Featured Articles

# International Standardization Activities for Hitachi System Security Concept and Social Infrastructure Security Based on It

Toshihiko Nakano, Ph.D.
Hideki Tonooka
Masashi Sato
Tadashi Kaji, Ph.D.
Yoichi Nonaka, Ph.D.

*OVERVIEW: The networking of social infrastructure in recent years has led to greater security risks in the systems used in this infrastructure. In response to these increased risks, international standardization bodies and other industry organizations are working on formulating security requirements for systems. Hitachi uses the Hitachi system security concept as a basis for dealing with the requirements demanded of social infrastructure, which include responding to trends in cyber-attacks and long-term operation, and has been engaging in studies at the IEC. These requirements were presented in a whitepaper entitled "Factory of the future" that describes how factories will look in the future and the technology they will require, and are currently being adopted. In the future, advances in the IoT and elsewhere will make security even more important. Hitachi intends to supply security solutions to create secure social infrastructure that everyone can use with confidence.*

## INTRODUCTION

THE threat of cyber-attacks has become greater and more severe in recent years as social infrastructure has become increasingly networked. Accordingly, diverse security measures to protect against cyber-attacks have become essential for social infrastructure systems.

A major prerequisite for the control systems used in social infrastructure is that they continue operating for a long period of time, and they need to be able to handle a wide variety of system interoperation associated with the evolution of threats and advances such as the Internet of things (IoT) and be able to respond rapidly to any attacks that occur.

Taking note of trends in how to deal with cyber-attacks, the characteristics of social infrastructure such as long-term operation, etc., and developments in open innovation, Hitachi has expressed three new security requirements for social infrastructure systems, namely adaptivity, responsivity, and cooperativity, in the form of the Hitachi system security concept. These requirements were presented by the International Electrotechnical Commission (IEC)[1], an international standardization body, in a whitepaper entitled "Factory of the future"[2] that describes how factories will look in the future and the technology they will require (subjects of study at the IEC), and are currently being adopted.

This article presents an overview of security in social infrastructure systems followed by a description of the Hitachi system security concept[3] in which Hitachi has proposed security requirements for social infrastructure systems, and solutions for implementing this concept.

## DEVELOPMENTS IN SECURITY FOR SOCIAL INFRASTRUCTURE SYSTEMS

This section presents an overview of developments relating to the threats, system configurations, and countermeasures required when implementing security for social infrastructure systems (see Fig. 1).

Security threats are continually changing, and along with attacks such as zero day and multi-vector attacks, which have become more diverse in recent years, there are also cases of attacks based on conditions that differ from conventional assumptions, such as malicious activity by insiders. Furthermore, with regard to the prerequisite system configurations, progress is anticipated on the symbiotic autonomous decentralized systems proposed by Hitachi in which system interconnections transcend the boundaries of industries and businesses, such as the IoT, supply chain developments, and the analysis of plant data. For these reasons, it is difficult to accurately predict what

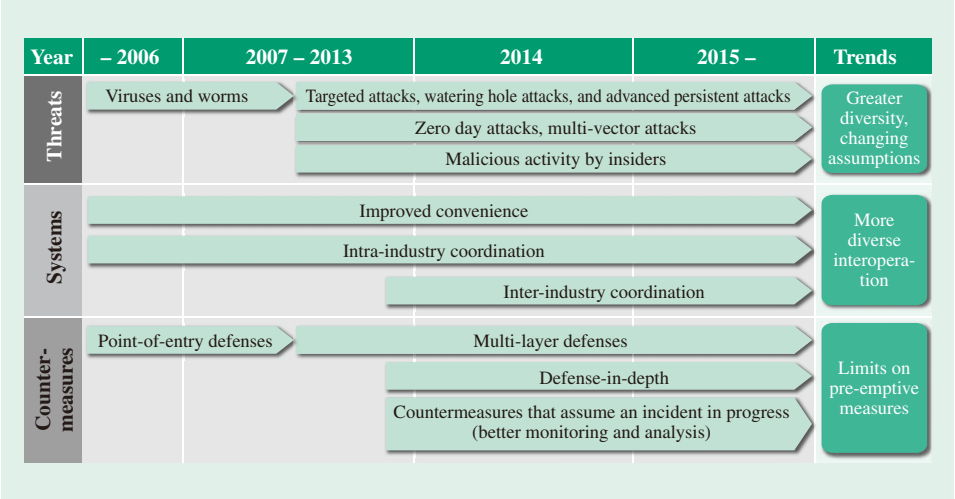


*Fig. 1—Security Developments. Along with security threats becoming more diverse in recent years, social infrastructure systems, too, are adopting various forms of interoperation. This means that countermeasure techniques also require a new approach.*

security threats will arise, making it hard to establish countermeasures in advance.

This means that, as a prerequisite, it is essential to have security measures that are based on threats and systems continually changing in these ways.

## HITACHI SYSTEM SECURITY CONCEPT

This section describes the Hitachi system security concept proposed by Hitachi (see Fig. 2).

A prerequisite for ensuring the security of a social infrastructure system is to ensure robustness (hardening) with respect to likely threats based on the target system's configuration. On top of this, Hitachi has proposed three new requirements for security: giving security measures the ability to adapt as needed to continually changing threats and system configurations (adaptivity), providing responses that will minimize the impact on the social infrastructure system if a security threat does materialize (responsivity), and having different organizations work together to ensure the early identification of security threats (cooperativity).

Recognizing that these three requirements play an important role in the implementation of social infrastructure or industrial systems and need to be adopted internationally, studies have been undertaken at the IEC, and they have been adopted in a whitepaper entitled "Factory of the future" that describes how factories will look in the future together with the technology required.

The details are described below.

(1) Hardening (see Fig. 3)

This refers to the primary measures used to protect the services and other functions of social infrastructure systems. However, providing complete security against continually changing threats is impractical. Instead,

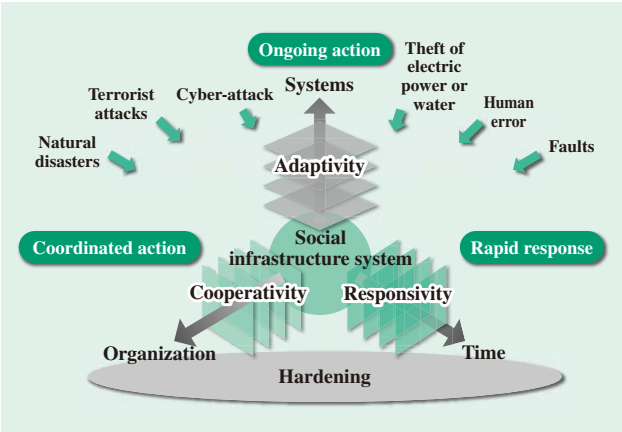


*Fig. 2—Hitachi System Security Concept. Hitachi has presented its views on the requirements for security in social infrastructure systems in the form of the Hitachi system security concept.*

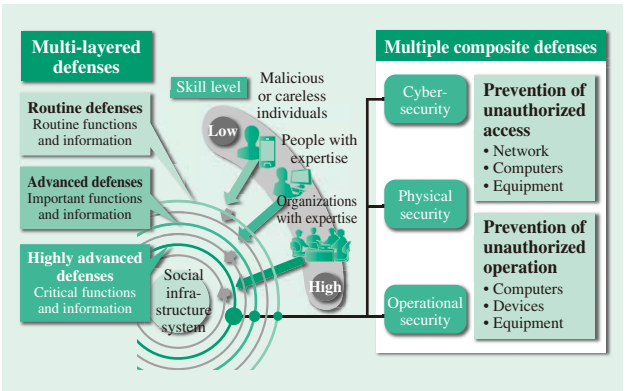


*Fig. 3—Ensuring Hardening. To harden systems against a variety of threats, it is important to implement multiple and multi-layered defenses.*

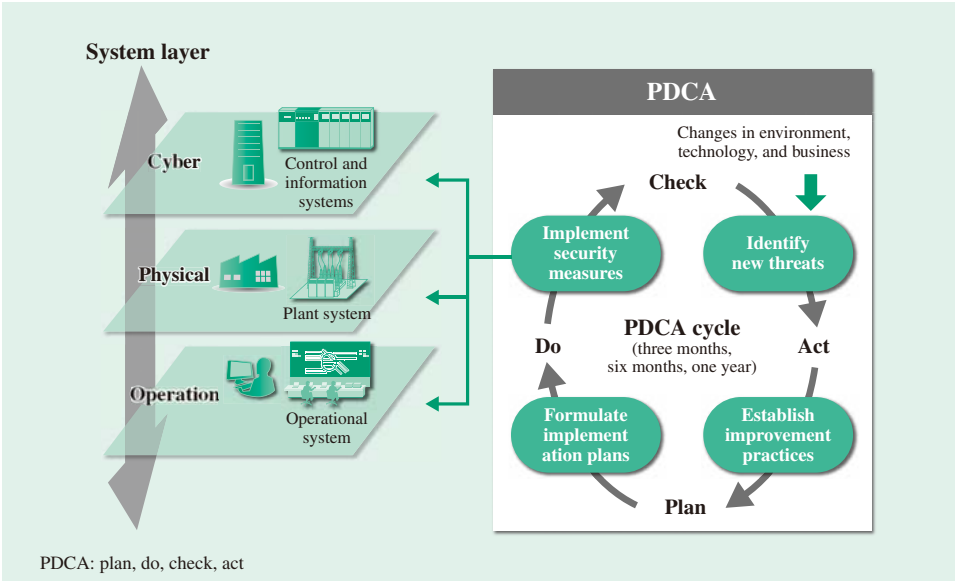


*Fig. 4—Ensuring Adaptivity. The PDCA process plays an important part in adapting quickly to changes in threats and technology.*

what is needed is a defense-in-depth approach with a good balance of physical, operational, and other measures. The adoption of defense-in-depth also involves reducing the risk of attacks on systems that provide important functions.

In addition to supplying security products focusing on control systems that provide reliable long-term operation, Hitachi also builds systems that comply with international and other industry standards and utilize business knowledge.

(2) Adaptivity (see Fig. 4)

Security threats are becoming more ingenious. System architectures, too, are continually changing, including the use of publically available technology through open innovation and interoperation between systems to create new businesses. This means that social infrastructure systems are continually being exposed to new threats. As noted in the section above about hardening, because it is essential to focus on control systems that operate reliably over long periods of time, there is a need to assess how to deal with threats before those threats materialize. In other words, it is important to provide security management for adapting to the changes to which the system is exposed.

To achieve this, management, engineering, operations, and human resources need to come together on an ongoing basis to work through the plan, do, check, act (PDCA) cycle. Specifically, in addition to choosing the improvements to make based on systematically identifying the new threats and other changes to which the system is exposed and assessing the risks they present, there is a need to establish improvement practices in terms of cyberspace, physical space, and operational management, and to formulate implementation plans based on these improvement practices. An important factor in this work is performing an objective risk assessment.

To achieve this adaptivity, Hitachi supplies engineering that draws on its past experience in developing control systems and is based on the Cyber Security Management System (CSMS) for control systems.

(3) Responsivity (see Fig. 5)

Because complete protection against security threats is impractical, the response when an incident does occur is an important aspect of protecting social infrastructure systems and minimizing damage. Along

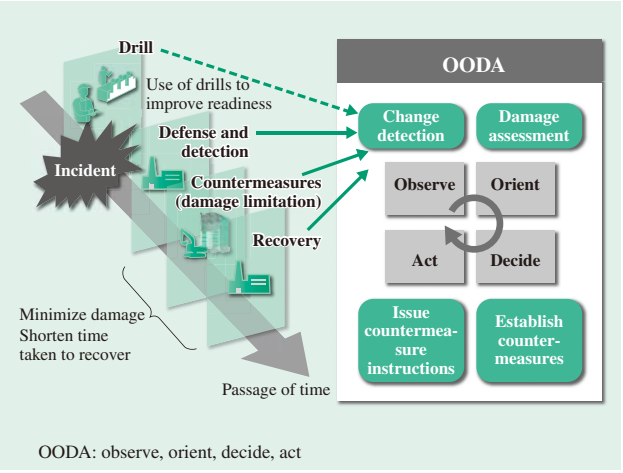


*Fig. 5—Achieving Responsivity. To minimize the impact of security threats on a system, it is important to identify the signs of a threat quickly and to take action against it.*

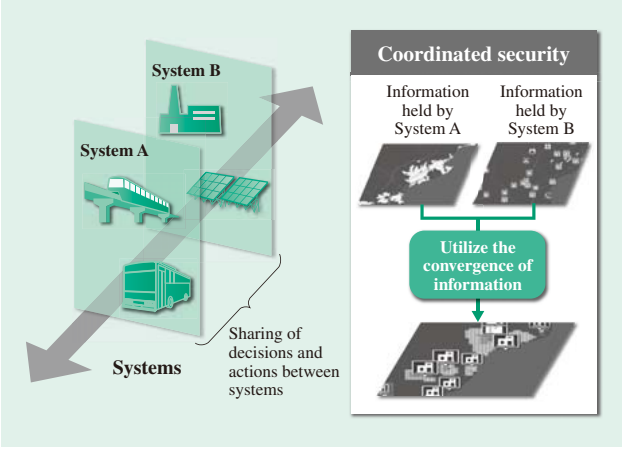


*Fig. 6—Achieving Cooperativity.*
*To protect social infrastructure systems, it is important to establish mechanisms for obtaining timely information about security threats in other related systems.*

with continuous monitoring for changes in the state of the system and assessing whether changes are due to security threats, achieving this requires a rapid response based on an assessment of the scope of the security threat and the formulation of responses. In addition to providing systems with ways of identifying system status changes, a dedicated organization for formulating responses and other practices is also essential.

Together with techniques for rapidly detecting changes in the status of a system at the IT level and business level, Hitachi also supplies specialist services such as providing the latest security information to support a dedicated organization and classifying security threats.

(4) Cooperativity (see Fig. 6)

To protect social infrastructure systems against threats, it is important to obtain information about security threats beforehand. Furthermore, when a number of systems are working together, there is the potential for a security threat to a system at one site to spread to the other systems.

Accordingly, not only do social infrastructure systems need to coordinate their security policies and other countermeasures, it is also important that they share security threat information.

To achieve this cooperativity, Hitachi offers a variety of gateway devices and supplies solutions that enable information sharing between organizations.

## SECURITY SOLUTIONS

Following the summary of Hitachi system security concept presented above, this section presents examples of security solutions that utilize that concept (see Fig. 7).

Providing security from the perspective of adaptivity involves conducting risk assessments that focus on the assets being protected, and supplying optimal security countermeasures by formulating the cyber-security and physical security measures needed to offer realtime protection. In terms of

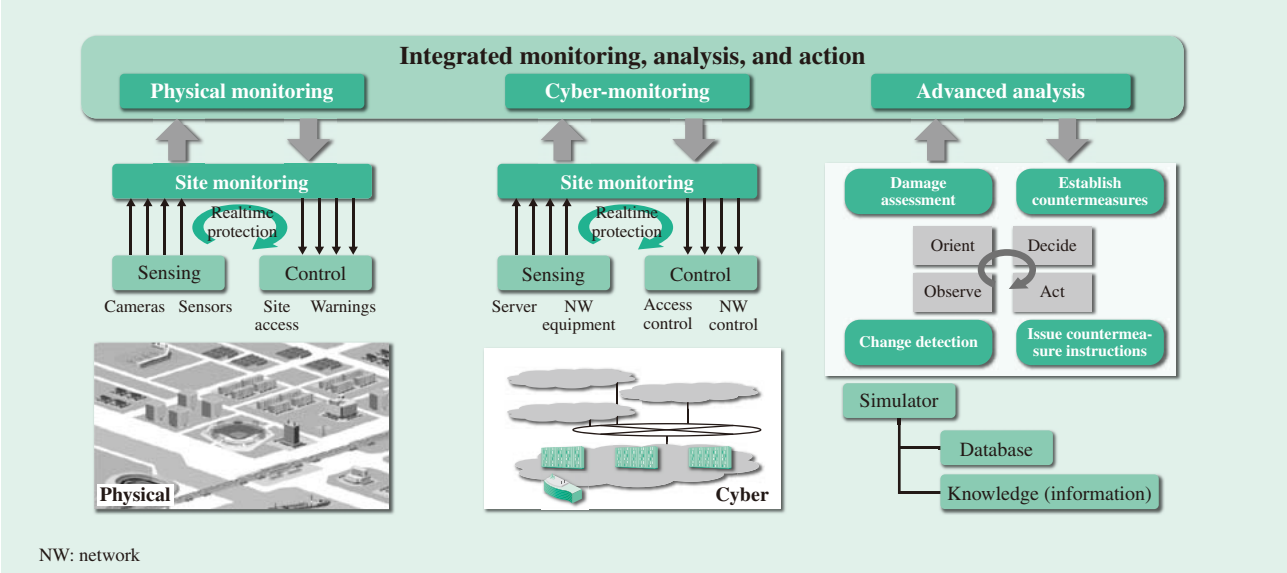


*Fig. 7—Example Security Solution that Uses the Hitachi System Security Concept.*
*The security of social infrastructure systems is maintained by providing realtime protection in terms of both cybersecurity and physical security, with integrated monitoring, analysis, and action.*

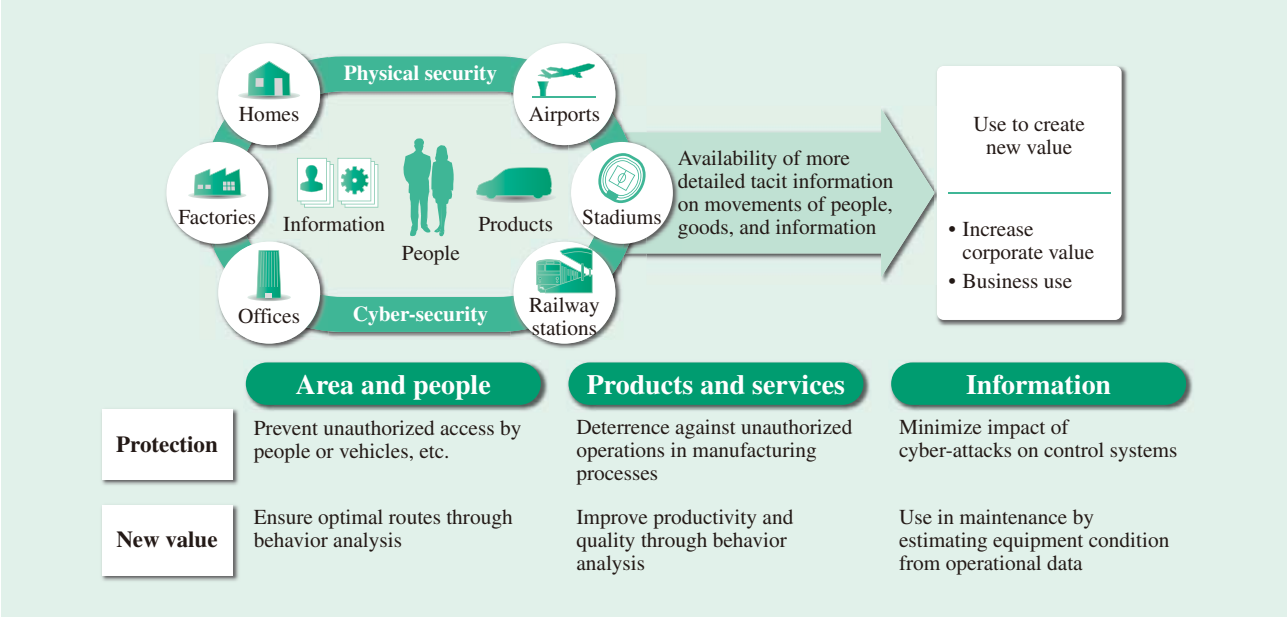


*Fig. 8—Add Value through Security.*
*In addition to offering protection, the shared use of information obtained from security systems can also create new value.*

responsivity, it involves providing engineering support for establishing the infrastructure needed to respond quickly to intrusions or new threats, and supplying systems for security threat analysis.

The implementation of security measures, meanwhile, involves obtaining information with even greater precision and granularity than in the past, and identifying the knowledge needed to decide whether or not the information is reliable. Use of this information helps improve corporate value and opens up possibilities in the form of new services. To this end, Hitachi is also promoting ways of making good use of the information obtained by security measures (see Fig. 8).

## CONCLUSIONS

This article has described new security requirements for building the control systems that underpin social infrastructure systems.

Security measures for control systems are an important requirement for protecting social infrastructure systems. To build secure social infrastructure that everyone can use with confidence, Hitachi intends to continue cooperating with organizations in Japan and elsewhere and working on the research and development of the technologies needed to protect against increasingly sophisticated threats, and also to supply products that utilize the technology it develops. It also plans to supply total services for social infrastructure systems that extend from security risk analysis to system implementation and operational support.

## REFERENCES

(1) IEC, http://www.iec.ch/
(2) IEC, "Factory of the Future," http://www.iec.ch/whitepaper/futurefactory/
(3) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).

## ABOUT THE AUTHORS

Toshihiko Nakano, Ph.D.
*Control System Platform Division Security Center, Services & Platforms Business Unit, 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).*

Hideki Tonooka
*Control System Platform Division Security Center, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the marketing and product development of information and control system products.*

Masashi Sato
*Security Engineering Department, Industry & Distribution Business Unit, Hitachi, Ltd. He is currently engaged in the integrated security solutions business.*

Tadashi Kaji, 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 information security technology. Dr. Kaji is a member of the IEEE Computer Society.*

Yoichi Nonaka, Ph.D.
*Center for Technology Innovation – Production Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in research into supply chain management, production control, and digital engineering. Dr. Nonaka is a member of The Japan Society for Precision Engineering (JSPE), The Society of Instrument and Control Engineers (SICE), The Japan Society of Mechanical Engineers (JSME), and The International Academy for Production Engineering (CIRP).*