Cross-ministerial Strategic Innovation Promotion Program (SIP)

Hitachi

1-3 Enhancement of Security Resistance of the Control System by Early Detection of Intrusion/Attacks

Operation monitoring and analysis technologies

Detects unauthorized operation that is hard to detect in the control system where availability is considered important.

Features Enhancement of system immunity by monitoring subtle changes in operation

I. Detection of unauthorized operation lurking in normal operation.

Even in the case of an authenticated operation that is hard to notice using existing technology, a subtle change that occurs in the control system is detected (integrated soundness determination technology).

II. Monitoring suitable for the characteristics of the control system

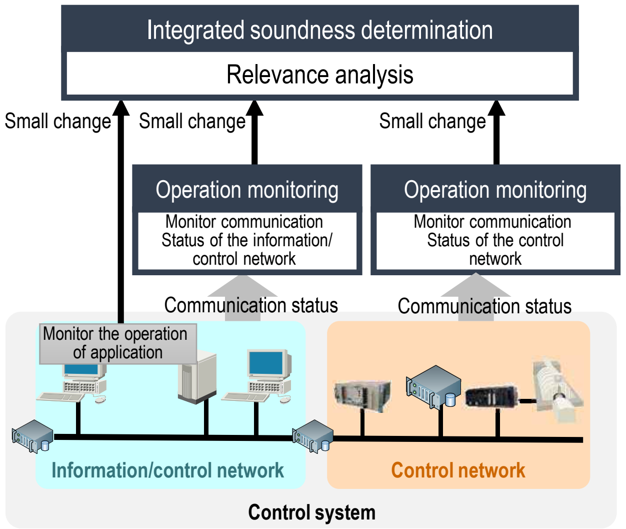
A subtle change is detected by learning and modeling the characteristics of the control system from the communication state and then monitoring the operation (operation monitoring technology). A system where availability is considered importance can be introduced with minimum influence.

Issues in the Current Critical Systems

With a growing number of unknown viruses and intrusions in a more sophisticated way, it is now difficult to prevent all intrusions by solely using intrusion prevention and attack defense technologies. There are intrusion and attack risks on the rise in control systems not directly connected to an external network. Therefore, intrusion/attacks detecting technologies suitable for the control system are needed in case of intrusion.

Technologies for Solving the Issues

Integrated soundness determination technology


Integrated soundness determination

Relevance analysis

Small change

Small change

Small change

Operation monitoring

Monitor communication Status of the information/ control network

Operation monitoring

Monitor communication Status of the control network

Communication status

Communication status

Monitor the operation of application

Information/control network

Control network

Control system

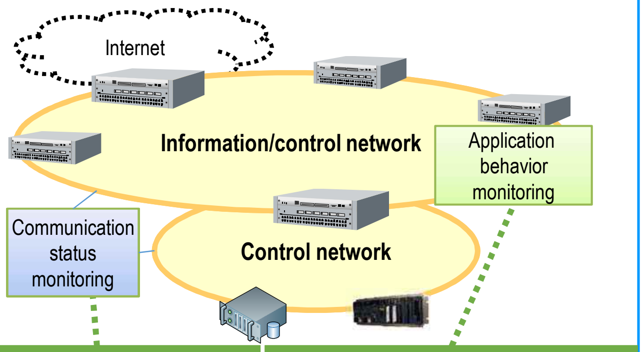
Comprehensive determination of unauthorized operation using small changes

Analysis of relevance of small changes reveals unauthorized operation that may have slipped past when looking at a single change and suppresses excessive invalid determination.

Operation monitoring technology

Adapted to the control system

The normal state is learned and modeled according to the characteristics of the control system. It is possible to select the communication status monitoring/application behavior monitoring according to the application destination.


Internet

Information/control network

Application behavior monitoring

Communication status monitoring

Control network

Communication status monitoring

Monitors the communication status in real time and detects small changes through comparison with the model.

Application behavior monitoring

Captures the activities within the device that is not shown in the communication status and detects small changes.

Implementation Status/Schedule

Verification was performed in collaboration with the critical infrastructure company in the end of FY2017, and the technology whose research and development had been completed ahead of the others was already commercialized in FY2017 (product: Hitachi Anomaly Detector). Hitachi continues conducting related activities after that and will plan to commercialize products of the results of ongoing researches.

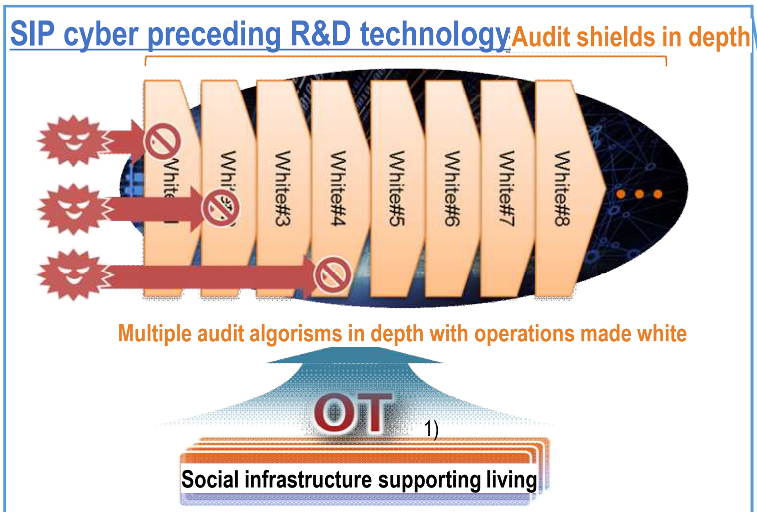
Cross-ministerial Strategic Innovation Promotion Program (SIP)

Hitachi

1-3 Enhancement of Security Resistance of the Control System by Early Detection of Intrusion/Attacks

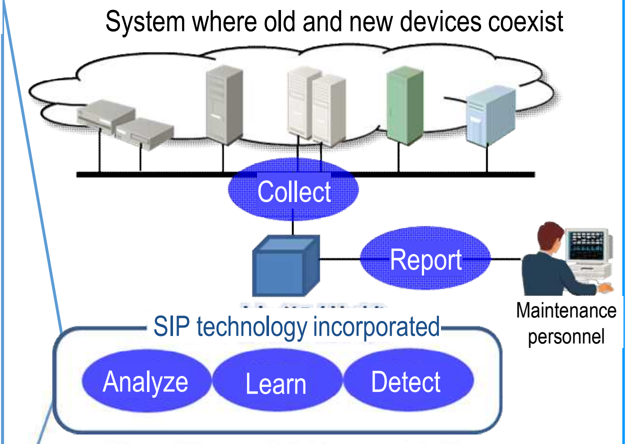
Commercialization of the technology with its research and development completed ahead of the others - Hitachi Anomaly Detector -

SIP cyber preceding R&D technology



Audit shields in depth
White#1
White#2
White#3
White#4
White#5
White#6
White#7
White#8
Multiple audit algorisms in depth with operations made white
OT
1)
Social infrastructure supporting living

Making use of know-hows on the control system accumulated for years, Hitachi makes operations white from diversified perspectives.



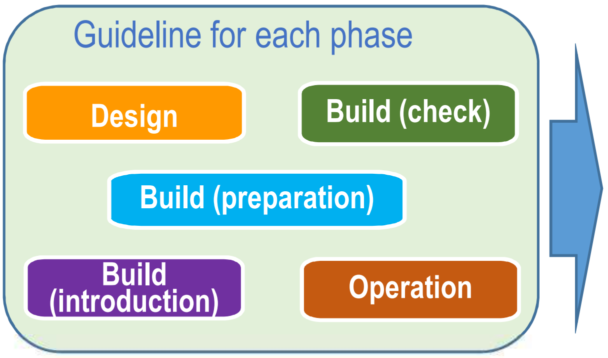
System where old and new devices coexist
Collect
Report
Maintenance personnel
SIP technology incorporated
Analyze
Learn
Detect

Security monitoring product
Hitachi Anomaly Detector

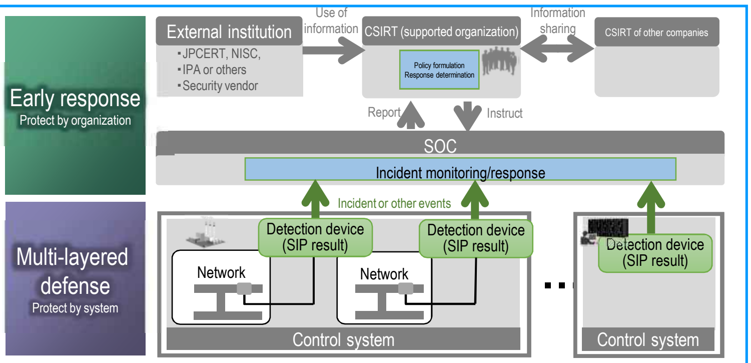
<Features> (i) Real-time detection of unknown threats by algorithms focusing on each operation
(ii) Analysis of business communications and self-learning of normal business communications from scratch
(iii) Availability of the product independent of the device model or OS version connected to the system

Protect safe operation of the system

How to Apply R&D Technologies



Describes key points of how to design/build security systems, organization structure, operation design, and other technical aspects.



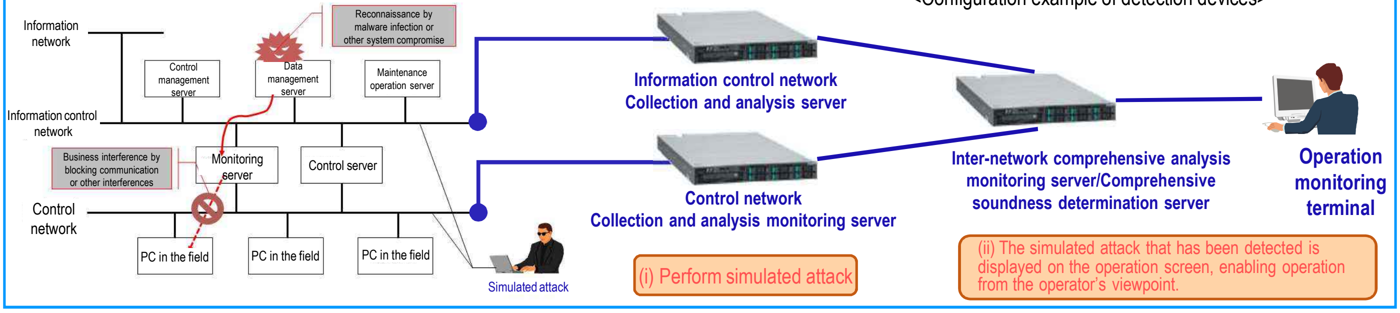
•Detection devices are incorporated into the control system in the field to detect every small change as an incident.
•Incidents are monitored in SOC2) and comprehensive determination is made for taking early response actions..

Presentation Overview

○Experience the display of incidents detected by the detection devices and how to operate the system.

<Image of the control system>

<Configuration example of detection devices>



Information network
Information control network
Control network
Control management server
Data management server
Maintenance operation server
Monitoring server
Control server
PC in the field
PC in the field
PC in the field
Reconnaissance by malware infection or other system compromise
Business interference by blocking communication or other interferences
Simulated attack
Information control network Collection and analysis server
Control network Collection and analysis monitoring server
Inter-network comprehensive analysis monitoring server/Comprehensive soundness determination server
Operation monitoring terminal

(i) Perform simulated attack

(ii) The simulated attack that has been detected is displayed on the operation screen, enabling operation from the operator's viewpoint.

1) OT: Operational Technology
2) SOC: Security Operation Center