Featured Articles

Control System Security for Social Infrastructure

Toshihiko Nakano, Ph.D.
Katsuhito Shimizu
Tsutomu Yamada
Tadashi Kaji, Dr. Info.

OVERVIEW: The wider use of networking in social infrastructure in recent years has exposed their control systems to greater security risks. In response, ongoing work is being done by international standards bodies and other industry associations on determining security requirements for control systems. Along with taking note of trends in cyber-attacks and social infrastructure requirements such as long operating life, Hitachi supplies solutions and products for satisfying these requirements. Hitachi has also been coordinating measures for improving the security of control systems through its participation in the Control System Security Center, a collaboration between industry, government, and academia set up for this purpose, since it was first established.

INTRODUCTION

THE threat of cyber-attack is a consequence of greater use being made of networks in social infrastructure over recent years. This makes it essential for social infrastructure systems also to adopt security measures against a broad range of cyber-attacks.

As these security measures need to be implemented in ways that do not leave any gaps, but also that do not impose an excessive overhead, ongoing study being undertaken at international standards bodies includes both security requirements and the criteria to consider in security assessments. The International Electrotechnical Commission (IEC), for example, in its IEC 62443 security standard for control systems[(1)], has stipulated security requirements, the requirements for analyzing impacts on health, safety, and the environment (HSE), and security assurance levels (SALs) for assessing the strength of security measures. The International Telecommunication Union (ITU), meanwhile, is working on the development and standardization of its Cybersecurity Indicator[(2)] and Global Cybersecurity Index[(3)] assessment criteria. Elsewhere, the European Telecommunications Standards Institute (ETSI) is also developing assessment criteria called Information Security Indicators[(4)].

These assessment criteria tend to provide an assessment or numerical indicator for the strength of security measures as they exist at a particular time (usually the design stage). However, a key prerequisite for the control systems used in social infrastructure is that they remain in operation over a long period of time. Because of this long timescale, social infrastructure tends to contain a mix of different types of system. Also, rapid advances in the technology of cyber-attacks mean that it is not uncommon for previously unanticipated attacks to become suddenly commonplace.

Given this background, security measures implemented in social infrastructure systems at the design stage cannot be assumed to provide adequate security, and therefore it is necessary to ensure that measures can be upgraded as required over the long operating life of social infrastructure in response to advances in the technology of cyber-attacks. Taking note of developments in cyber-attacks and the long operating life and other characteristics of social infrastructure, Hitachi has identified three new security requirements for social infrastructure, namely that security measures be adaptive, responsive, and cooperative.

This article describes the levels of security required in social infrastructure; strategies for achieving these levels of security; work on implementing measures at the system and component level; the activities of the Control System Security Center (CSSC), which was set up to ensure the security of control systems; and the work being done by Hitachi.

LEVELS OF SECURITY REQUIRED IN SOCIAL INFRASTRUCTURE

This section looks at the security levels defined in IEC 62443. It also describes the requirements identified by Hitachi for security measures to be adaptive, responsive, and cooperative, and the level required in each case, defining the required levels.

(1) Required level of security

IEC 62443 defines the SAL criteria for assessing the strength of security measures (see Table 1).

Looking at current trends in attacks against social infrastructure systems, it is clear that these systems are the subject of systematic attacks with a high level of malicious intent. This means they require level 3 or 4 security measures.

(2) Required level of adaptability

Adaptability defines the flexibility of measures for responding to a diverse range of attacks.

The requirement in the past has been to incorporate security measures that can deal with the types of attack anticipated at the design stage. However, factors such as the evolution of attack methods mean that new forms of attack will continue to appear. Accordingly, the ability to respond to types of attack not anticipated at the design stage has also become necessary.

Table 2 lists the levels used to represent the extent to which this adaptability requirement is satisfied.

Because control systems used in social infrastructure will very likely face types of attack not anticipated at the design stage, they require a higher level of adaptability than information and other systems. This means that their security measures need to achieve level 3, and they also require organizational initiatives aimed at upgrading this to level 4 in the future.

(3) Required level of responsiveness

Responsiveness defines how quickly a response can be mounted to an attack.

Whereas the emphasis in the past was on security measures for preventing attacks, what is needed to deal with the sophisticated attacks of recent times is the ability to quickly detect when such an attack has taken place and to instigate effective countermeasures.

Table 3 lists the levels for this responsiveness requirement.

As control systems used for social infrastructure need to deliver services continuously, they must respond quickly when a security attack occurs. This means they need to satisfy the level 3 requirement for responsiveness, whereby they can respond to an attack without interrupting service delivery. To deal with relentlessly evolving attacks, they also require organizational initiatives aimed at upgrading to level 4 in the future.

(4) Required level of cooperativeness

Cooperativeness defines the degree to which security measures are influenced by other systems with which they coexist.

Table 1. Security Levels

These levels indicate the strength of security measures as they exist at a given point in time.

Level	Description
1	Protection against casual or coincidental violation
2	Protection against intentional violation using simple means
3	Protection against intentional violation using sophisticated means
4	Protection against intentional violation using sophisticated means with extended resources

Table 2. Adaptability Levels

These levels indicate how flexibly countermeasures can cope with a diverse variety of threats.

Level	Description
1	No measures for dealing with security threats
2	Measures in place for dealing with security threats identified during the design stage
3	Measures in place for dealing with new security threats
4	Establishment of management systems for dealing with new threats

Table 3. Responsiveness Levels

These levels indicate how quickly a response can be mounted when a threat occurs.

Level	Description
1	No measures for detecting threats
2	Measures in place for detecting threats
3	Measures in place for countermeasures after threat occurs
4	Establishment of management systems covering time from threat occurring to countermeasures being implemented

Table 4. Cooperativeness Levels

These levels indicate the influence of other interdependent systems.

Level	Description
1	No measures for preventing negative influences
2	Measures in place for preventing negative influences
3	Measures in place for taking advantage of positive influences
4	Establishment of management systems for ongoing assessment of influences of one system on another

These influences can be both positive (such as the sharing of threat information to allow the detection of previously unknown threats) and negative (such as an attack from another system that has been infected by malware).

Levels are defined representing the extent to which this cooperativeness requirement is satisfied (see Table 4).

Because social infrastructure systems have a long operating life, they coexist with a wide variety of other systems, not all of which will have the same level of security measures. In such a situation, use of level 2

security measures that maintain system-wide security is required to prevent attacks against the weakest parts.

STRATEGIES FOR ACHIEVING CONTROL SYSTEM SECURITY

Hitachi has been in the practice of using a "2 × 3 security implementation model" to model its approach to maintaining security throughout the lifecycle of social infrastructure systems[5]. This model is based on the idea of achieving the ongoing provision of all-encompassing security by dealing with threats across two different lifecycle phases (development and operation), and in terms of three different perspectives (functions, environment, and organization and people) (see Fig. 1).

In terms of the security requirements, this seeks to utilize security measures in the development phase to satisfy both the required level of security and the adaptability requirement, and to establish a plan, do, check, and act (PDCA) cycle for security during the operational phase to satisfy the responsiveness and cooperativeness requirements. In particular, the development process needs to take account of operational phase considerations if a system is to be provided with level 3 or higher responsiveness and level 2 or higher cooperativeness as this requires continuous monitoring of system security to detect security incidents, and the establishment of operational security infrastructure that can respond to any incidents that are detected without interrupting services.

SECURITY IMPLEMENTATION AT SYSTEM LEVEL

Based on the 2 × 3 security implementation model, this section describes development-phase security measures applicable to control system development, and also operational-phase security measures.

Development Phase

An important part of control system development is to assess potential security threats and determine which security measures to incorporate. Hitachi has established system implementation guidelines that specify the relevant procedures, and which utilize the security concepts advocated in IEC 62443. These guidelines are used to provide appropriate security

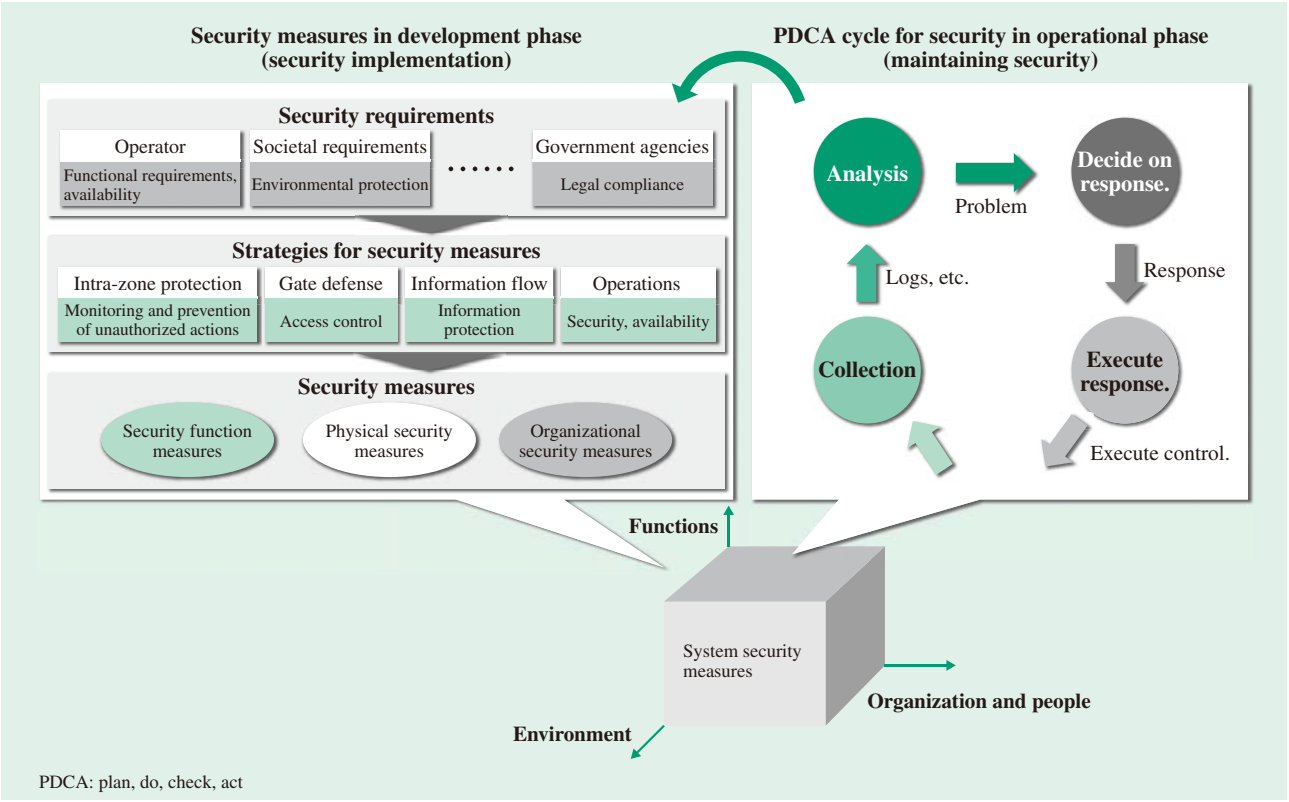

Fig. 1—2 × 3 Security Implementation Model.
This model provides all-encompassing security by dealing with threats across two different lifecycle phases (development and operation), and in terms of three different perspectives (functions, environment, and organization and people).

measures based on factors such as the importance of the system and its customer requirements.

Specifically, they cover the following procedures.

(1) Partitioning of the system into zones in which the same security policies apply based on a risk analysis of the system.

(2) Identification of "conduits" (interconnections) between zones.

(3) Formulation of security measures

(a) Measures for preventing unauthorized information entering a zone via a conduit (provision of conduit gates)

(b) Measures for preventing unauthorized operations within a zone

(i) Network measures

(ii) Device measures

The following section describes the security measures specified by these system implementation guidelines to satisfy the required levels (described above) in the case of the information and control zone (see Fig. 2).

(1) Security measures for conduit gates (measure 1)

The main purposes of security measures for conduit gates are to prevent unauthorized intrusions into the zone and leaks of information from the zone.

For a system to achieve security level 3 or 4, conduit gates must identify necessary communications and block unnecessary communications. Factors to consider when determining whether or not a communication is necessary include not only where the communication is being sent to or received from, but also its direction and content. To achieve level 3 adaptability, it must be possible to incorporate logic for determining such things as whether or not communication in necessary or whether it is suspicious. To achieve level 3 responsiveness, it is necessary to monitor communications continuously, and to allow the control system operator to decide how to respond when a suspicious communication is detected. Based on these considerations, the system is developed in accordance with the security policies for each zone.

(2) Security measures for preventing unauthorized actions within a zone: network (measure 2)

The main purposes of intra-zone network security measures are to prevent unauthorized users or malware that have entered the zone from accessing functions or information, and to detect unauthorized users.

To achieve security level 3 or 4, components within a zone must be identified and the connection of unnecessary components blocked. Hitachi supplies products for this purpose.

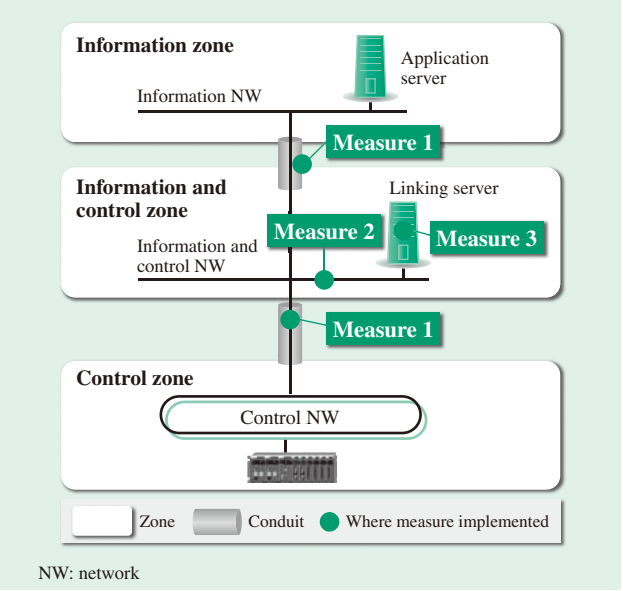

Fig. 2—Security Implementation Points for Control Systems. The control system is partitioned into zones and security measures implemented for the zone entry and exit points and for networks (information and control networks and components inside each zone).

Achieving level 4 responsiveness requires continuous monitoring within the zone and generation of an alarm to the security operation system whenever a suspicious action is detected. In a new approach to intra-zone monitoring, Hitachi has developed a solution that uses a decoy server. Located within the zone, the decoy server has deliberately downgraded security functions so that its becoming infected by malware will provide an early warning of any intrusion by malware into the zone.

(3) Security measures for preventing unauthorized actions within a zone: devices (measure 3)

The main purpose of security measures for control components within a zone is to prevent access to information or functions by any malware that has infected a device.

This requires functions for preventing operations by software other than that authorized for use in the control component, and the use of control components with enhanced security.

These security enhancements to control components are described later in this article.

Operational Phase

This section describes the security measures required for control systems during their operational phase, specifically measures for responding rapidly to security incidents, and formal security management

practices for dealing with risks such as the emergence of new threats.

(1) Measures for responding rapidly to security incidents

When a security problem is detected at a conduit gate, on an intra-zone network, or in a component within the zone, it is necessary to determine quickly whether the problem is the result of an actual security incident or simply a misdetection, and to respond accordingly. In addition to setting up a security operation center (SOC) for information systems, Hitachi has established an incident response team to build up its expertise in dealing with incidents. However, industry knowledge is also needed to determine whether a problem is due to an actual incident.

Hitachi has know-how in both incident response and business system implementation and operation, and is applying it in the development of security operation systems and services.

(2) Formal security management systems

Formal security management systems are essential if a control system is to achieve level 4 adaptability and responsiveness. Hitachi has focused in particular on cybersecurity management systems (CSMSs). CSMSs are intended to maintain ongoing security by having the operator of a control system undertake risk management for that system. For a system operator to maintain security, they need to collaborate with the system integrator and other product vendors. Hitachi has long strived to deliver highly reliable and secure control systems, and is also working on CSMSs.

INITIATIVES AT THE CONTROL COMPONENT LEVEL

To build secure control systems with level 3 or higher security, it is important that the components used in the system be able to operate safely and reliably. In addition to hardening control components (making them more secure) and strengthening security functions, Hitachi is also developing products for enhancing the security of control components that cannot implement their own security measures.

Hitachi is currently working toward Embedded Device Security Assurance (EDSA) certification[(6)], a certification system for the security assurance of control components that is administered by The International Society of Automation (ISA) Security Compliance Institute (ISCI). The certification process considers the following three criteria.

(1) Functional security assessment (FSA): This assesses the implementation of security functions

(2) Software development security assessment (SDSA): This covers each phase of software development

(3) Communication robustness testing (CRT)

INITIATIVES BY CSSC AND HITACHI

The CSSC was set up in March 2012 as a collaboration between industry, government, and academia with the aim of strengthening control system security. Its main objectives are the research and development of control system security technology, security auditing of control equipment, and the use of simulated plant to raise awareness and for personnel development. In the case of the security auditing of control equipment, CSSC is looking closely at EDSA certification, including joining ISCI as an associate member, and is working towards obtaining certification as an auditor.

Hitachi has been a member of CSSC since its establishment and is collaborating with the organization on joint research into measures for improving the security of control systems, the use of simulated plant for security training on control systems, and the security auditing of control equipment. As a member of CSSC, Hitachi intends to continue its active participation in the research and development of technology for enhancing control system security, and also other related measures.

CONCLUSIONS

This article has described the new security requirements for control systems used in social infrastructure systems, and the security technologies for satisfying these requirements.

Control system security measures have an important role in the protection of social infrastructure systems. To counter continually evolving threats, Hitachi intends to work with organizations such as the CSSC in Japan and overseas, as well as researching and developing the required technologies and supplying products that incorporate these technologies. Hitachi is also seeking to supply total services that extend from security risk analysis for control systems to system implementation and operational support. In doing so, Hitachi will contribute to the creation of secure social infrastructure that everyone can use with confidence.

REFERENCES

(1) IEC, "Industrial Network and System Security," IEC 62443 (2013).
(2) ITU-T, "A Cybersecurity Indicator of Risk to Enhance Confidence and Security in the Use of Telecommunication/ information and Communication Technologies," Recommendation ITU-T X.1208, 1204.
(3) ITU-D, "Global Cybersecurity Index," http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
(4) ETSI, "Information Security Indicators," http://www.etsi.org/images/files/ETSITechnologyLeaflets/InformationSecurityIndicators.pdf
(5) T. Kaji et al., "Cyber Security Technologies for Social Infrastructure Systems," Hitachi Review **62**, pp. 397–401 (Sep. 2013).
(6) ISCI, "Embedded Device Security Assurance (EDSA)," http://isasecure.org/ISASecure-Program.aspx

ABOUT THE AUTHORS

Toshihiko Nakano, Ph.D.
Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Katsuhito Shimizu
Control System Platform Design Department, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the design and development of servers and controllers for information and control systems.

Tsutomu Yamada
Department of Energy Management Systems Research, Hitachi Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of embedded computer architecture, network systems and cybersecurity for industrial control systems. He is a Professional Engineer, Japan (Information Engineering). Mr. Yamada is a member of the IEEE, the International Society of Automation (ISA), The Institute of Electronics, Information and Communication Engineers (IEICE), and The Society of Instrument and Control Engineers (SICE).

Tadashi Kaji, Dr. Info.
Infrastructure Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of information security technology. Dr. Kaji is a member of the IEEE Computer Society.