Featured Articles

Information and Control Platforms for Globalization and Enhancement of Service Extensibility

Katsuhito Shimizu
Eiji Nishijima
Takahiro Ohira
Satoshi Okubo
Takuma Nishimura
Toshiki Shimizu

OVERVIEW: Work on the provision of the social infrastructure that underpins economic development continues in sectors such as urban development, energy, and railways, particularly in emerging economies. In developed economies, meanwhile, there is growing demand for updating the aging social infrastructure. These economies constitute a global market for information and control components and for the implementation of systems, particularly information and control systems, that need to operate reliably over long periods of time. This market is anticipated to grow in both activity and size. On the other hand, providing social infrastructure that imposes a low load on the environment and is efficient in terms of both energy and economics requires that this infrastructure be capable of being expanded in a variety of ways to satisfy demands for a steady stream of new services and functions, such as applications for big data based on information collected from infrastructure field[1]. Achieving this expandability places a high priority on using the latest IT and adopting open communication standards (including in information and control systems), and on making operations more intelligent. Given this background, Hitachi is developing technologies to boost the ability of its information and control platforms to be used globally, and to enhance the scope for expanding services through the use of the latest IT in information and control systems.

INTRODUCTION

HITACHI develops and supplies information and control platforms for use in information and control systems that support high availability and the long-term reliable operation of social infrastructure that needs to run non-stop. In recent years, Hitachi has been working to make its information control components compliant with international standards to improve its ability to satisfy procurement requirements, particularly in global markets.

Information and control systems require expandability and reliable operation that can continue to be supported over the long term. In the case of upgrades to social infrastructure, in particular, there is strong demand for reducing system maintenance costs and extending the life of existing software assets. Hitachi is working on the development of technology for server virtualization[2], which is increasingly being adopted for the information technology (IT) systems used in the latest information systems, to improve realtime performance in control applications.

It is already common practice in conventional information and control systems for operations to be initiated in isolation from the Internet or other external systems, and there has been demand in recent times for diverse service expansion capabilities to support new services and functions that connect to external systems. Hitachi is continuing to develop technologies that can help improve the safety and security of social infrastructure and service expandability. These include enhancements to control system security to counter the threat of cyber-attacks on information and control systems, and the development of small and rugged computers that can help with the adoption of intelligent operations.

CHALLENGES FACING SOCIAL INFRASTRUCTURE SYSTEMS AND HITACHI'S INITIATIVES

As described above, information and control platforms require expandability and reliable system operation that can continue to be supported over the long

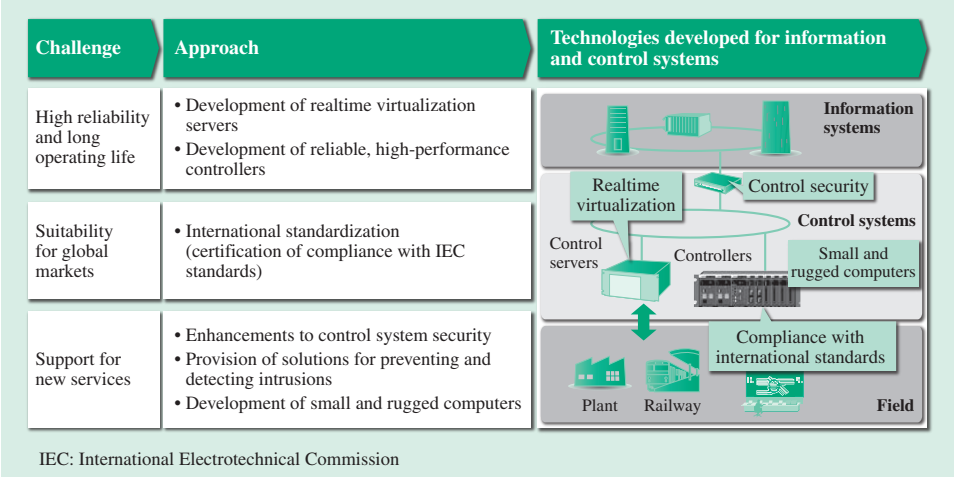


Fig. 1—Technologies being Developed for Information and Control Systems.
In developing technologies and products for information and control systems, Hitachi recognizes three particular challenges associated with satisfying the requirements for these systems and the changes in the circumstances surrounding them.

term. To become better able to satisfy procurement requirements in global markets, and to allow customers to create new services, it is important to strengthen security and enhance the scope for service expansion (see Fig. 1).

This article describes the following four technologies being developed by Hitachi to overcome these challenges.

(1) Realtime virtualization servers for control applications

(2) Certification of controller compliance with international standards

(3) Control system security that maintains control performance

(4) Small and rugged computers for making operations more intelligent

REALTIME VIRTUALIZATION SERVERS FOR CONTROL APPLICATIONS

Trends in Information and Control Servers, and Hitachi's Work on Server Virtualization

Hitachi's RS90 series of information and control servers feature long-term product availability and high reliability. They are used in information and control systems in a variety of industries, such as power generation and steel manufacturing.

Information and control systems have continued to get larger in recent years. Challenges include how to minimize maintenance costs and extend the life of software to keep pace with rapid advances in hardware and OSs. IT systems that feature high-level interoperation between different types of systems have become increasingly common in recent years in applications such as urban development and energy management. To reduce costs, these systems need the ability to grow into large and durable parts of the social infrastructure, being initially installed on a small scale and then progressively expanded. This requires information and control systems with a high degree of flexibility and expandability.

In information systems, meanwhile, server virtualization is widely used to help reduce maintenance costs. Server virtualization is a technique for running a number of virtual machines simultaneously on the same computer hardware (see Fig. 2). By running a proven OS on a virtual machine, virtualization allows the same OS to remain in use for a long period of time, even when the underlying computer hardware is upgraded. It can also cut maintenance costs by consolidating a number of servers with low loads on the same computer hardware.

Hitachi has implemented realtime virtual servers by developing realtime virtualization platform software for control use that allows virtual servers to satisfy information and control server requirements.

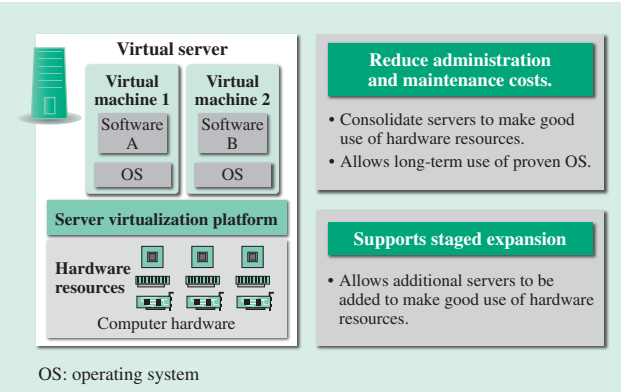


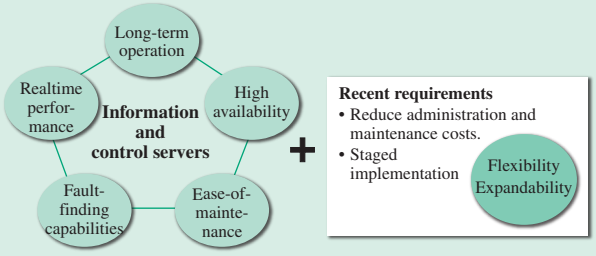
Fig. 2—Server Virtualization.
Virtualization allows a number of virtual machines to run on the same computer hardware.

Because information and control servers are used for the monitoring and control of plants, the conventional requirements include long-term operation (on the order of a decade), the realtime performance necessary for plant control, the ability for processing to continue even if a fault occurs on the server, a high level of availability to ensure reliable plant operation, fault-finding capabilities that can reliably isolate the cause of faults, and quick and reliable maintenance (see Fig. 3). The following sections describe the specific measures that Hitachi's realtime virtualization platforms use to satisfy these requirements.

Ensuring Realtime Control Performance on Virtual Machines

The realtime control performance required of information and control servers includes that processing be executed in a deterministic order, that it produces predictable results, starts at the required time intervals (regularity), and has low latency (meaning a short delay between the request to execute a process and the commencement of its execution). With the server virtualization used for conventional information systems, however, processing conflicts occur when a number of virtual machines are running concurrently. Also, access to physical hardware by software running on a virtual machine is emulated by the server virtualization platform, causing problems with variable latency due to delays in execution of the software on the virtual machine.

Accordingly, the new realtime virtualization platform developed by Hitachi provides a resource partitioning mechanism whereby virtual machines can reserve exclusive access to hardware resources (processors, disks, and network devices). This eliminates processing conflicts when virtual machines are running concurrently. Similarly, the latency of software execution on a virtual machine is kept within a fixed time by having the realtime virtualization platform run on a different processor core than those used to execute software on virtual machines. This overcomes the problem of server virtualization causing variable latency and, together with other measures to ensure predictability and regularity, ensures realtime control performance for the software running on virtual machines (see Fig. 4).



Requirement	Description
Long-term operation	Because servers operate alongside the plant they monitor and control, they need a life of around 10 years.
Realtime performance	High level of (predictable, regular, and low-latency) realtime performance needed to ensure control processing executes reliably on a time scale suitable for the time constant of the plant.
High availability	Switchover to the backup system when a fault causes a shutdown needs to occur on the order of seconds, without interfering with plant monitoring and control.
Fault-finding capabilities	Ability to identify and resolve the causes of faults is needed to maintain reliable operation of field.
Ease-of-maintenance	Ability to perform server maintenance quickly and accurately during short shutdown periods is needed to ensure high plant utilization.
Flexibility, expandability	Flexible server consolidation is needed to reduce server administration and maintenance costs. The expandability to allow staged implementations starting from a small system is needed to minimize initial installation costs.

Fig. 3—Requirements for Information and Control Servers. In addition to such requirements as long-term operation and high availability, these servers also need better flexibility and expandability.

Ensuring High Availability of Virtual Machines

Information and control systems have achieved improved availability and ensured processing continuity by using redundant configurations for information and control servers so that software execution can rapidly switch over to different computer hardware in the event of a fault. Likewise with virtualization, redundant configurations are used for the computer hardware that hosts the virtual information and control servers to ensure high availability by allowing rapid switchover.

In the past, reliable and rapid switchover has been achieved by using the reset mechanism provided by the computer hardware to shut it down after a fault is detected. Hitachi's realtime virtualization platform also supports use of the reset mechanism for rapid switchover. Furthermore, Hitachi's realtime virtualization platform has a mechanism for resetting a single virtual machine on which a fault has occurred in cases when a number of virtual machines are running on the same physical computer. In this mode, only the faulty virtual machine switches to the backup physical computer, with all other virtual machines continuing to execute without switchover [see Fig. 5 (1)]. This minimizes the impact on execution of the other virtual machines where no fault has occurred.

When information and control servers with a redundant configuration are shutdown to perform

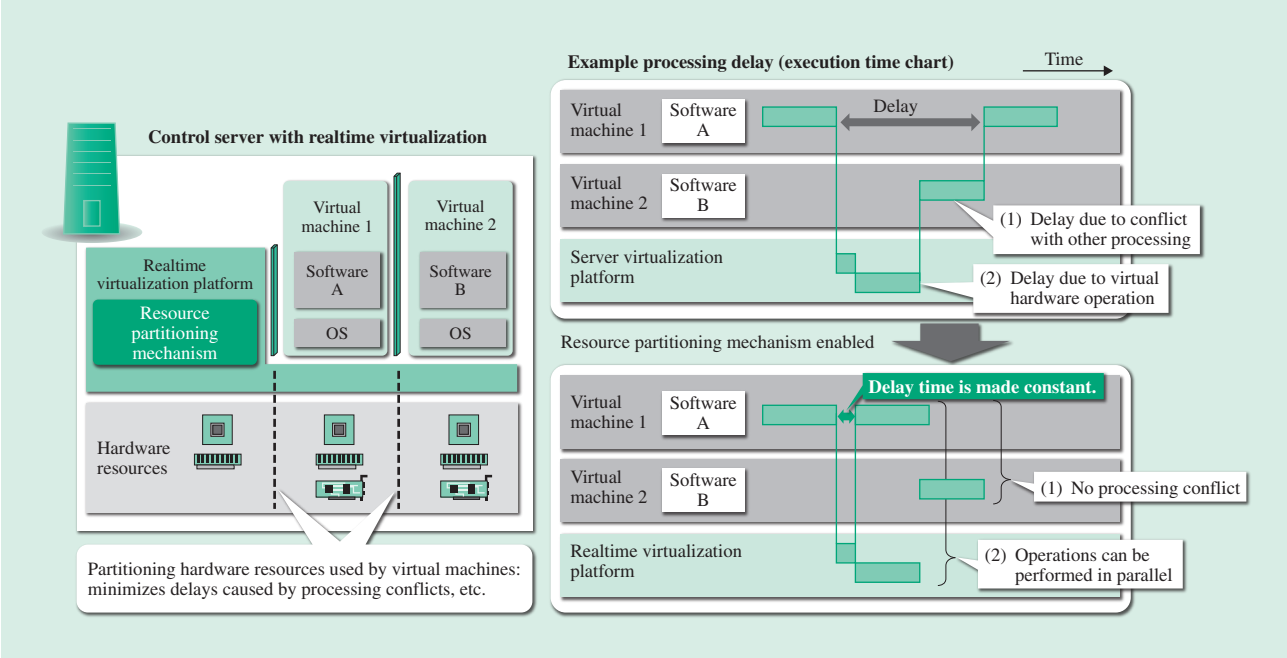


Fig. 4—Ensuring Realtime Control Performance.
The diagram shows the benefits of the resource partitioning mechanism in Hitachi's realtime virtualization platform. In the time chart on the top-right, the completion of software A is delayed for two different reasons [(1) and (2)]. In the time chart on the bottom-right, where the resource partitioning mechanism is used, the processing delay for software A is made constant.

maintenance tasks such as software updates, it is common practice to shut them down one at a time so that there is at least one server operating at all times, preventing any interruption to the operation of the plant. To achieve this, Hitachi's realtime virtualization platform allows individual virtual machines to be shut down manually. On the other hand, when switchover of virtual machines is performed one at a time, maintenance work such as replacing computer hardware parts is made difficult when the same physical computer is running both active and backup virtual machines. Accordingly, to improve operational efficiency, the realtime virtualization platform also has a mode for automatically switching over all virtual machines on a physical computer at the same time.

Improvements to Fault-finding on Virtual Servers

Because server virtualization requires a number of virtual machines to execute concurrently with the virtualization platform software, fault-finding can be made more difficult by problems such as processing delays. Similarly, because each virtual machine, as well as the virtualization platform software, operates on its own time frame, collecting trace logs and reviewing operational information in time sequence can be difficult.

Hitachi's realtime virtualization platform provides an integrated trace mechanism that allows all trace logs to be viewed in time sequence. This provides a common overview of operations in a particular virtual machine, the realtime virtualization platform, and the other virtual machines so that the cause of an execution delay can be identified more quickly [see Fig. 5 (2)].

Quick and Accurate Maintenance on Individual Virtual Machines

It is common practice in information and control systems to use comparatively small servers, with a separate information and control server assigned to each control function or item of the plant being controlled. As a result, software backups are typically performed by making a full system backup of the information and control server. Because virtualization environments consisting of multiple virtual machines will likely require software maintenance to be performed on individual virtual machines, Hitachi's realtime virtualization platform allows system backups to be performed separately for each virtual machine [see Fig. 5 (3)].

Since backups typically involve transferring large amounts of data from the disk to a backup storage device, it is necessary to ensure that this does not interfere with the operation of other virtual machines.

To achieve this, a mode is provided that uses the resource partitioning mechanism described above to limit the processor time, disk access bandwidth, and other resources available for the backup. This allows quick and accurate maintenance to be performed individually for each virtual machine.

CERTIFICATION OF CONTROLLER COMPLIANCE WITH INTERNATIONAL STANDARDS

As safety and security requirements for controllers are becoming stricter, Hitachi has been developing products that comply with the associated international standards.

International standards for the safety and security of controllers certify aspects such as functional safety, electrical safety, electromagnetic compatibility (EMC), and control system security. Hitachi is developing products that comply with these standards.

The following sections describe the development of controllers that comply with functional safety standards.

R800FS Functional Safety Controller

Hitachi has developed the R800FS functional safety controller and functional safety remote input/output (RI/O), which comply with the IEC 61508:2010 Edition 2.0[3] functional safety standard. R800FS Version 1 was certified by TÜV Rheinland Industrie Service GmbH of Germany in 2010.

Functional safety standards require that hardware failure and self-diagnosis rates satisfy the required levels, and certify that development processes guarantee that software will not include design faults that threaten safety. They also require a fail-safe design ensuring that the control output signal to the plant defaults to a safe value when a fault occurs.

Since the R800FS can combine both functional safety programs required by systems such as those used to ensure safety, and general programs used for ordinary control systems and information processing, it can provide highly flexible control functions in which these complement each other. Functional safety programs execute in parallel on the two microprocessors in the R800FS's central processing unit (CPU). Safe computation and control output are

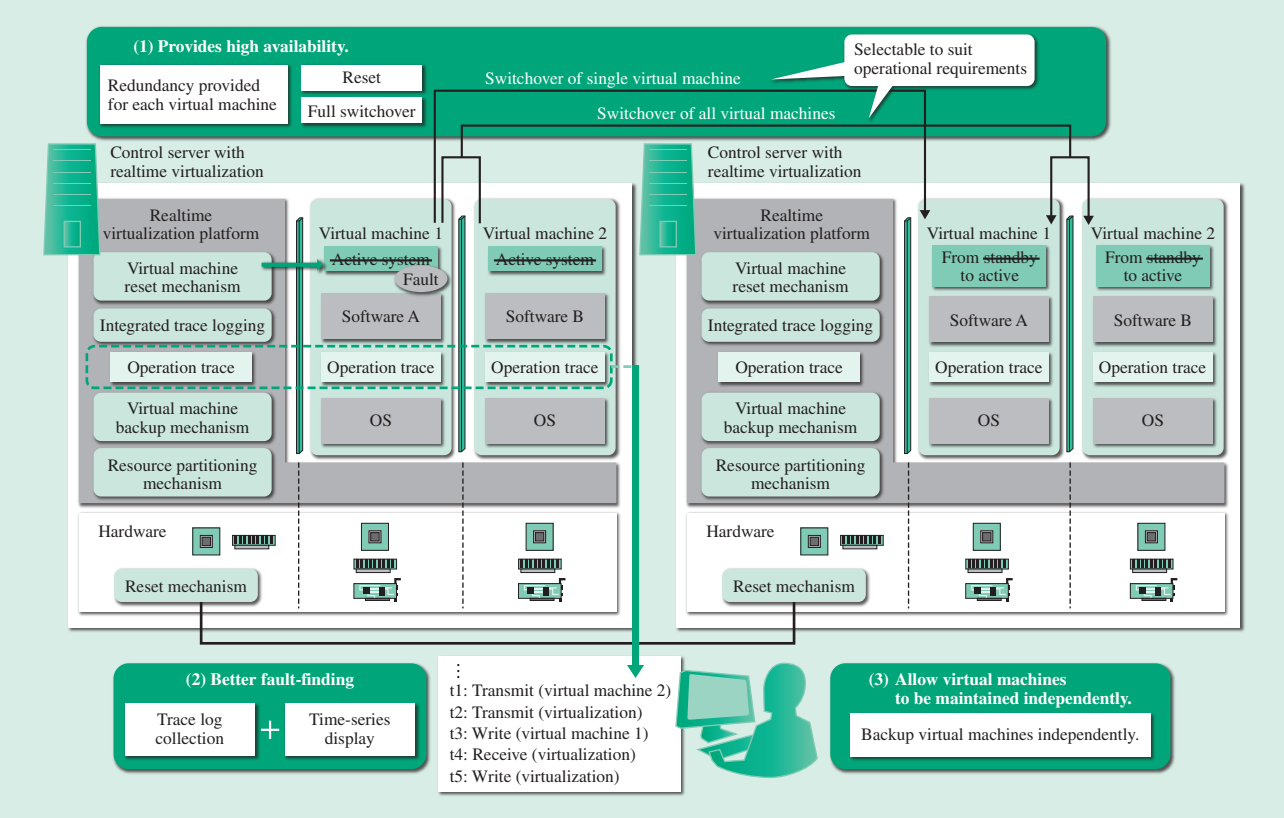
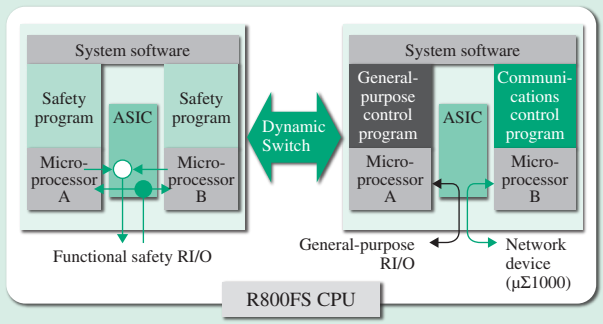


Fig. 5—Improvements to Availability, Fault-finding Capabilities, and Ease-of-maintenance.
The reset mechanism is used to achieve high-speed switchover, the integrated trace mechanism to facilitate analysis, and the resource partitioning mechanism to improve maintenance.



CPU: central processing unit
ASIC: application-specific integrated circuit RI/O: remote input/output

Fig. 6—R800FS CPU Support for Both Functional Safety and General-purpose Control.
Using two microprocessors improves the rate of diagnosis and allows both functional safety control and general-purpose control calculations to coexist.

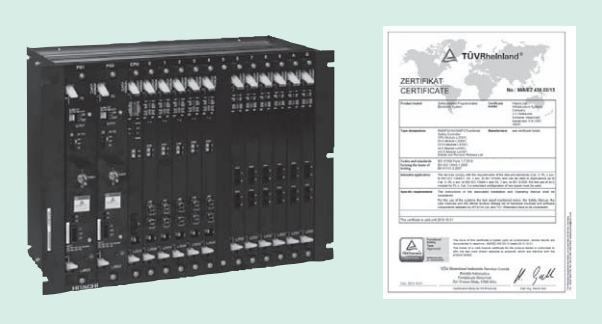


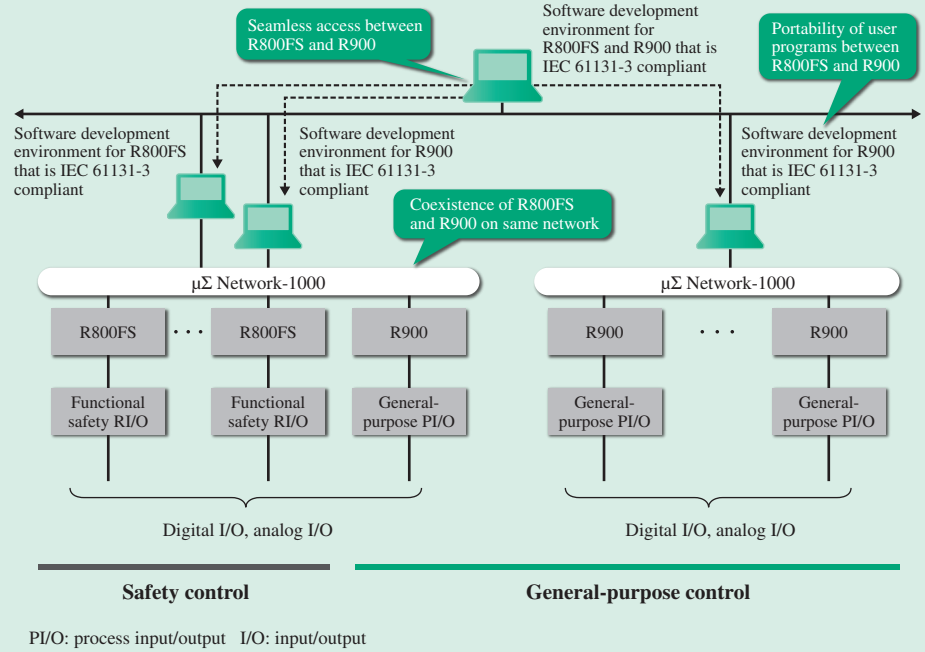
Fig. 7—CPU Unit of R800FS Functional Safety Controller (left) and Certificate from TÜV Rheinland (right).
Version 2 of the R800FS, which features enhanced performance, received updated certification in 2013.

achieved by using a comparison function implemented in an application-specific integrated circuit (ASIC) to check the intermediate values and results of these computations. For general programs, on the other hand, flexible high-speed processing is provided by the multiprocessor. The functional safety RI/O, meanwhile, achieves a high rate of self-diagnosis by using an ASIC with dual internal circuits to compare inputs and outputs (see Fig. 6).

R800FS Version 2 Designed for Better Availability, Maintenance, and Performance

Although halting control outputs when a fault occurs is fundamental to the concept of functional safety, it can result in a loss of plant availability. In response to this problem, Hitachi developed Version 2 of the R800FS to improve availability and ease-of-maintenance by enabling control to continue operating safely in the event of a fault. It received updated certification from TÜV Rheinland in 2013 (see Fig. 7).

The R800FS uses remote communications between the CPU and RI/O, with availability improved by using fully redundant communication paths over a ring topology. To prevent multiple overlapping faults, Version 2 has a function for the early detection of faults that retrieves fault information from all modules, including non-intelligent communication modules. To make maintenance easier, it also has functions to detect incorrectly connected communication lines and the locations of line breaks.



PI/O: process input/output I/O: input/output

Fig. 8—Unified Architecture.
The architecture allows the seamless incorporation of functional safety and the implementation of highly expandable systems.

Safe communications is used for the remote communications between the CPU and RI/O. Normally, the safety layer of processing used to achieve safe communications is performed by software, involving more processing than conventional communications. To improve performance, Version 2 of the R800FS implements the safety layer in the hardware. This enables parallel processing using both software and hardware, which improves performance by more than 50% over R800FS Version 1.

Certification has also been obtained under the UL 61131-2 and CAN/CSA E61131-2 electrical safety standards, and the product also complies with the environmental and EMC requirements specified in IEC 61131-2, and the functional safety EMC requirements of IEC 61326-3-1.

Unified Architecture Enabling Flexible System Configuration

The R800FS functional safety controller is able to connect to the same control networks as devices such as the R900 general-purpose controller, industrial personal computers (PCs), and information and control servers, and exchange data with these devices. It also supports software portability for user programs, using an integrated software development environment with an IEC 61131-3 compliant programming language. This improves usability and smoothes the adoption of functional safety in information and control systems, supporting the development and operation of safe information and control systems that are also more expandable (see Fig. 8).

CONTROL SYSTEM SECURITY ENSURING CONTROL PERFORMANCE

Concepts and Overview of Control System Security

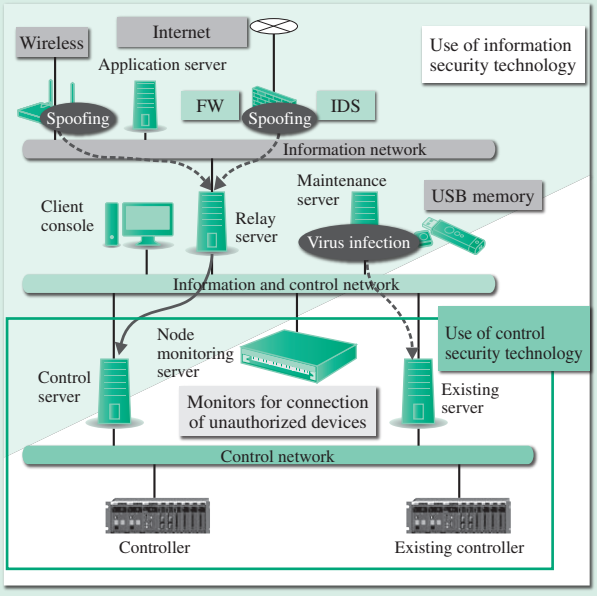
The vulnerability of information and control systems to cyber-threats has been highlighted in recent years by the Stuxnet incident in which malware was targeted at a control system. This has prompted the expediting of moves to formulate international standards for control system security, with certification under these standards increasingly being stipulated in procurement rules. In Japan, the Embedded Device Security Assurance (EDSA) security certification scheme for control devices has started by the Control System Security Center (CSSC).

Information and control systems need to remain in operation for long periods of time, during which they may be retrofitted with additional equipment or functions. They combine a wide variety of different systems, ranging from controllers to information and control servers, IT servers, and database systems, using system configurations that are optimized for the operation of each in-service system. Accordingly, ensuring the cyber-security of information and control systems requires that they incorporate information security products such as firewalls and intrusion detection systems (IDSs), control security components that comply with international standards and have international certification, and information and control network security products that can support the long-term operation of control systems (see Fig. 9).

EDSA Certification for Control Security Components

EDSA certification is a certification scheme for assuring the security of control components administered by the International Society of Automation Security Compliance Institute (ISCI). It defines the criteria for different levels of security (see Table 1).

The communication robustness test (CRT) is performed on equipment to verify that a predefined list



FW: firewall IDS: intrusion detection system
USB: universal serial bus

Fig. 9—Example Application in Control System.
The system supports both information security technology and control security technology.

TABLE 1. EDSA Certification Criteria and Assessment Level
EDSA certification defines the criteria for assessment levels that represent the strength of security.

Test	Description	Assessment level		
		Level 1	Level 2	Level 3
CRT	Communication robustness test	69	69	69
FSA	Functional security assessment	21	50	83
SDSA	Software development security assessment	129	148	169

EDSA: Embedded Device Security Assurance

of essential services (such as the continuity of control calculations) can continue to function either while an attack from a communication link is in progress or after the attack ends. Specifically, the equipment being tested is connected to the network along with human-machine interface (HMI) devices and the continuity of essential services is verified using the data displayed on the HMI and the control outputs from the process input/output (PI/O).

A functional security assessment (FSA) uses equipment testing and documentation to verify whether security function requirements are satisfied at a system level.

A software development security assessment (SDSA) models security threats in terms of the security requirements and uses documentation to verify whether the design and review processes throughout the software development lifecycle cover these threats.

Security Products for Information and Control Networks

Because the equipment used in information and control systems remains in service for a long time and is subject to modifications after the system commences operation, such as upgrades to equipment and functions, it is common for old and new equipment to coexist. This makes it difficult to maintain security simply by installing individual components with standalone security support.

Along with the use of firewalls and IDSs to prevent intrusion by external attacks, other effective techniques include monitoring changes in equipment configuration to identify which devices are permitted to connect to the network, blocking those components that are not needed, and early detection and response to infections or other attacks. For example, Hitachi's node monitoring server continuously monitors the network for the connection of unauthorized devices and issues a warning to the security operation system when one is detected.

SMALL AND RUGGED COMPUTERS FOR MAKING OPERATIONS MORE INTELLIGENT

Requirements for Making Operational Systems More Intelligent, and Hitachi's Initiatives

Social infrastructure systems that require high reliability and availability are creating new requirements with an operational focus, including the provision of a variety of services that are closely integrated with infrastructure operation and the utilization of detailed and up-to-date information from the field. To satisfy these requirements, Hitachi is working on initiatives aimed at making operations more intelligent.

The on-board display systems on trains, for example, need to provide passengers with a wide variety of information, not only accurate realtime service information but also things like news, advertising, and weather reports. This system requires the installation of small computers that process this diversity of display data in the confined space inside a train ceiling. Accordingly, these computers need to be not only small but also capable of operating in harsh environments, including the vibration from the moving train as well as temperature highs and lows, and condensation during wet weather, that occur when the train is out of service.

Similarly, the power monitoring devices used in smart grids may be installed on the tops of power poles where they experience harsh outdoor temperature and humidity conditions, or close to transformers where electrical noise levels are high. The controllers for industrial robots operate in production plants, where they often experience significant vibration, sulfur-containing or other corrosive gases, or high levels of dust. Also, because equipment such as power monitoring devices and industrial robot controllers is located in places where installation and replacement work is difficult, it is important that it operates reliably for long periods of time. As making operations more intelligent results in devices being installed in a wider range of sites, the demands for making them rugged enough to withstand these environments will become more diverse.

Development of Small and Rugged Computers

Hitachi has developed the above-mentioned small computers for train display systems and embedded computers for use in substations in the past. In response to the growing and increasingly diverse

TABLE 2. Small and Rugged Computer Specifications
The table lists the main specifications of the small and rugged computers developed by Hitachi.

Parameter		Specification
Processor (SoC)		Intel*1 Atom*1 processor (1.46 GHz) (1 core, 1 thread)
Memory	Main memory	2 Gbyte DDR3L-SDRAM with ECC
	Non-volatile memory	512 kbyte MRAM
Graphics	Controller	Integrated in SoC
	Graphics memory	Shares main memory.
	Display resolution	2,560 × 1,600 max. (WQXGA)
	Colors	16,700,000 (24 bpp)
File storage	CFast slot	CFast slot × 1 (replaceable from front panel)
I/O interface	Display	1 × display port
	USB port	1 × port (USB 3.0, USB A type connector) 3 × ports (USB 2.0, USB A type connector)
	LAN port	3 × ports (1000 Base-T, Wake-on-LAN)
RAS functions		LED, WDT, etc.
Supported OSs		Hitachi customized Linux*2 (planned)
BIOS		EFI

SoC: system on a chip DDR: double-data-rate
SDRAM: synchronous dynamic random access memory
ECC: error check and correction
MRAM: magnetoresistive random access memory
WQXGA: wide quad extended graphics array bpp: bits per pixel
LAN: local area network RAS: reliability availability and serviceability
LED: light-emitting diode WDT: watchdog timer
BIOS: basic input/output system EFI: extensible firmware interface
*1 Intel and Intel Atom are trademarks of Intel Corporation in the U.S. and/or other countries.
*2 Linux is a registered trademark of Linus Torvalds.

demand for ruggedized devices, Hitachi has embarked on the development of small and rugged computers that satisfy the following seven requirements.
(1) Wide operating temperature range (−10 to +60°C)
(2) Small size: 210 mm (W) × 70 mm (H) × 225 mm (D)
(3) Sealed, environment-proof design
(4) 10-year life with continuous 365-days-a-year operation
(5) Fanless (natural air cooling) design to eliminate need for replacing parts
(6) No hard disk drive (HDD) for better tolerance of vibrations
(7) Use of memory error checking and correction (ECC) for better reliability

For the new small and rugged computer, Hitachi uses small, high-performance system-on-a-chip (SoC) devices with low power consumption that includes a memory ECC function to reduce heat dissipation and allow the use of a sealed design. In addition, using thermal fluid analysis to check the component layout under natural air cooling conditions and minimizing hot spots, Hitachi also optimized the metal housing itself to incorporate measures for dealing with heat that took account of the 10-year product life, including using conduction to dissipate the heat from the SoC. These measures succeeded in achieving a sealed, fanless design with a 10-year life.

Fig. 10—Small and Rugged Computer.
Hitachi's small and rugged computers use a proprietary metal case design with excellent heat dissipation. The connectors and LEDs are located on the front panel for easier maintenance.

To achieve reliable operation in environments with a high level of vibration, these small and rugged computers do not include mechanical components that are vulnerable to vibration or shock. Instead they use a CFast* card for file storage. All plug-in connectors and light-emitting diodes (LEDs), including the CFast slot, are located on the front panel to improve maintenance, such as installation or replacement, unplugging of cables, or checking LED indicators (see Table 2 and Fig. 10).

CONCLUSIONS

This article has described the recent challenges facing the information and control systems that support the reliable, long-term operation and high availability of the social infrastructure, and the associated technological developments. Hitachi draws on its accumulated know-how to overcome the technical challenges of supporting a safe and secure social infrastructure in the face of rapidly changing IT and service expansion requirements, while also taking an active approach to incorporating the latest IT into its information and control systems.

Hitachi intends to continue developing technologies to help achieve a high-quality social infrastructure that is safer and more secure.

* CFast is a registered trademark of CompactFlash Association.

REFERENCES

(1) T. Mizuno, "Statistical Analysis of Socio-Economic Phenomena Using Big-Data- Econophysics," Research Report Knowledge System (ICS), 2014-ICS-173 (4), 1-3 (Jan. 2014) in Japanese.
(2) K. Seino, "Fundamentals and Technology of Virtualization," Shoeisha (2011) in Japanese.
(3) "Functional Safety of Electrical/electronic/programmable Electronic Safety-related Systems," IEC 61508 2nd edition (Apr. 2010).

ABOUT THE AUTHORS

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

Eiji Nishijima
Software Platform Research Department, Information Platform Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of software platforms for social infrastructure. Mr. Nishijima is a member of the The Institute of Electrical Engineers of Japan (IEEJ) and the Information Processing Society of Japan (IPSJ).

Takahiro Ohira
System Engineering Development Department, Control System Platform Development Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of middleware for information and control systems.

Satoshi Okubo
Control System Platform Design Department, Control System Platform Development Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of security for information and control systems.

Takuma Nishimura
Control System Platform Design Department, Control System Platform Development Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of components for information and control systems.

Toshiki Shimizu
Control System Platform Design Department, Control System Platform Development Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of components for information and control systems.