8. Impact Assessment and Countermeasure Execution Support Technology

C
Verification & Maintenance

NEC corporation

Automatic cyber-attack risks analysis of OT/IoT systems and support for risk visualization and countermeasure execution by using attack simulations.

Technical Features

■Visualize effects of the cyber attack

Analyze both system impacts and affected devices automatically in case of a cyber-attack. Operator understands potential cyber-attack risks without security knowledge.

■Automated risk assessment

Translate risk assessment results into a guideline format* and support operators to deal with the guideline. *)IPA "Security risk analysis guide for control systems"

■Provide countermeasure plans against the cyber attack

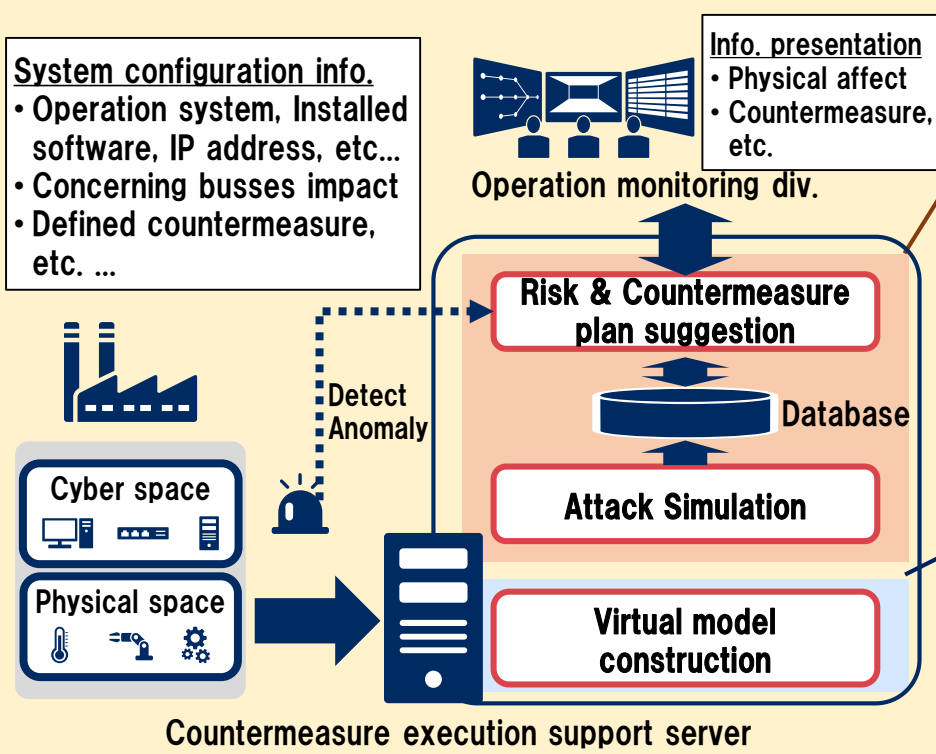
Evaluate countermeasure plans automatically and support operator to execute them.

Problems of Cyber Attack Countermeasure

Comprehension of cyber attack effects

Pre-evaluation of countermeasure efficacy

Overview of R&D Technologies toward Solving Problems



■Countermeasure execution support technology

Perform attack simulations and evaluate effectiveness of countermeasure plans on the virtual model. When an anomaly is detected, the technology suggests applicable countermeasure from evaluated plans.

■Virtual model construction technology

Create the model which is used to analyze cyber-attack risk without using actual systems.

Technical differences

Previous

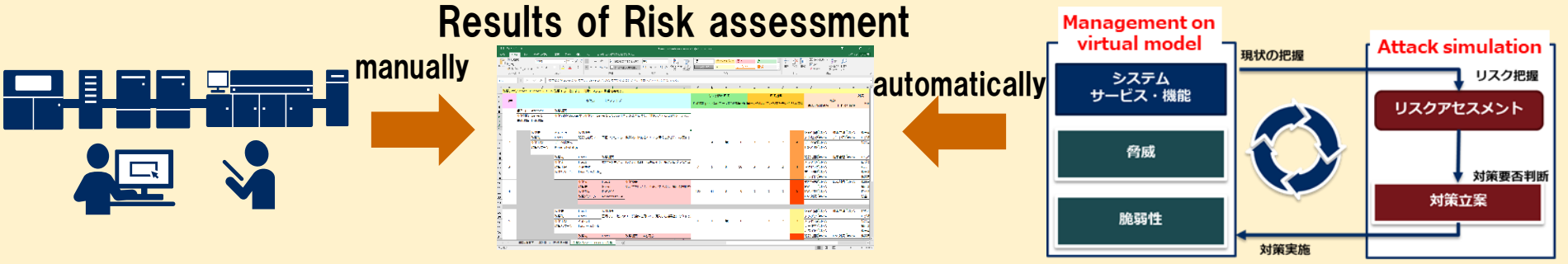
■Analysis results depend on analysts

Cyber-attacks are analyzed manually and countermeasures are considered based on the analysis result of cyber-attacks.

Proposed

■Analysis result is uniform, not depending on analyst.

Cyber-attacks are analyzed by using attack simulations and the risk countermeasures based on analysis result are provided automatically.



Use cases

Target

OT/IoT systems of manufacturing (plants), distribution, smart building and so on.

Use case

①Risk assessment

Perform risk assessment on a daily basis and countermeasures

②At the time abnormally detected

Execute countermeasures by considering attack simulation results and abnormal alarms

Required info.

Cyber side

OS info., Installed software, IP address

Physical side

PLC prog., P&ID