OMRON

Security Guideline for CS/CJ/CP-series CPU Unit

P176-E1-01

NOTE

- This document does not provide detailed instructions for use, including safety precautions. Be sure to obtain the manuals and operating instructions for each device listed in this document and confirm their contents, including *Safety Precautions*, *Precautions for Safe Use*, and *Precautions for Correct Use* and other safety precautions before use.
-
- No patent liability is assumed with respect to the use of the information contained herein. Moreover, because OMRON is constantly striving to improve its high-quality products, the information contained in this guide is subject to change without notice.
- Every precaution has been taken in the preparation of this document. Nevertheless, OMRON assumes no responsibility for errors or omissions.

Trademarks

- Sysmac and SYSMAC are trademarks or registered trademarks of OMRON Corporation in Japan and other countries for OMRON factory automation products.
- CX-One is a registered trademark for Programming Software made by OMRON Corporation.
- Microsoft, Windows, Excel, Visual Basic, and Microsoft Edge are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.
- ODVA, CIP, CompoNet, DeviceNet, and EtherNet/IP are trademarks of ODVA.
- The SD and SDHC logos are trademarks of SD-3C, LLC.

Other company names and product names in this document are the trademarks or registered trademarks of their respective companies.

Copyrights

- Microsoft product screen shots used with permission from Microsoft.

Introduction

Purpose of This Document

The purpose of this document is to provide you with an understanding of security initiatives of OMRON on its FA products and propose the security measures that the users of the FA products should take on their own. It describes the security measures that you can implement using a CS/CJ/CP-series CPU Unit and a CS/CJ-series EtherNet/IP Unit.
Please read this document together with the Security Guideline for Factory Automation System and related manuals.

Intended Audience

This document is intended for the following people who plan, examine, and implement security measures.

- Personnel in charge of introducing FA systems.
- Personnel in charge of designing FA systems.
- Personnel in charge of installing and maintaining FA systems.
- Personnel in charge of managing FA systems and facilities.

Applicable Products

This document covers the following products.

- CS-series CPU Units
- CJ-series CPU Units
- CP-series CPU Units

Refer to the user’s manual for each product for product specifications.

Disclaimer

The recommendations we make to our customers in this document are based on the results of our analysis and study.
Appropriate security measures vary with customer environment, so these recommendations do not guarantee prevention of all security breaches in customer environments.
Referring to this document, please consider and implement analysis and appropriate countermeasures in line with the customer’s environment on your own.

Sections in this Guideline

CONTENTS

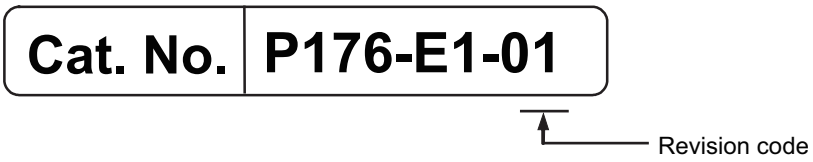
Related Guideline and Manuals

The followings are the guideline and manuals related to this document. Read them for reference.

Document name	No.	Application
Security Guideline for Factory Automation System	P162	Learning the concept of security for FA systems in general.
SYSMAC CS Series CS1G/H-CPU□□H Programmable Controllers OPERATION MANUAL	W339	Learning the details and usage of security functions provided in CS-series CS1G/H CPU Units.
SYSMAC CS Series CS1D Duplex System OPERATION MANUAL	W405	Learning the details and usage of security functions provided in CS-series CS1D CPU Units.
SYSMAC CJ Series CJ2 CPU Unit Software USER'S MANUAL	W473	Learning the details and usage of security functions provided in CJ-series CJ2 CPU Units.
SYSMAC CP Series CP2E CPU Unit Software USER'S MANUAL	W614	Learning the details and usage of security functions provided in CP-series CP2E CPU Units.
SYSMAC CP Series CP1H CPU Unit OPERATION MANUAL	W450	Learning the details and usage of security functions provided in CP-series CP1H CPU Units.
SYSMAC CP Series CP1L CPU Unit OPERATION MANUAL	W462	Learning the details and usage of security functions provided in CP-series CP1L CPU Units.
SYSMAC CP Series CP1E CPU Unit Software USER'S MANUAL	W480	Learning the details and usage of security functions provided in CP-series CP1E CPU Units.
SYSMAC CS and CJ Series EtherNet/IP Units OPERATION MANUAL	W465	Learning the details and usage of security functions provided in CS/CJ-series EtherNet/IP Units.
SYSMAC CX-One FA Integrated Tool Package Setup Manual	W463	Learning the details and usage of functions provided in the FA Integrated Tool Package CX-One Ver. 4.□.
SYSMAC CX-Programmer Ver. 9.□ Operation Manual	W446	Learning the details and usage of functions provided in the CX-Programmer Ver. 9.□.

Revision History

A revision code appears as a suffix to the catalog number on the front and back covers of this document.



Revision code	Date	Revised content
01	March 2026	Original production

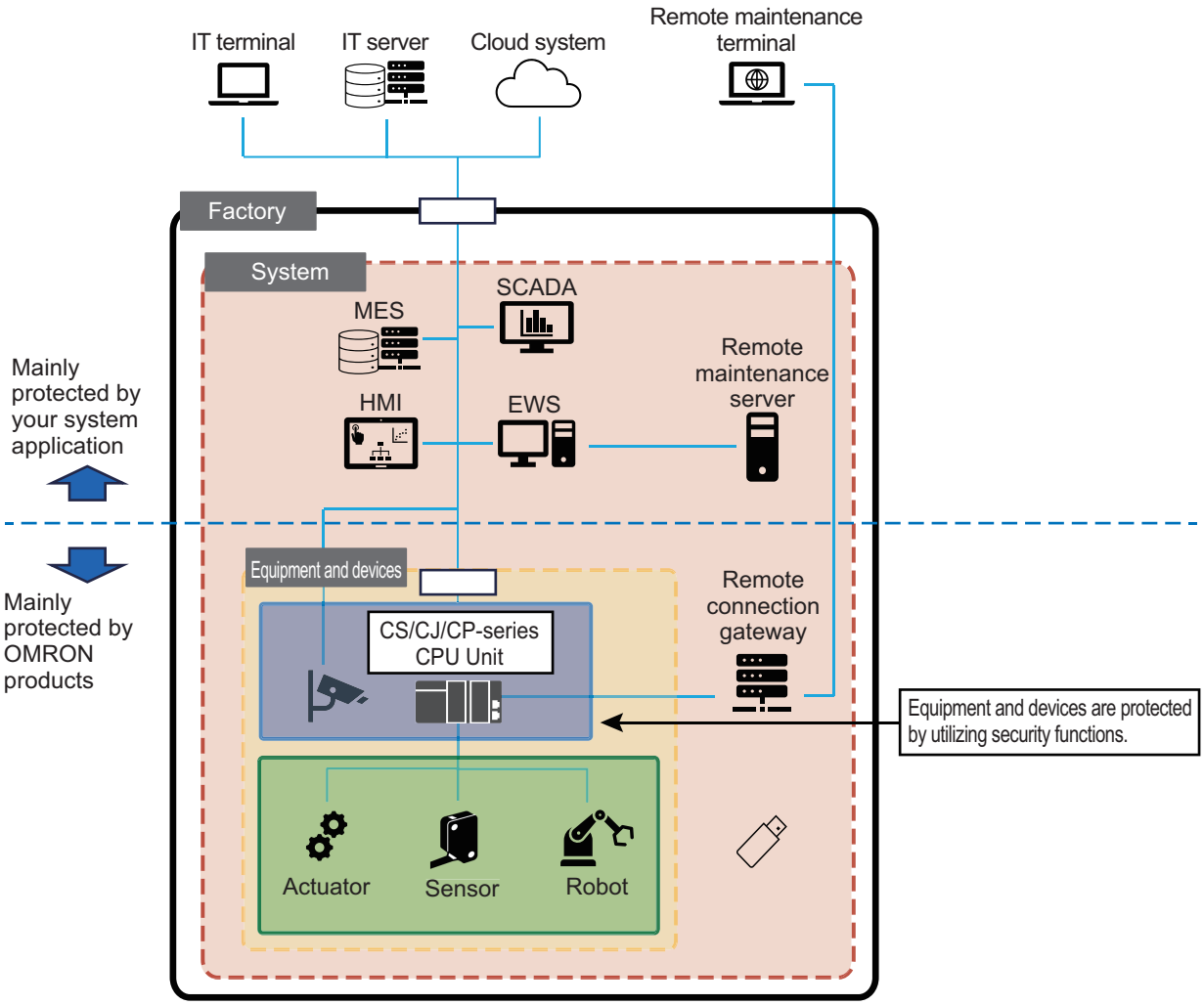
1

Defense in Depth in the Technical Layer

CS/CJ/CP-series CPU Units and CS/CJ-series EtherNet/IP Units provide multiple security functions to achieve Defense in Depth in the technical layer.
This section describes the Defense in Depth in the technical layer that the security functions of CS/CJ/CP-series CPU Units and CS/CJ-series EtherNet/IP Units provide.

1-1 Protecting Equipment and Devices with Defense in Depth

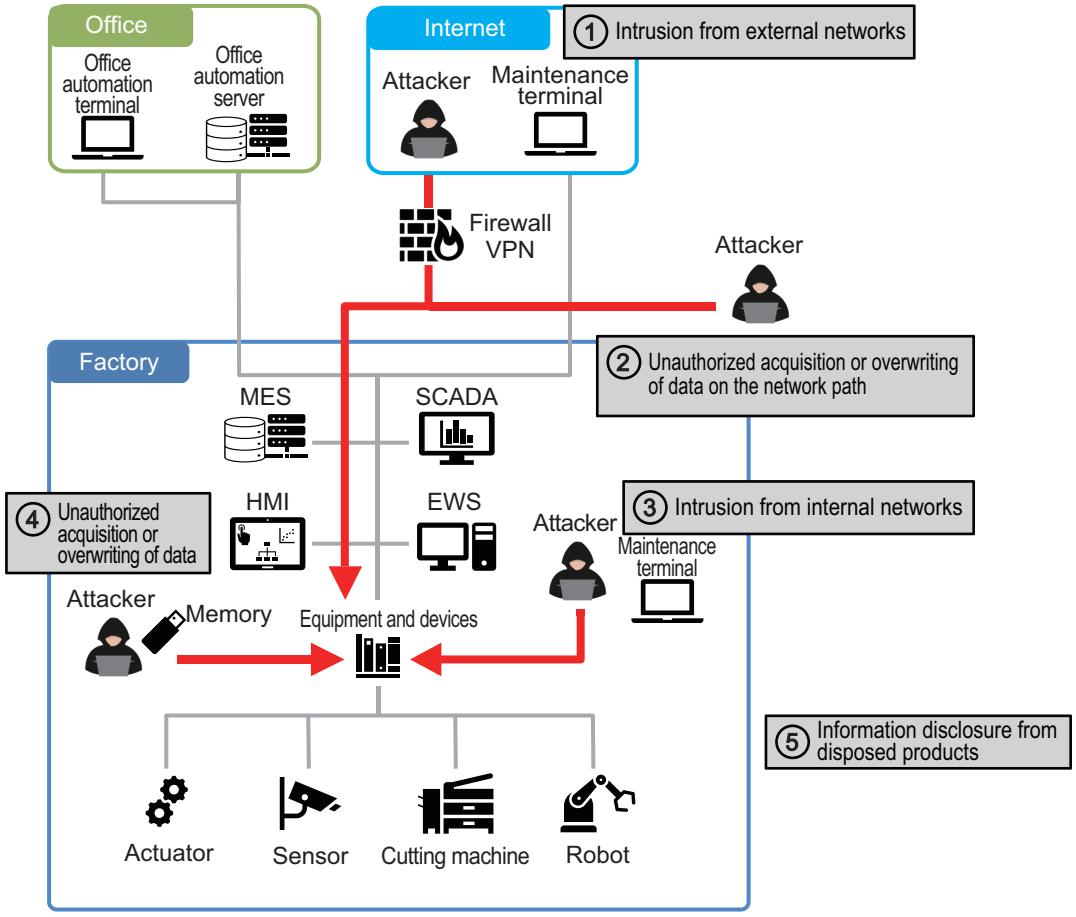
Defense in Depth is the basic concept for security measures. In this concept, security measures are implemented for each layer.
The factory layer typically establishes security policies and protects equipment and devices through operations (in the human/process and physical layers).
The system layer protects equipment and devices across the entire system while covering operational aspects. It also implements measures for the network, including communications access control, filtering, and firewalls. Measures up to this point should be implemented mainly by your system and application.
Equipment and devices effectively utilize the security functions that they provide to protect their operations and assets.



1-2 Threats to Equipment and Devices

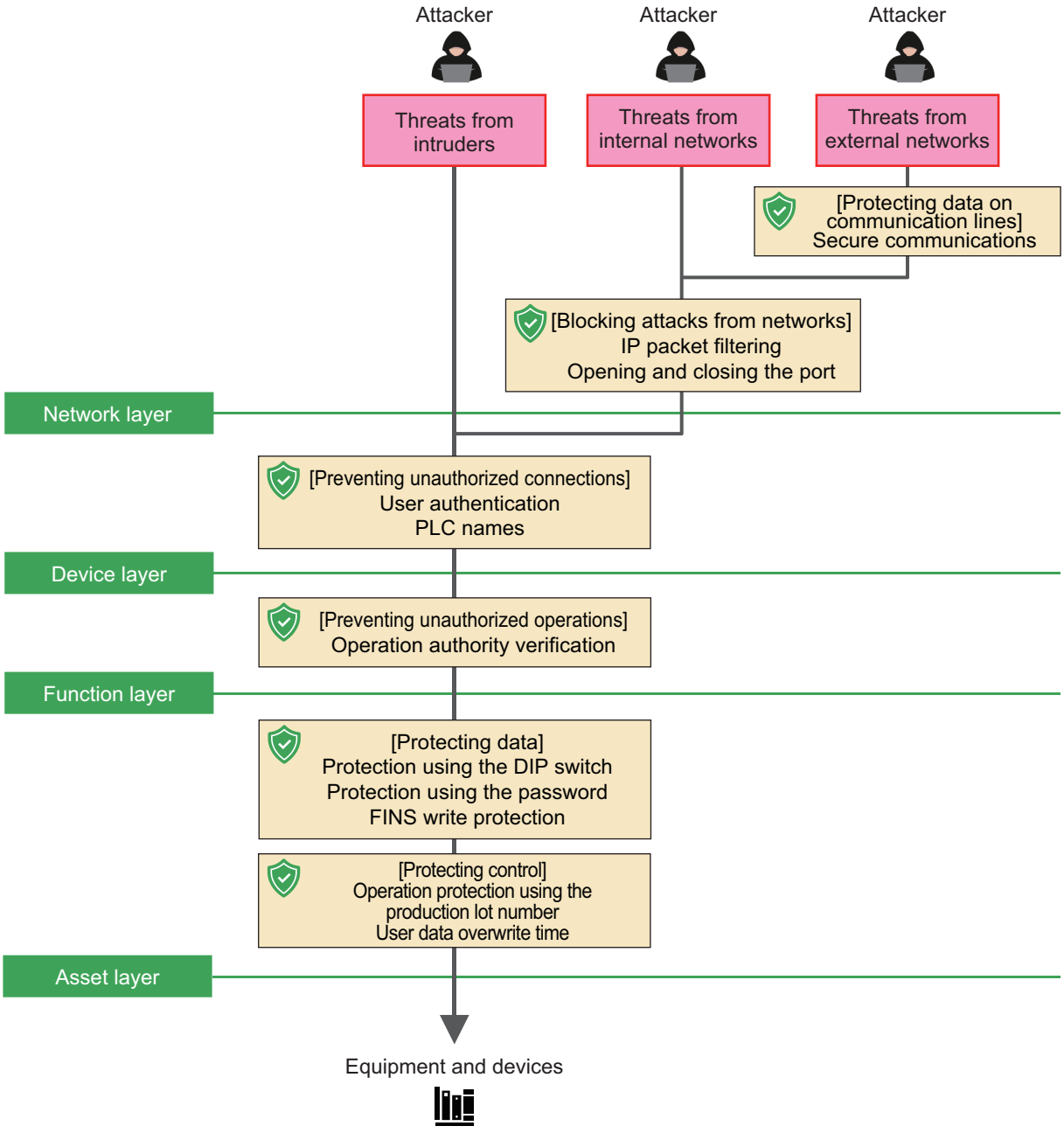
Threats to equipment and devices include not only attacks from external and internal networks, but also attacks by intruders entering the factory premises and disclosure of assets through disposed products.

Attack vectors



1-3 Security Functions to Protect Equipment and Devices from Threats

Even if an attacker could break through one layer, security functions in layers closer to equipment and devices can protect the assets. Depending on the purpose and the type of threat, provide Defense in Depth by combining the measures described in the *Security Guideline for Factory Automation System (Cat. No. P162)* and the multiple security functions described in this document.



The table below lists the functions provided in each layer.

Layer to protect equipment and devices	Purpose	Function provided by OMRON products	Reference
Network layer	Protecting data on communication lines	Secure communications	*2-1-1 Secure Communications* on page 2-2
	Blocking attacks from networks	IP packet filtering	*2-2-1 IP Packet Filtering* on page 2-4
		Opening and closing the port	*2-2-2 Opening and Closing the Port* on page 2-5
Device layer	Preventing unauthorized connections	User authentication	*2-3-1 User Authentication* on page 2-8
		PLC names	*2-3-2 PLC Names* on page 2-9
Function layer	Preventing unauthorized operations	Operation authority verification	*2-4-1 Operation Authority Verification* on page 2-11
Asset layer	Protecting data	Write protection using the DIP switch	*2-5-1 Write Protection Using the DIP Switch* on page 2-12
		Read protection using a password	*2-5-2 Read Protection Using a Password* on page 2-14
		FINS write protection	*2-5-3 FINS Write Protection* on page 2-14
	Protecting control	Operation protection using the production lot number	*2-5-4 Operation Protection Using the Production Lot Number* on page 2-15
		User data overwrite time	*2-5-5 User Data Overwrite Time* on page 2-16
Common to all layers	Preventing repudiation	Operation log	*2-6-1 Operation Log* on page 2-18

1-4 Secure Network Connection Using CS1W/CJ1W-EIP21S

The CS/CJ-series CS1W/CJ1W-EIP21S EtherNet/IP Unit provides a variety of security functions to achieve secure network connections with CS/CJ/CP-series CPU Units. This enables enhanced security in controlling programs and data as well as equipment and devices for access to these CPU Units via the network. Be sure to combine the CS1W/CJ1W-EIP21S EtherNet/IP Unit with your CPU Unit to build Defense in Depth depending on the purpose and the type of threats.

Note that the CS/CJ-series CS1W/CJ1W-EIP21 EtherNet/IP Unit, and CS/CJ-series CJ2H-CPU6□-EIP and CJ2M-CPU3□ CPU Units with built-in EtherNet/IP ports, do not provide security functions. This means that you must replace the EtherNet/IP Unit or use the CPU Units with the CS/CJ-series CS1W/CJ1W-EIP21S EtherNet/IP Unit to enhance the security of your equipment and devices.

Example Combinations of CPU Units and the EtherNet/IP Unit

CJ2H CPU Unit　CJ2M CPU Unit　CJ1W-EIP21S

CJ2 CPU Unit + CJ EtherNet/IP Unit

CS1D CPU Unit　CS1W-EIP21S

CS1D CPU Unit + CS EtherNet/IP Unit

1-5 Security Functions Available with Each CPU Unit

This section describes the security functions available when you use a CS/CJ/CP-series CPU Unit standalone or in combination with a CS/CJ-series EtherNet/IP Unit.

1-5-1 CS/CJ-series CPU Unit

The security functions available with a CS/CJ-series CPU Unit are as follows.

Security function provided by OMRON products	CS-series CPU Unit	CJ-series CPU Unit
Secure communications	Available in combination with CS1W-EIP21S	Available in combination with CJ1W-EIP21S
IP packet filtering	Available in combination with CS1W-EIP21S	Available in combination with CJ1W-EIP21S
Opening and closing the port	Available in combination with CS1W-EIP21S	Available in combination with CJ1W-EIP21S
User authentication	Available in combination with CS1W-EIP21S	Available in combination with CJ1W-EIP21S
PLC names	---	Available with CPU Unit only
Operation authority verification	Available in combination with CS1W-EIP21S	Available in combination with CJ1W-EIP21S
Write protection using the DIP switch	Available with CPU Unit only	Available with CPU Unit only
Read protection using a password	Available with CPU Unit only	Available with CPU Unit only
FINS write protection	Available with CPU Unit only	Available with CPU Unit only
Operation protection using the production lot number	Available with CPU Unit only	Available with CPU Unit only
Operation log	Available in combination with CS1W-EIP21S	Available in combination with CJ1W-EIP21S

1-5-2 CP-series CPU Unit

The security functions available with a CP-series CPU Unit are as follows.

Security function provided by OMRON products	CP-series CPU Unit			
	CP1H CPU Unit	CP1L CPU Unit	CP1E CPU Unit	CP2E CPU Unit
Secure communications	---	---	---	---
IP packet filtering	Available in combination with CJ1W-EIP21S	---	---	---
Opening and closing the port	Available in combination with CJ1W-EIP21S	---	---	---
User authentication	---	---	---	---
PLC names	---	---	---	---
Operation authority verification	---	---	---	---
Write protection using the DIP switch	Available with CPU Unit only	Available with CPU Unit only	---	---
Read protection using a password	Available with CPU Unit only	Available with CPU Unit only	Available with CPU Unit only	Available with CPU Unit only
FINS write protection	Available with CPU Unit only	---	---	---
Operation protection using the production lot number	Available with CPU Unit only	Available with CPU Unit only	Available with CPU Unit only	Available with CPU Unit only
Operation log	---	---	---	---

1-6 Things That You Should Do

The table below shows the things that you should do for each layer.

Layer to protect equipment and devices	Purpose	Things that you should do
Network layer	Protecting data on communication lines	• To improve security, install and use CX-One on an OS that is within the support period of Microsoft Windows. • For networks of control systems and equipment, install a firewall (blocking unused communications ports and restricting communications hosts) to isolate them from IT networks. Make sure that CX-One is connected to the control systems inside the firewall. • If you need remote access from CX-One to control systems and equipment, use a virtual private network (VPN), virtual desktop infrastructure (VDI), or other system with excellent security. • To read or write files on an SD Memory Card inserted into the Controller or files in the EM File Memory from FTP client software, take the following measures. a) To prevent the Controller from communicating with devices prepared by attackers, install the partner devices in a secure area. b) Use IP filtering or a user system (firewall, etc.) to limit the partner devices that can be connected.
	Blocking attacks from networks	• Use the function in combination with other measures, such as installing a firewall to prevent unauthorized packets from reaching the Controller or closing unused ports to prevent the Controller from accepting unauthorized packets. • For the IP packet filter, register all devices and conditions to permit packet reception. • The FINS protocol specifications do not define encrypted communications. This means that FINS messages on the communications path can be easily intercepted because they are sent and received in plain text. In addition, it is not possible to detect tampering with FINS messages. To reduce the risk that FINS protocol's vulnerabilities can be exploited, take measures such as disabling FINS or preventing unauthorized access by using the packet filter function. When you use the FINS protocol, use your application to ensure security. • Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks. FTP does not have password lock functionality. If password lock functionality is required, disable the FTP function. • Change your password by yourself on a periodic basis. • Use this function in combination with other measures, such as installing a firewall to prevent unauthorized packets from reaching the Controller or using the packet filter to prevent the Controller from accepting unauthorized packets.
Device layer	Preventing unauthorized connections	• Consider the following points when you use user authentication. a) Change your password by yourself on a periodic basis. b) Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
Function layer	Preventing unauthorized operations	• Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks. • Change your password by yourself on a periodic basis.

Layer to protect equipment and devices	Purpose	Things that you should do
Asset layer	Protecting data	• Consider the following points when you use read protection using a password. a) To improve security, install and use CX-One on an OS that is within the support period of Microsoft Windows. b) Set and manage your password appropriately to prevent unauthorized utilization by others. c) Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks. d) Change your password by yourself on a periodic basis.
	Protecting control	---

2

Security Functions

This section describes the security functions provided in CS/CJ/CP-series CPU Units and CS/CJ-series EtherNet/IP Units.

2-1 Protecting Data on Communication Lines

Equipment connected to the Internet is subject to the risk of cyberattacks over the network. Use the following functions to prevent information disclosure from data flowing over communication lines, tampering, and denial of service.

2-1-1 Secure Communications

This function aims to ensure the confidentiality and integrity of communication lines that are used to access critical data in a CPU Unit from Support Software.
Since it encrypts and then adds hash values to communications data before sending and receiving, it is useful to prevent eavesdropping and tampering by a third party.
Refer to the *SYSMAC CS/CJ-series EtherNet/IP Units Operation Manual (Cat. No. W465)* for details on secure communications.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes		Yes	Yes	

Things That You Should Do

- Use this function by combining the CPU Unit with your EtherNet/IP Unit.
- To use secure communications, save the user authentication settings to the EtherNet/IP Unit in advance using the EIP21S User Management Tool.
- Secure communications may affect the communications response performance and the execution processing performance of some instructions. When you use secure communications, check the operation sufficiently in advance.
- The secure communications function is intended for applications where the Support Software is connected to the CPU Unit via an unreliable network such as Internet connections. This means that you cannot use secure communications when connecting the Support Software to the CPU Unit via a USB or peripheral port. Be sure to connect the Support Software to the CPU Unit from the EtherNet/IP Unit.

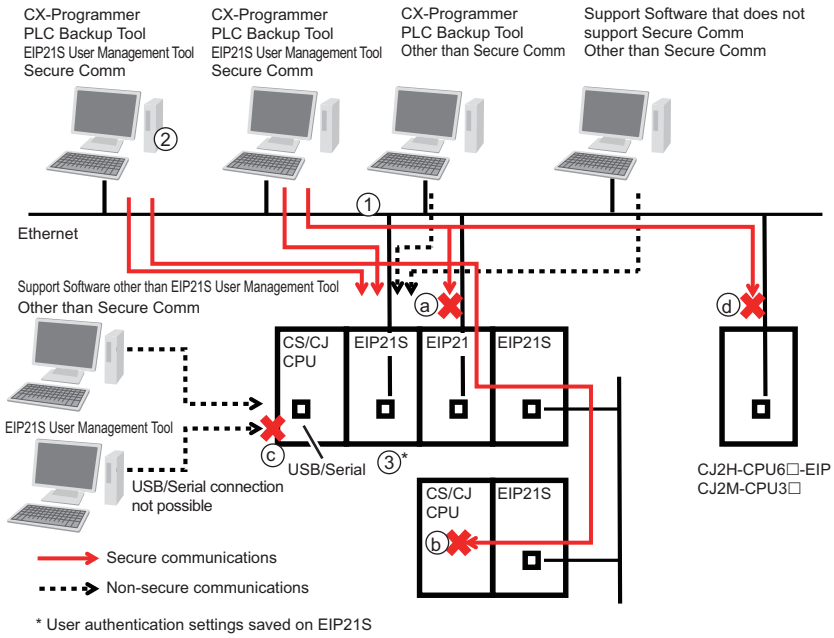
Conditions for Secure Communications

- Secure communications are possible when all of the following conditions are met.
  1. The Ethernet network to which the connected EtherNet/IP Unit belongs is used.
  2. One of the following Support Software is used to make connection settings for secure communications.
     - CX-Programmer
     - PLC Backup Tool

- EIP21S User Management Tool

3. User authentication settings are stored in the connected EtherNet/IP Unit.

- The following are examples where secure communications are not possible.
  a) The connection destination is an EtherNet/IP Unit or Ethernet Unit other than the CS1W/CJ1W-EIP21S EtherNet/IP Unit.
  b) The connection destination is located in a different network (beyond the allowable level of transparency).
  c) The connection destination has a USB, peripheral, or serial port.
  d) The connection destination is a CJ2H-CPU6□-EIP/CJ2M-CPU3□ CPU Unit with a built-in EtherNet/IP port, a CP1W-CIF41 Ethernet Option Board mounted on a CP-series CPU Unit, or a CJ1W-EIP21S EtherNet/IP Unit mounted on a CP (CP1H)-series CPU Unit.



2-2 Blocking Attacks on the CPU Unit from Networks

Equipment connected to the Internet is subject to the risk of cyberattacks over the network. Block both external and internal attacks to prevent malfunctions of production equipment and accidents.

2-2-1 IP Packet Filtering

IP packet filtering selectively permits packets that EtherNet/IP ports receive to pass through the filter according to the pre-defined conditions.
Use it to prohibit connections from unauthorized nodes, such as PCs brought into the site without permission.
This improves the security performance of the system.
Refer to the *SYSMAC CS/CJ-series EtherNet/IP Units Operation Manual (Cat. No. W465)* for details on IP packet filtering.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes		Yes	Yes	

Things That You Should Do

- Use this function by combining the CPU Unit with your EtherNet/IP Unit.
- Enabling the IP packet filter settings prevents the CPU Unit from communicating with devices via the filter target EtherNet/IP port. Be careful of the settings.
- The settings in the IP packet filter table are retained when you change from **Use IP Packet Filter** to **Not use IP Packet Filter** in the CX-Programmer. The settings in the IP packet filter table are transferred to the EtherNet/IP Unit regardless of the setting of whether or not to use the function.
- IP packet filtering supports stateful inspection. Therefore, when making a request to the partner device as a client, the EtherNet/IP Unit can receive responses from the partner without filter conditions added to the IP packet filter table. The protocols supported by stateful inspection are TCP, UDP, and ICMP.

Note

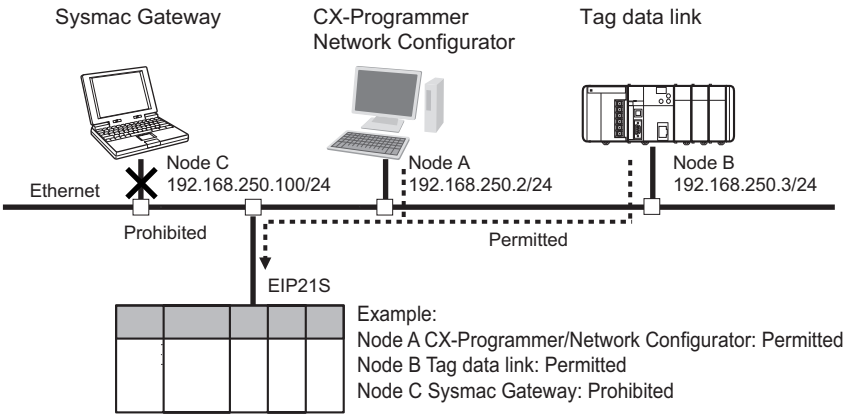
IP packet filtering does not apply to the following function. It is a client function that opens ports during use and closes them at completion.

- DNS/SNT

Application Example: Permitting Packet Reception from a Specific Source IP Address

● Configuration

This configuration permits only communications from specific PCs and external devices, and prohibits communications from other client devices.



● Settings for This Configuration

Make the settings in the **IP Packet Filter Setting** dialog box as shown in the following table.
Set the IP addresses of nodes A and B individually. Therefore, set *255.255.255.255* as the mask.

No.	IP filter		
	Source settings		
	Setting method	IP address	Mask
1	IP address specification	192.168.250.2	255.255.255.255
2	IP address specification	192.168.250.3	255.255.255.255

Register the IP addresses of all external devices to use because communications from IP addresses that are not registered in the IP Packet Filter Setting dialog box are blocked.

If you set the mask to other than 255.255.255.255, communications from multiple IP addresses will be permitted.
For example, the settings below permit communications from devices with IP addresses between 192.168.250.0 and 192.168.250.255.

No.	IP filter		
	Source settings		
	Setting method	IP address	Mask
1	IP address specification	192.168.250.0	255.255.255.0

2-2-2 Opening and Closing the Port

Opening and closing the port is a function that blocks and allows packets to pass through the TCP/UDP ports assigned to individual communications functions according to the settings.
By setting any communications functions that you will not use to **Not use**, you can reduce the number of entry points for external attacks to improve the security performance of the system.

Refer to the *SYSMAC CS/CJ-series EtherNet/IP Units Operation Manual (Cat. No. W465)* for details on opening and closing the port.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Yes	Yes		Yes	Yes	

Things That You Should Do

- Use this function by combining the CPU Unit with your EtherNet/IP Unit.
- Set only the communications functions that you will use to **Use**. This function enables or disables the communications functions for a node based on the settings. For example, when Use CIP message server is not set, the tag data link for that node will not work.
- If you need to verify the integrity of communications, use TCP communications.

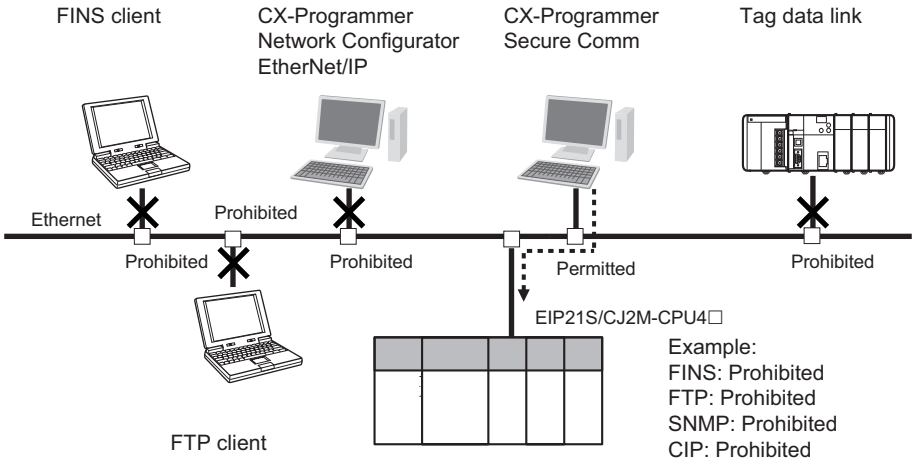
Note

The SNMP function, which can be disabled when not in use, allows communications with limited partner devices by specifying a community name for authentication or by using the IP filtering function.

Application Example: Permitting Packet Reception for a Specific Protocol

● Configuration

This configuration example permits Secure Comm communications with the CX-Programmer, and prohibits communications from other protocols.



● Settings for This Configuration

Make the settings as shown in the following table.

TCP/IP communications function	Setting
CIP message server	Not use
FINS/UDP	Not use
FINS/TCP	Not use
FTP server	Not use
SNMP	Not use

2-3 Preventing Unauthorized Connections to the CPU Unit

To protect user programs and equipment, which are your important intellectual property, from theft and unauthorized utilization, use this function to authenticate users when they connect to the CPU Unit so that unauthorized users cannot access the CPU Unit easily.

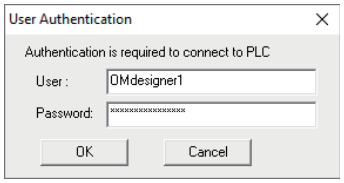
2-3-1 User Authentication

This function performs user authentication by user name and password when a user attempts to go online to identify who will perform online operations. User authentication is a function that identifies who will operate the CPU Unit online by registering users to operate the CPU Unit in advance.
When a user attempts to go online with the CPU Unit, the user is asked to enter a user name and password. The user cannot go online unless the user name and password match the pre-defined settings.
Refer to the *SYSMAC CS/CJ-series EtherNet/IP Units Operation Manual (Cat. No. W465)* for details on user authentication.

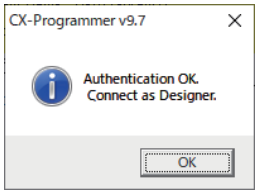
Example: User Authentication with the CX-Programmer

1 Connect the CX-Programmer online.

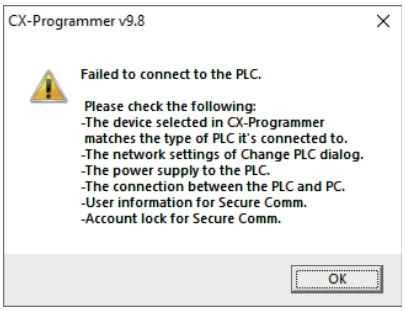
2 Enter your user name and password.



If the authentication is successful, your operation authority will be displayed with authentication OK.



If the authentication fails, an authentication failure message will be displayed.



Furthermore, each user is assigned operation authority, which is administrator, designer, maintainer, operator, or observer.
This ensures that users can operate the CPU Unit online only within the scope of authority assigned to them.
Refer to *2-4-1 Operation Authority Verification* on page 2-11 for detail.

User authentication settings such as the user name, password, and information on the user's operation authority are saved in the CPU Unit. Therefore, user authentication can be used even when you connect to the CPU Unit from a different PC. The user authentication settings are not saved in the project. Configure the user authentication settings for each CPU Unit that uses user authentication.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Yes	Yes	Yes	Yes	Yes	

Things That You Should Do

- Use this function by combining the CPU Unit with your EtherNet/IP Unit.
- Secure communications (Secure Comm) will not allow you to connect online with the CPU Unit due to an authentication failure if the user name and password do not match. Make a note of the user name and password. If there is no one who has the Administrator operation authority, you must initialize the EtherNet/IP Unit to the defaults. In this case, you will end up redoing all settings of the Unit, including user authentication settings, from scratch since they have been lost due to initialization. Keep the administrator account information strictly confidential.
- When the CJ1W-EIP21S EtherNet/IP Unit is connected to a CP1H-series CPU Unit, the CX-Programmer and PLC Backup Tool cannot use the corresponding functions. Please implement security measures on your own, with reference to *Security Measures for the Human and Process Layer* and *Security Measures for the Physical Layer* described in the *Security Guideline for Factory Automation System (Cat. No. P162)*.

2-3-2 PLC Names

You can have the CPU Unit memorize (register) its PLC name. This enables the CX-Programmer to check whether the PLC name in the project matches the PLC name of the CPU Unit at the connection destination when it goes online.

This function helps prevent incorrect connections from the CX-Programmer. Refer to the user's manual for your CPU Unit for the usage and details of the PLC names function.
You can find the user's manual in *Related Guideline and Manuals* on page 6.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes		Yes	Yes	

2-4 Preventing Unauthorized Operations on the CPU Unit

Prevent unauthorized operations on the CPU Unit to protect user programs and equipment, which are your important intellectual property, from theft and unauthorized utilization, malfunctions of production equipment, and accidents.

2-4-1 Operation Authority Verification

Changing CPU Unit data poses the risk of human or property damage due to operating mistakes. Prevent operating mistakes by restricting the functions that operators can operate based on their authority. Using the operation authority verification function, the administrator sets a password for each operation authority and notifies users of the operation authority name and password according to their skills.
Refer to the *SYSMAC CS/CJ-series EtherNet/IP Units Operation Manual (Cat. No. W465)* for details on operation authority verification.

Things That You Should Do

- Use this function by combining the CPU Unit with your EtherNet/IP Unit.
- When the CJ1W-EIP21S EtherNet/IP Unit is connected to a CP1H-series CPU Unit, the CX-Programmer and PLC Backup Tool cannot use the corresponding functions. Please implement security measures on your own, with reference to *Security Measures for the Human and Process Layer* and *Security Measures for the Physical Layer* described in the *Security Guideline for Factory Automation System (Cat. No. P162)*.

Types and Overview of Operation Authority

Type	Definition	Overview of operation authority
Administrator	A user who is responsible for operational management of the entire system, security, user access control, policy settings, etc.	Administrators can add and delete users and change their operation authority using the EIP21S User Management Tool. For the CX-Programmer and the PLC Backup Tool, they can perform the same operations as designers.
Designer	An engineer who plans and designs new factory automation systems or modifications to existing systems.	Designers can check the user list and change their own passwords using the EIP21S User Management Tool. They can perform almost all operations of the CX-Programmer and all operations of the PLC Backup Tool.
Operator	A user who directly operates factory automation systems and equipment in daily production activities.	Operators can change their own passwords using the EIP21S User Management Tool. Among the operations of the CX-Programmer, they can get data from the PLC. However, they cannot write data to the PLC.

User authentication allows you to operate the CPU Unit within the scope of the assigned authority by entering your user name and password when you connect the Support Software online.

2-5 Protecting Project Files and User Programs

Prevent theft and unauthorized utilization of project files and user programs, which are your important intellectual property. Taking multiple protective measures ensures that, even if one protective measure is broken, the next preventive measure can stop the spread of damage. Use multiple functions in combination.

2-5-1 Write Protection Using the DIP Switch

You can prohibit the CX-Programmer from overwriting the user program and data in the Parameter Area (e.g., PLC system settings and I/O tables). When the power supply is ON, you can prohibit the CPU Unit from simultaneously loading the user program, parameter data, and I/O memory stored on an SD Memory Card or memory cassette into the CPU Unit.
This function can prevent the program from being overwritten inadvertently.
Refer to the user's manual for your CPU Unit for details on write protection using the DIP switch.
You can find the user's manual in *Related Guideline and Manuals* on page 6.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes				

Things That You Should Do

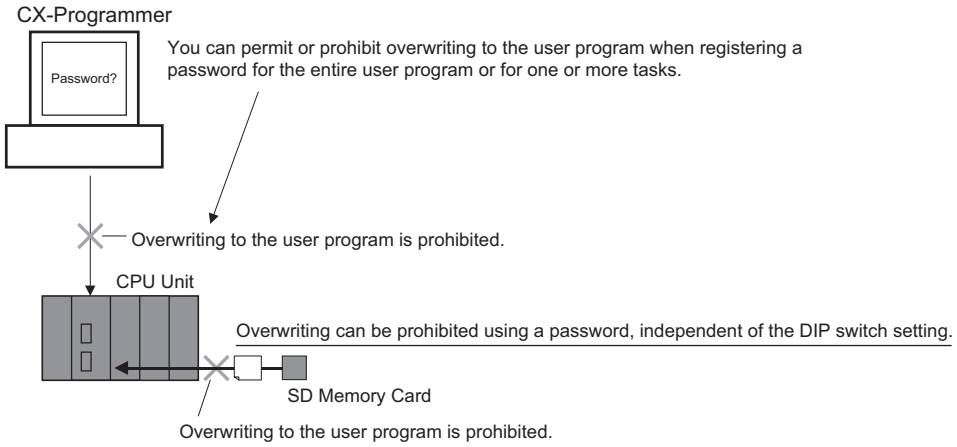
- The CP-series CP1E and CP2E CPU Units do not provide the corresponding functions. Please implement security measures on your own, with reference to *Security Measures for the Human and Process Layer* and *Security Measures for the Physical Layer* described in the *Security Guideline for Factory Automation System (Cat. No. P162)*.

Note

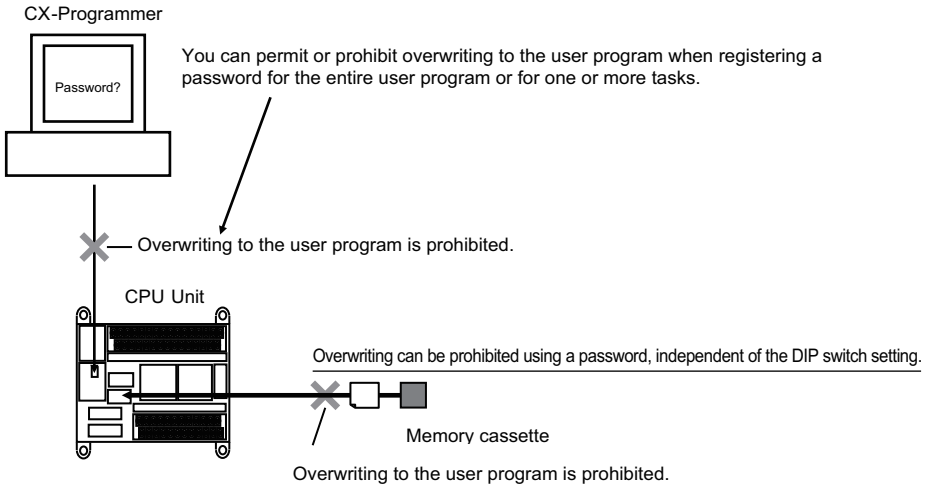
- **Prohibiting and Permitting Program Overwriting (Alternative to Write Protection Using the DIP Switch)**

  The CX-Programmer also allows you to permit or prohibit program overwriting when registering a password for the entire user program or for one or more tasks.
  This prevents the program from being overwritten by third parties or inadvertently.

Example for CS/CJ-series CPU Units



Example for CP-series CPU Units



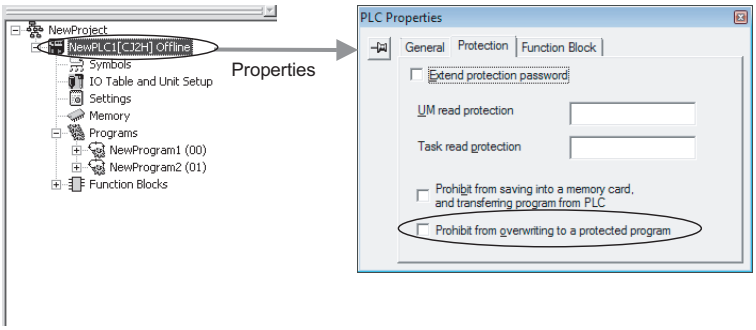
When Task read protection is set with the *Prohibit from overwriting to a protected program* option selected, only the protected tasks (programs) cannot be overwritten. Other tasks (programs) can be overwritten using online editing, task downloading, etc.

When no password is set for Task read protection, all tasks (programs) can be overwritten.

The settings for prohibiting or permitting program overwriting will not take effect until the program is transferred. Always transfer the program after changing this settings.

● Operating Procedure

1 Register a password in the **UM read protection** or **Task read protection** text box, select the **Prohibit from overwriting to a protected program** check box in the **Protection** tab page of the PLC Properties dialog box in the CX-Programmer.



2 Connect the CX-Programmer online. Either select **Transfer** – **Transfer To PLC** from the **PLC** menu to transfer the program, or select **Protection** – **Set Password** from the **PLC** menu and click the **OK** button.

2-5-2 Read Protection Using a Password

You can enable read protection using a password. When this function is enabled, you cannot display or edit the user program or specific tasks and function blocks in the protected program unless you enter the password.
Refer to the user's manual for your CPU Unit for details on read protection using a password.
You can find the user's manual in *Related Guideline and Manuals* on page 6.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes		Yes		

2-5-3 FINS Write Protection

You can protect the CPU Unit from write or operation attempts via the network using FINS commands and CIP message communications (including writing from applications using the CX-Programmer, CX-Protocol, CX-Process, or SYSMAC Gateway), while allowing read operations.
You can thus prevent all write operations, including downloading user programs, PLC system settings, and I/O memory, as well as operation mode changes and online editing.
However, you can also exclude write operations (remove write protection) from specific nodes that are initiated via FINS commands.
Refer to the user's manual for your CPU Unit for details on FINS write protection.
You can find the user's manual in *Related Guideline and Manuals* on page 6.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes				

Things That You Should Do

- CP-series CP1L, CP1E, and CP2E CPU Units do not provide the corresponding functions. Please implement security measures on your own, with reference to *Security Measures for the Human and Process Layer* and *Security Measures for the Physical Layer* described in the Security Guideline for Factory Automation System (Cat. No. P162).

2-5-4 Operation Protection Using the Production Lot Number

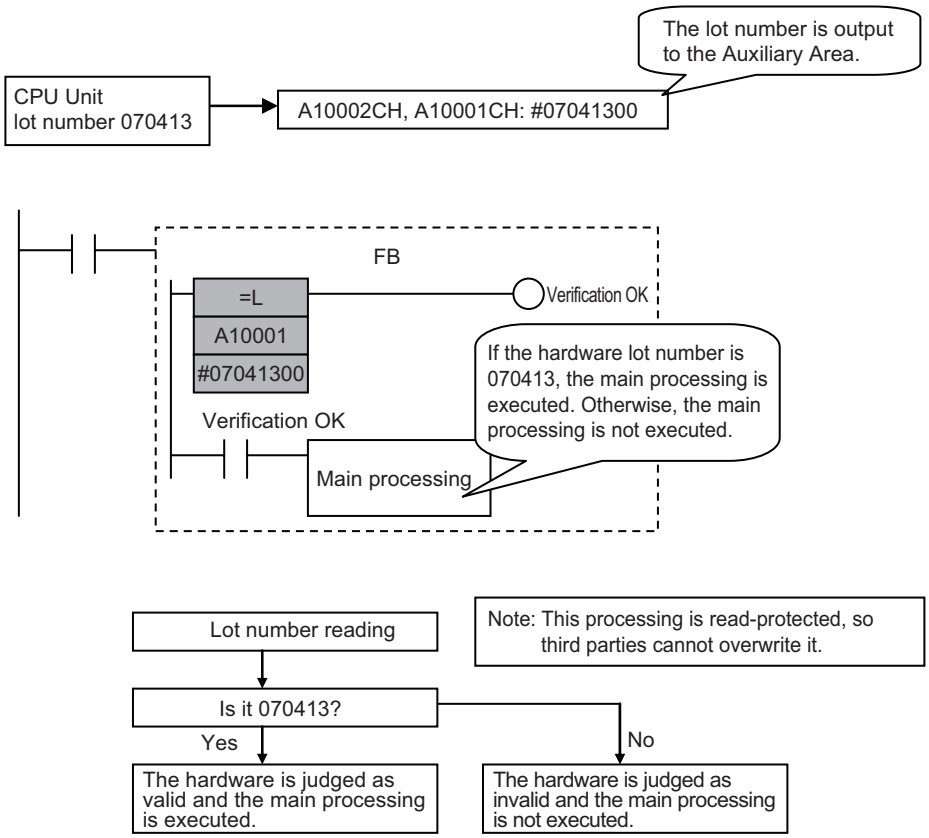
You can protect program operations using the production lot number stored in the Auxiliary Area. This production lot number cannot be changed by users.
Refer to the user's manual for your CPU Unit for details on operation protection using the production lot number.
You can find the user's manual in *Related Guideline and Manuals* on page 6.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
					Yes

Application Example: Permitting Project Execution on a Specific CPU Unit Only

The figure below shows how to run the program only on a CPU Unit with a specific production lot number.



2-5-5 User Data Overwrite Time

The user data rewrite time function records the time when the user program or data in the Parameter Area was overwritten to the Auxiliary Area.
The CPU Unit periodically loads data from this area and compares it with the previous value to detect tampering with the user program or parameters.
Refer to the user's manual for your CPU Unit for details on user data overwrite time.
You can find the user's manual in *Related Guideline and Manuals* on page 6.

Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
	Yes				

Types and Overview of User Data Overwrite Time

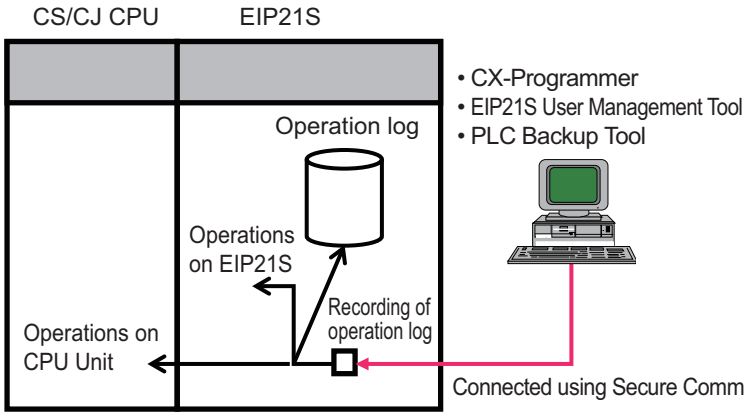
Type	Overview	Storage address (words)
User program overwrite date and time	The date and time (year, month, day, hour, minute, second, day of the week) when the user program was overwritten in BCD format. A90.00 to 90.07: Second (00 to 59), A90.08 to 90.15: Minute (00 to 59) A91.00 to 91.07: Hour (00 to 23), A91.08 to 91.15: Day (01 to 31) A92.00 to 92.07: Month (01 to 12), A92.08 to 92.15: Year (00 to 99) A93.00 to 93.07: Day of the week (00 to 06) 00: Sunday, 01: Monday, 02: Tuesday, 03: Wednesday, 04: Thursday, 05: Friday, 06: Saturday	A90 to A93
Parameter Area overwrite date and time	The date and time (year, month, day, hour, minute, second, day of the week) when the Parameter Area was overwritten. The storage format is the same as for the user program above.	A94 to A97

2-6 Preventing Repudiation

To protect your assets, it is also important to grasp the fact that they have been subjected to unauthorized operations. In addition, in the event of a security incident, it is necessary to determine the cause and circumstances of the incident. Recording security breaches and cyberattacks allows you to confirm who did what and when, and can be used as a repudiation preventive measure when problems occur.

2-6-1 Operation Log

The operation log function records important operations and results of users who connect the Support Software online using secure communications, along with information on the date and time, PC's IP address, and user name.
This allows you to confirm who did what operation and when, which can be used as a repudiation preventive measure when problems occur. This function is available only when the Support Software is connected using secure communications.
Refer to the *SYSMAC CS/CJ-series EtherNet/IP Units Operation Manual (Cat. No. W465)* for details on the operation log function.



Threats That Can Be Addressed

Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
		Yes			

Things That You Should Do

- An operation log saves to the EtherNet/IP Unit a record of operations that users performed on the CPU Unit and EtherNet/IP Unit from the EtherNet/IP Unit (using secure communications). To use this function, mount the EtherNet/IP Unit on a CS/CJ-series CPU Unit.
- The clock information used in the operation log (as the date and time of each operation) is acquired from the CPU Unit. For this reason, use the *automatic clock adjustment* function of the CX-Programmer or EtherNet/IP Unit to set the correct clock information on the CPU Unit.

- When the CJ1W-EIP21S EtherNet/IP Unit is connected to a CP1H-series CPU Unit, the CX-Programmer and PLC Backup Tool cannot use the corresponding functions. Please implement security measures on your own, with reference to *Security Measures for the Human and Process Layer* and *Security Measures for the Physical Layer* described in the Security Guideline for Factory Automation System (Cat. No. P162).

Note

The time when the CPU Unit power was turned ON and any errors that occurred while the CPU Unit was operating are stored as history in the CPU Unit's Auxiliary Area (AR). You can check the history stored in the CPU Unit from the CX-Programmer. Use this feature in conjunction with this function.

3

Applying Security Patches

To protect your assets and production from cyberattacks progressing day by day, it is effective to keep your devices up-to-date for higher security strength. This section describes how to update the devices and software.

3-1 Updating CS/CJ/CP-series CPU Unit and EtherNet/IP Unit

To add functionality, improve ease of operation, and enhance security, always keep the CS/CJ/CP-series CPU Unit and CS/CJ-series EtherNet/IP Unit updated to their latest versions for use. Contact your OMRON representative for details on the firmware update.

3-2 Updating CX-One

To add functionality, improve ease of operation, and enhance security, always keep CX-One updated to the latest version for use.

You can use the CX-One Auto Update function to update CX-One to the latest version.
CX-One Auto Update is a system that uses the Internet to keep the Support Software included with CX-One up-to-date.
Using CX-One Auto Update automatically searches for the latest updates that can be applied to the currently installed CX-One Support Software.
By installing the searched updates, you can keep the CX-One installed on your computer up-to-date.

- The auto update function becomes automatically available as soon as CX-One is installed.
- The auto update function requires CX-One version 2.0 or higher.

3-3 Updating the OS of Your PC

To avoid security risks arising from vulnerabilities in the OS, always keep the OS of your PC on which CX-One is running up-to-date.

4

Safely Disposing of Equipment

This section describes the functions that CS/CJ/CP-series CPU Units and CS/CJ-series EtherNet/IP Units provide for disposal.

4-1 Erasing Your Assets in the CPU Unit and EtherNet/IP Unit

Before disposing of your CS/CJ/CP-series CPU Unit and CS/CJ-series EtherNet/IP Unit, use the data erasure functions (Memory All Clear, Unit Restart) listed below to erase the internally stored information to prevent information leakage.
If the data erasure functions (Memory All Clear, Unit Restart) fail, the CS/CJ/CP-series CPU Unit or CS/CJ-series EtherNet/IP Unit may be malfunctioning. In such cases, contact your OMRON representative.

Target device for data erasure	Operation description
CS/CJ/CP-series CPU Unit	Perform a Memory All Clear operation.*1
CS/CJ-series EtherNet/IP Unit	Perform a Restart Unit operation (to restore factory defaults).

*1. Performing a Clear All Memory operation on the CS/CJ/CP-series CPU Unit does not initialize the CS/CJ-series EtherNet/IP Unit mounted on the CS/CJ/CP-series CPU Unit to the factory defaults. Perform a Restart Unit operation on the CS/CJ-series EtherNet/IP Unit separately to restore the factory default settings.

4-1-1 Procedure for Erasing the Internally Stored Information in the CS/CJ/CP-series CPU Unit

To erase the internally stored information in the CS/CJ/CP-series CPU Unit, use the CX-Programmer. Start the CX-Programmer and follow the steps below to erase the internally stored information in the CS/CJ/CP-series CPU Unit.

1 Select **Clear All Memory** from the **PLC** menu. Or, in the PLC Errors window, select **Clear All Memory** from the **Options** menu.
The **Clear All Memory Confirmation** dialog box appears.
The PLC name, PLC model, and areas to be cleared are displayed.

2 Select the *Initialize* check box and click the **OK** button.
The user program and data in the Parameter Area and I/O Memory Areas of the CPU Unit are all cleared (i.e., the CPU Unit is initialized to the default settings).
Click the **Cancel** button to close the dialog box.

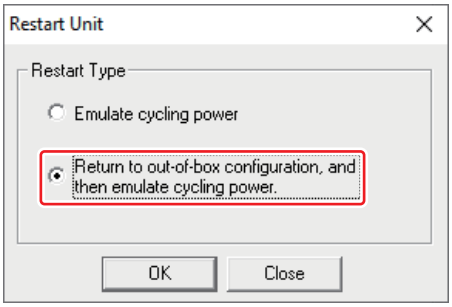
4-1-2 Procedure for Erasing the Internally Stored Information in the CS/CJ-series EtherNet/IP Unit

To erase the internally stored information in the CS/CJ-series EtherNet/IP Unit (i.e., to restore the factory default settings), use the CX-Programmer. For security reasons, connect the CX-Programmer to the USB port, peripheral port, or serial port of the CPU Unit to initialize the CPU Unit.

Start the CX-Programmer and follow the steps below to erase the internally stored information in the CS/CJ-series EtherNet/IP Unit.
To restart the Unit after restoring the default settings using the CX-Programmer, perform the following operations.

1 Click **Restart** in the **Edit Parameters** dialog box and, in a confirmation dialog box for restart, click the **Yes** button.
The **Restart Unit** dialog box appears.

2 Select the **Return to out-of-box configuration, and then emulate cycling power.** option and click the **OK** button.



A

Appendices

A-1 Available Support Software Versions

The available Support Software versions are listed in the table below. The Support Software of these versions is included with CX-One version 4.6.1 or higher.

Support Software	Version
CX-Programmer	9.81 or higher
PLC Backup Tool	1.03 or higher
EIP21S User Management Tool*1	1.0 or higher

*1. You cannot install the EIP21S User Management Tool on a PC running an OS earlier than Windows 10. If the OS is earlier than Windows 10 version 1803, the Support Software cannot establish online connections using Secure Comm or use the following functions that utilize Secure Comm. We recommend upgrading the OS to the latest version.

- User authentication
- Operation authority verification
- Operation log

Note: Do not use this document to operate the Unit.

OMRON Corporation **Industrial Automation Company**

Kyoto, JAPAN **Contact : www.ia.omron.com**

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

Cat. No. P176-E1-01 0326