DX with Cybersecurity to Protect Smart Factories from Security Threats

Smart factories are being developed at an accelerating pace as part of DX for business creation and production reform. However, cybersecurity threats are also appearing in control systems including operation and management due to their linking with networks and the use of open technologies. The development of smart factories entails a need to link with external networks, utilize cloud services, and establish supply chains, making it more necessary than ever to deal with security threats. This article describes solutions that support the promotion of DX to ensure security by drawing on Hitachi's experience in building smart factories.

Takayuki Kameda
Tsutomu Yamada, P.E. Jp
Kohei Yamaguchi

1. Introduction

In addition to providing attractive products and services, manufacturers are also required to maintain and improve the quality of increasingly complex products and services. Recently, there have been an increasing number of examples of companies that are promoting corporate transformation through digital transformation (DX)[1]. Even so, promoting DX has required new ways of thinking about security.

This article describes examples of conversion to smart factories, the security concepts required for this conversion, examples of security solutions, and security recommendations for the future of manufacturing.

2. DX in the Manufacturing Industry

DX in the manufacturing industry requires the utilization of data from the field and the realization of control systems that can keep up with the transformation of business. Also, linkage between on-site systems and internal and external company systems, as well as the use of general-purpose IT equipment and services, will be essential. And so, companies are focusing their attention on smart factories to achieve these goals.

2. 1 CPS

One concept related to smart factories is that of a cyber-physical system (CPS). A CPS is a system that gathers information from the real world (physical space), collects and analyzes it in cyberspace, and feeds back the information and value obtained from it to the real world to solve problems[2]. A high degree of integration between cyberspace and physical space will enable goods and services to be provided to those who need them, when they need them.

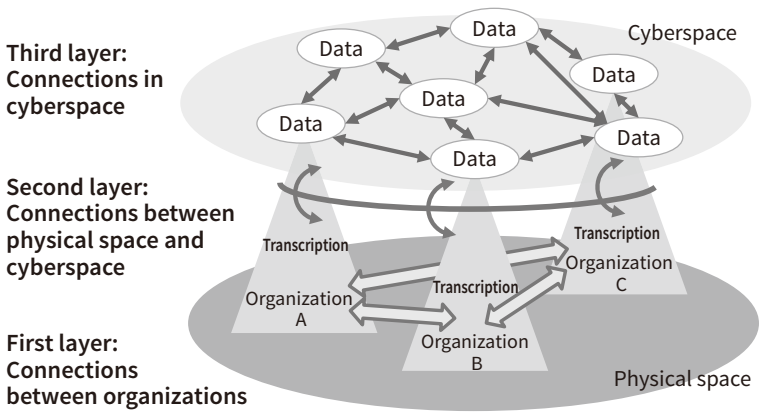
The Cyber-Physical Security Framework (CPSF) of the Ministry of Economy, Trade and Industry (METI) provides hints for potential solutions to security in a CPS[3]. **Figure 1** shows the connections between the field and the services presented in the CPSF. The CPSF defines the first layer as connections between inside and outside organizations

that ensure the trustworthiness of the enterprise's management, the second layer as the transcription of data between physical space and cyberspace, and the third layer as connections in cyberspace that distribute, process, and manage trusted data.

Some concerns about the CPSF are that attacks from cyberspace can easily reach the physical space and that the impact of cyber-incidents could expand due to complex supply chain connections.

2. 2
Smart Factory Configuration Example

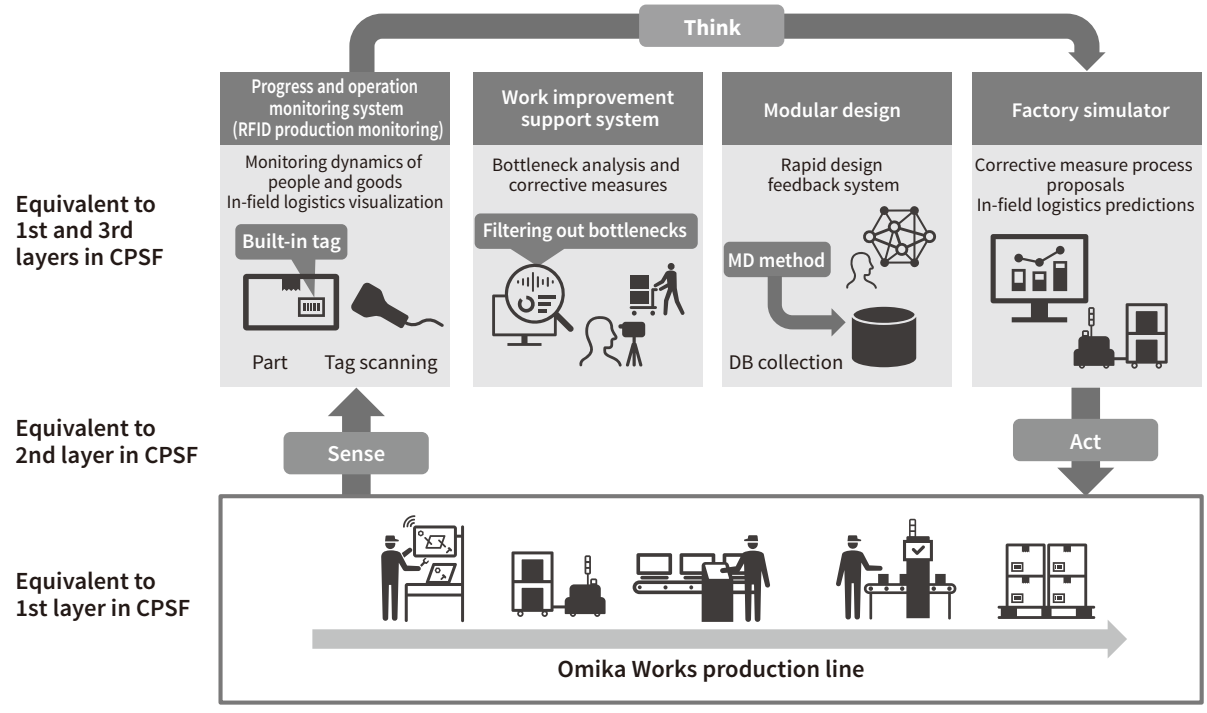
Figure 2 shows the production management system in the production line of the Omika Works of Hitachi, Ltd. as an example of a smart factory[4]. Omika Works has built a progress and operation monitoring system that collects data on the progress of workers and the flow of goods in physical space and provides a real-time overview of the dynamics of the entire production site in cyberspace. It



Note: This figure was prepared with elements added by Hitachi based on the "Cyber-Physical Security Framework (CPSF)" by the Ministry of Economy, Trade and Industry (METI).

Figure 1 — CPSF Conceptual Diagram
The industrial society in Society 5.0 is organized into three layers, and this figure shows the Cyber-Physical Security Framework (CPSF) three-layer model, which clarifies the basic points of trustworthiness for ensuring security.

Figure 2 — Example of a Smart Factory
Hitachi has established a highly efficient production model that utilizes people, goods, and equipment information between cyberspace and physical space by linking RFID production monitoring, work improvement support, modular design, and factory simulators.



RFID: radio frequency identifier MD: modular design DB: database

has also established a highly efficient production model by improving the efficiency of the design process and the accuracy of production planning using a factory simulator.

2. 3
Challenges of Smart Factories

The goals of the control system in the manufacturing industry are to produce and supply products ensuring the planned safety, quality, delivery, and cost (SQDC) from the standpoint of business continuity (BC). However, security incidents could pose a threat to these goals because they could cause business disruptions, thereby adversely impacting BC+SQDC.

Even if a device or system has maintained BC+SQDC up to now, the scope of assumed reliability must be reviewed when changing the configuration to a smart factory. In other words, the range of control the manufacturer can have will change. For example, the specifications of a conventional control system are fixed at the time of design, and the configuration and forms of use are rarely changed even after the system is installed. However, the following new forms of use are expected to expand in smart factories (see **Figure 3**).

(1) IT system linkage

For example, to streamline production, the control system is linked to business systems and engineering systems as needed.

(2) External system linkage

The control system is connected to external systems such as cloud systems in order to flexibly use server assets and off-the-shelf services.

(3) Use in urban environments (terminals)

For remote maintenance and similar operations, tablet terminals are used to monitor on-site conditions from locations other than the factory.

In a smart factory, it is necessary to review the conventional concept of perimeter defense, where communication partners within a boundary are uniformly trusted, and to configure control systems and implement security measures that assume various environmental changes.

3. Smart Factory Security

3. 1
Mindset Needed for Securing Smart Factories

The future of smart factories, which will be digitally transformed by utilizing open technologies while ensuring business continuity, safety, and quality (BC+SQDC), is expected to incorporate new forms of use such as IT system linkage, external system linkage, and urban use. In addition to the traditional security concepts of confidentiality, integrity, and availability and also health, safety, and environmental protection, the following characteristics will likely need to be protected.

(1) Authenticity

Authenticity ensures that the communication partner is the intended partner, and the communicated content is correct. For example, measures must be implemented to protect against the threat of spoofing when using external services.

(2) Reliability

Reliability ensures that the communication partner consistently performs as intended (does not perform unintended actions). For example, the service content provided by an external service must maintain the expected quality.

(3) Protectiveness

Protectiveness ensures that measures are taken to address security threats to the devices and communication information of communication partners. For example, this can be performed by implementing defenses and detection measures that have been identified as necessary by risk analysis.

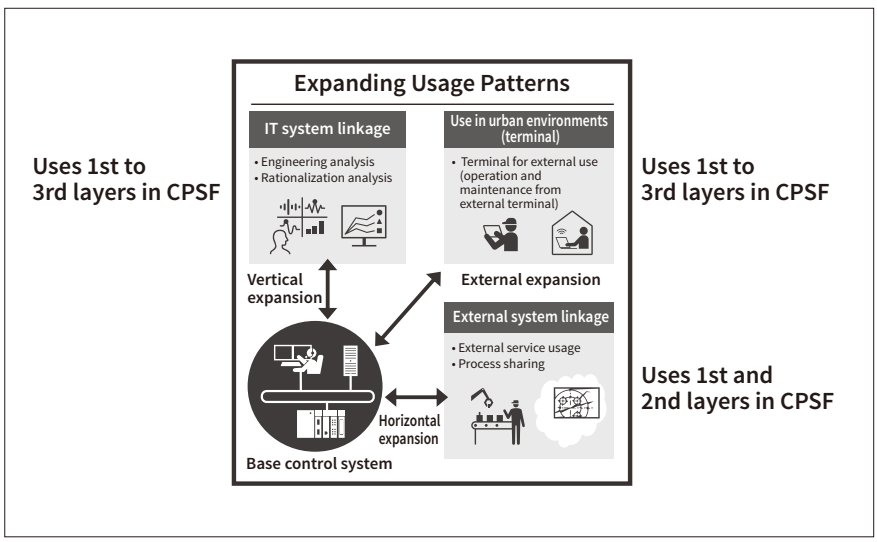


Figure 3 — Expanding Usage Patterns for DX
When examining security for DX, it is important to consider not only the traditional fixed linkages, but also IT system linkage, external system linkage, and urban use. Measures must be taken that anticipate these expanding usage patterns.

It is important to implement and maintain these characteristics of authenticity, reliability, and protectiveness (ARP) in order to ensure future-proof security in a DX-enabled smart factory.

3. 2
Examples of Security Measures for Smart Factories

Use of authentication techniques that prevent spoofing is one possible solution for ensuring authenticity. For example, multi-factor authentication using two or more of the following methods is effective: knowledge-based authentication, possession-based authentication, and biometric authentication. Another possible solution for ensuring reliability is standards certification, which indicates that a device conforms to a standard. For protectiveness, possible solutions include encryption of information and physical protection of devices. However, it is necessary to take into account the requirements of the control system.

4. Hitachi's Solutions for Security

Until now, Hitachi has provided solutions that were integrated from the standpoints of security and control systems. Now, with the shift to smart factories, it is providing DX-enabled security solutions that resolve the new issues described in section 3.1 (see **Table 1**).

4. 1
Strategic Planning

DX must be used to develop systems that support these solutions in conjunction with business and production reforms. Because these business and production reforms are wide-ranging and continuous, the implemented measures may have excesses or deficiencies when examined on an individual system basis.

Strategic planning solutions efficiently organize the requirements to be met for security and control systems to develop DX-enabled control systems, and provide the necessary security strategies for the realization of smart factories.

4. 2
Situation Assessment and Countermeasure Planning

The solution for situation assessment and countermeasure planning is to investigate the current situation from a management perspective, and identify the risks and issues for the current system, its operation, and its response to problems that may occur, in conjunction with the elements to be realized as a smart factory (see **Figure 3**). Based on the results, the necessary security measures are formulated for the elements to be realized as the smart factory from the standpoint of the control system.

To ensure security for DX, at this stage, it is important to consider authenticity, reliability, and protectiveness against threats such as spoofing.

4. 3
Building a System

Hitachi supports the entire process from design to implementation of control systems to ensure the security of DX-enabled smart factories.

A DX-enabled smart factory will use a wide variety of devices that are dynamically connected to the network. Hitachi uses its NX net monitor series to provide functions to control and manage the authenticity of these connections, as well as functions to support reliability and protectiveness (see **Table 2**).

4. 4
Operational Support

Security incidents that occur in control systems are often detected as anomalies (alarms) in devices or functions. Operational support provides solutions that help to determine whether the cause of the alarm is a security-related anomaly or a normal anomaly such as a device failure.

Table 1 — List of DX-enabled Security Solutions

In addition to traditional security solutions, this table shows the security measures that have been developed for enabling DX.

Classification	Solution
Strategic planning	Strategic planning of DX-enabled security
Situation assessment and countermeasure planning	Assessing the current situation and risk analysis for DX by objective
	Planning measures for DX by objective
Building a system	Support for building DX-enabled security systems
	Providing security devices and packages for control
Operational support	Alert integrated (control and security) monitoring
Human capital development	Developing "plus security" human capital needed to implement DX
	DX incident response training (security + control)

DX: digital transformation

Table 2 — NX Net Monitor Series Functions
This table shows the functions for ensuring security in DX-enabled smart factories.

Function		Outline	Tool
Control and management of device authenticity		• Detecting connection of malicious devices to network • Removal of malicious devices	Appliance
Control and management of authenticity of communications		• Monitoring of network communications • Detecting and notification of unauthorized communications	IDS
Operational support	**Device information analysis (protectiveness support)**	• Identifying the physical connection location of the device (physical port of switching hub) and the open logical port	Crawler
	Integrated management (reliability support)	• Integrated management of above functions • Notification to other systems	Manager

IDS: intrusion detection system

4. 5
Human Capital Development

Hitachi is conducting a security human capital development program called "NX Security Training Arena" using cyber-security training facilities. To develop the "plus security" human capital that will be needed to implement DX going forward, Hitachi provides education and training for human capital development from the standpoint of DX-enabled control systems combined with security.

5. Conclusions

This article presented the background of the conversion to smart factories and explained the CPS concept. It also explained the threats arising due to the shift to smart factories and the security solutions available to deal with them.

Smart factories will make it easier to respond to changes in production to increase the value of products and services. It will also enable remote maintenance at factories while off-site, changing the way people work.

On the other hand, the shift to smart factories will also entail a high possibility of cyber incidents as various people and objects exchange various information inside and outside the factory.

To support the security of smart factories, which will further develop in the future, there must be mechanisms in place that verify each time whether an exchange of information was intentional. Hitachi offers a full range of support to customers in developing smart factories by consulting on security policies, providing security components, and building entire systems.

References

1) Ministry of Economy, Trade and Industry (METI), "Guidelines for Promotion of Digital Transformations (DX Promotion Guidelines) Version 1" (Dec. 2018) in Japanese, https://www.meti.go.jp/press/2018/12/20181212004/20181212004-1.pdf
2) Hitachi, Ltd., "Cyber-physical system (CPS)," https://www.hitachi.com/rd/glossary/c/cyber_physical_system.html
3) METI, "The Cyber/Physical Security Framework Version 1" (Apr. 2019), https://www.meti.go.jp/english/press/2019/pdf/0418_001b.pdf
4) Hitachi, Ltd., "Production Planning Optimization" in Japanese, https://www.hitachi.co.jp/products/it/lumada/cs/00008/index.html

Authors

Takayuki Kameda
Control System Security Engineering Department, Control System Platform Development Division (Omika-Works), Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Design and development of security products for control systems.

Tsutomu Yamada, P.E. Jp
Control System Security Engineering Department, Control System Platform Development Division (Omika-Works), Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Security consulting for control systems. *Certifications*: IEC/TC 65/WG expert and CISSP. *Society memberships*: IEEE, the Society of Instrument and Control Engineers (SICE), and the Institute of Electronics, Information and Communication Engineers (IEICE).

Kohei Yamaguchi
Control System Security Engineering Department, Control System Platform Development Division (Omika-Works), Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Security consulting for control systems. *Certifications*: CISSP and Registered Information Security Specialist.