Physically Isolated Information Security (PIIS) and MemWiper: A New Security Concept for Control Systems in IoT Era and Its Embodiment

Takayuki Arai [*1] *Makoto Nakaya* [*1]

Yokogawa proposes physically isolated information security (PIIS), a new security concept for reducing the risk of remote attacks on industrial control systems. PIIS can protect plants from remote attacks. As a simple implementation, Yokogawa has developed MemWiper, a prototype device that erases the memory of USB devices. MemWiper reduces the risk of virus infection through physical operation. This paper explains the PIIS concept and the MemWiper memory erasers.

INTRODUCTION

Thanks to the progress of sensing, wireless, and micro device technologies in recent years, the Internet of Things (IoT) is increasingly being applied to a wide area and various things are connected, operated, and controlled via networks. The IoT is also being introduced into the manufacturing industry. As shown in Figure 1, data measured in actual plants are quantitatively analyzed, learned, and modeled, and a virtual plant is built in cyberspace called a "Cyber Physical System" or "Digital Twin." The model in cyberspace simulates the behavior of plants, and can be used to determine the optimum operation conditions for challenges that arise in actual production sites, such as diversification of raw materials and fuels and adjustment of output. In this way, IoT technology contributes to safe operation and efficient production [(1)(2)].

However, as various things become connected via the Internet, there is an increasing risk of virus infection and unauthorized access. If a part of some software is found to be vulnerable, more attacks will focus on this part. Although standard software is relatively secure, none is perfect and if any security hole is left unfixed, it could easily become the target of attacks. The IoT makes things convenient and improves productivity, but in this IoT era appropriate security measures must be taken against possible attacks from the outside.

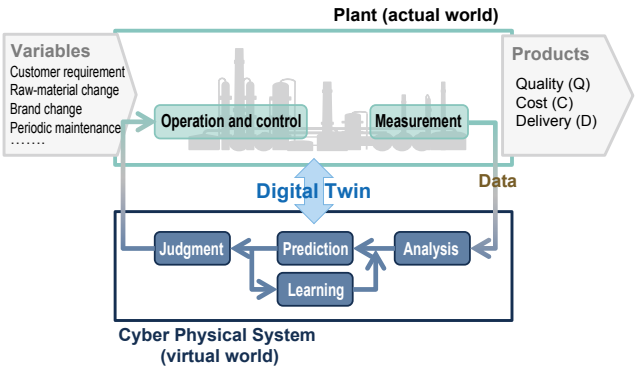

Figure 1 Improving operation by using Cyber Physical System

Information system technology (IT) should not be applied as it is to the security of control systems for plants. Control systems (operational technology: OT) in production sites have different features from IT. Table 1 compares the security of IT and OT.

*1 Incubation Department, Innovation Center, Marketing Headquarters

Table 1 Comparison of information system and control system

Security item	Information system (IT)	Control system (OT)
Priority	Confidentiality: Preventing data leakage	Availability: Continuing production
Possible results of incidents	Monetary loss, privacy abuse	Loss of human life, serious social damage
Target	Information	Facilities, instruments, products
Priority in measures against evolution of attacks	Speed: Defense technology quickly becomes obsolete	Integrity: Facilities and instruments operate for a long time
Operation period of the system	Less than five years	20 years or more
Distribution of security patches	At any time, periodical	During regular maintenance, irregular

Availability is crucial in plants that output raw materials and energy because operations must not be affected by a plant shutdown. Defense technology for IT rapidly become obsolete, and yet since these plants typically last for 20 years or more, security measures for OT must be effective and robust for a long time.

This paper explains physically isolated information security (PIIS), the optimum security concept for control systems, and introduces MemWiper as a security measure that embodies this concept for portable USB devices.

THREE-LAYER MODEL OF CONTROL SYSTEMS AND SECURITY MEASURES

The three-layer model is a typical configuration of control systems (Figure 2). This model consists of three network layers: the field network, control network, and control information network. This system is connected with external networks via a router on the control information network.

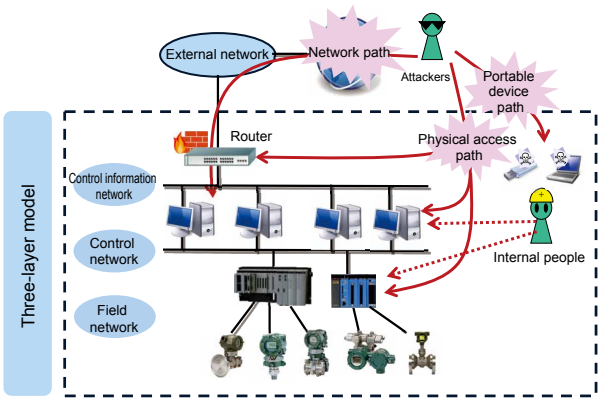

Figure 2 Three-layer model of a control system and major attack routes

Attackers try to invade the control system through three paths: networks, portable devices, and physical access. The network path is a route through which attackers try to invade via an external network into the control system. This path does not exist in control systems that are not connected with an external network. The portable device path is a route through which attackers try to invade the control system via devices that are carried in from the outside and connected to the control system, such as USB memory devices and PCs. The physical access pass is a route through which attackers try to invade the control system by trespassing on the premises of the control system.

Information security measures are used for the network path and portable device path. These include network security measures and end-point security measures. Physical security measures are used for the physical access path (Figure 3).

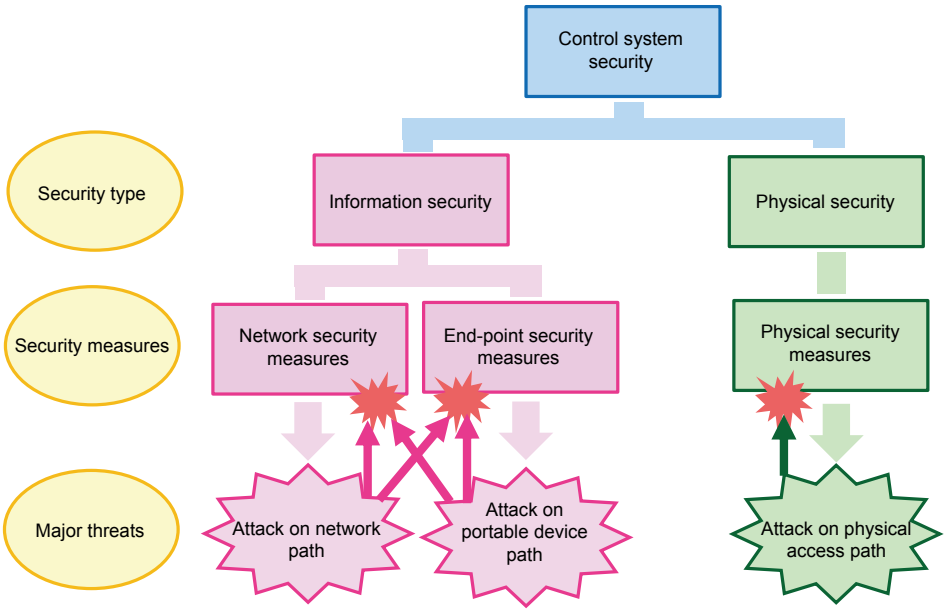

Figure 3 Security threats and corresponding security measures

As network security measures, instruments are installed in the networks to be protected (such as control information networks) in order to detect and restrict data transmission manipulated by attackers. These instruments include firewalls, intrusion detection systems (IDS), and intrusion protection systems (IPS). As end-point security measures, software is installed in the instruments to be protected (such as PCs) in order to detect and fend off access from attackers. These measures include anti-virus software, host-based firewalls, and white-listing. Physical security measures detect and prevent physical invasion by attackers. These include access control, locking, and physical invasion detection.

In addition to these measures, security policies are drawn up and human security measures (assigning persons in charge of security, providing security training, etc.) are taken as management measures.

PROBLEMS IN CURRENT SECURITY MEASURES

Nevertheless, information security measures (network security measures and end-point security measures) may be overridden by remote attacks [3].

These attacks target:

(1) Vulnerabilities in information security measures

When any security hole is found in software and firmware that are used for information security measures (such as anti-virus software in PCs and firmware for firewalls), information security measures may be overridden by remote attacks targeting this vulnerability.

(2) Vulnerabilities in management interface

When any security hole is found in the management interface, configuration file, or update file of an information security measure, or when the authentication information of a management interface is divulged, the information security measure may be overridden by remote attacks targeting this vulnerability.

(3) Vulnerabilities in related software

Even when no security hole is identified in an information security measure, if any security hole is found in the operating system, library, or communications protocol that are used with the information security measure, the measure may be overridden by remote attacks targeting this vulnerability.

To reduce the risk of remote attacks that exploit these vulnerabilities, enhanced security measures are taken. These include multi-layered defense and quick application of patches.

In multi-layered defense, multiple kinds of security measures are taken in multiple layers. Although this is expected to reduce the risk of attack, it increases the number of system components and thus adds overhead costs as well as other vulnerability factors.

In quick application of patches, patches that correct vulnerabilities are applied as quickly as possible. Although this is expected to improve the resistance to attacks on known security holes, it is not effective for zero-day attacks that exploit unknown security holes. Furthermore, it may be necessary to suspend the system to apply patches, so this measure is difficult to implement in systems in which availability is prioritized.

Although current security measures protect systems from remote attacks via network paths and portable device paths, such measures can also be targeted by remote attacks.

Air-gapping physically isolates the system from external networks. Although this is a powerful measure that blocks paths for remote attacks, it sacrifices the convenience of network connection. The IoT brings both the advantages of network connection and the risk of remote attacks; there is an urgent need to develop security measures best suited for the IoT era.

PIIS: A NEW SECURITY CONCEPT FOR CONTROL SYSTEMS

Conventional information security measures can be overridden by remote attacks. To solve this problem, we propose a concept of physically isolating the management interface of security measures from remote attackers (physically isolated information security: PIIS)[4]. PIIS protects control systems by using PIIS measures that are structured so they cannot be manipulated and monitored by remote attackers.

PIIS measures use the following approaches.

(1) Isolating software

To protect against attacks on software and firmware used as security measures, it is necessary to protect these software and settings from being changed by remote attackers. To do this, the system is structured so that physical access to the target instrument is needed in order to change the software or security settings of a security measure (for example, an electric switch that enables and disables rewriting of firmware).

(2) Isolating the management interface

To protect against attacks on the management interface used as a security measure, it is necessary to protect these software and settings from being changed by remote attackers. To do this, an interface structure is provided that requires physical access to the target instrument in order to change the software or settings of a security measure (for example, an interface with an electric switch that controls the power source of the wireless LAN adapter to enable or disable wireless LAN).

(3) Using a physical mechanism

To protect against remote attacks, security measures are designed to be set and operated by a combination of physical mechanisms and operations that cannot be operated by software (for example, a physical cover in front of the camera to enable and disable a built-in PC camera).

With these approaches, physical access is necessary to change PIIS software or settings, making it robust against remote attacks. PIIS measures are applied to network paths and portable device paths, which are targets of remote attacks, to make use of paths with low risk (physical attack paths)

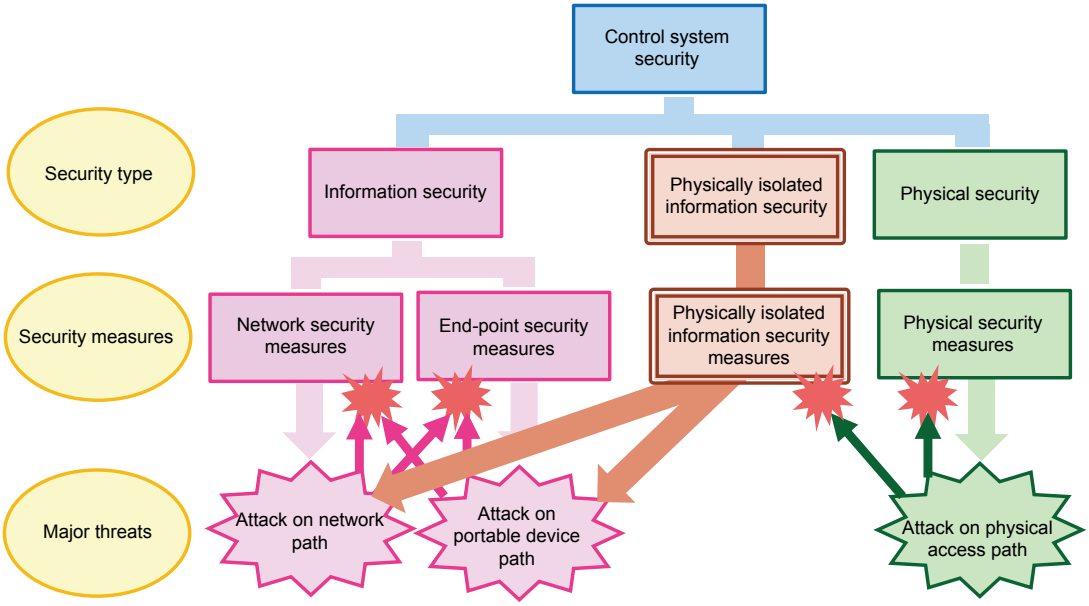

Figure 4 Classification of security measures and PIIS

to protect against paths with high risk (network paths and portable device paths) (Figure 4).

By incorporating the PIIS concept into the design phase of the product, system, service, and operation of a control system, the problem of protecting the information security of a control system can be handled as a physical security issue, which is easy to tackle.

By implementing PIIS measures in paths that are easily attacked from the outside, a robust control system against remote attacks can be built, securing the safety of connected systems in the IoT era.

MEMWIPER: AN EMBODIMENT OF PIIS

Background and Outline of MemWiper

As a simple implementation of PIIS, Yokogawa has developed MemWiper, a prototype device to erase the memory of USB devices. During the operation of control systems, it is necessary to take out daily reports and other files from the system PC, for which USB devices are convenient. However, if the USB device is infected, connecting it to a system PC could allow computer viruses and other malware to spread throughout the system.

Antivirus software is used to prevent USB devices infecting PCs with viruses. However, antivirus software can only detect and remove known viruses; it cannot eliminate the risk of infection with unknown viruses. Therefore, in systems where virus infection must never happen, the use of USB devices is prohibited, and recordable optical media such as CD-R are used instead. Although such media effectively eliminate the risk of virus infection, they are less convenient and take longer to take out files than USB devices.

To take out data safely with USB devices, Yokogawa has developed MemWiper (Figure 5), a prototype device based on the PIIS concept. MemWiper is a small device that is placed between a USB device and a PC. It erases the memory of the USB device and then allows it to connect with the PC, eliminating the risk of it infecting the PC (Figure 6).

Figure 5 External view of MemWiper USB memory device eraser

Operation of MemWiper

MemWiper is easy to use. Simply pushing a button erases the memory of the USB device and allows it to access the PC. The detailed procedure is described below.

(1) Connection

Insert a USB device into the USB port of MemWiper, and then insert the USB plug of MemWiper into a USB port of a PC.

The PC supplies power to MemWiper, and the USB switch IC in MemWiper connects the USB memory device to the eraser microcomputer in MemWiper. The eraser microcomputer checks the USB memory device. If it is normal, the status lamp blinks and MemWiper waits for the erase button to be pressed.

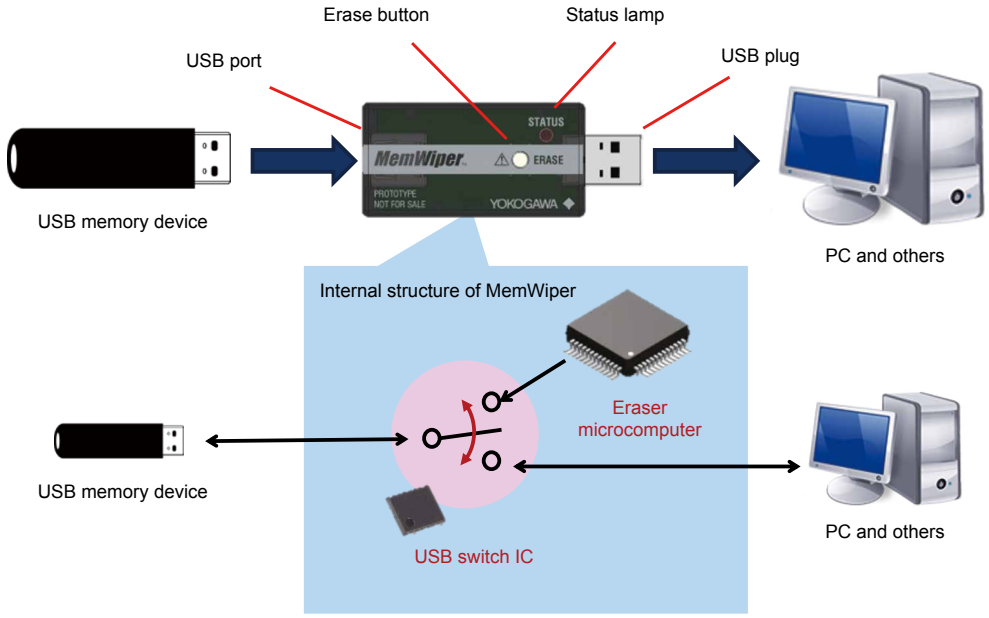

Figure 6 Internal structure and usage of MemWiper

(2) Operation of the Erase Button

When the erase button is pressed, the eraser microcomputer erases the contents of the USB device. After confirming that the memory is erased, the eraser microcomputer connects the USB device to the PC via the USB switch IC, and then turns on the status lamp. The PC detects the connection and recognizes the USB device as an unformatted device.

(3) Formatting operation

Users can format the USB device on the PC.

The Windows OS includes a formatting tool as standard, which is automatically activated. The USB device will be formatted in a few seconds, after which users can write files to this USB device in the same way as regular USB devices.

(4) Copying files

Users can use the PC to copy the required files to the USB device.

(5) Removing the USB

Take the necessary steps to safely remove hardware (the USB device) from the PC. When the status lamp of MemWiper turns off, MemWiper can be safely removed from the PC.

Remove MemWiper from the PC, and then remove the USB device from MemWiper.

MemWiper and PIIS

Based on the PIIS concept, MemWiper is designed as follows.

(1) The software of MemWiper is installed as firmware in the built-in microcomputer. It cannot be read or modified from the outside, making it difficult to attack the software remotely.

(2) The operation of MemWiper is managed by physical connection and the erase button, making it difficult to operate MemWiper remotely.

(3) MemWiper is independent hardware and cannot be operated from the PC to be connected, making it difficult to attack MemWiper via such PCs.

These physical access-oriented measures make remote attacks on MemWiper impractical, and so MemWiper avoids the information security problems of virus infection.

Feedback from Customers

Users and security personnel of control systems have commented on MemWiper (prototype) as follows:

- It is easy to operate.
- Its operation is straightforward, and will help improve security.
- We will ask external workers to use MemWiper.
- We will distribute MemWiper to all employees and encourage them to use it; it will improve security awareness in the workplace.
- MemWiper is attractive because it will be effective against new types of attack that emerge.

These comments indicate that MemWiper, an embodiment of PIIS, is a promising solution for control system security.

CONCLUSION

To securely enjoy the convenience of IoT connectivity, it is indispensable to take security measures against the risks of connectivity.

An IT connection exposes security measures to the risk of remote attacks. Existing security measures have a management interface and update system, which may be targeted by remote attacks, and security measures may become new risk factors.

To ensure the safety of connected systems, security measures that are more resistant to remote attacks need to be developed.

This paper introduced the PIIS concept as a security measure in the IoT era. PIIS measures are designed to protect against remote attackers, and can protect connected systems from remote attacks.

As an example of a PIIS measure, we developed MemWiper, a USB memory device eraser, which is designed so that it cannot be attacked remotely. This device allows users to safely take out files from a PC using USB memory devices.

MemWiper is currently being evaluated for commercialization. We are planning to distribute prototypes to customers in a wide range of fields, and hope they will evaluate them in various situations. We welcome inquiries about this device.

We will develop and provide inexpensive, effective products and services based on the PIIS concept, ensure safety in the IoT era, and help customers improve their operational efficiency by actively using data.

REFERENCES

(1) Makoto Nakaya, "The Introduction of a Cyber-physical System to Plant Operation and its Future," Separation Process Engineering, Vol. 48, No. 2, 2018, pp. 1-6 (in Japanese)
(2) Makoto Nakaya, "Use of IoT and ICT in Manufacturing Processes," (Chapter 2.5 of "Operation Transformation by Prediction Technologies of Mirror Plant"), Technical Information Institute (in Japanese)
(3) Feng Xue, "Attacking Antivirus," Black Hat 2008, http://www.blackhat.com/presentations/bh-europe-08/Feng-Xue/Whitepaper/bh-eu-08-xue-WP.pdf
(4) Takayuki Arai, "Concept of Physically Isolated Information Security and its Tools," Keiso, Vol. 61, No. 6, 2018, pp. 40-43 (in Japanese)