White Paper :

Yokogawa Innovative Plant Automation Security Solutions

Contents

1. Industrial Automation and Business Network Integration

The process control network has evolved from individual isolated computers with proprietary operating systems and networks to interconnect various systems and applications employing commercial-off-the-shelf technology. This process control network is now integrated to the business enterprise systems and other applications through various communication networks.

The list below is the network and system integration business benefits:

- Increased visibility of process control network activities (work in process, equipment status, production schedules) and integrated processing systems from the business level which contributes to the capability improvements to conduct analysis, to drive down production costs and improve productivity.
- Integrated manufacturing and production systems that have more direct access to business level information and enabling more responsive enterprise.
- Common interfaces that reduce overall support costs by permitting remote support to production processes.
- Remote monitoring of the process automation system that reduces support costs and allows problems to be resolved quickly.

Although the integration of the process control network and business network provides a lot of benefits, it also increases system vulnerability from misuse and attack by individuals with malicious intent. Another potential risk is the compromised business network spreading to process control network. The potential security breach from cyber-attack has far more serious consequences. The likelihood of the process control system under attack or virus/malware infection is real and is just a matter of time. With this, network and system security is now a necessity in process automation industry.

1.1. Necessity of IA System Security

Security Risk – Malware Attack in Ukrainian Power/Energy Production Facility

BlackEnergy is a crime ware that has been used for years by various criminal outfits targeting political organizations. This toolkit is popular among Russian cyber undergrounds dated back since 2007. Its original designed was a toolkit for creating botnets used in conducting Distributed Denial of Service (DDoS) attacks. In the summer of 2014, it is noted that certain samples of BlackEnergy malware began targeting Ukranian government organizations especially during Russian military annexation to Crimea. The BlackEnergy samples were identified as being the work of one group as “Quedagh”, which has a history of targeting political organizations.

Refer to Figure 1-1 How BlackEnergy Work

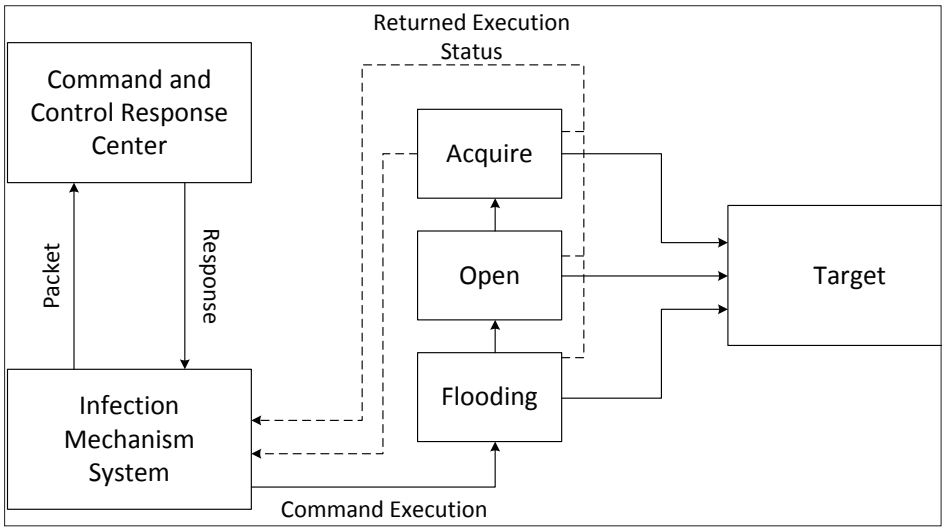

Figure 1-1 How BlackEnergy Work

Security Risk – Malware Attacks: It is not only Stuxnet!

Stuxnet is one of the well-known malware targeting the process control system. Base from the recent statistics, since the birth of Stuxnet virus in 2010, series of highly sophisticated malwares were reported and detected on process

control computers. These malwares unlike any other virus that came before, it is designed to steal sensitive plant operation data, gather information for next attack and wreak havoc and physical destruction on the target process automation system. These malwares are now capable of causing greater damage than what has been seen before.

The Stuxnet source code is now easily available in the internet. The possibility of another sophisticated malware will emerge emulating the Stuxnet infection philosophy with innovated technique. In fact, the Sality virus which infected industrial networks took advantage of the Stuxnet USB exploits. In 2011, the Duqu virus infected industrial network computers and is equipped with modules for SCADA attacks. It is designed to steal sensitive information from the infected host system.

Another case of industrial network infection was the Flame virus. Flame virus is designed to carry out a cyber-espionage. It can steal valuable information such as computer display contents, information about targeted systems, stored files, contract data and even audio conversations. Its complexity and functionality exceed those of all other known cyber weapons. To address this problem, the process control network needs security standards like the business network system but are these standards should be catered for the ICS.

Refer to Figure 1-2 How Stuxnet Work.

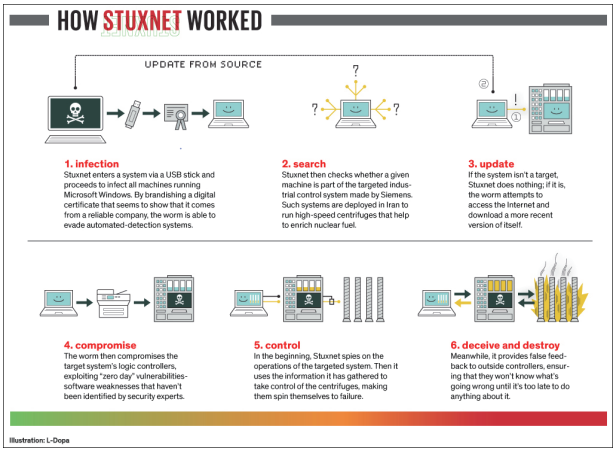

Illustration source: IEEE Spectrum
Figure 1-2 How Stuxnet Work

Attack and Detection History.

Over the years, there are several detection and attacks reported in the process control network. Refer to Table 1-1 for the list.

Table 1-1 Well-known Process Control Network infection/detection

YEAR	VIRUS/MALWARE NAME	VIRUS/MALWARE DESIGN
2009	Night Dragon	Remote Access Trojan distrubited through spearphising
2010	Stuxnet	Intercept and Changes Data targetting Siemen's PLC System
2011	Duqu	Cyberespionage equiped with modules for SCADA attacks
2012	Flame	Cyberespionage intended to steal sensitive operational data
2012	Shamoon	Eliminate and overwrite the information on the hard drives
2014	Dragonfly	Cyberespionage targetting energy sector
2016	BlackEnergy	Backdoor for cyberespionage and crimeware toolkit targetting energy sector

1.2. Yokogawa Cyber Security for Industrial Control System

Yokogawa developed a comprehensive network and system security for its industrial process control systems. These security solutions address common and known internal/external system vulnerabilities. And these security solutions can be deployed to a new project or to existing and running facility.

The following list is the Yokogawa approach in developing network and system cyber security:

Security Competence

The research and development centers of Yokogawa are located across the globe to develop security techniques for the process control system. With a long experience in control system integration, these centers develop security techniques and solution optimized to each industry, application and system configuration.

Security in Products

The product lifecycle ensures that vulnerabilities are reduced due to the improved system architecture design and applying latest technologies in developing process automation systems. External security assessment and certification are continuously done as part of the growth development.

Growing with the Industry Standard

The security expert and development team are actively participating in the development of international industrial standards from ISO, IEC and ISA. In addition, Yokogawa has been developing techniques and solutions for the purpose of security risk management for process automation systems.

Industry Best Practice

In the implementation of security controls, specific requirements and consideration are required for the process control network. In Yokogawa, based from its long years of experienced in the control system has established best practice in the implementation of security controls. These best practices are compliant with international and industrial security standards.

1.3. IA System Security Priorities

1.3.1. AIC vs. CIA

Although the security technologies for the control system and the business network are mostly the same, the priorities are completely different. The International Society of Automation (ISA) defined the priorities of the control system as Availability, Integrity and Confidentiality (AIC).

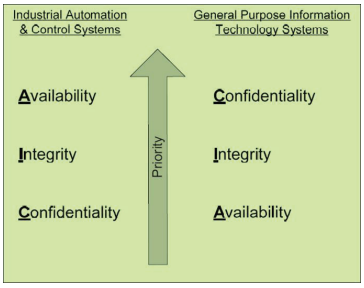

Figure 1-3 Priority (ANSI/ISA99)

Figure 1-3 Priority (ANSI/ISA99) shows the IAC comparison table between process automation systems and general purpose network.

Refer to Table 1-2 for Control System and IT System comparison.

Table 1-2 Cyber Security Consideration of IT System VS IA System

Category	IA System	IT System
Performance Requirements	Real-time Response is time-critical	Non-real-time Response must be consistent
Availability Requirements	Rebooting may not be acceptable Redundant systems may be required Outages must be planned and scheduled in advance	Rebooting are acceptable
Risk Management Requirements	Human safety is paramount; Followed by protection of the process; Fault tolerance is essential	Data confidentiality and integrity is paramount Fault tolerance is less important

Architecture Security Focus	Primary goal is to protect end devices (e.g., field devices such as process controllers)	Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets
Unintended Consequences	Security tools must be thoroughly tested to ensure that they don't compromise normal ICS operation	Security solutions are designed around typical IT systems
Communications	Many proprietary and standard communication protocols Networks are complex and sometimes requires the expertise of control engineers	Standard communications protocols Typical IT networking practices
Change Management	Software changes must be thoroughly tested and deployed incrementally throughout the system to ensure that the integrity of the control system are properly maintained	Software changes are applied in a timely fashion in the presence of good security policy and procedures

1.3.2. OT vs. IT

Connecting industrial devices, systems, and applications to provide plant and enterprise personnel with actionable information is not a new concept. Leading automation and software suppliers have been working diligently to address this requirement for decades. These efforts have not always been entirely successful, due in large part to poor interoperability between oper-ational technology (OT) and information technology (IT). This has hampered business performance.

At the OT level, a large number and variety of differ-ence sensors, intelligent field devices, control-lers, systems, mobility devices, application soft-ware, networking, and security com-ponents come into play relative to the Industrial Internet of Things. While these come in a wide variety of "shapes and siz-es," all feature some degree of built-in intelligence, self-diagnosis capabilities, connectivity, and support for analytics.

Refer to Figure 1-4 Yokogawa Integration of OT with IT Concenpt.

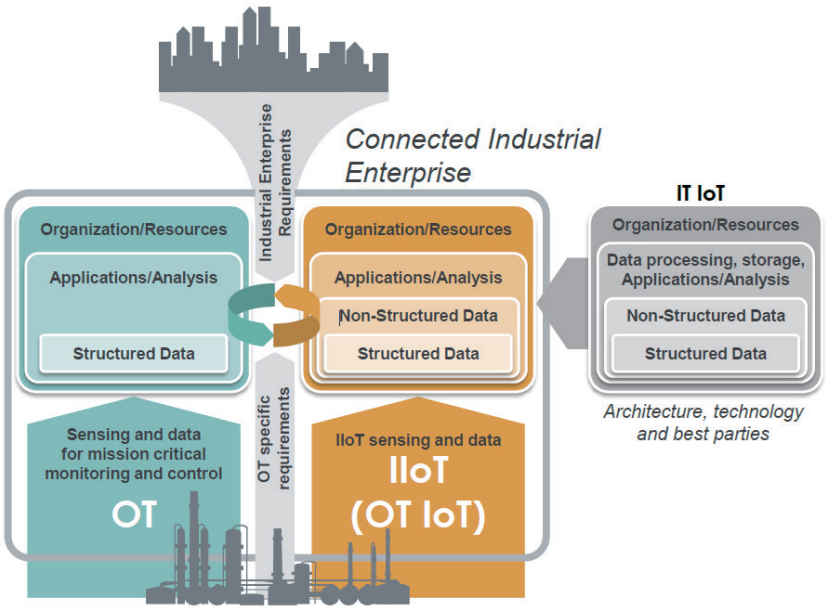

Figure 1-4 Yokogawa Integration of OT with IT Concenpt

Yokogawa believes that it can add significant value in the operational technology (OT) domain, while helping ensure the prerequisite integration of OT by work-ing closely with both IT enterprise solutions.

In addition of supplying a wide variety of related industrial hardware, software, and services, this includes taking advantage of the company's deep knowledge of industrial organizational issues; real-time data pro-cessing, data storage, and analysis; and managing data from devices, machines, and other "things" in the plant and in the field.

Yokogawa's VigilantPlant approach helps ensure the appropriate rigor required to make sure that OT integration with

IT solutions meet the demanding safety, security and availability requirements for mission-critical industrial automation. Refer to Table 1-3 OT and IT Operation Comparison Table for detailed comparison category between OT and IT.

Table 1-3 OT and IT Operation Comparison Table

Category	Operational Technology (OT)	Information Technology (IT)
Purpose	Control Systems; control or monitor physical processes or equipment, regulatory security standards	Transaction Systems; business systems, information systems, IT security standards
Architecture	Event-drive, real-time, embedded hardware and software (industrial)	Enterprise wide infrastructure and applications (business)
Interfaces	Electromechanical, sensors, Windows, actuators, coded displays – PLC, SCADA, DCS	Operating systems and applications, Unix, GUI, Web browser, terminal, and keyboard
Ownership	Engineers, technicians, operators, and managers	CIO, finance and admin. departments
Connectivity	Control networks, hard wired twisted pair and IP-based	Corporate network, Internet, IP-based
Role	Support controls processes and plant personal safety	Supports business applications and office personnel

An effective critical infrastructure cyber security plan requires clearly defined and coordinated roles and responsibilities among OT personnel and IT. However, as critical infrastructure systems and assets become more interconnected, accountability gaps as well as perceived overlaps have formed between the functional roles.

2. Continuous Security Concept

2.1. What are the Demands

The demands that are coming from process control system and customers are now different. Integration with open systems using the latest technology devices and network integration are now part of the list. And because of the fast changing technology, the possibilities are almost endless and security needs to cope up and address those know issues and vulnerabilities.

Demands from the operational perspective:

- More use of Commercial-Off-The-Shelf (COTS) infrastructure
- Continued integration of Operation Technology (OT) / Information Technology (IT) infrastructure
- Integrated sensor networks with embedded IT
- Use of industrial wireless for process control
- Need for big data infrastructure and low cost IT solutions
- Remote workforce and operation management
- Push towards un-manned operations

2.2. Security Lifecycle Approach

As the control system technologies are constantly evolving, security risks such as attack techniques are also evolving. Based from the reports, the attacks targeting industrial control systems have been increasingly in alarming rate. This means that one time deployment of security controls is not enough to mitigate those security risks. YOKOGAWA provides a service lifecycle solution for cyber security. This is to ensures that the security measures and deployments are continuously enhanced, monitored and inspected.

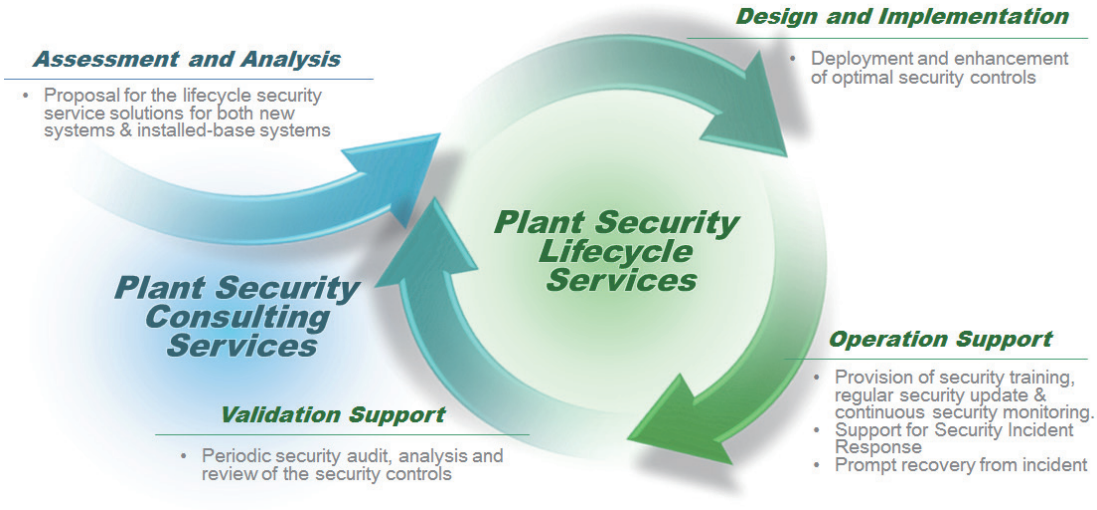

Figure 2-1 Lifecycle Approach

Referring to Figure 2-1 Lifecycle Approach, Yokogawa approach is composed of 4 items that would start from the assessment of the system until the validation of the security controls. This approach ensures that the design and implementation are catered not only for the industry but for each customer's environment.

Assessment

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

- Security assessment and discussions using a simple questionnaire for Yokogawa system and Non-Yokogawa system
- Conduct proof-of-concept for cyber security integration for the existing facility
- Conduct security technical seminars

Design & Implementation

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

- Design and plan security policy programs
- Design the network architecture and cyber security solutions from lifecycle perspective
- Design implement physical security solutions such as USB lockdown and unique cabinet keys
- Implementation of integrated network security solutions like AD, WSUS, AV, NMS, BRS, system hardening and so on
- CSMS during project execution
- Endpoint Security Service

Operation Support

Yokogawa provides customer training to ensure that customers can operate and maintain the security lifecycle appropriately. The following services will be provided to ensure that the threats are addressed accordingly and the vulnerabilities can be identified on time.

- Checking of the deployed security controls
- Update the virus definition files and security updates at regular intervals
- Check the negative impact to Yokogawa's products by the above updates and to provide a report
- Training of Security Awareness, Policy and Solutions
- Network and security system monitoring for automation control system
- Centralized Security Management Infrastructure and Managed Services
- Incident Response Support

Validation Support

Yokogawa also supports auditing the security level of the entire system to ensure that new threats can be addressed. Considering newly detected threats and vulnerabilities, Yokogawa will provide commercial and technical proposal upon request for the following security controls:

- Security controls reassessment against known threats and vulnerabilities
- New threats and vulnerabilities proposal
- Audit security program
- Security program efficiency analysis
- Recommend enhancement plan report

2.3. Defense in Depth

Yokogawa recommends a comprehensive approach based on the defense in depth strategy. This not only means deploying multiple technical controls, but the most important things is ensuring the safety and performance of the control systems. This balance is required for production activity and maintaining the process system healthiness. This followed by implementing technical, operational and managerial controls for cyber security, these can be improved by the continuous activities through cyber security lifecycle to ensure that risks to the control systems are prevented or mitigated. In case of confirmed infection, a quick system recovery can be initiated.

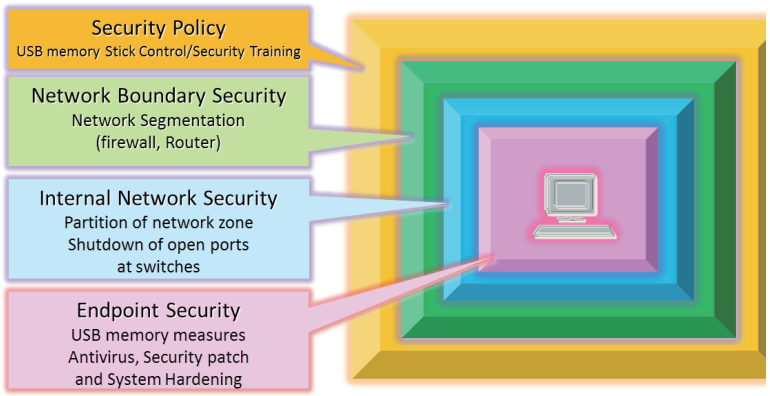

Figure 2-2 Defense in Depth

2.4. Yokogawa Security Competency Laboratories

Yokogawa's Security Competence Laboratories all over the world 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.

Figure 2-3 Cyber Security Compentency Laboratory

See the full report to consider the countermeasures for ICS cyber attack.

Register to the Yokogawa Partner Portal for access to the full report.

→ **Yokogawa Partner Portal ; Service Documents**

https://partner.yokogawa.com/global/member/service/svdoc_index.htm


White Paper :
Yokogawa Innovative Plant Automation Security Solutions

Contents

Yokogawa Electric Corporation

YOKOGAWA ELECTRIC CORPORATION
9-32, Nakacho 2-chome, Musashino-shi, Tokyo 180-8750, Japan

Represented by:

[Ed:02/d] 803

YOKOGAWA Co-innovating tomorrow®