CSSC, ALAXALA

1-4 System Defense Technologies That Enables Safe Operational Continuity Even When an Abnormality is Detected

Operation monitoring and Defense technologies

Protects the entire control system from hard-to-detect sophisticated attacks for safe operational continuity.

Features

I. Quick identification of abnormalities in the control system

Defense conditions are appropriately changed according to the plant operation status, and instructions to the control system is monitored hierarchically in three levels as follows: SCADA (Supervisory Control And Data Acquisition) (upper level), network switch (middle level), and controllers (lower level).

Attacked locations in the control system are quickly identified and protected by using the verification function making use of the characteristics of devices in each level including lower-level monitoring that is not found in the existing technologies (layered verification function).

II. Continuity of safe operation even when an abnormality is detected

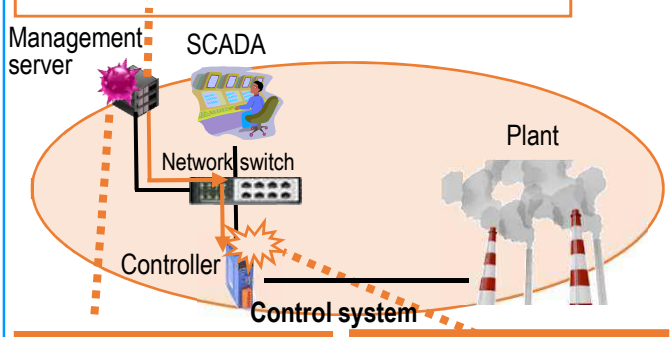
A terminal for cooperative function on is used to restrict the communication and processing of a device where an attack has been detected is restricted in the scope of business continuity.

The system protects the controllers from suspension or malfunction caused by attacks for business continuity (cooperative function).

Needs to be prepared for hard-to-detect sophisticated attacks

Attack using a normal command

An attack that slips through the defense conditions may be launched by a normal command.



Hard-to-detect attack

Sophisticated cyber attack may not be prevented with a single defense condition.

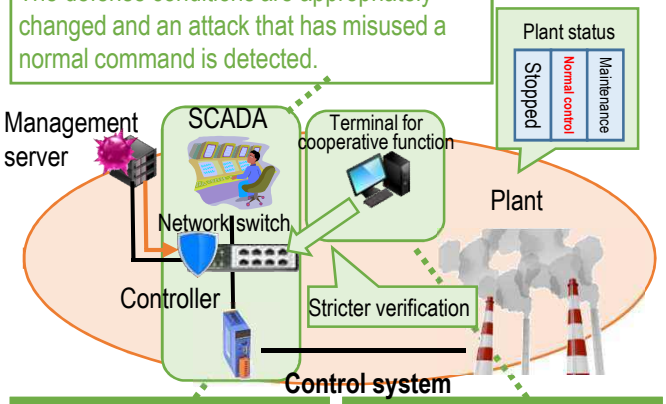
Risks of attacks to the controller

A cyber attack to equipment for maintaining the safety of the plant may cause a tragedy.

Protects the entire control system from sophisticated attacks

Defense according to the operation status

The defense conditions are appropriately changed and an attack that has misused a normal command is detected.



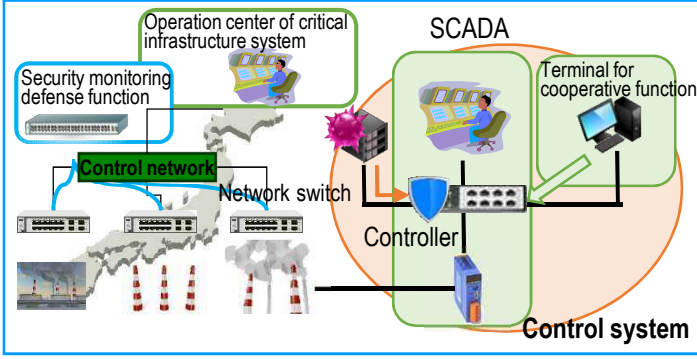
Defense in all layers

Multiple-layered defense network prevents sophisticated attacks from slipping through protection.

Defense at a distance from field

Attacks can be prevented as high a level as possible for safe operation of the entire plant.

Incorporation Into the Social Implementation



Progress

Technology development is conducted in collaboration with the critical infrastructure company with technology evaluation, introduction and operation procedures set for the goal.

For social implementation

- The technologies that are available ahead of the others have been introduced to and made use of in the critical infrastructure company.

About research techniques

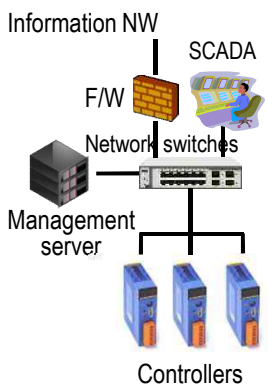
- The cooperative whitelist defense function has been developed and implemented into the simulated plant for testing.
- Verification has been conducted using multiple types of simulated plants for testing.

Cross-ministerial Strategic Innovation Promotion Program (SIP)

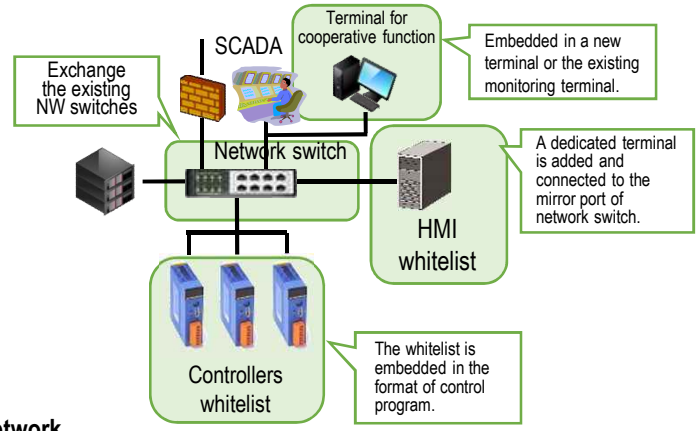
CSSC, ALAXALA

1-4 System Defense Technologies That Enables Safe Operational Continuity Even When an Abnormality is Detected

Introduction Image



Example of Industrial Control System Network

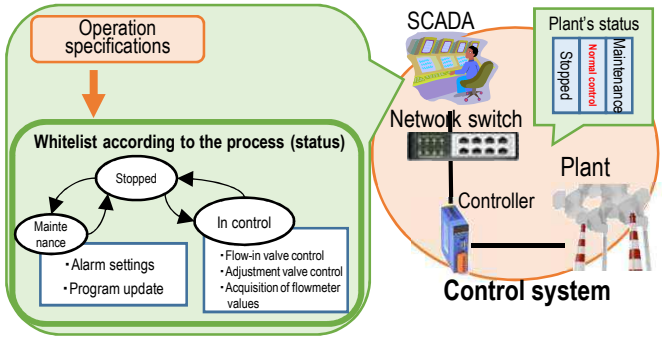


Example of application of the research result to the example of control system configuration

Introduction of R&D results

- The control system is protected from hard-to-detect sophisticated attack by introducing three types of whitelist security functions ns whitelist cooperative functions.
- It is possible to introduce needed elements individually according to the target control system.

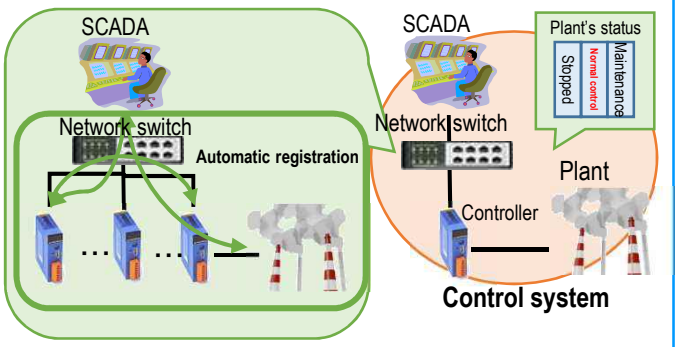
(Upper level) Detects instructions that are not normally issued and provides defense



Defense according to the plant's status

Defines instructions in the whitelist from the operation specifications for each status of the plant in order to detect instructions that are not used in a certain status as attacks and provide defense.

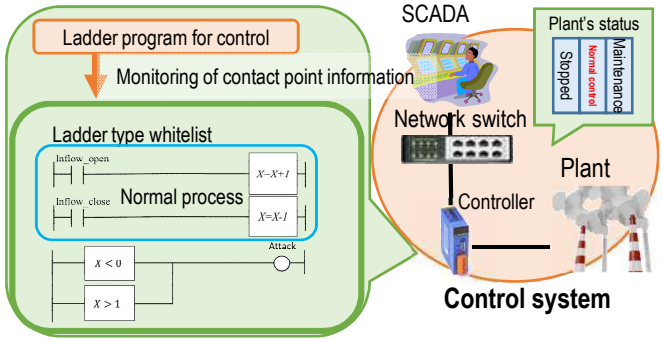
(Middle level) Detects attacks and provides defense without troublesome management



Defense using the learning function corresponding to the control protocol

Defines communication in the whitelist by self-learning for each plant detect instructions that are not used in a certain status as attacks and provides defense.

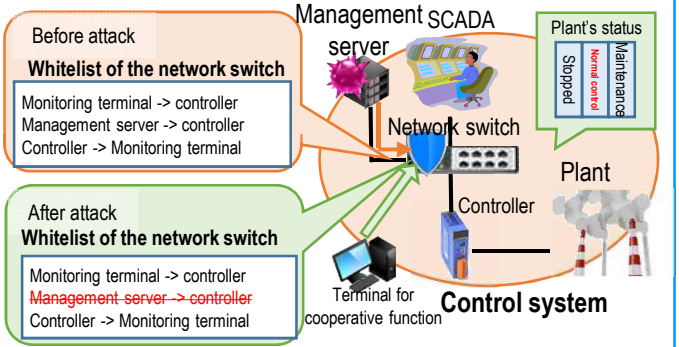
(Lower level) Monitors the operation status of plants and provides defense



Monitoring of the operation status of the plant and defense against abnormal operation

The ladder program that expresses the operation status (normal process of I/O) of the plant monitors the contact point information in order to detect operations that deviate the predetermined operation as an attack and provide defense against such operations.

Applies defense functions according to situations to provide defense against attacks



Protection by stricter upper-level defense function for defense against attacks in higher level

For safe operation of the entire plant, if an attack that has slipped through the protection in an upper level is detected, the conditions in the upper-level are reviewed and enhanced detection and defense are implemented.