vigilantplantservices.®

Cyber Security for Industrial Control Systems







Cyber Security for Industrial Control Systems

A New Age of Controlling Security Risks

The spread of malware and increasingly sophisticated cyber attacks are causing even more serious damage.

The threat of cyber security risks extends beyond information technology systems and into control systems. The use of information technology systems has advanced control systems and helps reduce costs and provides more functions. However, we now need to tackle the security risks.

We are in a new age of controlling security risks. What are the proper security controls for control systems? How can damage be minimized?

There's a long way to go to achieve secure plant operations. You need to be well-equipped and have enough stamina to go down that road, and maintain an appropriate pace and be prepared just in case.

Who can be your partner with whom you can travel and grow with?

That partner shall understand that what you need is not only security controls but also the safety and security beyond them.

Your best partner is Yokogawa which knows everything about security controls for control systems.



Integration of various systems

Combining open architecture and reliability

Increased scalability using general-purpose technologies

YODIC 500



World's first distributed control system

CENTUM C

Centralized digital control system Internal physical security controls

External physical security controls

CENTUMV

ntinuous tireless effort against

Security controls over a USB device

new threats

and network

Evolution of Security Controls

C/3000

Yokogawa's Way

Security Competence Laboratory

Yokogawa has research and development centers in Singapore, Japan, India, and the U.S. where technologies to apply security techniques to control systems in the best way are being developed. With a long experience of integrating control systems, these centers develop security techniques and solutions optimized to each industry, application, and system configuration. These results provide the foundation for helping customers securing their control systems against ever evolving security risks.

Contribution to Industries

Yokogawa's security experts have been actively participating in the development of international industrial standards from ISO, IEC and ISA such as IEC/ISA62443 (ISA99). Also, Yokogawa was one of founding members of the ISA Security Compliance Institute. In addition Yokogawa has been developing techniques and solutions for the purpose of security risk management to general networks. One of the achievements has been accepted and appreciated for the Internet.



Security in Yokogawa Products

Throughout the product lifecycle, Yokogawa ensures vulnerabilities are reduced due to the architectures and technologies of systems and products. Yokogawa has established a framework and the dedicated workforce that allows for quick response to incidents concerning vulnerabilities and new threats. Also, Yokogawa continually improves the security level of the products by subjecting them to assessment by external security experts. Furthermore, Yokogawa obtains security certification for its control systems from a certification authority and updates it at regular intervals.

Best Practice

When implementing security controls, specific and requirements and operational conditions to the control systems shall be considered. Yokogawa has established best practices to implement security controls based on its long years of experience of delivering control systems and services to customers. These best practices are compliant with international and industrial security standards and are the foundation of high quality security service offerings by Yokogawa engineers over the globe.



Yokogawa's Security Lifecycle

Deployment and Enhancement

Optimal security controls services are provided for customer's control systems to address presented threats and known vulnerabilities.

- Installation of antivirus software and security updates
- · Stringent control to application programs, restrictions on running unauthorized programs
- . Logical and physical controls against USB ports
- . Segmentation and zoning of control networks

A proposal is made on the best security service solution throughout the lifecycle of new and existing systems

> Introduction and Consultation

Assessment



Recovery Support

Deployment and

Enhancement

Deployment of optimal security

controls including those for

existing systems

Support for recovering to normal operation

Implementation

Operation

Support

Periodic training, maintenance and inspection, and maintenance of security controls

Recovery Support

A proposal is made on a recovery plan in case a security incident occurs with the customer's system. If an incident actually occurs, Yokogawa provides support to ensure that a quick recovery is made. Yokogawa also makes a proposal to prevent

- Back up of entire data and images including the operating system
- · Quick recovery support in the event of an incident response

Operation Support

Yokogawa provides customer training to ensure that customers can operate and maintain the security lifecycle appropriately and provides the following services to ensure that threats can be addressed accordingly and vulnerabilities can be identified in time in place.

- Check the deployed security controls work properly
- Update the virus definition files and security updates at regular intervals
- Check the negative impact to Yokogawa's products by the above updates, and provide a report

Introduction and Consultation

Yokogawa runs a preliminary diagnosis of new and existing systems to identify threats and vulnerabilities, and makes a proposal on the optimal security lifecycle for the customer's system.

- Security assessment and discussions using a simple
- . Conduct security technical seminars

Management Support

Periodic audit and diagnosis Review of security controls



Management Support

Yokogawa supports auditing the security level of the entire system to ensure that new threats can be addressed. Considering newly detected threats and vulnerabilities, Yokogawa makes a proposal on the optimal security controls.

- Reassessment of the controls against known threats and vulnerabilities
- Proposal on controls if new threats and vulnerabilities are reported

Importance of Security Lifecycle

As control system technologies are constantly evolving, security risks such as attack techniques are also evolving. For example, attacks targeting specific industries and control systems have been increasingly reported. This means the one time deployment of security controls is not enough to control security risks. Thus, a periodic review of controls is required. It is called a security lifecycle of control systems. According to this idea, Yokogawa supports customers in securing their control systems.

Defense in depth

Yokogawa recommends a comprehensive approach based on the defense in depth strategy. This not only means deploying multiple technical controls, but also more important things, such as ensuring safety and performance of the control systems that is required for production activity, and maintaining control system health. They are followed by implementing technical, operational and managerial controls for cyber security. These are improved by the continuous lifecycle activities to ensure that risks to the control systems are **prevented** or **mitigated** and preparation for a quick **recovery** is ready just in case.

Technical controls: Antivirus software and security updates, PC protection, network reinforcement, etc.

Operational controls: Preparation of operational procedures, operational training, periodic inspection, backup, preparation for

Managerial controls: Preparation of the security policy and guidelines, periodic audits, establishment of the incident response



vigilantplantservices.®

Cyber Security for Industrial Control Systems

Trademarks

CENTUM, VigilantPlant, and VigilantPlant Services are registered trademarks of Yokogawa Electric Corporation.

All other company brand or product names in this bulletin are trademarks or registered trademarks of their respective holders.









VigilantPlant is Yokogawa's automation concept for safe, reliable, and profitable plant operations. VigilantPlant aims to enable an ongoing state of Operational Excellence where plant personnel are watchful and attentive, well-informed, and ready to take actions that optimize plant and business performance.

YOKOGAWA ELECTRIC CORPORATION World Headquarters

9-32, Nakacho 2-chome, Musashino-shi, Tokyo 180-8750, Japan http://www.yokogawa.com/

