Technical Information

Security Standard of System Product

TI 33Y01B30-01E

YOKOGAWA

Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

TI 33Y01B30-01E

7th Edition Nov. 2019 (YK)

Blank Page

Introduction

This document is a guide to the security countermeasures that can be used to protect the production control system from threats and reduce the risks for assets related to production activities. In this document, risks and measures are explained in generalized terms as much as possible, and the security control techniques are explained and referenced to industry standard models.

To cope with the growing threats, this guide will be revised as necessary. Also, there are other documents for each product to describe the detailed implementation procedures.

Target Products

This document is written for the following system products. However, the general explanations can be used for other equipments and software products.

- Integrated Production Control System — CENTUM VP
- Safety Instrumented System — ProSafe-RS
- Network Based Control system — STARDOM
- Plant Resource Manager — PRM
- Paper Quality Measurement and Control System — B/M9000 VP
- Solution-Based Software Packages
  - OPC Interface Package — Exaopc
  - Plant Information Management System — Exaquantum
  - Operation Efficiency Improvement Package — Exapilot
  - Event Analysis Package — Exaplog
- SCADA Software — FAST/TOOLS

Trademark Acknowledgements

The names of corporations, organizations, products and logos herein are either registered trademarks or trademarks of Yokogawa Electric Corporation and their respective holders.

Blank Page

Security Standard of System Product

TI 33Y01B30-01E 7th Edition

CONTENTS

1. Quick Start

First we will show the outline of the network configurations of the system for which this document is written and the sections where each configuration is described in this document. Please use this part as a navigator to the contents of this document.

Outline of the configuration

Chapter 2 : Necessity for Security

In this chapter, the outline of the environment surrounding the production control system is shown. The assets that should be protected by security measures and examples of security risks will be explained.

Chapter 3 : Security Standards and Certifications

In this chapter, frameworks and standards are explained when security measures are applied to IACS (*1).

*1: IACS is an abbreviation for “Industrial Automation and Control System(s).” It is a generic name for industrial control systems,and it consists of control systems such as DCS, SIS, PLC, SCADA, networked electronic sensing, and monitoring diagnostic systems. This term is often used in security related documents for control systems.

Chapter 4: Security control

The main theme of this chapter is technical security measures. Please see “Figure Outline of the system” for the description and its actual application to the system configuration.

Chapter 5: Physical protection

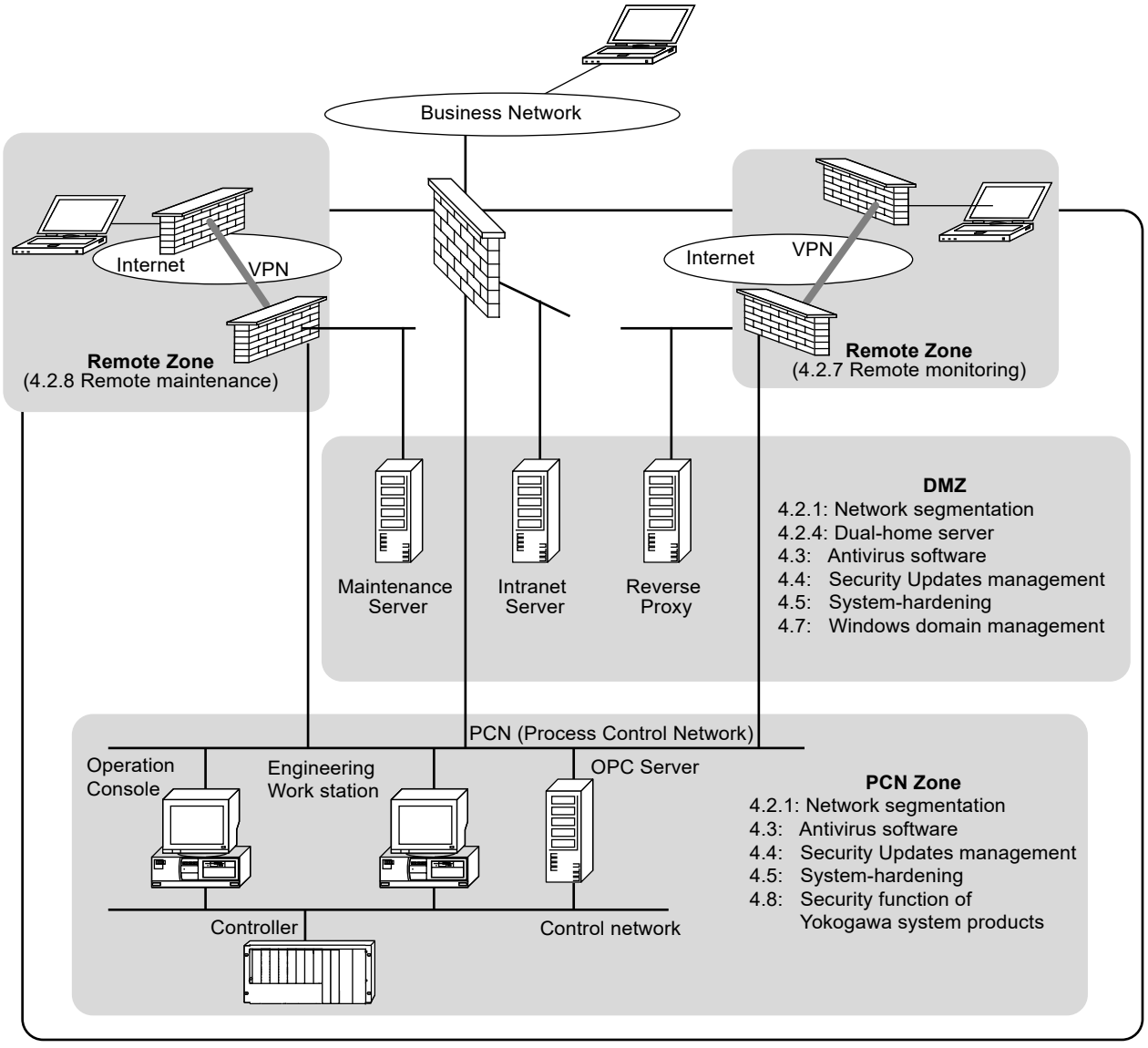
In this chapter, the consideration of physical protection of instruments is explained.

Chapter 6: Business continuity plan

In this chapter, we provide the users with information about what is to be planned for the time when the security incidents should happen and result in damages.

Sections where each configuration is described

Guide about system configuration



F0101E.ai

Figure Outline of the system

Guide about management of systems

3: Information Security Management System (ISMS)

4.9: Staff Security Policy

5: Physical Protection

6: Business Continuity Plan

Glossary

The following table describes the terms commonly used in this document.

Table Glossary terms(1/2)

Term	Description
ANSI	Abbreviation for “American National Standards Institute.”
CSMS	Abbreviation for “Cyber Security Management System.” It is modified from ISMS for control systems. It is standardized by ISA99 (to IEC 62443).
DCS	Abbreviation for “Abbreviation for “Distributed Control System.” In Yokogawa products, CENTUM VP falls under this category.
DMZ	Abbreviation for “Demilitarized Zone.”
DoS	Abbreviation for “Denial of Service.” It is an attack that sends a large (meaningless) service connection request to various servers such as Web server, FTP server, mail server, etc., increases the load on the server, causes the server to go down due to overload, or hinders in services for other legitimate users.
EDSA	Abbreviation for “Embedded Device Security Assurance.” It is a certification program for control devices. Originally, it was a certification program based on ISA99 by ISCI, and called as "ISASecure EDSA certification. It is now proposed as IEC 62443-4.
ENG	Engineering Station of CENTUM VP.
FCS	Field Control Station of CENTUM VP.
HIS	Human Interface Station of CENTUM VP.
HMI	Abbreviation for “Human-Machine Interface.”
IACS	Abbreviation for “Industrial Automation and Control Systems.” It is a term used in ISA99 and IEC 62443, and it means a generic expression for industrial control systems. It includes DCS, SIS, PLC, SCADA, SBP. Moreover, advanced control solutions, manufacturing execution system (MES), etc. are included.
ICS	Abbreviation for “Industrial Control System.” This term is used in NIST, etc. It is the same meaning as PCS in this document.
IEC	Abbreviation for “International Electrotechnical Commission.”
IPS	Abbreviation for “Intrusion Prevention/Protection System.” It is a real-time system that detect an intrusion to networks or servers, defends by cutting off connections, informs administrators, and outputs logs. The one that has an intrusion detection function only is called "Intrusion Detection System (IDS)."
ISA	Abbreviation for “International Society of Automation.” Originally, it was "Instrument Society of America," but changed to "The Instrumentation, Systems, and Automation Society" in 2000. Moreover, it has changed to the current name in 2008.
ISA99	It points to ANSI/ISA-99 series "Security for Industrial Automation and Control Systems." It was called ISA-SP99 before. At present, ISA-99 is unified to IEC 62443. In accordance with this situation, its ISA number has changed from ISA-99 to ISA-62443.
ISCI	Abbreviation for “ISA Security Compliance Institute.” It is a subordinate organization of ISA, and specialized in security.
ISMS	Abbreviation for “Information Security Management System.” It is organized security measures for general information systems. It became an international standard as the ISO/IEC 27000 series.
NIST	Abbreviation for “National Institute of Standards and Technology” in USA.
NMS	Abbreviation for “Network Management System.” It manages network devices and network information (IP address, port connection information, circuit information, etc.), and grasps the operating situation and an omen of disorder in real-time.
OPC	Abbreviation for “Open Productivity & Connectivity.” At first, it was used as an abbreviation for "OLE for Process Control," but it was changed to the current name in 2008.
PCN	Abbreviation for “Process Control Network.” A control bus used by DCS and SIS. This term is defined in this document.
PCS	Abbreviation for “Production Control System.” It includes DCS and SIS. This term is defined in this document.
PLC	Abbreviation for “Programmable Logic Controller.” In Yokogawa products, FA-M3 falls under this category.

Table Glossary terms (2/2)

Term	Description
RAS	Abbreviation for “Remote Access Server.”
SBP	Abbreviation for “Solution-Based Package.” In Yokogawa products, Exa series software falls under this category.
SCADA	Abbreviation for “Supervisory Control and Data Acquisition.” In Yokogawa products, FAST/TOOLS falls under this category.
SCS	Safety Control Station of ProSafe-RS.
SENG	Safety Engineering Station of ProSafe-RS.
SIS	Abbreviation for “Safety Instrumented System.” In Yokogawa products, ProSafe-RS falls under this category.
VPN	Abbreviation for “Virtual Private Network.”

2. Necessity for Security

Along with the recent advancement in network and information technologies, latest production control systems have adopted open technologies used in information systems, such as OS and communication protocols. It is an accelerating factor for establishing close connections between information systems and production control systems.

On the other hand, in this kind of open environment, production control systems are targeted by malicious attackers represented by computer viruses and others that cause hazardous incidents.

Nowadays, security threats aimed at production control systems are increasing by malwares (i.e. worms, viruses, Trojan horse, etc.) and appearance of Advanced Persistent Threats (APT) (i.e. targeted attacks).

In order to operate industrial plants and factories in safe and stable conditions, it is inevitable to protect the plants' production equipment.

The assets to protect

Followings are examples, but not limited to, of the important assets related with the activities of production.

Examples of data assets

- Production schedules information
- System configuration
- Application configuration
- Tuning parameters for control
- Recipes information
- Audit trails information

Example of instrument assets

- Engineering work stations
- Operator consoles
- Controllers
- Field instruments
- Network devices

Example of human and environmental assets

- Employees
- Factories and plants
- Natural environment

When the security of the assets mentioned above is threatened, it will lead to:

- the confusion and interruption of the production activities
- the leakage of the confidential information such as recipes that may affect the production activities
- the damages to human beings
- the destruction of factories and plants
- the destruction of the environment

Such consequences can bring a lot of harm to the enterprises.

The goal of the security measures is to protect such assets from the threats and to help the enterprises reduce the risks of losing property.

TIP

The standard of “ISA 99.00.01-2007: Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts, and Models” is referenced by this document. Hereinafter, this standard will be referred to as ISA 99.00.01

TIP

In ISA 99.00.01 standard, the Asset-Based criteria have defined what assets to be protected and the Activity-Based criteria have defined the activities. These criteria are referenced by this document.

TIP

Moreover, this document consults “ANSI/ISA-99.02.01-2009: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program,” and standards/draft of “ISA/IEC 62443.” Security related information that is opened to the public on the Internet is referred too.

3. Security Standards and Certifications

In the industrial control system, various standards have been independently established for each industry and region in the past. However, the adoption of open technologies such as UNIX / Windows and Ethernet has led to common problems such as security vulnerabilities.

ISA (International Institute of Measurement and Control), which is mainly based in the United States, has been addressing this problem from an early stage. As a security standard for production control systems (DCS, PLC, SCADA), standardization began as ISA SP 99 in 2002. After that, the ISA 99 was compiled as a security standard that supervises the control system (= IACS) including not only a single control device, but also the surrounding IT equipment and MES (Manufacturing Execution System).

Meanwhile, IEC (International Electrotechnical Commission) was independently aiming to formulate standards related to the security of industrial control systems. However, it has not progressed quite easily, and the whole industry has become an era to strongly demand security standards. Therefore, IEC 62443 was enacted in a form to incorporate the preceding ISA 99 almostly.

Conversely, the ISA side also changed the ISA 99 to ISA 62443 in a form adjusted to the IEC number. Therefore, now it is becoming written as ISA/IEC 62443.

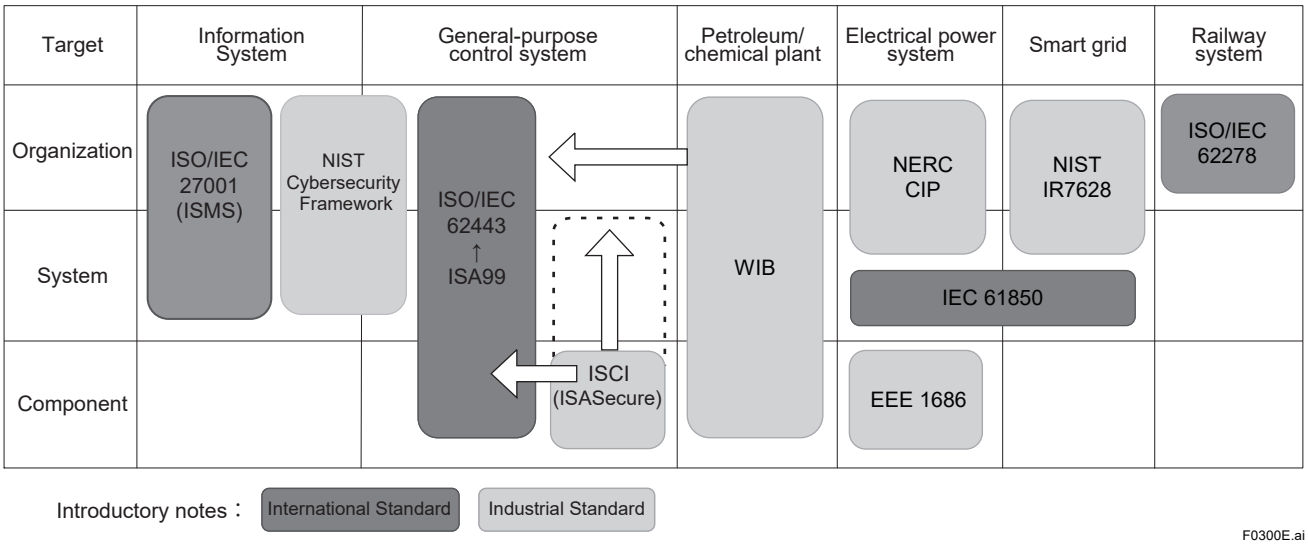


Figure International/Industrial standards for IACS

This chapter introduces the overview of the standards related to the security of industrial control systems. Because the security related information changes quickly, the contents of this document may not be up-to-date. Organizations involved in industrial control systems are constantly required to observe their trends and to respond to the times.

3.1 ISMS

The threats to the information system are increasing day by day and one after another new threats are emerging. Therefore, the security measures need to be reconsidered all the time. This program is called Information Security Management System (ISMS). It is a management framework for an information system based on the risk assessment. In this chapter, the procedures to construct ISMS for operational organizations of the information system is explained.

The following procedures are taken to construct ISMS.

- Organization of the security committee
- Identification of the assets
- Identification and evaluation of the threats
- Identification and evaluation of the vulnerability
- The evaluation of the risks
- Design and implement of the security measures
- Examination and enforcement of system change management
- Continuous monitoring and revision

SEE ALSO ISMS became an international standard as ISO/IEC 27001. For more details, refer to the Web site below:

https://www.iso.org/isoiec-27001-information-security.html

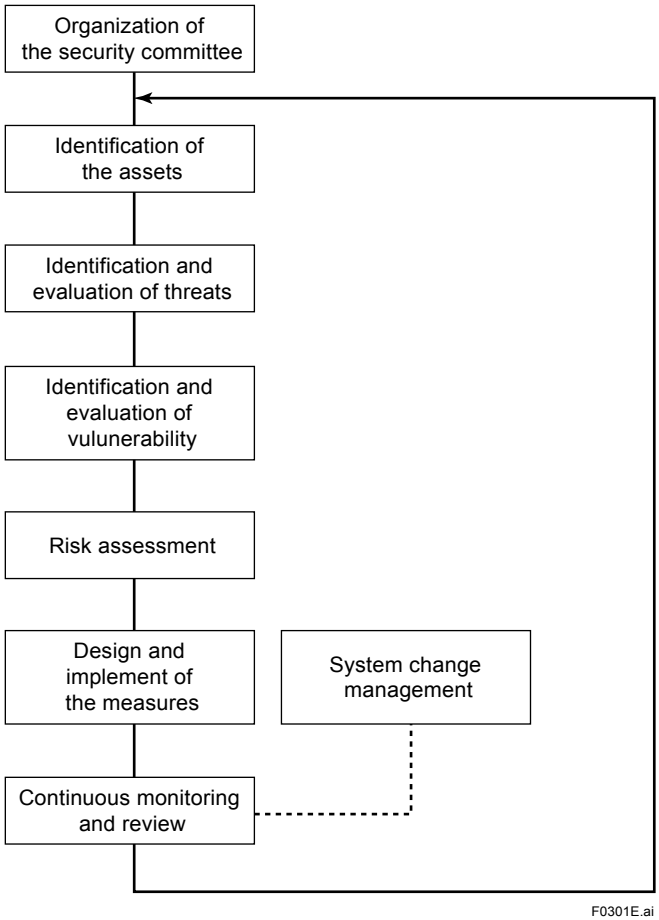


Figure Procedures to construct ISMS

Organization of the Security Committee

The security committee is the leading organization of the activities of ISMS. Please take notice of the following when it is organized.

Commitment of management

The objective of the security committee is to protect the assets of enterprises. That means that the management is responsible for this. In addition, it is necessary to get the collaboration of everybody involved in the production activities in order to enforce efficiently the security measures. Therefore, the management should express their opinions about the security activities clearly.

The management should commit itself to the security committee and take the initiative.

The cross-functional organization

The security committee consists of the representatives of all the divisions involved in the production activities. For example, we can assume an organization with the following divisions.

- Production division
- Production control system management division
- IT system management division
- Business management division
- Maintenance division

Identification and Evaluation of the Assets

The purpose of this phase is to list all the assets to be protected, identify the asset owners and evaluate the value of each asset. The assets with larger value have the higher criticality. In chapter 2, an example of assets to be protected is described.

Followings are the examples how the criticality of the assets are classified.

- Criticality A : Very High
- Criticality B : High
- Criticality C : Low
- Criticality D : Very Low

Identification and Evaluation of the Threats

Here, we need to make clear the potential threats to the assets listed above.

In identifying the list of threats, it is necessary to think from the following points of view.

Illegal access to the assets by the people with malicious intent, the people are:

- Those inside the enterprise
- Those outside the enterprise
- Those hacking around by way of networks
- Those having chance to physically access the assets (Who can perform direct operation and enter the area where the assets are placed.)

- **Illegal access to the assets by the software with malicious intent**
  - By way of networks
  - By way of removable media

- **Incidental illegal access to the assets caused by mistaken or careless operations**

  The level of possible occurrence of the identified threats will be evaluated.

  The example of the classification of this will go as follows.
  - Level A: The possibility of its occurrence is high.
  - Level B: The possibility of its occurrence is moderate.
  - Level C: The possibility of its occurrence is low.

Identification and Evaluation of Vulnerability

The purpose of this phase is to identify the vulnerability of each asset, also to identify the vulnerability of each equipment of the asset. The term “vulnerability” means the situation or condition that threats can affect the assets.

The followings are examples of the vulnerability.

- Incompleteness of the security measures or their implementations
- Incompleteness of the enforcement procedure or the procedure documentation
- Incompleteness of the security committee organization
- The lack of physical protection
- Incompleteness of Firewall settings placed on the border of the network to be protected against the external networks
- Inadequate virus definition files or engine of antivirus software (Non-updated Virus definition file or engine)
- Incompleteness of the Security Updates (Non-updated Security Updates)
- Incompleteness of backups (The system is not backed up.)
- The lack of understanding to PCS (process control system) and it’s operational environment
- The lack of the awareness of security among the people such as operators

Risk Assessment

In this phase, the risk of each asset or each instrument housing the assets is evaluated.

The risk is shown as below:

Risk = Threat x Vulnerability x Consequences

By doing risk-assessment, you can clarify the priority of the security measures. In risk assessment, the consequences are estimated such as loss of business by the stop of system function, and the expense for restoring from the damage of the production control system. By the degree of these quantitative consequences, the priority of each measure needs to be determined. Then, you can clarify which part should need concrete measures, considering which measures have to be taken over which risk, or which risk is tolerable.

However, consequences may include the damages to environment and human being, and the damages to public confidence to the enterprise. Therefore sometimes it is difficult to estimate the consequences as uniform operation loss of money.

Design and Implement of the Measures

In planning the security measures for production control system, it is necessary to make the security policy that regulates the rule of the security management. The actual security measures should be designed or selected along this rule.

Security policy

The security policy is made to regulate how the security of production control system can be managed. The followings are the examples of security controls that should be included in the security policy.

- User ID management
- Password management
- Connection to business network
- Remote access
- Computer virus
- Media management
- Physical protection
- Education, training

Notes about the measures

There are many cases where the technique or customs developed in IT systems are applied to the security measures for the production control systems. However, production control systems have different characteristics from those of IT systems, so it is necessary to take them into consideration in making the measures. We will show the differences between IT systems and production control systems as follows.

Availability

High level availability is required for production control systems. In IT systems, some operations are made on the assumption of reboot, but in case of production control systems, uninterrupted operation is most common.

Real-time ability

Real-time ability is important for production control system. For instance, it is necessary to respond quickly to the operations from HMI and so on. It is also required to make a stable throughput as well as a real time response to the data-collections and setting requirements from the upper level systems.

Consideration of Security Updates and anti-malware software

Since the high level availability and real-time ability are required for production control system, it is necessary to check the Security Updates and anti-malware software updated beforehand and consider the application, the means and timing of update for them to a large extent.

- **Priority of Availability, Integrity and Confidentiality**

When considering the security objects in the Production Control System, the availability of system, network, endpoint equipments such as controller and PC should have the first priority. Another important security object is integrity of data used by Production Control System. If there is loss of integrity, the reliability of production control is reduced. Finally it is possible to cause a safety problem. Also, production management may not function correctly by the loss of correct data, and the excessive cost concerning the opportunity loss and restoration may occur. Moreover, availability of system and network may be affected by loss of the data integrity. Therefore, it is very difficult to determine the priority between availability and integrity.

On the other hand, when considering the confidentiality of data and information of Production Control System, the confidentiality generally has lower priority than other two security objects. However, consideration on confidentiality may be important. User ID and the password of the production control system can flow on the network; and if they are sniffed, an attacker can attack the system as an authorized user.

System Change Management

It is a very important element to decide the procedures of System change management in order to keep the system secure. Whatever addition or change may be made, it has to be done in such a way as to maintain the availability, real-time ability and the degree of security. For this purpose, when some additions or changes are made, it is necessary to decide the procedure of System change management, such as going back to the first step and repeating the whole procedure from the identification of the assets to risk assessment, and to carry it out.

Apart from the addition, deletion and replacement of hardware and software, the followings are regarded as system changes, but not limited to.

Changes in settings of network devices

Changes in the settings of network devices such as in switches, routers or firewalls.

Security Updates

Before the applying the Security Updates, it is necessary to make sufficient tests.

Operation

After the construction of ISMS and the application of the security measures to the system, the system begins to operate. In this section, we will explain the activities to carry out in the phase of operation.

Organization of the team for the incident

In the operation phase, it is necessary to organize the team that will play the major role in handling the incidents.

This team takes the responsibility for the followings.

- Evaluation of the consequences caused by the security incident and the influence upon the production activities. These consequences include the damages upon health, safety, environment and public confidence.
- Inquiry into the cause and the planning and enforcement of the measures to prevent such an incident from happening again.
- Restoration of production control system from the incident.
- Gathering information on the latest threats and incidents

The procedures to take care of the incidents must be planned as a business continuity plan. This topic is explained in the chapter 6.

Daily monitoring of the system

Daily monitoring is done so as to detect the illegal access to the system in operation. The log information on the following instruments will be monitored, but not limited to.

- Monitoring log of the PC component
- Access control log of firewall
- Monitoring log of network monitoring device
- Detecting event of IPS (*1) if IPS is installed.

*1: Intrusion Prevention/Protection System:
This is a system to detect hackers to our network and/or server and to protect our system by blocking unauthorized connection, notifying a system manager and outputting logs in real time.

We will describe the monitoring of the systems in detail in Chapter 4.6.

Regular auditing

The system in operation is regularly audited to check if the settings are appropriately defined and managed. The information on the settings of the following instruments will be audited, but not limited to.

- Network devices: Information on routing control devices such as routers or switches.
- Security devices: Access control rules of firewall, detecting rules of IPS.
- System hardening of PC components: Setting information of personal firewall of PC components and the like.
- Software in use: Installations of application software to PCs are controlled, and all software is configured appropriately.

3.2 CSMS

CSMS Overview

Regarding the management and operation of information systems, application of information security management (ISMS) by ISO/IEC 27001 is common. However, regarding IACS, a mechanism of security management that takes into consideration its characteristics and properties is required. Therefore, security management for IACS based on ISMS was formulated and standardized as ISO/IEC 62443-2-1.

In Japan, as the CSMS (Cyber Security Management System for IACS), the world first certification system was built.

In ISMS, the outflow of information to be protected is a problem, and Confidentiality, Integrity, Availability are often emphasized in the order of “CIA”. But CSMS cited interruptions in operation as the most avoidable situation, focusing on the order of “AIC” and characterized by considering HSE (Health, Safety & Environment).

SEE ALSO For CSMS, please refer to the following web page.

https://isms.jp/csms/doc/JIP-CSMS120E-10.pdf

CSMS Program

CSMS is introduced and operated in the following procedure.

- Initiate CSMS program
- High-level risk assessment
- Detailed risk assessment
- Establish security policy, organization and awareness
- Select and implement countermeasures
- Maintain the CSMS

Target Organization of CSMS

CSMS certification means that the target organization establishes a security management system for the construction and operation of IACS and objectively evaluates the suitability and effectiveness by a third party.

The following companies are subject to CSMS.

- Organization that own control systems (asset owners)
- Organization that handle the operation and maintenance of control systems
- Organization that develop control systems (system integrators)

3.3 NIST

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) published “Framework for Improving Critical Infrastructure Cybersecurity” in February 2014. It is mainly written for enterprises engaged in important infrastructure, but it can be fully utilized by other organizations. It is also called “CSF” and its use is expanding abroad.

This framework classifies cyber security measures into five functions, “Identify”, “Protect”, “Detect”, “Respond”, “Recover”, and shows these functions in 23 categories.

Table NIST Cybersecurity Framework

Functions		Categories		Subcategories	Informative References
ID (Blue)	Identify	ID.AM	Asset Management	.	.
		ID.BE	Business Environment	.	.
		ID.GV	Governance	.	.
		ID.RA	Risk Assessment	.	.
		ID.RM	Risk Management Strategy	.	.
		ID.SC	Supply Chain Risk Management	.	.
PR (Purple)	Protect	PR.AC	Identity Management and Access Control	.	.
		PR.AT	Awareness and Training	.	.
		PR.DS	Data Security	.	.
		PR.IP	Information Protection Processes and Procedures	.	.
		PR.MA	Maintenance	.	.
		PR.PT	Protective Technology	.	.
DE (Yellow)	Detect	DE.AE	Anomalies and Events	.	.
		DE.CM	Security Continuous Monitoring	.	.
		DE.DP	Detection Processes	.	.
RS (Red)	Respond	RS.RP	Response Planning	.	.
		RS.CO	Communications	.	.
		RS.AN	Analysis	.	.
		RS.MI	Mitigation	.	.
		RS.IM	Improvements	.	.
RC (Green)	Recover	RC.RP	Recovery Planning	.	.
		RC.IM	Improvements	.	.
		RC.CO	Communications	.	.

Each category is further divided into several sub categories, and 108 sub categories in total. Measures are not very detailed and it have not mentioned any technical means.

In the informative references, links to other standards etc. related to each sub category are shown.

SEE ALSO For more information about NIST Cybersecurity Framework, please refer to the following Web page.

https://www.nist.gov/cyberframework

3.4 ISASecure

ISASecure is a security certification system developed by ISCI (ISA Security Compliance Institute), a lower-level organization of the United States-based industry association ISA (International Society of Automation). ISASecure is integrated into IEC 624434.

ISCI prepares certification programs for each subject to be certified. EDSA (Embedded Device Security Assurance) certification for control devices, SSA (System Security Assurance) certification for control systems, and SDLA (Security Development Lifecycle Assurance) certification for development process.

SEE ALSO For information about ISASecure's authentication, please refer to the following Web page.

http://www.isasecure.org/en-US/Certification

Embedded Device Security Assurance (EDSA) Certification

EDSA focuses on the security of embedded devices of control systems. There are three levels of certification level, and the level becomes higher in order of level 1 → 2 → 3.

EDSA has the following three tests.

- Functional Security Assessment (FSA)
- Software Development Security Assessment (SDSA)
- Communication Robustness Testing (CRT)

Yokogawa CENTUM VP and ProSafe-RS controllers have obtained EDSA certification.

http://www.yokogawa.com/pr/news/2014/pr-news-2014-20-en.htm

http://www.yokogawa.com/pr/news/2014/pr-news-2014-02-en.htm

https://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Components

System Security Assurance (SSA) Certification

SSA is an authentication program for a specific subset of the control system developed by ISCI.

- Security Development Artifacts for systems (SDA-S)
- Functional Security Assessment for systems (FSA-S)
- Functional Security Assessment for embedded devices (FSA-E)
- System robustness testing (SRT)

Security Development Lifecycle Assurance (SDLA) Certification

SDLA is a program to evaluate the secure product development life cycle for suppliers of industrial control systems. Depending on the level of development life cycle, it is certified with four levels (ISASecure SLDA levels 1 to 4).

3.5 ISA99

ISA99 Overview

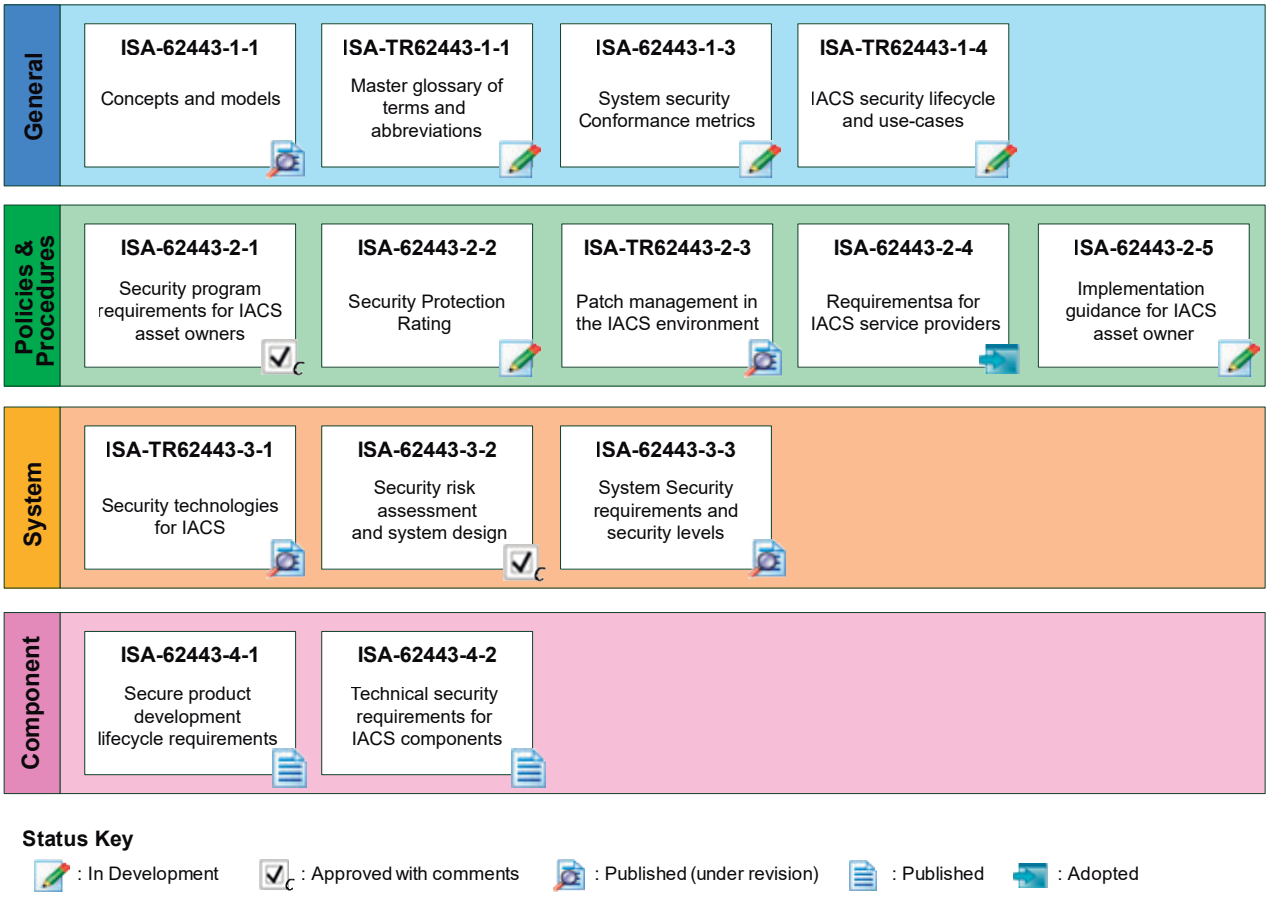
ISA99 is a security standard for Industrial Automation and Control Systems (IACS) formulated by ISA described in section 3.4. Recognizing that comprehensive security measures are necessary for IACS has been in the 1990s. However, depending on the end user and system / equipment provider, and the country and regional differences, the essential requirements were different.

Therefore, it was difficult to formulate internationally unified standards. Meanwhile, the US led the way to establish security standards as ISA. That is ISA99.

The ISA99 was eventually to be incorporated into IEC (International Electrotechnical Commission) 62443 as an international standard. Then, the ISA side changed the number from ISA-99 to ISA-62443 in accordance with the number of the IEC.

ISA-62443

As mentioned above, now ISA99 changed ANSI/ISA-62443 has been developed together with IEC 62443. ISA-62443 is not yet complete as it is trying to encompass various security measures. The figure below shows the outline of ISA-62443 as of 2019.



F030501E.ai

Figure ISA-62443 Overview

SEE ALSO For more information about ISA 99 (ISA/IEC 62443), refer to the following Web page.

https://www.isa.org/isa99/

3.6 IEC 62443

IEC 62443 Overview

As mentioned in Section 3.5, IEC 62443 is a standard created based on ISA99. Although the contents are almost the same, the requirement of WIB which was not found in ISA99 was imported as IEC 62443-2-4. In addition, it is being rewritten from the following point of view as being an international standard.

- Terms and language usage are being revised to make it easier for people who are not English native speakers.
- Consideration is given to operations in organizations with different situations in various countries and regions, and expressions are widely generalized.

Table IEC 62443 Overview

Category	IEC No.	Edition	Type	Title	Publication date
General	62443-1-1	1.0	Technical Specification	Terminology, concepts and models	2009-07-30
Policies and Procedures	62443-2-1	1.0	International Standard	Establishing an industrial automation and control system security program	2010-11-10
		2.0	(in preparation)	Security program requirements for IACS asset owners	–
	62443-2-2	1.0	(in preparation)	IACS protection levels	–
	62443-2-3	1.0	Technical Report	Patch management in the IACS environment	2015-06-30
	62443-2-4	1.1	International Standard	Security program requirements for IACS service providers	2017-08-24
System	62443-3-1	1.0	Technical Report	Security technologies for industrial automation and control systems	2009-07-30
	62443-3-2	1.0	(in preparation)	Security risk assessment and system design	–
	62443-3-3	1.0	International Standard	System security requirements and security levels	2013-08-07
Component	62443-4-1	1.0	International Standard	Secure product development lifecycle requirements	2018-01-15
	62443-4-2	1.0	International Standard	Technical security requirements for IACS components	2019-02-27

As of 2019, IEC 62443 has not been completed yet. Items in various states, such as those under formulation, those under voting, or those under revision.

For this reason, it is important for organizations involved in IACS to constantly observe their trends and take actions in line with the times.

Related Standards and Certifications

WIB Certification

WIB is an international organization of end users in the process industry, mainly in the Netherlands and Belgium. This WIB summarizes the security requirements for the supplier of the control system and it is subject to certification as "Achilles Practices Certified Solutions" by WurldTech Inc. of Canada (now under of GE digital). This is what we call WIB certification.

Yokogawa's CENTUM VP and ProSafe-RS have obtained this WIB certification.

https://www.ge.com/digital/applications/achilles-practices-certified-solutions

WIB certification is incorporated into IEC 62443-2-4.

Achilles Certification

In the world of IACS, "Achilles certification" usually means "Achilles Communications Certified Products". This is the CRT for ISASecure EDSA authentication described in Section 3.4.

Yokogawa's CENTUM VP and ProSafe-RS and STARDOM controllers have acquired this Achilles certification.

https://www.ge.com/digital/applications/achilles-communications-certified-products

4. Security Control

This chapter explains how the security controls protect the production related assets from the threats. The security countermeasures for production control system should be examined, designed, operated and evaluated while the process safety and physical defense are simultaneously taken into consideration.

4.1 Basic Strategy

It is necessary to consider the basic strategy we will describe in this chapter when carrying out the actual security control.

Risk Definition

Risk is defined by a formula as follows.

Risk = Threat x Vulnerability x Consequences

Threat is a potential attack over the system vulnerability. And risk means the potential damage or loss that is caused by the attacks over the vulnerability. Therefore, the measures to reduce risks can be categorized as follows.

- Removal of vulnerability
- Restriction of use
- Control of attack
- Mitigation of consequences

Each security control explained in this chapter corresponds to these measures.

Security Zone

ISA99.00.01 defines security zone as a logical or physical group which share common security requirements and the same security level. By making the multiple zones where each zone satisfies different security requirements, defense-in-depth strategy can be realized. The security controls are explained in this chapter, and these security controls should be designed based on the concept of zone.

Defense-in-depth strategy

Threats to information system are under daily evolution. What is more, the threats can happen not only in the external networks like business networks, but also on PCN (Process Control Network), which is an internal network. We have to get armed with the defense-in-depth strategy.

As shown in the figure, by defense-in-depth strategy, we mean the protection measures composed of more than one security control to protect the assets. By the use of this kind of multi-layer measures, another layer will protect the assets even if one layer is destroyed, so the assets are protected more firmly.

Network boundary security

It is a contact point between control network and an external network such as a business network, and it prevents the external threats from entering control networks.

vInternal network security

It tries to decrease the consequences of the threats occurring on the control network as much as possible. For instance, it divides the control network into multiple zones, and constructs the network in order not to allow the damages in one zone to affect other zones.

End point security

It is a measure for excluding the vulnerability of end point and increasing the strength of the security. For example, it applies Security Updates to PC, and excludes the security hole.

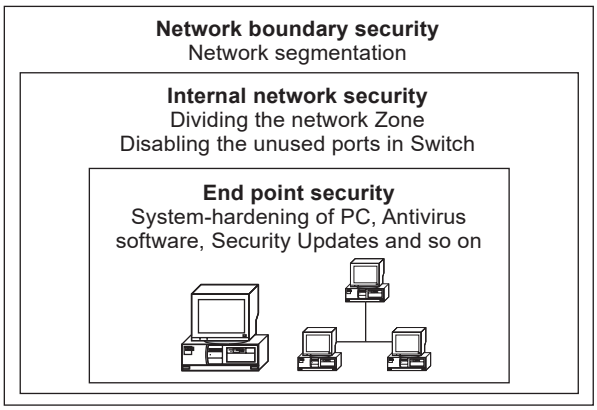


Figure Defense-in-depth strategy

Deny-all strategy

Deny-all strategy is a strategy that allows only the minimum accesses and prohibits the others. Security control with deny-all strategy makes it possible to protect the assets firmly, for it does not permit more accesses to the assets than necessary and it limits the space for illegal accesses to the least. It is necessary to take it into consideration, especially when enforcing the access control rule of firewall or system hardening of PC components.

4.2 Network Architecture

A secure network configuration is explained for connecting a Production Control System (PCS) with an external network such as a business network.

4.2.1 Network Segmentation

Segmentation of networks is the basis of security control. There are two types of segmentation, vertical and horizontal.

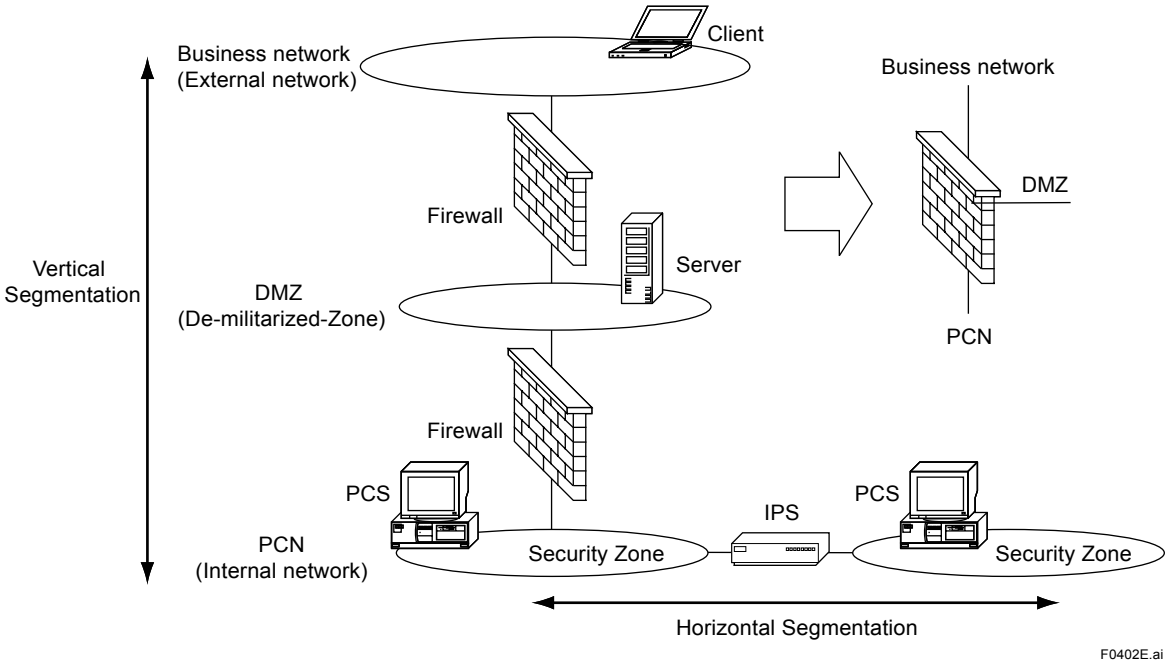


Figure Network segmentation

TIP

In terms of logic, the configuration of DMZ is supposed to be a network protected by two firewalls, as shown in the figure. However, it is usually only a single firewall with three or more network ports.

Vertical segmentation

In the vertical segmentation, the network is divided into the following three segments. Among the segments, the passage of network traffic is controlled and the threats from external networks are excluded. The access from business network is possible only to the servers on DMZ, and it is not possible to access PCN directly. In addition, it can conceal the PCS addresses from client on business network. That is, the vertical segmentation is for protecting the PCN from external networks such as business networks.

Business network

This is an external network on which the clients that may access the data of production control system are connected. This segment belongs to Level 4 of ISA 99.00.01 Reference Model.

DMZ (De-Militarized Zone)

The servers that directly communicate with the clients are placed in this zone. The servers placed here communicate with both PCS and the clients. DMZ is a buffering area placed between PCN and business network. The servers on DMZ need to be firmly fortified with the antivirus software and Security Updates, for the servers may be directly accessed from the external networks. This segment is located between Level 4 and Level 3 of ISA 99.00.01 Reference Model.

PCN (Process Control Network)

PCN is an external network that the production control system is connected. The devices placed here can not be accessed directly from business networks. The data of PCS are passed to the business networks through the servers on DMZ, so it is not necessary to access PCN directly from the business networks. This segment belongs to Level 3 of ISA 99.00.01 Reference Model.

Horizontal segmentation

The internal network is divided into multiple security zones. For example, IPS (Intrusion Prevention/Protection System) is connected in between the 2 security zones, and filters out the illegal traffics that run between the security zones. By dividing PCN into security zones, it is possible to prevent other security zones from the threats of worms that occurred in one security zone.

SEE ALSO For notices about constructing IPS, refer to “4.6.2 IDS/ IPS”.

4.2.2 Classification of Devices Composing the System

The devices are placed in different segments according to the following classification.

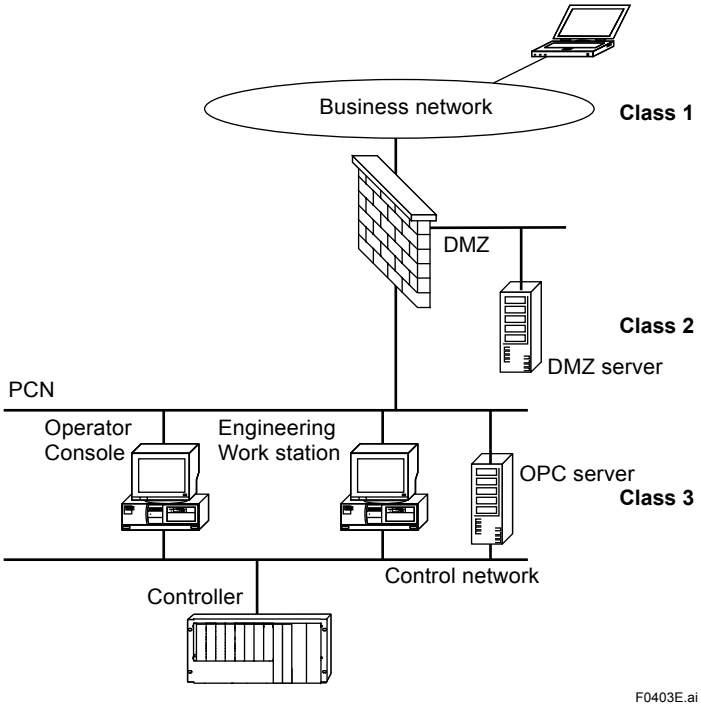


Figure Equipment class

- **Class 1: Computers connected on business network (external network)**

  The computers in this class are connected on a business network and access the data on the PCS via a server in the DMZ. This computer is usually managed by the information system department in an enterprise.

- **Class 2: DMZ server**

  The servers in this class are used for publishing the data of PCS to the computers of Class 1. It communicates with both the clients on the business network and the PCS connected on PCN. That is, the server obtains the data by accessing PCS and publishes the data to the devices of Class 1. The servers used for publishing the virus definition files or Security Updates are also classified in this class.

- **Class 3: PCS (Production Control System)**

  The devices of this class do not communicate directly with computers on the business network. The PCS devices belong to this class. They are not directly accessed from the business network.

Classification is based on the consequences of a security incident. The devices that are closer to the process have the higher priority, because the consequences are more serious. In this classification, Class 3 has the highest priority.

4.2.3 Access Control by Firewall

A firewall can restrict the communications of the three network segments to a minimum level. Moreover, applying a deny-all strategy can block all communication traffics except those permitted. (*1)

*1: It is called “Cleanup” and is specified at the end of Access Control Rule.

■ Port (service), IP address control

With a firewall, external accesses to the servers on the open segments, and the accesses to the control devices on the internal segments (control system segment) from the servers on the open segments are restricted to a minimum level so that only the permitted accesses are allowed.

More over, a firewall generally hides itself from the outside so that the accesses to firewall are prohibited. (*1) Therefore, the access control rule should be configured comprehensively by permitting only the necessary accesses from/to the specific sources/destinations and the accesses through the designated communication ports (or identified by the specific service names).

*1: It is called “Stealth”, for it conceals the firewall. As an exception, only the communications from the administrator console that manages the firewall need to be permitted.

■ DoS (*1) defense

The features of firewalls vary with firewall types. Some types of firewalls are able to defend against the DoS attacks by temporarily restricting the number of TCP connections. Applying this feature would protect the DMZ servers from the DoS attacks that would make them overloaded.

*1: Denial of Service attack: It is a kind of attacks by sending a large amount (meaningless) of service connection requirements to servers such as Web servers, FTP servers, Mail servers and so on, to make the servers overloaded and block the services to the legal users.
It is expanded to Distributed Denial of Service (DDoS) that attacks all at once from multiple places by using third party computers as a stepping-stone.

■ IP Spoofing (*1) defense

Restricting the network addresses from all the segments can defend against IP spoofing attacks. It can also repel the illegal packet sent from an outsider but disguised as if it were from an internal network address.

Therefore, the addresses permitted for each segment should be defined to the firewall so that only the packets with the permitted addresses can enter the segment.

*1: IP Spoofing: It means creating and sending packets with false IP addresses of the senders in order to conceal the origin of attackers. When the server receives a packet from the outsider but the packet is disguised with an internal network address, the server may assume the packet is from an address of an internal sender and relay the packet in the internal network. Because the sender is not insider, the server may fail when tries to respond. Many DoS attacks are taking advantage of this mechanism.

4.2.4 Dual-Home Server

It is not recommended that the dual-home servers (*1) for both Ethernet and Control bus be placed in DMZ. As an alternative, the dual-home server can be placed on PCN and place a reverse proxy server (*2) in DMZ.

The reverse proxy server will take the requirements from the business networks and then, pass them to the dual-home server on PCN.

*1: Dual-Home Server: a server with two or more network interfaces.
*2: Reverse Proxy Server: a proxy server to relay demands for a particular server. Every access to this particular server goes through this proxy server.
Regular proxy relays access from internal network to external network. Reverse proxy, on the other hand, relays access from external network to internal network.

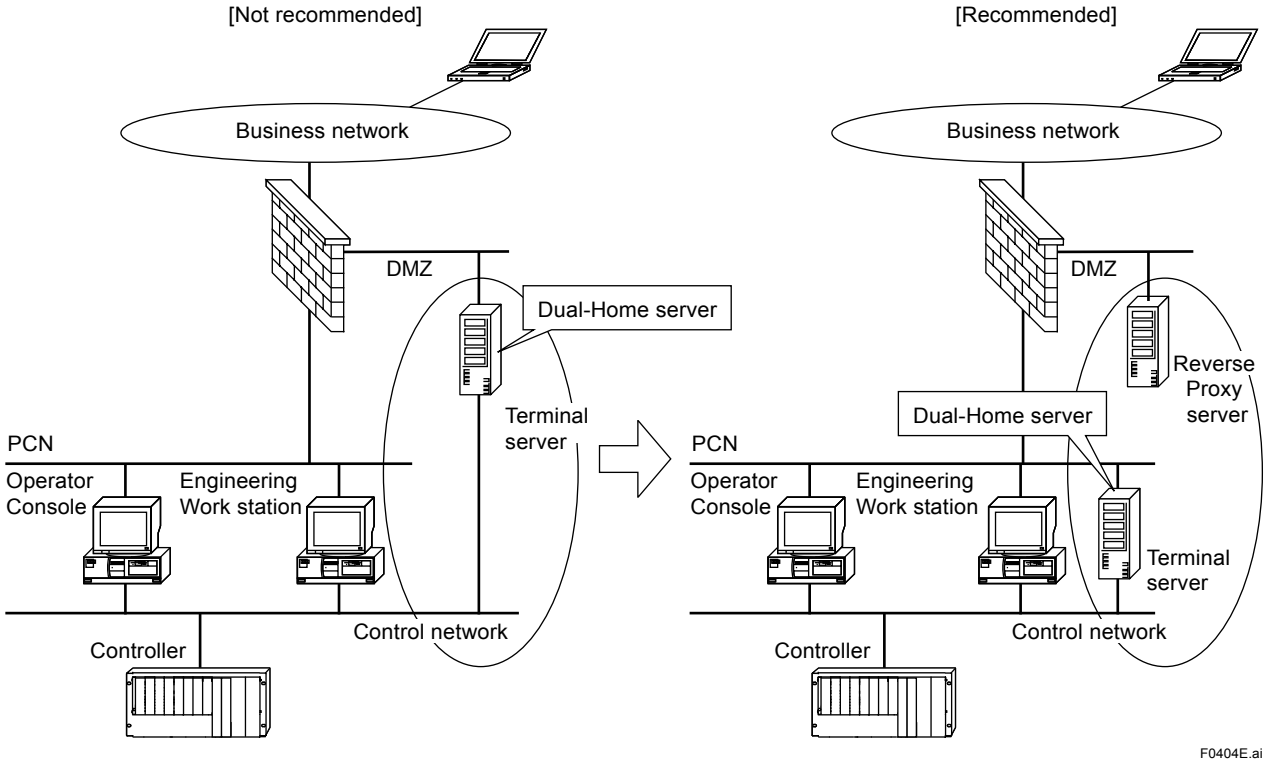


Figure Dual-Home Server

In the recommended example in the right-hand side, the terminal server is placed as a dual-home server. The applications, such as the operator console applications, are running in the terminal server. Via reverse proxy server in DMZ, it is possible for the users in the PC placed on business network to display and operate the applications running in the terminal server.

4.2.5 OPC Interface

This configuration shows that a user on a PC located on the business network can display and operate the OPC client applications by using a terminal server. The terminal server is used because the reverse proxy server can not be directly used to route to the OPC server. The terminal server is placed in PCN, and OPC client is running in the terminal server PC. OPC server is placed as a dual-home server, and it is connected to both of PCN and control network.

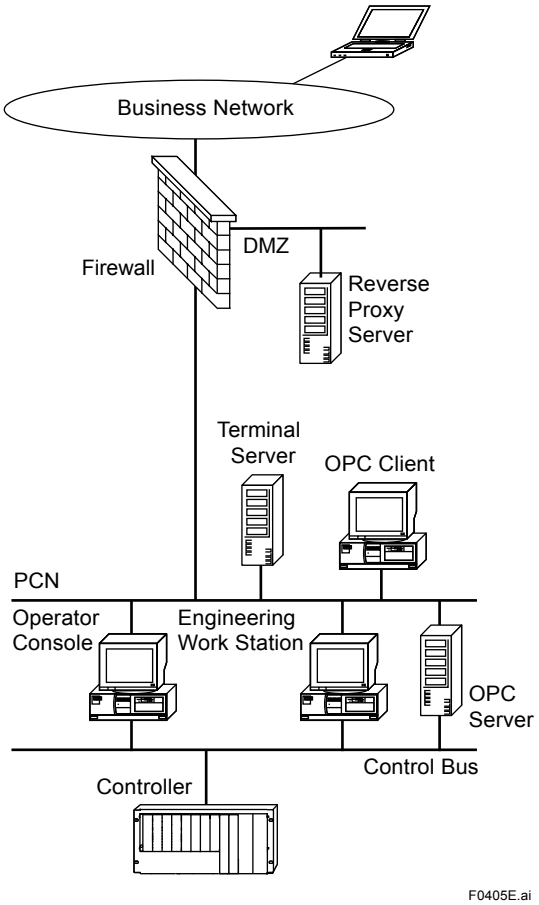


Figure Example of OPC interface configuration

By this configuration, it is possible to display and operate the OPC client applications via a Reverse Proxy Server in DMZ from the PC of business network, while the OPC client applications are running in the terminal sever of PCN.

4.2.6 Application of Wireless Networks

In this section, we will explain the security of wireless network.

■ Wireless LAN (IEEE 802.11)

These days, the use of wireless LAN of IEEE 802.11 series has been increasing rapidly. It became widely known to the public as “Wi-Fi” and now used in private and business environments.

In control systems, the cases have been increasing where the fieldsmen using the mobile terminals to access PCN through the wireless access points located in the company premises. The characteristics of wireless LANs increase the security risk that an outsider may use an over-the-counter wireless card for illegal access from the locations wherever the wireless transmission reaches. Moreover, outsiders may sniff the communication, tamper with the data,or hack the system by using tools such as the War driving (*1) tool.

Therefore, when wireless LANs are connected with PCN, it is necessary to take care of the following points.

*1: War driving: It is a means of cracking technique to seek for the access points of wireless LAN, moving by car in the streets lined with office buildings.

● Connection of access points

Do not connect access points with PCN directly, but connect it with DMZ, and control accesses to PCN with firewall.

● Authentication of terminals

It is necessary to register MAC addresses of terminals which are allowed to be connected so that to prevent the illegal terminals from getting connected. If an unauthenticated terminal is connected, the network will be threatened by the illegal usage. Moreover, it is nearly impossible to detect illegal wireless access such as wireless sniffing.

● The setting of ESSID (*1)

Set the ESSID of access points and prohibit “Any connections”.

*1: ESSID: The network identifier of wireless LAN of Extended Service Set Identifier IEEE 802.11 series. It can prevent any terminals other than those with the same identifier as ESSID from accessing the access points. When “Any access” is permitted, the terminals with any ID can be connected.

● Encryption

It is necessary to encrypt communication data by using WPA (*1).

*1: WPA is an encryption standard developed by the Wi-Fi Alliance to protect wireless LANs. It overcomes the weaknesses of the WEP encryption that was used and strengthens network security.
Moreover, WPA2 which is improved from WPA adopts Advanced Encryption Standard (AES), so weak points of WEP and WPA are all relieved. However, vulnerabilities of WPA2 were publicly disclosed on October, 2017. Thus, updating for the revised program is required when using WPA2.
Incidentally, WPA3 that solved the vulnerabilities of WPA2 fundamentally will be released to the public in the latter half of 2018.

The system-hardening of access points

It is highly recommended to harden the access points with the following preventions so that they can be concealed from the scanning of access points such as War-driving.

- Disable the broadcast of ESSID (Beacon signal).
- Disable the response to a probe request.

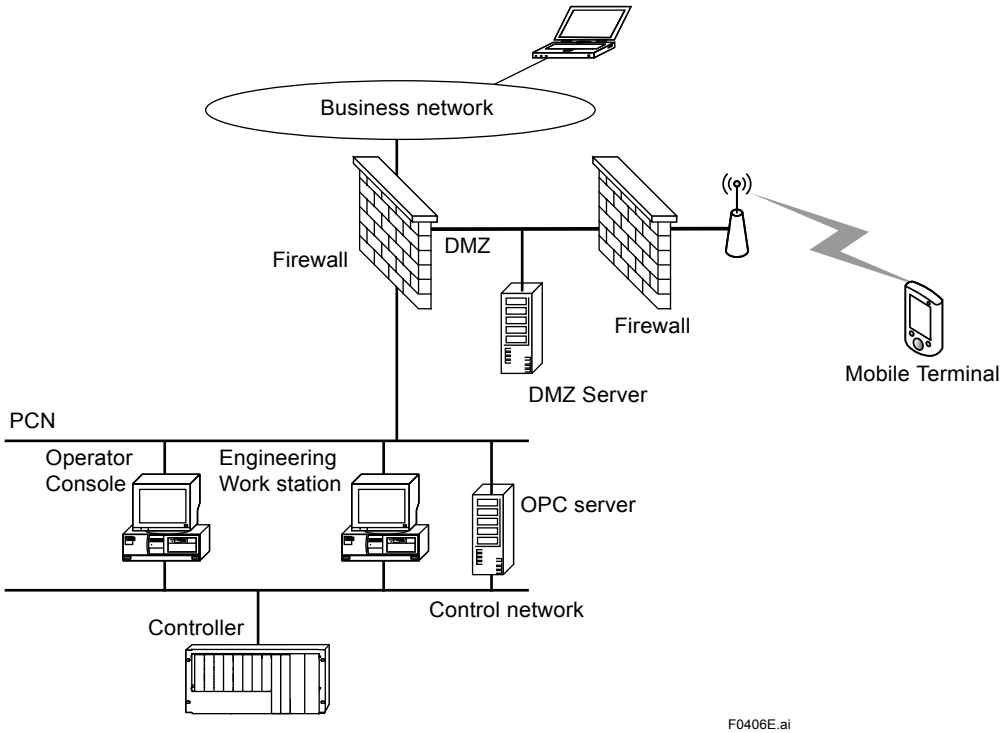


Figure Example of Wireless Network Configuration

Wireless application to control bus

When you extend the control channel of Vnet/IP or HSE (High Speed Ethernet) of STARDOM with a wireless network, you need to pay attention to the following points.

- The available band width will be restricted. (11Mbps - 54Mbps)
- The state of electric wave easily gets deteriorated because of the obstruction of electric wave and rainfall
- When the state of electric wave gets deteriorated, the performance in the band width will be lower.

In addition, control the accesses with a L3 switch and apply access points so that only the communications between the two domains connected with each other can be relayed.

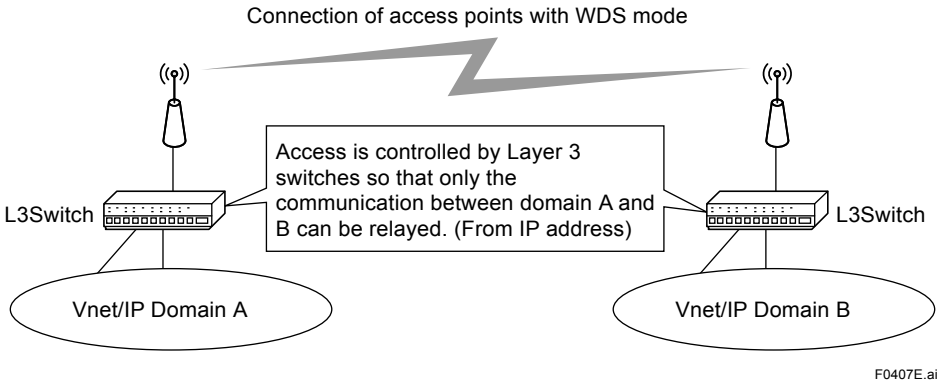


Figure Example of the configuration of the extension of Vnet/IP control channel

Field wireless (ISA 100.11a)

Field wireless networks compliant with ISA 100.11a are highly relaible in ensuring the safety of production sites and the security of information. They take care of concerns such as message confidentiality (encryption, authentication, access control), message integrity, and network availability.

You can obtain a higher level of security by implementing the following measures when building a system that handles field wireless devices.

Basic measures

- Completely separate the network for control system usage from that for field wireless usage.
- Control access by installing a switch between ISA100 gateway (*1) and computers.
- Set up firewalls for both the system and ISA100 gateway and build a VPN between them to connect to the Wide-area Universal Field Network (*2).

*1: A device that connects to the field wireless and the wired Ethernet. The Yokogawa product “YFGW710 Field Wireless Integrated Gateway” is an example of such a device.
*2: A system that uses monitoring devices such as CENTUM to monitor the process data of wireless devices by passing through the ISA100 gateway in a wide area network. It may pass through open IT networks on the way, reducing reliability and real-time performance.

Additional measures for higher security

- Separate the network for control system usage from that for field wireless usage even if they are at the same security level, and set up a firewall between the networks. (horizontal integration)
- Set up a firewall between all layers. (vertical integration)
- Install the PRM Field Communication Server on two different computers. One is for CENTUM while the other is for field wireless.
- The Field Wireless Configurator and Field Wireless Management Tool are also installed on different computers.

The following figure shows an example of a field wireless system configuration that takes security into account.

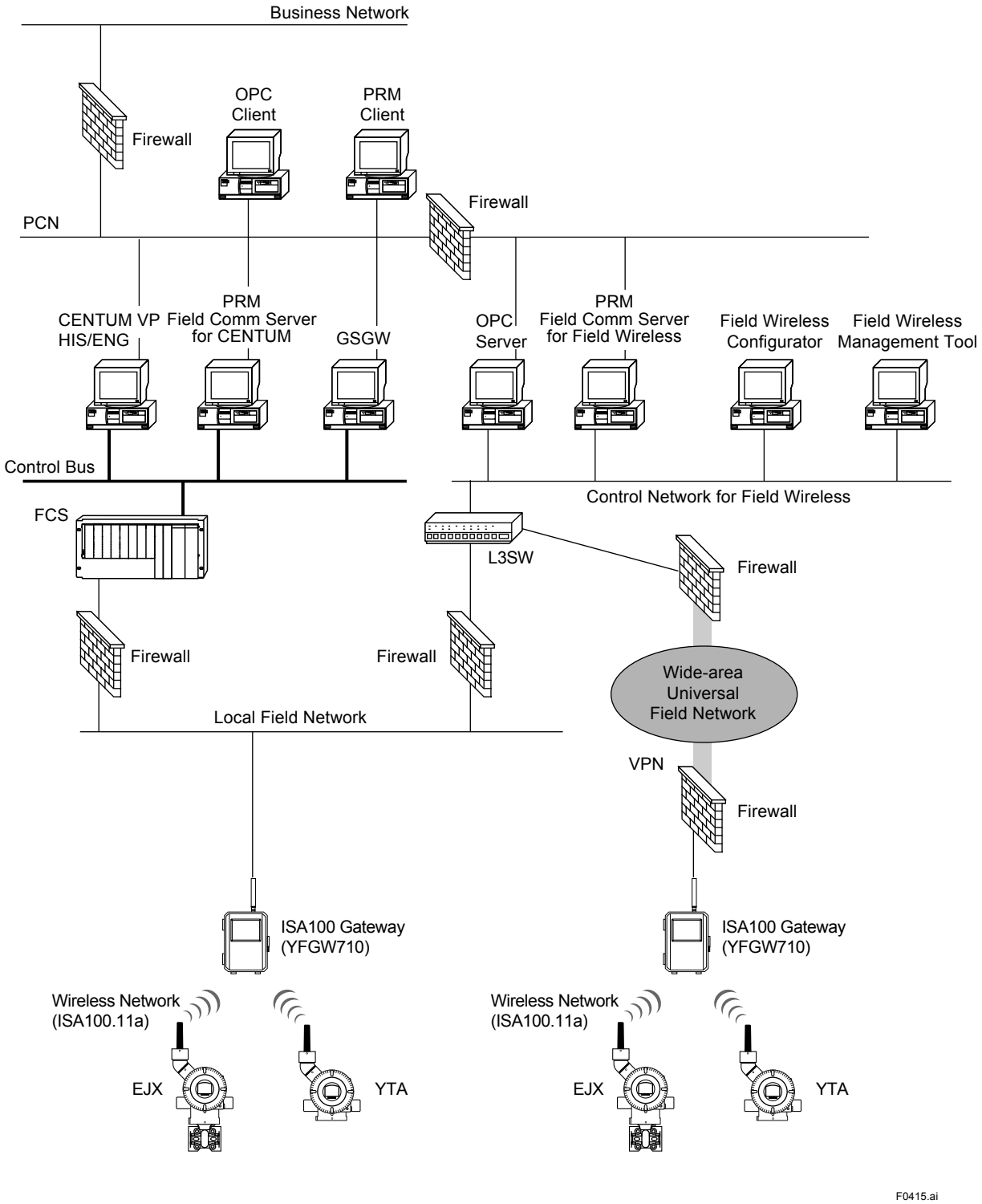


Figure An example of a field wireless system configuration with consideration for security

4.2.7 Remote Monitoring

We will explain the configuration of remote control networks for the physically remote- located clients through the terminal server.

Wide area network

The communication route for remote monitoring between the remote clients and the local firewall, the wide area network provided by the public communication services will be used.

The wide area network could be:

- Digital dedicated line
- Dial-up connection by ISDN (*1)
- Closed network (IP-VPN (*2), Wide-area Ethernet (*3) and the like)
- Internet

Although a dedicated digital line is a recommended option from the viewpoint of security and the quality of network transmission, it is not economical.

Internet is economical, since the inexpensive high speed Internet connections are available, but it has such disadvantages as unstable network quality and insufficient network security.

*1: ISDN: Integrated Services Digital Network
It is one of the telephone networks, such as analogue line network, mobile-phone network and PHS network. In using it in dial-up as a data communication line, it can be used as 64kbps or 128kbps line.

*2: IP-VPN
It signifies the Virtual Private Network constructed by way of Wide area IP communication network owned by public communication services. The use of IP-VPN makes it possible to operate remotely separated networks as if they were directly connected by LAN. The actual network consists of a large number of routers connected with one another.

*3: Wide area Ethernet
It is a wide area communication network provided by some public communication services, combining switching hubs (layer 2 switches) used in Ethernet. It is possible to construct VPN environment where only the contracted points are connected by Ethernet like IP-VPN. In case of IP-VPN the only protocols that can relay are IP protocols, but in the wide area Ethernet, it is possible to use various protocols, not just IP.

WAN that can constitute a close network is recommended.

(Digital dedicated line, IP-VPN, Wide area Ethernet and so on.)

In connection through internet, it is necessary to construct VPN tunnel between the points where Client is set and the plant.

We will cite the example of the configuration of network through IP-VPN network and Internet.

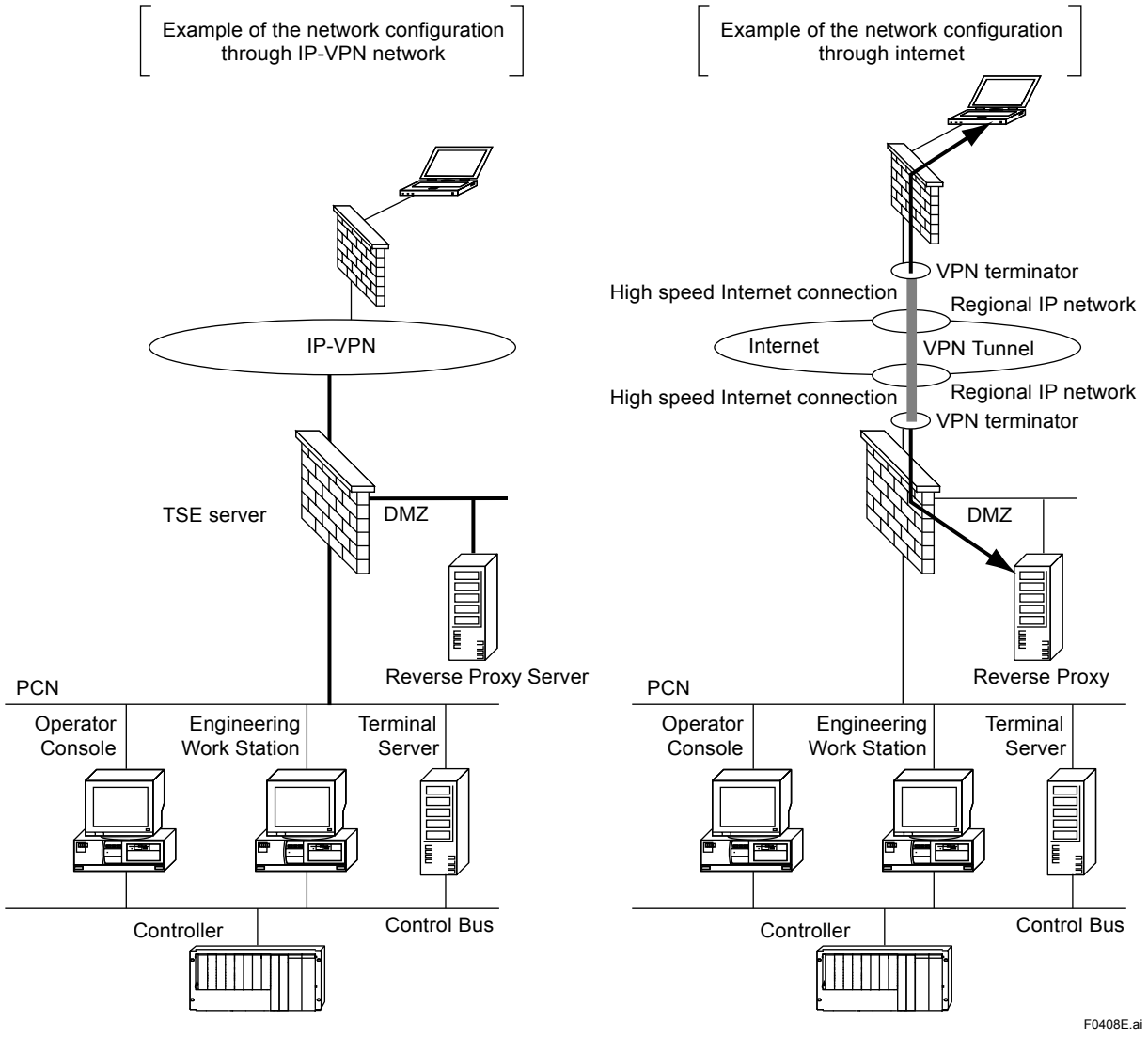


Figure Example of the configuration of remote monitoring network

Personal authentication

In remote monitoring system, sometimes, there is necessity for identifying a person to operate and monitor the plant as well as restricting his access rights to the specified devices.

In this case, a reverse proxy server that capable of authenticating the remote users for accessing the PCN should be applied. An example configuration of the system is shown below.

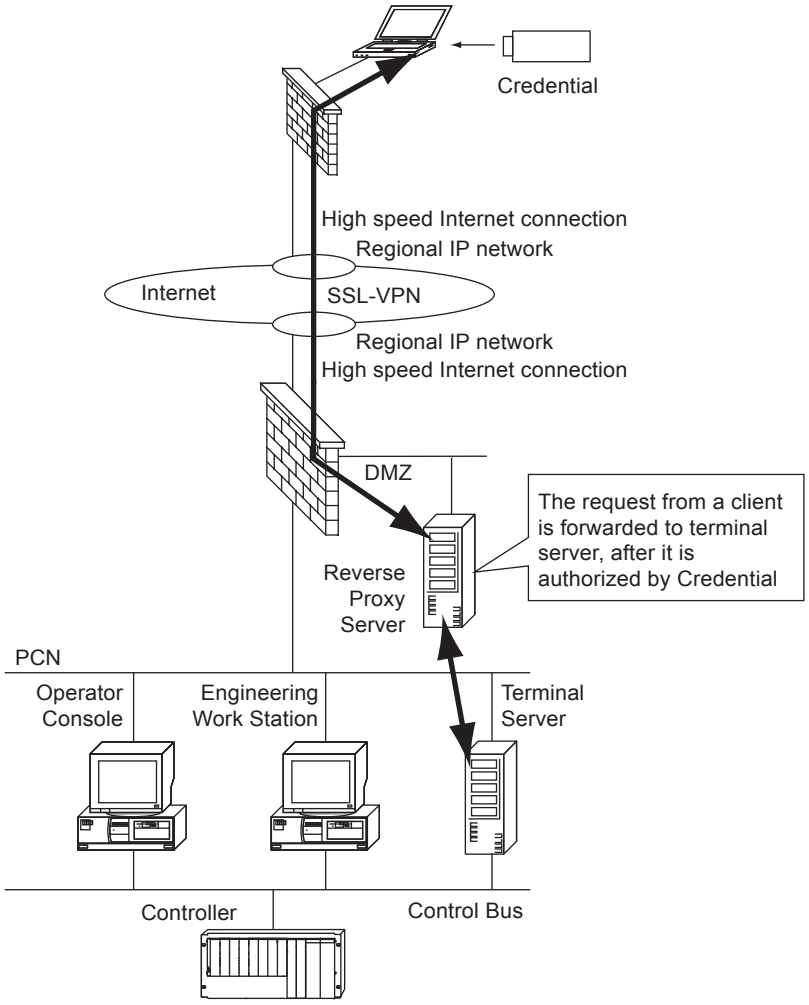


Figure Example of Personal Authentication

Before operation and monitoring, a user is authenticated between a client and the Reserve Proxy server based on individual credential. If the authentication is successful, the Reverse Proxy server will relay the request from the client to the terminal server.

The communication between the clients and the Reverse Proxy server is encrypted by SSL-VPN (*1).

*1: SSL-VPN : SSL-VPN is a technique to realize VPN, by using SSL (Secure Socket Layer), an encrypting protocol, widely used in internet. Since it is not necessary to install special software in the side of Client, unlike IPSec, it is widely used in the remote access environment of the enterprises.

4.2.8 Remote Maintenance

The remote maintenance through modem refers to the situation that a production control device or a network device vendor is using the telephone line or internet to establish the connection to access PCN for maintenances.

In a system like this, PCN can be accessed by through the telephone network or public line like internet. If there are any vulnerability in this system, it will open a backdoor (*1) to PCN, so that the PCN will be exposed to the threats of security.

*1: Backdoor: a backdoor which enables hacking.

■ Remote maintenance through modem

If a remote access environment or the remote access to PCN is established by using modem, the access route will bypass the protection of the firewall. Consequently, the remote access environment will not be secure, the remote access route will be the backdoor to PCN and the production control system will be exposed to the threats of security.

When constructing the environment for remote maintenance by use of modem, security should be obtained by the following measures.

● Use of RAS (Remote Access Server)

Make sure that every remote access to PCN be made via RAS. A remote access protocol such as PPP (point to point protocol) that authenticates all the remote access connections between a remote PC and RAS should be used.

● Use of callback

After the authentication with RAS, if it turns out to be a previously registered client, the client will get a callback.

● Authentication by using the caller ID

By using a modem that have the caller ID feature with the phone number, only the calls of the previously registered phone numbers can be accepted. Also it is possible to use the caller ID feature of RAS instead of the modem's authentication feature.

● Modem management

Turn off the power supply of the modem or disconnect the telephone line from the modem unless the remote maintenance is necessary.

The system-hardening of RAS

- User management

  The user IDs of minimum required users should be registered in the maintenance server. Moreover, when there is a user change, registration of the user ID should be changed accordingly.

- Password management

  The password registered in RAS should be the one impossible to guess and should be changed regularly.

- Antivirus

  Harden RAS with antivirus software and get it prepared for computer viruses. See the chapter 4.3 for more details.

- Security Updates

  Apply the latest Security Updates to RAS and exclude the security holes ever known. See the chapter 4.4 for more details.

For more descriptions about system-hardening, refer to the text on system-hardening in the chapter 4.5.

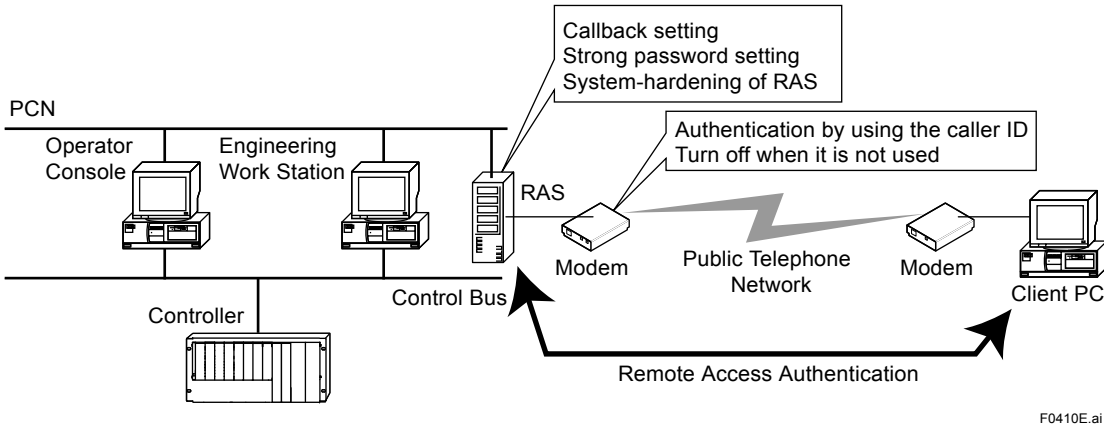


Figure Example of the configuration of remote maintenance by Modem

Remote maintenance through internet

When internet is used as a relaying line, PCN will be put in an environment where an unlimited number of people can freely access it. Therefore, it is important to enforce the security.

Security should be enforced with the following measures.

Internet VPN

For remote maintenance through internet, it is necessary to construct VPN between the two connected points.

Access control by firewall

The communication from outside should be restricted by firewall in accordance with the explanations in 4.2.3.

Maintenance server

Do not allow the remote maintenance terminals to access PCN directly but allow the access to PCN though a maintenance server set in DMZ.

The system-hardening of the maintenance server

- User management

  The user IDs of minimum required users should be registered in the maintenance server.

- Password management

  The password registered in the maintenance server should be the one impossible to guess and should be changed regularly.

- Antivirus

  Harden the maintenance server with antivirus software and make it robust against computer viruses. See the chapter 4.3 for more details.

- Security Updates

  Apply the latest Security Updates to the maintenance server and exclude the security holes ever known. See the chapter 4.4 for more details.

For more descriptions about system-hardening, refer to the text on system-hardening in the chapter 4.5.

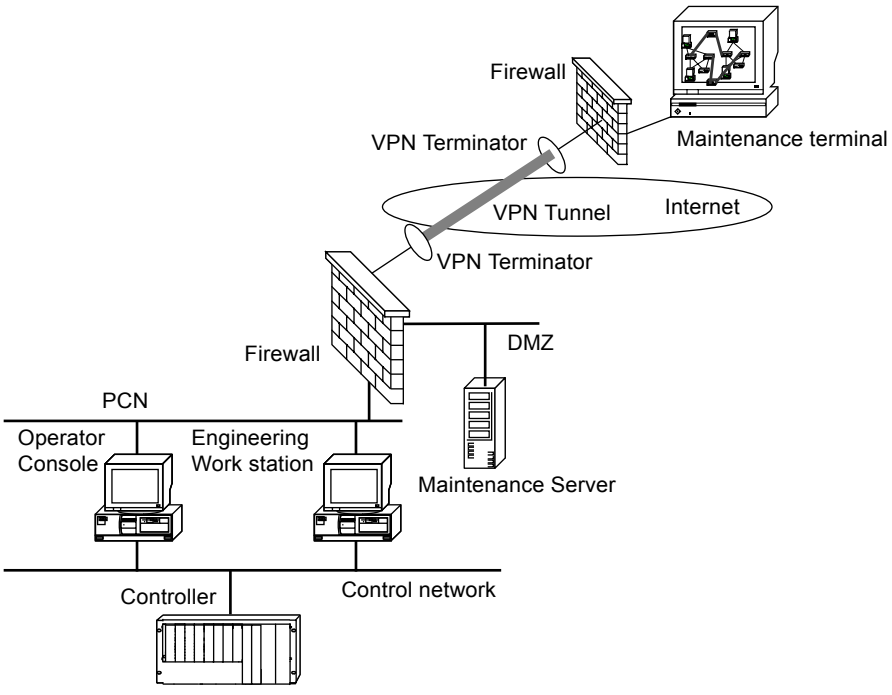


Figure Example of the configuration of remote maintenance via internet

4.3 Anti-malware Software

4.3.1 Antivirus Software

Antivirus software is effective as one of the countermeasures against malwares. Installation of antivirus software in Windows-based devices is strongly recommended, if those are components of a production control system, along with the following suggestions.

Applying antivirus software products

A production control system requires real time response and stable throughput to the operator actions via HMI and data acquisition by its supervisory systems. Due to its characteristics, antivirus software may have influence over performance of the PC.

Yokogawa has verified the performance of standard antivirus software in combination with Yokogawa's control system software.

SEE ALSO Yokogawa offers antivirus software as a fundamental solution. For more information, refer to:
Basic Endpoint Security solution (GS 43D02T30-05EN)

Environment of antivirus engine and virus definition file updates

When using antivirus software, it is most important to keep updating antivirus engine and virus definition files.

It is recommended to provide a server for updating these files in the DMZ, as accessing the external server for updating directly is vulnerable to the network configuration.

Daily management

In some cases, rebooting of a PC is required when a antivirus engine or virus definition file is updated. In other cases, the updating may bring an unexpected influence over operations of the PC. Therefore, a management procedure is required to verify if updating the antivirus engine or the virus definition file is safe before distributing them to all the PCs.

Prior confirmation

To reduce risks in conducting a prior confirmation, either one of the following measures can be taken.

- Use a system dedicated for testing. Then perform the test on the actual system.
- Conduct a test on one of the PCs in the actual system, and apply the tested updates to the rest after confirming that there is no problem.

4.3.2 Whitelisting Software

Malware inactivation

If only authorized programs are set to executable in advance, the execution of malware or unauthorized programs can be blocked. This is the malware inactivation by whitelisting method. This measure is most effective in reducing the security risk of PCs on which Microsoft Security Updates are not applicable or difficult to install. For more details, contact Yokogawa service window.

SEE ALSO Yokogawa offers antivirus software as a fundamental solution. For more information, refer to:
Standard Whitelisting Software for Endpoint Security (GS 30A15A30-01E)

4.4 Security Updates Management

Security Updates (Microsoft Security Updates) remove vulnerabilities known to Windows and protect production control system from unauthorized accesses and invasion by malwares.

Installing Security Updates

Yokogawa constantly investigates Microsoft Security Updates and conduct integration tests if those security Updates are relevant to Yokogawa products before offering. And Yokogawa let customers know the importance and priority of each security Updates.

For applying those Security Updates, it has to follow customers' security policies. Customers are to perform testing prior to applying those Security Updates considering the influences to the production control systems in advance.

Yokogawa suggests that all the applicable Security Updates must be applied to the control system as soon as possible. For installation of the Security Updates, please contact Yokogawa service department.

SEE ALSO For more information about security service, refer to:
Endpoint Security Service (GS 43D02T30-02EN)

Prior confirmation

To reduce the risk in applying Security Updates, ensure that those Security Updates works before those are applied to the PCs in the production control system.

To reduce risks, either one of the following measures can be taken in advance.

- Use a system dedicated for testing. Then perform the test on the actual system.
- Conduct a test on one of the PCs in the actual system, and apply the tested Security Updates to the rest after confirming that there is no problem.

SEE ALSO For more information about applying security Updates, refer to:
Basic Policy for Microsoft Software Updates (Including Security Patches) with Yokogawa ICSS Products (TI 33Y01B30-02E)

4.5 System-Hardening

System-hardening is explained here, to protect our system from hacking.

4.5.1 System-Hardening of PC Components

Assignment of passwords

The passwords used on the PC components are the information to prove that the user is an authorized user. If a password is leaked to an outsider, it may result in the illegal use or destruction of the data in the system. It is important to make some rules concerning the password management and to manage the passwords safely by obeying the rules.

The password policy is as follows:

- When setting a password, do not use an easily guessed password such as your name, your birth date or your telephone number.
- Change the password regularly.
- Do not tell your password to anyone but those concerned.
- Do not let anyone but those concerned take a glimpse of your password, when you are typing it.
- Do not write down your password on the paper.
- Contact the system administrator as soon as possible when you feel that your password may have leaked out.

We suggest using the following password policy in the PC components.

- The length of the password: 8 letters or more.
- The password must meet complexity requirements.

  A password must contain the characters from at least three (3) of the following types:

  English uppercase letters (A, B, ……., Z)

  English lowercase letters (a, b, ……., z)

  Westernized Arabic numerals (0, 1, ……., 9)

  Non-alphanumeric (special characters) such as punctuation symbols

Access control by personal firewall

A personal firewall helps decrease number of unauthorized accesses from external networks by restricting accesses to services on PC components.

The following personal firewall policy for PC components is recommended.

- Enable Windows firewall function
- Generate a list of services or TCP/UDP port numbers connected with outside, then register them on the firewall. If the scope (IP address and subnet) of the senders who ask for connections are already known, set the scope up.

The personal firewall settings are different by product.

SEE ALSO About Yokogawa's approach to the system-hardening of PC components, refer to
"4.8 Security Function of Yokogawa System Products."

4.5.2 System-Hardening of Network Devices

Hardening network devices with defensive measures against malwares and unauthorized accesses is important. In this section, guides for system hardening for each network device are described.

■ Firewall

Firewall, a main device for a boundary security, is exposed to external networks and system hardening for it is of high importance. System-hardening of the firewall must be performed in the following manners:

● Use a dedicated firewall

The use of a dedicated firewall is recommended for preventing the network from various troubles, rather than using a device with a firewall built with many other functions.

● Administrator password

When assigning an administrator password, use one that cannot be easily guessed, by using the following rules:

English uppercase letters (A, B, ……, Z)

English lowercase letters (a, b, ……, z)

Westernized Arabic numerals (0, 1, ……, 9)

Non-alphanumeric (special characters) such as punctuation symbols

The administrator password must contain characters from at least three (3) of the above types.

Mnagement of Management Segment (*1)

Firewall needs a management console in order to set the access control rules or confirm the logs and alerts. Usually, the special tools are installed in PC or Web browsers are used. The management console can change the access control rules, so in order to prevent the illegal operations of the outsiders, it is necessary to put the management console in the environment where it is not possible to be accessed from the outside. The following measures should be taken.

- Make the independent segment for it and separate it from other segments.
- The settings in the firewall should allow only the operations from the designated management console.

*1 When the remote management service of the vender is used, these restrictions are not valid. In that case, the rules for the system requirements of the service should be followed.

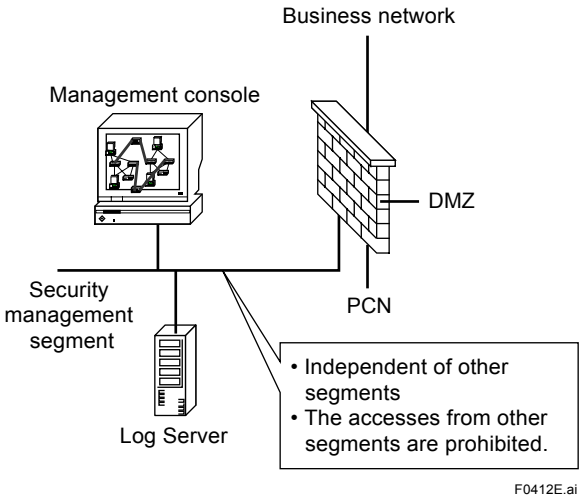


Figure Segment of security management

The restriction on network services

Only the services of minimal requirements should be allowed. Especially for the permissions on using ftp, tftp, telnet should be very careful. If they are not necessary, they should be blocked.

Management of the information on change in the setting

Set the firewall to remain the logs of all setting changes.

Software update

Update only the necessary software after confirming the release information of the vender and taking care of the security holes.

Switch

Recently, the intelligent switches are widely used. The settings of an intelligent switch can be changed through networks. Therefore, if this part is vulnerable, the devices connected to the switch will be exposed to the threats of illegal accesses. It is necessary to do the system-hardening of this part in the following way.

Disable the management via networks

The maintenance port should be used when changing the switch settings and stop the services like telnet or http so as to avoid the setting changes from the network.

Privileged password

When a user changes the settings of a switch, checking the password is the most common way for user authentication. Therefore a password that cannot be easily guessed should be set as the privileged password for changing the switch settings.

Port security

If the unused ports of a switch can be used freely, the danger of being connected by the unauthorized devices will exist. Do the followings on the switches with the port security features.

- Disable the unused ports.
- Check the MAC addresses to restrict the connection to the ports.

For a non-intelligent switch, such measures cannot be applied so that some physical measures should be taken to prevent the ports from the unauthorized accesses (for example, by installing the switch in a locked rack).

SNMP setting

Intelligent switches support SNMP. SNMP enables the network management tool to monitor the state of switches. It is possible to read and write the management information with SNMP by an outsider so that the following measures need to be taken to prevent the illegal operations.

- Restrict the communications of the switch to those with network management tools.
- Disable the setting change through SNMP. (Deny SET command)
- Set a community name that cannot be easily guessed. Treat it with the same care as a password.

Network monitoring device

Network monitoring device monitors the state of network devices such as the switches by using SNMP or Ping. The following measures should be taken.

Restriction on the accesses from the outside

If a network monitoring device is used to monitor the devices on PCN and DMZ, there will be no need to allow any access from the external network, so that the settings on the firewall should be set to block the outside accesses.

Restriction on network service

Only the services of minimal requirements should be allowed. Especially for the permissions on using ftp, tftp, telnet should be very careful. If they are not necessary, they should be blocked.

Wireless access points

Take the following measures to the access points so that they can be concealed from the scanning of access points by War-driving or other similar tools.

- Disable the broadcast of ESSID. (Beacon signal)
- Disable the response to the broad request.
- Assign an administrator password that cannot be easily guessed.

4.6 Monitoring the System and the Network

Day by day, the new vulnerability of OS or network service is found and the way of attacking them is under constant evolution.

Therefore, whatever security measure the system may take, still, it is impossible to wipe out all the possibility of security incidents. It is important to monitor the system and the network without fail and if something should be wrong with them, detect the signs that may lead to incidents and try to minimize the damage as much as possible.

4.6.1 Audit Logs

Using the audit logs is effective for detecting and tracking the signs of illegal accesses. It is necessary to assign some persons responsible for regularly monitoring the audit logs.

Time-stamps are important for logs. Time should be kept accurate using NTP and so on.

TIP

It is necessary to keep the logs for a certain time in order to track the security incidents or to secure the evidence.

■ PC

Enable the logs for the following events.

● PC component

- Audit logon events (Success / Failure)
- Audit account management (Success / Failure)

● Windows Domain controller

- Audit logon events (Success / Failure)
- Audit account logon events (Success / Failure)
- Audit account management (Success / Failure)

■ Firewall (including personal firewall)

Regular monitoring the logs of firewall may detect the illegal access attempts from the outside.

- All the packets that violate the access control rules set in firewall should be logged.
- Worrying that the log files may become too big for the firewall, a log server can be placed in the security management segment to store the logs output from the firewall.

4.6.2 IDS/ IPS

IDS stands for Intrusion Detection System. IPS, on the other hand, is called Intrusion Prevention/ Protection System. IDS and IPS have a mechanism to inform administrators when fraud or abnormality is detected. In order to catch the omen, the logs should be audited on a regular basis.

IDS

IDS can be divided into two types, network type and host type, depending on the monitoring method of communication results. The network type IDS (Network-Based IDS: NIDS) is what monitors data flowing over the network. The host type IDS (Host-Based IDS: HIDS) is placed on the server to be monitored and monitors the data and logs received on the server generated as a result of communication. In addition to intrusion detection, it also supports tampering with files.

IDS is also classified as “Misuse detection type” and “Anomaly detection type” depending on a method of detecting unauthorized intrusion or malicious access. The misuse detection adopted in many IDS is a method to detect intrusion by matching it with a pattern or rule called a pre-registered “signature.” If the IDS finds a packet that matches the signature, it treats it as an intrusion or attack. With this type of algorithm, only intrusions using known methods can be detected.

The other hand, the anomaly detection is possible to find intrusions using unknown method by detecting traffic different from usual. Set the threshold of normal times for conditions such as login time, network traffic status, usage command etc, and judge it as abnormal when it is different. Recent IDS products often adopt both of these detection methods.

IPS

IPS is connected with networks by in-line. Basically, the IPS functions as a bridge, monitoring the traffics, detecting and excluding illegal packets like worms.

It is used:

- To segregate the PCN network into zones. (See the chapter 4.2.1)
- To protect the devices that cannot update the Security Updates and the virus definition file of at real time.

Besides excluding the illegal packets, IPS also broadcasts the notification and logs the events, so that it can also be used for monitoring the network.

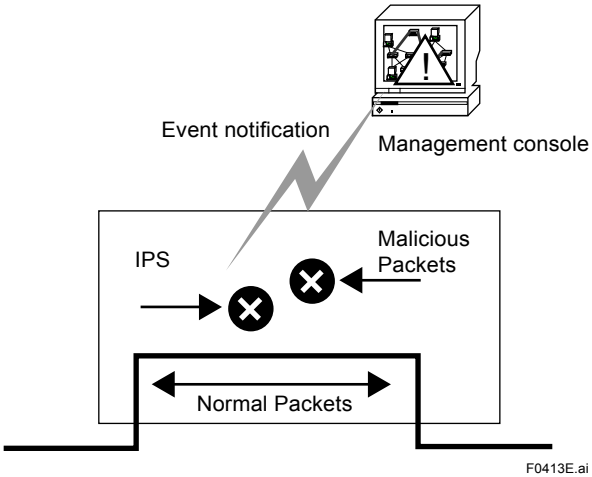


Figure The operation of IPS

Monitoring of detection events

When IPS detects and excludes the illegal packets, the notification about the events will be sent to the management console. Right after the notification is sent from IPS, a team for handling the incidents should act immediately to take care of the situation.

Notices about constructing IPS

- Handling excessive self-defense

  The communication settings defending IPS needs to be tuned in according to the environment where the IPS is placed. When the tuning is not appropriate, some inconveniences such as the intercepting the required communication frames may occur.

- Setup a route for handling troubles

  When IPS is installed in a network by in-line, if some trouble occurs in IPS, the communication between the two networks connected to IPS will be interrupted. Some IPSs have a (fail open) feature to pass all the communications at the time of troubles. However, how to handle communication packets at the time of troubles need to be decided according to the requirements of the actual systems.

- Updating signature

  In IPS, a signal called signature is used to detect the illegal packet. This signal functions the same as virus definition file in the antivirus software, so that it is necessary to update it periodically.

Difference between IDS and IPS

The difference between IDS and IPS is as follows.

- IDS only notifies that there is abnormal communication.
- IPS notifies abnormal communication and carries out even further blocks.

Yet another major difference is that IDS monitors the original copy of the communication and notifies the anomaly, but because IPS needs to block abnormal communication, it will be in between communication routes.

Therefore, in the event that a device of IPS fails, priority is given to maintaining communication, so it is necessary to pay attention that all communications are permitted as basic operation.

4.6.3 NMS

NMS (Network Management System) manages the network devices and the configuration information (IP address, port connection information, line information, etc.) present on the network, and grasps the operational status and signs of failure in real time. By performing network management, it is possible to prevent the occurrence of failures beforehand. In addition, it can gather information necessary for measures to efficiently use the network.

NMS mainly collects various information from network equipment using SNMP (Simple Network Management Protocol) and tells the administrator in an easy-to-understand manner.

SNMP

SNMP (Simple Network Management Protocol) is a UDP/IP based protocol for network monitoring and network management. It is used for status monitoring, resource monitoring, performance monitoring, traffic monitoring of network devices such as routers and switches, Windows and UNIX servers, etc. In general, CPU usage, memory usage, disk usage, process monitoring, Windows event log monitoring, and syslog monitoring are performed for the server. For network devices, it monitors the number of packets sent and received on each port, the number of error packets, the port status, CPU usage, memory usage, and so on. Some vendors have published items specific to the device, and fine monitoring is possible.

4.7 Windows Domain Management

**As Windows computers were used to run the HMI of production control systems, the Windows Domain Controller has been introduced to manage the HMI.
This section describes the operations of Windows Domain Management with considerations for security.**

TIP

The Windows domain is managed by Active Directory. Active Directory is a directory service created by Microsoft. It was released first with Windows 2000 Server. It enables centralized management of hardware resources—servers, clients, printers—on the networks, and information about users—user attributes, access rights—that use these resources. In Active Directory, the server that contains the domain database is called the Domain Controller.

Windows domain configuration for an office environment

In recent years, the needs for the clients in the office environment using their user accounts in the PC to access the process data server become more and more popular.

Generally the accounts of the PCs in office LAN are managed in a shared resource managed in the Windows domain. This section describes the Windows domain configuration for an office environment.

The users allowed to access the open process data server need to be managed. However, since the domain administrator may be different from the process data server administrator, the authorizations for accessing the process data server should be granted by the process data server administrator and independent from the Windows domain administrator.

To group the users into local groups is an effective way to manage the users for accessing the process data server.

1. Register the process data server as a member server of the domain.
2. Create a local group in the server and grant the group with the permission to access the server.
3. Register the users in the domain into this group for accessing the process data server.

In this way, the accounts of the users are managed by the domain, and it becomes possible for the local group to manage the right of the server to access.

In addition, the local groups can be granted with different privileges for accessing the process data server so that the rights of each user can be managed accordingly. The accesses are as follows.

- Permission to read data

  User has right to logon the server and read data in the server.

- Permission to write data

  User has right to logon the server and read/write data in the server.

- Permission to change the engineering settings

  In addition to the above privilege, user also has right to change the engineering settings.

By setting these privileges, it is possible to manage the user access rights properly.

Windows domain management in the production control system

Windows domain management in the PCN enables centralized management of user accounts and increases system availability. However, if the domain controller is down, there is a risk that the names cannot be resolved. It is, therefore, recommended to have a redundant Windows Domain Controller.

TIP

If a computer in the system is installed with applications that are not supported by Windows Domain Management, use the existing stand-alone management for that computer.

4.8 Security Function of Yokogawa System Products

In this clause, the security functions of Yokogawa system products that should be applied to the control system as the security countermeasures are explained from the technical point of view. Each system product is provided with the function to strengthen the security for the operation and monitoring consoles, control units and engineering stations. The security functions of an operation and monitoring console is prepared for the securities on operating the industrial plant; The security functions of an engineering station is prepared mainly for protecting the database of the system. Both operation and monitoring console and engineering station manage the security by identifying the users with the User ID and Password. The ProSafe-RS system is provided with the strengthened security functions in the controllers so that safety control means more safety.

Security of system products

Different measures have been implemented to ensure the security of Yokogawa system products. This section describes the generic IT security that uses Windows security function, and product-specific security functions.

IT security

The IT Security Setting that uses Windows security function was supported since CENTUM VP R4.01 and ProSafe-RS R2.01. Configuring IT security hardens the computer and protects it from threats.

The threats handled by IT security can be categorized as follows:

(1) Network attacks

(2) Direct attacks by manipulating computer components

(3) Theft of computer components or important data

Three different security models are available to enable you to handle these threats. These models flexibly support different system configurations and operations.

Table Security models

Model	Feature
Legacy model	This model does not strengthen the security. It prioritizes collaboration with old products and products where IT security is not applied.
Standard model	This model focuses on the relevant system operations and collaboration with other systems. It can counter threats (1) and (2).
Strengthened model	This model is used to counter all the three threats stated above. Operations may be affected if full security is in place.

Yokogawa IA system products provide a tool that automatically configures the security setting for the threats above. There are two kinds of security settings - IT security version 1.0 and IT security version 2.0.

- IT security version 2.0

  This version was designed after reconsidering the IT security version1.0 and includes more security measures. It supports the Standard and Strengthened (*1) security models.

- IT security version 1.0

  This version had been offered as the security measures of CENTUM VP R6.03 and earlier versions. It supports the Legacy, Standard, and Strengthened (*1) security models.

*1: Please contact Yokogawa for more details about settings of the strengthened model.

IT security version 2.0 and IT security version1.0 can coexist in the same project in CENTUM VP. The following tables show the security threats that are coped by this security measures.

Table IT security version 2.0

Security measure	Threat handled		
	(1)	(2)	(3)
Password Policy-[Minimum password length]	Yes	Yes	No
Password Policy-[Minimum password age]	Yes	Yes	No
Password Policy-[Maximum password age]	Yes	Yes	No
Password Policy-[Enforce password history]	Yes	Yes	No
Disable 'Password Policy-[Store passwords using reversible encryption]'	Yes	Yes	No
Password Policy-[Password must meet complexity requirements]	Yes	Yes	No
Access Control for files and folders	Yes	Yes	No
Access control for product registry	Yes	Yes	No
Access Control for DCOM (OPC) objects	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Set 'Personal Firewall-[Allow unicast response]' to 'No'	Yes	No	No
Stopping unused Windows services	Yes	No	No
Account Lockout Policy-[Account lockout threshold]	Yes	Yes	No
Account Lockout Policy-[Reset account lockout counter after]	Yes	Yes	No
Account Lockout Policy-[Account lockout duration]	Yes	Yes	No
Disabling NetBIOS over TCP/IP	Yes	No	No
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Applying the software restriction policies	Yes	Yes	No
. . . (0mission) . . .			
Security-[Require secure RPC communication]	Yes	No	No
Security-[Require user authentication for remote connections by using Network Level Authentication]	Yes	No	No
Sync your settings-[Do not sync Apps]	Yes	No	No
Sync your settings-[Do not sync start settings]	Yes	No	No
Disable 'Windows Error Reporting-[Automatically send memory dumps for OS-generated error reports]'	Yes	No	No
Disable 'Windows Logon Options-[Sign'-in last interactive	No	Yes	No
user automatically after a system'-initiated restart]'	No	Yes	No
Notifications-[Turn off toast notifications on the lock screen]	Yes	Yes	No
Disabling Built-in Administrator Account or Changing User Name	No	No	Yes

Table IT security version 1.0

Security measure	Threat handled		
	(1)	(2)	(3)
Access control	Yes	Yes	No
Personal firewall tuning	Yes	No	No
Stopping unused Windows services	Yes	No	No
Disabling the built-in Administrator account or changing its user name	Yes	Yes	No
Hiding the last logon user name	Yes	Yes	No
Applying the software restriction policies	Yes	Yes	No
Applying AutoRun restrictions	No	Yes	No
Applying the StorageDevicePolicies function	No	Yes	Yes
Disabling USB storage devices	No	Yes	Yes
Disabling NetBIOS over TCP/IP	Yes	No	No
Changing the LAN Manager authentication level	Yes	No	No
Applying the password policy	Yes	Yes	No
Applying the audit policy	Yes	Yes	No
Applying the account lockout policy	Yes	Yes	No
HDD password function by BIOS	No	No	Yes

For details about IT security, refer to IM of each product.

- CENTUM VP Security Guide (IM 33J01C30-01EN)
- ProSafe-RS Security Guide (IM 32P01C70-01EN)
- STARDOM IT Security (IM 34P02Q93-01E)
- Plant Resource Manager Security Guide (IM 33Y05Q13-11E)
- Exaopc Security Guide (IM 36J02A01-01E)
- Exapilot Security Guide (IM 36J06B01-01E)
- Exaplog Event Analysis Package Security Guide (IM 36J06A01-01E)
- FAST/TOOLS Windows IT Security Guide (TI 50A 01A10-04EN)

TIP

The content of “IT Security Guide for System Products (for each product)” issued as TI 30A15B3x-01E is old. For the latest information, please refer to the above IM.

4.8.1 CENTUM VP

The security settings of CENTUM can be classified into two functions, the IT security function based on Windows security feature, and the CENTUM VP peculiar security function.

IT security function of CENTUM VP

The IT security function to enhance security is supported on CENTUM VP. System-hardening of CENTUM VP IT environment is realized by using Windows functions. For example, the usage of CENTUM VP tools and access permissions to folders/files are managed by access control for users and groups of Windows. Therefore, it is possible to apply the security countermeasures in such circumstances to allow a Windows user as an operator to logon to the PC for using the operator windows and tools but restricted from starting the engineering to tools.

Moreover, some communication types and communication ports can be disabled by Windows firewall and DCOM settings.

IT security version 2.0 is applicable for CENTUM VP R6.04 or later.

Authentication mode

In R4.02 or earlier of CENTUM, you can define users and their respective access rights for CENTUM Engineering or CENTUM Operation and Monitoring function. These users are independent from Windows users. That is the CENTUM Authentication mode. By using the Windows Authentication Mode that was newly added in CENTUM VP R4.03, you can integrate Windows accounts with Operation and Monitoring users, and ensure a secure system within the Windows user management framework. In case of necessity more strong security, it is recommend to use windows authentication mode. And, by making good use of the centralized user management made possible with Windows domain configuration, you can significantly improve the usability of the system.

CENTUM VP specific security function

CENTUM VP have a specific security function for controlling accesses, mainly for controlling the accesses to the controller data and application database. The HIS user used for this access control is specially defined for CENTUM VP. As mentioned earlier, from CENTUM VP R4.03 onwards, the Windows Authentication Mode is available to associate Windows User Account function with CENTUM User management.

In CENTUM VP, the users are usually divided into 4 groups; Operators, System engineers, Recipe engineers and Report users. The access control is applied to each user group. The user groups are largely divided into the following 2 categories.

- HIS group user: Operators (Operation and Monitoring Function)
- ENG group user: System engineers (System View/Builders)

  Recipe engineers (Recipe Management Function)

  Report users (Report Function)

These are the access control functions. (*1)

- Register or delete user IDs
- Set user rights for each user ID
- Automatic User-Out
- Check Illegal access
- Lockout users
- Release locked user IDs
- Reconfirm with double authentications (*2)
- Check validity period of password
- Check and block the obsolete password
- Set minimum password length
- Automatic logon Windows
- Set CENTUM desktop environment

*1: With the Windows Authentication Mode, some of these access control functions are handled by the Windows User Account Management function.
*2: In security terms, this is known as Dual Lock function.

For the security of the system, we recommend that the above mentioned access control functions be applied according to the privileges of the users.

SEE ALSO For more details about the access control functions of ENG group user, refer to:

Access Control Package (GS 33J10D20-01EN)

Access Administrator Package (FDA:21 CFR Part 11 compliant) (GS 33J10D40-01EN)

4.8.2 ProSafe-RS

ProSafe-RS supports the IT security function based on Windows security feature, also the CENTUM VP peculiar security function can be applied on ProSafe-RS/CENTUM integrated system. In addition, ProSafe-RS has peculiar security functions to enhance security as Safety Instrumented System.

IT security function of ProSafe-RS

The IT security function to enhance security is supported on ProSafe-RS R2.01 and later. System-hardening of ProSafe-RS IT environment is realized by using Windows functions. Moreover, the IT security function can be applied on ProSafe-RS/CENTUM VP integrated system. Therefore, it is possible to apply the security countermeasures in such circumstances to allow a Windows user as a CENTUM VP engineer to logon the PC for using the CENTUM VP engineering tools but restricted from starting the ProSafe-RS engineering tools.

IT security version 2.0 is applicable for ProSafe-RS R4.03 or later.

CENTUM VP specific security function

This security function can be used on ProSafe-RS and CENTUM VP integrated system. By using the security control function with HIS user, it is possible to control access permission to the data of SCS (Safety Control Station).

ProSafe-RS specific security function

ProSafe-RS has the following securities in order to inhibit the access to the system by the unauthorized users or from the unauthorized devices to prevent the unintended changes resulted from the operation errors of the users.

Table Outline of the security function of ProSafe-RS

	Access control by password	Access control by hardware key switch	Remarks
Change in project database	Applicable	N/A	Access control rule can be set for the whole SCS or for each program in SCS.
Non-safety operations to SCS	Applicable	N/A	Access control by SCS Maintenance Support Tool in SENG
Safety-related operations to SCS	Applicable	Applicable	Access control is applied to both the operations from SENG and from HIS. Permit or Deny is handled in SCS.

The passwords should be used and the passwords should be difficult for an outsider to guess. For more information about assigning passwords, see the descriptions about the password assignment rules cited in the chapter 4.5.

In addition, a hardware key switch can also be used for access control according to the requests from the customers.

SEE ALSO There is a function that sets the operation rights of engineers. For details, refer to:

Access Control and Operation History Management Package (GS 32P04D30-01EN))

4.8.3 STARDOM

STARDOM has two types of security functions, an IT security function based on the Windows security function, and a STARDOM specific security function.

IT security function of STARDOM

The IT security function to enhance security is supported on STARDOM R3.20 or later. It makes use of Windows functions to harden the STARDOM IT environment. For example, it uses the access control function for Windows users and groups to control usage of STARDOM tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to limit communication types and communication port numbers.

Security settings are easy to use by the tool that is included in this product. STARDOM supports Legacy model and Standard model.

STARDOM specific security function

In STARDOM, the operators are divided into various groups and the operable range for each group is specified, as in CENTUM VP. Moreover, the record of the operation by the operators can be kept. Manage the passwords carefully so as not to allow an outsider masquerading as a user to operate the system. The following are the security functions of STARDOM. Apply these functions to the PCs according to the requirements for preventing the operational errors and improving the operation safety.

- Set operation range for each user group
- Protect the operation files
- Manage HMI server passwords
- Notify the password change
- Notify the password expiration in advance
- Notify the password expiration
- System inhibitions: Inhibit some Windows functions
- Desktop inhibitions: Inhibit some operations on Windows desktop
- Application inhibitions: Inhibit some operations on Internet Explorer

4.8.4 Plant Resource Manager (PRM)

PRM has two types of security functions, an IT security function based on Windows security function, and a PRM specific security function.

IT security function of PRM

The IT security function to enhance security is supported on PRM R3.03 or later. It makes use of Windows functions to harden the PRM IT environment. For example, it uses the access control function for Windows users and groups to control usage of PRM tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

IT security version 2.0 is applicable for PRM R4.01 or later.

PRM specific security function

With regards to security, PRM is equipped with the functions of access control of users, access control of the connected devices and management of operation history.

Access control of operators

In PRM, users are managed by their user names. In order to use the functions of PRM, it is necessary to have a user name and a password. The passwords should be carefully managed so as not to allow an outsider to operate the system illegally.

A user must belong to a user group. Moreover, each window on PRM is provided with a setting for the access privilege of each user group. A number of default user group are already built in the PRM, however, the new user groups can be added according to the actual security management policy.

A further concept in PRM is the permissions for each user. The operation privilege of a user is not only subject to the privileges set for each user group but also subject in detail to the permissions for the individual user.

Access restrictions on the connected devices

PRM can not only restrict the users on operating various PRM functions, but also restrict users on accessing various devices connected with PRM. The permissions for accessing the connected devices need to be configured according to the authority of each user.

Audit trails of the operations

PRM keeps the records of all operations. All the operation events on PRM, all the operations on the devices connected to PRM and all the inspection events and inspection results of these devices are logged as audit trails. The audit trails can be displayed and printed out.

4.8.5 B/M9000 VP

B/M9000 VP has two types of security functions, an IT security function based on the Windows security function, and a B/M9000 VP specific security function.

IT security function of B/M9000 VP

This function was prepared to strengthen the security for B/M9000 VP, similar to that of CENTUM VP. It makes use of Windows functions to harden the B/M9000 VP IT environment. For example, it uses the access control function for Windows users and groups to control the usage of B/M9000 VP and CENTUM VP tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

B/M9000 VP specific security function

B/M9000 VP has unique access control functions for screen customization. This security function is managed separately from Windows security. Users are classified into operators, staff, and engineers, and different access control functions are used for each of these user groups.

User groups are classified into three major categories:

- Operator group: operators
- Maintenance group: staff
- Engineer group: instrument engineers, engineers

The following access control functions are available:

- System installation and uninstallation, system device registration and deletion. (engineer group)
- System backup and restore, screen customization. (maintenance group)
- Screen operation. (operator group)

To ensure that the system is secure, it is recommended to configure these access control functions according to user rights.

4.8.6 Exaopc

Exaopc has two types of security functions, an IT security function based on the Windows security function, and an Exaopc specific security function.

IT security function of Exaopc

This function makes use of Windows functions to harden the Exaopc IT environment. For example, it uses the access control function for Windows users and groups to control usage of Exaopc tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

IT security version 2.0 is applicable for Exaopc R3.76 or later

Authentication mode

Exaopc R3.70 or later uses the user authentication mode when accessing to CENTUM data. Either “CENTUM authentication mode” or “Windows authentication mode” is applicable.

Exaopc specific security function

OPC security interface

Exaopc can set its security by OPC Security compliant interface, when OPC client uses DA/A&E/HDA/Batch server function. The username/password specified here is used by the following CENTUM security function.

CENTUM security function

CENTUM VP specific security functions can also be applied to Exaopc. For example, access restrictions by user groups can be used. This allows you to set fine security for OPC clients.

4.8.7 Exaquantum

Exaquantum has its own unique security functions, which are as follows.

Exaquantum specific security function

The security function of Exaquantum is realized according to the users and groups managed by Windows. Each user can be defined with adequate security. For an example, an engineer or a user can change the process data, while another user can only read the process data by registering the different users to different groups as explained in below. As a result, the operation errors and illegal operations by the unauthorized users can be prevented. In addition, the operation events by the users can be recorded as audit trails.

Exaquantum has preset the default users beforehand in the system. It is especially important to manage the passwords of default users strictly. On assigning the passwords, you should follow the rules explained in the chapter 4.5 System-Hardening.

The following shows the groups regarding to the security management.

Connection security group

This group is for the users to connect with Exaquantum server; and granted with the following privileges.

- Referencing data
- Displaying graphics

Management security group

This group is for the users to change the management information or write data on Exaquantum; and granted with the following privileges.

- Changing database settings
- Creating tags
- Writing data

Writing data security group

This group is for the users to write tag data; and granted with following privileges:

- Changing data
- Writing to DCS

Graphic editing security group

This group is for the users to edit graphics; and granted with following privileges:

- Editing graphic displays

RBNS security

This is a set of settings about the permissions for reading and writing to the tags corresponding to each security groups regarding the following privileges:

- Referencing data
- Changing data

4.8.8 Exapilot

Exapilot security functions can be classified into two types, an IT security function based on the Windows security function, and an Exapilot specific security function.

IT security function of Exapilot

This function is created to strengthen the security for Exapilot R3.70 and later versions. It makes use of Windows functions to harden Exapilot VP IT environment. For example, it uses the access control function for Windows users and groups to control the usage of Exapilot tools and access to folders/files. In addition, this function configures Windows Firewall and DCOM to restrict communication types and communication port numbers.

IT security version 2.0 is applicable for Exapilot R3.97.00 or later.

Authentication mode

Exapilot has two types of user authentication mode below.

- Windows authentication mode

  The way to authenticate a user by using the Windows function.

- Exapilot authentication mode

  The way to authenticate a user by using Exapilot specific function.

Exapilot specific security function

Exapilot has a security function to authorize operation permissions for each user, where the user is controlled by Exapilot. Exapilot specific security is classified into three types; system security to apply on all operations; main procedure security to apply on main procedures; and subprocedure security to apply on sub procedures. By setting these securities, each user can have suitable security rights for administrator, operator and engineer privileges. As a result, operation errors and illegal operations by the unauthorized users can be prevented. In addition, the operation events by the users can be recorded as audit trails.

It is recommended to assign the passwords that cannot be easily guessed by the outsider to the users and set the operation privilege of each user to a minimum level. On assigning the passwords, you should follow the rules explained in the chapter 4.5 System-Hardening.

System security

Exapilot system security restricts access and permissions on the following operations for each user.

Operations that can be restricted

- Operation window
- Builder window
- Utilities window
- Security window
- The other tools

Main procedure security

Main procedure security restricts the building and running operations of individual procedures for each user.

Operations that can be restricted

- Building operation
- Running operation

Subprocedure security

Subprocedure security restricts the building and running operations of individual procedures for each user.

Operations that can be restricted

- Building operation
- Running operation

4.8.9 Exaplog

Exaplog has two types of security functions, an IT security function based on the Windows security function, and an Exaplog specific security function.

IT security function of Exaplog

This function makes use of Windows functions to harden the Exaopc IT environment. For example, it uses the access control function for Windows users and groups to control usage of Exaopc tools and access to folders/files. In addition, this function configures Windows Firewall to restrict communication types and communication port numbers.

Exaplog specific security function

Execution of the Exaplog program is limited by the user group as shown in the table below.

Window name/ Tool name	PLG_ANALYST (PLG_ANALYST_LCL)	PLG_SUPER_ ANALYST (PLG_SUPER_ ANALYST_LCL)	PLGMAINTENANCE (PLG_MAINTENANCE _LCL)	EXA_MAINTENANCE (EXA_MAINTENANCE_ LCL)
Event analysis tool (PLView)	Yes	Yes	Yes	
Long-term summary tool (PLSummary)	Yes	Yes	Yes	
Exaplog administration (PLAdmin)		Yes	Yes (*3)	
Tri-REPORT data import tool		Yes	Yes	
Command under Exaplog¥tool		Yes	Yes	
Password change tool			Yes	
IT security tool				Yes
Software Configuration View	Yes (*1)	Yes (*1)	Yes	Yes
EXA Information Gathering Tool				Yes (*2)
Install				Yes
Client Install				Yes

*1: Exaplog information can be displayed. User accounts without administrator's authority cannot display registry information.
*2: For the start method, refer to the instruction manual for the EXA Package Information Gathering Tool.
*3: PLG_MAINTENANCE is used to change the setting for automatic start of Exaplog with PLAdmin.

4.8.10 FAST/TOOLS

FAST/TOOLS has two types of security functions, an IT security function based on the Windows security function, and a FAST/TOOLS specific security function.

IT security function of FAST/TOOLS

IT security version 2.0 is applicable for FAST/TOOLS R10.04 or later. This function makes use of Windows functions to harden the FAST/TOOLS IT environment. For example, this function configures Windows Firewall to restrict communication types and communication port numbers, stops unused Windows services, and uses the access control function for Windows users and groups to control usage of FAST/TOOLS and access to folders/files.

FAST/TOOLS specific security function

The FAST/TOOLS specific security function falls into two categories.

(1) User Management function

FAST/TOOLS has security mechanism considering the SCADA based application security. This mechanism is possible to manage users considering functional authorization such as read-only permission and full system configuration permission versus area authorization. Additionally, FAST/TOOLS supports sophisticated user profiles which can integrated with Active Directory user management by mapping user group name on AD to FAST/TOOLS user profiles. And, FAST/TOOLS supports “Single sign-on” based on Active Directory.

(2) Communication function

FAST/TOOLS enables users to Monitor, Control and Engineer their application systems in a wide distributed network configuration. FAST/TOOLS supports security countermeasures to data connections as below.

- Secure Communication by encryption (Client to Server)
  Operation data is displayed in Web-HMI client and Mobile client via FAST/TOOLS Web server. FAST/TOOLS supports Secure Socket Layer(SSL) to secure this data connections.
- Secure Connection by encryption (Server to Server)
  Communication between two FAST/TOOLS Systems used in FAST/TOOLS distributed systems is encrypted. FAST/TOOLS multi-node network security is based on industry standards that are also used for secure communication on the Internet, including DTLS and public/private keys.
- OPC UA
  OPC UA is the next-generation standard of OPC developed by OPC foundation. OPC UA provides a cohesive, secure, and reliable cross-platform framework for access to real-time and historical data and events. FAST/TOOLS supports both Server (DA/AC/HA) and Client (DA) roles of OPC UA. FAST/TOOLS together with the security features of the OPC UA, supports users connecting new or existing equipment to secure, high reliable and manageable network.

4.9 Staff Security Policy

One of the major threats that may lead to security incidents is “human.” A human mistake, such as an incorrect operation, can be a major threat.

4.9.1 Education

The purpose of the education is to make the staff to have skills and knowledge of security so that they act in accordance with the security rules in daily works.

Education should include below items, but not limited to:

- To make the staff be matured for understanding about security.
- To make the staff to aware of the threats and influence to production control system correctly.
- To make the staff to implement security countermeasures and improvement adequately.
- To make the staff to operate the system correctly and manage it tidily. For example, make the staff to understand how to confirm the log to identify the existence of an attack to the system.

The education should be done on these occasions.

- When the staffs are employed
- When the staffs are moved to a new position or the accessed targets of the staffs are changed, an so on

4.9.2 Training

The first purpose of training is to enable the staff to perform the right operation and management so that to prevent the security incidents. Another purpose of the training is to make the stuffs to respond properly on the security incidents, and to make them capable to cope with such occasions. It is also important to make the staff in readiness over incidents.

The procedure in detail is provided in the Business Continuity Plan described in Chapter 6. It is necessary to regularly train the stuffs under the assumed the security incidents for taking the right actions.

5. Physical Protection

To obtain the physical security for a control room where the system is located is a very important element in decreasing the threats of security.

5.1 Define Physical Boundary

The control room where the system is located should be regarded as a security area and physical security must be defined. The secured area is an area protected the barriers.

The barriers here also include the management of the ID cards, the code numbers and the keys for entering the secured rooms. More than one security area can be defined according to the level of security required. Security areas have effects as follows, but not limited to:

- To prevent an unauthorized equipment be connected to the network.
- To prevent the loss of equipments such as PC or backup medias be stolen.

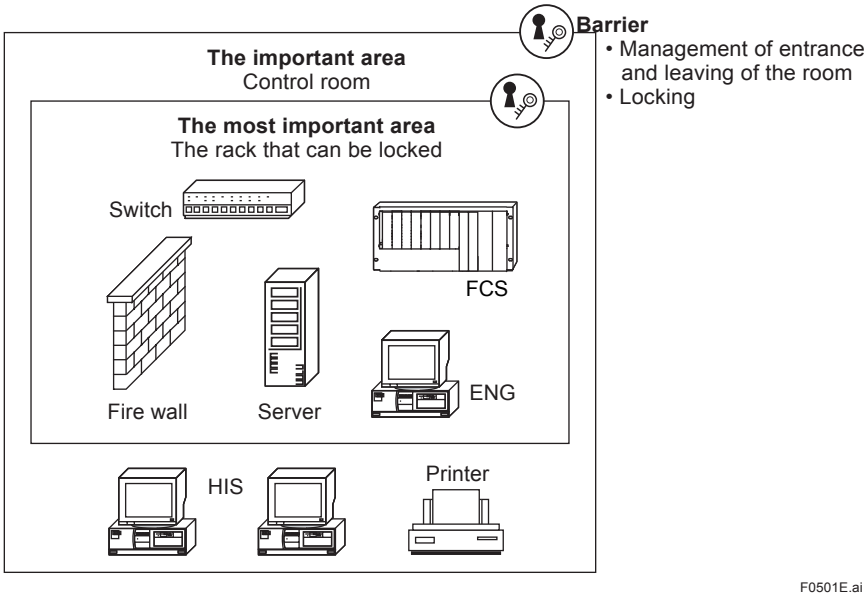


Figure Example of the configuration of security area

Moreover, PC components such as HIS and ENG should be placed in the security area by following reasons.

- To eliminate the opportunity of illegal usage.
- To prevent from installing the tool for stealing information, such as Key Logger.
- To keep the entrance and leaving records and the records can be used as forensic evidences.

Important areas

The control room where the operators operate the devices to control plant every day is considered to be an important area. The devices necessary for the operations are placed here. Only a limited number of people, i.e. operators and engineers should be allowed to enter this area.

Example of devices should be placed in the important area

- Operator stations (HIS etc.)
- Printers

Printer should be placed in the important area to secure the confidentiality of printouts.

The most important area

The important devices are placed in this area, where the devices are not necessarily operated for the daily operations. For an example, the racks that can be locked should be placed in this area. Entering to this area should be strictly controlled so that only a small number of people such as engineers are allowed.

Example: The devices that should be placed in the most important area

- Controllers including the wirings to the devices (FCS,FCJ/FCN,SCS)
- Engineering stations (ENG)
- Network devices (Switches and Gateway Units)
- Security devices (Firewalls)
- Spare equipments such as the PCs.

Example: The media that should be placed in the most important area

- Media used for installing system software to PC.
- Backup media

5.2 Management of Removable Devices

The removable devices such as CD/DVDs, floppy disks or USB memory sticks are not needed in the daily plant operation. It is dangerous to keep them in the freely accessible environment, for there may be the possibility that the files infected by computer viruses or illegal programmes are installed. Thus, it is very important to prevent the removable devices from being used illegally.

We recommend the following measures.

Disabling AutoRun

Windows has a function that automatically runs programs from atached removable drives.

Disable the AutoRun function to prevent virus infection due to misuse of AutoRun.

Disabling the removable devices

Disable the floppy disks, CD/DVD drives and USB devices in the control room. In this case, it is necessary to strictly protect the BIOS settings from the outsiders by authenticating the password and the administrator privilege.

Detaching removable drives

Consider to physically detach removable drives if it does not trouble the operating environment.

Handling USB memory sticks

IMPORTANT

USB memory sticks are widely used as external storage devices due to their large capacity, low price, and easy usage. However, USB worms or virus infection from USB memory sticks have become a very common problem.

Therefore, we need to control the usage of USB memory sticks in production control systems. This can be done by building a stringent management system that restricts the usage of USB memory sticks to limited devices, and enforces absolute compliance to regulations.

5.3 Third Party Maintenance

Some maintenance works of security devices such as PCS or Network devices, the maintenance workers of the third party vendors need to work in the important area or the most important area. Since these works are carried out to the critical devices, it is essential to guarantee the security.

The maintenance works should be carried out in the presence of the user all the time, and the user must check if the third-party maintenance works are properly performed in accordance with the work procedures.

6. Business Continuity Plan

Business continuity plan is explained here.

Since a high level of availability is required for the production system, it is important to decide the business continuity plan in advance. And make sure that the plan, including the training programs, would guarantee the system be properly restored in case an incident happened.

6.1 Plan

When creating a business continuity plan, the following has to be taken into consideration.

Recovery plan

Disaster recovery plan should be made to secure the recovery of the system on an incident. The plan should include the roles and responsibilities of the departments, persons in charge and their contact information. The plan should also include activities of restoration to deal with the confusions and obstacles occurred by the incident.

Acceptable time for restoration

Decide how much time will be required for backup and restore and if redundancy is necessary.

Backup interval

Keep a number of backups to prepare for unexpected incidents such as corrupted storage mediums.

Backup objects

Backup should contain the following three objects.

- Operating system and other system software.
- Application software
- Application parameters. The parameters tailored by the process engineer. For example, Tuning Parameter of CENTUM VP.

Backup management

Keep a number of backups to prepare for unexpected incidents such as corrupted storage mediums.

Storage location of backup media

Keep the backup media in a safe place such as a cabinet that can be locked so that the security is guaranteed. This is required because if the backup information is passed to an attacker, the possibility of cyber attack will be largely increased.

TIP

Yokogawa system products provide tools for efficiently backups.

Clarification of responsibility

It is necessary to make clear what department or who is responsible for the activities in the business continuity plan.

- Backup activity
- Training activity
- Restore activity

Review and update the plan

When the system configuration or the system environment changes, it is necessary to review and update the business continuity plan.

Review and update the plan is required when:

- the new devices are installed,
- the system is upgraded,
- the location of the equipment is changed,
- the business is expanded or changed.

6.2 Training

It is necessary to conduct regular trainings in accordance with the business continuity plan so that in case of emergency, the system can be certainly restored.

It is also essential for the staffs in charge of each activity in the business continuity plan to take part in these trainings.

Not only internal education but also external institution training and public qualification acquisition should be planned. For example, it is necessary to take measures to encourage acquisition of GICSP (Global Industrial Cyber Security Professional), which is international certification for security measures engineering of control systems.

- Global Industrial Cyber Security Professional (GICSP)

  https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

Yokogawa trains engineers with GICSP qualifications.

- Yokogawa Promotes GICSP Training to Enhance Plant Safety

  http://www.yokogawa.com/pr/topics/2015/pr-topics-2015-0508-02-en.htm

6.3 Maintenance

Security measures should not be done once at installation. Daily new vulnerabilities are discovered, and the threat to the control system is increasing. It is necessary to always execute PDCA cycle (plan-do-check-act cycle) for security measures.

Yokogawa prepares the following security countermeasure service and support the continuous operation of IA control system.

(1) AV/OS(*1) Implementation Service

(2) AV/OS(*1) Update Service

(3) Security Information Service

(4) Virus Check Service

(5) Software Backup Service

(6) USB Port Lock Service

(7) Malware Inactivated Service

(8) Security Effectiveness Service

*1: Antivirus software / Microsoft Security Updates

SEE ALSO For details of the above services, please refer to:

Endpoint Security Service (GS 43D02T30-02EN)

6.4 Measures against Software Vulnerability

Vulnerability of software is defined as “a security flaw in a software product or other item that may be attacked by computer viruses or unauthorized access to cause damage to its function or performance.”

Vulnerability and software defect are often confused with each other, and many causes of the vulnerabilities are, in fact, defects. However, vulnerabilities are different from the defects that cause system hang-up or other failures in usual operation by customers. Vulnerability is a potential risk under the usual operation environment of customers, which causes incidents such as system hang-up only after being attacked. From the viewpoint of preventing security incidents, vulnerability must be handled while it is in the state of potential risk.

Yokogawa makes every effort to collect the latest vulnerability information, feed it back to the operations, and makes use of it for improving development processes, operation standards and operating procedures. Yokogawa offers customers not only secure products but also support regarding vulnerability through providing measures and workarounds for vulnerabilities based on the latest information.

- Yokogawa Security Advisory Report List

  https://www.yokogawa.com/library/resources/white-papers/yokogawa-security-advisory-report-list/

- Yokogawa Innovative Plant Automation Security Solutions

  https://www.yokogawa.com/library/resources/white-papers/yokogawa-innovative-plant-automation-security-solutions/

Blank Page

Revision Information

Title: Security Standard of System Product
Manual No.: TI 33Y01B30-01E

Sep. 2006/1st Edition
Newly published

Apr. 2008/ 2nd Edition

Introduction	B/M 9000CS addition to Target Products.
4.2.7	Deleted a description of the Secure Ticket of Personal authentication.

Sep. 2008/3rd Edition

Introduction	CENTUM VP added to Target Products
1	Figure Outline of the system revised
2	Some items added to Examples of data assets
	TIP ISA 99.00.01 added
	TIP Activity-based criteria and Asset-based criteria added
3.4	Examples of the vulnerability revised and some items added
3.5	Risk Assessment revised
	Formula showing Risk revised
3.6	The title is revised to “Design and Implement of the Measures”
	Priority of Availability, Integrity and Confidentiality added
3.8	Description of health, safety, environment added
	Monitoring log of network added to Daily monitoring of the system
	Software in use added to Regular auditing
4.1	Risk Definition and Security Zone added
4.2.1	Level of ISA 99.00.01 Reference Model descriptions added
	Description of IPS revised at Horizontal segmentation
	SEE ALSO 4.6.2 IPS added
4.2.2	Figure Equipment class revised
	Description of classification added
4.2.4	Description of Dual-Home Server revised
4.2.5	Title is changed from “Vnet/IP Open Channel” to “OPC Interface”, and all contents are revised
4.2.6	Description added at Authentication of terminals
4.2.7	Figure Example of the configuration of remote monitoring network revised
	Figure Example of Personal Authentication revised
4.2.8	Description added at Use of RAS, Authentication by using the caller ID and The system-hardening of RAS
	Figure Example of the configuration of remote maintenance by Modem revised
4.4	Security Patches Management revised
4.8.1	The title is changed to “CENTUM VP/CS3000”
	CENTUM VP security description added
4.8.2	Revised “4.8.3 ProSafe-RS” to “4.8.2 ProSafe-RS”
	ProSafe-RS security description revised
4.8.3	Revised “4.8.2 STARDOM” to “4.8.3 STARDOM”
4.8.5	Exaquantum security description revised
4.8.6	Exapilot security description revised
4.9.1	Education revised
4.9.2	Training revised
5.1	Define Physical Boundary revised
6.1	Recovery plan and Backup objects added

Feb. 2011/4th Edition

Introduction	Deleted “R3” from “CENTUM CS 3000 R3” in Target Products
	Deleted the sentence of “CENTUM CS 1000 R3” from Target Products
	Changed “B/M9000 CS” to “B/M9000 VP” in Target Products
	Added “-Based Software” between “Solution” and “Packages”
1	Changed “Security Patches” to “Security Patch” in Figures
	Changed “Public Server” to “DMZ Server” in Figures

4.2.6	Added a lead sentence for this section Added the 1st headline “Wireless LAN (IEEE 802.11)” Changed “wireless network” to “wireless LAN” in the text Changed the 2nd headline “Application to control bus” to “Wireless application to control bus” Added the 3rd headline “Field wireless (ISA 100.11a)” and its description
4.4	Changed “Patches” to “Patch” in the title Added SEE ALSO about security patches
4.7	Changed the title “Configuration of Windows Domain” to “Windows Domain Management” Added a lead sentence and TIP Added the headline “Windows domain configuration for an office environment” Added the headline “Windows domain management in the production control system” and its description
4.8	Changed the title “Security Functions Specific to Each Product” to “Security Function of Yokogawa System Products” Added the headline “Security of System Products” and its description
4.8.1	Changed the description for the authentication mode of CENTUM VP R4.03
4.8.3	Changed “CENTUM CS 3000” to “CENTUM VP/CS 3000”
4.8.4	Added a lead sentence for this section Added the 1st headline “IT security function” and its description Added the 2nd headline “PRM specific security function” Changed “operators” to “users” in the text
4.8.5	Added the chapter “B/M9000 VP” Added 1 to chapter numbers after this chapter
4.8.7	Added a lead sentence for this section Added the 1st headline “IT security function” and its description Added the 2nd headline “Exapilot specific security function”
5.2	Added the headline “Disabling AutoRun” and its description Added the subheading “Handling USB memory sticks” and its description Changed “CD” to “CD/DVD” Changed “the removable devices” to “removable drives”
6.1	Changed “CENTUM is provided with the” to “Yokogawa system products provide” Corrected grammatical errors, usage and wording (Chapter 1, 4.2, 4.2.1, 4.2.2, 4.2.3, 4.2.5, 4.2.6, 5.1, 6)

June 2013/5th Edition

2	Added a description about the recent security threats
4.3	Added a description about antivirus software
4.4	Added a description about applying security patches
4.5.1	Deleted the description about the old security holes

Apr. 2018/6th Edition

All	Deleted descriptions about CS 3000
1	Changed the explanation about chapter 3
3	Reformed chapter 3 in its entirely (Changed “ISMS” to “Security Standards and Certifications”)
4.3	Changed the title of this chapter to “Anti-malware”, and added Whitelisting software
4.6.2	Added “IDS”
4.6.3	Added the whole chapter of “NMS”
4.8	Added the description about IT security version 2.0
4.8	Added and/or changed the descriptions in accordance with the latest version of the products
4.8.6	Added the whole chapter of “Exaopc”
4.8.9	Added the whole chapter of “Exaplog”
6.3	Added the whole chapter of “Maintenance”
6.4	Added the whole chapter of “Measures against Software Vulnerability”

Nov. 2019/7th Edition

All	Change “security patches” to “Security Updates”.
All	Change “pattern” to “virus definition file”.
3.2	Delete a description regarding CSMS certification.
3.3	Update a description regarding NIST Cybersecurity Framework.
3.4	Update a description regarding ISASecure.
3.5	Update a description regarding ISA99.

3.6 Update a description regarding IEC62443.
4.3 Change referenced document to Endpoint Security Service.
4.8.1 Add a description regarding Athentication mode.
4.8.10 Add a description regarding FAST/TOOLS.

Written by Yokogawa Electric Corporation

Published by Yokogawa Electric Corporation
2-9-32 Nakacho, Musashino-shi, Tokyo 180-8750, JAPAN