7. Anomaly Detection for Cyber-Physical Systems

C
Verification & Maintenance

NTT Corporation and Mitsubishi Electric Corporation

This technology can avoid irreparable damage caused by attacks on cyber-physical systems by realizing a quick initial response through advanced monitoring and cause estimation.

Technical Features

- "Immediate monitoring" realizes spatial and temporal leak-free monitoring through continuous monitoring of configuration changes.
- "Immediate detection" detects anomalies including signs of attack against various control protocols by anomaly detection using machine learning.
- "Immediate support" estimates the cause of known and unknown anomalies by utilizing detection information and various system information, such as normal communication patterns, work plans, etc.

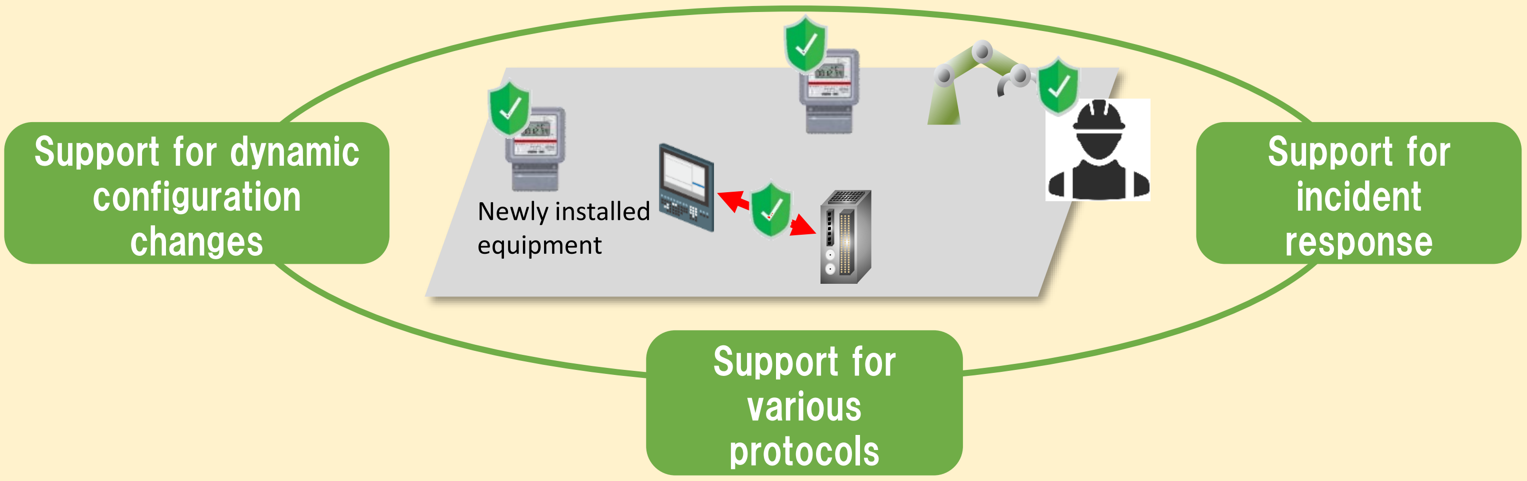
Overview

The threat of cyber-attacks to cyber-physical systems (CPS) is increasing year by year, and physical damage has actually been reported.
Immediate action is key to such threats, which are characterized by serious physical damage caused by attacks from cyberspace.

[Dynamicity of systems]
A wide variety of devices and dynamically changing system configuration in CPS

[Variety of attacks]
Advanced attacks targeting small surveillance gaps resulting from protocol diversity

[Complexity of IR]
Incident response (IR) becomes complicated due to the fusion of IT and OT



Support for dynamic configuration changes

Support for incident response

Support for various protocols

Immediate monitoring

The system configuration monitoring technology and high-speed, high-precision communication monitoring technology achieve both shortened time to start monitoring and detection accuracy when the configuration is changed.

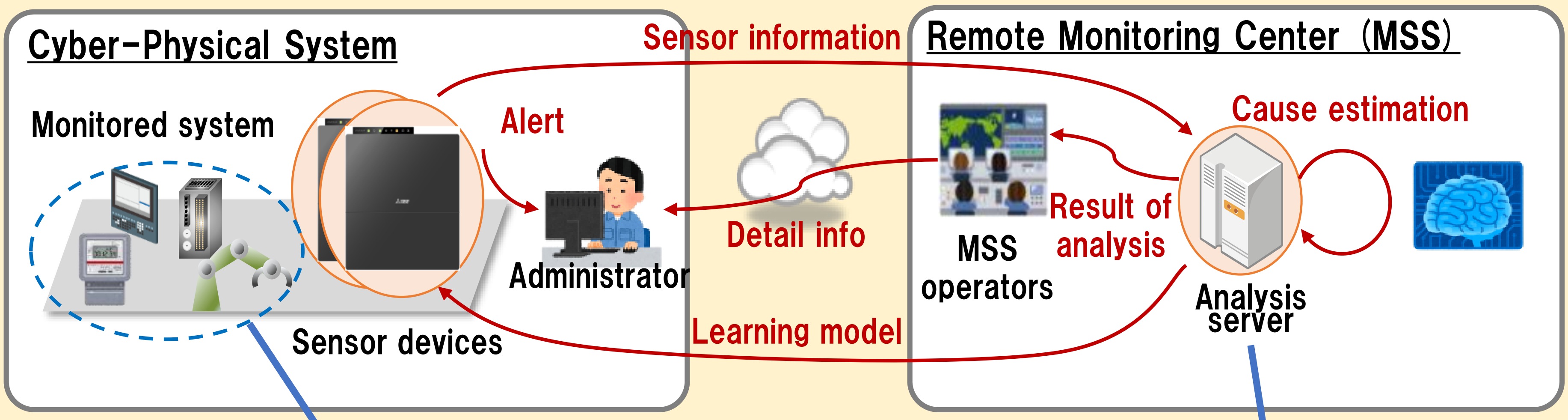
Immediate detection

AI learns communication patterns without depending on a specific protocol and detects attacks including signs. It is also possible to support original protocols.

Immediate support

The location where the anomaly causes are identified from the detection information and the possible root cause is estimated by collating it with the system information.

Configuration



Installation to the monitored system

- Sensor devices collect information in the system by connecting them to the configured mirror port
- Monitoring starts immediately after the sensor device automatically detects the device

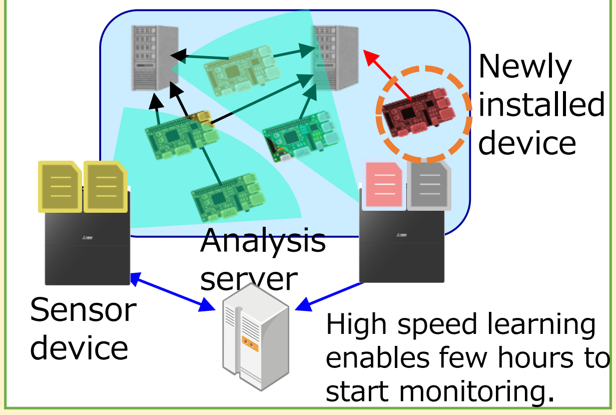
System monitoring

- Remote monitoring services are provided using information collected by the sensor device
- Monitoring work that requires human resources, security tools, and operation time is provided as a service.

Details

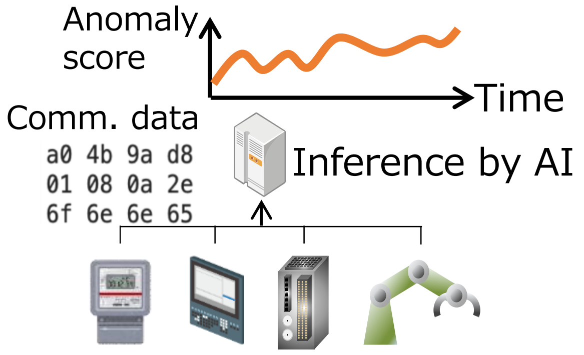
Immediate monitoring

Constantly monitors the system and immediately detects config changes



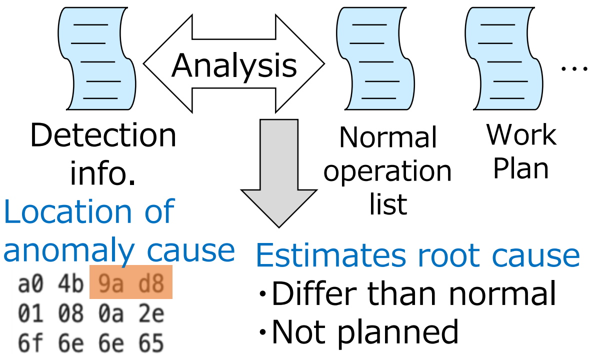
Immediate detection

Detects anomaly by learning communication patterns without depending on the specific protocol.



Immediate support

Identify the location of anomaly cause in the packet and estimate the possible root cause.



Plan

By shortening the time to start monitoring, expanding the protocol to be monitored, and improving the analysis accuracy of cause estimation, it is aimed to achieve spatial and temporal leak-free monitoring and significantly reduce the initial response time in the event of an anomaly.

FY2020	FY2021	FY2022	FY2023 -
Experiment STEP1	Exp. STEP2	Exp. STEP3	
R&D			Implementation/Productization

Contact：
Nippon Telegraph and Telephone Corporation
NTT Secure Platform Laboratories E-mail: scpflab@hco.ntt.co.jp
Mitsubishi Electric Corporation E-mail: xs5n02@nh.MitsubishiElectric.co.jp