Featured Articles II

Control Security

Security Solutions that Protect the Life Cycle of Control Systems

Satoshi Okubo
Kohei Yamaguchi
Tetsuaki Nakamikawa, P.E.Jp
Hiroki Uchiyama, Ph.D.

OVERVIEW: As the control systems used in social infrastructure become more general-purpose and connected to a greater range of networks, security problems are continually being found. However, since long-term stable operation is a priority for control systems, it is not easy to use security measures such as security patches. So, there is a need for security management that monitors for vulnerabilities and provides early detection and handling of attacks that target vulnerabilities. To respond to this need, Hitachi is ensuring the safety and security of social infrastructure by creating security solutions that help reduce the workload needed for control system security management and ensure security across the entire control system life cycle.

INTRODUCTION

SOCIAL infrastructure systems (such as power, railways, gas, and water), and vehicle control systems have conventionally been considered immune from cyber-attacks since they use their own operating systems and protocols, and are installed in environments that are not accessible from the Internet or other external networks. However, the use of general-purpose operating systems such as Windows*1 and Linux*2, and general-purpose protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) has recently been on the rise as a cost-cutting measure. Connections to information systems such as production control systems have also become increasingly common as a way of improving efficiency, resulting in control systems (for which security was previously not a concern) requiring the same security measures as information systems.

Control systems have different requirements from typical information systems, namely availability and long-term maintainability. These different requirements make it difficult to apply security technology and products designed for information systems to control systems as-is. For example, when a vulnerability or other security problem is discovered in a control system, it is not easy to use patches or other security measures that might have unknown effects on the system's operation. Installing security products can also change the system configuration after restarting, resulting in known vulnerabilities becoming actualized or new vulnerabilities being discovered, thereby preventing complete handling of the problem.

A certification system has been created for security management of information systems, in the form of information security management systems (ISMSs) defined by the ISO/IEC 27001 standard(1). The aim of an ISMS is to protect information resources (client information and confidential information). It calls for tasks such as security risk analysis, risk handling (preventive measures), creation of an operation organization/system, and creation of procedures for responding to incidents (detection measures, response measures). The organization also needs to create a security life cycle loop (review current situation → prevent → detect → respond). In the future, this type of security management will likely be needed not just for information systems, but also for control systems.

This article discusses the need for control system security management to ensure the safety and security of social infrastructure systems, Hitachi's security management concept, and solutions for assisting it.

*1 Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.
*2 Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

TABLE 1. Differences between an ISMS and a CSMS
The differences between the requirements of an ISMS and a CSMS are listed below.

Difference	ISMS	CSMS
Protected assets	Information assets	Information assets, personal/physical assets, operation (IACS)
Anticipated threats	Damage to CIA of protected assets	Damage to CIA of protected assets, as well as damage to HSE
Protected life cycle	Mainly operations	All areas of system life cycle

ISMS: information security management system
CSMS: cyber security management system
CIA: confidentiality, integrity, availability
IACS: industrial automation and control systems
HSE: health, safety, environment

NEED FOR CONTROL SYSTEM SECURITY MANAGEMENT

As control system security management becomes increasingly important, its requirements are being set forth in security standards for control systems, and in guidelines created by governments. This chapter looks at some of the developments taking place in this area.

Security Standards

IEC 62443[(2)] has been created as a security standard for general-purpose control systems. The standard consists of 13 standard groups that specify requirements for businesses, for system integrators, and for component vendors. Among these standard groups, IEC 62443-2-1[(3)] defines cyber security management systems (CSMSs). Table 1 shows the differences between an ISMS and a CSMS. As with ISMSs, the world's first certification system for CSMSs was created in 2014[(4)], and certification by social infrastructure providers may increase in the future.

Government Guidelines

Japan's Ministry of Economy, Trade and Industry (METI) has teamed up with Information-technology Promotion Agency, Japan (IPA) to create cybersecurity guidelines for the chief executives of information technology (IT) system or service providers, or of companies that depend on IT for their corporate strategy[(5)]. The guidelines list the following four items as key management items:
(1) Demonstrating leadership, organization-building
(2) Setting a framework for cybersecurity risk management
(3) Attack-prevention measures that understand the risks
(4) Preparations in readiness for cyber-attacks

The creation of control system standards and guidelines in Japan and abroad reflects how IT-dependent social infrastructure providers need to implement security management over the long term.

CONTROL SYSTEM SECURITY MANAGEMENT CONCEPT

Social Infrastructure Security Concept

A number of security requirements are needed to protect social infrastructure from threats such as natural disasters, cyber-attacks and terrorism. Hitachi has distilled these requirements into four properties–hardening, adaptive, responsive and cooperative. They form the basis of Hitachi's system security concept[(6)].
(1) Hardening: Acquiring the defensive ability to withstand the attack skills of attackers
(2) Adaptive: Continually improving preventive/defensive measures against new threats
(3) Responsive: Improving after-the-fact handling ability to minimize damage and recovery time after an attack has occurred
(4) Cooperative: Different organizations or businesses working together with a common understanding of the situation

Approach to Control System Security Management

Hitachi applies its system security concept to implement control system security management by continually improving responses to new threats through the plan, do, check, act (PDCA) cycle (see Fig. 1).
(1) Identify new threats

New threats that need to be investigated due to events such as system configuration changes are uncovered, and their effects on the system to be protected are identified by means such as risk analysis.
(2) Propose improvement methods

The risk analysis results from (1) are used to investigate improvement methods for the anticipated risks.
(3) Set implementation plan

A plan for implementing the improvement methods investigated in (2) is set.
(4) Implement security measures

The security measures set in (3) are implemented.

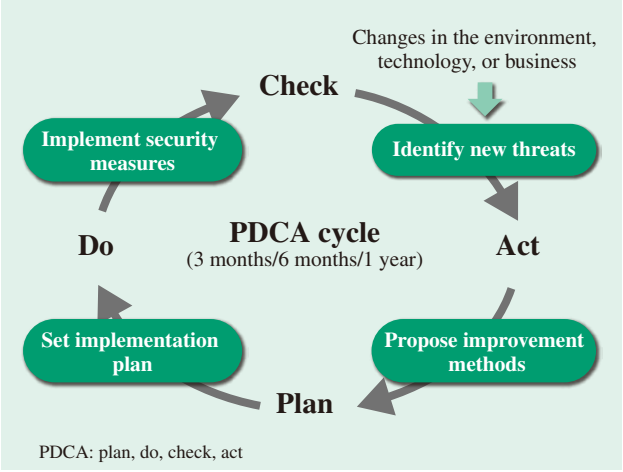

Fig. 1—Measures Driven by Security Operation Management PDCA.
Responses to new threats are continually improved through the PDCA cycle.

CONTROL SECURITY SOLUTIONS ASSISTING SECURITY MANAGEMENT

To provide security measures for a control system, the system must first be divided into zones according to the security level required by each zone, and then security measures must be provided for each zone's portal and the communication channels linking the zones.

Hitachi's control system security measures draw on the system security concept to propose two solutions: (1) Assist in preventing unauthorized cyber access, and (2) Assist in preventing unauthorized system operation (see Fig. 2).

Assist in Preventing Unauthorized Cyber Access

Assisting in preventing unauthorized cyber access is a solution that prevents unauthorized access via cyberspace at the portal of each zone (hardening), and prevents the spread of security problems after unauthorized access has been detected (responsive).

Devices that prevent unauthorized access block unauthorized data packets that do not match a predefined whitelist. Installing these devices at the portals of the control system to be protected enables prevention of unauthorized control system access. Hitachi has a tool that can generate the whitelist previously mentioned by using an access log during system trial operation. These benefits make it easy to install the solution in a control system. If a security problem (such as malware infiltration) occurs in another system connected to the control system, devices that prevent unauthorized access can prevent the problem from spreading to the control system by blocking communication data packets from the other system.

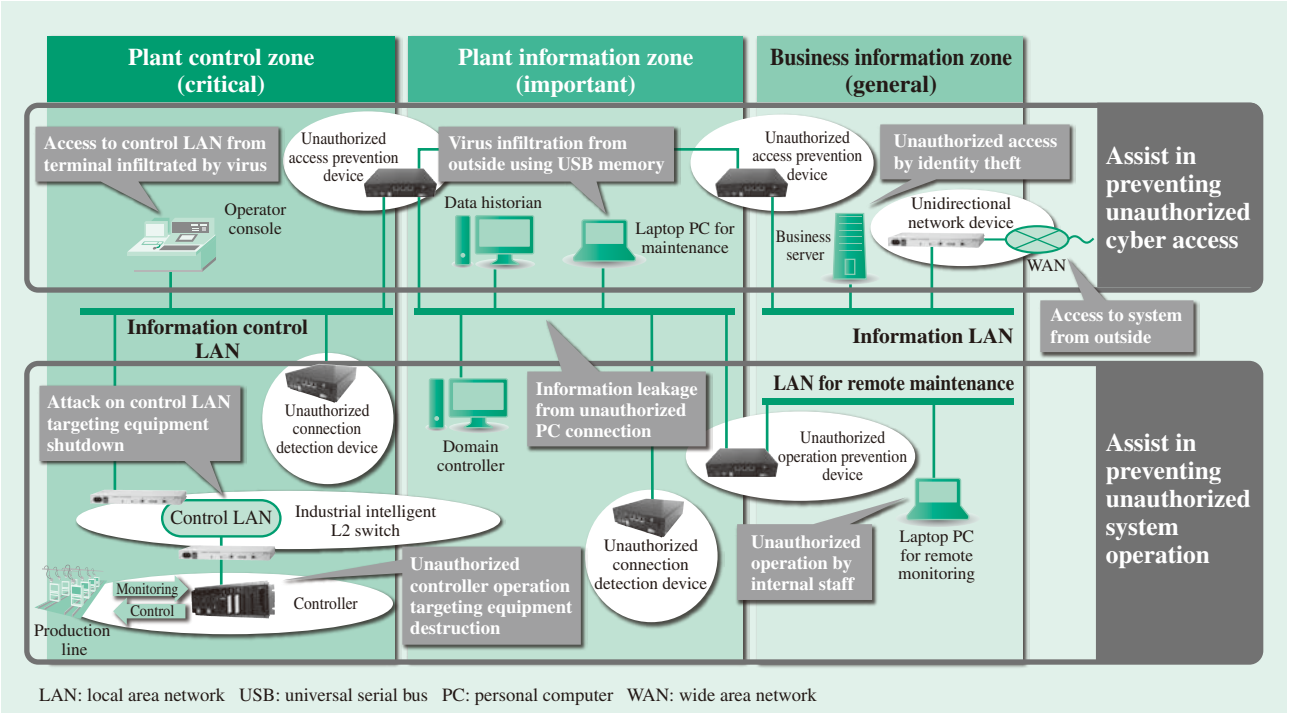

Fig. 2—Control System Security Solutions.
Two control system security solutions are provided by combining a wide range of security products for control systems.

Fig. 3—Unidirectional Network Device.
This device's software-free implementation reduces the risk of configuration errors and reduces the workload during operation.

Fig. 4—Unauthorized Connection Detection Device.
This device prevents the threat of cyber-attacks by detecting and automatically eliminating network connection attempts by unregistered devices.

In addition, Hitachi's unidirectional network device provides a software-free data diode function (a function that permits communication in one direction only, like a diode) so that when transmitting information from a core system to the outside world, unauthorized access from the outside world can be physically blocked, protecting the core system. It also reduces the workload during operation by providing benefits such as not needing software upgrades and an extended life (see Fig. 3).

Assist in Preventing Unauthorized System Operation

In the future, control systems are expected to have various Internet of Things (IoT) devices connected to them via networks. Installing a wireless network at a manufacturing site increases the chance of an unauthorized device (such as an IoT device the administrator is unaware of, or an employee's personal terminal) being connected to a control system, creating new risks of malware infiltration or information leakage. Assistance in preventing unauthorized system operation is provided by solutions that defend control systems from threats caused by this type of unauthorized device connection within the system (hardening), and detect and eliminate unauthorized operations on authorized devices such as malware infiltration (responsive).

Hitachi's unauthorized connection detection device has a function that detects when a non-preregistered device has connected to the network, and excludes it from the network. It can also support connections via wireless networks, preventing unauthorized devices from connecting to control systems (see Fig. 4).

Measures for handling the targeted attacks that have recently been on the rise must assume that it is difficult to completely prevent unauthorized access to systems, such as infiltration by malware that is not perceived as a cyber-attack, and not handled by antivirus software. To detect cyber-attacks, behavior detection products with a proven track record for information systems can be used in coordination with the aforementioned unauthorized connection detection device to detect devices that perform unauthorized operations, and eliminate them from the network.

In addition, measures of increasing robustness against cyber-attacks are also used to minimize the effects of cyber-attacks that manage to penetrate network defenses.

Hitachi has developed a controller that is certified under the Embedded Device Security Assurance (EDSA) certification system for security assurance of control components administered by the International Society of Automation (ISA) Security Compliance Institute (ISCI), and provides increased resistance to cyber-attacks (see Fig. 5).

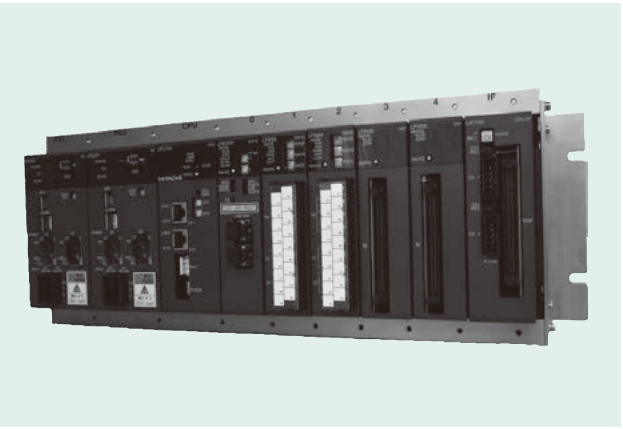

Fig. 5—Controller with EDSA Certification.
The controller demonstrates resistance to cyber-attacks by satisfying preset security requirements.

CONCLUSIONS

This article has examined the need for control system security management that reflects the developments taking place in Japan and abroad, and has presented Hitachi's security concept and the solutions used to support it.

With the use of the latest IT and coordination with information systems and IoT devices, control systems are expected to continue growing as platforms that support social infrastructure. The risk of cyber-attacks is expected to grow as well. To help ensure safe and secure social infrastructure systems, Hitachi will continue to develop control security technologies and provide high added-value solutions.

REFERENCES

(1) JIPDEC, ISMS Conformity Assessment Scheme, http://www.isms.jipdec.or.jp/english/isms.html
(2) International Electrotechnical Commission (IEC), IEC TS 62443-1-1, "Terminology, Concepts and Models," (Jul. 2009).
(3) International Electrotechnical Commission (IEC), IEC 62443-2-1, "Establishing an Industrial Automation and Control System Security Program," (Nov. 2010).
(4) JIPDEC, CSMS Conformity Assessment Scheme, http://www.isms.jipdec.or.jp/csms.html in Japanese.
(5) Ministry of Economy, Trade and Industry, "Cybersecurity Management Guidelines Version 1.0," in Japanese.
(6) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).

ABOUT THE AUTHORS

Satoshi Okubo
Control System Platform Security Center, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of security components for industrial control systems.

Kohei Yamaguchi
Control System Platform Security Center, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of security components for industrial control systems.

Tetsuaki Nakamikawa, P.E.Jp
Control System Platform Development Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of control system components. Mr. Nakamikawa is a member of the Information Processing Society of Japan (IPSJ).

Hiroki Uchiyama, Ph.D.
Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of security technology for control systems. Dr. Uchiyama is a member of The Institute of Electrical Engineers of Japan (IEEJ) and the IPSJ.