Featured Articles II

Security Platforms

Hitachi's Security Solution Platforms for Social Infrastructure

Toshihiko Nakano, Ph.D.
Takeshi Onodera
Tadashi Kamiwaki
Takeshi Miyao

OVERVIEW: Recent years have seen an increase in the number of security threats to social infrastructure systems, including targeted attacks directed at more specific objectives and attacks that affect the public. Advances in IoT technology, meanwhile, are increasing the potential for cyber-attacks from a wide range of sources. Insider and terroristic incidents are also on the rise. Hitachi uses the Hitachi system security concept as a basis for considering the security requirements for protecting social infrastructure systems, and is working on the development of a security solution platform that combines various measures required by management, operations, and on-site systems. To provide safe social infrastructure systems that everyone can be confident of using, Hitachi intends to supply solutions that can be precisely tailored to changes such as the proliferation of security threats and open architectures.

INTRODUCTION

SECURITY threats to social infrastructure systems are increasing in both the cyber and physical realms. In cyberspace, this includes an increase in targeted attacks directed at more specific objectives and attacks on the equipment used to control social infrastructure systems. Advances in Internet of Things (IoT) technology are accelerating use of system interoperation and increasing the potential for cyber-attacks from a wider area to have an impact on functions that are intimately involved in operations. In the physical realm, meanwhile, insider and terroristic incidents are also on the rise.

Taking note of the trends in these threats, the characteristics of the social infrastructure systems to be protected, and developments in techniques for open innovation starting with the IoT, Hitachi proposed its views on the security requirements for social infrastructure systems, a subject being worked on at the International Electrotechnical Commission (IEC)[1], an international standards body. The proposal was expressed as the Hitachi system security concept, requiring that these systems be adaptive, responsive, and cooperative. The requirements were presented and adopted in a whitepaper entitled *Factory of the Future*[2] on how factories will look in the future and

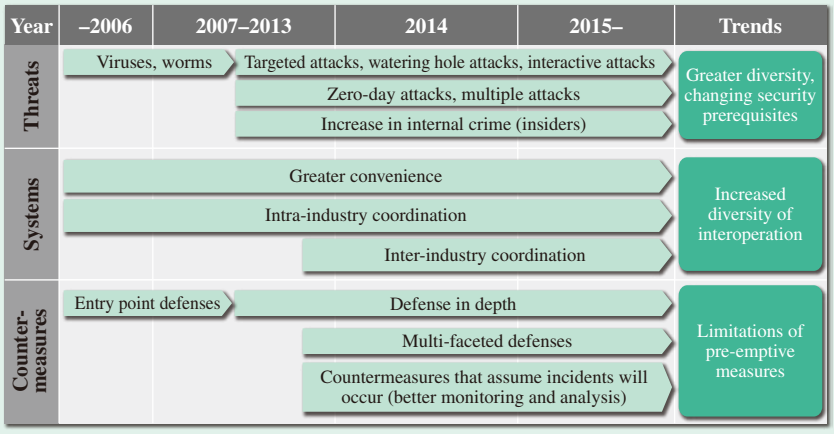

Fig. 1—Security Trends.
Along with security threats becoming more diverse in recent years, interoperation between social infrastructure systems is also increasing and taking on various forms. This demands new thinking about how to provide countermeasures.

the technologies that will be required. Hitachi is promoting the development of a variety of security solution platforms based on this concept.

This article contains an overview of security trends in social infrastructure systems that includes examples of the types of social infrastructure systems being considered, and presents a profile of a security solution platform based on the Hitachi system security concept[3] for the security requirements of social infrastructure systems.

TRENDS IN SECURITY

This chapter gives an overview of trends in threat identification, system configuration, and countermeasures that are essential to the security of social infrastructure systems (see Fig. 1).

While security threats are continually changing, the nature of attacks has become more diverse in recent years, including zero-day attacks in cyberspace and attacks that have both a cyber and a physical aspect. Insider incidents, in which an attack is perpetrated by someone involved with the system, also need to be considered. In terms of the system configurations on which all this is based, growing use of symbiotic autonomous decentralized architectures in which systems are interconnected in ways that transcend industries, applications, and nations is anticipated due to such developments as the proliferation of the IoT and supply chains. Fig. 2 shows examples of social infrastructure systems that interoperate over an open architecture. In addition to operating in ways that go beyond their locations, these systems utilize a variety of services for making the best use of planning, operational, and other data. A point to note about these social infrastructure systems is that each one operates autonomously, and so it is important that each system also maintains its own security in an autonomous way. As a result, maintaining security is also essential for the social infrastructure as a whole.

Unfortunately, greater use of interoperation makes it more difficult to predict the incidence and consequences of security threats accurately, making pre-emptive countermeasures increasingly problematic. Two important factors in considering how to respond to such security trends are to formulate security measures on the assumption that threats will manifest and to maintain on-site safety. This means ensuring the safety of those things that social infrastructure systems are intended to protect (including people, goods, information, and the environment), making it essential that systems provide protection on multiple fronts and incorporate security measures that satisfy this requirement for both the cyber and physical realms.

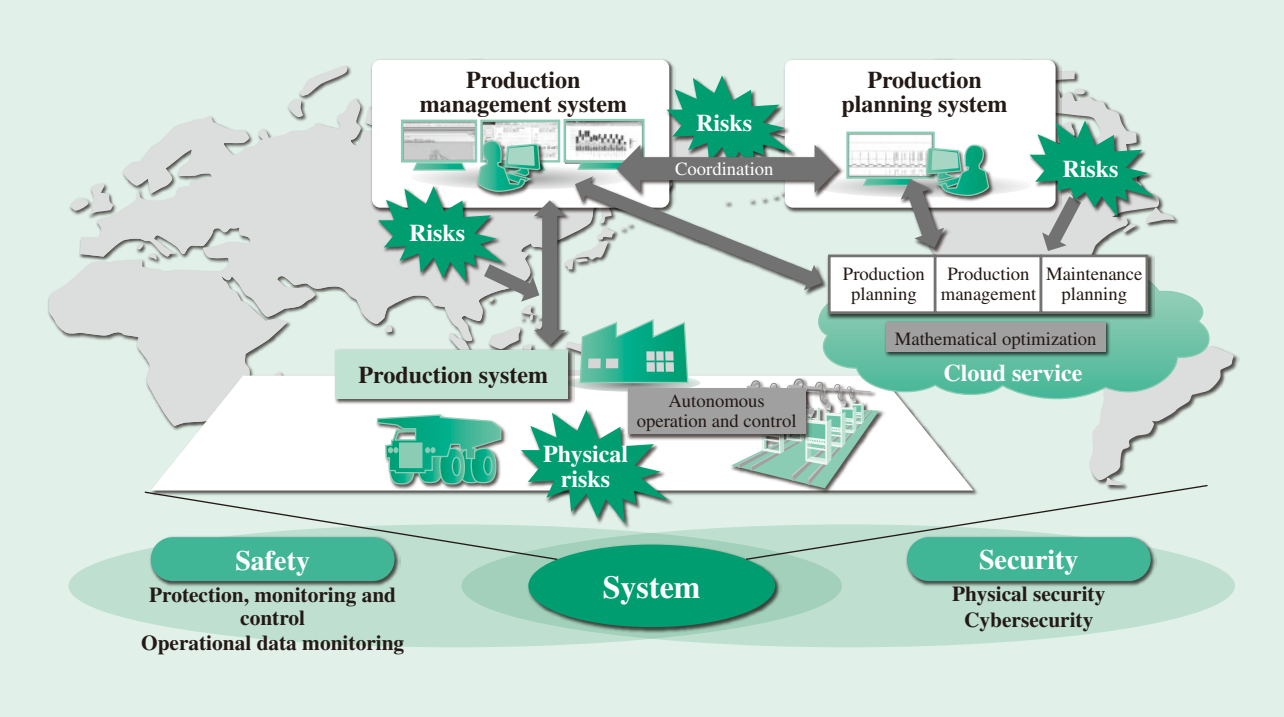

Fig. 2—Maintaining Safety and Security of Social Infrastructure Systems.
Systems interoperate across an open architecture, so maintaining safety and security is important.

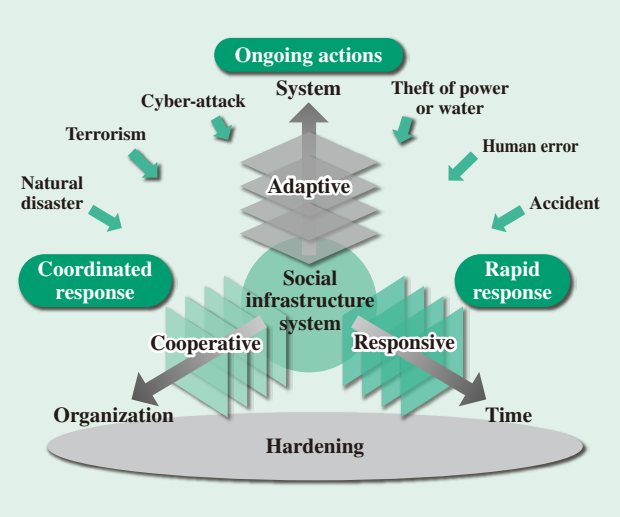

Fig. 3—Hitachi System Security Concept.
Hitachi has proposed the Hitachi system security concept for the requirements needed to maintain security on social infrastructure systems.

HITACHI SYSTEM SECURITY CONCEPT

This chapter describes the Hitachi system security concept proposed by Hitachi.

Hitachi expresses the requirements for maintaining the security of social infrastructure systems in terms of this Hitachi system security concept (see Fig. 3). Specifically, this means being more resilient to anticipated threats using the configuration of the systems concerned as a base (hardening). With this base, the concept also describes new requirements for security in terms of being adaptive, so that security measures, too, can change as needed in response to continually changing threats and system configurations; being responsive, so as to take actions to minimize the impact on social infrastructure systems when a security threat does arise; and being cooperative in the sense of multiple organizations working together to identify security threats at an early stage.

Recognizing that these requirements are important for the implementation of social infrastructure systems and need to be shared throughout the world, the requirements have been discussed at the IEC, an international standards body, where they were presented and adopted in a whitepaper entitled *Factory of the Future* on how factories will look in the future and the technologies that will be required. Table 1 lists the details of what is required for each requirement.

TABLE 1. Hitachi System Security Concept Implementation
The table lists what is needed to implement each aspect of the Hitachi system security concept.

Type of countermeasure	Summary
Making systems more resilient (Hardening)	Divide the system into separately managed zones, and detect unauthorized intrusions or behavior in each zone
Ongoing adaptation to threats (Adaptive)	Routinely assess system risks with reference to threat trends and update or strengthen measures for making system more resilient
Rapid response to threats (Responsive)	Continually monitor and analyze status of measures for making system more resilient and respond quickly if a threat gets into the system
Share information about threats (Cooperative)	Prepare for incidents by sharing information about threats and risks with stakeholders, including operational and management staff, other companies in same industry, and customers (risk communication)

SECURITY SOLUTION PLATFORMS

This chapter describes security solution platforms that implement the Hitachi system security concept that was summarized in the previous chapter.

To provide systems that combine safety and security, Hitachi supplies not only standard security solutions, but also security solutions that take advantage of the services and other business knowledge provided by the systems themselves. Hitachi supplies security solution platforms that are optimized for specific social infrastructure systems using common security solutions as a base (see Fig. 4).

In addition to solutions for the security of on-site systems, these security solution platforms provide solutions that take account of everything from security management at the planning stage to daily security operations. The following gives an overview of the solutions provided by Hitachi.

(1) Adaptive solutions

To be adaptive, it is important for organizations to put a security management system in place. Accordingly, Hitachi supplies consulting for establishing in-house security management systems that comply with standards such as the IEC 62443 and the International Organization for Standardization (ISO) 27000 series. To ensure that management is undertaken correctly, this includes assistance with security risk analysis as well as assessing the status of security on existing systems.

(2) Cooperative solutions

In terms of being cooperative, there is a mechanism in place for linking information between organizations inside and outside a company to protect systems from security threats. By having organizations inform

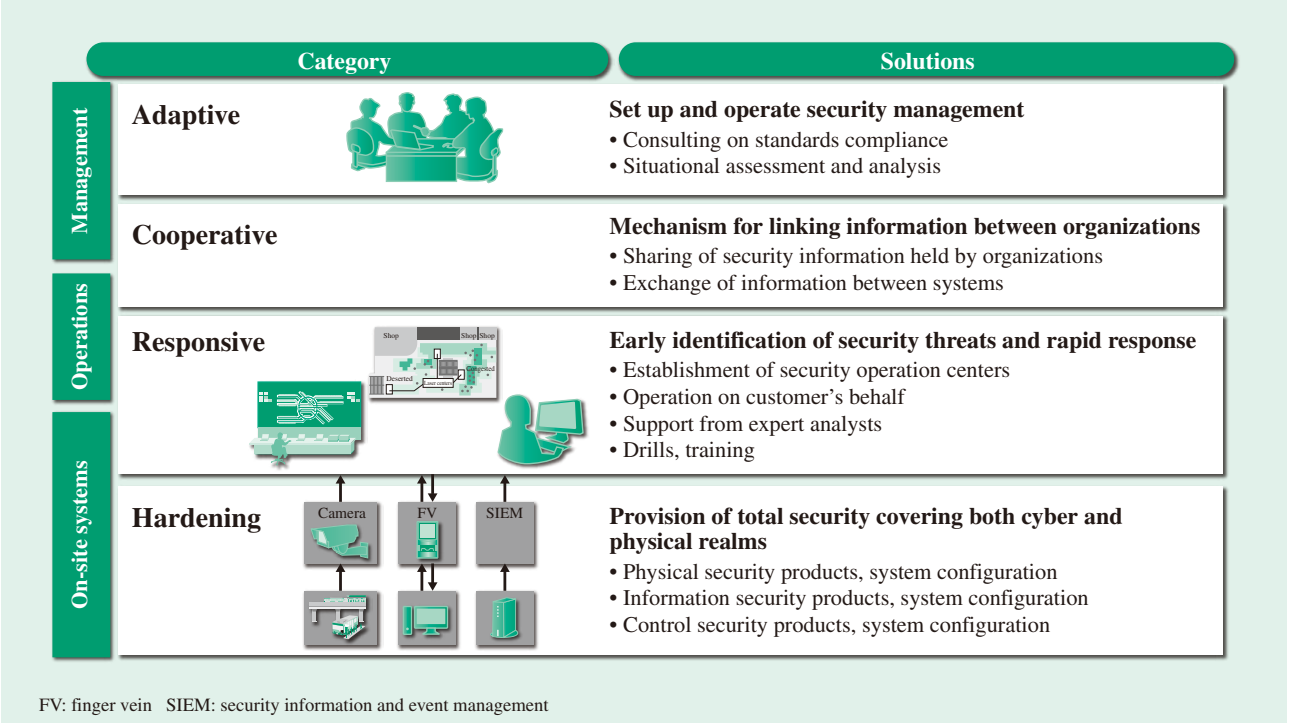

Fig. 4—Security Solution Platform.
The security solution platform implements the Hitachi system security concept.

each other about things like new security threats and how to deal with them, this exchange of information enables the security management systems referred to above to take advantage of the latest information. The exchange of information is also needed to make systems responsive, as discussed below. Attackers are continually looking in a systematic manner for new methods and routes of attack. This makes it essential that the defenders, too, collect and share information about the characteristics of attacks widely across a number of organizations. It is particularly important to share images and other information from the physical realm as well as from cyberspace. Hitachi supplies solutions that establish the infrastructure and support the practice of sharing information on both the cyber and physical realms.

(3) Responsive solutions

In terms of being responsive, the essential factors in enabling the early identification of security threats and a rapid response are to collect on-site information in a timely manner, to have effective ways of assessing situations, to formulate the correct responses, and to implement them quickly. Hitachi supplies support for establishing security operation centers to perform these steps, operating them on the customer's behalf, and conducting analyses using specialists in security technology and experts with operational know-how from Hitachi's own centers, and also training staff on how to deal with security threats, including the staging of drills.

(4) Hardening solutions

To protect on-site systems by making them more resilient, it is necessary to equip them with the means to protect the targets of security threats in ways that combine both cyber and physical defenses. Hitachi supplies security products and system configurations for the protection of physical spaces and in the form of solutions for protecting cyberspace.

Other articles in this edition of *Hitachi Review* describe solutions for information security, control security, physical security, and IoT systems.

CONCLUSIONS

This article has described Hitachi's security solution platforms for maintaining the safety and security of social infrastructure systems.

Security threats to social infrastructure systems are having a greater impact than ever on the activities of organizations and people, and on society. Meanwhile, advances in society and the development of IoT technology are linking the activities of organizations and people together into more extensive networks. As a result, it is becoming more difficult to predict

the incidence of security threats or the routes that attacks or infection will take. This makes it important that security measures be undertaken by people and organizations working together in networks rather than just as individual entities. To achieve this, security guidelines and the infrastructure for information sharing are being put in place by governments and organizations. Progress is also being made on turning these into international standards and on establishing certification programs.

Hitachi intends to continue contributing to the creation of safe and secure social infrastructure systems through collaborative creation with numerous organizations as well as by accurately identifying changes and supplying the best possible solutions.

REFERENCES

(1) IEC, http://www.iec.ch/
(2) IEC, "White Paper: Factory of the Future," http://www.iec.ch/whitepaper/futurefactory/
(3) T. Nakano et al., "International Standardization Activities for Hitachi System Security Concept and Social Infrastructure Security Based on It," Hitachi Review **65**, pp. 64–69 (Jun. 2016).

ABOUT THE AUTHORS

Toshihiko Nakano, Ph.D.
Security Business Division, Social Innovation Business Division, Hitachi, Ltd. He is currently engaged in the development of security solutions. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Takeshi Onodera
Information System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the business development of service platforms.

Tadashi Kamiwaki
Security Business Division, Social Innovation Business Division, Hitachi, Ltd. He is currently engaged in the development of security business.

Takeshi Miyao
Security Business Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in supervising security business operations.