# Integrated Security Monitoring Solutions for Social Infrastructure

A recent rise in cyberattacks (including targeted types on specific companies and organizations) has resulted in damage to some of the infrastructure systems that underpin society and is making security measures to protect social infrastructure from these attacks increasingly important. Hitachi has released the Hitachi Anomaly Detector, a technology for early detection of cyberattacks that provides real-time intrusion detection. It is also working on verifying and applying a set of integrated monitoring solutions designed to assist in making business continuity decisions and formulating primary responses after a breach is detected, and is active in security monitoring response work around the world. This article looks at Hitachi's integrated security solutions designed to prevent damage through early detection of cyberattacks.

**Tsuneo Iida, P.E.Jp**
**Hiromi Harada**
**Daiki Nozue**
**Masashi Ohmori**
**Guillaume Daleux**

## 1. Introduction

Early detection of unauthorized intrusions is a key requirement for preventing cyberattack damage. Security breaches can be prevented by monitoring communications found when worm-type malware like WannaCry start to spread, or monitoring communications generated at times such as when the attackers behind targeted attacks engage in a series of concealment behaviors.

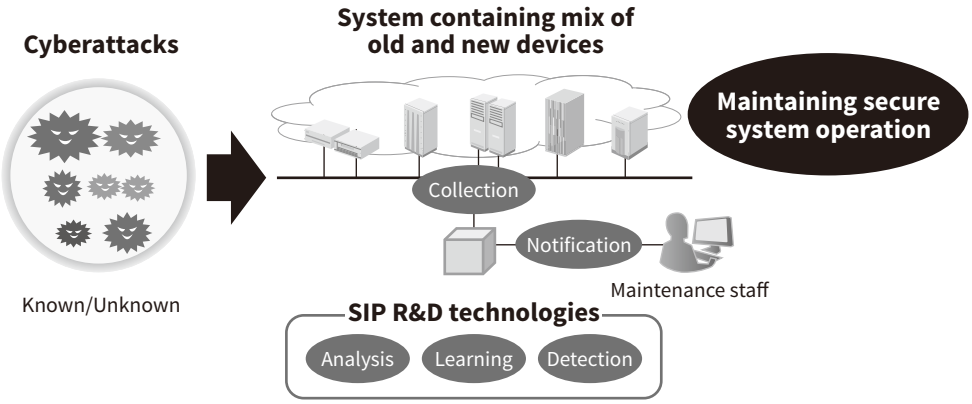
As one approach to detecting unauthorized intrusions, Hitachi has created technology for the real-time detection of breaches in control systems used in applications such as social infrastructure. The technology has been released as the Hitachi Anomaly Detector, and is discussed below in Section 2.

After threat detection technologies have detected a breach or similar incident, the primary response and business continuity decision are important requirements for social infrastructure systems in which secure operation is top priority. Section 3 describes example applications of Hitachi's integrated monitoring solutions used to assist these processes.

The importance of worldwide security monitoring responses is growing as social infrastructure systems become increasingly global. Section 4 looks at the security monitoring work Hitachi is doing around the world.

**Figure 1 — Overview of Developed Technologies**

Technologies for control system operation monitoring are provided in an easily connectable configuration.




SIP: Cross-ministerial Strategic Innovation Promotion Program R&D: research & development

## 2. Hitachi Anomaly Detector

### 2. 1
### Development Background

Control systems in facilities such as the key infrastructure that underpins society were once considered to have low exposure to security threats due to the closed environment of the networks they run on. But this threat exposure level is growing along with the rise of the Internet of Things (IoT). Research & development (R&D) work to ensure cybersecurity for these facilities is being done as part of an initiative called the Cross-ministerial Strategic Innovation Promotion Program (SIP) created by Japan's Cabinet Office and organized by the New Energy and Industrial Technology Development Organization (NEDO). Hitachi has released the Hitachi Anomaly Detector[(1)] by applying the project's technical findings (see **Figure 1**).

### 2. 2
### Challenges Facing Security Measures

Targeted attacks against specific companies and organizations have recently been on the rise, and damage to control systems once considered secure is growing. Work on security measures to protect against cyberattacks on control systems is therefore needed. But since the challenges facing control systems are different from those facing information systems, it is difficult to respond with conventional security technology that is designed for information systems.

Some of challenges unique to control systems are: (1) it is difficult to install products inside systems and assess effects because they require deployment without service outages; (2) it is required to support devices running on old operating systems unsuited to software additions, and devices with limited resources; and (3) it is required to accommodate the use of proprietary protocols. There is an urgent need for security measures that can accommodate these demands.

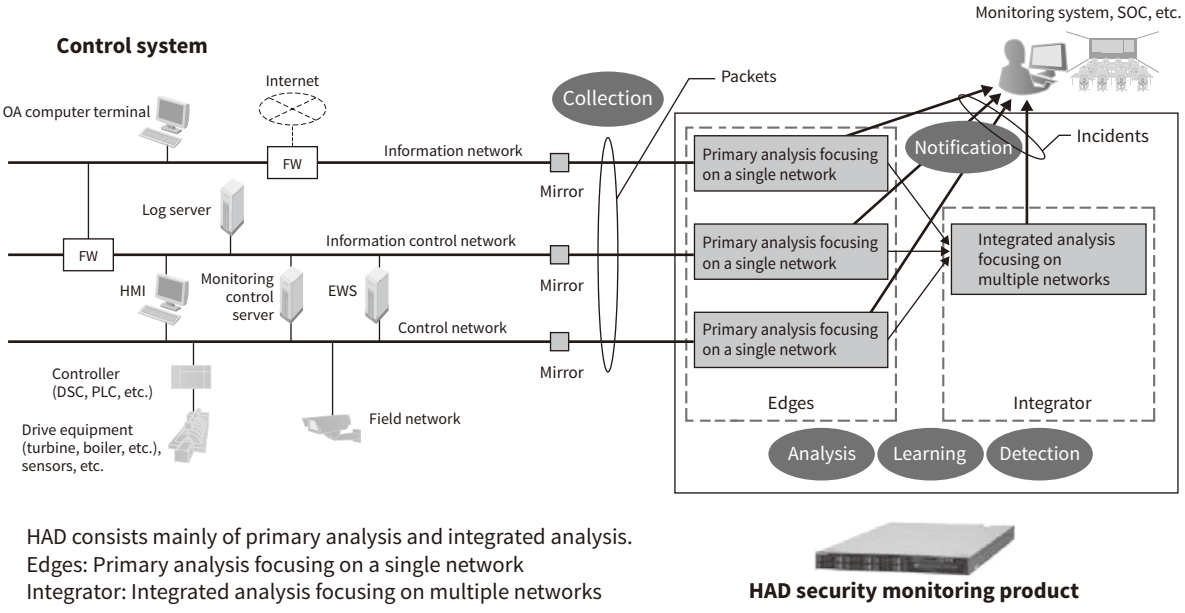
### 2. 3
### Product Features

Hitachi worked on the technology development and implementation configuration needed to solve the challenges unique to control systems and developed a threat detection product. To enable easy product installation without affecting normal operation or causing service outages, it adopted a configuration implemented by network tap/switch port mirroring for the existing network, with monitoring of the network from outside (see **Figure 2**). This approach provides the following benefits: (1) it is deployable without service outages; (2) no additional software is needed in existing devices; and (3) it is independent of the communication protocol.

Using this configuration requires sophisticated technology for detecting advanced cyberattacks and

**Figure 2 — Logical Configuration of Overall System**

The system is connected to control network mirror ports, collects data on system operations, analyzes and learns normal system operations, and detects operational anomalies.




OA: office automation FW: firewall HMI: human-machine interface EWS: engineering workstation DSC: diameter signaling controller PLC: programmable logic controller
SOC: security operations center HAD: Hitachi Anomaly Detector

unknown threats in real-time from the behavior of data on the network. Hitachi has developed a multilayer detection algorithm that compares communications in normal system operation with real-time communications to identify unusual communication behavior, and recognizes threats such as probe behaviors by cyberattacks or springboard attacks. The multilayer detection algorithm enables real-time detection with the capability of fine tuning, and can detect advanced cyberattacks and unknown threats.

The product learns normal system operations automatically from the communications on the network, eliminating the need to register the system's normal data in advance, and making the product easy to adapt to existing systems. Beside learning automatically, the product supports operators in modifying learned models manually.

Currently, the product supports edge deployment connected to individual networks, but R&D is now being done on functions to detect suspicious behaviors spanning multiple edge networks.

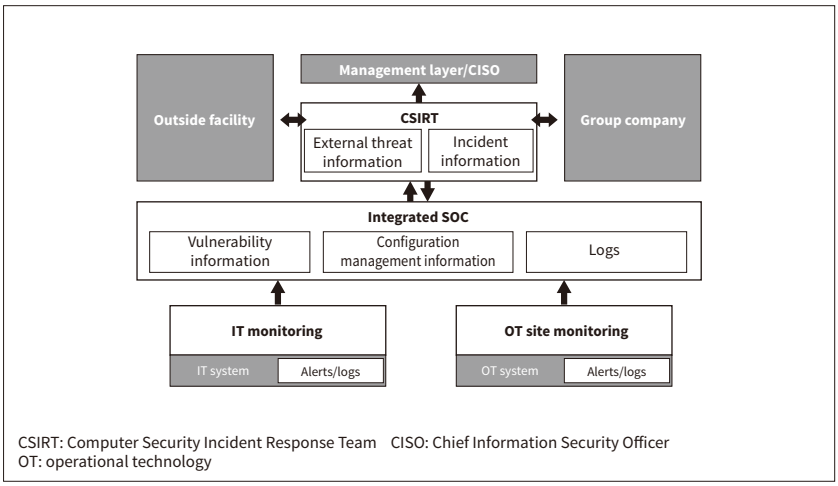
## 3. Integrated Monitoring Solution Application Examples

### 3. 1 Continuous Monitoring of Control System Security

The recent rise in the risk of cyberattacks on infrastructure systems has been accompanied by a rise in the sophistication and complexity of the attack methods used. The same type of security measures used for information systems (IT systems) also need to be deployed in control systems (operational technology systems, OT systems), but the difficulty of shutting down OT systems makes it difficult to frequently deploy security measures that require system updates. Therefore, today's security solutions need to monitor the system continuously and respond to cyberattacks that evolve on a daily basis while verifying the effectiveness of the security measures used.

Hitachi has developed security monitoring solutions for control systems by drawing on its many

**Figure 3 — Integrated Security Monitoring Approach**
Hitachi's proposed approach to integrated security monitoring is shown below.




CSIRT: Computer Security Incident Response Team CISO: Chief Information Security Officer
OT: operational technology

years of technology and expertise in OT systems and its experience in applying IT system monitoring services[2].

### 3. 2
### Assisting Business Continuity Decisions through Early Incident Detection/Primary Response

Security monitoring has traditionally been handled by using a security operations center (SOC) to centrally monitor the entire system. But OT systems also require on-site decisions to be made at locations such as plants or production lines to keep facilities running, and recent collaboration between IT and OT systems have resulted in security attacks spreading from IT to OT. In response, Hitachi proposed a method that divides the security monitoring work between the site and the integrator (see **Figure 3**). Working together, the site and integrator deploy primary responses when incidents are detected at the site, tailoring each response to the nature of the incident, its scope, and its effect on operations. The integrator executes a policy of gathering information and IT system statuses from the site and information from outside facilities, analyzing these inputs in an integrated manner to issue instructions on basic responses.

### 3. 3
### Verification Using In-house IT + OT Environment

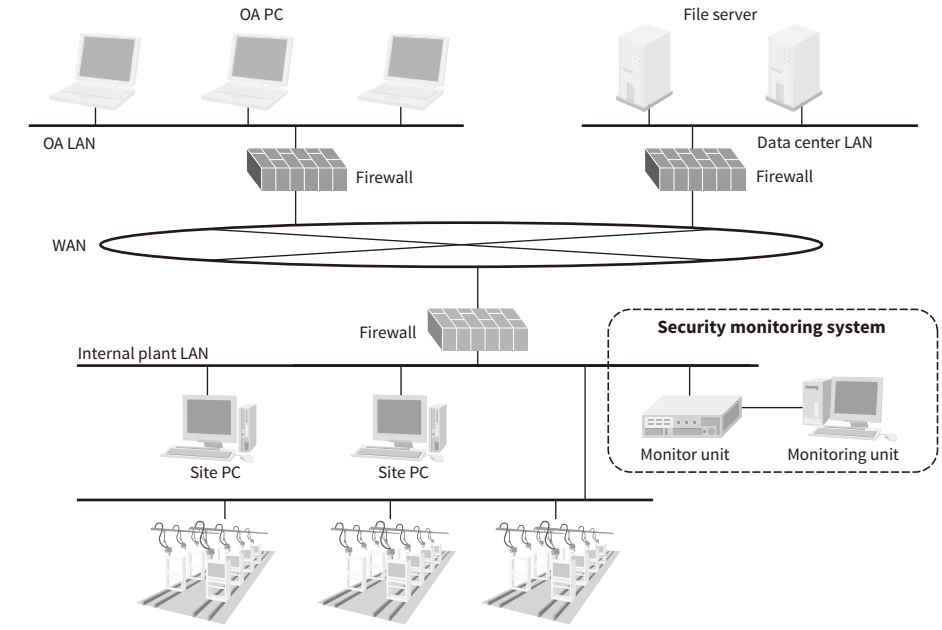
Hitachi is currently verifying its control system security monitoring solutions using one of its own plants. **Figure 4** shows the configuration of the verification system. The security monitoring system is composed of a monitoring unit used to monitor the local area network (LAN) in the plant, and another monitoring unit that monitors and analyzes the logs of the first unit. This configuration can detect incidents such as unauthorized PC connections to the plant's LAN, and notify the site's maintenance staff.

To respond to a broad range of attack patterns such as breaches that spread from IT to OT systems, Hitachi is now working on verifying its integrated security monitoring solutions through measures such as IT-OT log correlation analysis and vulnerability management done by comparing security vulnerability information from outside sources with system configuration information to detect vulnerabilities in the system.

## 4. Global Security Monitoring Work

### 4. 1
### Globalization of Threats

The IT that underpins business infrastructure is playing a key role as a business driver in becoming more globalized. It makes business possible worldwide and around the clock in an environment of interconnected overseas bases. However, IT management throughout multiple bases and differences in user IT literacy rates often result in varying levels of information security risk. Unless this situation is addressed, overseas bases with low levels of security can become entry points for attacks, with damage spreading throughout the world rapidly. A worldwide approach to monitoring security and coordinating with each other is a key factor from the standpoint of business continuity.




WAN: wide area network LAN: local area network

**Figure 4 — Plant Verification System Configuration**

The system configuration used to verify Hitachi's control system security monitoring solutions is shown below.

The Hitachi Systems Group (Hitachi Systems and Hitachi Systems Security) provides an SOC service to clients in 45 countries. It is provided through four worldwide bases and supports four languages (English, French, Spanish, and Japanese)[3] (see **Figure 5**).

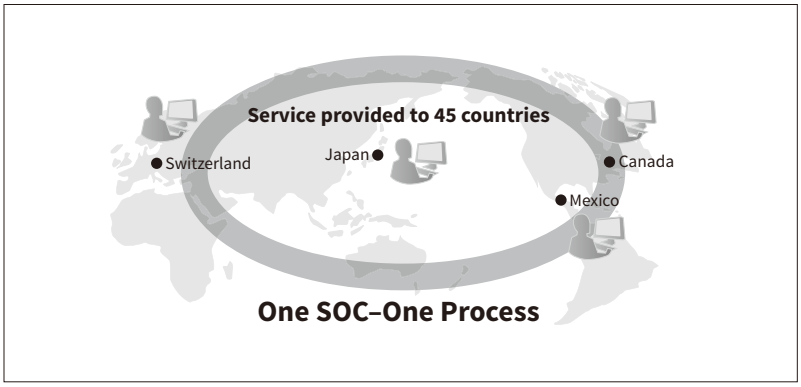
### 4. 2
### Real-time Monitoring and Correction of Security Level in Each Region

The SOC service provided by Hitachi Systems can be thought of as an IT security doctor for clients. The role of SOC providers is to help make improvements to client security by monitoring it to ensure a safe level.

Keeping security risks at the optimum level requires responses to be made effectively after the current state of each region's security risks have been recognized and information has been coordinated with responders. Hitachi Systems' security monitoring service enables separate security risk management for each IT asset in each region and department, providing views that let managers identify problems visually and quantitatively. Security risks change along with trends in the outside world and with system conditions, making it unrealistic for busy managers to continually monitor conditions. The service provides a system that reports problems and recommended responses to managers in real time for IT assets that have exceeded an appropriate risk level.

**Figure 5 — Worldwide SOC Bases Provided by Hitachi Systems Group**

Bases at four locations throughout the world provide operation that enables efficient turnaround of business processes using the same SOC operation platform for all four bases. The approach is described by the service's slogan, One SOC–One Process.



### 4. 3
### Bringing Together People, Processes, and Technologies

Providing high-quality service throughout the world requires an operation model that closely intertwines processes to enable the four SOC bases to make effective use of technologies and people. Hitachi Systems provides the service using the Intelligent Security Management Platform, ArkAngel, developed by Hitachi Systems Security as a way of efficiently and organically coordinating people, processes, and technologies. ArkAngel is a knowledge-base platform that enables maximum use of the expert knowledge of security analysts. It has functions needed to provide the service, organized around a core of functions for correlatively analyzing a large number of security events. Service is provided with no loss of quality by operating this platform using the same process, and based on knowledge gathered from around the world by security analysts with experience and expertise (see **Figure 6**).

Hitachi Systems will continue to improve service features, drawing on the strengths that Hitachi possesses as a corporate group developing business worldwide.

## 5. Conclusions

This article has looked at Hitachi's solutions for protecting social infrastructure, presenting real-time intrusion detection technologies for control systems, integrated monitoring solutions that assist in primary responses and business continuity decisions after breaches are detected, and its global security monitoring work.

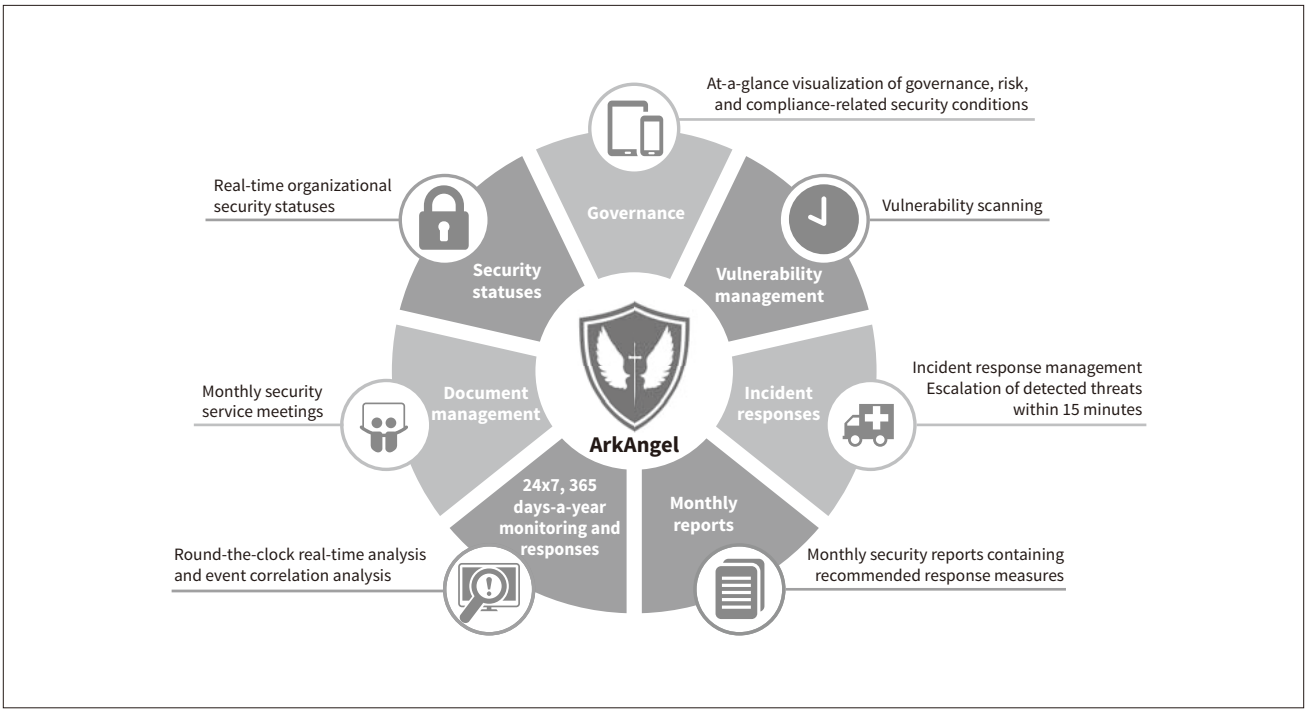
Hitachi will continue to work on developing the latest technologies, providing solutions designed to ensure secure and worry-free social infrastructure.

### Acknowledgments

The Hitachi Anomaly Detector presented in Section 2 of this article is a software product developed by Hitachi based on R&D findings. This work was supported by the Council for Science, Technology and Innovation (CSTI) and the Cross-ministerial Strategic Innovation Promotion Program (SIP)/ "Cyber-Security for Critical Infrastructure" (funding agency: NEDO).

**Figure 6 — Overview of ArkAngel SOC Operation Platform**

The ArkAngel proprietary SOC operation platform developed by Hitachi Systems Security is designed to enable security analysts to carry out SOC operations efficiently.



## References


1) New Energy and Industrial Technology Development Organization (NEDO), Hitachi, Ltd. News Release, "Hitachi Develops New Algorithm for Early Detection of Cyberattack Threats; Will Bring to Market as 'Hitachi Anomaly Detector'—Will contribute to improving security of systems in critical infrastructure fields—," (Oct. 2017), http://www.nedo.go.jp/english/news/AA5en_100329.html
2) Control System Security Monitoring Solutions Website, http://www.hitachi.co.jp/products/it/security/solution/integrated/monitoring/index.html in Japanese.
3) Hitachi Systems Security Inc. Press Release, "Canadian Group Company Above Security Re-branded as Hitachi Systems Security," (Jul. 2017), https://www.hitachi-systems-security.com/press-room/press-release-canadian-group-company-above-security-re-branded-as-hitachi-systems-security/


## Authors


**Tsuneo Iida, P.E.Jp**
Security Innovation Promotion Department, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Development of security technology businesses. *Certifications:* P.E.Jp (Professional Engineer, Japan) of Information Engineering. *Society memberships*: The Information Processing Society of Japan (IPSJ).

**Hiromi Harada**
Edge Computing Department, Engineering Services Operation 1, IoT & Cloud Services Business Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Development of security solution businesses.

**Daiki Nozue**
Security Business Planning Department, Business Management Division, Security Businesses Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Security integrated monitoring business. *Society memberships*: The Physical Society of Japan (JPS).

**Masashi Ohmori**
Network Security Operations Office, North America Business Promotion Department, Hitachi Systems, Ltd. *Current work and research:* Security business planning, security consultation, and designing for the Security Operations Center. *Certifications:* Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Project Management Professional (PMP).

**Guillaume Daleux**
Managed Security Services Department, Operations Division, Hitachi Systems Security Inc. *Current work and research:* Security consultation, designing for security architecture, and deploying security services worldwide.