YOKOGAWA

Co-innovating tomorrow™

OpreX™ Safety & Security

YOKOGAWA Security Program

Supporting Business Continuity

Bulletin 43D07T31-02EN

What a company should do

Toward Achieving Safe and Uninterrupted Production Operation.

In today's manufacturing environment, resolving complex challenges is essential.

1. Compliance and Operational Efficiency

It is necessary to enhance productivity and cost efficiency while meeting legal and regulatory requirements.

2. Balancing Risk and Cost

When addressing various risks, it is important to determine how much cost should be invested to mitigate them effectively.

3. Integrated Protection of IT and OT

Protecting both IT and OT environments simultaneously is critical for security.

YOKOGAWA supports companies in addressing these challenges by providing practical solutions tailored to their specific situations.

Through OpreX™ Safety & Security , we deliver internationally recognized security programs and help ensure safe and uninterrupted production activities.

NIST CYBER SECURITY FRAMEWORK, IEC62443

A framework and standard widely used across industries when considering security measures for control systems.*1

67%

Percentage of respondents who answered "very" or "extremely" regarding cybersecurity as a technology that will become a top concern within the next 3–5 years. Ranked first among 16 items, including data communications, AI, and cloud.*2

OpreX™ Safety & Security

OpreX™ stands for excellence in technology as well as solutions in industrial automation and control where co-innovating value for a prosperous future is consistently delivered to our business partners.
This major brand consists of five categories: transformation, control, measurement, execution, and lifecycle. The activities covered by OpreX™ Lifecycle contribute substantially to attain high levels of maintenance efficiency required for stable and efficient operation over the entire length of the plant lifecycle. They also strive to provide solutions that can further improve operability.

OpreX™ Safety and Security measures deliver comprehensive solutions that utilize the strategy of defense-in-depth with our safety & security lifecycle approach. Defense-in-depth is a multi-layered protection to enhance the cybersecurity protection level of the whole system. If one layer gets affected, other layers continue to protect against the attack.
In this way, we effectively minimize both the safety and security risks for our customers' systems.

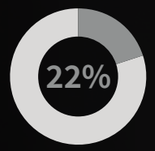
*1 SANS 2024 State of ICS/OT Cybersecurity, SANS, October 2024

*2 Accelerate Industrial Transformation, Microsoft, June 2024

Cybersecurity Attacks Are Bringing Industrial Plants to a Halt

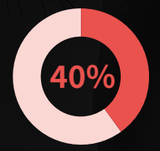
Cybersecurity incidents are increasing year by year. In particular, ransomware, and malware such as Emotet, as well as other attacks on manufacturing and infrastructure pose significant risks, and there have been incidents where damage exceeded several billion yen.
This is not just about the numbers—such incidents can lead to production downtime, brand damage, and loss of business opportunities, making cybersecurity a critical management issue.

The Reality of OT Security | SANS 2025 Global Survey*1



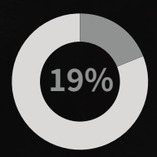
CONFIRMED INCIDENTS

Percentage of industrial organizations that experienced a cyber incident last year.



OPERATIONAL IMPACT

Of incidents resulted in immediate Operational Disruption and production halts.



RECOVERY

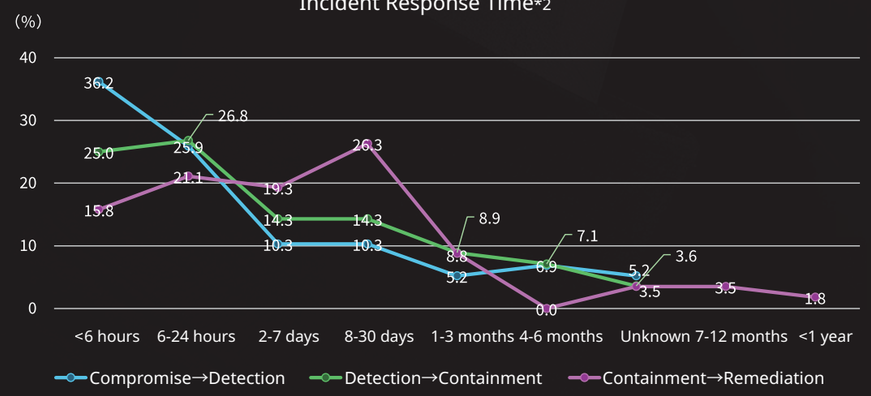
Required **over a month** to restore full operational integrity.

*1 SANS Institute, “State of ICS/OT Security 2025”

When OT systems are breached by a cyberattack, production lines may not only experience temporary downtime, but the impact can spread to entire plants or corporate-wide operations, potentially causing severe and long-lasting consequences.
In systems that require continuous operation (such as production control systems running 24/7/365), recovery can take several days to more than a year, depending on the severity of the intrusion.
During this recovery period, the burden on operators increases, productivity declines, and the risk of secondary incidents grows.
In some cases, the inability to supply products due to system disruption can harm customer trust and negatively affect the entire supply chain, especially for companies that deliver parts and materials.

Unlike IT environments, OT environments often run on proprietary protocols and long-term operation cycles, making them harder to update or replace. This results in many cases where legacy environments remain for extended periods. Without appropriate patching or system lifecycle updates, even a single attack can cause prolonged operational risk.

Incident Response Time*2



*2 SANS Institute, “SANS 2024 State of ICS/OT Cybersecurity”, October 2024, Figure 14. Reconfigured at Yokogawa

Case 1: A Manufacturer of Spare Parts Suffers from a Ransomware Attack, Causing Multiple Factory Shutdowns

A related company of a major automobile group suffered a ransomware attack, causing its production management system to shut down.
As a result, several key domestic factories of partner companies were forced to halt operations for at least one full day, and the impact spread across the entire supply chain. The attack is believed to have originated from malware delivered via email. Encryption of file servers disrupted the supply of spare parts, affecting entire production lines.
Consequently, approximately 13,000 vehicles were affected in terms of shipment volume. This is a typical case where an IT failure caused an OT environment to shut down, reaffirming the importance of supply-chain security and network segmentation.

Case 2: A Major Beverage Manufacturer Hit by Ransomware, Leading to Operational Shutdown and Threat of Information Leakage

A leading beverage manufacturer experienced a ransomware attack, impacting its order, shipping, and logistics systems. At multiple domestic sites, product shipment delays and partial operational interruptions occurred. Unauthorized access to internal systems was suspected, raising concerns that “manufacturing control systems might also have been compromised.”
This illustrates a common pattern in which OT environments may be affected by IT disruptions. The incident shows the importance of enhancing security measures and strengthening network segmentation across both IT and OT environments.

Case 3: Water Treatment Facility’s Chemical Concentration Altered Through Compromised Remote Access

An operator’s remote-access tool (TeamViewer) was exploited and gained unauthorized access to the SCADA system controlling a water treatment facility.
The chemical concentration of drinking water was altered to 100 times of the normal level, prompting an emergency shutdown when operators noticed the abnormality. Although no injuries occurred, the incident demonstrated the potential risk of cyberattacks directly impacting public safety.
This case highlights how even a single intrusion can create hazardous conditions in critical infrastructure, clearly showing the real-world danger of cyberattacks on essential services.

YOKOGAWA Security Program

1. Awareness & Training

Provide content tailored to customer needs, from basic to advanced levels.
Awareness Training / Overview of IEC62443 / Risk Assessment Procedures / Tabletop Exercises for Incident Response, and more.

6. Managed Services

Provide support for monitoring necessary to maintain stable operations, as well as operations and coordination with relevant departments when anomalies are detected. Enable integrated monitoring not only for a single site but also across multiple plants.
Asset Management / Remote Maintenance Systems / SOC (Security Operations Center)

5. Design & Implementation

Propose, design, and implement security solutions for systems based on the existing environment and customer requirements.

2. Risk Assessment

Evaluate the current security posture and identify risks within the customer's system based on IEC62443, considering national and industry regulations and guidelines, as well as customer-specific security policies.
Organizational Security / Network Security / Host-based Security / User and Access Control / Incident Response and Recovery / Physical Security and more.

3. Policies & Procedures

Support the development and improvement of security policies and procedures necessary to achieve the target security level.
Governance / Business Environment / Risk Management / Asset Management / Maintenance / Access Control / Data Security / Business Continuity and more.

4. Business Case

Support the development of medium- and long-term plans and budget considerations for implementing security solutions in line with established security requirements, policies and procedures.
Assistance in planning for security system implementation and more.

Endpoint Security Measures:

We provide endpoint security measures that protect against external threats by applying OS update programs, installing and updating antivirus software, blocking unauthorized programs, controlling USB ports, and more.

User Accounts and Access Rights Management:

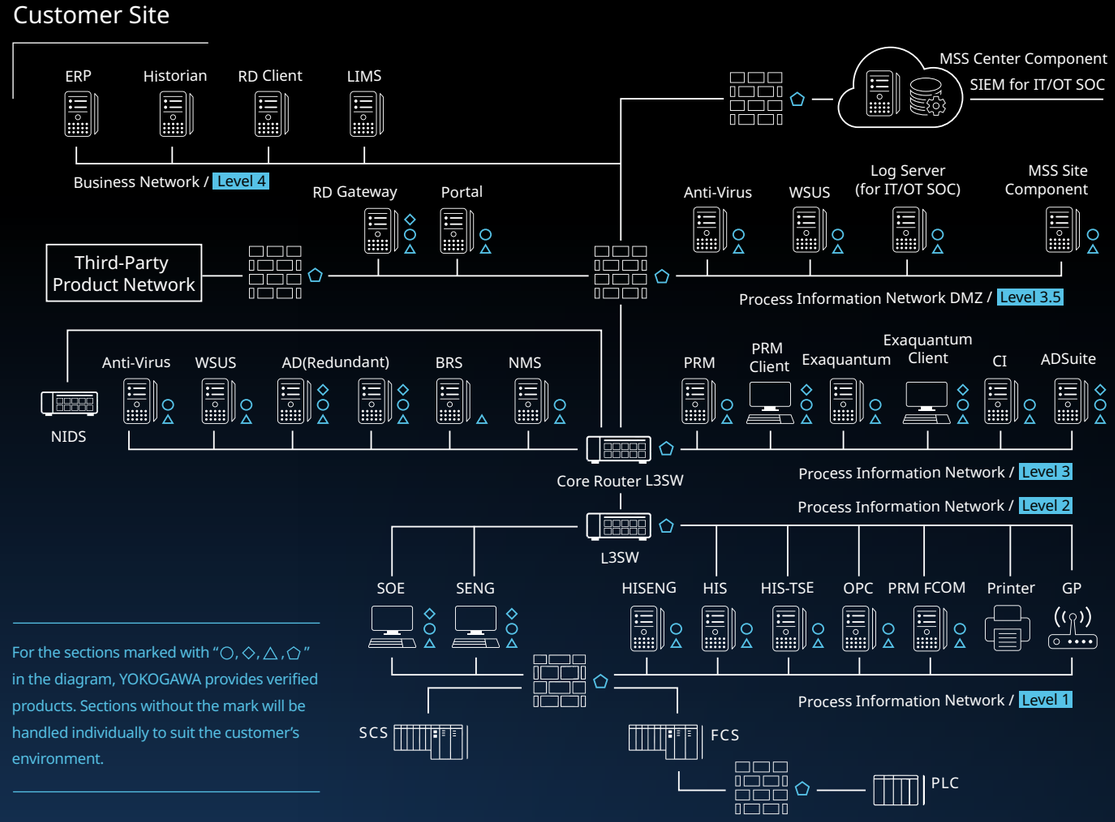
By utilizing directory services by using Active Directory, we centralize user account authentication and access rights. This ensures secure access to devices and systems. By aligning security policies with system lifecycle management, unauthorized access and information leakage risks can be significantly reduced.

Backup & Recovery:

We offer regular backups for production systems for quick restoration in the event of failures or cyberattacks. For control systems, we provide comprehensive backups of OS, applications, and parameter settings. Additionally, through shared use of on-premise and cloud security environments, we achieve strong security and high system availability.

Network Segmentation & Segregation:

We design segmented network layers adapted to usage and security requirements, clearly separating business systems and control systems within the corporate network. By limiting the spread of threats and minimizing their impact on systems, effective network segmentation supports long-term safe and secure operation.



For the sections marked with "○, ◇, △, ⬠" in the diagram, YOKOGAWA provides verified products. Sections without the mark will be handled individually to suit the customer's environment.

Implementation Case Studies

1. OT Security Design & Implementation for an Electric Power Company

Challenges

- Lack of visibility of assets within the distribution system, transmission system, ICT (data center) headquarters, and multiple key locations
- Required knowledge regarding security measures and require a partner capable of providing consultation, including planning.

Solutions

- Technical Support for OT System Monitoring
- Design, Project Management, and Implementation of OT Threat Monitoring Solutions
- Providing total solutions including equipment procurement, engineering, and installation

Customer Benefits

- Real-time monitoring facilitates timely detection of OT security threats
- Remote and integrated monitoring across multiple locations
- Established a Decision Processes for Incident Response Through Visualization

2. Support for Acquiring Security Certification for a Gas Company

Challenges

- Strengthening cybersecurity measures is necessary to obtain High-Pressure Gas Type A certification.

Solutions

- Security Risk Assessment for the Entire OT System
- Security Policy and Procedure Development
- Support for Security Roadmap Development and Certification Compliance

Customer Benefits

- Established a Sustainable Security Operations Framework
- Implemented a robust security measures in OT systems
- Acquired a High-Pressure Gas A Certification

3. Small-Group Security Training

Challenges

- The customer's employees understood the importance of security awareness, but there was no training provider with expertise in the OT field.

Solutions

- Provide materials demonstrating the necessity of training and encourage participation.
- Conduct multiple training sessions for small groups
- Arrange additional trainers when handling parallel schedules across multiple venues

Customer Benefits

- Security knowledge among all stakeholders has improved, even reducing human-related security risk.

4. Integrated Monitoring Solution for Urban Infrastructure

Challenges

- Required a centralized monitoring environment across multiple infrastructure enviro.
- Compliance to meet strict security requirements.
- Continued support is required even after the start of operations.

Solutions

- Project Management
- Integrated architecture design and construction, including SCADA and cybersecurity
- Development of Startup Plan and Procedure Manual
- Integrations including third-party products
- Long-term remote operation support

Customer Benefits

- Improved operational efficiency through centralized management and integrated monitoring and control of multiple systems
- Enhanced Security Posture Through System Design and Architecture Implementation Addressing Security Risks

YOKOGAWA's Competencies

1. Over 100 Years of Expertise in Manufacturing and Plant Operations

For more than a century since YOKOGAWA was founded, we have been deeply involved in the manufacturing and plant control industry.
Through this extensive experience, it has given us a deep understanding of the operational requirements, limitations, and on-site conditions unique to control systems (OT).
This allows us to design and implement security measures that do not compromise the availability, safety, and real-time performance of control systems—something that cannot be achieved by simply extending IT security concepts. This is a distinctive strength of YOKOGAWA, unmatched by typical IT consulting firms.

2. Practical Asset Management for Control System Users, Informed by IEC 62443 and Other Security Standards

YOKOGAWA possesses extensive expertise in asset management, risk assessment, and security implementation aligned with domestic and international standards such as IEC 62443.
For companies using industrial control equipment, our deep knowledge of equipment configurations and communication specifications allows us to significantly reduce the effort required for site surveys and interviews. As a result, we can deliver solutions with more realistic cost levels and achievable schedules.

3.Optimized, Cost-Effective Proposals and Execution Based on Risk Levels

We optimize security solutions based on the customer's industry, scale, operational structure, and projected risk level. For example, we establish advanced monitoring and response systems for critical facilities and plants where high risk is anticipated. Conversely, in environments with limited risk, we can propose solutions that prioritize the balance between cost and effectiveness, such as phased implementation of the minimum necessary measures.

Security risk control concept

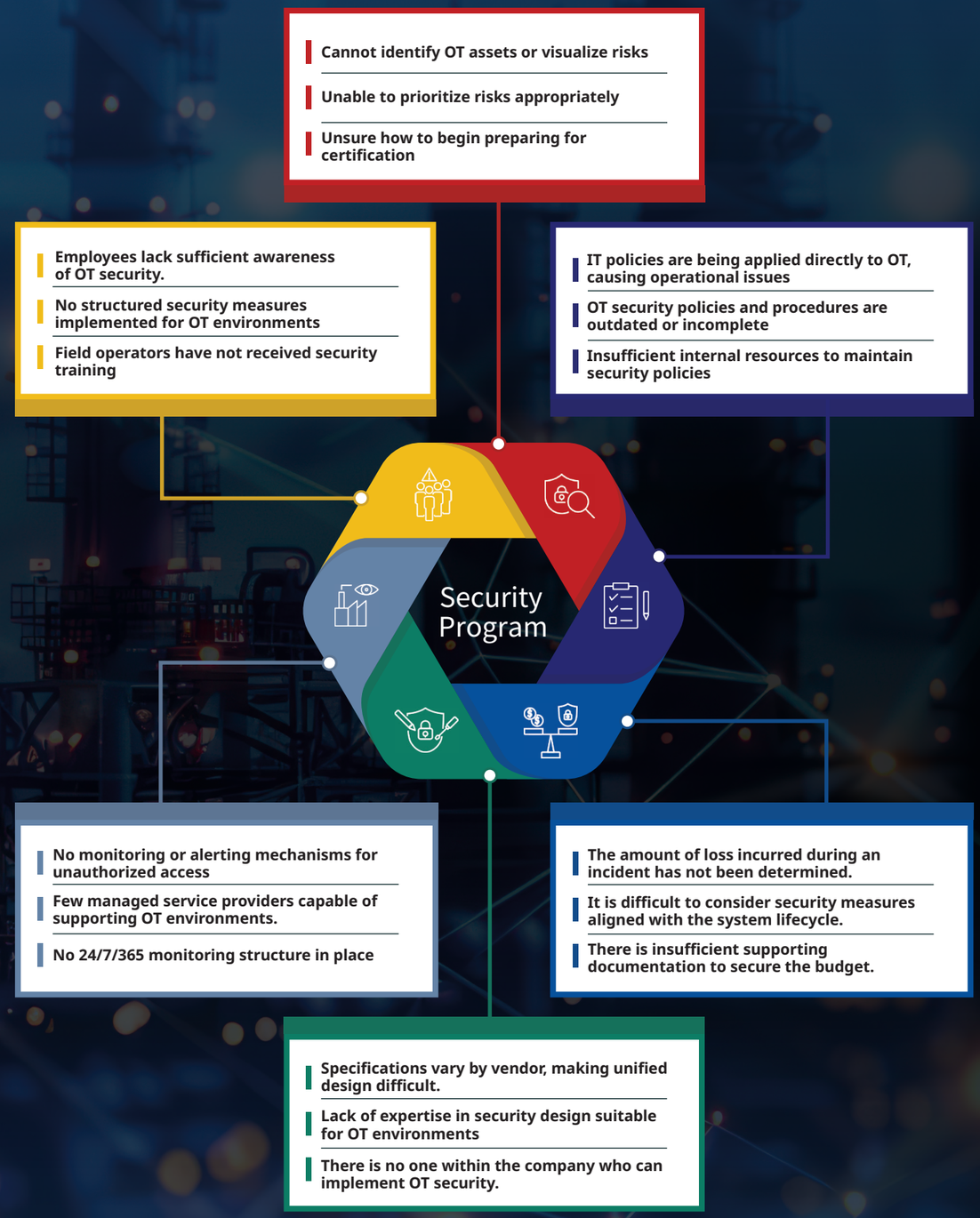
Risk level: the existing risk level that the industrial plant is facing

Acceptable Risk level: the risk level that plant owners can accept as low as reasonably practical

A Security risk level rising
B Start of security roadmap and mitigation of risk by implementing countermeasures
C Maintaining countermeasures and applying improvement
D Without maintenance and improvement

Consult with YOKOGAWA, whose extensive knowledge and experience stem from over 100 years of business operations.

We will propose the optimal solution balancing risk levels and countermeasure costs to support your business continuity.



Yokogawa Electric Corporation

Yokogawa Electric Corporation
World Headquarter
9-32,Nakacho 2-chome, Musashimno-shi,Tokyo
180-8750, Japan
https://www.Yokogawa.com

Printed in Japan, 501(HT) [Ed:05/d]

YOKOGAWA Co-innovating tomorrow™