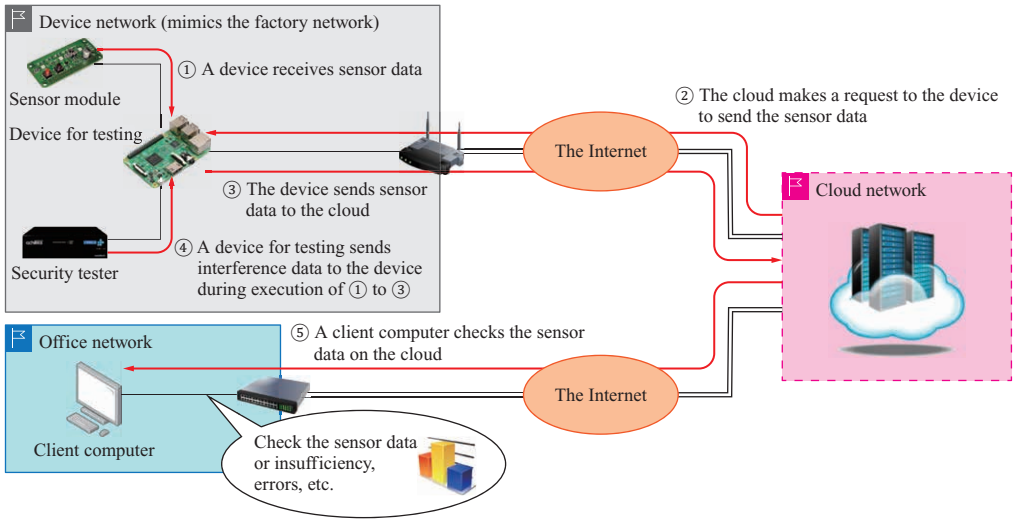
As a security evaluation, we performed tests based on the IEC62443-4-2 (device vulnerability test and communication robustness test).

- Vulnerability test

  To check if the OS, middleware, and application of the control device had any reported vulnerabilities, we sent test packets to the device. No fatal vulnerabilities were detected.

- Communication robustness test

  We checked the behaviors of the remote control



Security test configuration of the remote control system

device when a large volume of packets that might induce a breakdown or malfunction of the device or packets having incorrect structures were sent to the device. The data sent from the device to the cloud had no missing parts, and the usage rates of the CPU and memory were maintained at a steady level. As a result, we concluded that the device has a certain level of robustness.

Based on the above results of communication response and security evaluations, we confirmed that there were found no technological obstacles for operations of our prototype remote control system.

Future issues and perspective

The cloud-based remote control system is available not only for practical device operations such as control parameter adjustment but also throughout the entire lifecycle, including setting operations for introduction, disposal, and reuse of IoT devices. On the other hand, the network configuration environment and communication processing method differ greatly from those of conventional systems, and the system requires actions to be taken in terms of operation such as compliance with security policies and establishment of a management system. In addition, the system configuration and security implementation must be reviewed as necessary along with major updates to various cloud applications and developments in security regulations. We will work with internal and external cloud platform support teams, security experts, etc. to address these issues. In the future, we will identify the scope of use for this technology and applicable measures to make the most of the cloud in our activities through the promotion of the experimental cloud use project.

From a technological perspective, we think it is necessary to provide the prototype function as a web application that can be operated via an Internet browser. By doing so, we will be able to provide the function to all devices, including computers and smartphones, which we expect will improve both development efficiency and usability. In addition to remote control technology, by using maintenance support and preventive maintenance technologies in the digital transformation and lifecycle business fields, we hope to provide value to maximize the customer experience.

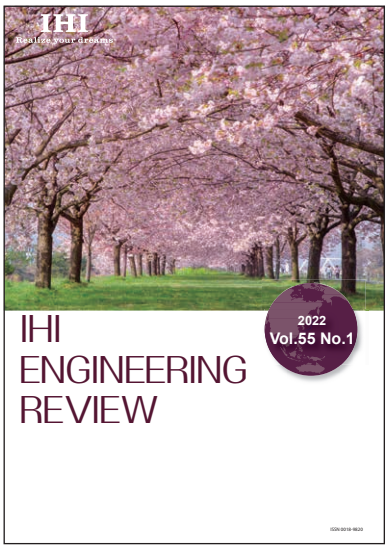
INFORMATION

Thank you very much for reading the article of IHI ENGINEERING REVIEW.
We hope you will take a look at other articles.

Webpages of our journals on technology are as follows:

Journal of IHI technologies (in Japanese)

IHI ENGINEERING REVIEW (in English)



Vol. 55 No. 1

Contents page of Vol.55 No.1

Our corporate website introduces our technology categorized according to social issues: “IHI Challenges with Society”. The articles of IHI ENGINEERING REVIEW are also provided there. We would appreciate it if you would visit our website.

IHI Challenges with Society

Technologies supporting IHI

Inquiries:
Editorial office of IHI ENGINEERING REVIEW
ihi-ty9776@ihi-g.com