Security Guideline for NJ/NX-series Controller

P166-E1-02

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.
- All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, mechanical, electronic, photocopying, recording, or otherwise, without the prior written permission of OMRON.
- 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.
- 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

- This product incorporates certain third party software. The license and copyright information associated with this software is available at http://www.fa.omron.co.jp/nj_info_e/.

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 NJ/NX series CPU Units.
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.

- NX-series CPU Units
- NJ-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

1
2
3
4
A

CONTENTS

Section 1 Defense in Depth with NJ/NX Controller

Section 2 NJ/NX Controller's Security Functions to Protect Assets

Section 3 Applying Security Patches

Section 4 Safely Disposing of Equipment

Appendices

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.
NJ/NX-series CPU Unit Software User's Manual	W501	Learning the details and usage of security functions provided in NJ/NX-series CPU Units.
Sysmac Studio Version 1 Operation Manual	W504	Learning the details and usage of security functions provided in the Sysmac Studio.
NJ/NX-series CPU Unit Built-in EtherNet/IP™ Port User's Manual	W506	Learning the details and usage of security functions provided in the built-in EtherNet/IP ports of NJ/NX-series CPU Units.
NJ/NX-series CPU Unit OPC UA User's Manual	W588	Learning the details and usage of the OPC UA Server function provided in NJ/NX-series CPU Units.
NJ/NX-series Database Connection CPU Units User's Manual	W527	Learning the details and usage of the database connection service function provided in NJ/NX-series CPU Units.
NJ/NX-series Troubleshooting Manual	W503	Learning about the access log to register in NJ/NX-series CPU Units.

Revision History

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

Cat. No.
P166-E1-02
Revision code

Revision code	Date	Revised content
01	March 2025	Original production
02	July 2025	• Made changes accompanying the release of unit version 1.69 of the NJ-series, NX502, NX102, and NX1P2 CPU Units. • Made changes accompanying the release of unit version 1.36 of NX701 CPU Units.

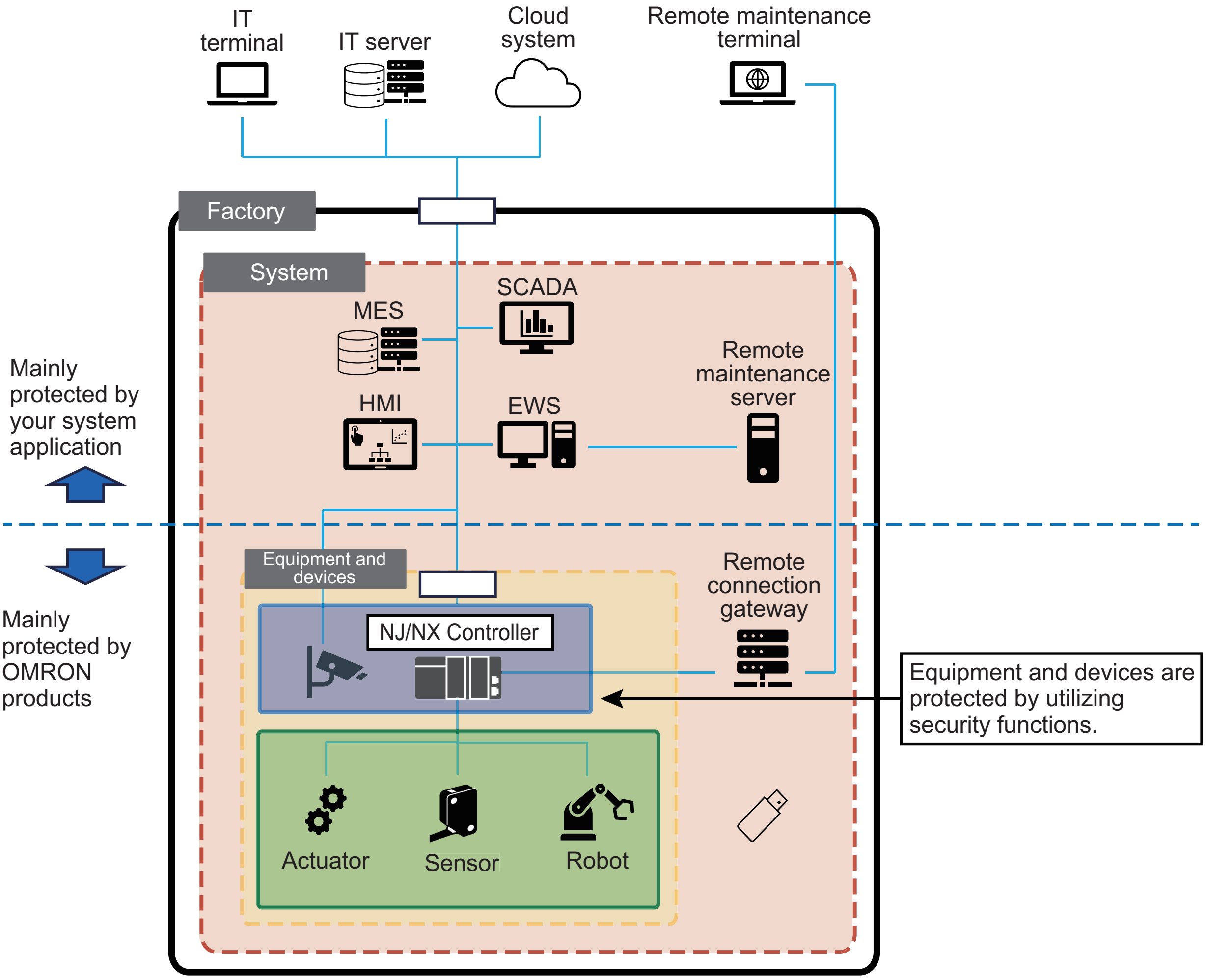
1

Defense in Depth with NJ/NX Controller

The NJ/NX Controller provides multiple security functions to achieve Defense in Depth.
This section describes the Defense in Depth that the security function of NJ/NX Controller provides.

1-1 Operating Environment of the NJ/NX Controller

The NJ/NX Controller effectively utilizes its security functions to protect the operations and assets of equipment and the Controller itself.

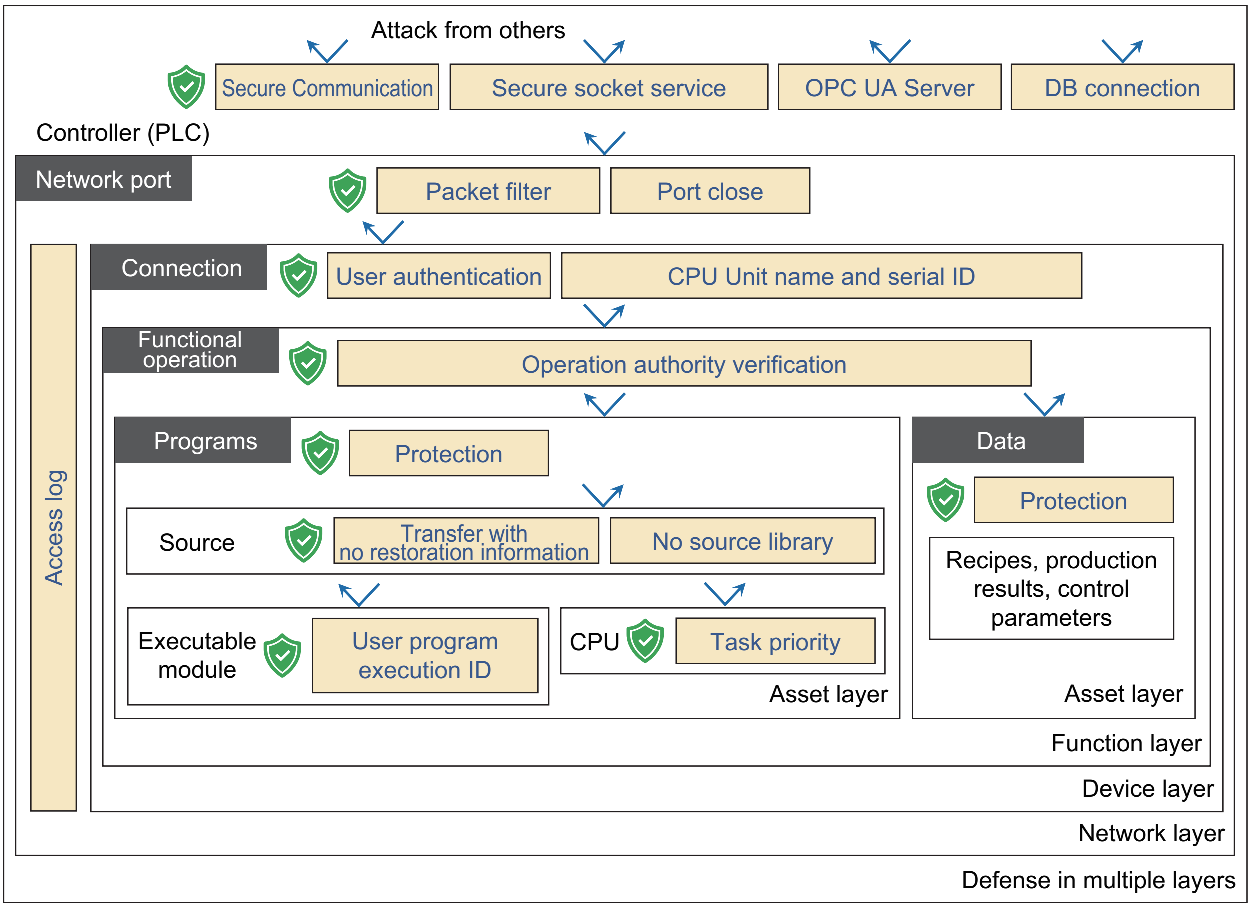

IT terminal
IT server
Cloud system
Remote maintenance terminal
Factory
System
MES
SCADA
Remote maintenance server
HMI
EWS
Mainly protected by your system application
Mainly protected by OMRON products
Equipment and devices
Remote connection gateway
NJ/NX Controller
Equipment and devices are protected by utilizing security functions.
Actuator
Sensor
Robot

1-2 Security Measures for the Technical Layer by Using the NJ/NX Controller

The NJ/NX Controller provides security functions to protect your assets in the Defense in Depth concept. Even if an attacker could break through one layer, security functions in the layer closest to assets will be able to 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.

In this document, things that you should do in particular using the security functions are described. Read the section in conjunction and take necessary measures.



The table below lists the functions provided in each layer.

Layer to protect assets	Purpose	Function provided by OMRON products	Reference
Network layer	Protecting data on communication lines	Secure communication function	page 2-2
		Secure socket services	page 2-3
		OPC UA Server	page 2-4
		DB connection	page 2-5
	Blocking external attacks on the Controller	Packet filter	page 2-6
		TCP/UDP port close function	page 2-6
Device layer	Preventing unauthorized connection to the Controller	User authentication	page 2-8
		Confirming CPU Unit names and serial IDs	page 2-9
Function layer	Preventing unauthorized operations on the Controller	Operation authority verification	page 2-10
Asset layer	Preventing the disclosure of program and data	Password protection for project files	page 2-11
		Data protection	page 2-11
		Library without source code	page 2-12
		User program transfer with no restoration information	page 2-12
		Write protection of the CPU Unit	page 2-13
	Preventing unauthorized utilization of programs	Authentication of user program execution IDs	page 2-14
	Protecting stable operation of the Controller	Setting the task period of the Controller	page 2-16
Common to all layers	Preventing repudiation	Access log	page 2-18

2

NJ/NX Controller's Security Functions to Protect Assets

This section describes the security functions that the NJ/NX Controller provides.

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 Communication Function

The secure communication function is intended to improve the security of communications between Sysmac Studio and the Controller.
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 *NJ/NX-series CPU Unit Software User’s Manual (Cat. No. W501)* for details on the secure communication function.

Threats That Can Be Addressed

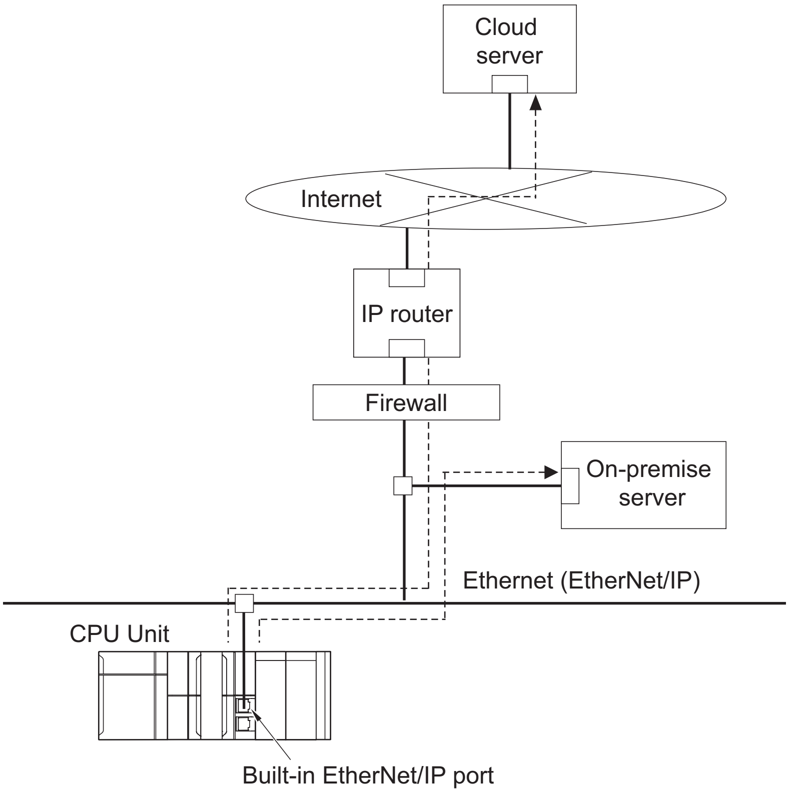
Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Yes	Yes		Yes	Yes	

Things That You Should Do

- To improve security, install and use the Sysmac Studio on an OS that is within the support period of Microsoft Windows.
- The secure communication function may affect the communications response performance and the execution processing performance of some instructions. When you use a CPU Unit that supports secure communication, check the operation sufficiently in advance. If there is a problem with the performance, consider changing settings to *allow connection to Sysmac Studio or an NA-series Programmable Terminal that do not support secure communication*.
- If you need to securely configure the EtherNet/IP settings, use the Sysmac Studio instead of the Network Configurator.
- The SysmacGateway does not support authentication functionality. If necessary, implement authentication functionality in your application.
- If you need to securely transfer files on SD cards, use the Sysmac Studio instead of an FTP client. If you need to use an FTP client to transfer files, 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.
- 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 the Sysmac Studio is connected to the control systems inside the firewall.
- If you need remote access from the Sysmac Studio to control systems and equipment, use a virtual private network (VPN).

2-1-2 Secure Socket Services

The secure socket service function allows the CPU Unit’s built-in EtherNet/IP ports as a client to perform secure socket communications with on-premise servers on a private network or with cloud servers on an external network. It performs encrypted communications using TLS and supports client private keys and certificates to ensure secure communications.
Refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User’s Manual (Cat. No. W506)* for details on the secure socket service function.



Threats That Can Be Addressed

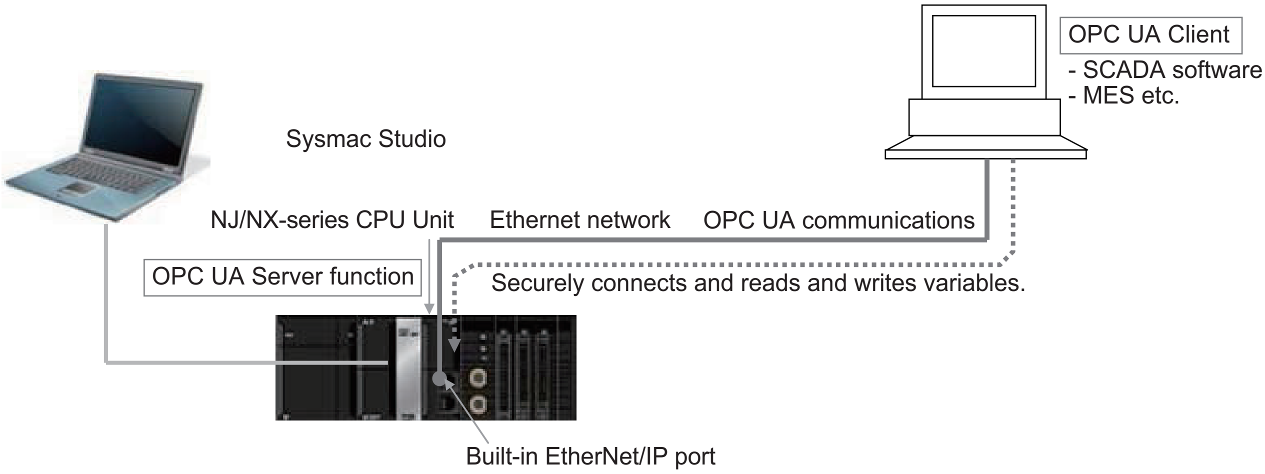
Spoofing	Tampering	Repudiation	Information disclosure	Denial of service	Elevation of privilege
Yes	Yes		Yes	Yes	

Things That You Should Do

- The Network Configurator does not use secure communications. Use IP filtering or a user system (firewall) to prohibit the Network Configurator from connecting to the Controller from a network that cannot ensure security.
- To prevent devices prepared by attackers from communicating with the Controller, install all the devices connected to the Controller in a secure area.
- Use your user application to verify that the Controller is connected to the correct devices.

2-1-3 OPC UA Server

The OPC UA Server function enables NJ/NX-series CPU Units to operate as *OPC UA servers*.
With this function, OPC UA clients can connect to the built-in EtherNet/IP ports of an NJ/NX-series CPU Unit operating as an OPC UA server via Ethernet network and then read and write variables in the CPU Unit through OPC UA communications. Since it supports OPC UA communications that realize both versatility of the connection method and security risk response at the same time, it is possible to securely exchange manufacturing progress information collection, manufacturing instructions, etc. from OPC UA-compliant host systems such as SCADA and MES.
Refer to the *NJ/NX-series CPU Unit OPC UA User’s Manual (Cat. No. W588)* for the details and usage of the OPC UA Server function.



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

- The Network Configurator does not support user authentication, client authentication, and encrypted communications for connection to the Controller. If you need to perform secure communications, disable the use of EtherNet/IP and use OPC UA instead.
- If authentication is required for communications with applications, use OPC UA. Alternatively, use IP filtering to limit the partner devices that can be connected.
- If you create client functionality, implement it so that the user is notified before logging in.
- Be sure to publish as least variables as possible to network in order to avoid information disclosure via the variables.
  It is recommended not to publish global variables to network. If publishing global variables is required, 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.
  c) Disable the use of EtherNet/IP.

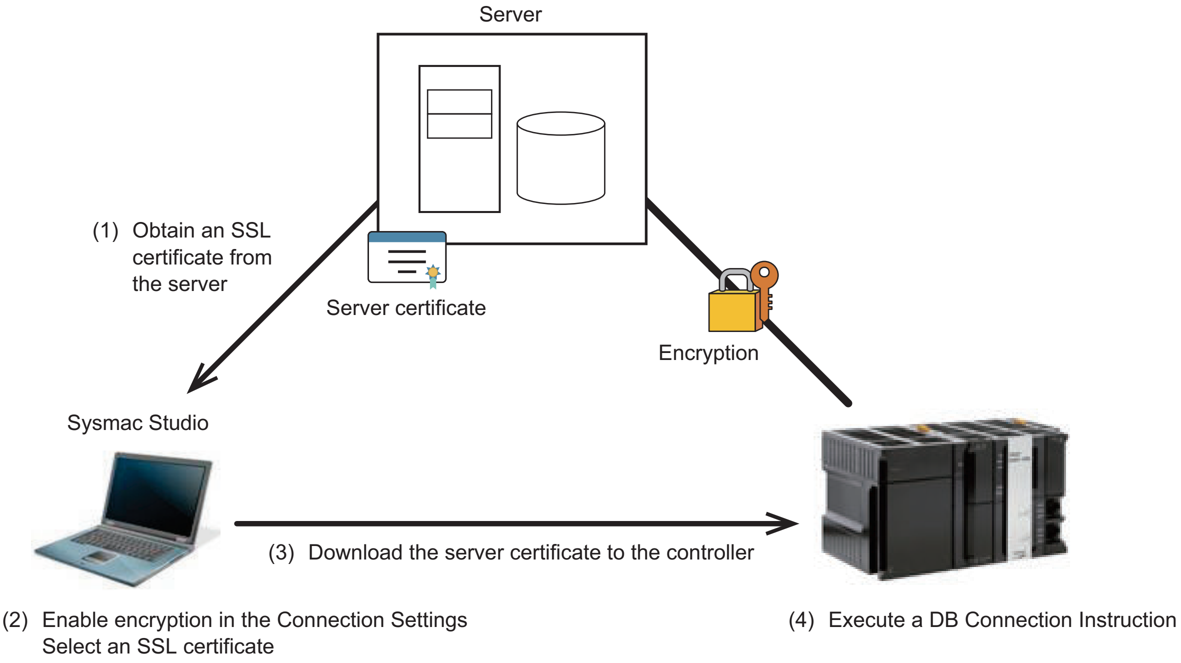
- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
- Change your password by yourself on a periodic basis.

2-1-4 DB Connection

The DB connection service performs encrypted communications using SSL/TLS encrypted communications.

Encrypted communications is a function to prevent eavesdropping and tampering by encrypting communications data between the Controller and the DB. Encrypted communications are supported by DB connection service version 2.00 or later and can be used by configuring the DB connection settings in the Sysmac Studio.

Refer to the *NJ/NX-series Database Connection CPU Units User's Manual (Cat. No. W527)* the for details on the settings for encrypted communications.


Server
(1) Obtain an SSL certificate from the server
Server certificate
Encryption
Sysmac Studio
(3) Download the server certificate to the controller
(2) Enable encryption in the Connection Settings
Select an SSL certificate
(4) Execute a DB Connection Instruction

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 a DB that supports TLS1.2.
- Server authentication is not possible with any DB other than Oracle Database. Either use Oracle Database to perform server authentication or use a user application to confirm that it is the correct server. Alternatively, install the server in a secure area to prevent the Controller from communicating with servers prepared by attackers.

2-2 Blocking External Attacks on the Controller

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

2-2-1 Packet Filter

You can filter IP packets in the receiving process in the built-in EtherNet/IP port to limit access from an external device.
The packet filter function allows more detailed settings, such as allowing only certain clients to use specific server functions.
Refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual (Cat. No. W506)* for how to use the packet filter function.

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

- You can use the Controller's packet filter function to restrict the IP addresses and TCP/UDP ports used for the source (FTP client).
- 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.

2-2-2 TCP/UDP Port Close Function

There is a risk of unauthorized access to the Controller and theft of user programs and other data. To reduce the risk, close unused ports to prevent unauthorized access.
With the NJ/NX Controller, you can close the TCP/UDP port used by the server function provided in the built-in EtherNet/IP ports. This allows you to open only TCP/UDP ports that you want to use in the system.
Refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual (Cat. No. W506)* for details on the server function provided in the built-in EtherNet/IP ports.

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

- If you need to verify the integrity of communications, use TCP communications.
- 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.
- 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.
- 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.

2-3 Preventing Unauthorized Connection to the Controller

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 Controller so that unauthorized users cannot access the Controller 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 Controller online by registering users to operate the Controller in advance. When a user attempts to go online with the Controller, 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.
Furthermore, each user is assigned operation authority, which is administrator, designer, maintainer, operator, or observer. This ensures that users can operate the Controller online only within the scope of authority assigned to them.
User authentication settings such as the user name, password, and information on the user’s operation authority are saved in the Controller. Therefore, user authentication can be used even when you connect to the Controller from a different PC.
The user authentication settings are not saved in the project. Configure the user authentication settings for each Controller 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	Yes

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 Sysmac Studio online. Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on how to operate this function.

Things That You Should Do

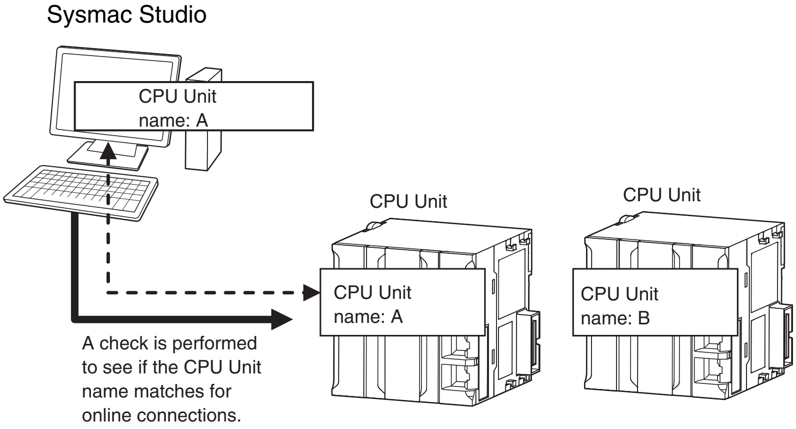
- Change your password by yourself on a periodic basis.
- Set a complex password (at least eight characters long containing multiple character types) to prevent possible password analysis by brute-force attacks.
- Use user authentication when using the Sysmac Studio to go online with the Controller or when using the OPC UA Server as it is supported in these situations. Since the authentication function is not supported for other communications, do not use (disable) communications that are not necessary. If necessary, implement authentication functionality in your application. For example, use a device that supports user authentication, or use SysmacGateway/Compolet, etc. to implement authentication

functionality in your application. When you implement authentication functionality in your application, note the following.

a) To avoid fixed password values in the system, be sure to take measures such as changing the default password value.
b) Consider providing a mechanism to periodically update passwords, etc.
c) Take measures to prevent disclosure of passwords, etc.

2-3-2 Confirming CPU Unit Names and Serial IDs

When you go online with a CPU Unit from the Sysmac Studio, the CPU Unit name in the project is compared to the name of the CPU Unit being connected to.
This helps prevent incorrect connections to the CPU Unit from the Sysmac Studio. It is particularly effective for operations performed over an EtherNet/IP network.


Sysmac Studio
CPU Unit name: A
CPU Unit
CPU Unit
CPU Unit name: A
CPU Unit name: B
A check is performed to see if the CPU Unit name matches for online connections.

In addition to the CPU Unit name, it is also possible to use serial ID identification based on the CPU Unit production information (optional).

Threats That Can Be Addressed

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

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for how to use the CPU Unit name and serial ID.

2-4 Preventing Unauthorized Operations on the Controller

Prevent unauthorized operations on the Controller 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 Controller 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.

Threats That Can Be Addressed

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

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for setting the operation authority verification function.

Things That You Should Do

- 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.

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 Password Protection for Project Files

To prevent user programs and settings contained in a project file from being viewed or tampered with, apply password protection to the entire project file.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for how to use this function.

Threats That Can Be Addressed

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

Things That You Should Do

- To improve security, install and use the Sysmac Studio on an OS that is within the support period of Microsoft Windows.
- Set and manage your password appropriately to prevent unauthorized utilization by others.
- 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.

2-5-2 Data Protection

Use this function to protect only part of data contained in a project file, for example, when more than one person is working on design or maintenance. Set a password for each unit of data to prohibit viewing, modifying, and copying it (access restriction).
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for how to use this function.

Threats That Can Be Addressed

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

Things That You Should Do

- To improve security, install and use the Sysmac Studio on an OS that is within the support period of Microsoft Windows.
- Set and manage your password appropriately to prevent unauthorized utilization by others.
- 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.

2-5-3 Library without Source Code

To prevent malicious attackers from accessing user programs in a project file, create a library file (called "library without source code") that does not contain the restoration information (source) for the user programs. You can create a project file that does not contain the source code you want to protect by referencing the library without source code from the project.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for how to use this function.

Threats That Can Be Addressed

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

Things That You Should Do

- To improve security, install and use the Sysmac Studio on an OS that is within the support period of Microsoft Windows.
- To prevent attackers from stealing project files from maintenance terminal PCs, set up user accounts on each maintenance terminal PC and install the PCs in a secure area.

2-5-4 User Program Transfer with No Restoration Information

This function does not transfer the program restoration information (source) to the CPU Unit when you upload a user program from another PC so that the user program cannot be displayed. Use it to prevent theft of user program data when on-site maintenance of user programs is not required.
Refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for user program transfer with no restoration information.

Threats That Can Be Addressed

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

Things That You Should Do

- To improve security, install and use the Sysmac Studio on an OS that is within the support period of Microsoft Windows.

2-5-5 Write Protection of the CPU Unit

Use this function to protect data in the CPU Unit so that it cannot be rewritten from the Sysmac Studio. Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for how to use this function.

Threats That Can Be Addressed

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

Things That You Should Do

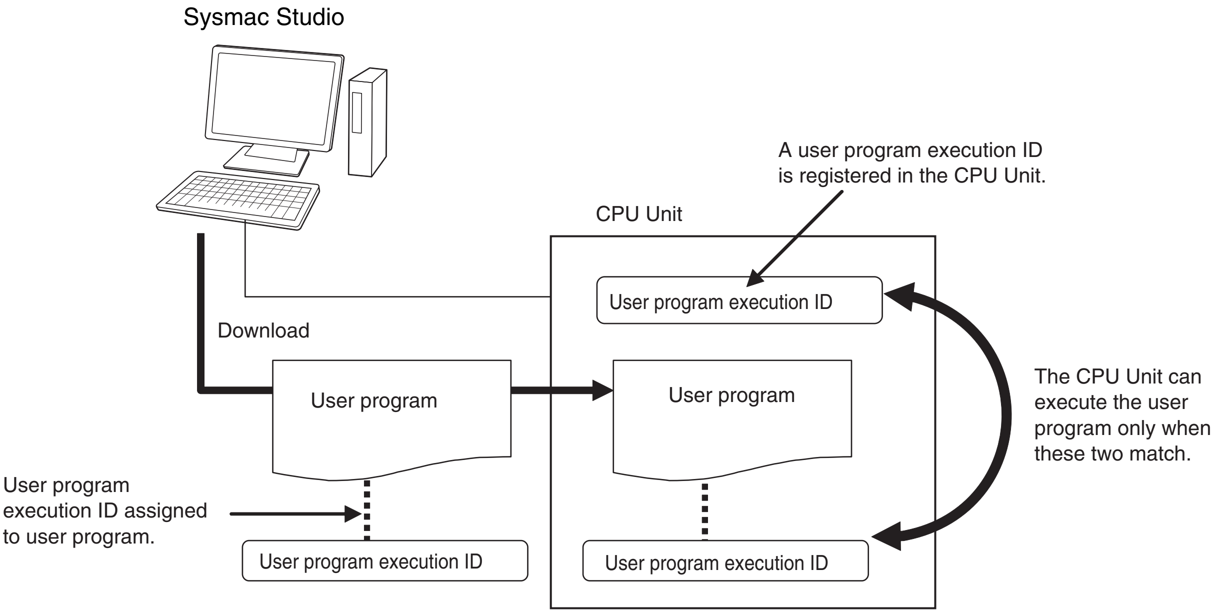
- To improve security, install and use the Sysmac Studio on an OS that is within the support period of Microsoft Windows.

2-6 Preventing Unauthorized Utilization of the Controller

Protect your user programs and equipment, which are your important intellectual property, from theft and unauthorized utilization.

2-6-1 Authentication of User Program Execution IDs

Even if your user program is stolen, this function prevents the execution of the user program, thereby protecting it from unauthorized use.
By entering a specific ID (called *user program execution ID*) in the Controller in advance, it is possible to make only the user programs assigned to that ID executable.


Sysmac Studio
A user program execution ID is registered in the CPU Unit.
CPU Unit
User program execution ID
Download
User program
User program
The CPU Unit can execute the user program only when these two match.
User program execution ID assigned to user program.
User program execution ID
User program execution ID

This function has the following advantages.

- You can restrict certain Controllers to execute only specific user programs.
- You can prevent different Controllers (hardware) from executing certain user programs.

Unlike the protection function, this function allows user programs to be displayed and edited.
Refer to the *NJ/NX-series CPU Unit Software User’s Manual (Cat. No. W501)* for details on the user program execution ID.

Threats That Can Be Addressed

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

Things That You Should Do

- To improve security, install and use the Sysmac Studio 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 the Sysmac Studio is connected to the control systems inside the firewall.
- If you need remote access from the Sysmac Studio to control systems and equipment, use a virtual private network (VPN).

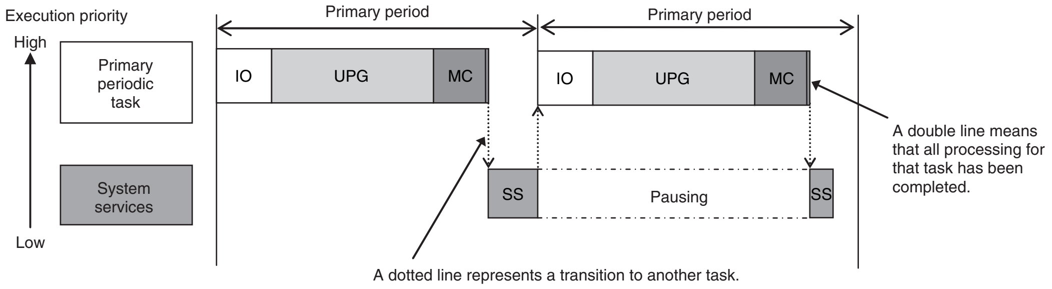
2-7 Protecting Stable Operation of the Controller

If the Controller is subjected to excessive control or communications load through a DOS attack by a malicious third party or virus-infected production PC, the Controller’s control processing or communications processing may experience delays, resulting in operational delays or abnormal shutdown of equipment. Prevent delays in production takt time, production suspension, damage to equipment and people, quality degradation of products, etc. caused by these problems.

2-7-1 Setting the Task Period of the Controller

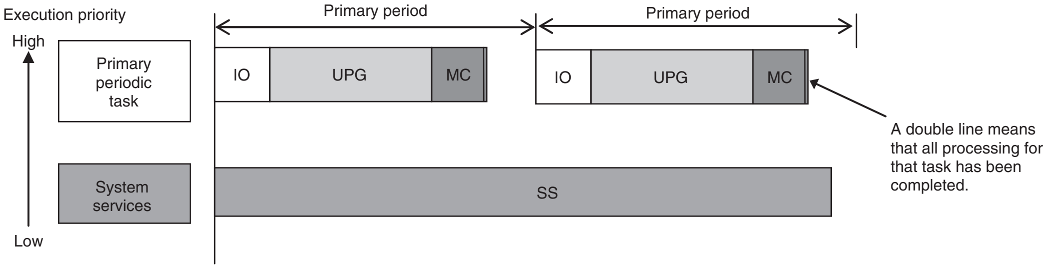
The NJ/NX Controller has adopted a multi-core CPU and task priority management. Due to this design, even if a DoS attack occurs through external communications, etc., the control period is not affected. By designing tasks that must be executed within a control period to have a high priority, it is possible to maintain control of production equipment.

For the NJ Controller, due to task priority management, system services are executed during the unused time between execution of the tasks. Even if a DoS attack occurs, control tasks remain unaffected and therefore do not affect the control period.


Execution priority
High
Low
Primary periodic task
System services
Primary period
Primary period
IO
UPG
MC
IO
UPG
MC
SS
Pausing
SS
A double line means that all processing for that task has been completed.
A dotted line represents a transition to another task.

IO: Indicates I/O refreshing (data outputs and then data inputs).
UPG: User program execution.
MC: Indicates motion control.
SS: Indicates system services.

For the NX Controller that incorporates a multi-core CPU, tasks and system services are executed in parallel. Even if a DoS attack occurs, control tasks remain unaffected and therefore do not virtually affect the control period.



A double line means that all processing for that task has been completed.

IO: Indicates I/O refreshing (data outputs and then data inputs).
UPG: User program execution.
MC: Indicates motion control.
SS: Indicates system services.

Refer to the *NJ/NX-series CPU Unit Software User’s Manual (Cat. No. W501)* for the mechanism and types of tasks.

Threats That Can Be Addressed

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

2-8 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.

2-8-1 Access Log

The NJ/NX Controller registers online operations that users perform on the Controller using Support Software as an access log. If the user authentication function is used the user name is also recorded in the access log, which is important for security.
Refer to the *NJ/NX-series Troubleshooting Manual (Cat. No. W503)* for the access log to be registered.

Threats That Can Be Addressed

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

Things That You Should Do

- If the log is deleted, you cannot prevent repudiation. If the number of events exceeds the number of records permitted, the NJ/NX Controller overwrites the access log from older information. It is recommended to back up the logs periodically and keep them for a certain period of time.

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 the functions that the NJ/NX Controller provides for updates.

3-1 Updating the NJ/NX Controller

To add functionality, improve ease of operation, and enhance security, always keep the NJ/NX Controller updated to the latest version for use.
Contact your OMRON representative for details on the firmware update.

3-1-1 Firmware Update Prohibition

This function prohibits the update of the NJ/NX Controller to prevent malicious third parties from illegally updating equipment.
Set whether or not to prohibit firmware update in the Sysmac Studio. Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for how to set this function.

Threats That Can Be Addressed

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

3-1-2 Displaying the Firmware Update Log

Display the NJ/NX Controller's firmware update log.
Refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for displaying the firmware update log.

Threats That Can Be Addressed

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

3-2 Updating the Sysmac Studio

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

Refer the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on auto-updating.

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 the Sysmac Studio and its Support Software are running up-to-date.

4

Safely Disposing of Equipment

This section describes the functions that the NJ/NX Controller provides for disposal.

4-1 Erasing Your Assets in the NJ/NX Controller

Disposing of or transferring your OMRON products poses the risk of information disclosure, allowing third parties to view user data and other information saved in the devices.
Before disposing of or transferring the products, erase the user data with your responsibility.

4-1-1 Complete Data Erasure Function

The complete data erasure function completely erases user data. Use the function to completely erase all the user-set data in the CPU Unit.
Since the data in the memory is not completely erased with the Clear all memory function, the data may be restored. The complete data erasure function prevents data restoration by writing random data to unused areas of the built-in non-volatile memory that stores user programs and various settings after clearing all memory.
Refer to the *NJ/NX-series CPU Unit Software User's Manual (Cat. No. W501)* for details on the complete data erasure function.

4-2 Destroying the NJ/NX Controller

Before you dispose of the NJ/NX Controller, erase the user data in the product using the complete data erasure function to ensure that the data will not be disclosed. If the data erasure fails, we recommend to physically and electrically destroy the NJ/NX Controller as the product itself may be failed. Contact your OMRON representative for details on how to destroy the product.

A

Appendices

A-1 Contact Information for This Guide and Factory Automation Products of OMRON

If you have any questions about this guide or FA products of OMRON, please contact your nearest OMRON branch or sales office from the following links.
https://www.ia.omron.com/global_network/

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

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 (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. P166-E1-02 0725