7. Anomaly Detection for Cyber-Physical Systems

Application Area

IoT | ICT vendor
Manufacturer | Infrastructure | Distribution
Local Government | Building / Smart City

NTT Corporation and Mitsubishi Electric Corporation

Advanced monitoring technology for cyber-physical systems supports initial response and avoids irreparable damage caused by cyber attacks.
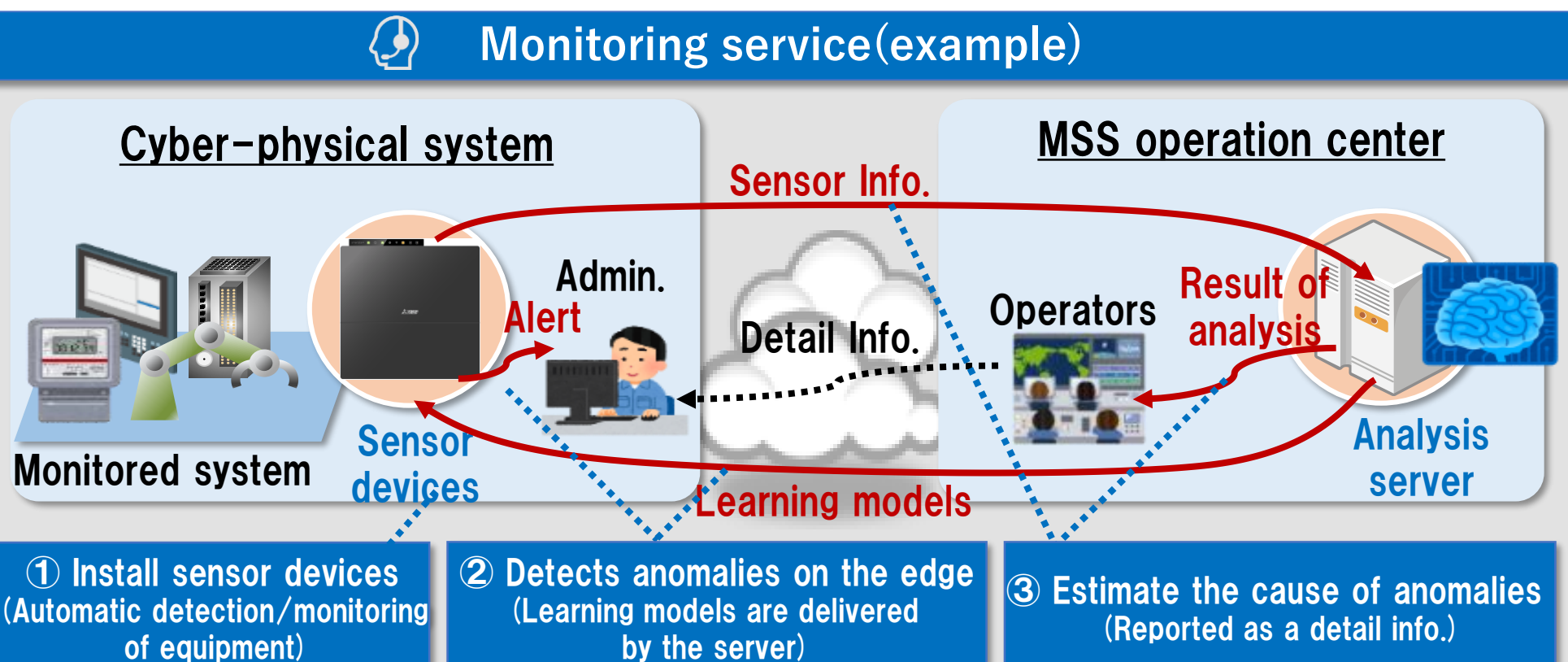
Technology Features

- It achieves <u>detailed monitoring</u> of most of the various control protocols in the OT field, <u>considering the differences in its usage in each monitored system</u>.

- Even if it is a proprietary protocol, it <u>automatically and quickly learns the characteristics</u> of communication and can <u>detects security anomalies including unknown ones</u>.

Effects

- By <u>quickly detecting anomalies and signs without omission</u>, this technology enables operator to take a <u>quick and proactive response</u> against them.

- This technology <u>avoids irreparable damage caused by cyber attacks</u> before it occurs and <u>supports the continuous operation of the monitored system.</u>

Use case

Supports various installation and operation forms, from on-premise installation and in-house operation to use as a monitoring service.


Monitoring service(example)

Cyber-physical system — Sensor Info. — MSS operation center

Monitored system | Sensor devices | Admin. Alert | Detail Info. | Learning models | Operators | Result of analysis | Analysis server

① **Install sensor devices**
(Automatic detection/monitoring of equipment)

② **Detects anomalies on the edge**
(Learning models are delivered by the server)

③ **Estimate the cause of anomalies**
(Reported as a detail info.)

7. Anomaly Detection for Cyber-Physical Systems

NTT Corporation and Mitsubishi Electric Corporation

Technology Description

Anomaly detection technology that automatically learns its normal usage in the monitored system for a wide variety of control protocols and can quickly detect even slight differences in control commands or values as anomalies.

Normal A — Control command / Control command

Normal B — Control command / Control command

Anomaly B — Control command / Control Command
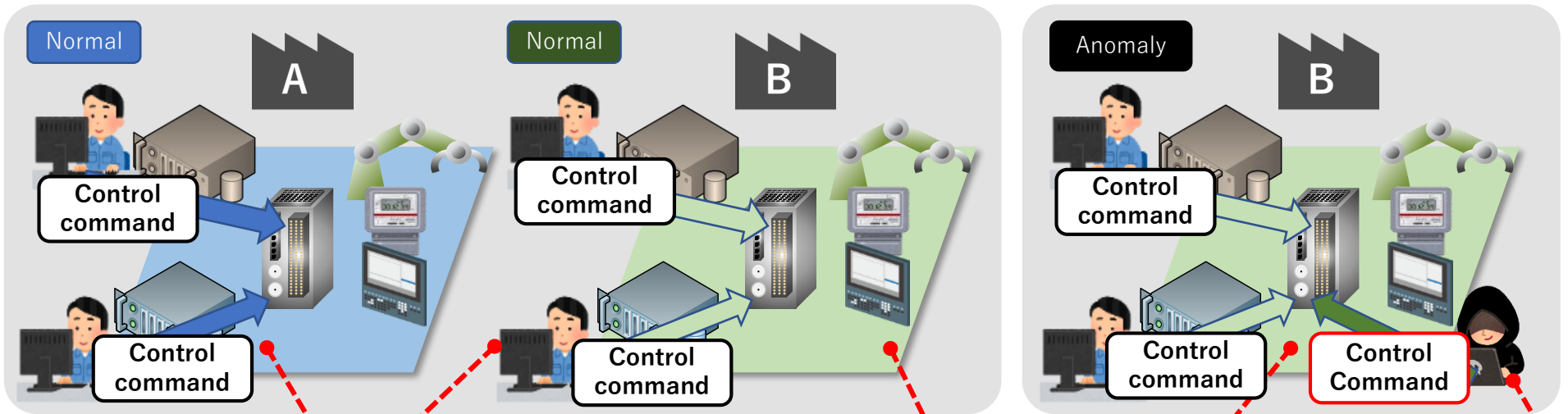
Even in the same system, A and B have different definitions of normal / anomaly.

It is required to discover slight differences in control commands or values unique to B.

**Quick detection of attacks is the key**

The challenge is to be able to define the criteria for the normal state of each system and to realize detailed and quick monitoring.

Technologies for the challenge

Technology that achieves both "support for a wide variety of control protocols" and "immediateness"

Immediate monitoring

Configuration changes are immediately detected by monitoring communication. Edge device can handle burst communication peculiar to CPS.
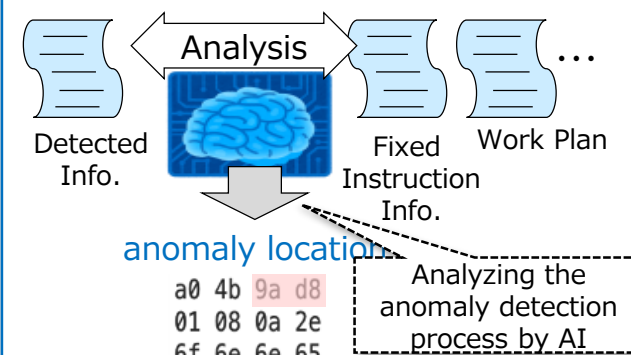
newly installed device

Edge device — Analysis Server — Edge device

Detects configuration changes
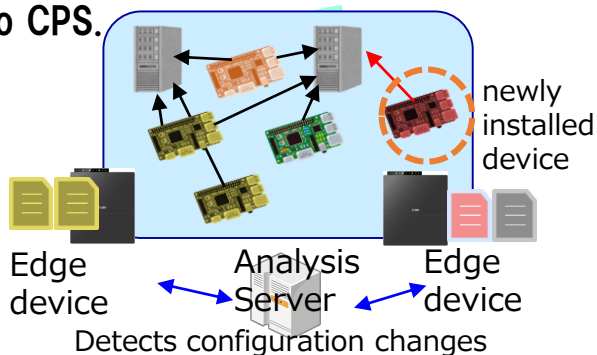
Immediate detection

Supports a wide variety of CPS protocols, including proprietary specifications, by automatically learning communication features.

Anomaly Score — Time

Comm Data
a0 4b 9a d8
01 08 0a 2e
6f 6e 6e 65

Analysis by AI
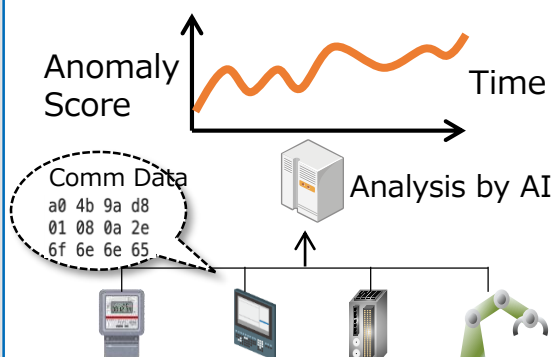
Immediate support

Automatically identifies the anomaly location in the packet that triggered the detection and estimate the cause.

Analysis

Detected Info. — Fixed Instruction Info. — Work Plan …

anomaly location
a0 4b 9a d8
01 08 0a 2e
6f 6e 6e 65

Analyzing the anomaly detection process by AI

Contact

Nippon Telegraph and Telephone Corporation
NTT Social Informatics Laboratories
Mitsubishi Electric Corporation

Email: solab@hco.ntt.co.jp
Email: xs5n02@nh.mitsubishielectric.co.jp

内閣府 Cabinet Office　NEDO　SIP Cross-ministerial Strategic Innovation Promotion Program