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

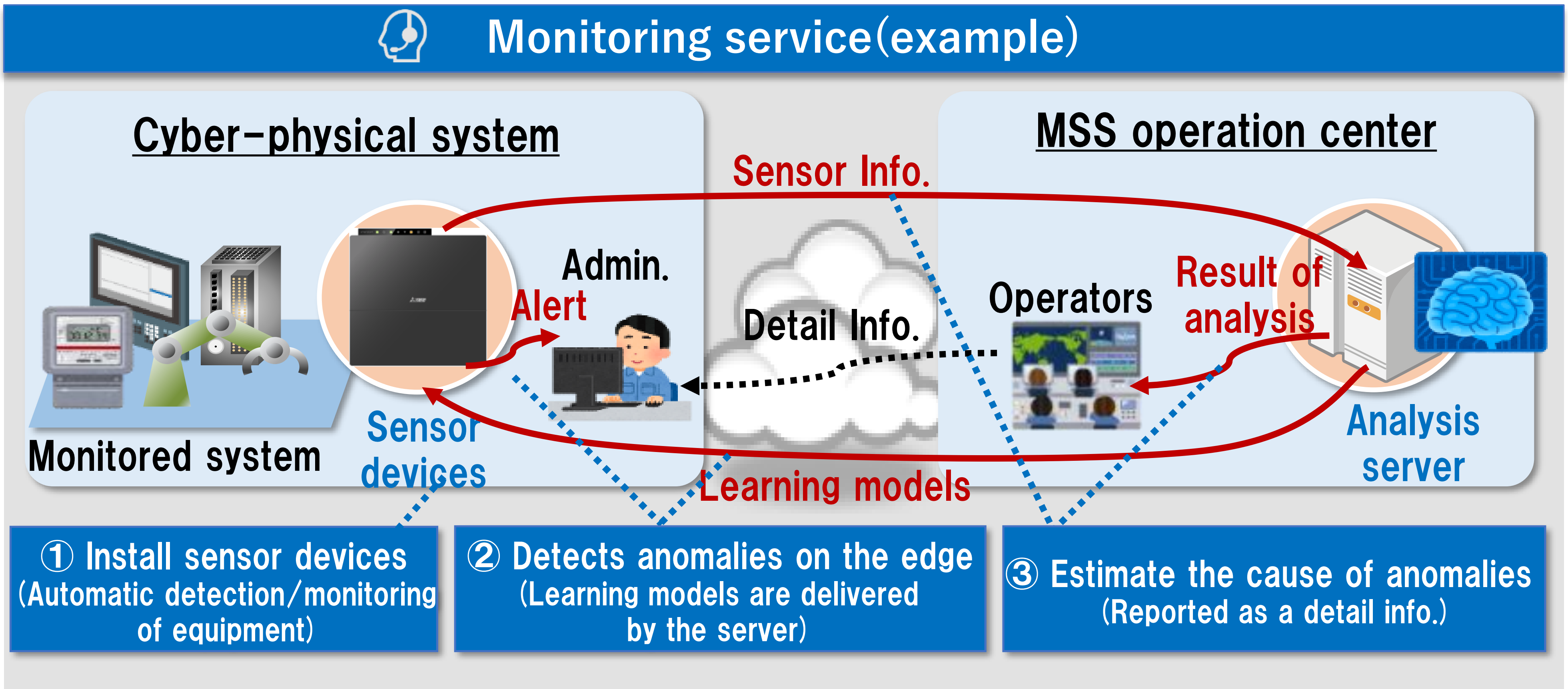
- It achieves detailed monitoring of most of the various control protocols in the OT field, considering the differences in its usage in each monitored system.
- Even if it is a proprietary protocol, it automatically and quickly learns the characteristics of communication and can detects security anomalies including unknown ones.

Effects

- By quickly detecting anomalies and signs without omission, this technology enables operator to take a quick and proactive response against them.
- This technology avoids irreparable damage caused by cyber attacks before it occurs and supports the continuous operation of the monitored system.

Use case

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



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

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

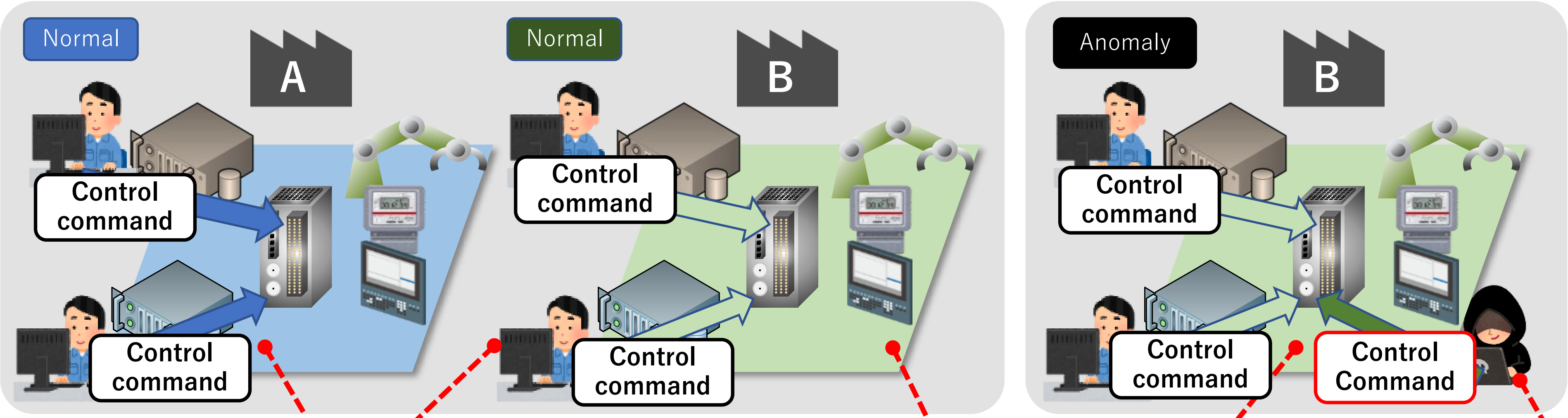
③ Estimate the cause of anomalies (Reported as a detail info.)

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.



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

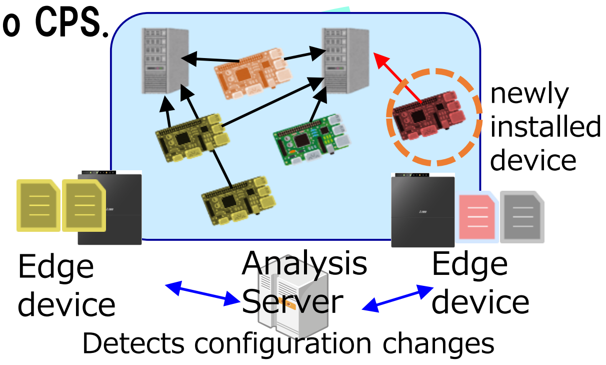
The challenge is to be able to define the criteria for the normal state of each system and to realize detailed and quick monitoring.

Technologies for the challenge

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

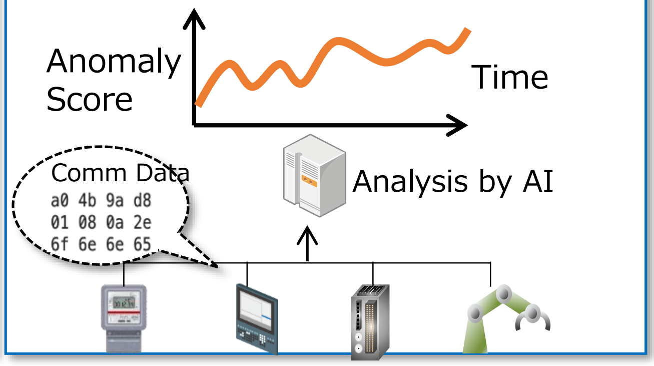
Immediate monitoring

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



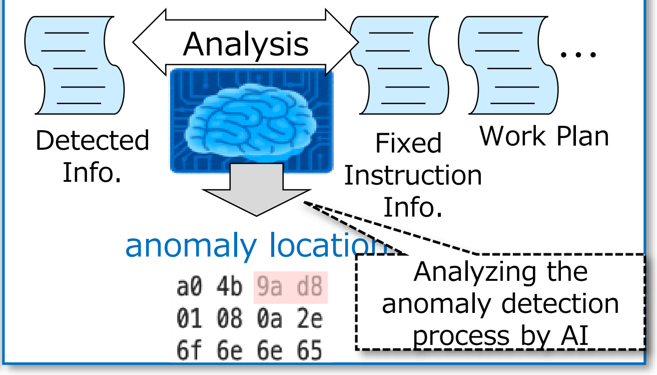
Immediate detection

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



Immediate support

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



Contact

Nippon Telegraph and Telephone Corporation
NTT Social Informatics Laboratories Email: solab@hco.ntt.co.jp
Mitsubishi Electric Corporation Email: xs5n02@nh.mitsubishielectric.co.jp