Featured Articles

Information and Control Platform for Utilization of Plant Data

Hideki Osonoi
Takahiro Ohira
Kei Takezawa
Takuma Nishimura
Daisuke Yokota
Shunsuke Mori, Ph.D.

OVERVIEW: Along with the growing adoption of IoT practices for plant devices in recent years, potential is seen for the establishment of business models and the creation of new added value through the use of big data obtained from such devices. To achieve this, it will be important that control systems satisfy new requirements for the collection and use of plant data, flexible interconnection with IoT devices, and the maintenance of security when these permit open execution. Against this background, Hitachi is developing technology for offering new solutions that utilize plant data in control systems based on its symbiotic autonomous decentralization concept.

INTRODUCTION

TO maintain the operation of important social infrastructure that is required to operate non-stop, reliability and expandability are two crucial requirements for the systems that monitor and control such infrastructure equipment. In the past, the ability to build autonomous decentralized control systems with excellent reliability and expandability has been achieved by having the servers, controllers, and other control nodes exchange the information required for these control systems based on the autonomous decentralization concept, and by supplying information and control platforms that operate autonomously based on exchanging this information between individual control nodes[1].

In more recent years, advances in sensing, networks, and big data analytics have led to growing adoption of Internet of things (IoT) practices for the on-site equipment used in control systems. It is anticipated that the plant information made available as a result will not only be used by the control system itself, but also provided for use by management and other stakeholders for the creation of new added value and business models through open innovation[2].

This article describes the development of technology for information and control platforms (platform technology) using the symbiotic autonomous

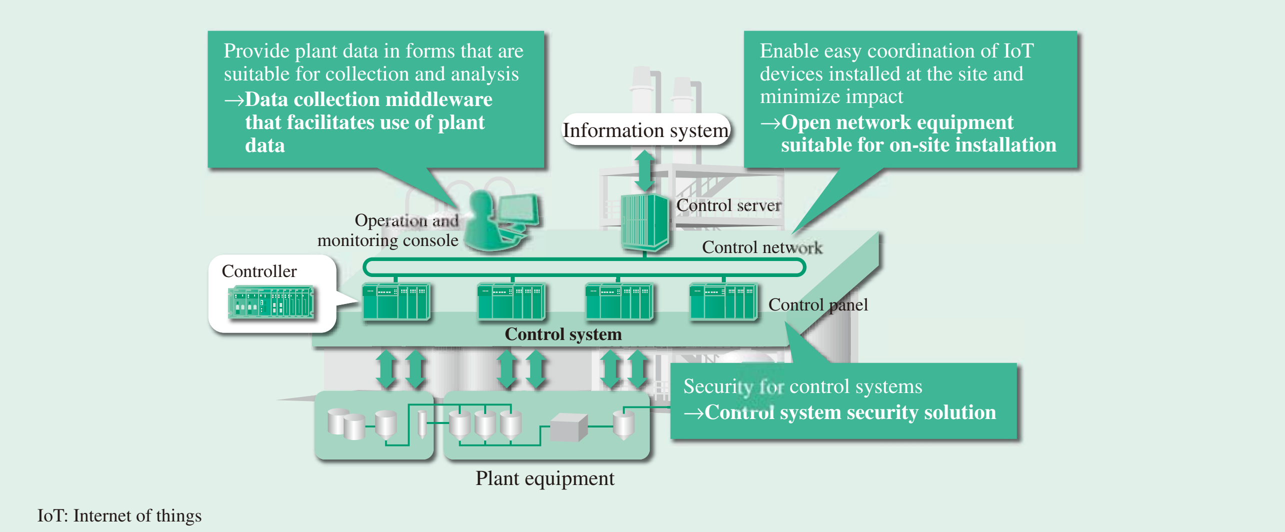

Provide plant data in forms that are suitable for collection and analysis
→Data collection middleware that facilitates use of plant data
Information system
Enable easy coordination of IoT devices installed at the site and minimize impact
→Open network equipment suitable for on-site installation
Control server
Operation and monitoring console
Control network
Controller
Control panel
Control system
Security for control systems
→Control system security solution
Plant equipment
IoT: Internet of things

Fig. 1—New Functions Provided by Information and Control Platforms.
Hitachi is developing new functions needed to satisfy the new requirements for information and control platforms associated with implementing the symbiotic autonomous decentralization concept.

decentralization concept, which extends the autonomous decentralization concept at the system level in response to these trends.

WORK ON CONTROL SYSTEMS AND THE CHALLENGES THEY FACE

Control systems are implemented on information and control platforms that are made up of servers running a control operating system (OS), a network, controllers, and the middleware that ties these components together.

The implementation of the symbiotic autonomous decentralization concept described above requires control systems to satisfy new requirements for collecting and using plant data, flexible interconnection with IoT devices, and maintaining security when these functions are executed in an open environment.

To satisfy these requirements, Hitachi is developing new functions that enable information and control platforms to collect plant data and provide it in forms that are suitable for analysis, to enable the easy coordination of IoT devices installed at a site and minimize the impact of doing so, and to maintain control system security (see Fig. 1).

This article describes the following three aspects of these technical developments.

(1) Data collection middleware that facilitates use of plant data

(2) Open network equipment suitable for on-site installation

(3) Control system security solution

DATA COLLECTION MIDDLEWARE THAT FACILITATES USE OF PLANT DATA

Plants are likely to hold data that could potentially be used to improve energy, economic, or other forms of efficiency. Meanwhile, advances in big data analytics have created an environment in which services that utilize this plant data can be provided. To achieve this, these services require many different ways of collecting this plant data, while the collection methods require the expandability to allow users to obtain the data they want to use.

Middleware for “Pull” Information Collection

In a typical control system, the controllers use sensors to obtain information about the process being controlled and use actuators to control actions. This information is processed in the form of monitoring data and transmitted across the control network to be monitored by the control server (monitoring system) (see Fig. 2).

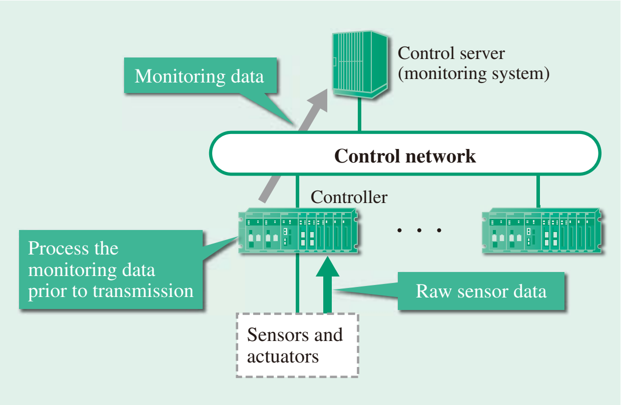

Monitoring data
Control server (monitoring system)
Control network
Controller
Process the monitoring data prior to transmission
Raw sensor data
Sensors and actuators

Fig. 2—Flow Chart of Data Acquisition by a Control System.
Rather than raw sensor data, control servers collect monitoring data that has been pre-processed by controllers.

The information is transmitted in the form required for monitoring by the server, not as raw sensor data. When monitoring the flow in a pipe, for example, the flow rate may be calculated from a number of different sensor readings for things like temperature and pressure. Accordingly, a new operation and maintenance (O&M) service for identifying or anticipating faults on individual sensors would need to obtain not only the data transmitted by the controllers but also the sensor readings it holds internally.

Unfortunately, to obtain these values in an existing control system would require modifications to the controller software or settings whenever the data points to be collected are added or changed. The resulting impact on production, such as having to shut down the controller, is a major problem.

To overcome this difficulty, Hitachi has developed middleware for “pull” information collection that can obtain data held inside controllers as required.

The middleware can add or change the data being retrieved without modifying the controller software or settings by having an application that runs on a control server specify which controller data it requires. Furthermore, because the collection of data from the controller uses a request/response (“pull”) model, a controller that receives a request can send the requested data to the server at a time that does not interfere with execution of control functions. The middleware also includes a function that specifies the available bandwidth in advance so as to prevent data requests from overloading the controller and interfering with execution of control functions (see Fig. 3).

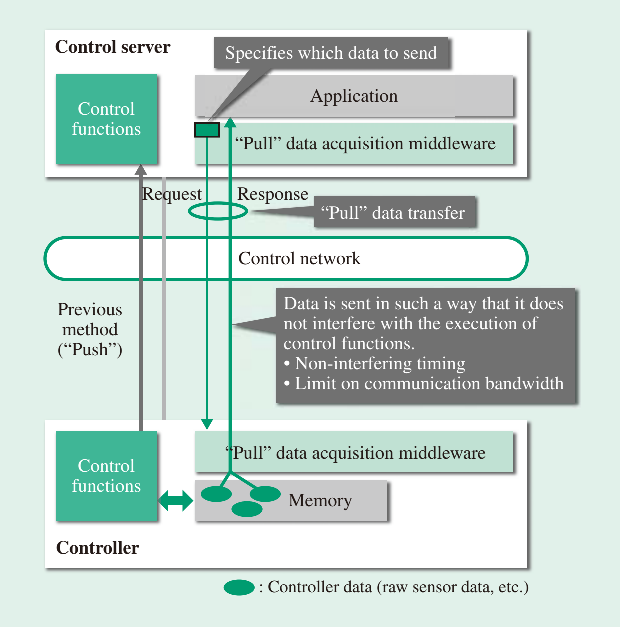

Control server
Specifies which data to send
Control functions
Application
"Pull" data acquisition middleware
Request
Response
"Pull" data transfer
Control network
Previous method ("Push")
Data is sent in such a way that it does not interfere with the execution of control functions.
• Non-interfering timing
• Limit on communication bandwidth
Control functions
"Pull" data acquisition middleware
Memory
Controller
● : Controller data (raw sensor data, etc.)

Fig. 3—Overview of Access Functions for "Pull" Data Acquisition Middleware.
Controllers return data in response to requests from control servers in such a way that it does not interfere with the execution of control functions.

In the future, Hitachi plans to add another function for converting the collected data into forms that are suitable for analysis.

Operation Monitoring Middleware

The growing diversity and complexity of social infrastructure systems is increasing the time it takes to identify the location of faults when they occur, and the associated losses are a drain on profits.

While the hardware and software used in control equipment already have the ability to acquire operational data, they are subject to the following problems that limit the use of this data.

(a) An inability to collect information required for investigating causes

Delays in action by operators to collect information can result in necessary data being lost.

(b) Limited availability of staff with skills for log analysis

Because the analysis of information requires specialist knowledge, only certain staff can do this work.

(c) Difficulty narrowing down the scope of investigation

The required information cannot be identified.

Hitachi has developed operation monitoring middleware as a means of solving these problems(3). The middleware is made up of the following components.

(1) Operation data (fault information) acquisition middleware

Automatic acquisition and storage on a disk of the relevant fault information when a predefined trigger occurs (such as an error message). The middleware also provides batch commands that maintenance staff can use to collect all types of fault information.

(2) Operation data archiving middleware

The collection and archiving on a single computer of information collected by the data acquisition middleware, memory dumps, and network data for devices connected to the system.

(3) Alarm management middleware

Performs the initial analysis of fault information collected by the operation data archiving middleware and outputs the likely fault location on a local console.

(4) Fault information analysis tool

Performs more detailed fault analysis based on information collected by the operation data archiving middleware. Along with combining information from a number of computers or faults and displaying it with a graphical user interface (GUI) in time-series, hierarchical, or other format, the tool also includes a function for learning specialist analysis know-how.

The first three of these components of the operation monitoring middleware are easy to customize for individual systems, including being able to add collection and analysis commands for fault information from specific applications.

The current purpose of operation monitoring software is to reduce loss costs, and Hitachi also plans to adapt it for use by remote maintenance services for which there is growing demand from an increasing number of projects in other countries.

OPEN NETWORK EQUIPMENT SUITABLE FOR ON-SITE INSTALLATION

New requirements are emerging that are important to plants that host social infrastructure systems with high criteria for reliability and availability, such as the requirement to provide a variety of services that work closely with these plants or the requirement to use detailed and up-to-date plant information. The establishment of plant networks for the interconnection of plant equipment and transmission of valuable plant information is essential to satisfying these requirements.

These networks require core components that can operate reliably over long periods of time at sites with harsh environmental conditions and limited space available for installation. These components in turn

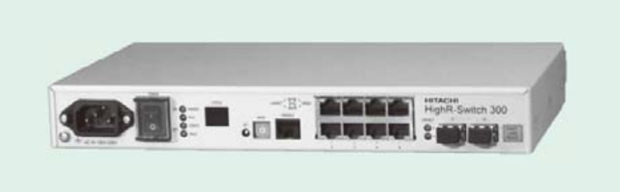


Fig. 4—Intelligent L2 Switch.
The switch features improved ruggedness to allow on-site installation. In addition to common network functions, it is also equipped with proprietary functions for high reliability.

need to support Ethernet. Ethernet has spread rapidly in industry over recent years, being a general-purpose open standard, with the standardization of things like quality of service (QoS) and virtualization still ongoing.

An Intelligent L2 Switch for Industrial Use

To provide a platform for implementing site networks that satisfy these requirements, Hitachi has developed its Intelligent L2 Switch, which is a small 10-port intelligent L2 switch for industrial use that features long life (10-year design life) and advanced functions together with excellent reliability and ruggedness (see Fig. 4).

Intelligent L2 Switch supports more than 40 common network functions, including simple network management protocol (SNMP), spanning tree protocol (STP), and virtual local-area network (VLAN).

They also include a proprietary optical ring protocol based on the core technology of a control network that complies with International Electrotechnical Commission (IEC) Publicly Available Specification (PAS) 62953. They are equipped with high-reliability functions, including the ability to recover automatically from a network fault in 500 ms or less in the maximum configuration of 64 nodes, re-routing around intermittent as well as fixed faults, and redundancy of blocking.

They also provide the following three features thanks to a specially optimized metal case and component mounting design.

(1) Able to operate at ambient temperatures from −10ºC to 60ºC

(2) Better resistance to dust due to having no fan or ventilation slots

(3) 4G seismic tolerance

These features enable the switches to be installed at sites with a harsh environment (see Table 1).

In the future, Hitachi intends to increase the number of Ethernet ports to allow use in large systems.

CONTROL SYSTEM SECURITY SOLUTION

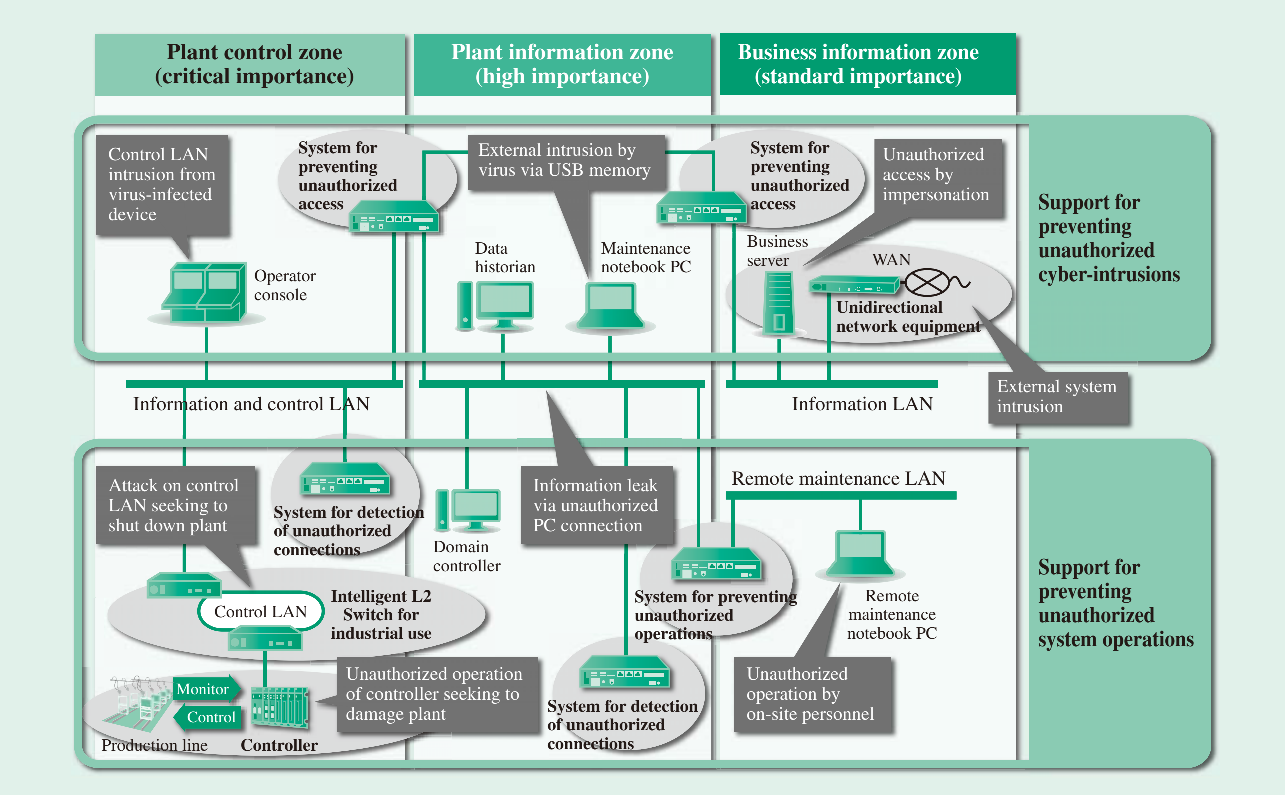
More control system vulnerabilities to cyber threats have become apparent in Japan and elsewhere since the first appearance of the Stuxnet malware that targeted control systems, meaning that security measures for control systems are needed to deal with these threats.

The provision of security measures for control systems involves first dividing the system into zones with different security protection levels, deciding on the level of security measures for each of these zones and the communication links between them, and then reviewing and implementing these (prevention,

TABLE 1. Intelligent L2 Switch Specifications
The table lists the main specifications of the Intelligent L2 Switch.

Ambient temperature	In operation	−10 to 60ºC
Fan, vent	Fanless, ventless	
Vibration tolerance	4G	
Standards compliance	Vibration	JIS E3014 class 1 (0.5 G)
	Impact	JIS E3015 class 1 (10 G)
	Air pressure	TB/T 1433-1999, KX3
	EMI standard	VCCI class A IEC 61000-6-2
	EMS standard	IEC 61000-6-4
	EMC standard	CE mark
	Safety certification	CB test report (IEC 60950-1)
	Environment	EU RoHS directive
Network management	SNMP	SNMPv1, SNMPv2c
	SNMP MIB	RFC 1213 MIB II RFC 1215 Traps
Optical ring protocol (based on IEC PAS 62953)	Maximum range	Optical loop: 500 km total
	Maximum number of nodes	64
	Re-routing time	500 ms or less
Special functions	• STP extended functions (loop guard) • QoS [priority control, bandwidth control (input policing)] • Port security (restricts access based on MAC address) • Packet filter function (levels L1–L4) • Loop protection • Broadcast storm control • Reset reboot on hardware fault	
Self-diagnostics	WDT, main memory ECC, cache parity, voltage monitoring for all DC power supplies	
External dimensions	300 (W) ×180 (D) ×43.5 (H) mm	
Installation	Vertical, horizontal	
Power supply	Input voltage	AC 90–250 V
Product life	10 years	

JIS: Japanese Industrial Standards VCCI: Voluntary Control Council for Interference by Information Technology Equipment CB: certification body
EU: European Union RoHS: Restriction of Hazardous Substances
IEC: International Electrotechnical Commission
EMI: electromagnetic interference EMS: environmental management system
EMC: electromagnetic compatibility
SNMP: simple network management protocol
RFC: request for comments MIB: management information base
PAS: Publicly Available Specification STP: spanning tree protocol
QoS: quality of service MAC: media access control WDT: watchdog timer
ECC: error checking and correction DC: direct current AC: alternating current


Plant control zone
(critical importance)
Plant information zone
(high importance)
Business information zone
(standard importance)
Control LAN intrusion from virus-infected device
System for preventing unauthorized access
External intrusion by virus via USB memory
System for preventing unauthorized access
Unauthorized access by impersonation
Support for preventing unauthorized cyber-intrusions
Operator console
Data historian
Maintenance notebook PC
Business server
WAN
Unidirectional network equipment
Information and control LAN
Information LAN
External system intrusion
Attack on control LAN seeking to shut down plant
System for detection of unauthorized connections
Domain controller
Information leak via unauthorized PC connection
Remote maintenance LAN
Control LAN
Intelligent L2 Switch for industrial use
System for preventing unauthorized operations
Remote maintenance notebook PC
Support for preventing unauthorized system operations
Monitor
Control
Production line
Controller
Unauthorized operation of controller seeking to damage plant
System for detection of unauthorized connections
Unauthorized operation by on-site personnel

LAN: local-area network USB: universal serial bus PC: personal computer WAN: wide-area network

Fig. 5—Control System Security Solution.
Hitachi supplies two different control system security solutions that combine security products for a wide range of control systems.

detection, preventing threats from escalating, and recovery)[4].

Hitachi has extended this approach to develop the Hitachi system security concept for social infrastructure security[5]. For security measures for control systems in particular, the recommended practice is to use measures that focus on resilience by adopting a whitelist approach that forms part of the Hitachi system security concept and only permits pre-approved operations, and Hitachi offers two control system security solutions that support the prevention of unauthorized cyber-access and unauthorized system operations, respectively (see Fig. 5).

Support for Prevention of Unauthorized Cyber-access

Preventing unauthorized access via cyberspace through connections to other systems is important for protecting control systems against external threats and ensuring their availability. Along with preventing unauthorized access, the challenge when installing security measures on a control system is also to minimize the load imposed by their installation and operation.

Accordingly, the installation of control system security is simplified by providing systems for preventing unauthorized access that permit the definition of whitelist security policies with tools to assist with this definition of security policies (see Fig. 6).

Similarly, the features of unidirectional network equipment, which include having a long life without requiring maintenance, reduce the work associated with system operation by acting as a software-less “data diode” (a hardware device that only permits communications in one direction, like a diode) (see Fig. 7).

Fig. 6—System for Preventing Unauthorized Access.
Installation in control systems is simplified by providing a support tool for defining whitelist security policies.

Fig. 7—Unidirectional Network Equipment.
Operational maintenance is minimized by eliminating the use of software. The device itself has a simple design to prevent mistakes.

These technologies improve measures for preventing unauthorized access while being designed for easy installation and operation.

Support for Prevention of Unauthorized System Operations

Before the targeted attacks that have been increasing in recent years, it was necessary to implement countermeasures on the assumption that it is not possible to eliminate unauthorized access entirely. Accordingly, there is a need for ways of limiting the damage that results if unauthorized access is permitted. Behavior detection techniques are widely used to detect cyber-attacks on information systems. They are more difficult to use on control systems, however, because they cannot tolerate misdetection. Accordingly, measures are adopted instead that improve their robustness to an attack.

Systems for preventing unauthorized operations protect critical equipment from denial of service (DoS) and other similar attacks by providing functions that include limiting the bandwidth of communication data and disconnecting the network.

Hitachi has developed a controller that is certified under the Embedded Device Security Assurance (EDSA) certification program for guaranteeing the security of control components run by the Security Compliance Institute (ISCI) of the International Society of Automation (ISA). It offers improved resilience to cyber-attacks by satisfying a predefined set of security requirements[6] (see Fig. 8).

EDSA: Embedded Device Security Assurance

Fig. 8—Controller with EDSA Certification.
The controller offers improved resilience to cyber-attacks by satisfying a predefined set of security requirements.

By building control systems using equipment that has such a high degree of robustness with respect to cyber-attacks, the impact on the plant equipment being controlled can be minimized in the event that an incident does occur.

CONCLUSIONS

This article has described the latest challenges and technical developments for the use of plant data from control systems based on the symbiotic autonomous decentralization concept.

As it can be anticipated that control systems will continue to develop in the future by adopting the latest information technology (IT) in their role as a platform underpinning the social infrastructure, Hitachi intends to continue developing technology for information and control platforms and supplying new solutions.

REFERENCES

(1) S. Hori et al., “Autonomous Decentralized Computer Control System for Rolling Mills and Finishing Lines,” Hitachi Hyoron **72**, pp. 455–460 (May 1990) in Japanese.

(2) Mizuho Information & Research Institute and Mizuho Bank, “Current and Future Outlook for Internet of Things (IoT) –Review of Studies Dealing with IoT and AI–,” Mizuho Industry Focus, Vol. 51, No. 3 (Aug. 2015) in Japanese.

(3) T. Yamagata et al., “Proposed Tool for Use of Operational Data for Fault Cause Investigation on Social Infrastructure Systems,” the 77th National Convention of Information Processing Society of Japan (Mar. 2013) in Japanese.

(4) IEC, “Industrial Network and System Security,” IEC 62443 (2013).

(5) M. Mimura et al., “Hitachi’s Concept for Social Infrastructure Security,” Hitachi Review **63**, pp. 222–229 (Jul. 2014).

(6) S. Okubo et al., “Plant Monitoring and Control System for Building Secure Systems,” Keiso, Vol. 58, No. 12, pp. 34–37 (Dec. 2015) in Japanese.

ABOUT THE AUTHORS

Hideki Osonoi

Control System Platform Design Department, Control System Platform Development Division, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of components for control systems.

Takahiro Ohira

Control System Platform Development Department, Control System Platform Development Division, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of middleware for control systems.

Kei Takezawa

Control System Platform Security Center, Control System Platform Development Division, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the marketing of cyber security in control systems.

Takuma Nishimura

Control System Platform Design Department, Control System Platform Development Division, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of components for control systems.

Daisuke Yokota

Control System Platform Development Department, Control System Platform Development Division, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of middleware for control systems.

Shunsuke Mori, Ph.D.

Infrastructure Systems Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of technology for data acquisition from control systems. Dr. Mori is a member of the Information Processing Society of Japan (IPSJ) and the Society of Instrument and Control Engineers (SICE).