ARC WHITE PAPER

By ARC Advisory Group

SEPTEMBER 2011

Yokogawa's Comprehensive Lifecycle Approach to Process Control System Cyber-Security

Executive Overview 3

Introduction 4

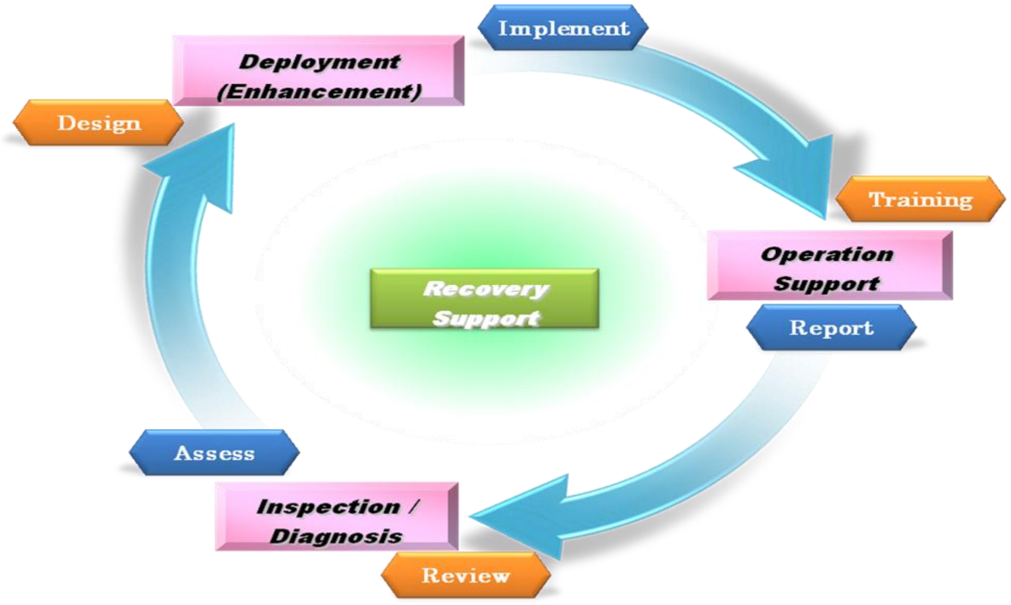
Security Lifecycle Approach 5

System Products, Platforms, and Conduits 9

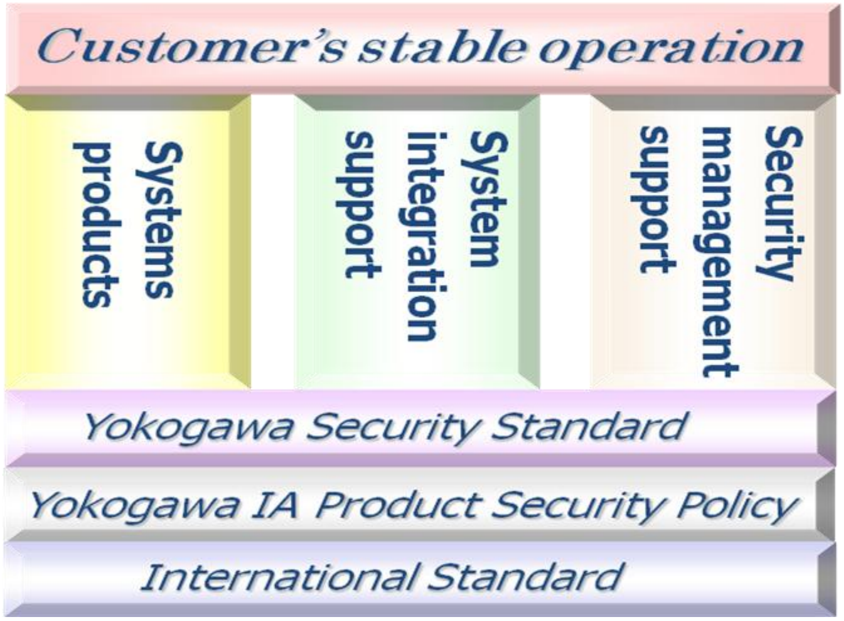
System Integration Competencies 11

Security Management Support 14

Recommendations 17



Yokogawa Security Lifecycle


Customer's stable operation
Systems products
System integration support
Security management support
Yokogawa Security Standard
Yokogawa IA Product Security Policy
International Standard

Yokogawa Security Lifecycle Concept

Executive Overview

Today's process control systems can take advantage of advanced general-purpose IT to reduce costs, improve performance, enable interoperability and add other important new capabilities. However, the very same technologies make today's industrial systems increasingly vulnerable to security intrusions – malicious or otherwise – from both within and without the plant. Certainly, the IT world has developed powerful tools and techniques to help prevent, identify, and mitigate the effects of intrusions. However, requirements specific to industrial systems (such as the need to maintain nonstop operations and provide deterministic response) often make employing these tools and techniques in industrial environments problematic.

Today's cyber-security threats mean that industrial process control system users and suppliers alike must be increasingly vigilant against current and future intrusions that could compromise the security of the system itself, the production process, intellectual property, or negatively impact health, safety, or the environment.

Today's cyber-security threats mean that industrial process control system users and suppliers alike must be increasingly vigilant against current and future intrusions that could compromise the security of the system itself, the production process, intellectual property, or negatively impact health, safety, or the environment (HSE).

Since industrial process control systems typically have a much longer lifecycle than do commercial systems (fifteen or more years for industrial systems, vs. three to five years for commercial systems) and since both system technology and cyber-threats are ever-changing, automation system suppliers must embrace a lifecycle approach to industrial cyber-security. Ideally, this should involve a continuous improvement process of assessment, implementation, monitoring, and maintaining. As explained in this white paper, this is precisely the approach that Yokogawa, one of the world's leading suppliers of process automation systems and related technologies and services, takes with its CENTUM process control systems, ProSafe-RS safety systems, STARDOM and FAST/TOOLS SCADA systems and related instrumentation and software applications.

Yokogawa built its security lifecycle approach upon industry cyber-security standards; plus its own internal product security policy that incorporates both the company's security standards and engineering standards.

Introduction

In the past, industrial automation systems (DCS, SIS, SCADA, etc.) were largely closed, proprietary, and standalone (unconnected) in nature. While this made interoperability challenging, from a security perspective, it minimized opportunities for and the likelihood of external intrusions (malicious or otherwise) from outside the immediate network. Of course, careless, inept, or disgruntled employees still had plenty of opportunities to compromise the security of the process control system, a company's operations, or its intellectual property.

While today's process control systems can take advantage of advanced general-purpose IT to reduce costs, improve performance, enable interoperability and add other important new capabilities; the very same technologies have made today's industrial systems increasingly vulnerable to security intrusions – malicious or otherwise – from both within and without the plant.

However, today's more advanced process control systems are moving closer to the ARC Advisory Group's vision of an open and interoperable Collaborative Process Automation System (CPAS). Furthermore, modern industrial systems increasingly incorporate general-purpose, internet-enabled information technology (IT) developed for commercial and business applications. We often refer to this as "commercial, off-the-shelf technology" or "COTS."

As a result, while today's process control systems can take advantage of this advanced general-purpose IT to reduce costs, improve performance, enable interoperability and add other important new capabilities; the very same technologies have made today's industrial systems increasingly vulnerable to security intrusions – malicious or otherwise – from both within and without the plant. Certainly, the IT world has developed powerful tools and techniques to help prevent, identify, and mitigate the effects of intrusions. However, requirements specific to industrial systems (such as the need to maintain nonstop operations and provide deterministic response) often make employing these tools and techniques in industrial environments problematic.

Several issues and trends further exacerbate the situation. These include the increasing sophistication and resources of the "hackers" themselves and the tools and approaches they use. Even more troubling, are recent incidences of highly sophisticated attacks targeted specifically at industrial systems and networks. Stuxnet and Night Dragon provide two well-publicized examples. In the past, many in the industrial community believed that their systems and networks were "obscure" to the general public and thus safe from cyber-attacks. Clearly, this is no longer the case.

Today's cyber-security threats mean that industrial process control system users and suppliers alike must be increasingly vigilant against current and future intrusions that could compromise the security of the system itself, the production process, intellectual property, or negatively impact health, safety, or the environment (HSE).

Users, suppliers, industry organizations, and national governments – as well as the automation and IT groups within individual user organizations – will need to work together closely to be able to identify and generate effective deterrents and counter-measures to the constantly evolving threat.

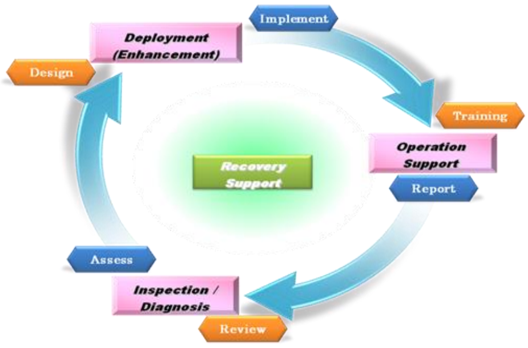
Users, suppliers, industry organizations, and national governments – as well as the automation and IT groups within individual user organizations – will need to work together closely to be able to identify and generate effective deterrents and counter-measures to the constantly evolving threat.

Since industrial process control systems typically have a much longer lifecycle than do commercial systems (fifteen or more years for industrial systems, vs. three to five years for commercial systems) and since both system technology and cyber-threats are ever-changing, automation system suppliers must embrace a lifecycle approach to industrial cyber-security. Ideally, this should involve a continuous improvement process of assessment, implementation, monitoring, and maintaining. As explained in this white paper, this is precisely the approach that Yokogawa, one of the world's leading suppliers of process automation systems and related technologies and services, takes with its CENTUM process control systems, ProSafe-RS safety systems, STARDOM and FAST/TOOLS SCADA systems and related instrumentation and software applications.

Security Lifecycle Approach

Cyber-security experts agree that, given enough time and resources, a dedicated hacker could breach the security of virtually any system – industrial or otherwise. And while networked or internet-connected systems may be a bit more vulnerable than standalone systems, there are many other ways that viruses, trojans, or other malware could be introduced into an industrial system. For example, it's common knowledge that the Stuxnet trojan was probably introduced into affected systems via thumb drives inserted into local USB ports on Windows workstations.

However, with its comprehensive security lifecycle approach that addresses system products, system integration support, and ongoing security management support over the entire lifecycles of its customers' automation systems, Yokogawa believes that it can minimize cyber-security risk for its customers to an acceptable level, and do so without either compromising system performance or incurring excessive cost. With the clear objective of helping to ensure the stable operation of its customers' systems, Yokogawa built its security lifecycle approach upon industry cyber-security standards; plus its own internal product security policy that incorporates both the company's security standards and engineering standards.



Yokogawa Security Lifecycle

Yokogawa invests in the human and technical resources it believes are required to sustain a high level of competence in the cyber-security area. The company supports international cyber-security standards; develops and rigidly enforces internal engineering standards; carefully considers security issues in the development of the company's system products, platforms, and interfaces; and delivers a variety of related lifecycle services. Together, these efforts are intended to help the company's customers reduce cyber-security risk to a degree that is as low as reasonably practical (ALARP).

Industry Standards Provide the Starting Point

ARC strongly advocates that automation suppliers and users alike adhere to appropriate industry standards to the greatest practical extent. While cyber-security is a relatively new discipline, a number of key industry standards for both IT security in general and mission-critical industrial automation systems, have emerged at the national and international levels, with a welcome trend towards convergence. These include standards for policies, procedures, and technologies that address both general-purpose IT cyber-security and industrial automation system-specific cyber-security. Both categories are relevant for the industrial world, since so many industrial systems and applications today are built using general-purpose IT technology and because cyber-security responsibilities for the industrial systems often falls largely on the shoulders' of corporate IT people.

Yokogawa's lifecycle approach to cyber-security recognizes all major established industry cyber-security standards and the company closely tracks relevant standards currently in development. These include the ISA S99 Series, the ISO/IEC 27000 Series, and the NIST SP 800 Series. Yokogawa cyber-security specialists also participate in work groups and technical committees to contribute actively to key industry standardization efforts. These include ISO/IEC (JTC1/SC27, WG3, WG4), IEC (TC65/WG10, TCS7/WG15), and ISA (ISA S99, ISA Security Compliance Institute).

Yokogawa's lifecycle approach to cyber-security recognizes all major established industry cyber-security standards and the company closely tracks relevant standards currently in development.

Yokogawa Product Security Policy

Yokogawa created its Industrial Automation (IA) Product Security Policy based on established industry standards (ISA S99, NIST SP Series, etc.) to help ensure that the company provides secure IA products that protect the integrity of its customers' production-related information assets, while maintaining the functionality of the automation products, systems, and applications. The overall product security policy comprises both a general *Basic Security Policy* and more specific *Product Security Standards* for each product category. Together, they specify issues that a supplier must address at each phase of the product lifecycle: planning, research & development, engineering, quality assurance, sales, after-sales services, and so on.

Significantly, these are "living documents," subject to periodic review by the company's designated, executive-chaired steering committee. In this manner, Yokogawa can continually update its security policies and internal standards as needed to clarify and provide the most effective protective measures possible for its customers.

System Security Standards

Yokogawa's System Security Standard documents provide guidelines and best practices for security countermeasures intended to help protect the company's automation systems and applications from external or internal intrusions or other threats and reduce the risks for its customers' production-related assets. The System Security Standard explains risks and measures (using easily understood language, wherever possible); explains security control techniques; and references both to industry-standard models.

The comprehensive document covers both system configuration and system management issues. Individual sections:

- Outline the **security environment** surrounding the production control system and associated risks
- Provide a systematic framework for an **information security management system** (including identifying specific points of vulnerability and designing and implementing protective measures)
- Provide **technical security control measures** (network architecture, virus protection, patch management, system hardening, system and network monitoring, Windows domain management, security functions of the various Yokogawa systems, and staff security policy)
- Consider **physical protection issues** (defining physical boundaries, managing removable devices, managing third-party maintenance, etc.)
- Provide guidelines for developing a **business continuity plan** to minimize risk and damages from a security intrusion.

Target products for the Yokogawa System Security Standards include the **CENTUM VP** and **CENTUM CS 3000** process automation systems, **ProSafe-RS** safety integrated system, **STARDOM** and **FAST/TOOLS** SCADA system. The standard also covers the company's many solution-based software packages such as the **Exaquantum** plant information management system, **Exapilot** operation efficiency improvement package, **Exaopc** OPC interface package, and **Exaplog** event analysis package.

The overall Yokogawa System Security Standard incorporates a number of documents used across all lifecycle stages (development, system integration, support services) to cover major threats. These include:

- Industrial Automation System Standard
- Applications Security
- Endpoint Security
- Network Security
- Integrated Management System

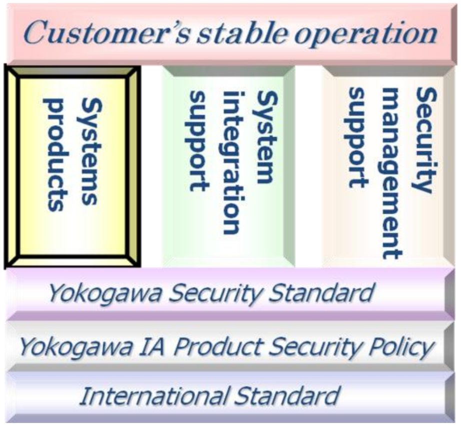
The Security Standard also includes best practices for system hardening, networking, user and account management, monitoring, maintenance, and others.

Global Engineering Standards

Yokogawa has also developed Global Engineering Standards (GES), which it uses to execute projects across its geographically distributed resources. These standards cover a broad range of critical areas, including both physical security and cyber-security. They help bridge the diversity of languages, cultures, and expertise across the company's global organization to help ensure that Yokogawa automation systems implemented anywhere in the world reflect current best practices. Specific GESs include:

- Security and Administration
- Firewall
- Network Management System
- Remote Access Facilities
- Anti-Virus Software Facilities
- Operating System Patch Management
- Windows Domain and Account Management, and
- Backup and Recovery Management

System Products, Platforms, and Conduits


Customer's stable operation
Systems products
System integration support
Security management support
Yokogawa Security Standard
Yokogawa IA Product Security Policy
International Standard

A complete industrial automation system solution is comprised of individual hardware and software products residing on a common platform with a variety of different interfaces, or "conduits," both internal and external to the system. To achieve cyber-security defense in depth, appropriate security must be designed into each system component and conduit, supported by appropriate integration, operation, and management practices. Defense in depth also requires appropriate security between plant control networks and external networks (via firewall-protected "demilitarized zones"); within the plant control network itself; and robust, well-structured endpoint security at the workstation level.

Security Zones and Conduits

To help ensure appropriate system security, the system supplier must match the security assurance levels (SAL) of various physical or logical groups of system products to the specific requirements of the different plant areas, or "zones" in which they are applied. Security assurance levels and security zones, which are somewhat analogous to the safety integrity levels (SIL) used for process protective and other safety systems, are described within the ANSI/ISA S99 security standards.

According to the company, Yokogawa system products provide the mission-critical reliability and robustness required to help ensure safety and security. The company also aligns the critical conduits between zones (a prime target for intrusions) with the appropriate target SAL. This includes zone-to-zone conduits, component-to-component conduits, and operator interface-to-component conduits.

Security Designed into Individual System Products

Consistent with the company's lifecycle approach to cyber-security, rather than viewing security as a pasted-on afterthought, Yokogawa system architects, engineers, and product development experts start the product design process from a clean sheet of paper. This enables them to design security into the actual product specifications. This security focus at the component specification level provides the company with a basic advantage when it comes to achieving a high level of security at the system integration stage.

> Consistent with the company's lifecycle approach to cyber-security, rather than viewing security as a pasted-on afterthought, Yokogawa system architects, engineers, and product development experts start the product design process from a clean sheet of paper.

In the product development stage, Yokogawa's development engineers check the source code for software-based products, using third-party tools to remove common vulnerabilities.

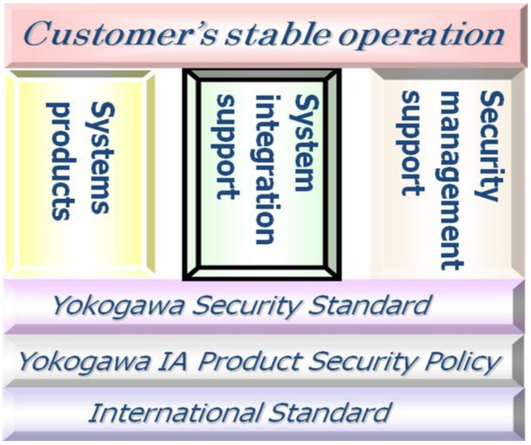
Prior to commercialization, Yokogawa system products are certified using the company's extremely rigid internal certification process, based on established international standards. In addition, as a fundamental part of the product lifecycle, Yokogawa system products undergo security evaluation conducted by external security consultants based upon their prescribed practices and proven technologies.

Finally, as part of the lifecycle approach, the company's development engineers based at various locations around the world participate in an ongoing education program designed to familiarize them with the latest threats, potential vulnerabilities, and countermeasures.

Building Secure Industrial Control Systems

Many established practices exist for building security into both commercial IT systems and industrial control systems. Yokogawa has borrowed from these and developed its own best practices, technical standards, procedures, and tools to meet customer requirements for safe and secure industrial automation systems. These provide a solid bridge between individual Yokogawa industrial control system products (I/O, controllers, data servers, application services, workstations, software applications, etc.) and a total system solution.

System Integration Competencies


Customer's stable operation
Systems products
System integration support
Security management support
Yokogawa Security Standard
Yokogawa IA Product Security Policy
International Standard

Designing and certifying the individual industrial control system components with security in mind is all well and good, but what really counts when production and human health and safety are on the line, is how safe and secure the total system functions as a whole. For this reason, Yokogawa places considerable emphasis on how its engineers go about integrating the various system hardware and software components into a functioning system intended to monitor, control, and manage critical industrial processes on an uninterrupted basis 24 hours a day, 7 days per week.

Yokogawa has been supplying its customers with complete process control systems for over 30 years. In this time, the company has developed unique expertise in systems integration that carries over into the security domain. Specifically, it is extending well-proven knowledge management tools – such as its Global Engineering Standards, Yokogawa's internal standard for executing projects that provides the standards and templates for unifying project implementation – into the physical and cyber-security domains.

Since industrial control systems typically have much longer life cycles than do commercial information technology systems, Yokogawa has developed a total system architecture that avoids the potentially negative impacts of periodic technology updates. The company's internal system integration standards and practices further support this critical independence from the frequent technology refreshes encountered in the IT world.

Furthermore, Yokogawa engineers receive comprehensive training in both systems integration and cyber-security to improve their security knowledge and skills. This includes basic, advanced, and practical (hands on) training courses, with mandatory periodic testing to help ensure the effectiveness of the training:

- Basic course – covers total system architecture
- Advanced course – covers Windows domain and account management, OS patch management, firewalls, Level 2/Level 3 switches, remote access, anti-virus software, network management, and backup and recovery management
- Practical course – provides hands-on experience in all of the above

Yokogawa also offers similar training for its users. These training courses, based upon the company's comprehensive internal training courses, are detailed enough for users to implement the security lifecycle for their control systems.

Design, Implement, Verify

The company's internal system integration process involves a three-stage design/implement/verify process, supplemented by a training and certification program for its engineers based in various Yokogawa engineering centers around the world. Yokogawa's Global Engineering Standard and Security Standard govern the system integration design process. The Yokogawa Security Standard, supported by the company's system design tool, governs implementation. Specialized tools test the robustness of the integrated system and verify that the integrated system conforms to the Yokogawa Security Standard.

System Hardening Tools and Verification

Typically, Windows operating systems are designed to provide home and office users with maximum functionality and ease of use. However, in industrial environments, safety and security take precedence over potentially vulnerable, non-essential functionalities and ease-of-use features. To minimize vulnerabilities for its industrial users, Yokogawa employs system hardening tools to configure Windows OS parameters in a manner that eliminates non-required functionalities and possibly exploitable weaknesses, and to increase the dependa-

Typically, Windows operating systems are designed to provide home and office users with maximum functionality and ease of use. However, in industrial environments, safety and security take precedence over potentially vulnerable, non-essential functionalities.

bility of the OS. Target operating systems include Windows XP, Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2.

This hardening tool runs two different procedures depending on the designed security policy and the integrated system in question and the relative sensitivity of the application. The objectives are to:

- Harden Yokogawa systems products throughout with a single security model in which the OS is secured against attack from both internal or external networks, such as third-party devices or networks
- Allow Yokogawa systems products to be combined with legacy systems, for which latest and most recommended security procedures in industrial environments do not apply

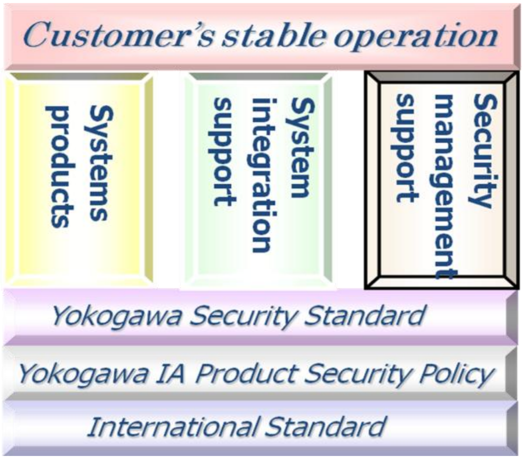
Furthermore, additional strengthened procedures are supported for Yokogawa systems products, which the company implements as needed to match the specific risk levels for different environments.

Using Security Standards as a basis, Yokogawa engineers use the company's system hardening tools to configure the PC/server so that base (registries, services, and local security policy), networking (personal firewall, file sharing control, NetBIOS over TCP/IP, DCOM setting, etc.), user account management and access control, and USB control are all configured securely.

These actions – supplemented by a rigorous verification program that uses custom plug-in tools to verify robustness – help ensure that the company can deliver an integrated, yet secure system to its global customers. The company can also use these tools to verify the robustness of customers' existing system. During the verification program, users are provided with a simple and comprehensive view of the security level of their control systems based upon the company's defined indexes. Yokogawa has developed "PARM" indexes that make it easier for users to comprehend industrial control system security levels. Here, the P stands for "data protectability," A for "availability," R for "recoverability," and M for "manageability." PARM translates all seven ISA99 foundational requirements into a simplified view using these four indexes.

As the original equipment manufacturer, Yokogawa has the specific knowledge, expertise, and tools needed to verify the robustness of the company's systems. However, the company also subscribes to third-party organizations, such as the Industrial Security Compliance Institute ("ISA Secure") to certify appropriate Yokogawa system products. The company has set up the policy to incorporate security steps into systems and products development processes, to develop a user security guide, and to continuously improve both process and user security with support from independent subject matter expert (SME) consultants.

Security Management Support


Customer's stable operation
Systems products
System integration support
Security management support
Yokogawa Security Standard
Yokogawa IA Product Security Policy
International Standard

As previously mentioned, the constantly evolving nature of the cyber-security threat and the dynamic nature of modern automation technology and applications, require a lifecycle approach to cyber-security. Yokogawa is equipped to ensure that the systems the company delivers, installs, and commissions in its customers' plants are as up to the challenge as humanly and technically possible.

However, constant vigilance is required to anticipate, identify, and mitigate the inevitable vulnerabilities and cyber-security threats that emerge after the system is commissioned. And, unfortunately, while user organizations often have adequate internal resources to deal with cyber-security threats against the corporate network, only in rare cases do corporate IT departments fully understand the operating environment and security-related ramifications for process control, process protective, SCADA, and other plant-level systems and networks. This is where automation supplier-provided security management services – such as those that Yokogawa offers under its VigilantPlant Services offering – can provide so much value to user organizations. The company's cyber-security consultants combine in-depth expertise in latest cyber-security approaches, techniques, and toolsets; with a full understand of industrial environments in general and inner-knowledge of Yokogawa system products, process control networks, and software applications. Yokogawa's VigilantPlant Service is designed to offer users the ability to achieve continuous improvement throughout the lifecycle based upon the DMAIC concept.

Assessment and Consultation

While older plant control systems can be particularly vulnerable to cyber-security threats, even recently commissioned systems could have been exposed to new threats in the interim since commissioning. Yokogawa's VigilantPlant Service offers security assessment and consultation services in which customers are encouraged to deploy required countermeasures into installed control systems. This service is designed to help users manage risks and maintain business continuity by assessing, inspecting, and diagnosing installed systems to detect and identify specific weaknesses and potential cyber-security vulnerabilities.

Yokogawa's deliverable from this important service is a detailed assessment report and recommendations for appropriate countermeasures. The countermeasure implementation service then follows up on these recommendations.

Countermeasure Implementation

Many industrial organizations lack the internal resources needed to deal with identified threats to their industrial systems and networks in a manner that will not negatively impact production operations or health, safety, and environment. To respond to this need, Yokogawa created an additional VigilantPlant Service to deliver appropriate, non-intrusive countermeasures to the assessed threats and/or vulnerabilities of installed control systems following the assessment and consultation service.

The service includes:

- Virus check
- USB port lock
- Security patch update
- Software backup and recovery
- Unauthorized software control

Even in the face of constantly evolving cyber-security threats and evolving platform technology, these services can help ensure that installed systems remain as robust and secure over their entire lifecycles as they are at commissioning.

Maintenance and Support

It's important to be able to maintain all deployed countermeasures in a cost-effective manner. An essential part of the lifecycle, this is required as part of the security management system to continuously secure the control system. Yokogawa offers a support and maintenance service in VigilantPlant Service to keep the deployed countermeasures running and apply updates for vulnerabilities uncovered during normal operations. The company also offers users training to help customers implement their security lifecycle. This can be followed by additional assessment and consultation, as needed.

Yokogawa Security Competency Laboratories

Yokogawa's Security Competence Laboratories in Singapore; Tokyo, Japan; Bangalore, India; and Houston, Texas play a key role in the company's overall cyber-security activities. Collectively, these laboratories serve as a dedicated center-of-excellence in which Yokogawa system and cyber-security specialists can collaborate to link current security technologies to the company's systems to help protect the company's customers from constantly evolving and increasingly sophisticated cyber-security threats.

The Security Competence Laboratories research today's security technologies and real-world cyber-security implications for industrial operating environments and develop solutions and countermeasures that are best suited for different industry sectors, applications, and system configurations. The labs build upon the company's technical expertise to develop, validate, and deploy new procedures and tools for the Yokogawa engineers and security specialists who deliver the company's security and other services.

Another role for Yokogawa's Security Competence Laboratories is to continually update the Yokogawa security standard, including documents and work processes.

Recommendations

Security experts agree that, given adequate time and resources, any system – even hardened, relatively segregated, industrial control systems – can be penetrated by determined external hackers or careless or disgruntled employees. However, clearly, there are ways to reduce the risk to an acceptable level (as low as reasonably practical) and to do so without compromising the basic functionality of the system.

ARC believes that Yokogawa's lifecycle approach to automation system security (built on industry security standards and best practices), plus the company's own security and engineering standards, work together to enforce defense in depth to help provide a solid foundation for secure industrial control systems and stable plant operation.

ARC believes that Yokogawa's lifecycle approach to automation system security (built on industry security standards and best practices), plus the company's own security and engineering standards, work together to enforce defense in depth to help provide a solid foundation for secure industrial control systems and stable plant operation. The company's well-trained global services organization is also available to provide ongoing cyber-security support to help users meet new daily threats with a technology platform that evolves over time.

However, it's equally important for end users in manufacturing companies and other industrial organizations to recognize that they can't expect their automation suppliers – no matter how vigilant – to provide a total cyber-security solution. To reduce security risks to an acceptable level, users must cultivate a "security culture" across all departments and develop and enforce internal security processes and practices based on ANSI/ISA S99, NIST SP 800, and other industry standards and best practices.

YOKOGAWA
Security Competence Laboratory

Analysts: Barry Young and Paul Miller

Editor: Dick Hill

Acronym Reference: For a complete list of industry acronyms, refer to our web page at www.arcweb.com/Research/IndustryTerms/

API	Application Program Interface
B2B	Business-to-Business
BPM	Business Process Management
CAGR	Compound Annual Growth Rate
CAS	Collaborative Automation System
CMM	Collaborative Management Model
CPG	Consumer Packaged Goods
CPM	Collaborative Production Management
CRM	Customer Relationship Management
DCS	Distributed Control System
EAM	Enterprise Asset Management
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
IOp	Interoperability
IT	Information Technology
MIS	Management Information System
OpX	Operational Excellence
PAS	Process Automation System
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
RFID	Radio Frequency Identification
ROA	Return on Assets
RPM	Real-time Performance Management
SCM	Supply Chain Management
WMS	Warehouse Management System

Founded in 1986, ARC Advisory Group is the leading research and advisory firm for industry. Our coverage of technology from business systems to product and asset lifecycle management, supply chain management, operations management, and automation systems makes us the go-to firm for business and IT executives around the world. For the complex business issues facing organizations today, our analysts have the industry knowledge and first-hand experience to help our clients find the best answers.

This research has been sponsored in part by Yokogawa. However, the opinions expressed by ARC in this paper are based on ARC's independent analysis.

You can take advantage of ARC's extensive ongoing research plus experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For membership information, please call, fax, or write to:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA
Tel: 781-471-1000, Fax: 781-471-1100, Email: info@arcweb.com
Visit our web pages at www.arcweb.com

ARC
arcweb.com