OMRON

Safety Network Controller

NX-series

Communication Control Unit

Built-in Function User's Manual

NX-CSG□□□

Communication Control Unit

SYSMAC always in control

Z396-E1-05

NOTE

1. All rights reserved. No part of this publication 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.
2. 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 manual is subject to change without notice.
3. Every precaution has been taken in the preparation of this manual. Nevertheless, OMRON assumes no responsibility for errors or omissions.
Neither is any liability assumed for damages resulting from the use of the information contained in this publication.

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.
• Safety over EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.
• ODVA, CIP, CompoNet, DeviceNet, EtherNet/IP and CIP Safety 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.
• 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

Thank you for purchasing an NX-series Communication Control Units.
This manual contains information that is necessary to use the NX-series Communication Control Units.
Please read this manual and make sure you understand the functionality and performance of the Unit before you attempt to use it in a control system.
Keep this manual in a safe place where it will be available for reference during operation.

Intended Audience

This manual is intended for the following personnel, who must also have knowledge of electrical systems (an electrical engineer or the equivalent).

- 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.

For programming, this manual is intended for personnel who understand the programming language specifications in international standard IEC 61131-3 or Japanese standard JIS B 3503.

Applicable Products

This manual covers the following products.

- NX-series Safety Control Units
  NX-CSG□□□

Sections in this Manual

1 Data Management and Clock Functions

2 Automatic Clock Adjustment

3 Management Functions for NX Units

4 SD Memory Card Operations

5 Security

6 Event Logs

7 Changing Event Levels

8 CIP Message Communications

9 TCP/UDP Message Service Function

10 SNMP Agent

A Appendices

I Index

CONTENTS

Introduction **1**
Intended Audience 1
Applicable Products 1

Sections in this Manual **3**

Relevant Manuals **9**

Manual Structure **11**
Page Structure 11
Special Information 12
Precaution on Terminology 12

Terms and Conditions Agreement **13**
Warranty, Limitations of Liability 13
Application Considerations 14
Disclaimers 14
Statement of security responsibilities for assumed use cases and against threats 15

Safety Precautions **16**

Precautions for Safe Use **17**

Precautions for Correct Use **18**

Regulations and Standards **19**

Versions **20**
Checking Versions 20
Unit Versions of Units and Sysmac Studio Versions 21

Related Manuals **22**

Terminology **24**

Revision History **28**

Section 1 Data Management and Clock Functions

1-1 Clearing All Memory **1-2**

1-2 Clock **1-3**
1-2-1 Overview 1-3
1-2-2 Setting the Clock Data 1-3
1-2-3 Correcting the Clock from an NTP Server 1-4
1-2-4 Reading the Clock Data 1-4
1-2-5 Logging 1-4
1-2-6 Related System-defined Variables 1-5

Section 2 Automatic Clock Adjustment

2-1 Automatic Clock Adjustment **2-2**

2-1-1 Overview 2-2
2-1-2 Specifications 2-2

2-2 Procedure to Use the Automatic Clock Adjustment Function 2-4
2-2-1 Procedure 2-4
2-2-2 Settings Required for Automatic Clock Adjustment 2-4

Section 3 Management Functions for NX Units

3-1 NX Bus Function Module 3-2
3-1-1 Status of NX Units Managed by the NX Bus Function Module as the NX Bus Master 3-2
3-1-2 I/O Data for Individual NX Units 3-4
3-1-3 Assigning Device Variables to I/O Ports 3-4

3-2 Mounting Settings of NX Units on the Communication Control Unit 3-7
3-2-1 Overview of Function 3-7
3-2-2 Setting NX Units as Unmounted Units 3-8

3-3 Restarting NX Units on the Communication Control Unit 3-9
3-3-1 Types of Restarts 3-9
3-3-2 Restarting an NX Unit 3-9

3-4 Fail-soft Operation for NX Units on the Communication Control Unit 3-10
3-4-1 Operations for Errors 3-11
3-4-2 Setting Fail-soft Operation 3-11
3-4-3 Errors to Which Fail-soft Operation Applies 3-11
3-4-4 Causes of Unit Configuration Verification Errors and Error Operation 3-12

3-5 Monitoring Total Power-ON Time for NX Units on the Communication Control Unit 3-13
3-5-1 Specifications of Monitoring Total Power-ON Times 3-13
3-5-2 Checking Total Power-ON Times 3-13

Section 4 SD Memory Card Operations

4-1 SD Memory Card Operations 4-2

4-2 Specifications of Supported SD Memory Cards, Folders, and Files 4-3
4-2-1 SD Memory Card Specifications 4-3
4-2-2 Folder and File Specifications 4-4

4-3 FTP Server 4-6
4-3-1 Overview and Specifications 4-6
4-3-2 FTP Server Function Details 4-7
4-3-3 Using the FTP Server Function 4-9
4-3-4 FTP Server Application Example 4-10
4-3-5 Using FTP Commands 4-11
4-3-6 Table of Commands 4-11
4-3-7 Using the Commands 4-12

4-4 File Operations from the Sysmac Studio 4-18

4-5 SD Memory Card Life Expiration Detection 4-19

4-6 SD Memory Card Self-diagnostic Functions 4-20

4-7 Exclusive Control of File Access in SD Memory Cards 4-22

Section 5 Security

5-1 Overview of Security Functions 5-2

5-2 Overall Project File Protection 5-3
5-2-1 Operating Procedure 5-3

5-3 Operation Authority Verification 5-4

5-3-1 Introduction 5-4
5-3-2 Operating Procedure 5-4
5-3-3 Specifications 5-4

5-4 Communication Control Unit Write Protection 5-6

5-5 Communication Control Unit Names and Serial IDs 5-8
5-5-1 Introduction 5-8
5-5-2 Setting Methods 5-8
5-5-3 Serial IDs 5-9

Section 6 Event Logs

6-1 Overview 6-2
6-1-1 Features 6-2

6-2 Detailed Information on Event Logs 6-3
6-2-1 Event Sources 6-3
6-2-2 Category 6-3
6-2-3 Number of Records 6-3
6-2-4 Event Codes 6-3
6-2-5 Event Levels 6-4
6-2-6 Displaying Event Logs 6-4
6-2-7 Clearing Event Logs 6-5
6-2-8 Exporting Event Logs 6-5

Section 7 Changing Event Levels

7-1 Overview of Changing Event Levels 7-2

7-2 Applications of Changing Event Levels 7-3

7-3 Events for Which the Event Level Can Be Changed 7-4

7-4 Procedure to Change an Event Level 7-5

Section 8 CIP Message Communications

8-1 Overview of the CIP Message Communications Service 8-2
8-1-1 Overview of the CIP Message Communications Service 8-2
8-1-2 Message Communications Service Specifications 8-2

8-2 CIP Communication Server Function 8-3
8-2-1 CIP Message Structure for Accessing CIP Objects 8-3
8-2-2 CIP Message Structure for Accessing Variables 8-4

8-3 Specifying Request Path 8-5
8-3-1 Examples of CIP Object Specifications 8-5
8-3-2 Examples of Variable Specifications 8-6
8-3-3 Logical Segment 8-6
8-3-4 Data Segment 8-6
8-3-5 Specifying Variable Names in Request Paths 8-7

8-4 CIP Object Services 8-11
8-4-1 CIP Objects Sent to the Built-in EtherNet/IP Port 8-11
8-4-2 Identity Object (Class ID: 01 hex) 8-11
8-4-3 NX Configuration Object (Class ID: 74 hex) 8-14
8-4-4 TCP/IP Interface Object (Class ID: F5 hex) 8-28
8-4-5 Ethernet Link Object (Class ID: F6 hex) 8-30
8-4-6 Controller Object (Class ID: C4 hex) 8-36

8-5 Read and Write Services for Variables 8-38
8-5-1 Read Service for Variables 8-38
8-5-2 Write Service for Variables 8-39

8-6 Variable Data Types 8-42
8-6-1 Data Type Codes 8-42
8-6-2 Common Format 8-42
8-6-3 Elementary Data Types 8-43
8-6-4 Derived Data Types 8-44

Section 9 TCP/UDP Message Service Function

9-1 Overview of the TCP/UDP Message Service Function 9-2
9-2 System Configuration for Using the TCP/UDP Message Service 9-3
9-3 TCP/UDP Message Service Specifications 9-4
9-3-1 TCP/IP and UDP/IP Message Format 9-4

Section 10 SNMP Agent

10-1 SNMP Agent 10-2
10-1-1 Overview 10-2
10-1-2 Specifications 10-3
10-1-3 SNMP Messages 10-3
10-1-4 MIB Specifications 10-4
10-2 Procedure to Use the SNMP Agent 10-20
10-2-1 Procedures 10-20
10-2-2 Settings Required for the SNMP Agent 10-20

Appendices

A-1 Sysmac Studio Settings for the Built-in EtherNet/IP Port A-2
A-1-1 **TCP/IP Settings** Display A-2
A-1-2 **LINK Settings** Display A-6
A-1-3 **FTP Settings** Display A-7
A-1-4 **NTP Settings** Display A-8
A-1-5 **SNMP Settings** Display A-9
A-1-6 **SNMP Trap Settings** Display A-11
A-1-7 **TCP/UDP Message Service Settings** Display A-13
A-2 Testing Communications A-14
A-2-1 PING Command A-14
A-2-2 Using the PING Command A-14
A-2-3 Host Computer Operation A-14
A-3 Variable Memory Allocation Methods A-16
A-3-1 Data Type Alignment and Memory Allocation Amounts A-16
A-3-2 Basic Data Types A-18
A-3-3 Arrays A-20
A-3-4 Structures A-21
A-3-5 Unions A-23
A-4 System-defined Variables A-25
A-4-1 System-defined Variables for the Overall Controller (No Category) A-26
A-4-2 PLC Function Module, Category Name: _PLC A-28
A-4-3 NX Bus Function Module, Category Name: _NXB A-29
A-4-4 EtherNet/IP Function Module, Category Name: _EIP A-31
A-4-5 Meanings of Error Status Bits A-51
A-5 Specifications for Individual System-defined Variables A-53
A-5-1 System-defined Variables for the Overall Controller (No Category) A-53
A-5-2 PLC Function Module, Category Name: _PLC A-56
A-5-3 NX Bus Function Module, Category Name: _NXB A-57
A-5-4 EtherNet/IP Function Module, Category Name: _EIP A-59

Index

Relevant Manuals

The following table provides the relevant manuals for this product. Read all of the manuals that are relevant to your system configuration and application before you use the product.
Most operations on this product are performed from the Sysmac Studio Automation Software. For details on the Sysmac Studio, refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)*.

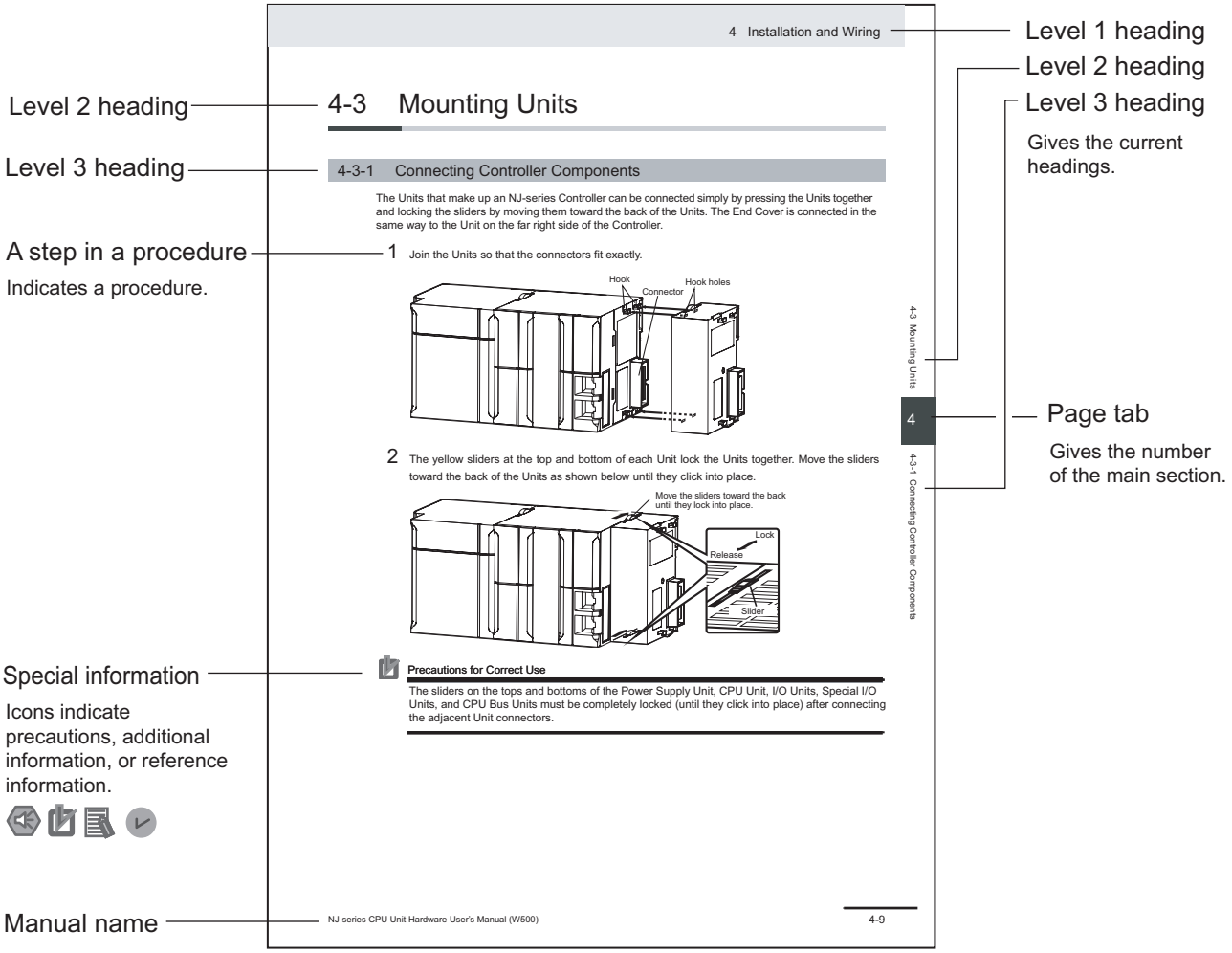
Purpose of use	NX-series Safety Control Unit User's Manual	NX-series Safety Control Unit / Communication Control Unit User's Manual	NX-series Communication Control Unit Built-in Function User's Manual	NX-series Safety Control Unit Instructions Reference Manual
Building a safety control system integrated with NJ/NX-series CPU Units	●			
Building a standalone safety control system with EtherNet/IP Coupler Units	●			
Building a safety network control system with Communication Control Units		●		
Introduction to Communication Control Unit	●	●		
Setting devices and hardware				
NX-SL5□□□ Safety CPU Unit	●	●		
NX-SL3□□□ Safety CPU Unit	●			
NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
NX-CSG□□□ Communication Control Unit		●		
Software settings				
NX-SL5□□□ Safety CPU Unit	●	●		
NX-SL3□□□ Safety CPU Unit	●			
NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
NX-CSG□□□ Communication Control Unit		●	●	
Creating safety programs	●	●		●
Testing operation and debugging				
Safety programs	●	●		●
Safety process data communications	●	●		
Safety I/O functions	●	●		
Tag data links		●		
Built-in functions for Communication Control Unit		●	●	
Learning about error corrections				
NX-SL5□□□ Safety CPU Unit	●	●		●
NX-SL3□□□ Safety CPU Unit	●			●
NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
NX-CSG□□□ Communication Control Unit		●		
Maintenance				

Purpose of use		NX-series Safety Control Unit User's Manual	NX-series Safety Control Unit / Communication Control Unit User's Manual	NX-series Communication Control Unit Built-in Function User's Manual	NX-series Safety Control Unit Instructions Reference Manual
	NX-SL5□□□ Safety CPU Unit	●	●		
	NX-SL3□□□ Safety CPU Unit	●			
	NX-SI□□□□ and NX-SO□□□□ Safety I/O Units	●	●		
	NX-CSG□□□ Communication Control Unit		●		

Manual Structure

Page Structure

The following page structure is used in this manual.



This illustration is provided only as a sample. It may not literally appear in this manual.

Special Information

Special information in this manual is classified as follows:

Precautions for Safe Use

Precautions on what to do and what not to do to ensure safe usage of the product.

Precautions for Correct Use

Precautions on what to do and what not to do to ensure proper operation and performance.

Additional Information

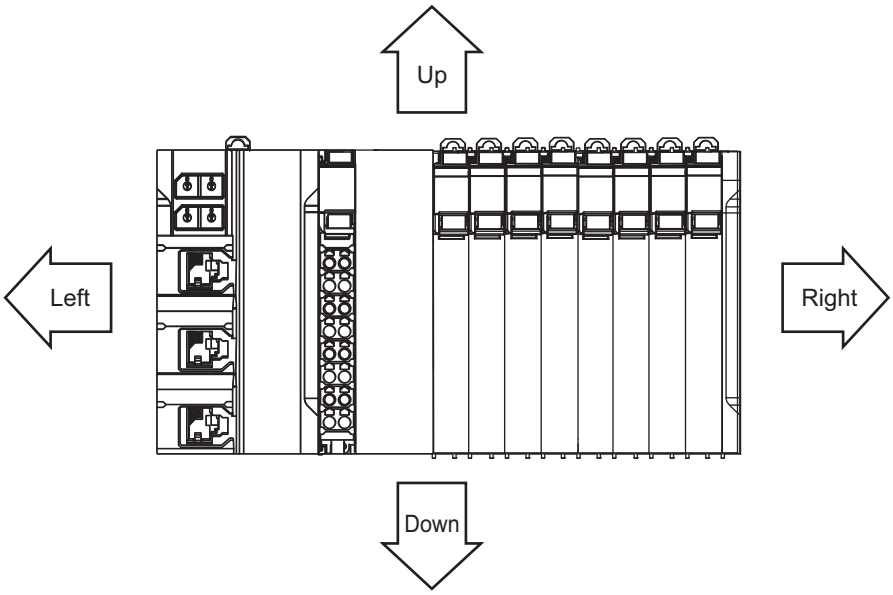
Additional information to read as required.
This information is provided to increase understanding or make operation easier.

Version Information

Information on differences in specifications and functionality for Controller with different unit versions and for different versions of the Sysmac Studio is given.

Precaution on Terminology

In this manual, the directions in relation to the Units are given in the following figure, which shows upright installation.



Terms and Conditions Agreement

Warranty, Limitations of Liability

Warranties

- **Exclusive Warranty**

  Omron's exclusive warranty is that the Products will be free from defects in materials and workmanship for a period of twelve months from the date of sale by Omron (or such other period expressed in writing by Omron). Omron disclaims all other warranties, express or implied.

- **Limitations**

  OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, ABOUT NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE PRODUCTS. BUYER ACKNOWLEDGES THAT IT ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE.

  Omron further disclaims all warranties and responsibility of any type for claims or expenses based on infringement by the Products or otherwise of any intellectual property right.

- **Buyer Remedy**

  Omron's sole obligation hereunder shall be, at Omron's election, to (i) replace (in the form originally shipped with Buyer responsible for labor charges for removal or replacement thereof) the non-complying Product, (ii) repair the non-complying Product, or (iii) repay or credit Buyer an amount equal to the purchase price of the non-complying Product; provided that in no event shall Omron be responsible for warranty, repair, indemnity or any other claims or expenses regarding the Products unless Omron's analysis confirms that the Products were properly handled, stored, installed and maintained and not subject to contamination, abuse, misuse or inappropriate modification. Return of any Products by Buyer must be approved in writing by Omron before shipment. Omron Companies shall not be liable for the suitability or unsuitability or the results from the use of Products in combination with any electrical or electronic components, circuits, system assemblies or any other materials or substances or environments. Any advice, recommendations or information given orally or in writing, are not to be construed as an amendment or addition to the above warranty.

  See https://www.omron.com/global/ or contact your Omron representative for published information.

Limitation on Liability; Etc

OMRON COMPANIES SHALL NOT BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR PRODUCTION OR COMMERCIAL LOSS IN ANY

WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE OR STRICT LIABILITY.

OMRON SHALL NOT BE RESPONSIBLE AND/OR LIABLE FOR ANY LOSS, DAMAGE, OR EXPENSES DIRECTLY OR INDIRECTLY RESULTING FROM THE INFECTION OF OMRON PRODUCTS, ANY SOFTWARE INSTALLED THEREON OR ANY COMPUTER EQUIPMENT, COMPUTER PROGRAMS, NETWORKS, DATABASES OR OTHER PROPRIETARY MATERIAL CONNECTED THERETO BY DISTRIBUTED DENIAL OF SERVICE ATTACK, COMPUTER VIRUSES, OTHER TECHNOLOGICALLY HARMFUL MATERIAL AND/OR UNAUTHORIZED ACCESS.

It shall be the users sole responsibility to determine and use adequate measures and checkpoints to satisfy the users particular requirements for (i) antivirus protection, (ii) data input and output, (iii) maintaining a means for reconstruction of lost data, (iv) preventing Omron Products and/or software installed thereon from being infected with computer viruses and (v) protecting Omron Products from unauthorized access.

Further, in no event shall liability of Omron Companies exceed the individual price of the Product on which liability is asserted.

Application Considerations

Suitability of Use

Omron Companies shall not be responsible for conformity with any standards, codes or regulations which apply to the combination of the Product in the Buyer’s application or use of the Product. At Buyer’s request, Omron will provide applicable third party certification documents identifying ratings and limitations of use which apply to the Product. This information by itself is not sufficient for a complete determination of the suitability of the Product in combination with the end product, machine, system, or other application or use. Buyer shall be solely responsible for determining appropriateness of the particular Product with respect to Buyer’s application, product or system. Buyer shall take application responsibility in all cases.

NEVER USE THE PRODUCT FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY OR IN LARGE QUANTITIES WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCT(S) IS PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

Programmable Products

Omron Companies shall not be responsible for the user’s programming of a programmable Product, or any consequence thereof.

Disclaimers

Performance Data

Data presented in Omron Company websites, catalogs and other materials is provided as a guide for the user in determining suitability and does not constitute a warranty. It may represent the result of Omron's test conditions, and the user must correlate it to actual application requirements. Actual performance is subject to the Omron's Warranty and Limitations of Liability.

Change in Specifications

Product specifications and accessories may be changed at any time based on improvements and other reasons. It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without any notice. When in doubt, special part numbers may be assigned to fix or establish key specifications for your application. Please consult with your Omron's representative at any time to confirm actual specifications of purchased Product.

Errors and Omissions

Information presented by Omron Companies has been checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical or proofreading errors or omissions.

Statement of security responsibilities for assumed use cases and against threats

OMRON SHALL NOT BE RESPONSIBLE AND/OR LIABLE FOR ANY LOSS, DAMAGE, OR EXPENSES DIRECTLY OR INDIRECTLY RESULTING FROM THE INFECTION OF OMRON PRODUCTS, ANY SOFTWARE INSTALLED THEREON OR ANY COMPUTER EQUIPMENT, COMPUTER PROGRAMS, NETWORKS, DATABASES OR OTHER PROPRIETARY MATERIAL CONNECTED THERETO BY DISTRIBUTED DENIAL OF SERVICE ATTACK, COMPUTER VIRUSES, OTHER TECHNOLOGICALLY HARMFUL MATERIAL AND/OR UNAUTHORIZED ACCESS.

It shall be the users sole responsibility to determine and use adequate measures and checkpoints to satisfy the users particular requirements for (i) antivirus protection, (ii) data input and output, (iii) maintaining a means for reconstruction of lost data, (iv) preventing Omron Products and/or software installed thereon from being infected with computer viruses and (v) protecting Omron Products from unauthorized access.

Safety Precautions

Refer to the following manual for details on safety precautions.
NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)

Precautions for Safe Use

Refer to the following manuals for precautions for safe use.
NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)

Precautions for Correct Use

Refer to the following manuals for precautions for correct use.
NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)

Regulations and Standards

Refer to the following manual for the standards that the NX-series Communication Control Unit is certified for.
NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)

Versions

Hardware revisions and unit versions are used for version control of hardware and software of NX-series Communication Control Units. The hardware revision or unit version is updated each time any change is made to hardware or software specifications. Accordingly, Communication Control Units of the same model may have functional or performance differences, depending on their hardware revisions and unit versions.

Checking Versions

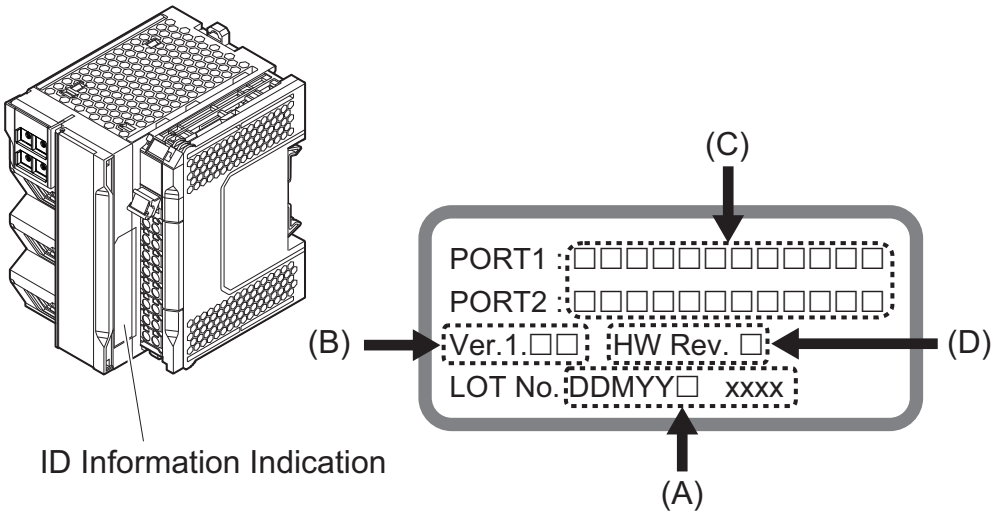
You can check versions on the ID information indications or with the Sysmac Studio.

Checking Unit Versions on ID Information Indications

The unit version is given on the ID information indication on the side of the product.

● Communication Control Unit

ID Information is given with the ID information indication on the side of the Unit.



Letter	Name	Function
A	Lot number and serial number	Gives the lot number and the serial number of the Unit. DDMYY: Lot number, □: Used by OMRON, SSSS: Serial number “M” gives the month (1 to 9: January to September, X: October, Y: November, Z: December)
B	Unit version	Gives the unit version of the Unit.
C	MAC addresses	Gives the MAC addresses of the built-in EtherNet/IP port (port 1) and the built-in EtherNet/IP port (port 2) on the Unit.
D	Hardware revision	Gives the hardware revision of the Unit. *1

*1. The hardware revision is not displayed for the Unit that the hardware revision is in blank.

Checking Unit Versions with the Sysmac Studio

You can check unit versions with the Sysmac Studio.

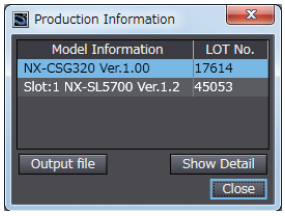
● Checking the Unit Version of a Communication Control Unit

You can use the Production Information while the Sysmac Studio is online to check the unit version of a Unit. You can do this for the Communication Control Unit, NX Units on the CPU Rack.

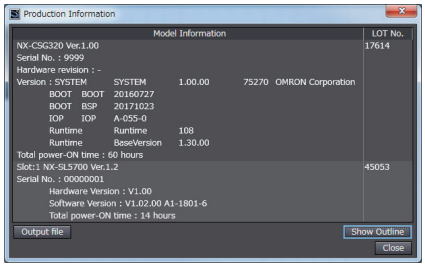
1 Right-click **CPU Rack** under **Configurations and Setup - CPU/Expansion Racks** in the Multi-view Explorer and select **Display Production Information**.
The Production Information Dialog Box is displayed.

● Changing Information Displayed in Production Information Dialog Box

1 Click the **Show Detail** or **Show Outline** Button at the lower right of the Production Information Dialog Box.
The view will change between the production information details and outline.



Outline View



Detail View

The information that is displayed is different for the Outline View and Detail View. The Detail View displays the unit version, hardware revision, and various versions. The Outline View displays only the unit version.

Note The hardware revision is separated by "/" and displayed on the right of the hardware version. The hardware revision is not displayed for the Unit that the hardware revision is in blank.

Unit Versions of Units and Sysmac Studio Versions

The functions that are supported depend on the unit version of the NX-series Communication Control Unit. The version of Sysmac Studio that supports the functions that were added for an upgrade is also required to use those functions.
Refer to the *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)* for the relationship between the unit versions of the Units and the Sysmac Studio versions, and for the functions that are supported by each unit version.

Related Manuals

The followings are the manuals related. Use these manuals for reference.

Manual name	Cat. No.	Model numbers	Application	Description
NX-series Safety Control Unit / Communication Control Unit User's Manual	Z395	NX-SL5□□□ NX-SI□□□□ NX-SO□□□□ NX-CSG□□□	Learning how to use the NX-series Safety Control Units and Communication Control Units.	Describes the hardware, setup methods, and functions of the NX-series Safety Control Units and Communication Control Units.
NX-series Communication Control Unit Built-in Function User's Manual	Z396	NX-CSG□□□	Learning about the built-in functions of an NX-series Communication Control Unit.	Describes the software setup methods and communicantions functions of an NX-series Communication Control Unit.
GI-S Series Safety I/O Terminal User's Manual	Z400	GI-S□□□□□□	Learning how to use the GI-S Series Safety I/O Terminals.	Describes the hardware, setup methods, and functions of the GI-S Series Safety I/O Terminals.
Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for CIP Safety User's Manual	W645	NXR-SXD1204□-CST	Learning how to use the NXR-S Series Simple Logic Safety I/O Block.	Describes the hardware, setup methods, and functions of the NXR-S Series Simple Logic Safety I/O Block.
Environment-resistive Remote Terminal NXR-S-series Simple Logic Safety I/O Block for EtherNet/IP User's Manual	W646	NXR-SXD1204-EIT		
NX-series Safety Control Unit Instructions Reference Manual	Z931	NX-SL□□□□	Learning about the specifications of instructions for the Safety CPU Unit.	Describes the instructions for the Safety CPU Unit.
NX-series Digital I/O Units User's Manual	W521	NX-ID□□□□ NX-IA□□□□ NX-OC□□□□ NX-OD□□□□ NX-MD□□□□	Learning how to use NX-series Digital I/O Units.	The hardware, setup methods, and functions of the NX-series Digital I/O Units are described.
NX-series Analog I/O Units User's Manual for Analog Input Units and Analog Output Units	W522	NX-AD□□□□ NX-DA□□□□	Learning how to use NX-series Analog Input Units and Analog Output Units.	The hardware, setup methods, and functions of the NX-series Analog Input Units and Analog Output Units are described.
NX-series Analog I/O Units User's Manual for Temperature Input Units and Heater Burnout Detection Units	W566	NX-TS□□□□ NX-HB□□□□	Learning how to use NX-series Temperature Input Units and Heater Burnout Detection Units.	The hardware, setup methods, and functions of the NX-series Temperature Input Units and Heater Burnout Detection Units are described.
NX-series Data Reference Manual	W525	NX-□□□□□□	Referencing lists of the data that is required to configure systems with NX-series Units.	Lists of the power consumptions, weights, and other NX Unit data that is required to configure systems with NX-series Units are provided.
Sysmac Studio Version 1 Operation Manual	W504	SYSMAC -SE2□□□	Learning about the operating procedures and functions of the Sysmac Studio.	Describes the operating procedures of the Sysmac Studio.

Manual name	Cat. No.	Model numbers	Application	Description
NX-series System Units User’s Manual	W523	NX-PD1□□□ NX-PF0□□□ NX-PC0□□□ NX-TB□□□X	Learning how to use NX-series System Units	The hardware and functions of the NX-series System Units are described.

Terminology

Term	Description
standard	The generic term for devices, functions, and data that are used for general control purposes as opposed to those that are used for safety measures.
safety function	A function that is executed by the safety control system to achieve a safe state for a machine hazard.
safe state	The status of a device or piece of equipment when the risk of danger to humans has been reduced to an acceptable level.
safety signal	A signal that is used for safety controls. In this safety control system, the data type of a variable determines whether a signal is related to the safety controls. Broadly speaking, there are two data types: safety data types and standard data types.
standard signal	A signal or data that is used for general control purposes.
Safety data type	The data type for a safety signal.
Standard data type	The data type for a standard signal.
safety reaction time	The time required for the system to enter a safe state in a worst-case scenario after the occurrence of a safety-related input (press of an emergency stop pushbutton switch, interruption of a light curtain, opening of a safety door, etc.) or device failure. The reaction time of the system includes the reaction times of sensors and actuators, just like the reaction time for a Controller or network.
safety control	A type of control that uses devices, functions, and data that are designed with special safety measures.
standard control	A type of control that use devices, functions, and data that are designed for general control purposes. This term is used to differentiate from a safety control
safety process data communications	A type of I/O data communications that is used for safety control purposes.
standard process data communications	A type of I/O data communications that is used for standard control purposes.
Safety I/O connection	A type of connections that is used for safety process data communications.
CIP Safety connection	Safety I/O connection that is used to transmit safety process data by the communication protocol called CIP Safety. CIP Safety originator connection and CIP Safety target connection are available depending on the roles of communications.
CIP Safety originator connection	A CIP Safety connection when an own node is a CIP Safety originator.
CIP Safety target connection	A CIP Safety connection when an own node is a CIP Safety target.
CIP Safety originator	A role in CIP Safety communications. A CIP Safety originator manages a CIP Safety connection for a CIP Safety target. CIP Safety originator exists in a connection unit, and not in a device unit.
CIP Safety target	A role in CIP Safety communications. A CIP Safety target receives a request to open a CIP Safety connection from a CIP Safety originator. CIP Safety target exists in a connection unit, and not in a device unit.
single-cast connection	A safety process data communications method in CIP Safety. A CIP Safety originator and a CIP Safety target communicate one-to-one in this connection. You can apply this setting for both of input data and output data.
multi-cast connection	A safety process data communications method in CIP Safety. A CIP Safety target sends the input data of the CIP Safety target in multi-cast to multiple CIP Safety originators in this connection. This is a connection type you can set only for input data of a CIP Safety target. You cannot apply this setting for output data.
FSoE master connection	Master safety I/O connection that is used to transmit safety process data by the communication protocol called FSoE.
safety master connection	The generic term for the CIP Safety originator connection and the FSoE master connection.
exposing global variables to the Communication Control Unit	Exposing specified global variables to the Communication Control Unit to allow the exchange of standard signals between the standard controller and the Safety CPU Unit. Exposed variables can be transmitted to the standard controller via tag data links.
Safety Control Unit	The generic term for a Unit that is used in safety controls.
Safety CPU Unit	A CPU Unit that is used for safety controls. This is a type of NX Unit.

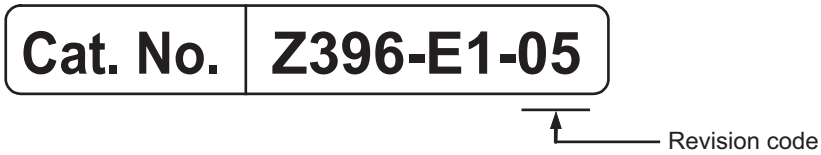
Term	Description
Safety I/O Unit	An I/O Unit that is used for safety controls. This is a type of NX Unit.
safety input device	An input device that is designed with special safety measures for use in safety controls. The generic term for safety input devices, such as emergency stop pushbutton switches and safety switches.
safety output device	An output device that is designed with special safety measures for use in safety controls. The generic term for safety output devices, such as safety relays.
EtherNet/IP Slave Terminal	An EtherNet/IP Slave Unit Terminal is a building-block slave that is created by mounting a group of NX Units.
Communication Control Unit	The generic term for the interface units to have CIP Safety communications on a network between the Safety CPU Unit and CIP Safety on EtherNet/IP devices.
Safety Network Controller	The generic term for the building-block type safety controllers that have mounted the Safety Control Unit with the Communication Control Unit.
Safety program	User programming for safety controls in the Safety CPU Unit. This term is used to differentiate from the user program of the standard controller. Safety programs are programmed in the FBD language.
FBD language	The abbreviation for the function block diagram programming language. This is a graphical language used to program algorithms with connecting lines that represent the flow of inputs and data, and rectangular boxes that represent functions or function blocks. Unlike the ladder diagram language, the FBD language does not have bus bars, and the connecting lines represent the flow of inputs and data rather than the power flow. Algorithms are executed in order from top to bottom in units that are called networks. A network consists of configuration elements that use connecting lines to connect inputs to outputs. The FBD language does not have an END instruction. Execution for the task period ends when the last network is executed. You use the FBD language to write safety programs for the Safety CPU Unit.
user program	All of the programs that are created by the user. User program refers to the programs for standard controls of the standard controller and the safety program of the Safety CPU Unit.
operating mode	The status of the Safety CPU Unit, when it is in normal operation, that the user changes to run or check the operation of the Safety CPU Unit. There are the three modes: PROGRAM mode, DEBUG mode, and RUN mode. You can use DEBUG mode only when the Sysmac Studio is online with the Safety CPU Unit.
safety validation	The process of appending confirmation information to the safety application data if safety validation testing demonstrates that the safety controls meet the required specifications of a safety system. You execute the safety validation from the Sysmac Studio when the Safety CPU Unit is in DEBUG mode. The validated safety programs are automatically transferred to the non-volatile memory of the Safety CPU Unit.
DEBUG mode	The mode that is used to debug unvalidated safety programs. DEBUG mode is only available when the Sysmac Studio is online with the Safety CPU Unit. Use this mode to check that the safety programs and external devices operate correctly. After you confirm that the system meets the required specifications, perform the safety validation. This will enable you to change to RUN mode. When you change from PROGRAM mode to DEBUG mode, the unvalidated safety programs are automatically transferred to the main memory of the Safety CPU Unit.
DEBUG mode (RUN)	A status that indicates that an unvalidated safety program is in execution in DEBUG mode. You can control BOOL variables, use forced refreshing, and change present values.
DEBUG mode (STOPPED)	A status that indicates that an unvalidated safety program is stopped in DEBUG mode. You can control BOOL variables, use forced refreshing, and change present values.
PROGRAM mode	A mode indicates that execution of the safety program is stopped. You cannot control BOOL variables, use forced refreshing, or change present values.
RUN mode	A mode that indicates that execution of the validated safety programs is in progress. Unlike DEBUG mode (RUN), the validated safety programs in the non-volatile memory of the Safety CPU Unit are executed. You cannot control BOOL variables, use forced refreshing, or change present values.
before safety validation	A status that indicates that safety validation has not been performed on the safety application data from the Sysmac Studio because it has not yet been determined whether the safety controls meet the required specifications of the safety system.

Term	Description
after safety validation	A status indicates that safety validation has been performed on the safety application data from the Sysmac Studio because it has been determined that the safety controls meet the required specifications of the safety system.
CPU Rack	A Rack to which a CPU Unit or Communication Control Unit is mounted. For NX-series CPU Units to which NX Units can be connected, a CPU Rack has a CPU Unit with NX Units and an End Cover mounted to it. For NX-series Communication Control Units, a CPU Rack has a Communication Control Unit with NX Units and an End Cover mounted to it.
CPU Rack settings	It consists of the following data: • Configuration information • Unit operation settings • Unit application data
configuration information	It consists of the following data: • Unit configuration information • I/O allocation information
I/O allocation information	The set of information that specifies the I/O data to be processed by I/O refreshing. On the Sysmac Studio, this is shown as configuration information and includes the Unit configuration information.
Unit configuration information	The set of information that specifies the configuration of the NX Units that are connected to the NX bus master. On the Sysmac Studio, this is shown as configuration information and includes the I/O allocation information.
safety application data	The data that contains the settings that are used to operate the NX-series Safety Control Units. It consists of the safety programs, safety task, and variables. You use the Sysmac Studio to create this data, and then transfer and execute it on the Safety CPU Unit. On the Sysmac Studio, this data is shown as the slave parameters. The location where the safety application data is stored on the Safety CPU Unit depends on whether the safety programs have been validated. (Unvalidated safety programs are stored in the main memory, while validated safety programs are stored in the non-volatile memory.)
safety input function	A function that evaluates whether the signals that are input on a safety input terminal are normal or abnormal. Specific safety evaluation functions include test pulse evaluation and dual channel evaluation. When the evaluation result shows an abnormality, the safety input data is made inactive (OFF).
safety output function	A function that evaluates whether the values of safety output data and the output signals on safety output terminals are normal or abnormal. Specific safety evaluation functions include test pulse evaluation and dual channel evaluation. When the evaluation result shows an abnormality, the output signal on the safety output terminal is turned OFF.
dual channel evaluation	This function uses a pair of safety input or safety output terminals as redundant terminals that are checked for consistency to evaluate the status of the safety input or safety output.
single channel	The input or output is used as a single point.
dual channels	Two inputs or outputs are used as a pair of points for redundancy.
test pulse evaluation	This function outputs a test pulse that is used to evaluate a safety input or safety output for failures or wiring errors with the connected external device.
change tracking	A pin is used to manage whether the safety application data has been changed after the finalized data is created.
UNID	An ID assigned to a device so that it can be uniquely identified by all the networks on the safety system for CIP Safety communications. An UNITD is a 10-byte value, consisting of a 6-byte Safety Network Number and a 4-byte Node ID.
Safety Network Number (SNN)	A number assigned to a safety network so that it can be uniquely identified for CIP Safety communications. The Safety Network Number is set for the NX bus, the built-in EtherNet/IP ports 1 and 2.

Term	Description
Node ID	An ID assigned to each of devices on a network so that the devices with the same Safety Network Number (SNN) can be uniquely identified for CIP Safety communications. The Safety CPU Unit is the only CIP Safety device on the NX bus, and the Node ID is always *1*. For a CIP Safety device on an EtherNet/IP network, its IP address is used as the Node ID.

Revision History

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



Revision code	Date	Revised content
01	April 2018	Original production
02	April 2022	• Corrected descriptions related to SD Memory Cards.
03	July 2024	• Corrected mistakes.
04	July 2026	• Made revisions accompanying the upgrade to Sysmac Studio version 1.67.
05	October 2026	• Corrected mistakes.

1

Data Management and Clock Functions

This section describes the data management and clock functions.

1-1 Clearing All Memory 1-2

1-2 Clock 1-3

1-2-1 Overview 1-3
1-2-2 Setting the Clock Data 1-3
1-2-3 Correcting the Clock from an NTP Server 1-4
1-2-4 Reading the Clock Data 1-4
1-2-5 Logging 1-4
1-2-6 Related System-defined Variables 1-5

1-1 Clearing All Memory

You can initialize the Controller Configurations and Setup and variables in the Communication Control Unit to the defaults from the Sysmac Studio. This is called the *Clear All Memory* operation.

Precautions for Correct Use

- You cannot execute the *Clear All Memory* operation when write protection of the CPU Unit is set in the security functions.
- Do not turn OFF the power supply to the Communication Control Unit during the Clear All Memory operation.

After you clear the memory, the Controller operates in the same way as immediately after you create the system configuration with the Communication Control Unit in the factory default condition.

Operations from the Sysmac Studio

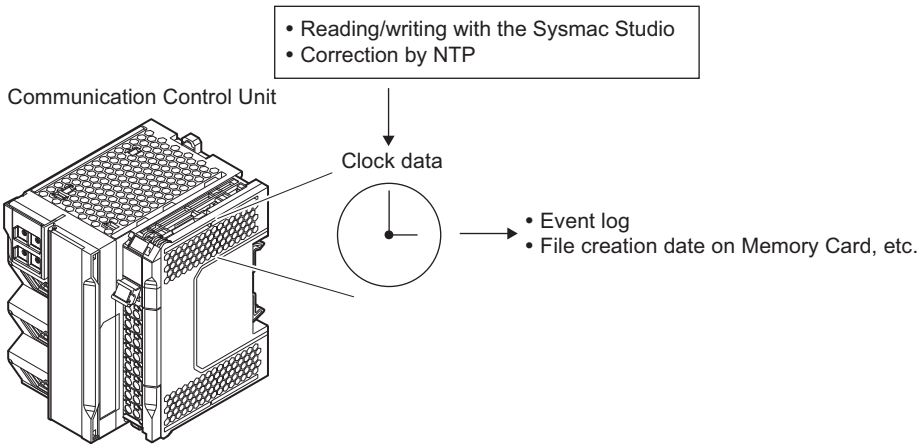
Connect the Sysmac Studio to the Communication Control Unit online, and select the **Clear All Memory** from the **Controller** Menu.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for specific procedures.

1-2 Clock

1-2-1 Overview

A clock (RTC) is built into the Communication Control Unit.
The clock data from this clock is used for timestamps in the event logs and for the time and date of files that are created on the SD Memory Card.
The following functions are supported.

- Reading/writing the clock from the Sysmac Studio
- Reading the clock from system-defined variables (Writing is not possible.)
- Correcting the clock from an NTP server



Precautions for Correct Use

The clock data is retained by a built-in capacitor in the Communication Control Unit. When the power of the device is turned OFF if the retention time in the built-in capacitor is exceeded, the clock data are initialized. If you use the clock data in the event log and other functions, specify the clock data when you turn ON the power supply every time.

Clock Data Range

- 1970-01-01 to 2069-12-31 (January 1, 1970 to December 31, 2069).

Setting the Time Zone and the Local Time

Before you use the Controller for the first time, set the time zone and local time in the clock data.
You can set the time zone and local time from the Sysmac Studio in the Controller Clock Dialog Box.

1-2-2 Setting the Clock Data

Use one of the following methods.

Changing Clock Data from the Sysmac Studio

You can use the Sysmac Studio to synchronize the clock data of the built-in clock with the clock on the computer.

Changing the Clock Data from an NTP Server

You can use an NTP server on EtherNet/IP to set the clock data.

1-2-3 Correcting the Clock from an NTP Server

Application

In a network system, the clock data must be shared by the entire system. NTP is supported to enable easy time synchronization.

Specifications

An NTP client is provided.
Refer to *Section 2 Automatic Clock Adjustment* on page 2-1 for details.

1-2-4 Reading the Clock Data

If the clock data is incorrect, the incorrect value is read.

Reading the Clock from System-defined Variables (Writing Is Not Possible)

You can use the following system-defined variable to read the clock data.
_CurrentTime (System Time)
For the details on how to read, refer to *8-5 Read and Write Services for Variables* on page 8-38.

Sysmac Studio Procedure

You can select **Controller Clock** from the Controller Menu of the Sysmac Studio to display the clock data.

1-2-5 Logging

When you change the clock data, an event is recorded in the event log.
However, nothing is recorded in the event log if the time is corrected for the NTP.

1-2-6 Related System-defined Variables

Variable names	Meaning	Function	Data type	R/W
_CurrentTime	System Time	This variable contains the Communication Control Unit's internal clock data.	DATE_AND_TIME	R

2

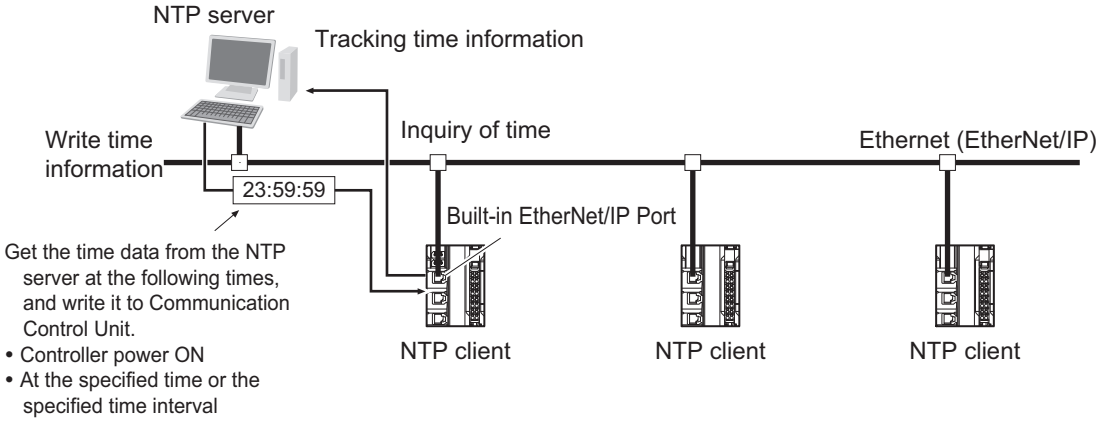
Automatic Clock Adjustment

2-1 Automatic Clock Adjustment 2-2
2-1-1 Overview 2-2
2-1-2 Specifications 2-2
2-2 Procedure to Use the Automatic Clock Adjustment Function 2-4
2-2-1 Procedure 2-4
2-2-2 Settings Required for Automatic Clock Adjustment 2-4

2-1 Automatic Clock Adjustment

2-1-1 Overview

The built-in EtherNet/IP port reads clock information from the NTP server and updates the internal clock time in the Communication Control Unit at the specified time or at a specified interval after the power supply to the Controller is turned ON.

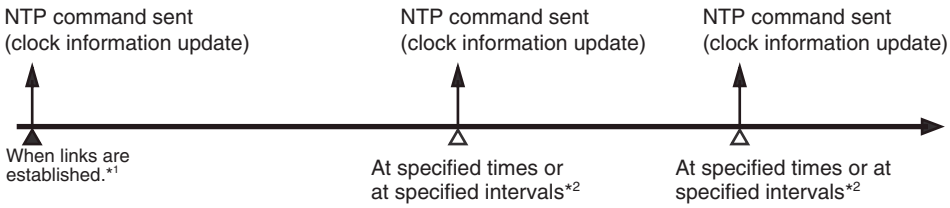


The NTP (Network Time Protocol) server is used to control the time on the LAN.

2-1-2 Specifications

Item	Specification	
Protocol	NTP	
Port No.	123 (UDP) However, you can change the port number in the Built-in EtherNet/IP Port Settings on the Sysmac Studio.	
Access to NTP server	Writes the clock information from the NTP server to the local Communication Control Unit.	Obtains the clock information from the NTP server set up on the Network, and applies the information obtained to the local Communication Control Unit.
NTP Operation Timing	Clock information is automatically updated at the following times if the NTP function is used. • After links are established when the power supply to the Controller is turned ON • At specified times or at specified intervals (according to the option selected for the **NTP operation timing**)	

Clock information is updated at the following times.



*1. This is performed when the **Get** Option is selected for the **NTP server clock information** in the **NTP Settings** Display.
*2. Depends on the option set for the **NTP operation timing** in the **NTP Settings** Display.

Additional Information

- NTP clock synchronization is normally performed as follows:
  - If the clock deviation is within 128 ms: The clock is synchronized every 0.5 ms.
  - If the clock deviation exceeds 128 ms: The clock is synchronized immediately.
- If the NTP operation timing is set for a specified time interval, the timing will not change even if the time in the Communication Control Unit is changed during operation.
  (For example, if the time interval is set to 60 minutes, the information is updated 60 minutes after the last time it was updated even if the time in the Communication Control Unit is changed.)

2-2 Procedure to Use the Automatic Clock Adjustment Function

2-2-1 Procedure

1 Select **Controller Setup** - **Built-in EtherNet/IP Port Settings** on the Sysmac Studio.
Set the following on the **NTP Settings** Display.
- NTP server settings (required)
- NTP operation timing

2 Select **Synchronization** from the **Controller** Menu. The built-in EtherNet/IP port settings are transferred to the Communication Control Unit.

2-2-2 Settings Required for Automatic Clock Adjustment

The following Built-in EtherNet/IP Port Settings are made from the Sysmac Studio to use automatic clock adjustment.

Tab page	Setting		Setting conditions	Reference
NTP	NTP server clock information		Required.	page A-8
	Port No.		Specified by user.*1	
	Server specifying method		Required	
		IP address	One of these must be set, depending on the **Server specification type** setting.	
		Host name		
	NTP operation timing		Required	
		Specify a Time	One of these must be set. (Set according to the **NTP operation timing**.)	
		Specify a time interval		
		Timeout time	Specified by user.*2	

*1. Required to change from the default value of 123.
*2. Required to change from the default value of 10 seconds.

Additional Information

Make the settings in the **NTP Settings** Display if automatic clock adjustment is used. Refer to *A-1-4* ***NTP Settings*** *Display* on page A-8 for information on the **NTP Settings** Display.

3

Management Functions for NX Units

This section describes the management functions used for NX Units on Communication Control Unit.

3-1 NX Bus Function Module 3-2
3-1-1 Status of NX Units Managed by the NX Bus Function Module as the NX Bus Master 3-2
3-1-2 I/O Data for Individual NX Units 3-4
3-1-3 Assigning Device Variables to I/O Ports 3-4

3-2 Mounting Settings of NX Units on the Communication Control Unit 3-7
3-2-1 Overview of Function 3-7
3-2-2 Setting NX Units as Unmounted Units 3-8

3-3 Restarting NX Units on the Communication Control Unit 3-9
3-3-1 Types of Restarts 3-9
3-3-2 Restarting an NX Unit 3-9

3-4 Fail-soft Operation for NX Units on the Communication Control Unit 3-10
3-4-1 Operations for Errors 3-11
3-4-2 Setting Fail-soft Operation 3-11
3-4-3 Errors to Which Fail-soft Operation Applies 3-11
3-4-4 Causes of Unit Configuration Verification Errors and Error Operation 3-12

3-5 Monitoring Total Power-ON Time for NX Units on the Communication Control Unit 3-13
3-5-1 Specifications of Monitoring Total Power-ON Times 3-13
3-5-2 Checking Total Power-ON Times 3-13

3-1 NX Bus Function Module

The NX Bus Function Module performs processing such as a management of event logging, management of status, and I/O refreshing for the NX Units that are connected to the NX bus of the Communication Control Unit as a master of the NX bus (hereafter NX bus master).

For I/O data that are handled by the NX Bus Function Module, there are two kinds of I/O data, the status of NX Units managed by the NX Bus Function Module as the NX bus master and I/O data for individual NX Units. The variables are the assignable I/O ports for both of them.

Device variables assigned to the I/O ports are used to access the I/O data.

The following describes the status of NX Units managed by the NX Bus Function Module as the NX bus master, I/O data for individual NX Units, assigning device variables to I/O ports, and programming sample using device variables.

3-1-1 Status of NX Units Managed by the NX Bus Function Module as the NX Bus Master

For the status of NX Units managed by the NX Bus Function Module as the NX bus master, you can use device variables assigned to I/O ports to access.

A List of Status of NX Units Managed by the NX Bus Function Module as the NX Bus Master

Name	I/O port
NX Unit Registration Status	NX Unit Registration Status
NX Unit Message Enabled Status	NX Unit Message Enabled Status
NX Unit I/O Data Active Status	NX Unit I/O Data Active Status
NX Unit Error Status	NX Unit Error Status

Descriptions of Status of NX Units Managed by the NX Bus Function Module as the NX Bus Master

Name	Description
NX Unit Registration Status	This status tells whether the NX Units are registered in the Unit configuration. Each bit has the following meaning. TRUE: Registered FALSE: Not registered If the Unit configuration information is registered, the status is TRUE for each Unit that is registered. If the Unit configuration information was automatically created (with only the actual Unit configuration information and no registered information), the status is FALSE for all Units. The status is TRUE for NX Units that are set as unmounted Units. Each bit is updated at the following times. • If the Unit Configuration Information Is Registered: The status changes to TRUE when the system is started. The status changes to FALSE when the configuration information is cleared. • If the Unit Configuration Information Is Automatically Created: The status changes to TRUE when the configuration information is confirmed. The status is always FALSE if the Unit configuration information is automatically created.
NX Unit Message Enabled Status	This status tells whether the NX Units can process message communications. Each bit has the following meaning. TRUE: Message communications possible. FALSE: Message communications not possible. The status says that message communications are enabled for NX Units that meet the following conditions. • The comparison shows no differences (only if the Unit configuration information is registered). • The NX Unit does not have a WDT error. The status is FALSE for NX Units that are set as unmounted Units. Each bit is updated when the message communications status changes on the corresponding NX Unit.
NX Unit I/O Data Active Status	This status tells whether the NX Units can process I/O data communications. Each bit has the following meaning. TRUE: The I/O data in the NX Unit can be used for control. FALSE: The I/O data in the NX Unit cannot be used for control. The status is FALSE for NX Units that are set as unmounted Units. Each bit is updated when the operating status changes on the corresponding NX Unit. If both of NX Unit Registration Status and NX Unit I/O Data Active Status are TRUE, the target NX Units operate normally.

Name	Description
NX Unit Error Status	This status tells whether an error exists on the NX Units. Each bit has the following meaning. TRUE: Error FALSE: No error Each bit is set to TRUE when the level of the error is as follows: • Major fault • Partial fault • Minor fault • Observation The status is FALSE for NX Units that are set as unmounted Units. Each bit is updated at the following times. The status changes to TRUE when an error occurs. The status changes to FALSE when the error is reset. Even if the cause of the error has been removed, you must reset the error for the status to change to FALSE.

3-1-2 I/O Data for Individual NX Units

I/O data are determined by the model number of the NX Unit and the functionality. You can use only device variables that are assigned to an I/O port of an NX Unit to access I/O data.

Refer to the user's manual for the specific NX Units for details on I/O data for individual NX Units.

3-1-3 Assigning Device Variables to I/O Ports

When you create the Unit configuration information on the Sysmac Studio, the status of NX Units managed by the NX Bus Function Module as the NX bus master and I/O data for NX Units mounted on the Communication Control Unit are automatically registered as I/O ports.
The variables that are assigned to I/O ports for status and I/O data are device variables.

I/O Port Names

The status of NX Units managed by the NX Bus Function Module as the NX bus master is given as the following six kinds of I/O port names for each NX Unit.

Name	I/O port name	Data type
NX Unit Registration Status	Device name + NX Unit Registration Status	BOOL
NX Unit Message Enabled Status	Device name + NX Unit Message Enabled Status	BOOL
NX Unit I/O Data Active Status	Device name + NX Unit I/O Data Active Status	BOOL
NX Unit Error Status	Device name + NX Unit Error Status	BOOL

Example for NX Unit Registration Status with a device name N1:
N1 NX Unit Registration Status
Example for Time Stamp of Synchronous Input with a device name N2:
N2 Time Stamp of Synchronous Input

I/O port names are determined by the model number of the NX Unit and the functionality for I/O data for NX Units mounted on the Communication Control Unit.

Example for a Digital Input Unit:

Input Bit 00
Example for an Analog Output Unit:
Ch1 Analog Output Value

Registering Device Variables

You assign device variables to I/O ports in the I/O Map of the Sysmac Studio. The device variables that you create are registered in the variable table.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details on registering device variables with the Sysmac Studio.

Device Variable Attributes

The attributes of the device variables are described in the following table. You can change the settings of some of the attributes, but not all of them.

Attribute	Description	Setting	Changes to settings
Variable Name	The variable name is used to identify the variable.	Automatically generated variables: [device_name] + [I/O_port_name] The default device name starts with a *N* followed by *a sequential number starting from 1*. If entered manually, the variable name is the string you enter.	Allowed.
Data Type	The data type defines the format of the data that is stored in the variable.	According to the data type of the I/O port.	Allowed.
AT Specification	If you want to handle an I/O port for an NX Unit as a variable, specify the address to assign to that variable.	• NX Units on the Communication Control Unit IOBus://unit#[NX_Unit_number]/[I/O_port_name]	Not allowed.
Retain	Specify whether to retain the value for one of the following situations: • When power is turned ON after a power interruption • When the mode is changed to RUN mode • When a major fault level Controller error occurs	• Device variables for NX Units: Not retained.	Not allowed.
Initial Value	You can select to set or not set an initial value. If the initial value is set, specify the value of the variable in the following cases and do not specify the Retain attribute. • When power is turned ON • When operating mode changes • When a major fault level Controller error occurs If the initial value is not set, the value is not retained.	None	Allowed.

Attrib-ute	Description	Setting	Changes to settings
Constant	If you set the Constant attribute, you can set the initial value of the variable when it is downloaded, but you cannot overwrite the value afterward.	None	Allowed.
Network Publish	This attribute allows you to use CIP communications or data links to read/write variables from outside of the Controller.	Not published.	Allowed.

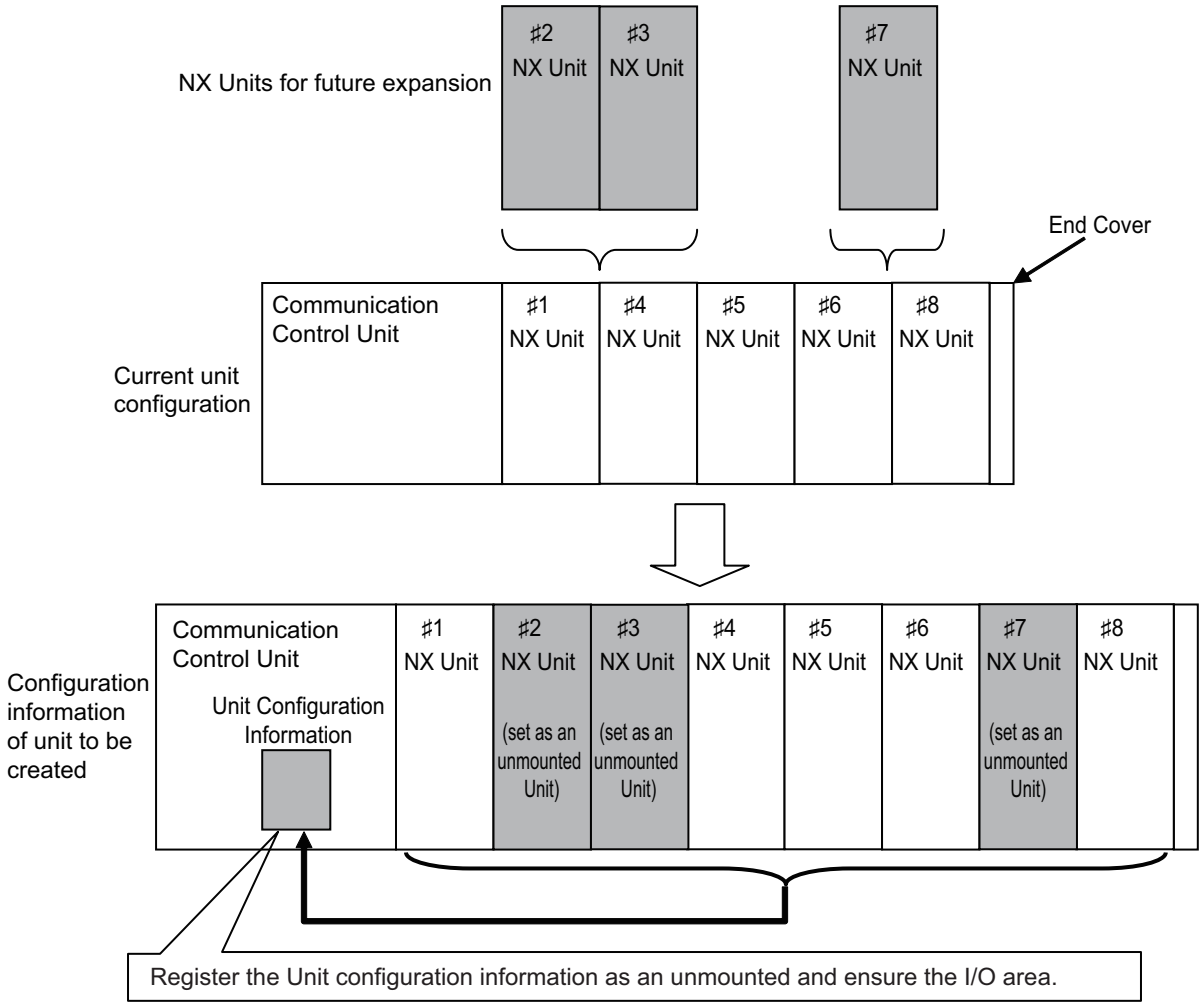
3-2 Mounting Settings of NX Units on the Communication Control Unit

This section describes the mounting settings of NX Units on the Communication Control Unit.

3-2-1 Overview of Function

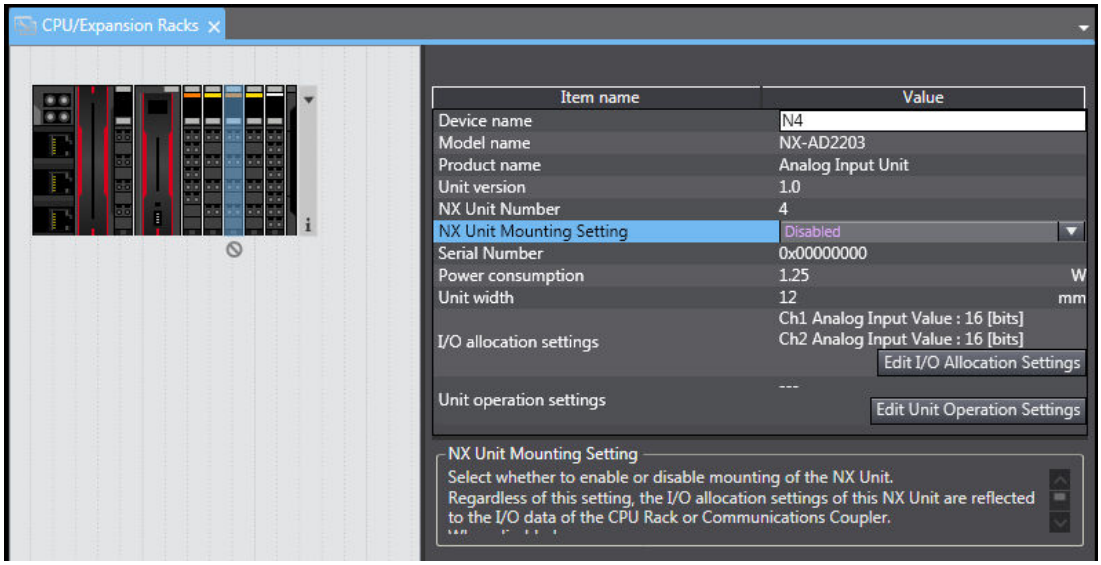
You can use this function to register NX Units that will be added to at a later time in the Unit configuration information as unmounted Units. With this function, you can create the program in advance for NX Units that are not mounted to the actual configuration.
You can use this function even if a specific Unit is temporarily unavailable such as when commissioning the system.

- I/O memory area is reserved for these unmounted NX Units in the same way that it is reserved for NX Units that are mounted to the actual configuration.
- Unmounted NX Units are also assigned NX Unit numbers. This prevents the NX Unit numbers of other NX Units on the Communication Control Unit from changing when you change the setting of an NX Unit that is not mounted to the setting of an NX Unit that is mounted to the actual configuration.



3-2-2 Setting NX Units as Unmounted Units

In the CPU and Expansion Racks Tab Page on the Sysmac Studio, select the target NX Unit and set the **NX Unit Mounting Setting** to **Disabled**. The selected NX Unit is set as an unmounted Unit. After you change the settings for any NX Units, always transfer the Unit configuration information to the actual device.



3-3 Restarting NX Units on the Communication Control Unit

This section describes restarting an NX Unit on the Communication Control Unit. The restart function is used to enable values that are set for the NX Unit without cycling the power supply to the Controller.

3-3-1 Types of Restarts

The following table gives the types of restarts for individual NX Units.

Type	Function
Restarting NX Bus Function Module	All NX Units on the Communication Control Unit are restarted.
Restarting Individual NX Units	The specified NX Unit is restarted.

3-3-2 Restarting an NX Unit

Place the Sysmac Studio online. In the CPU and Expansion Racks Tab Page, right-click the Communication Control Unit and select **Restart for NX Bus/NX Unit** – **Yes**. All NX Units on the Communication Control Unit are restarted.
In the same way, right-click the NX Unit to restart and select **Restart for NX Bus/NX Unit** – **Yes**. The specified NX Unit is restarted.

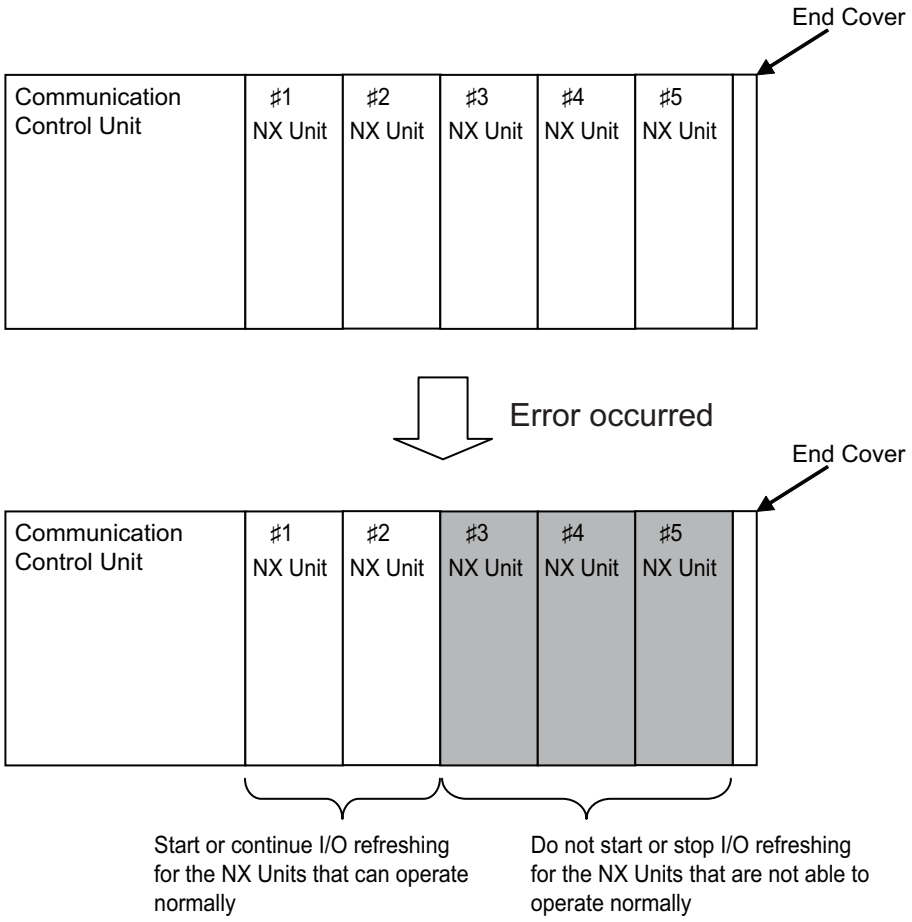
3-4 Fail-soft Operation for NX Units on the Communication Control Unit

This section describes the fail-soft operation for the NX Bus Function Module of the Communication Control Unit.

This function allows the NX Bus Function Module to start or continue I/O refreshing only with the NX Units on the Communication Control Unit that can operate normally when an error occurs for the NX Bus Function Module.

For example, you can use this function in the following cases.

- When it is dangerous to stop all NX Units on the Communication Control Unit at once.
- To continue the operation of the NX Units on the Communication Control Unit until the system can be stopped safely through the user program or user operation.
- To not stop all devices, i.e., to continue operation for only some devices



Precautions for Safe Use

If you change the fail-soft operation setting, the output status when the error occurs may also change. Confirm safety before you change the setting.

3-4-1 Operations for Errors

The following table describes the operation of the NX Bus Function Module when the NX Bus Function Module is used with and without fail-soft operation.

Operating status	Operation when an error occurs while starting	Operation when an error occurs during normal operation
With fail-soft operation	The NX Bus Function Module starts I/O refreshing for the NX Units that can operate normally. It does not start I/O refreshing for NX Units that cannot operate normally.	The NX Bus Function Module continues I/O refreshing for the NX Units that can operate normally. It stops I/O refreshing for NX Units that cannot operate normally.
Without fail-soft operation*1	The NX Bus Function Module does not start I/O refreshing for any of the NX Units.	The NX Bus Function Module stops I/O refreshing for any of the NX Units.

*1. When an error occurs, I/O refreshing for the NX Units on the Communication Control Unit that is not started, i.e., I/O refreshing for the NX Units on the Controller that is stopped is called “entire stop”.

Except for the I/O refreshing, the operation when an error occurs for the NX Bus Function Module is the same regardless of whether fail-soft operation is used. Specifically, error notification is provided and errors are recorded in the event log.

3-4-2 Setting Fail-soft Operation

Using Fail-soft Operation

To enable fail-soft operation, select the Communication Control Unit in the CPU and Expansion Racks Tab Page on the Sysmac Studio and set the **Fail-soft Operation Setting** to **Fail-soft operation**.
The default for the **Fail-soft Operation Setting** for the NX Bus Function Module is **Fail-soft operation**.

Not Using Fail-soft Operation

To disable fail-soft operation, select the Communication Control Unit in the CPU and Expansion Racks Tab Page on the Sysmac Studio, and set the **Fail-soft Operation Setting** to **Stop**.

Precautions for Correct Use

- After you change the setting, always transfer the changed settings to the Communication Control Unit.

3-4-3 Errors to Which Fail-soft Operation Applies

The following errors are examples of the errors to which fail-soft operation applies.

- NX Bus Communications Error
- Registered NX Unit Not Mounted
- NX Unit Communications Timeout
- NX Unit Initialization Error

- NX Unit Startup Error

Even if you enable **Fail-soft operation**, the NX Bus Function Module may not start I/O refreshing for all of the NX Units when the Communication Control Unit is started, depending on the cause of the error.
Refer to *3-4-4 Causes of Unit Configuration Verification Errors and Error Operation* on page 3-12 for details on the operation for different error causes.

If an error occurs to which fail-soft operation does not apply, the NX Bus Function Module will stop I/O refreshing for all NX Units even if you enable fail-soft operation.

3-4-4 Causes of Unit Configuration Verification Errors and Error Operation

Even if you enable **Fail-soft operation**, I/O refreshing may not start depending on the cause of the error when the Communication Control Unit starts.
Examples are provided below.

Example of Unit configuration information and actual configuration		NX Unit numbers					Description of configuration	Operation when the Communication Control Unit starts
		1	2	3	4	5		
Unit configuration information		A	B	C	D	E*1	The following models of Units are mounted after the Communication Control Unit in the order given on the left: A, B, C, D, and E.	---
Actual configuration	Case 1	A	B	C	---	---	Unit D is not mounted.	I/O refreshing does not start for NX Unit numbers 1, 2, and 3 because fail-soft operation is enabled.
	Case 2	A	C	D	---	---	Unit B is not mounted.	I/O refreshing does not start for any of the NX Units.
	Case 3	A	B	D	C	---	Unit C and D are mounted in reverse order.	I/O refreshing does not start for any of the NX Units.
	Case 4	A	B	C	D	D	An extra Unit D is mounted for NX Unit number 5.	I/O refreshing does not start for any of the NX Units.
	Case 5	A	B	C	F	---	Unit F is mounted for NX Unit number 4, but it does not exist in the Unit configuration information.	I/O refreshing does not start for any of the NX Units.
	Case 6	A	B	C	D	E	Unit E is mounted for NX Unit number 5 even though its NX Unit Mounting Setting is set to *Disable*.	I/O refreshing does not start for any of the NX Units.

*1. Unit E has the **NX Unit Mounting Setting** set to **Disable**.

3-5 Monitoring Total Power-ON Time for NX Units on the Communication Control Unit

This section describes how to monitor the total power-ON time for NX Units on the Communication Control Unit.
Each of the NX Units on the Communication Control Unit records the total time that the Unit power supply is ON to it. You can display these times on the Sysmac Studio.

3-5-1 Specifications of Monitoring Total Power-ON Times

The specifications of monitoring the total power-ON times are given in the following table.

Item	Specification
Display unit	• When total power-ON time is less than 1 hour : Minutes • When total power-ON time is 1 hour or longer : Hours
Update interval	• When total power-ON time is less than 24 hours : 10 minutes • When total power-ON time is 24 hours or longer : 1 hour
Measurement error	1 hour/month max.
Default setting	0 minutes

3-5-2 Checking Total Power-ON Times

You can use the Sysmac Studio to check the total power-ON times of NX Units on the Communication Control Unit.

Checking Total Power-ON Times with Sysmac Studio

You can use the Production Information on the Sysmac Studio to check.

1 Go online.

2 Right-click **CPU Rack** under **Configurations and Setup** - **CPU/Expansion Racks** in the Multi-view Explorer and select **Production Information**.
The Production Information Dialog Box is displayed.
You can check the total power-ON times of each NX Unit when you change the view to the production information details.

Display When Times Cannot Be Recorded

If the total power-ON time cannot be recorded because of a non-volatile memory hardware error, the total power-ON time is displayed as *Invalid record* on the Sysmac Studio.

Display for Units That Do Not Support Monitoring the Total Power-ON Time

If a Unit does not support monitoring the total power-ON time, the total power-ON time for the Unit is displayed as "---" on the Sysmac Studio.

Display When Reading the Time Failed

If reading the time failed, the total power-ON time is displayed as "---" on the Sysmac Studio.

4

SD Memory Card Operations

This section describes the functions that you can use for SD Memory Cards.

4-1 SD Memory Card Operations 4-2

4-2 Specifications of Supported SD Memory Cards, Folders, and Files 4-3

4-2-1 SD Memory Card Specifications 4-3
4-2-2 Folder and File Specifications 4-4

4-3 FTP Server 4-6

4-3-1 Overview and Specifications 4-6
4-3-2 FTP Server Function Details 4-7
4-3-3 Using the FTP Server Function 4-9
4-3-4 FTP Server Application Example 4-10
4-3-5 Using FTP Commands 4-11
4-3-6 Table of Commands 4-11
4-3-7 Using the Commands 4-12

4-4 File Operations from the Sysmac Studio 4-18

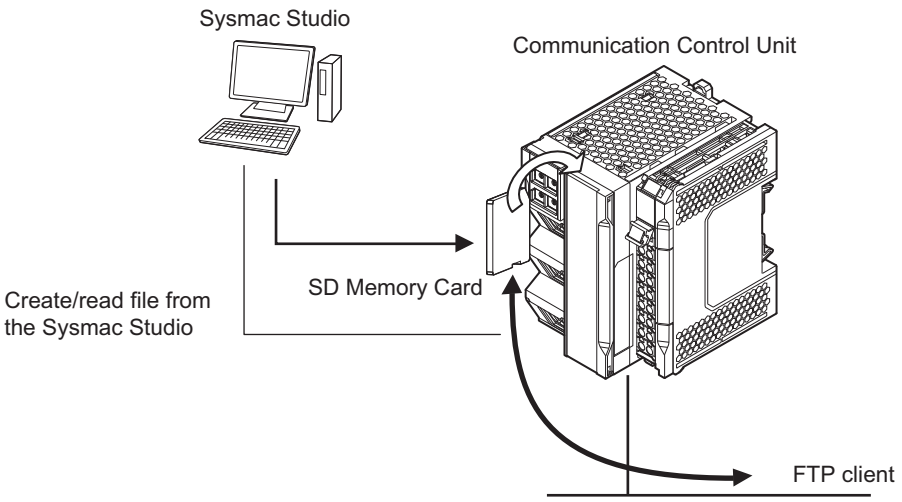
4-5 SD Memory Card Life Expiration Detection 4-19

4-6 SD Memory Card Self-diagnostic Functions 4-20

4-7 Exclusive Control of File Access in SD Memory Cards 4-22

4-1 SD Memory Card Operations

The Communication Control Unit supports the following functions for SD Memory Cards.



Function	Introduction
FTP server	You can use FTP commands from an FTP client on the Intranet to read and write files in the SD Memory Card through EtherNet/IP.
File operations from the Sysmac Studio	You can perform file operations from the Sysmac Studio for the SD Memory Card inserted in the Communication Control Unit. You can perform file operations for Controller files in the SD Memory Card and save standard document files on the computer.
SD Memory Card life expiration detection	Notification of the expiration of the life of the SD Memory Card is provided in an event log.
SD Memory Card backups	Refer to *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.
Safety Data Logging	The I/O data is recorded in the chronological order in the SD Memory Card. Refer to the *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)* for details.

4-2 Specifications of Supported SD Memory Cards, Folders, and Files

4-2-1 SD Memory Card Specifications

The NJ/NX-series Controllers support both SD cards and SDHC cards. However, operation was confirmed only for the OMRON SD Memory Card given in the following table. Correct operation may not be possible if you use any other SD or SDHC card.

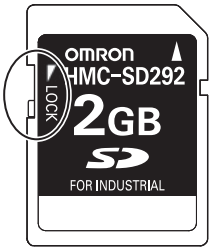
Model	Card type	Capacity [GB]	Formatting	Number of rewrites (per block)	Write protection	Weight
HMC-SD291	SD card	2	FAT16	60,000 times	You can write-protect the SD Memory Card with a hardware switch on the Card.	Approx. 2g
HMC-SD292 *1				50,000 times		
HMC-SD293						
HMC-SD491	SDHC card	4	FAT32	60,000 times		
HMC-SD492 *1				100,000 times		
HMC-SD493						
HMC-SD1A1		16		60,000 times		
HMC-SD1A2 *1				100,000 times		
HMC-SD1A3						

*1. *4-5 SD Memory Card Life Expiration Detection* on page 4-19 cannot be used.

If a format error occurs, the *SD PWR* indicator on the front of the Communication Control Unit goes out, and accessing the SD Memory Card will not be possible.

Additional Information

Write Protection Key
You will not be able to write to the SD Memory Card if the key is set to the LOCK position. Use this setting to prevent overwriting.



4-2-2 Folder and File Specifications

Character Restrictions

Object named by user	Usable characters	Reserved words	Multibyte character compatibility	Case sensitivity	Maximum size (without NULL)
Volume label	0 to 9, A to Z, and a to z, as well as % - _ @ ! ‘ ( ) ~ = # & + ^ [ ] { } , . ; and single-byte kana*1	CON, PRN, AUX, CLOCK$, NUL, COM0, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT0, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9	Not supported.*2	Case insensitive	11 bytes
Directory name	0 to 9, A to Z, and a to z, as well as $ % ' - _ @ ! ` ( ) ~ = # & + ^ [ ] { } , . ; and single-byte kana				65 bytes
File names					65 bytes

*1. You cannot begin volume label names with a space.
*2. Even if the computer supports multibyte characters (e.g., for Japanese), you cannot use them in the Communication Control Unit.

Subdirectory Levels

You can create up to 5 levels (example: f1/f2/f3/f4/f5/abc.txt)

Maximum Number of Stored Files

The number of files that you can store on an SD Memory Card depends on the directory level in which you store the files. The maximum number of files for each is given in the following table. However, the values in the table assume that 8.3 filename is used. If you use long file names, the maximum number of stored files is less than the value given in the following table.

Directory level	Format	Maximum number of stored files
Root directory	**FAT16**	511
	FAT32	65,533
Subdirectory	**FAT16, FAT32**	65,533

Maximum Size of One File

The maximum size of any one file is 2,147,483,647 bytes (2 GB −1 byte).

Precautions for Correct Use

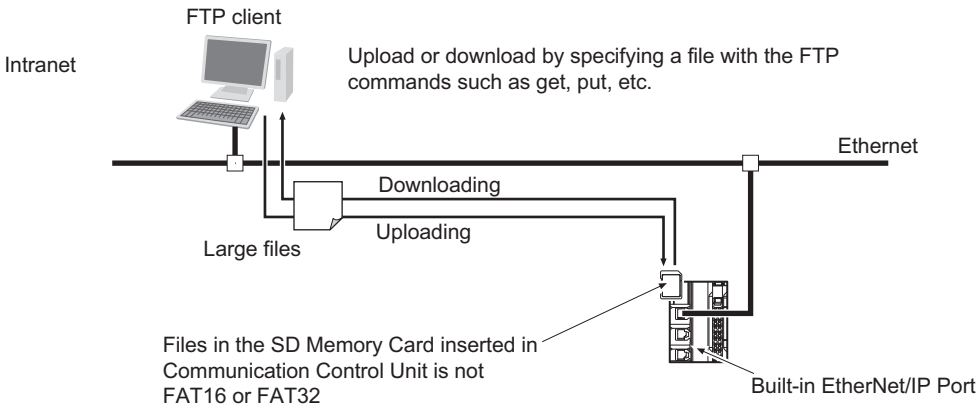
- According to the specifications of FAT16 and FAT32, the update dates of files and folders are in the range from January 1, 1980 to December 31, 2107.
- If the clock data of the CPU Unit is before January 1, 1980, the update dates of files and folders will be January 1, 1980.

4-3 FTP Server

4-3-1 Overview and Specifications

Overview

The built-in EtherNet/IP port has FTP (File Transfer Protocol) server capabilities. You can therefore send FTP commands from an FTP client software application on a computer on the Ethernet network to upload and download large files from and to an SD Memory Card.



Specifications

Item	Specifications	
Executable commands	open	: Connects the specified host FTP server.
	user	: Specifies a user name for the remote FTP server.
	ls	: Displays file names in the remote host.
	mls	: Displays file names in multiple remote hosts.
	dir	: Displays file names and details in the remote host.
	mdir	: Displays file names and details in multiple remote hosts.
	rename	: Changes a file name.
	mkdir	: Creates a new directory in the working directory on the remote host.
	rmdir	: Deletes a directory from the working directory on the remote host.
	cd	: Changes the work directory on the remote host to the specified directory.
	pwd	: Displays the work directory on the remote host.
	type	: Changes the file transfer type.
	get	: Transfers a specified remote file to the local host.
	mget	: Transfers specified multiple remote files to the local host.
	put	: Transfers a specified local file to the remote host.
	mput	: Transfers specified multiple local files to the remote host.
	delete	: Deletes a specified file from the remote host.
	mdelete	: Deletes specified multiple files from the remote host.
	append	: Uses the currently specified file data type to append a local file to the remote host.
	close	: Disconnects the FTP server.
	bye	: Closes the FTP client.
	quit	: Closes the FTP client.
Protection	Login name (up to 12 characters) Password consists of 8 to 32 characters.	
Protocol used	FTP (Port No.: 20/TCP, 21/TCP)	
Number of connections	6	

4-3-2 FTP Server Function Details

Supported Files

The file system in the Controller that can be accessed by the built-in EtherNet/IP port includes files in any SD Memory Card mounted in the Communication Control Unit.
The directory tree is shown below.

```
/: root
├── MEMCARD1:SD
├── usr  ┐
├── bin  ├ Used by system
└── dev  ┘
```

A connection is initially made to the root directory.

Additional Information

- The date of the MEMCARD1 directory displayed for ls, dir, and mkdir commands in the root directory is the date of the file system volume label.
- The login date is displayed for MEMCARD1 if a volume label has not been created.

Connecting to the FTP Server

Input the FTP login name and password to login to the built-in EtherNet/IP port from an FTP client application. Use the Built-in EtherNet/IP Port Settings in the Sysmac Studio to set the FTP login name and password.

Additional Information

When a general-purpose FTP application is used, you can use a graphical user interface similar to Explorer to transfer and read files.

Login Name and Password Setting

The FTP login name and password are not set by default.
Use the Built-in EtherNet/IP Port Settings to set any login name and password.

Login Messages

Status	Message
Normal connection	220 xxx.xx.xx.xx FTP server ready. xxx.xx.xx.xx: Communication Control Unit model (example: NX-CSG320)
Connected to maximum number of connections (6)	530 FTP server busy, Goodbye.

Restrictions on Login Name and Password Setting

The following restrictions apply to login names and passwords.

- Only single-byte alphanumeric characters can be used for login names and passwords. The login name and password are case sensitive.
- A login name consists of up to 12 characters.
- A password consists of 8 to 32 characters.
- Always set a password when you set a new login name. The login name will not be valid unless a password is set for it.
- The login name is invalid if the login name is not set or characters other than single-byte alphanumeric characters are used.

FTP File Transfer Mode

FTP has two file transfer modes: ASCII mode and binary mode. Before you start to transfer files, use the type command (specifies the data type of transferred files) to select the required mode.

- To transfer a file in binary format: Select binary mode.
- To transfer a file in ASCII format: Select ASCII mode.

Multiple Accesses to the Same File

Files accessed with the FTP server function may be accessed simultaneously by several users when they use the communication commands on different FTP clients.

Do not read or overwrite a file if another user is writing the file. In addition, do not write a file if another user is reading the same file.

- **Restrictions on Connection to FTP Server**

  If you repeat connection to and disconnection from the FTP server frequently in a short period of time, access to the server may be restricted temporarily for system protection. If you cannot connect to the FTP server, wait for 10 minutes and try again.

4-3-3 Using the FTP Server Function

Procedure

1. Set up the FTP server on the Sysmac Studio. (Refer to *A-1-3* ***FTP Settings*** *Display* on page A-7.)
2. Select **Controller Setup** - **Built-in EtherNet/IP Port Settings** on the Sysmac Studio. Make the following settings on the **FTP Settings** Display.
   - FTP server
   - Port number
   - Login name
   - Password
3. Connect the Communication Control Unit online and transfer the settings to the Controller.
4. Insert the SD Memory Card into the Communication Control Unit.
5. Connect to the built-in EtherNet/IP port from an FTP client.
6. Input the FTP login name and password that you set in the Built-in EtherNet/IP Port Settings to log in to the built-in EtherNet/IP port.
7. After you are logged in, you can use ftp commands, such as cd (Change Directory) and get (Obtain File) for the MEMCARD1 directory in the SD Memory Card in the Controller.
8. Close the connection.

List of Settings Required for the FTP Server Function

Make the following settings for the unit setup when the FTP server function is used.

Built-in EtherNet/IP Port Settings Tab Page on Sysmac Studio	Setting	Setting conditions	Reference
FTP	FTP server	Required	page A-7
	Port No.	Any number*1 Required when changing the default value of 21.	
	Login name	Required*1	
	Password	Required*1	

*1. If the **Do not use** Option is selected for the **FTP server**, these settings are not required.

Additional Information

Make settings in the **FTP Settings** Display if the FTP server is used. Refer to *A-1-3* ***FTP Settings*** *Display* on page A-7 for information on the **FTP Settings** Display.

4-3-4 FTP Server Application Example

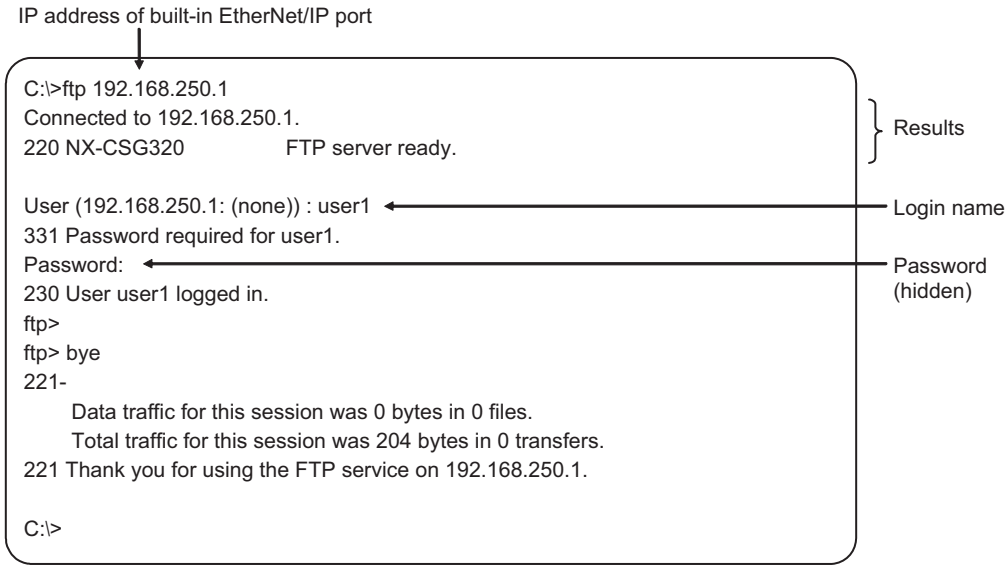
An example of using the FTP server with the login name "user1" and the password "password" is shown below.

Additional Information

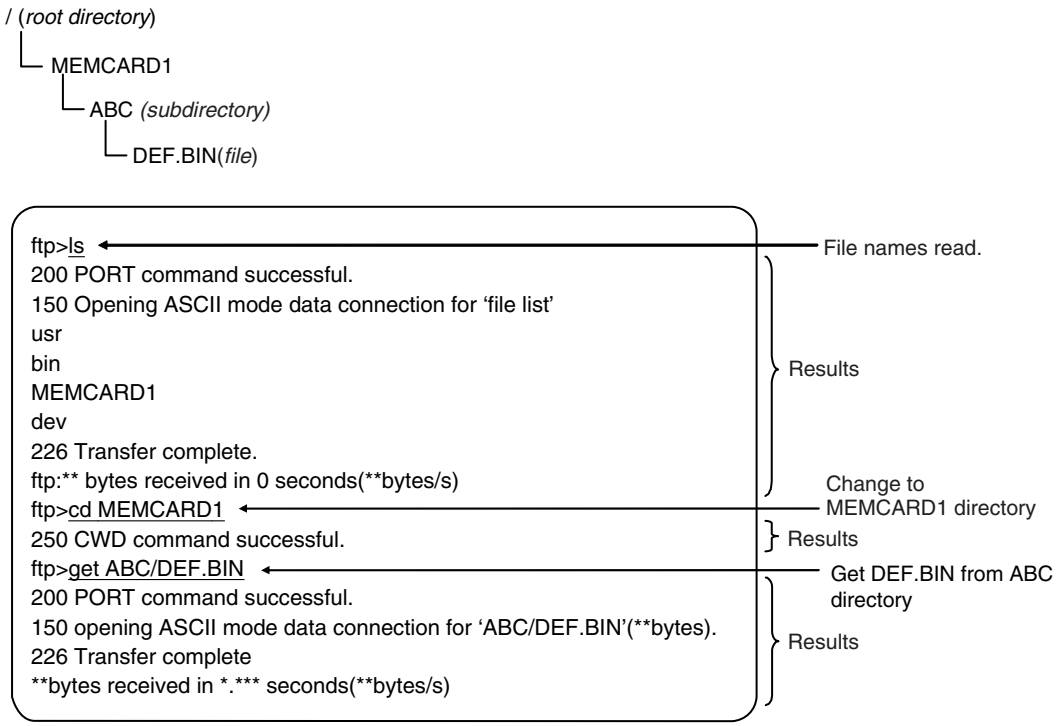
When a general-purpose FTP application is used, you can use a graphical user interface similar to Explorer to transfer and read files.

● Step

1. Make sure that an SD Memory Card is inserted and turn ON the power supply to the Controller.
2. Connect to the FTP server from a computer on the Ethernet by entering the text that is underlined in the following diagram.



3. Enter FTP commands (underlined in the following diagram) to read and write files. The following directory tree is used in this example.



4-3-5 Using FTP Commands

This section describes the FTP commands which the host computer (FTP client) can send to the FTP server of the built-in EtherNet/IP port.
There may be slight differences in the descriptions depending on the model of your workstation. Refer to your workstation's operation manuals for details.

4-3-6 Table of Commands

The FTP commands which can be sent to the built-in EtherNet/IP port are listed in the following table.

Command	Description
open	Connects the specified host FTP server.
user	Specifies a user name for the remote FTP server.
ls	Displays file names in the remote host.
mls	Displays file names in multiple remote hosts.
dir	Displays file names and details in the remote host.
mdir	Displays file names and details in multiple remote hosts.
rename	Rename a file
mkdir	Creates a new directory in the working directory on the remote host.
rmdir	Deletes a directory from the working directory on the remote host.
cd	Changes the work directory on the remote host to the specified directory.
pwd	Displays the work directory on the remote host.
type	Changes the file transfer type.
get	Transfers a specified remote file to the local host.
mget	Transfers specified multiple remote files to the local host.
put	Transfers a specified local file to the remote host.
mput	Transfers specified multiple local files to the remote host.

Command	Description
delete	Deletes a specified file from the remote host.
mdelete	Deletes specified multiple files from the remote host.
append	Uses the file data type that is specified by the type command to append a local file to the remote host.
close	Disconnects the FTP server.
bye	Closes the FTP client.
quit	Closes the FTP client.

Note 1. "Remote host" refers to the built-in EtherNet/IP port.
Note 2. "Remote file" refers to a file on the SD Memory Card in the Communication Control Unit.
Note 3. "Local host" refers to the host computer (FTP client).
Note 4. "Local file" refers to a file on the host computer (FTP client).

4-3-7 Using the Commands

open

● Format

open [IP_address or host_name_of_FTP_server]

● Function

- Connects the FTP server. Normally, the FTP server IP address is specified to execute this command automatically when the FTP client is booted.

user

● Format

user [user_name]

● Function

- Specifies the user name. Specify the FTP login name set in the built-in EtherNet/IP port system setup.
- The user name is automatically requested immediately after connection to the FTP server is opened.

ls

● Format

ls [-l] [remote_file_name [local_file_name]]

● Function

- Displays the names of files on the remote host (on the SD Memory Card).
- Set the switch [-l] to display not only the file names but the creation dates and sizes as well. If the switch is not set, only the file names are displayed.

- Specify a file on the SD Memory Card for the remote_file_name.
- If the local_file_name is specified, the file information is stored in the specified file.

mls

Format

mls remote_file_name local_file_name

Function

- Displays a list of the names of files on multiple remote hosts (on the SD Memory Card).
- For the remote_file_name, specify a directory on the SD Memory Card in which you wish to list files contained, or a file name. Input an asterisk (*) to display a list of the current working directory.
- If the local_file_name is specified, the file information is stored in the specified file. Input a hyphen (-) to display a list of the remote hosts but not store the list of file names.

dir

Format

dir [remote_file_name [local_file_name]]

Function

- Displays the names, creation dates, and sizes of files on the remote host (on the SD Memory Card).
- It displays the same information as command [ls -l].
- Specify a file on the SD Memory Card for the remote_file_name.
- If the_local_file name is specified, the file information is stored in the specified file.

mdir

Format

mdir remote_file_name local_file_name

Function

- Displays the names of files, subdirectories, creation dates, and sizes on multiple remote hosts (on the SD Memory Card).
- For the remote_file_name, specify the directory or file name on the SD Memory Card you wish to list. Input a hyphen (-) to display a list of the current working directory.
- If the_local_file_name is specified, the file information is stored in the specified file. Input a hyphen (-) to display a list of the remote hosts and not store the file information.

Format

mdir RemoteFiles [...] LocalFile

RemoteFiles: Input a hyphen (-) to use a current working directory.

LocalFile: Input a hyphen (-) to display a list on the screen.

Function

- It displays a list of files and subdirectories under the remote directory.

rename

Format

rename current_file_name new_file_name

Function

- Changes the specified current file name to the specified new file name.
- If the new file name is already used by an existing file on the remote host (on the SD Memory Card), the existing file is overwritten by the file whose name was changed.
- rename can just change the file name. It cannot be used to move the file to a different directory.

mkdir

Format

mkdir directory_name

Function

- Creates a directory of the specified name on the remote host (on the SD Memory Card).
- An error will occur if a file or directory of the same name already exists in the working directory.

rmdir

Format

rmdir directory_name

Function

- Deletes the directory with the specified name from the remote host (from the SD Memory Card).
- The directory must be empty to be deleted.
- An error will occur if the specified directory does not exist or is not empty.

pwd

Format

pwd

Function

- Displays the work directory on the remote host.

append

Format

append local_file_name [remote_file_name]

Function

- Uses the file data type that is specified by the type command to append the local file to the remote host (on the SD Memory Card).

cd

Format

cd [directory_name]

Function

- Changes the remote host work directory to the specified remote directory.
- Files on the SD Memory Card are stored in the MEMCARD1 directory under the root directory (/).
- The root directory (/) is the directory that is used when you log onto the built-in EtherNet/IP port. The MEMCARD1 directory does not exist if an SD Memory Card is not inserted in the Communication Control Unit or if the SD Memory Card power indicator on the Communication Control Unit is not lit.

type

Format

type data_type

Function

- Specifies the file data type.
- The following data types are supported:
  ascii: Files are transferred as ASCII data.
  binary (image): Files are transferred as binary data.
  The Communication Control Unit handles binary files. Use the type command to specify binary transfers before you upload or download files.
- The default file type is ASCII.

get

Format

get file_name [receive_file_name]

Function

- Transfers the specified remote file from the SD Memory Card to the local host.

- You can specify the name of the file to be received on the local host by setting receive file name.

mget

Format

mget file_name

Function

- With wildcards (*) included in the file_name, transfers multiple remote files from the SD Memory Card to the local host.

put

Format

put file_name [destination_file_name]

Function

- Transfers the specified local file to the remote host (to the SD Memory Card).
- You can save the transfered file with the name you specify for the destination_file_name.
- Any existing file with the same name in the remote host (on the SD Memory Card) is overwritten by the contents of the transferred file.

mput

Format

mput file_name

Function

- With wildcards (*) included in the file_name, transfers multiple local files to the remote host (to the SD Memory Card).
- Any existing file with the same name in the remote host (on the SD Memory Card) is overwritten by the contents of the transferred file.

delete

Format

delete file_name

Function

- Deletes the specified remote file (on the SD Memory Card).

mdelete

Format

mdelete file_name

Function

- With wildcards (*) included in the file_name, deletes multiple remote files from the SD Memory Card.

close

Format

close

Function

- Disconnects the FTP server of the built-in EtherNet/IP port.

bye

Format

bye

Function

- Ends the FTP session.

quit

Format

quit

Function

- Ends the FTP session.

4-4 File Operations from the Sysmac Studio

You can perform file operations from the Sysmac Studio for the SD Memory Card inserted in the Communication Control Unit.
In addition to Controller files, you can also store document files or other files on the SD Memory Card.

4-5 SD Memory Card Life Expiration Detection

You can determine the remaining life of the SD Memory Card before the Card becomes physically deteriorated.
You can determine the remaining life of the SD Memory Card with the following functions.

- SD Memory Card Life Exceeded (Observation) record in the event log

The life of the SD Memory Card is checked when the power is turned ON and periodically while the SD Memory Card is inserted.

When the end of the life of the SD Memory Card is detected, save the data on the SD Memory Card and replace the SD Memory Card.
(You can use the SD Memory Card life expiration detection function on some specific SD Memory Cards. Refer to *4-2 Specifications of Supported SD Memory Cards, Folders, and Files* on page 4-3.)

4-6 SD Memory Card Self-diagnostic Functions

You can perform self-diagnosis on the inserted SD Memory Card when the power supply is turned ON.

You can select whether to perform self-diagnosis when the power is turned ON in the **Operation Settings** of the **Controller Setup** under the **Configurations and Setup** from the Sysmac Studio as shown below.

- File system check
- Check equivalent to CHKDSK
- Restoration attempt when check fails

Access point	Setting group	Setting	Description	Set value
Operation Settings, Operation Settings Tab, Basic Settings	SD Memory Card Settings	Memory Card Diagnosis at Startup*1	Sets whether to execute self-diagnosis (file system check and restoration) on the inserted SD Memory Card when the power is turned ON.	Do not check. Check.

*1. Self-diagnosis is not executed if write protection is set on the SD Memory Card itself.

Results of Self-diagnosis

Case	Indicators			Error type	Correction	Remarks
	RUN	SD PWR	SD BUSY			
Self-diagnosis in progress	Flashing	Not lit	Lit	---	---	---
When self-diagnosis found no problems	---	Lit	Not lit	Normal	None	---
The format of the SD Memory Card is not correct.	---	Not lit	Not lit	Observation	Use the Sysmac Studio to format the SD Memory Card.	---
An error was detected during the file system check and the file system was automatically restored.	---	Lit	Flashes during restore operation. Not lit after restore operation is completed.	Observation	Use file operations in the Sysmac Studio or insert the SD Memory Card into the computer to check whether any files were deleted by the restore operation.	If a corrupted file is detected, an attempt is made to restore the file.
The SD Memory Card failed.	---	Not lit	Not lit	Observation	Replace the SD Memory Card.	---

Precautions for Correct Use

Never interrupt the power supply to the Communication Control Unit during SD Memory Card access even when the SD Memory Card diagnosis at startup is enabled.
An attempt is made by the SD Memory Card restoration function to restore any corrupted files. If the restoration fails, these files may be deleted automatically at startup.

4-7 Exclusive Control of File Access in SD Memory Cards

Access to files on the SD Memory Card is possible with the following two methods.

1. FTP server
2. File operations from the Sysmac Studio

However, if the same file on the SD Memory Card is accessed from different sources, unintended operations such as reading a file while it is being written or writing a file while it is being read may occur. Avoid accessing the same file at the same time.

5

Security

This chapter describes the security functions.

5-1 Overview of Security Functions 5-2

5-2 Overall Project File Protection 5-3

5-2-1 Operating Procedure 5-3

5-3 Operation Authority Verification 5-4

5-3-1 Introduction 5-4

5-3-2 Operating Procedure 5-4

5-3-3 Specifications 5-4

5-4 Communication Control Unit Write Protection 5-6

5-5 Communication Control Unit Names and Serial IDs 5-8

5-5-1 Introduction 5-8

5-5-2 Setting Methods 5-8

5-5-3 Serial IDs 5-9

5-1 Overview of Security Functions

This section describes the security functions that are supported by the Communication Control Unit.

To protect your assets, you can use security functions to protect the user program and data in the Controller. To prevent incorrect operation, you can use security functions to restrict operations on the Sysmac Studio.

The Communication Control Unit supports the following security functions.

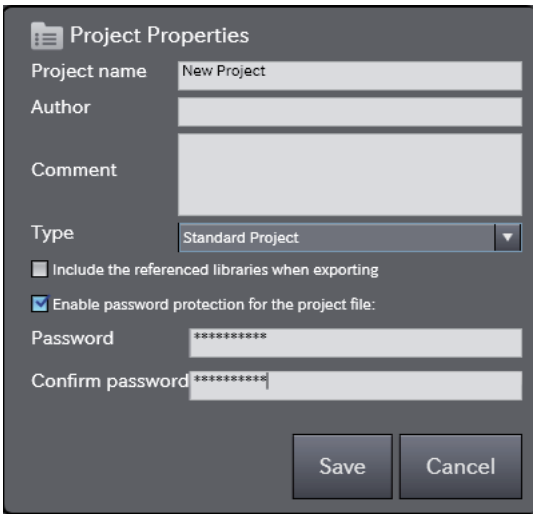
Purpose	Security function	Outline of function	Reference
Prevention of the theft of assets	Overall project file protection	You can place a password on a project file to protect your assets.	*5-2 Overall Project File Protection* on page 5-3
Prevention of incorrect operation	Operation authority verification	You can set operation authorities to restrict the operations that can be performed on the Communication Control Unit from the Sysmac Studio.	*5-3 Operation Authority Verification* on page 5-4
	Communication Control Unit write protection	You can prevent rewriting data in the Communication Control Unit from the Sysmac Studio.	*5-4 Communication Control Unit Write Protection* on page 5-6
Prevention of incorrect connections	Communication Control Unit name	You can check to see if the controller name and serial ID on the computer and in the Communication Control Unit are the same to prevent going online with the wrong Controller.	*5-5 Communication Control Unit Names and Serial IDs* on page 5-8

5-2 Overall Project File Protection

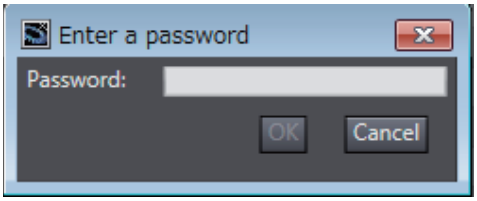
You can place a password on a project file to protect your assets.

5-2-1 Operating Procedure

This section describes how to set a password for a project.
When you use Save As to save the project file, select the **Enable password protection for the project file** Check Box to enable the password setting.



Use the following procedure to open a project for which a password is set.
If you try to open or import a project file for which a password is set, the **Enter a password** Dialog Box is displayed.



Refer to the *Sysmac Studio Version 1 Operation Manual* (Cat. No. W504) for specific procedures.

5-3 Operation Authority Verification

5-3-1 Introduction

Online operations are restricted by operation rights to prevent damage to equipment or injuries that may be caused by operating mistakes.

You can register passwords for operation authority for each Communication Control Unit in the Sysmac Studio. If a correct password is entered when an online connection is made to a Controller, the online operations for the operation authority category for the password that was entered will be allowed.

The Administrator sets a password for each operation authority. Users are notified of the operation authority name and password according to their skills.

Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for specific operating procedures for operation authorities.

5-3-2 Operating Procedure

For operation authority verification, select **Security − Setting of Operation Authority** from the Controller Menu on the Sysmac Studio.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for specific procedures.

5-3-3 Specifications

Types of Operation Authorities

You can use the following five operation authorities on the Sysmac Studio. They are given in descending order of authority.

Type	Password
Administrator	Required.
Designer	Optional*1 Whether a password is required is determined by the default operation authority that is set in the **Setting of Operation Authority** Dialog Box.
Maintainer	
Operator	
Observer	Not required.

*1. Whether a password is required is determined by the default operation authority that is set in the **Setting of Operation Authority** Dialog Box. A password must be entered to perform operations that require an operation authority that is higher than the default operation authority. A password is not required to perform operations that require an operation authority that is equal to or lower than the default operation authority.

Examples of Online Operations for Operation Rights

Examples of the online operations that are allowed for each operation authority are given below.
Refer to the *Sysmac Studio Version 1 Operation Manual (Cat. No. W504)* for details.

(OK: Operation possible, VR: Verification required for each operation, NP: Operation not possible)

Status monitor (example)	Adminis-trator	Designer	Maintain-er	Operator	Observer
Monitoring errors for troubleshooting	OK	OK	OK	OK	OK

Controller operations (examples)	Adminis-trator	Designer	Maintain-er	Operator	Observer
Resetting the Controller	OK	OK	NP	NP	NP
Resetting errors for troubleshooting	OK	OK	OK	VR	NP
Communication Control Unit write-protection	OK	OK	OK	NP	NP

Password Specifications

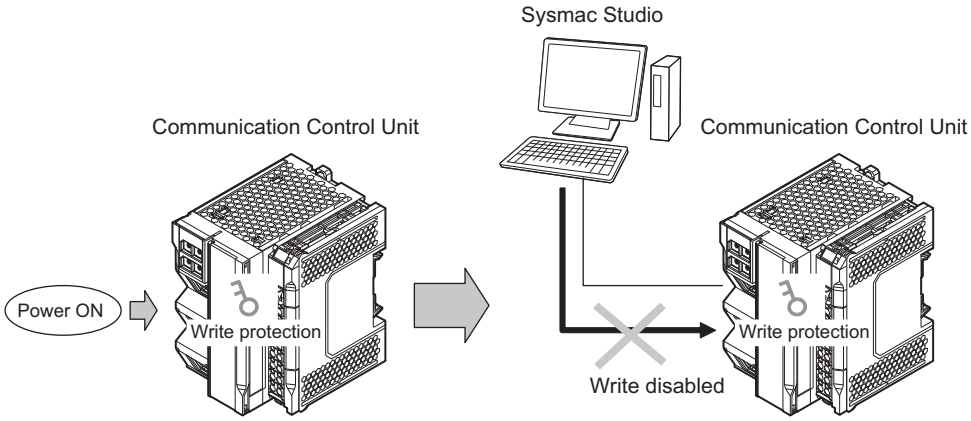
Item	Description
Valid number of characters	8 to 32
Applicable characters	Single-byte alphanumeric characters (case sensitive)

5-4 Communication Control Unit Write Protection

This function disables the ability to write data to Communication Control Unit to protect user program assets and prevent misuse. The following two settings are available:

Communication Control Unit Write Protection at Startup

This setting automatically enables write protection when you turn ON the power supply to the Communication Control Unit.

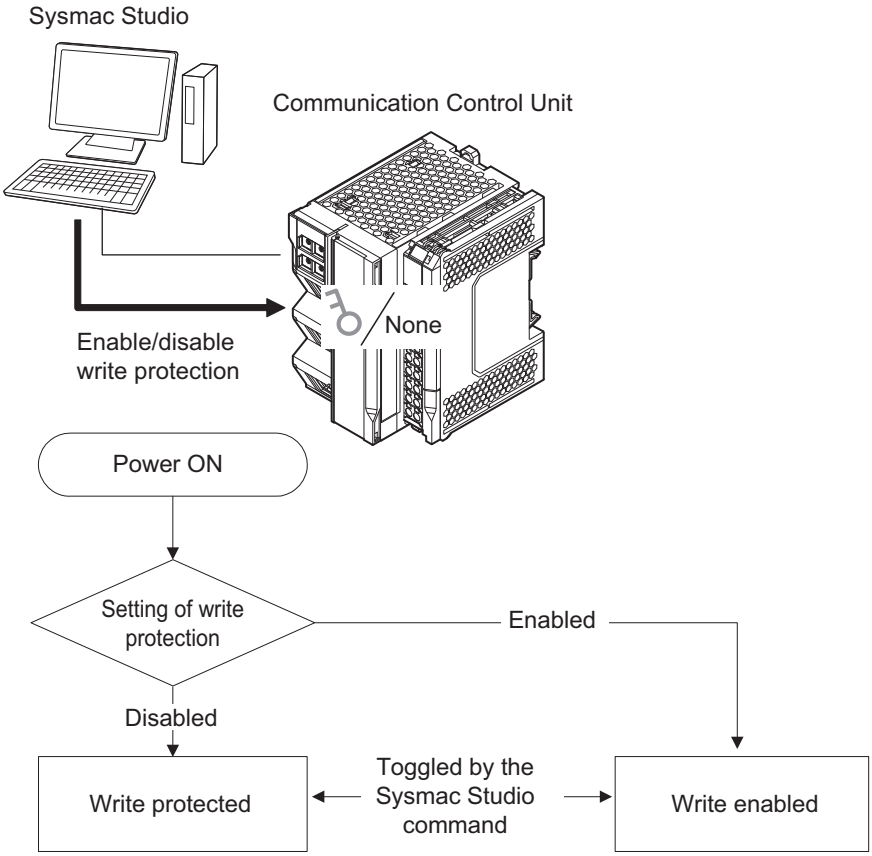


Set whether to automatically enable write protection when the power supply is turned ON in the **Operation Settings** under the **Configurations and Setup** - **Controller Setup** of the Sysmac Studio.

Setting point	Setting group	Setting	Description	Set value
Operation Settings, Operation Settings Tab, Basic Settings	Security Settings	Write Protection at Startup	Sets whether to enable write protection.	Do not use. Use.

Setting and Removing Write Protection from the Sysmac Studio

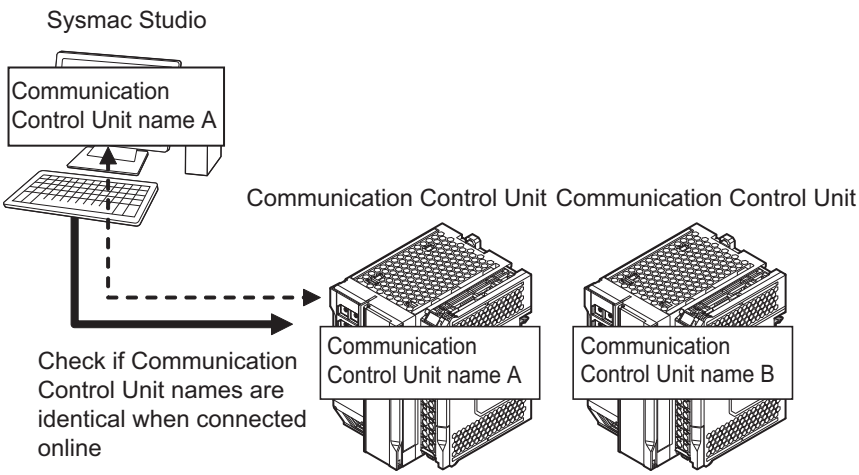
In the Sysmac Studio, go online and select **Security** − **Communication Control Unit Write Protection** from the **Controller** Menu to toggle write protection.


Sysmac Studio
Communication Control Unit
RO
None
Enable/disable
write protection
Power ON
Setting of write
protection
Enabled
Disabled
Write protected
Toggled by the
Sysmac Studio
command
Write enabled

5-5 Communication Control Unit Names and Serial IDs

5-5-1 Introduction

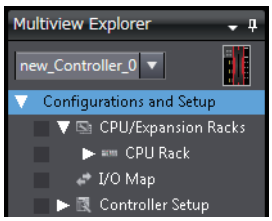
Register a Communication Control Unit name in the Communication Control Unit.
When going online to a Communication Control Unit from the Sysmac Studio, the name in the project is compared to the Communication Control Unit name of the Communication Control Unit being connected to.
This helps prevent incorrect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



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

5-5-2 Setting Methods

1 Set the Communication Control Unit name when you create a project on the Sysmac Studio.
The Communication Control Unit name is displayed as shown below.



To change the name, right-click the Communication Control Unit icon and select *Rename*.

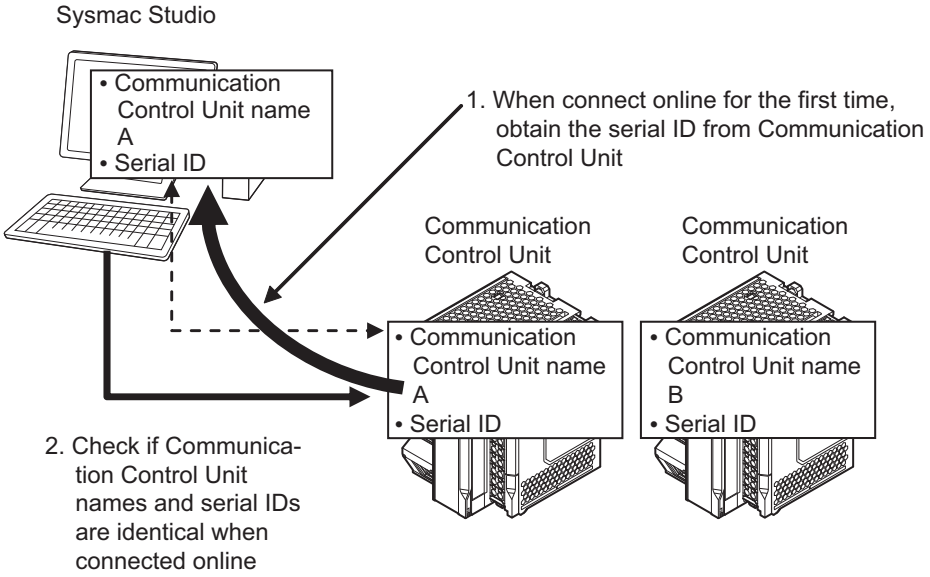
2 When you first connect to the Communication Control Unit online, the Sysmac Studio prompts you to store the Communication Control Unit name in the Communication Control Unit.

3 After that, when you connect to the Communication Control Unit online, the Sysmac Studio refers to the Communication Control Unit name in the project and the Communication Control

Unit name of the Communication Control Unit you connect to. A warning dialog box is shown if they do not match, and you are asked whether to continue to connect.

5-5-3 Serial IDs

When the Sysmac Studio goes online for the first time, you can obtain a serial ID from the Communication Control Unit's production information and store it in the project.
When Sysmac Studio goes online again, both the Communication Control Unit name and serial ID are compared. This enables stricter verification of the Communication Control Unit.



6

Event Logs

This section describes the event logs.

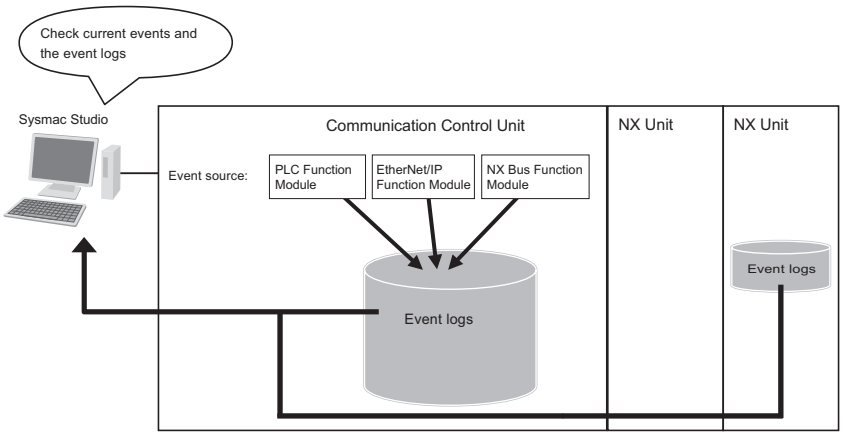
6-1 Overview 6-2
6-1-1 Features 6-2

6-2 Detailed Information on Event Logs 6-3
6-2-1 Event Sources 6-3
6-2-2 Category 6-3
6-2-3 Number of Records 6-3
6-2-4 Event Codes 6-3
6-2-5 Event Levels 6-4
6-2-6 Displaying Event Logs 6-4
6-2-7 Clearing Event Logs 6-5
6-2-8 Exporting Event Logs 6-5

6-1 Overview

The event logs contain records of events*, such as errors, status changes, and user operations, that occurred in the NX-series Communication Control Units.
* Here, "events" are unscheduled events that occur on the Controller, such as errors. Event refers to an error or to information that does not indicate an error but of which the user must be notified by the Controller.
There are one type and two classifications of events as shown in the following table.

Event type	Event classification	Description
Controller events	Controller errors	These are system-defined errors. "major fault level", "partial fault level", "minor fault level", "observation level" Controller events. Errors in the function modules of the Communication Control Unit and NX Units are detected. When one of these events occurs, a Controller error is recorded in the event log.
	Controller information	Controller information is system-defined notification information. This information does not indicate errors. It represents "information level" Controller events. Examples include events other than errors, such as turning the power ON and OFF, starting and stopping operation, connecting the Sysmac Studio online, and downloading settings.



Note: Event logs are only saved on the non-volatile memory.

6-1-1 Features

Event logs have the following features.

- In addition to error records, various records are recorded for events such as the time the power supply is turned ON or OFF, and the time when operation is started.
- You can check these records based on the time. You can therefore use them to isolate the causes of errors when problems occur.

6-2 Detailed Information on Event Logs

6-2-1 Event Sources

This information identifies where an event occurred in the Controller.
The sources of the controller events are specified as follows.

Sources of Controller Events

Controller events occur in the function modules in the Communication Control Unit.
For some function modules, there is more detailed information about the event source. This information is called the "detailed event source".
The following are Controller events.

Event Sources	Detailed event source
PLC Function Module	Power supply or I/O bus master
NX Bus Function Module	Master or NX Unit
EtherNet/IP Function Module	Communications port/communications port 1/communications port 2, CIP/CIP1/CIP2, FTP, NTP, or SNMP

6-2-2 Category

This information displays the category of event log.
It is used to access error logs from the Sysmac Studio or an NA-series PT.

Event type	Event log category	Description
Controller events	System log	The Controller automatically detects and records these events. NX-series Unit errors are also included.
	Access log	This is a record of events that have affected Controller operation due to user actions.

6-2-3 Number of Records

Each event log can contain the following number of records.
If the number of events exceeds the number of records permitted, the Communication Control Unit overwrites the oldest events.

Event type	Event log category	Maximum number of records
Controller events	System log	768
	Access log	576

6-2-4 Event Codes

Event codes are assigned to Controller events by the system in advance according to the type of event. Controller event codes are 8-digit hexadecimal values.

6-2-5 Event Levels

Each event has an "event level" that indicates its level.
The event level depends on the type of event.

Controller Events

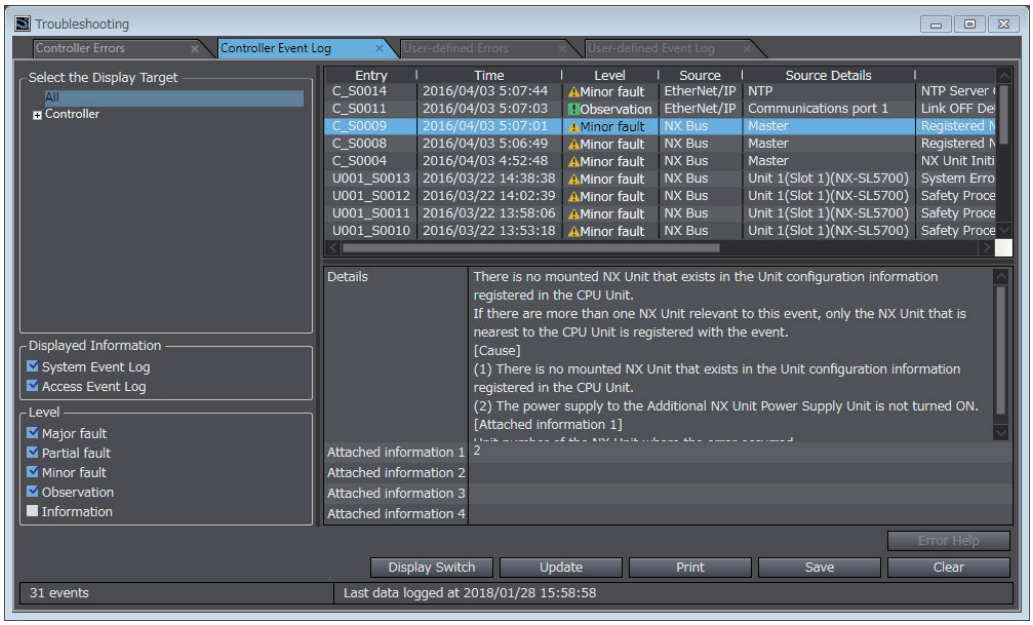
Controller events are classified into five levels according to the degree of the effect that the events have on control, as shown in the following table.

No.	Level		Classification
1	High	Controller errors	Major fault level
2	↑		Partial fault level
3			Minor fault level
4	↓		Observation level
5	Low	Controller information	Information level

Errors with a higher level have a greater impact on the functions that the Controller provides, and are more difficult to recover from.

6-2-6 Displaying Event Logs

The Sysmac Studio displays a list as shown below. When you select an event in the list, the details will appear.



Additional Information

If an event occurs in the Controller that is not supported by the version of the Sysmac Studio, the source is displayed as **Unknown** and the event name is displayed as **Unknown Event**. The event code and attached information are displayed correctly.

6-2-7 Clearing Event Logs

Clearing Event Logs from Sysmac Studio

You can clear event logs from Sysmac Studio.

Precautions for Correct Use

If you need to delete event log from the Sysmac Studio, make sure you do not need any of the event information before you delete the event log. You may have overlooked some important information and observation level Controller events or user-defined events. Always check for these before you delete an event log.

Clearing Event Logs with the Clear All Memory Operation

When you perform the Clear All Memory operation for an NX-series Communication Control Unit from the Sysmac Studio, you can select whether to clear the event logs.

6-2-8 Exporting Event Logs

You can use the Sysmac Studio to export the displayed event log to a CSV file.

7

Changing Event Levels

This section describes the Changing Event Levels.

7-1 Overview of Changing Event Levels 7-2
7-2 Applications of Changing Event Levels 7-3
7-3 Events for Which the Event Level Can Be Changed 7-4
7-4 Procedure to Change an Event Level 7-5

7-1 Overview of Changing Event Levels

Errors, status changes, and user operations that occur in the Communication Control Unit are all called events. You can tell what type of event has occurred by viewing the display in Sysmac Studio, or by checking the indicators on the front panel of the Communication Control Unit.
Events that are predefined by the system are called Controller events. The Controller events are classified into five event levels. Refer to *6-2-5 Event Levels* on page 6-4 for details on event levels.
You can change the event levels that are assigned to some of the Controller events.

7-2 Applications of Changing Event Levels

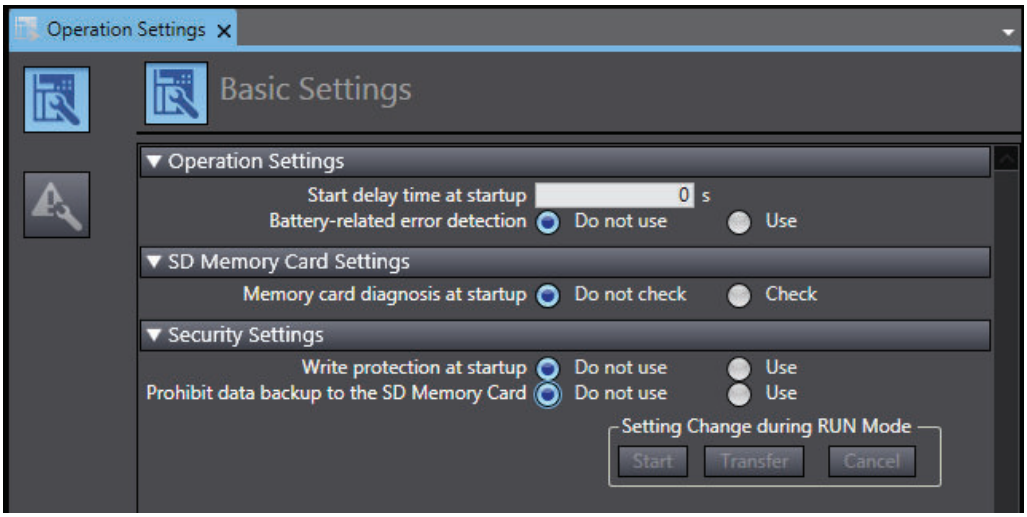
The lighting pattern for the indicators on the front panel of the Communication Control Unit is predefined according to the event level that is assigned to each Controller event. You can change the event level for some events to change how the Controller operates when that event occurs.
For example, the ERROR indicator flashes for minor fault level events and stays unlit for observation level events. You can change the lighting pattern of the ERROR indicator so that it goes out or flashes for a given event.

7-3 Events for Which the Event Level Can Be Changed

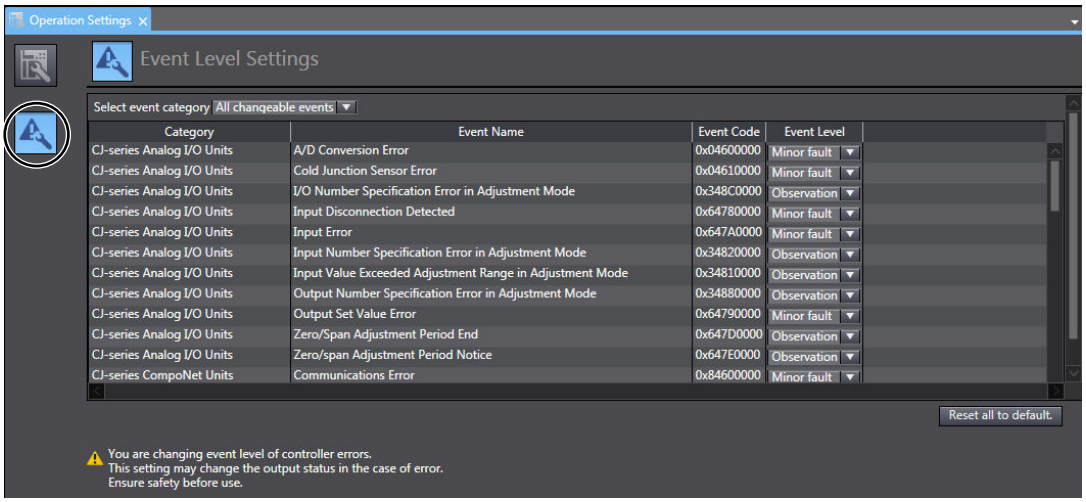
Whether an event level can be changed depends on the specific event.
Refer to the *NX-series Safety Control Unit/Communication Control Unit User's Manual (Cat. No. Z395)* for details on the types and levels of the Controller events, and whether the event levels can be changed.

7-4 Procedure to Change an Event Level

1 Under **Configurations and Setup** - **Controller Setup** in the Sysmac Studio, double-click **Operation Settings**, or right-click and select **Edit** from the menu.
The **Basic Settings** Display is displayed on the Operation Settings Tab Page in the Edit Pane.



2 Click the **Event Level Settings** Button.
A list of the events for which you can change the event level is displayed.



3 Change the levels of the required events in the **Event Level** column.

Precautions for Correct Use

If you change an event level on the Sysmac Studio and download the event level setting to the Controller when the event already exists on the Controller, the event will be reset when the download is started. If the same event occurs again while the download is in progress, the Controller will operate according to the previous event level. If the same event occurs after the download is completed, the Controller will operate according to the new level.

8

CIP Message Communications

8-1 Overview of the CIP Message Communications Service 8-2
8-1-1 Overview of the CIP Message Communications Service 8-2
8-1-2 Message Communications Service Specifications 8-2

8-2 CIP Communication Server Function 8-3
8-2-1 CIP Message Structure for Accessing CIP Objects 8-3
8-2-2 CIP Message Structure for Accessing Variables 8-4

8-3 Specifying Request Path 8-5
8-3-1 Examples of CIP Object Specifications 8-5
8-3-2 Examples of Variable Specifications 8-6
8-3-3 Logical Segment 8-6
8-3-4 Data Segment 8-6
8-3-5 Specifying Variable Names in Request Paths 8-7

8-4 CIP Object Services 8-11
8-4-1 CIP Objects Sent to the Built-in EtherNet/IP Port 8-11
8-4-2 Identity Object (Class ID: 01 hex) 8-11
8-4-3 NX Configuration Object (Class ID: 74 hex) 8-14
8-4-4 TCP/IP Interface Object (Class ID: F5 hex) 8-28
8-4-5 Ethernet Link Object (Class ID: F6 hex) 8-30
8-4-6 Controller Object (Class ID: C4 hex) 8-36

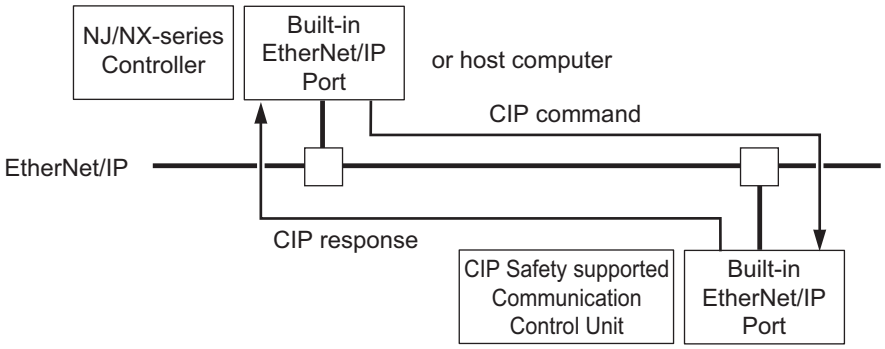
8-5 Read and Write Services for Variables 8-38
8-5-1 Read Service for Variables 8-38
8-5-2 Write Service for Variables 8-39

8-6 Variable Data Types 8-42
8-6-1 Data Type Codes 8-42
8-6-2 Common Format 8-42
8-6-3 Elementary Data Types 8-43
8-6-4 Derived Data Types 8-44

8-1 Overview of the CIP Message Communications Service

8-1-1 Overview of the CIP Message Communications Service

The CIP Safety-compliant Communication Control Unit has the CIP message communications server capabilities.
You can use the CIP message communications clients on CS/CJ-series CPU Units or NJ/NX-series CPU Units to read and write the memory of the CIP Safety-compliant Communication Control Unit.



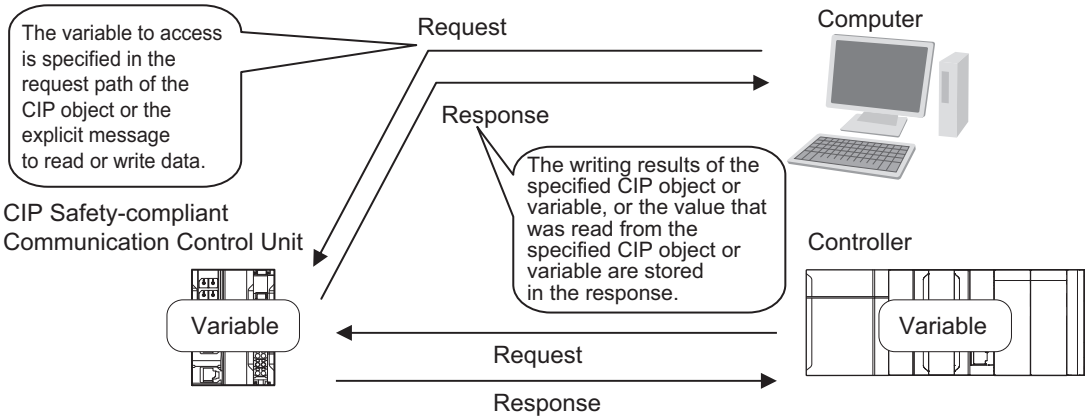
8-1-2 Message Communications Service Specifications

Item		Specification
Message type		CIP unconnected message (UCMM) CIP connected message (Class3)
Maximum data length per connection	Non-connection type (UCMM)	502 bytes
	Connection type (class 3)	• Using Forward_Open 502 bytes • Using Large_Forward_Open 1994 bytes

8-2 CIP Communication Server Function

When receiving a CIP message from an external device, the CIP Safety-compliant Control Unit executes services for specified self-contained objects.
This function is called, the "CIP Communication Server function".

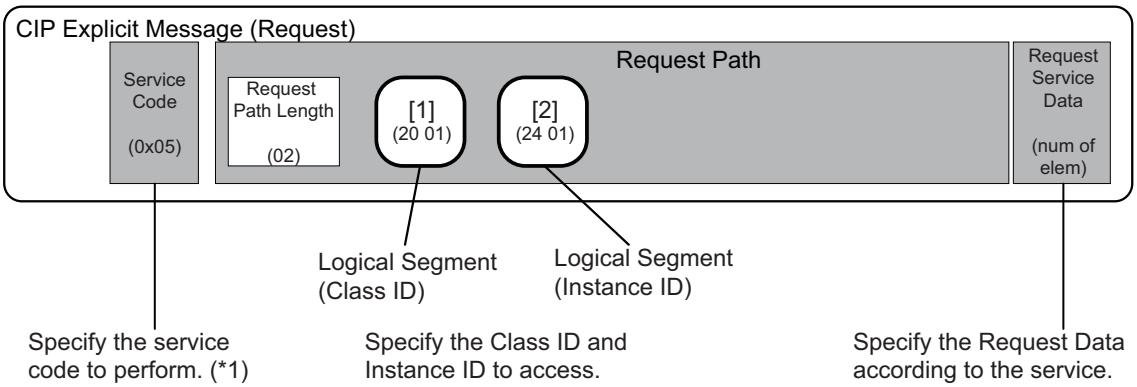
This section describes information on CIP messages structure along with information about how to use CIP messages. The CIP Communication Server function allows users to read and write CIP objects as well as to read and write values of variables by issuing a CIP message to the CIP Safety-compliant Communication Control Unit from a program that runs on a computer or a controller.



8-2-1 CIP Message Structure for Accessing CIP Objects

This section shows how to specify messages to access CIP objects.
The CIP objects to be accessed are expressed by connecting the segments defined in the CIP Common Specifications in the request path field in a CIP explicit message.

Example: Performing the Reset service (0x05) to the Instance (01 hex) of the Identity object (class: 01 hex)



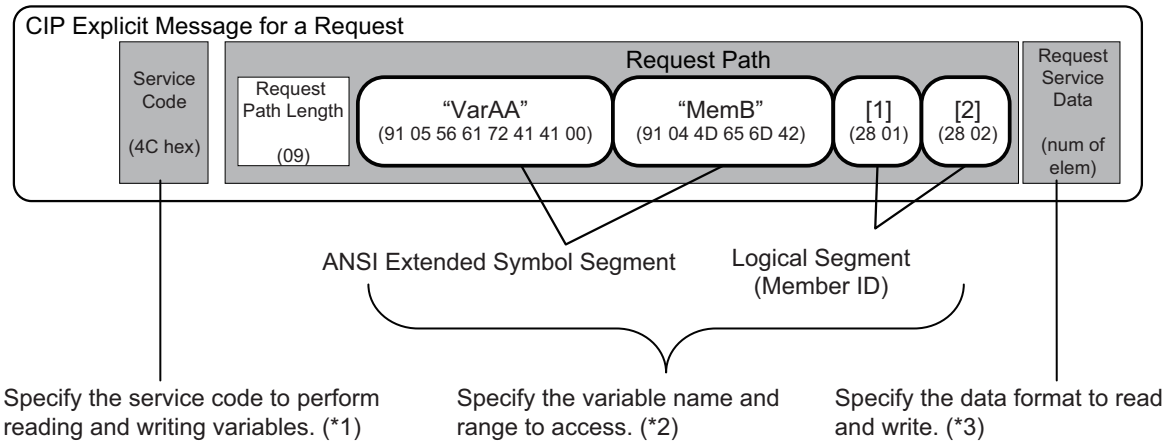
*1. Refer to *8-4 CIP Object Services* on page 8-11 for information about the service codes.

8-2-2 CIP Message Structure for Accessing Variables

This section shows how to specify messages to access variables.
The variables to access are given by connecting the segments that are defined in the CIP Common specifications so that explicit message can be set in the request path field.

The following elements are combined to make the specification.
Specifying the variable to access: The elements are stored in the CIP segments and then joined to make the message.

Example: Reading the Present Value of One Member of the VarAA.MemB[1.2] Structure Variable
Example for Using the CIP Read Data Service for a Variable Object



*1. Refer to *8-5 Read and Write Services for Variables* on page 8-38 for information about the service codes.
*2. Refer to *8-3-5 Specifying Variable Names in Request Paths* on page 8-7 for information about how to specify variables names.
*3. Refer to *8-6 Variable Data Types* on page 8-42 for details about how to specify data formats.

8-3 Specifying Request Path

The CIP object, variable name, structure member name, and array index are specified in the request path.
In CIP, the EPATH data type is used for the request path.
With this method, the request path is divided into segments and a value is assigned to each segment.
The request path notation shows the path to the final destination when the data segments are joined together.
Each segment includes the segment type information and the segment data.

Segment 1	Segment 2	Segment 3	Segment 4	· · · ·

The first byte gives the interpretation method for the segment. It consists of two parts; a 3-bit segment type and a 5-bit segment format.

Segment Type			Segment Format				
7	6	5	4	3	2	1	0

The segment type specifications are defined as follows in the CIP specifications.

Segment Type			Meaning
7	6	5	
0	0	0	Port Segment
0	0	1	Logical Segment
0	1	0	Network Segment
0	1	1	Symbolic Segment
1	0	0	Data Segment
1	0	1	Data Type
1	1	0	Data Type
1	1	1	Reserved

The specifications for the segment format are different for each segment type. Use the segment format to request a service from a particular object of a particular device.
Logical segments and data segments, which are needed to specify variables in CIP message communications, are described below.

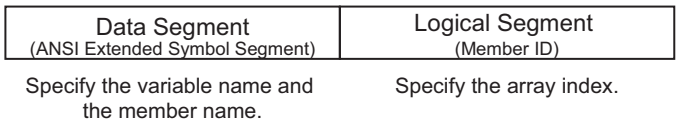
8-3-1 Examples of CIP Object Specifications

Logical Segments are joined to form the request path that specifies the object to access.

Logical Segment (Class ID)	Logical Segment (Instance ID)	Logical Segment (Attribute ID)
Specify the Class ID.	Specify the Instance ID.	Specify the Attribute ID.

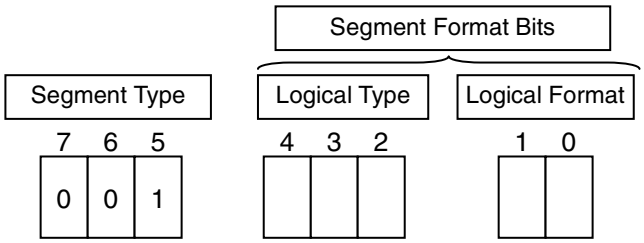
8-3-2 Examples of Variable Specifications

Segments are joined to form the request path that specifies the variable to access.



8-3-3 Logical Segment

A logical segment is used to give the range of the CIP Object or variable (array) in the request path.



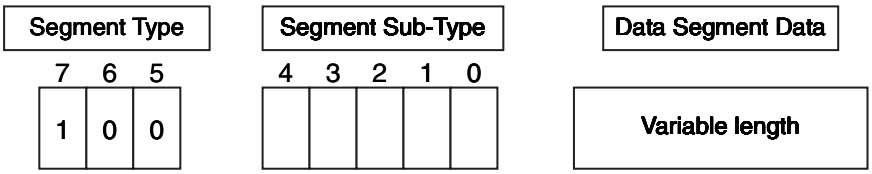
Logical Type			Meaning
4	3	2	
0	0	0	Class ID
0	0	1	Instance ID
0	1	0	Member ID
0	1	1	Connection Point
1	0	0	Attribute ID
1	0	1	Special (Do not use the logical addressing definition for the Logical Format.)
1	1	0	Service ID (Do not use the logical addressing definition for the Logical Format.)
1	1	1	Reserved

Logical Format		Meaning
1	0	
0	0	8 bit logical address
0	1	16 bit logical address
1	0	32 bit logical address
1	1	Reserved

An 8-bit or 16-bit logical address can be used for the class ID and attribute ID.
An 8-bit,16-bit, or 32-bit logical address can be used for the instance ID.

8-3-4 Data Segment

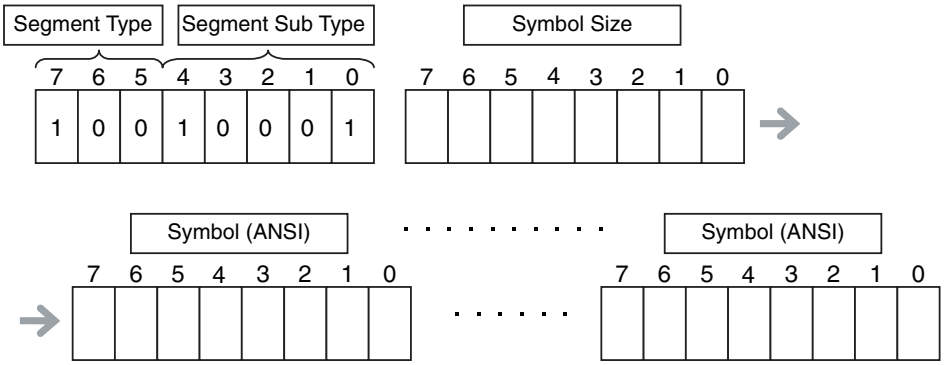
A data segment is used to give the specified variable name in the request path.



Segment Sub-Type					Meaning
4	3	2	1	0	
0	0	0	0	0	Simple Data Segment
1	0	0	0	1	ANSI Extended Symbol Segment

A data segment is mainly used for an ANSI extended symbol segment.
This segment sub-type is used to read and write the values of variables.

ANSI Extended Symbol Segment



8-3-5 Specifying Variable Names in Request Paths

Variable Names

A variable name is specified as a symbolic segment (ANSI extended symbol segment).
Variable Name Specification Format

BYTE	91 hex	ANSI Extended Symbol Segment
BYTE	Length in BYTE	Length of variable name in bytes
Array of octet	: Variable_name :	Variable name encoded in UTF-8
Octet	(pad)	00 hex. One byte is padded if the variable name length is an odd number of bytes.

Variable Names

Variable names are encoded in UTF-8.

Structure Member Names

Structure member names are specified in the same way as variable names.
Store UTF-8 character codes in the ANSI extended symbol segment.

Array Indices

Specify the array index in a logical segment that is set as a member ID.
You can specify an array index ([x]) in a variable name.

(Specification Method 1: 8-bit Index)

BYTE	28 hex	Logical Segment (Member ID)
USINT	Index	Array index from 0 to 255

(Specification Method 2: 16-bit Index)

BYTE	29 hex		Logical Segment (Member ID)
octet	00 hex		Pad
UINT	Index	(L)	Array index from 0 to 65,535
		(H)	

Range Specifications with the Num of Element Field

There is a Num of Element field in the request data for the variable read and variable write services.
You can use these services to access the specified range of an array with the following specifications.

- Specify the first element in the range of elements to access in the array variable as the variable to read or write.
- Specify the number of elements to access in the Num of Element field.

Specification Examples

This example shows how to specify VarAA.MemB[1.2] for the following structure variable.

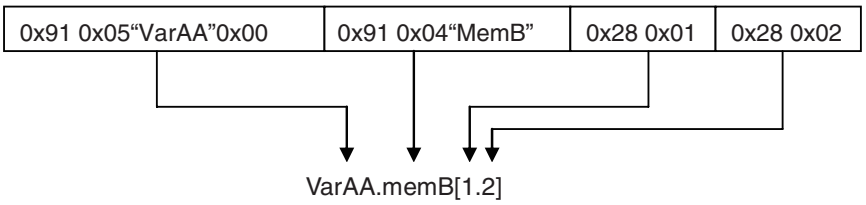
```
struct
{
    UINT    MemA;
    BOOL    MemB[10][10];
} VarAA;
```

Variable Name Specification Format

BYTE	91 hex	ANSI Extended Symbol Segment
BYTE	05 hex	Length of variable name in bytes
Array of octet	'V'	Variable name
	'a'	
	'r'	
	'A'	
	'A'	
Octet	00 hex	Pad
BYTE	91 hex	ANSI Extended Symbol Segment
BYTE	04 hex	Length of variable name in bytes
Array of octet	'M'	Variable name
	'e'	
	'm'	
	'B'	
BYTE	28 hex	Logical Segment (Member ID)
USINT	01 hex	Array index for the first element
BYTE	28 hex	Logical Segment (Member ID)
USINT	02 hex	Array index for the second element

The variable name that is specified in the symbolic segment (ANSI extended symbol segment) must be converted to a text string to pass it to the communications thread. The following conversion rules apply.

Specification Example for Structure Members and Array Elements



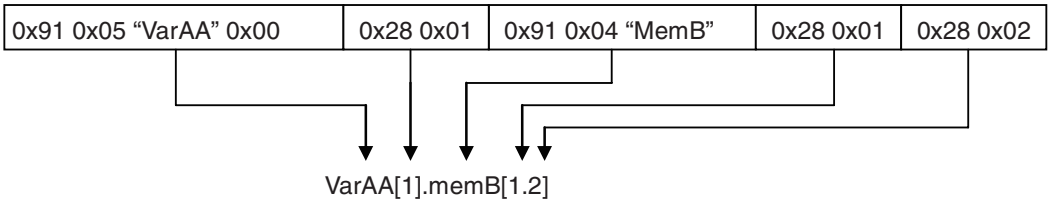
This example shows how to specify VarAA[1].MemB[1.2] for the following structure variable.

```
struct
{
    UINT    MemA;
    BOOL    MemB[10][10];
} VarAA[3]
```

Variable Name Specification Format

BYTE	91 hex	ANSI Extended Symbol Segmer
BYTE	05 hex	Length of variable name in byte:
Array of octet	'V'	Variable name
	'a'	
	'r'	
	'A'	
	'A'	
Octet	00 hex	Pad
BYTE	28 hex	Logical Segment (Member ID)
USINT	01 hex	Array index
BYTE	91 hex	ANSI Extended Symbol Segmer
BYTE	04 hex	Length of variable name in byte:
Array of octet	'M'	Variable name
	'e'	
	'm'	
	'B'	
BYTE	28 hex	Logical Segment (Member ID)
USINT	01 hex	Array index for the first element
BYTE	28 hex	Logical Segment (Member ID)
USINT	02 hex	Array index for the second elem

Specification Example for Structure Array



8-4 CIP Object Services

This section shows services that specify the CIP object in the Request Path and access the CIP message server function of the CIP Safety-compliant Communication Control Unit.

8-4-1 CIP Objects Sent to the Built-in EtherNet/IP Port

The following types of CIP objects can be sent to the built-in EtherNet/IP port.

Object name	Function	Reference
Identity object	• Reads ID information from the Communication Control Unit. • Resets the built-in EtherNet/IP port.	page 8-11
NX configuration object	• Controls NX Units.	page 8-28
TCP/IP interface object	• Reads and writes TCP/IP settings.	page 8-28
Ethernet link object	• Specifies and reads Ethernet settings. • Reads Ethernet status.	page 8-30
Controller object	• Gets the Controller status. • Changes the operating mode of the Controller.	page 8-36

8-4-2 Identity Object (Class ID: 01 hex)

This object reads the ID information of the Communication Control Unit and resets the built-in EtherNet/IP port.
Use the route path to specify the port number (1 or 2) of the built-in EtherNet/IP port to access.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported service range	
			Class	Instance
01 hex	Get_Attribute_All	Reads the values of the attributes.	Supported	Supported
0E hex	Get_Attribute_Single	Reads the value of the specified attribute.	Supported	Supported
05 hex	Reset	Resets the built-in EtherNet/IP port. This parameter is used to reset the built-in EtherNet/IP port when you change the IP address or other parameter settings and want to apply them. Input one of the following values for Request Service Data to specify the reset method. 00 hex: Resets the built-in EtherNet/IP port. 02 hex: Clears the saved tag data link settings and resets the built-in EtherNet/IP port.	Not supported	Supported

Class ID

Specify 01 hex.

Instance ID

Specify 00 or 01 hex.

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attrib-ute	Read data	
				Data type	Value
01 hex	Revision	Revision of the object	Read	UINT	0001 hex
02 hex	Max Instance	The maximum instance number	Read	UINT	0001 hex

● Instance Attribute ID

The instance attribute ID specifies the attribute of the instance.

Attribute ID	Parameter name	Description	Attribute	Read data	
				Data type	Value
01 hex	Vendor ID	Vendor ID	Read	UINT	002F hex
02 hex	Device Type	Device Type	Read	UINT	000C hex
03 hex	Product Code	Product Code	Read	UINT	Refer to (a) for details.
04 hex	Revision	Device revision	Read	Struct	---
	Major Revision	Major revision	Read	USINT	Refer to (b) for details.
	Minor Revision	Minor revision	Read	USINT	
05 hex	Status	Status of the built-in EtherNet/IP port	Read	WORD	Refer to (c) for details.
06 hex	Serial Number	Serial number	Read	UDINT	Set value
07 hex	Product Name	Product name	Read	STRING	Set value

a. Product Codes for Each Model
Model: NX-CSG320
Product code: 0BC0 hex

b. Major and Minor CIP Revisions
Unit version: Unit version 1.00

CIP major revision: 02 hex
CIP minor revision: 06 hex

c. Status Details of the Built-in EtherNet/IP Port

Bit	Name	Description
0	Owned	Indicates when the built-in EtherNet/IP port has an open connection as the target of a tag data link.
1	Reserved	Always FALSE
2	Configured	Tag data link settings exist.
3	Reserved	Always FALSE
4 to 7	Extended Device Status	Indicates the status of the built-in EtherNet/IP port.*1
8	Minor Recoverable Fault	TRUE when any of the following errors occurs. • IP Rout Table Setting Error • DNS Server Connection Failed • Tag Data Link Setting Error • Tag Data Link Timeout • Tag Data Link Connection Timeout • FTP Server Setting Error • NTP Client Setting Error • SNMP Setting Error • NTP Server Connection Failed • Tag Name Resolution Error
9	Minor Unrecoverable Fault	TRUE when the following error occurs. • Identity Error
10	Major Recoverable Fault	TRUE when any of the following errors occurs. • IP Address Duplication Error • BOOTP Server Connection Error • Basic Ethernet Setting Error • IP Address Setting Error
11	Major Unrecoverable Fault	TRUE when any of the following errors occurs. • Communications Controller Failure • MAC Address Error
12 to 15	Reserved	Always FALSE

*1. Status of the built-in EtherNet/IP port for b4 to b7

b7	b6	b5	b4	
0	1	0	1	A major fault occurred.
0	0	1	0	A timeout occurred in one or more target connections.
0	0	1	1	Indicates that there are no tag data link settings.
0	1	1	0	Indicates that one or more connections are performing communications normally.
0	1	1	1	Other than the above.

Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
01 hex	Get_Attribute_All	01 hex	• Specifying a service for a class : 00 hex • Specifying a service for an instance : Always 01 hex	Not required
0E hex	Get_Attribute_Single			• Reading a class attribute : 01 or 02 hex • Reading an instance attribute : 01 to 07 hex
05 hex	Reset		Always 01 hex	Not required

8-4-3 NX Configuration Object (Class ID: 74 hex)

The NX Configuration object is used to control NX Units.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported service range	
			Class	Instance
33	Read NX object	Reads the value of an NX object.	Not supported	Supported
34	Write NX object	Writes the value of an NX object.	Not supported	Supported
35	Restart NX Unit	Restarts an NX Unit.	Not supported	Supported
36	Save parameter	Saves the settings of an NX Unit.	Not supported	Supported
37	Switch parameter write mode	Changes the write mode of the NX Unit.	Not supported	Supported
38	Read total power on time	Reads the total power-ON time of an NX Unit.	Not supported	Supported
3A	Get current error	Reads current errors from an NX Unit.	Not supported	Supported
3B	Get event log	Reads the event log from an NX Unit.	Not supported	Supported
3C	Clear event log	Clears the event log from an NX Unit.	Not supported	Supported
3D	Initialize unit operation parameter	Initializes the setting parameters in an NX Unit.	Not supported	Supported

● Read NX Object (Service Code: 33 hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Read NX object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	33
Request Path Size	Size of request path	USINT	02

Parameter name	Description	Data type	Value (hex)
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Not supported 0001 to 0020: NX Unit 0021 or higher: Not supported
Index	Object dictionary index	UINT	Object dictionary index
Sub index	Object dictionary subindex	USINT	Object dictionary subindex
Control Field	Complete access specification	USINT	00: Not specified

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Read NX object service	USINT	B3
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00
Length	Read data size	UINT	Read data size in bytes
Read data	Read data	Depends on the type of data.	Read data

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Read NX object service	USINT	B3
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
10	Device state conflict
11	Read data too large
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

● Write NX Object (Service Code: 34 hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Write NX object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	34
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Not supported 0001 to 0020: NX Unit 0021 or higher: Not supported
Index	Object dictionary index	UINT	Object dictionary index
Sub index	Object dictionary subindex	USINT	Object dictionary subindex
Control Field	Complete access specification	USINT	00: Not Specified
Length	Write data size	UINT	Data size in bytes
Write data	Write data	Depends on the type of data.	Write data

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Write NX object service	USINT	B4
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Write NX object service	USINT	B4
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
0E	Attribute not settable
10	Device state conflict
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

● Restart NX Unit (Service Code: 35 hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Restart NX unit are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	35
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: All NX Units (excluding Communication Control Unit) 0001 to 0020: NX Unit 0021 or higher: Not supported

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Restart NX unit service	USINT	B5
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Restart NX unit service	USINT	B5
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
10	Device state conflict
13	Not enough data
15	Too much data
1F	Vendor specific error*2
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.
*2. A vendor specific error will occur if you execute this service for an NX Unit that does not support restarting.

Save Parameter (Service Code: 36 hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Save parameter object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	36
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Not supported 0001 to 0020: NX Unit 0021 or higher: Not supported

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Save parameter service	USINT	B6
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Save parameter service	USINT	B6
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
13	Not enough data
15	Too much data
19	Store operation failure
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

Switch Parameter Write Mode (Service Code: 37 hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Switch parameter write mode object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	37
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: All NX Units (excluding Communication Control Unit) 0001 to 0020: NX Unit 0021 or higher: Not supported

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Switch parameter write mode service	USINT	B7
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Switch parameter write mode service	USINT	B7
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
10	Device state conflict
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

● Read Total Power On Time (Service Code: 38 hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Read total power on time object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	38
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Not supported 0001 to 0020: NX Unit 0021 or higher: Not supported

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Read total power on time	USINT	B8
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00
Total power on time	Total power-ON time	ULINT	Total power-ON time

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Read total power on time	USINT	B8
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

● Get Current Error (Service Code: 3A hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Get current error object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	3A
Request Path Size	Size of request path	USINT	02

Parameter name	Description	Data type	Value (hex)
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Communication Control Unit 0001 to 0020: NX Unit 0021 or higher: Not supported
Start number of read record	Number of first record to read	UINT	Number of first record to read
Number of request read record	Requested number of records to read	UINT	Requested number of records to read*1

*1. For Communication Control Unit, the range of values is 0 to 5. For NX Units, it is 0 to 9.

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Get current error service	USINT	BA
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00
Error update count	Total number of errors	UINT	Total number of errors
Record size	Size of one record (bytes)	UINT	0060: Communication Control Unit 0032: NX Unit
Number of registered record	Number of registered records	UINT	Number of registered records
Number of readout record	Number of records that were read*1	UINT	Number of records that were read
Current error record	Current error	ARRAY[0..8] OF STRUCT OF Current error record*2	Current error

*1. The number of current error records specified by Number of readout record are stored in the Current error record array. The remaining elements in the Current error record array are not included in the response data.

*2. The structure specifications are given below.

Structure Specifications for Current Error Record

Communication Control Unit Error

Member name	Meaning	Data Type
Index	Index number of current error*1	UDINT
Event occurred time	Time when error occurred	ULINT
Event source	Event source	UINT
Event priority	Event level	UINT
Event code	Event code*2	UDINT
Code system	Code system	UINT
Event source details	Event source details	UINT
Reserved1	Reserved	UINT
Reserved2	Reserved	UINT
Vendor code	Vendor code of the Unit where an error occurred	UDINT

Member name	Meaning	Data Type
Device type code	Device type code of the Unit where an error occurred	UDINT
Product code	Product code of the Unit where an error occurred	UDINT
Additional information	Attached information for the error	ARRAY[0.. 31] OF BYTE
Reserved3	Reserved	ARRAY[0…23] OF BYTE

NX Unit Error

Member name	Meaning	Data Type
Index	Index number of current error*1	UDINT
Unit number	Unit number 1 to 32: NX Unit	USINT
Event priority	Event Level	UINT
Event occurred time	Time when error occurred	UDINT
Product code	Product code of Unit where error occurred	UDINT
Event code	Event code*2	UDINT
Additional information	Error additional information	ARRAY[0..31] OF BYTE

*1. These numbers are attached in the order that the errors occurred.
*2. Refer to *Error Descriptions and Corrections* in the *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)* for details.

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Get current error service	USINT	BA
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

● Get Event Log (Service Code: 3B hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Get event log object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	3B
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Communication Control Unit 0001 to 0020: NX Unit 0021 or higher: Not supported
Event log type	Type of event log	UINT	0000: System event log 0001: Access event log
Start index of read record	Index number of first record to read	UDINT	Number of first record to read
Number of read record	Number of records to read	UINT	Number of records to read*1

*1. For Communication Control Unit, the range of values is 0 to 5. For NX Units, it is 0 to 9.

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Get event log service	USINT	BB
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00
Record size	Size of one record (bytes)	UINT	0060: Communication Control Unit 0032: NX Unit
Number of registered record	Number of registered records	UINT	Number of registered records
Latest index of registered record	Index number of most recently registered record	UDINT	Index number of most recently registered record
Last index of readout record	Index number of record that was read last	UDINT	Index number of record that was read last
Number of readout record	Number of records that were read*1	UINT	Number of records that were read
Reserved	Reserved	UINT	0000
Event log record[0]	Event log record 0	STRUCT OF Event log record*2	Event log record 0
:	:	:	:
Event log record[8]	Event log record 8	STRUCT OF Event log record*2	Event log record 8

*1. The number of event log records specified by Number of readout record are stored in the Event log record array. The remaining elements in the Event log record array are not included in the response data.
*2. The structure specifications are given below.

Structure Specifications for Event Log Record

Communication Control Unit Event

Member name	Meaning	Data Type
Index	Index number of event log record*1	UDINT
Event occurred time	Time when event occurred	ULINT
Event source	Event source	UINT
Event priority	Event level	UINT
Event code	Event code*2	UDINT
Code system	Code system	UINT
Event source details	Event source details	UINT
Reserved1	Reserved	UINT
Reserved2	Reserved	UINT
Vendor code	Vendor code of the Unit where an error occurred	UDINT
Device type code	Device type code of the Unit where an error occurred	UDINT
Product code	Product code of the Unit where an error occurred	UDINT
Additional information	Event additional information	ARRAY[0.. 31] OF BYTE
Reserved3	Reserved	ARRAY[0…23] OF BYTE

NX Unit Event

Member name	Meaning	Data Type
Index	Index number of event log record*1	UDINT
Unit number	Unit number 1 to 32: NX Unit	USINT
Event priority	Event level	UINT
Event occurred time	Time when event occurred	UDINT
Product code	Product code of Unit where event occurred	UDINT
Event code	Event code*2	UDINT
Additional information	Event additional information	ARRAY[0..31] OF BYTE

*1. These numbers are attached in the order that the errors occurred.
*2. Refer to *Error Descriptions and Corrections* in the *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)* for details.

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Get event log service	USINT	BB
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict

General status code (hex)	Error code*1
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

● Clear Event Log (Service Code: 3C hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Clear event log object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code	USINT	3C
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Communication Control Unit 0001 to 0020: NX Unit 0021 or higher: Not supported
Event log type	Type of event log	UINT	0000: System event log 0001: Access event log 0002: Not used 0003: Both system event log and access event log

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Clear event log service	USINT	BC
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to Clear event log service	USINT	BC
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

● Initialize Unit Operation Parameter (Service Code: 3D hex)

The request format, format for normal responses, format for error responses, and CIP error codes for the Initialize unit operation parameter object are given below.

Request Format

Parameter name	Description	Data type	Value (hex)
Service	Service code*1*2*3	USINT	3D
Request Path Size	Size of request path	USINT	02
Request Path	Request path	Padded EPATH	20742401
Unit No	Unit number	UINT	0000: Not supported 0001 to 0020: NX Unit 0021 or higher: Not supported

*1. The initialized parameters are enabled after the Unit is restarted.
*2. After this service is executed, the NX Unit Memory All Cleared event (event code 95810000hex) is registered.
*3. The NX-series Safety CPU Units do not support this service. An error will occur if you execute this service for an NX-series Safety Control Unit.

Format for Normal Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to the Initialize unit operation parameter service	USINT	BD
Reserved	Reserved	USINT	00
General Status	Code that indicates normal	USINT	00
Size of Additional Status	Size of Additional status	USINT	00

Format for Error Response

Parameter name	Description	Data type	Value (hex)
Reply Service	Reply to the Initialize unit operation parameter service	USINT	BD
Reserved	Reserved	USINT	00
General Status	Current error code defined by CIP	USINT	Current error code
Size of Additional Status	Size of Additional status	USINT	00 or 01*1
Additional status	Additional status	UINT	Additional status*2

*1. If the general status code in the response code is 0x1F (Vendor specific error), the value is 0x01.
*2. The value is stored only when the value of the Size of Additional Status is 0x01.

CIP Error Code

General status code (hex)	Error code*1
02	Resource unavailable
0C	Object state conflict
10	Device state conflict
13	Not enough data
15	Too much data
1F	Vendor specific error
20	Invalid parameter

*1. For details of the individual errors, refer to the appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

Class ID

Specify 74 hex.

Instance ID

Specify 01 hex.

Attribute ID

None

Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
33 hex	Read NX object	74 hex	01 hex (fixed)	Not required
34 hex	Write NX object			
35 hex	Restart NX Unit			
36 hex	Save parameter			
37 hex	Switch parameter write mode			
38 hex	Read total power on time			
3A hex	Get current error			
3B hex	Get event log			
3C hex	Clear event log			
3D hex	Initialize unit operation parameter			

8-4-4 TCP/IP Interface Object (Class ID: F5 hex)

This object is used to read and write settings such as the IP address, subnet mask, and default gateway.
It is necessary to use the route path of the CIP communications command (the *RoutePath* in-out variable) to specify the port number (1 or 2) of the built-in EtherNet/IP port to access.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported service range	
			Class	Instance
01 hex	Get_Attribute_All	Reads the values of the attributes.	Supported	Not supported
0E hex	Get_Attribute_Single	Reads the value of the specified attribute.	Supported	Supported
10 hex	Set_Attribute_Single	Writes a value to the specified attribute. The built-in EtherNet/IP port restarts automatically after the value is written to the attribute. When the next Set_Attribute_Single is executed before the restart process is completed, the general status "0C hex" (Object State Conflict) is returned.	Not supported	Supported

Class ID

Specify F5 hex.

Instance ID

Specify 00 or 01 hex.
00: Specify the class
01: Built-in EtherNet/IP Port

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attribute ID	Parameter name	Description	Attribute	Read data	
				Data type	Value
01 hex	Revision	Revision of the object	Read	UINT	0004 hex
02 hex	Max Instance	The maximum instance number	Read	UINT	0001 hex

Attribute ID	Parameter name	Description	Attribute	Read data	
				Data type	Value
03 hex	Number of Instances	The number of object instances	Read	UINT	0001 hex

● Instance Attribute ID

The instance attribute ID specifies the attribute of the instance.

Attribute ID	Parameter name	Description	Attribute	Write/Read data	
				Data type	Value
01 hex	Interface Configuration Status	Indicates the IP address setting status for the interface.	Read	DWORD	bit 0 to 3: Interface Configuration Status: 0 = IP address is not set. (This includes when BOOTP is starting.) 1 = IP address is set. bit 4 to 5: Reserved (always FALSE) bit 6: AcdStatus: FALSE = IP address collisions have not been detected. TRUE = IP address collisions have been detected. bit 7 to 31: Reserved (always FALSE)
02 hex	Configuration Capability	Indicates the Controller Configurations and Setup that can be set to the interface.	Read	DWORD	bit 0: BOOTP Client: Always TRUE bit 1: DNS Client: Always TRUE bit 2: DHCP Client: Always FALSE bit 3: DHCP - DNS Update: Always FALSE bit 4: Configuration Settable: Always TRUE bit 5: Hardware Configurable: Always FALSE bit 6: Interface Configuration Change Requires Reset: Always FALSE bit 7: ACD Capable: Always TRUE bit 8 to 31: Reserved (always FALSE)
03 hex	Configuration Control	Sets the method used to set the IP address when the interface starts.	Write	DWORD	bit 0: Static IP address bit 1: Set by BOOTP
04 hex	Physical Link Object	The path to the link object in the physical layer	Read	Struct	---
	Path size	The path size (WORD size).		UINT	0002 hex
	Path	The path to the link object in the physical layer (static).		EPATH	20 F6 24 01 hex

Attribute ID	Parameter name	Description	Attribute	Write/Read data	
				Data type	Value
05 hex	Interface Configuration	The interface settings	Write	Struct	---
	IP Address	IP address		UDINT	Set value
	Network Mask	Subnet mask		UDINT	Set value
	Gateway Address	Default gateway		UDINT	Set value
	Name Server	Primary name server		UDINT	Set value
	Name Server2	Secondary name server		UDINT	Set value
	Domain Name	Domain name		STRING	Set value
06 hex	Host Name	Host name (reserved)	Write	STRING	Always 0000 hex

Request Paths to Specify Objects

When you specify an object, specify the request path for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
01 hex	Get_Attribute_All	F5 hex	• Specifying a service for a class: 00 hex • Specifying a service for an instance: 01 hex	Not required
0E hex	Get_Attribute_Single			• Reading a class attribute: 01 to 03 hex • Reading and writing an instance attribute: 01 to 06 hex
10 hex	Set_Attribute_Single			

● Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
0E hex	Get_Attribute_Single	C4 hex	00 hex	Specifies the attribute of the class to read or write : 01 hex, 02 hex, or 64 to 66 hex
10 hex	Set_Attribute_Single			

8-4-5 Ethernet Link Object (Class ID: F6 hex)

This object is used to set and read Ethernet communications and to read Ethernet communications status information.
It is necessary to use the route path of the CIP communications command (the *RoutePath* in-out variable) to specify the port number (1 or 2) of the built-in EtherNet/IP port to access.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported service range	
			Class	Instance
0E hex	Get_Attribute_Single	Reads the value of the specified attribute.	Supported	Supported

Service code	Parameter name	Description	Supported service range	
			Class	Instance
10 hex	Set_Attribute_Single	Writes a value to the specified attribute.	Support-ed	Support-ed
4C hex	Get_and_Clear	Specify Attribute4 or Attribute5 to reset the value of the attribute to 0.	Not sup-ported	Support-ed

Class ID

Specify F6 hex.

Instance ID

Specify 00 or 01 hex.
00: Specify the class
01: Built-in EtherNet/IP Port

Attribute ID

The attribute ID specifies the information to read.

● Class Attribute ID

The class attribute ID specifies the attribute of the entire object.

Attrib-ute ID	Parameter name	Description	At-trib-ute	Read data	
				Data type	Value
01 hex	Revision	Revision of the object	Read	UINT	0004 hex
02 hex	Max Instance	The maximum instance num-ber	Read	UINT	0001 hex
03 hex	Number of Instances	The number of object instan-ces	Read	UINT	0001 hex

● Instance Attribute ID

The instance attribute ID specifies the attribute of the instance.

Attribute ID	Parameter name	Description	Attrib-ute	Write/Read data	
				Data type	Value
01 hex	Interface Speed	Gives the baud rate for the in-terface.	Read	UDINT	Reads the current val-ue.
02 hex	Interface Flags	Gives the status of the inter-face.	Read	DWORD	Refer to (a) Interface Flags Details, below.
03 hex	Physical Address	Gives the MAC address of the interface.	Read	ARRAY [0...5] OF USINT	Reads the current val-ue of the MAC ad-dress.

Attribute ID	Parameter name	Description	Attrib-ute	Write/Read data	
				Data type	Value
04 hex	Interface Counters	The number of packets sent and received through the interface.	Read	Struct	---
	In Octets	The number of octets received through the interface. This includes unnecessary multicast packets and discarded packets counted by InDiscards.		UDINT	Reads the current value.
	In Unicast Packets	The number of unicast packets received through the interface. This does not include discarded packets counted by In Discards.		UDINT	Reads the current value.
	In NonUnicast Packets	The number of non-unicast packets received through the interface. This includes unnecessary multicast packets, but does not include discarded packets counted by InDiscards.		UDINT	Reads the current value.
	In Discards	The number of discarded incoming packets received through the interface.		UDINT	Reads the current value.
	In Errors	The number of incoming packets including errors. This is not included in InDiscards.		UDINT	Reads the current value.
	In Unknown Protos	The number of incoming packets that were of an unknown protocol.		UDINT	Reads the current value.
	Out Octets	The number of octets sent through the interface.		UDINT	Reads the current value.
	Out Unicast Packets	The number of unicast packets sent through the interface.		UDINT	Reads the current value.
	Out NonUnicast Packets	The number of non-unicast packets sent through the interface.		UDINT	Reads the current value.
	Out Discards	The number of discarded sent packets.		UDINT	Reads the current value.
	Out Errors	The number of sent packets that had errors.		UDINT	Reads the current value.

Attribute ID	Parameter name	Description	Attribute	Write/Read data	
				Data type	Value
05 hex	Media Counters	Media counters for the communications port.	Read	Struct	---
	Alignment Errors	Number of frames received that were not octets in length.		UDINT	Reads the current value.
	FCS Errors	Number of frames received that did not pass the FCS check.		UDINT	Reads the current value.
	Single Collisions	Number of frames sent successfully with only one collision.		UDINT	Reads the current value.
	Multiple Collisions	Number of frames sent successfully with two or more collisions.		UDINT	Reads the current value.
	SQE Test Errors	Number of times a SQE test error message was generated.		UDINT	Reads the current value.
	Deferred Transmissions	The number of frames for which the first attempt to send was delayed because the media was busy.		UDINT	Reads the current value.
	Late Collisions	The number of collisions detected in packets that were sent after 512 bit times.		UDINT	Reads the current value.
	Excessive Collisions	The number of frames that failed to be sent because of excessive collisions.		UDINT	Reads the current value.
	MAC Transmit Errors	The number of frames that failed to be sent due to an internal MAC sublayer transmission error.		UDINT	Reads the current value.
	Carrier Sense Errors	The number of times the carrier sense conditions were lost or the number of times an assertion failure occurred when an attempt was made to send the frame.		UDINT	Reads the current value.
	Frame Too Long	The number of frames received that exceeded the maximum allowed frame size.		UDINT	Reads the current value.
	MAC Receive Errors	The number of frames that could not be received through the interface due to an internal MAC sublayer reception error.		UDINT	Reads the current value.
06 hex	Interface Control	Control settings for the interface.	Write	Struct	---
	Control Bits	Specify Auto Nego and full duplex for Ethernet communications.		WORD	Refer to (b) Control Bits Details, below.
	Forced Interface Speed	Gives the set value of the Ethernet baud rate.		UINT	Reads the setting value.

Attribute ID	Parameter name	Description	Attribute	Write/Read data	
				Data type	Value
0C hex	HC Interface Counters	The number of packets sent/received through the HC interface.	Read	Struct	---
	HCInOctets	The number of octets received through the interface. This counter is the 64-bit edition of In Octets.		ULINT	Reads the current value.
	HCInUnicastPkts	The number of unicast packets received through the interface. This counter is the 64-bit edition of In Ucast Packets.		ULINT	Reads the current value.
	HCInMulticastPkts	The number of multicast packets received through the interface.		ULINT	Reads the current value.
	HCInBroadcastPkts	The number of broadcast packets received through the interface.		ULINT	Reads the current value.
	HCOutOctets	The number of octets sent through the interface.		ULINT	Reads the current value.
	HCOutUnicastPkts	The number of unicast packets sent through the interface. This counter is the 64-bit edition of Out Octets.		ULINT	Reads the current value.
	HCOutMulticastPkts	The number of multicast packets sent through the interface.		ULINT	Reads the current value.
	HCOutBroadcastPkts	The number of broadcast packets sent through the interface.		ULINT	Reads the current value.

Attribute ID	Parameter name	Description	Attribute	Write/Read data	
				Data type	Value
0D hex	HC Media Counters	Media counters for the communications port.	Read	Struct	---
	HCStatsAlignmentErrors	The number of frames received that were not octets in length. This counter is the 64-bit edition of Alignment Errors.		ULINT	Reads the current value.
	HCStatsFCSErrors	The number of frames received that did not pass the FCS check. This counter is the 64-bit edition of FCS Errors.		ULINT	Reads the current value.
	HCStatsInternalMacTransmitErrors	The number of frames that failed to be sent due to an internal MAC sublayer transmission error. This counter is the 64-bit edition of MAC Transmit Errors.		ULINT	Reads the current value.
	HCStatsFrameTooLongs	The number of frames received that exceeded the maximum allowed frame size. This counter is the 64-bit edition of Frame Too Long.		ULINT	Reads the current value.
	HCStatsInternalMacReceiveErrors	The number of frames that could not be received through the interface due to an internal MAC sublayer reception error. This counter is the 64-bit edition of MAC Receive Errors.		ULINT	Reads the current value.
	HCStatsMASymbolErrors	The number of frames that could not be received through the interface due to an internal MAC sublayer rsymbol error.		ULINT	Reads the current value.

a. Interface Flag Details

Bit	Name	Description
0	LinkStatus	FALSE: The link is down. TRUE: The link is up.
1	Half/FullDuplex	FALSE: Half duplex TRUE: Full duplex
2 to 4	Negotiation Status	00 hex: Auto-negotiation is in progress. 01 hex: Auto-negotiation and speed detection failed. 02 hex: Auto-negotiation failed, but speed detection succeeded. 03 hex: Speed and duplex mode negotiation succeeded. 04 hex: Auto-negotiation was not attempted.
5	Manual Setting Requires Speed	Always FALSE: Changes can be applied automatically.
6	Local Hardware Fault	Always FALSE
7 to 31	Reserved	Always FALSE

b. Control Bits Details

Bit	Name	Description
0	Auto-negotiate	FALSE: Auto-negotiation is disabled. TRUE: Auto-negotiation is enabled.
1	ForcedDuplex Mode	FALSE: Half duplex TRUE: Full duplex*1
2 to 16	Reserved	Always FALSE

*1. When auto-negotiation is enabled (bit 0 is TRUE), this should always be FALSE.

Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
0E hex	Get_Attribute_Single	F6 hex	• Specifying a service for a class: 00 hex • Specifying a service for an instance: Always 01 hex	• Reading a class attribute: 01 to 03 hex • Reading and writing a instance attribute: 01 to 06 hex, 0C hex, and 0D hex
10 hex	Set_Attribute_Single			
4C hex	Get_and_Clear			Specify an attribute to clear the value to 0: 04 hex, 05 hex, 0C hex, 0D hex

8-4-6 Controller Object (Class ID: C4 hex)

This object is used to get the status of the Controller or to change the operating mode of the Controller.

Service Codes

Specify the service to execute with the service code.

Service code	Parameter name	Description	Supported service range	
			Class	Instance
0E hex	Get_Attribute_Single	Reads the value of the specified attribute.	Supported	Not supported
10 hex	Set_Attribute_Single	Writes a value to the specified attribute.	Supported	Not supported
51 hex	Reset_System_Alarm_All	Clears all errors of Communication Control Unit.	Supported	Not supported

Class ID

Specify C4 hex.

Instance ID

Specify 00 hex.

● Class Attribute ID

The class attribute ID specifies the attribute (value) of the entire object.

Attribute ID	Parameter name	Description	Attrib-ute	Write/Read data	
				Data type	Value
01 hex	Revision	Revision of the object	Read	UINT	Always 0002 hex
02 hex	Max Instance	The maximum instance number	Read	UINT	Always 0001 hex
65 hex	PLC Error Status	Indicates when there is a Controller error. Changes to TRUE when a fatal or non-fatal error occurs.	Read	UINT	0000 hex: There is no Controller error. 0001 hex: There is a Controller error.
66 hex	PLC Model	Indicates the model of the Controller. The length is always 2 bytes for the size + 20 bytes for the name. Unused area is padded with spaces.	Read	STRING	

● Instance Attribute ID

None

Request Paths (IOIs) to Specify Objects

When you specify an object, specify the request path (IOI) for each service code as given below.

Service code		Class ID	Instance ID	Attribute ID
0E hex	Get_Attribute_Single	C4 hex	00 hex	Specifies the attribute of the class to read or write: 01 hex, 02 hex, or 64 to 66 hex
10 hex	Set_Attribute_Single			

8-5 Read and Write Services for Variables

This section shows services that specify the variables in the Request Path and access the CIP message server function of the CIP Safety-compliant Communication Control Unit.

8-5-1 Read Service for Variables

Specify service code 4C hex to read the value of the variable that is specified by the request path.

Service code: 4C hex

● Request Data Format

Request Path Data

Variable name specification

Request Service Data

+0	Num of Element (L)	UINT	Specify the number of elements to read for an array variable.
+1	(H)		

Response Service Data

Data Type	USINT	Data type of variable to read
AddInfo Length	USINT	Additional information: Field length in bytes
(AddInfo)		Additional information: CRC value of structure
Actual data*		

*1. The actual data is stored in little-endian format.

Data Type	Code for data type of variable to read. Refer to *8-6-1 Data Type Codes* on page 8-42.
AddInfoLength	The size of the AddInfo area is stored only when accessing a structure variable. Set 02 hex for a structure variable. Otherwise, set 00 hex.
AddInfo	The CRC code of the structure definition is stored only when accessing a structure variable. In this case, the size of AddInfo will be 2 bytes.
Actual data	The actual data is stored in little-endian format. If 0001 hex is specified for an array, the actual data is stored in the same format as when you access a variable with the data type of the elements of the array.

Response Codes

CIP status	Meaning	Add status	Cause
00	SUCCESS	---	The service ended normally.
02	RESOURCE_UNAVAILABLE	---	The internal processing buffer is not available.
04	PATH_SEGMENT_ERROR	---	The request path specification is not correct.
05	PATH_DESTINATION_UNKNOWN	---	The variable specification is not correct.
0C	OBJECT_STATE_CONFLICT	8010	Downloading, starting up, online editing
		8011	There is an error in tag memory.

CIP status	Meaning	Add status	Cause
11	REPLY_DATA_TOO_LARGE	---	The response exceeds the maximum response length.
13	NOT_ENOUGH_DATA	---	The data length was too short for the specified service.
15	TOO_MUCH_DATA	---	The data length was too long for the specified service.
1F	VENDOR_SPECIFIC_ERROR	0102,2104	An attempt was made to read an I/O variable that cannot be read.
		0104,1103	The specified address and size exceed a segment boundary.
		8001	An internal error occurred.
		8007	An inaccessible variable was specified.
		8031	An internal error occurred. (A memory allocation error occurred.)
20	INVALID_PARAMETER	8009	A segment type error occurred.
		800F	There is an inconsistency in data length information in the request data
		8017	More than one element was specified for a variable that does not have elements.
		8018	Zero elements or data that exceeded the range of the array was specified for an array.
		8023	An internal error occurred. (An illegal command format was used.)
		8024	An internal error occurred. (An illegal command length was used.)
		8025	An internal error occurred. (An illegal parameter was used.)
		8027	An internal error occurred. (A parameter error occurred.)
		8028	• An attempt was made to write an out-of-range value for a variable for which a subrange is specified. • An attempt was made to write an undefined value to an enumeration variable.

8-5-2 Write Service for Variables

Specify service code 4D hex to write the value of the variable that is specified by the request path.

Request Data Format for Writing a Variable

Request Path Data

Variable name specification

Request Service Data

Data Type	USINT	Data type of variable to write
AddInfo Length	USINT	Additional information: Field length in bytes
(AddInfo)		Additional information: CRC value of structure
Num of Element (L)	UINT	
(H)		
Actual data*		

Response Service Data

There is no response service data.

*1. Data to write: Store the data to write in little-endian format.

Data Type	Code for data type of variable to write. Refer to *8-6 Variable Data Types* on page 8-42.
AddInfoLength	Specify the size of the AddInfo area only when accessing a structure variable. Set 02 hex for a structure variable. Otherwise, set 00 hex.
AddInfo	The CRC code of the structure definition is specified only when accessing a structure variable. In this case, the size of AddInfo will be 2 bytes.
NumOfElement	Specify the number of elements in the array. Do not specify 0000 hex. (An error will occur.) For variables other than arrays, set 0001 hex.
Actual data	Specify the actual data in the little-endian format. If 0001 hex is specified for an array, the actual data is specified in the same format as when you access a variable with the data type of the elements of the array.

Response Codes

CIP status	Meaning	Add status	Cause
00	SUCCESS	---	The service ended normally.
02	RESOURCE_UNAVAILABLE	---	The internal processing buffer is not available.
04	PATH_SEGMENT_ERROR	---	The request path specification is not correct.
05	PATH_DESTINATION_UNKNOWN	---	The link was followed to the end, but the variable was not found.
0C	OBJECT_STATE_CONFLICT	8010	Downloading, starting up
		8011	There is an error in tag memory.
13	NOT_ENOUGH_DATA	---	The data length was too short for the specified service.
15	TOO_MUCH_DATA	---	The data length was too long for the specified service.

CIP status	Meaning	Add status	Cause
1F	VENDOR_SPECIFIC_ERROR	0102, 2103	An attempt was made to write a constant or read-only variable.
		0104, 1103	The specified address and size exceed a segment boundary.
		8001	An internal error occurred. (An information inconsistency was detected in the interface in the Module.)
		8007	An inaccessible variable was specified.
		8029	A region that all cannot be accessed at the same time was specified for SimpleData-Segment.
		8031	An internal error occurred. (A memory allocation error occurred.)
20	INVALID_PARAMETER	8009	A segment type error occurred.
		800F	There is an inconsistency in data length information in the request data.
		8017	More than one element was specified for a variable that does not have elements.
		8018	Zero elements or data that exceeded the range of the array was specified for an array.
		8021	A value other than 0 and 2 was specified for an AddInfo area.
		8022	• The data type that is specified in the request service data does not agree with the tag information. • The AddInfo Length in the request service data is not 0.
		8023	An internal error occurred. (An illegal command format was used.)
		8024	An internal error occurred. (An illegal command length was used.)
		8025	An internal error occurred. (An illegal parameter was used.)
		8027	An internal error occurred. (A parameter error occurred.)
		8028	• An attempt was made to write an out-of-range value for a variable for which a subrange is specified. • An attempt was made to write an undefined value to an enumeration variable.

8-6 Variable Data Types

This section provides the data types of variables that can be used with CIP message communications.

8-6-1 Data Type Codes

The following codes are given to variable data types.

Data Type	Code (hex)	Group*1
Boolean (bit)	C1	CIP Common
SINT (1-byte signed binary)	C2	CIP Common
INT (1-word signed binary)	C3	CIP Common
DINT (2-word signed binary)	C4	CIP Common
LINT (4-word signed binary)	C5	CIP Common
USINT (1-byte unsigned binary)	C6	CIP Common
UINT (1-word unsigned binary)	C7	CIP Common
UDINT (2-word unsigned binary)	C8	CIP Common
ULINT (4-word unsigned binary)	C9	CIP Common
REAL (2-word floating point)	CA	CIP Common
LREAL (4-word floating point)	CB	CIP Common
STRING	D0	CIP Common
BYTE (1-byte hexadecimal)	D1	CIP Common
WORD (1-word hexadecimal)	D2	CIP Common
DWORD (2-word hexadecimal)	D3	CIP Common
TIME (8-byte data)	DB	CIP Common
LWORD (4-word hexadecimal)	D4	CIP Common
Abbreviated STRUCT	A0	CIP Common
STRUCT	A2	CIP Common
ARRAY	A3	CIP Common
UINT BCD (1-word unsigned BCD)	04	Vendor Specific
UDINT BCD (2-word unsigned BCD)	05	Vendor Specific
ULINT BCD (4-word unsigned BCD)	06	Vendor Specific
ENUM	07	Vendor Specific
DATE_NSEC	08	Vendor Specific
TIME_NSEC	09	Vendor Specific
DATE_AND_TIME_NSEC	0A	Vendor Specific
TIME_OF_DAY_NSEC	0B	Vendor Specific
Union	0C	Vendor Specific

*1. “CIP Common” indicates codes that are defined in the CIP Common Specifications. “Vendor Specific” indicates codes that are assigned by OMRON.

8-6-2 Common Format

The basic format on the data line is shown below.

Data Format

USINT	Data Type		Refer to *Data Type Codes* on page 8-43 for specific values.
USINT	AddInfo Length		Additional information: Field length in bytes
	(AddInfo)		Additional information: CRC value of structure or other information
UINT	Num of Element	(L)	This field exists only in the parameters for the variable write service.
		(H)	
	Actual data		

8-6-3 Elementary Data Types

Fixed-length Byte Data

Applicable data types: BYTE, USINT, and SINT

Data Format

USINT	Data Type		
USINT	00h		
UINT	Num of Elem	(L)	01 hex
		(H)	00 hex
USINT	Data		

Fixed-length 2-byte Data

Applicable data types: INT, UINT, UINT BCD, and WORD

Data Format

USINT	Data Type		
USINT	00h		
UINT	Num of Elem	(L)	01 hex
		(H)	00 hex
	Data	(L)	
		(H)	

Fixed-length 4-byte Data

Applicable data types: DINT, UDINT, UDINT BCD, REAL, and DWORD

Data Format

USINT	Data Type		
USINT	00h		
UINT	Num of Elem	(L)	01 hex
		(H)	00 hex
	Data	(LL)	
		(LH)	
		(HL)	
		(HH)	

Fixed-length 8-byte Data

Applicable data types: LINT, ULINT, ULINT BCD, LREAL, and LWORD

Data Format

USINT	Data Type		
USINT	00 hex		
UINT	Num of Elem	(L)	01 hex
		(H)	00 hex
	Data	(Least-significant byte)	
		:	
		:	
		:	
		:	
		:	
		:	
		(Most-significant byte)	

Boolean Data

Data Format

USINT	Data Type		C1 hex
USINT	00 hex		
UINT	Num of Elem	(L)	01 hex
		(H)	00 hex
USINT	Status		01 hex: TRUE, 00 hex : FALSE
USINT	Forced set/reset information*		01 hex: Forced, 00 hex: Not forced

*1. Specify 0 when writing data.

8-6-4 Derived Data Types

Arrays and structures are handled as derived data types.

Accessing One Member

The data format for accessing one element of an array or one member of a structure is the same as the data format for the corresponding elementary data type.
Example: If you specify Var[5] to access a variable defined with UINT Var[10], use the same data format as for UINT data.

Accessing More Than One Element at the Same Time

● Arrays

- Accessing an Entire Array
  If you access an array variable without specifying an element, the entire array is accessed.

The following data format is used.

Data Format

USINT	Data Type		Data type of array elements (D0 hex is not used.)
USINT	00 hex		
UINT	Num of Elem	(L)	Gives the number of elements in the array.
		(H)	
	Data		The actual data for the elements of the array are given in order in the same format as when the elements are accessed individually.
	:		
	Data		

*1. For STRING data, the output format differs from the format when accessing individual elements in the following ways.

- There is no field for the text string length. Only the text strings (including NULL) are given.
- The transferred data length is not the combined lengths of the text strings, but the memory size that is allocated to the STRING variable.
- Upper and lower bytes are reversed.

Example: The outputs will be as follows for a STRING array named s that has two elements (with the data quantity around elements is set to 4 bytes) when s[0] is “ab” and s[1] is “d”.
s[0]="ab",s[1]="d".
Individual [0]: D0 00 03 00 61 62 63 (hex)
Entire array: D0 00 62 61 ?? 00 00 64 ?? ?? (hex) (??: Invalid data)

- Handling Multi-dimensional Array

  Elements for a multi-dimensional array are given in order from the deepest elements.
  For example, the data is read in the following format when Var is specified for a variable defined with UINT Var[2][2].

Data Format

USINT	C7 hex		Data type code for UINT
USINT	00 hex		
UINT	Value of *Var[0][0]*	(L)	
		(H)	
UINT	Value of *Var[0][1]*	(L)	
		(H)	
UINT	Value of *Var[1][0]*	(L)	
		(H)	
UINT	Value of *Var[1][1]*	(L)	
		(H)	

The following data format is used for a BOOL array (Example: BOOL b[2][3]).

Data Format

USINT	C1 hex (data type code for BOOL)							
USINT	00 hex							
(WORD)	rsv	rsv	b[1][2]	b[1][1]	b[1][0]	b[0][2]	b[0][1]	b[0][0]
	rsv	rsv	rsv	rsv	rsv	rsv	rsv	rsv

- Exceptions When Specifying the Num of Element Field

The following data format is used if a specification is made in the Num of Element field for a BOOL array. (Refer to *8-3-5 Specifying Variable Names in Request Paths* on page 8-7 for information on the Num of Element field.) The status (TRUE/FALSE) is given in order for each element of the BOOL variable.

Data Format

USINT	Data Type		C1 hex
USINT	00 hex		
UINT	Num of Elem	(L)	Gives the number of elements in the array.
		(H)	
USINT	Status		01 hex: TRUE, 00 hex: FALSE
:	:		
USINT	Status		

Structure Variables

- Accessing an Entire Structure
  If a structure variable is specified, it is treated as an access request for all of the members of the structure.

Data Format

USINT	Data Type		A0 hex (Abbreviated STRUCT)
USINT	02 hex		
UINT	CRC	(L)	CRC value for the structure de
		(H)	
UINT	Num of Elem	(L)	01 hex
		(H)	00 hex
	:		
	Data		
	:		

9

TCP/UDP Message Service Function

This section describes the TCP/UDP message service function.

9-1 Overview of the TCP/UDP Message Service Function 9-2

9-2 System Configuration for Using the TCP/UDP Message Service 9-3

9-3 TCP/UDP Message Service Specifications 9-4

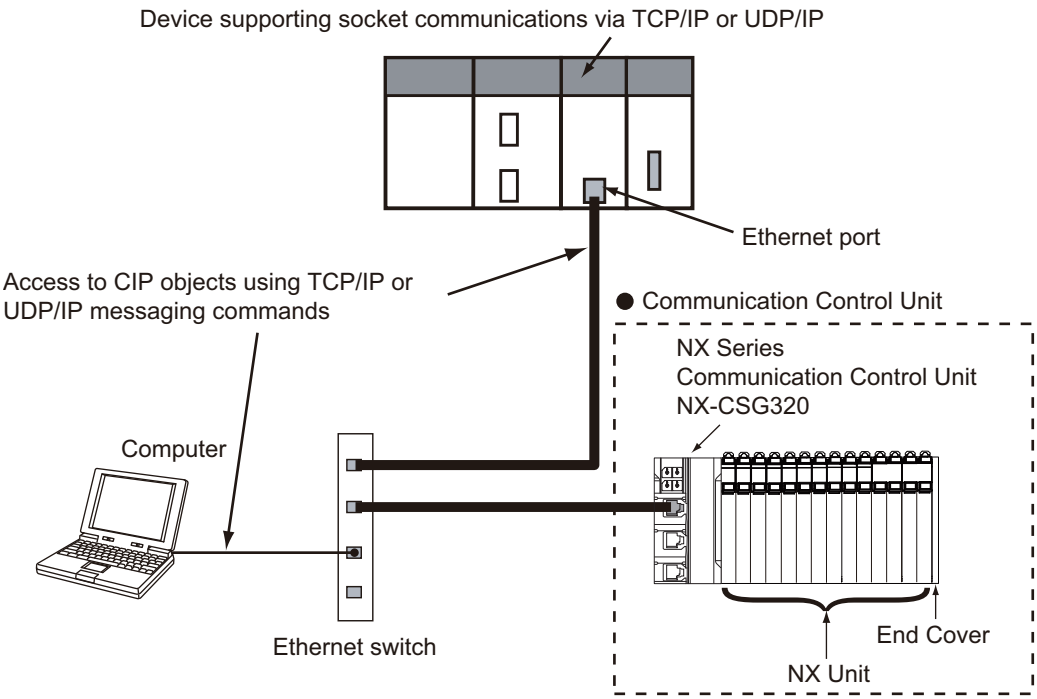
9-3-1 TCP/IP and UDP/IP Message Format 9-4

9-1 Overview of the TCP/UDP Message Service Function

The Communication Control Unit supports the TCP/UDP message service.
You can use the TCP/UDP message service from a PLC or general-purpose computer that does not support the EtherNet/IP protocol to make settings in the Communication Control Unit, control I/O, and perform troubleshooting.
You can send TCP/UDP commands from a device that supports the TCP/IP protocol or UDP/IP protocol (socket communications) to access CIP objects in the Communication Control Unit and thereby control the Communication Control Unit. For details on request commands, refer to *8-4 CIP Object Services* on page 8-11.
Sysmac Studio also allows you to enable and disable the TCP/UDP message service function. Refer to *A-1-7* ***TCP/UDP Message Service Settings*** *Display* on page A-13 for details.

9-2 System Configuration for Using the TCP/UDP Message Service

For a device that does not support EtherNet/IP, you can use the TCP/UDP message service as an alternative to EtherNet/IP communications. Devices such as computers or other controllers can send and receive Omron specific TCP/IP commands and UDP/IP commands to access CIP objects as shown in the figure below.
For details on the CIP objects, refer to *8-4 CIP Object Services* on page 8-11.



9-3 TCP/UDP Message Service Specifications

The Communication Control Unit supports a TCP/UDP message service based on the following specifications.

Item	Name
Maximum number of clients that can connect at one time	64 (TCP: 32, UDP: 32)
Maximum message size	Request: 492 bytes Response: 496 bytes
Maximum data size of NX output	490 bytes*1
Maximum data size of NX input	496 bytes*1
Port number	Default: 64,000 decimal The port number can be changed by Network Configurator (restart required). Acceptable port number ranges are shown below in decimal format. • 1,024 to 2,221 • 2,223 to 44,817 • 44,819 to 65,535

*1. 2 bytes are used for the attribute field in the explicit message UDP/IP command and TCP/IP command.

9-3-1 TCP/IP and UDP/IP Message Format

Command Format

The following format is used to send commands (TCP/IP messages or UDP/IP messages) from a device on Ethernet. The least-significant byte for multi-byte parameters is in the lower address.
The command format is shown below.
The examples of values in the table are the parameter values in little-endian format when the Vendor ID (instance attribute ID 01 hex) in the Identity object (class ID 01 hex) is read.

+0	Message sequence number	2 bytes
+2	Reserved 1	2 bytes
+4	Data size	2 bytes
+6	Reserved 2	1 byte
+7	Service code	1 byte
+8	Class ID	2 bytes
+10	Instance ID	2 bytes
+12	Attribute ID	2 bytes
+14	Data	490 bytes max.

Parameter*1	Address offset	Size (bytes)	Description	Example of a value (hex)
Message sequence number	0	2	Numbers are set to differentiate frames when there is more than one send frame. An arbitrary value is assigned by the device that sends the message. The same value is stored in the corresponding response. Setting range: 0 to 65535	0000
Reserved 1	2	2	Always set to 0.	0000
Data size	4	2	The data size from Reserved 2 to the end of the data is set. The unit is bytes. Setting range: 6 to 498	0800
Reserved 2	6	1	Always set to 0.	00
Service code	7	1	The service code for the destination object is set.	0E
Class ID	8	2	The class ID of the destination object is set.	0100
Instance ID	10	2	The instance ID of the destination object is set.	0100
Attribute ID*2	12	2	Set the attribute ID of the destination object.	0100
Data	14*3	490 max.*4	Set the data. The contents of the data depends on the service code.	---

*1. Parameters in the command are in little-endian order.
*2. This parameter exists only when the command service requires specification of an attribute ID.
*3. If there is no attribute ID, the address offset is 12.
*4. If there is no attribute ID, the maximum size is 492 bytes.

Response Format

The response format is illustrated in the following figure.
The examples of values in the table are the parameter values in little-endian format when the Vendor ID (instance attribute ID 01 hex) in the Identity object (class ID 01 hex) is read.

+0	Message sequence number	2 bytes
+2	Data size	2 bytes
+4	Reserved	1 byte
+5	Service code	1 byte
+6	General status	1 byte
+7	Size of Additional status	1 byte
+8	Data	496 bytes max.

Parameter*1	Address offset	Size (bytes)	Description	Example of a value (hex)
Message sequence number	0	2	The sequence number that was set when the command was sent is returned.	0000
Data size	2	2	The data size from the next parameter to the end of the data is stored. The unit is bytes. Size range: 4 to 500	0600
Reserved	4	1	Always set to 0.	00

Parameter*1	Address offset	Size (bytes)	Description	Example of a value (hex)
Service code	5	1	The service code for the destination object that was set when the command was sent is stored. For a normal response, the most significant bit in the requested service code is turned ON.	8E
General status	6	1	General status code.	00
Size of Additional status	7	1	The number of 16 bit words in additional status array.	00
Data	8	496 max.	If there is no error, the response data is stored here. If there is an error (General status > 0x00), this parameter contains the data for the Additional status array.	2F00

*1. Parameters in the command are in little-endian order.

TCP/IP and UDP/IP Port Number Setting

Refer to *A-1-7* ***TCP/UDP Message Service Settings*** *Display* on page A-13.

Troubleshooting Errors Related to the TCP/UDP Message Service

Use the following information to determine the cause and corrective actions of problems in the TCP/UDP message service.

Observation	General status	Causes	Corrective action
Reading or writing data is not possible. An error response is returned by the Communication Control Unit.	NOT_ENOUGH_DATA (0x13)	The total frame size is larger than 504 bytes. The data-field size value does not match the actual received frame size.	Specify the frame size value under 504 bytes. For details, refer to *9-3 TCP/UDP Message Service Specifications* on page 9-4.
	TOO_MUCH_DATA (0x15)	The data field size value does not match the actual received frame size.	Check the frame size field is calculated correctly. For details, refer to *9-3 TCP/UDP Message Service Specifications* on page 9-4.
	Other error codes	---	Refer to an appendix of *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)*.

Observation	General status	Causes	Corrective action
Reading or writing data is not possible. No error response is returned by the Communication Control Unit.	---	The frame length is smaller than the minimum frame length of 12 bytes.	Check the size of the frame is within specifications.
	---	The data field size value does not match the actual transmitted number of bytes.	Check the size of the frame is the same as the specified number of bytes in the data field.
	---	Unstable network communications.	Check network connections and other sources of interference.
	---	The TCP/UDP message service has not been enabled in the Communication Control Unit.	Check the TCP/UDP message service setting is enabled. Refer to *A-1 Sysmac Studio Settings for the Built-in EtherNet/IP Port* on page A-2 for details.
	---	The frame is sent to a Communication Control Unit with an incorrect port number setting	Check the port number settings. Refer to *TCP/IP and UDP/IP Port Number Setting* on page 9-6 for details.
An unexpected frame size restriction violation occurred during usage of the TCP/UDP message service.	---	The MTU/maximum datagram size is less than the required frame length.	Specify the maximum frame size is the same or less than the maximum allowed datagram size on the client.
Cannot establish a TCP/IP connection.	Standard TCP error	A total of 32 active TCP clients are already connected with the Communication Control Unit.	To establish new TCP/IP connection, make sure that the number of active units connected will be less than 32.
		The TCP/UDP message service function is not enabled in the Communication Control Unit.	The TCP/UDP message service function is disabled. Enable the TCP/UDP message service function in the **TCP/UDP Message Service Settings** Display. Refer to *A-1-7* ***TCP/UDP Message Service Settings*** *Display* on page A-13 for details.
A TCP/IP connection is lost and the client must reconnect.		The TCP/IP connection was idle for more than 30 seconds and a 9th client attempted a connection. In this condition, an idle active client will be automatically closed.	Specify the idle state to less than 30 seconds and keep the client connection active at all times.

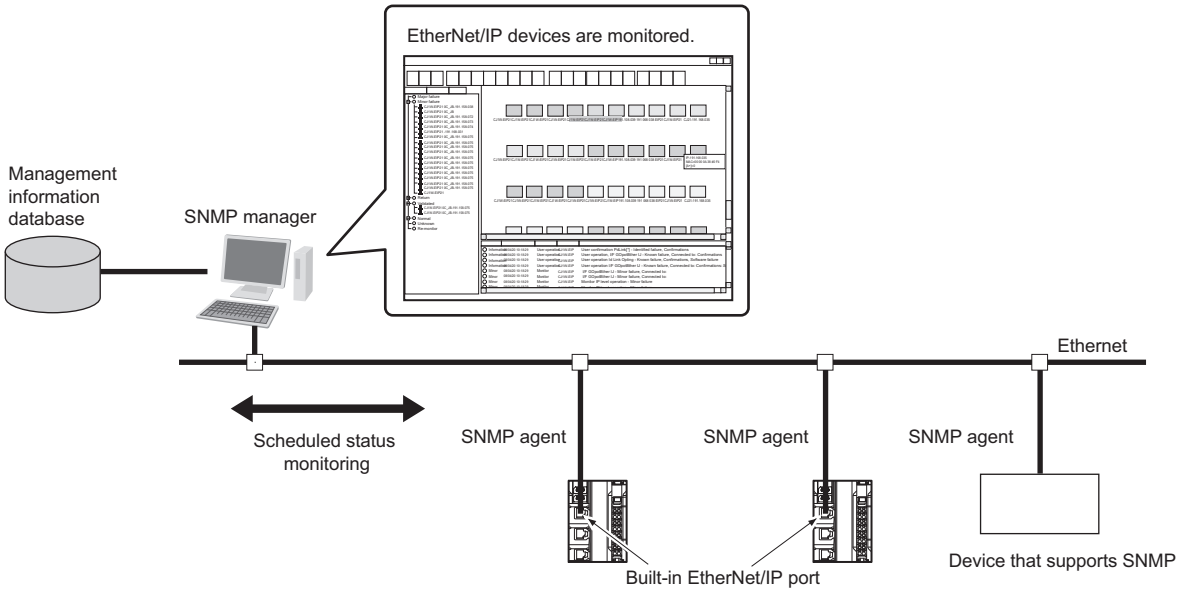
10

SNMP Agent

10-1 SNMP Agent 10-2
10-1-1 Overview 10-2
10-1-2 Specifications 10-3
10-1-3 SNMP Messages 10-3
10-1-4 MIB Specifications 10-4
10-2 Procedure to Use the SNMP Agent 10-20
10-2-1 Procedures 10-20
10-2-2 Settings Required for the SNMP Agent 10-20

10-1 SNMP Agent

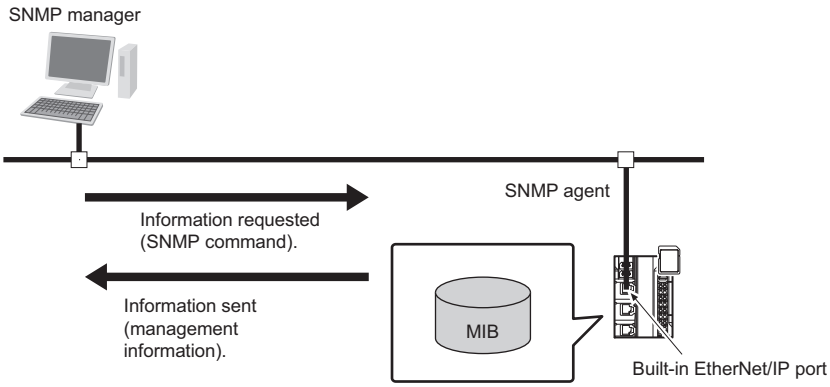
The SNMP (simple network management protocol) is a network management protocol.
You can use the SNMP to manage any network that consists of devices that support SNMP.
The server that manages the network is called the SNMP manager. The managed network devices are called SNMP agents.



10-1-1 Overview

SNMP Agent

The built-in EtherNet/IP port has its own management information called the MIB (management information base). This information can be provided to the SNMP manager.
The SNMP manager is software that gathers and processes information about devices on the SNMP network and provides that information to the network administrator.
You can use the SNMP manager to monitor the built-in EtherNet/IP port.

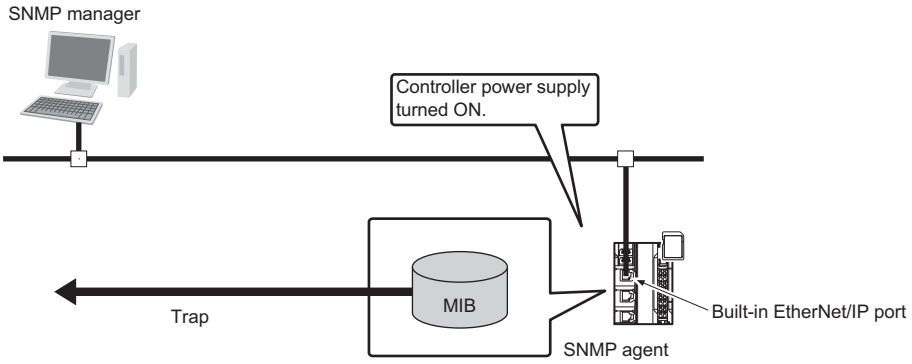


The SNMP manager has a SNMP command to request MIB information.

The built-in EtherNet/IP port SNMP agent function supports SNMPv1 (RFC1157) and SNMPv2C (RFC1901).
Use the SNMPv1 or SNMPv2C protocol to manage the built-in EtherNet/IP port with the SNMP manager. You can also use both the SNMPv1 and SNMPv2C protocols together at the same time.

SNMP Traps

When a failure or some other specific problem occurs, a status report called a trap is sent.
This enables monitoring changes in status even if the SNMP manager does not monitor the built-in EtherNet/IP port periodically.
However, traps use UDP. Therefore, you cannot check to see if the SNMP manager receives traps from the EtherNet/IP port.
Thus, depending on the network status, some traps may not reach the SNMP manager.

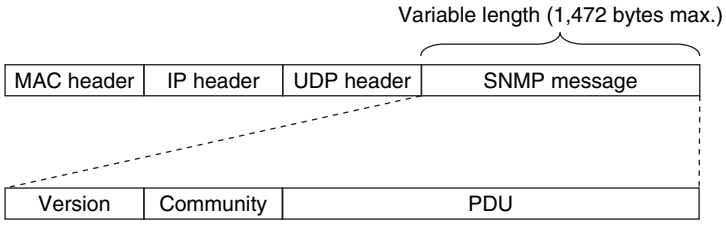


10-1-2 Specifications

Item	Specification
Protocol	SNMP
Agent	SNMPv1, SNMPv2C
MIB	MIB-II
Port No.	SNMP agent: 161 (UDP) SNMP trap: 162 (UDP) These can be changed in the Built-in EtherNet/IP Port Settings from the Sysmac Studio.
Timing of SNMP trap operation	Status reports are sent to the SNMP manager at the following times. • When the Controller is turned ON • When links are established • When an SNMP agent fails to be authorized
Supported MIB commands	GetRequest/GetNextRequest

10-1-3 SNMP Messages

The structure of SNMP messages is as follows:



Item	Set value
Version	This value gives the SNMP version. SNMPv1: 0 SNMPv2C: 1
Community	Community name for verification
PDU	This depends on the PDU type.

10-1-4 MIB Specifications

This section describes the specifications of the MIB that is supported by the built-in EtherNet/IP port.

MIB System Diagram

The built-in EtherNet/IP port MIB consists of the following tree structure.

```
root
└ iso (1)
    └ org (3)
        └ dod (6)
            └ internet (1)
                └ mgmt (2)
                    └ mib-2 (1)
                        ├ -system (1)      Unit information
                        ├ interface (2)    Interface information
                        ├ ip (4)           IP information
                        ├ icmp (5)         ICMP information
                        ├ tcp (6)          TCP information
                        ├ udp (7)          UDP information
                        └ snmp (11)        SNMP information
```

MIB Groups

MIB group		Stored information
Standard MIB	system group	The MIB for information related to the device.
	interfaces group	The MIB for information related to the interface.

MIB group			Stored information
	ip group	ip	The MIB for IP information.
		ipAddrTable	The MIB for addressing table information related to IP addresses.
		ipRouteTable	The MIB for information related to IP routing tables.
		ipNetToMediaTable	The MIB for information related to IP address conversion tables.
		ipForward	The MIB for information related to IP forwarding tables.
	icmp group		The MIB for ICMP information.
	tcp group	tcp	The MIB for TCP information.
	udp group	udp	The MIB for UDP information.
	snmp group	snmp	The MIB for SNMP information.

Detailed Descriptions of MIB Objects

System Group

Subtree name	Standard [(identifier) attribute]	Support	Specifications of implementation
sysDescr	[(1) RO] Device information (including hardware, OS, software names, and versions) ASCII characters only.	Supported	"OMRON Corporation" + CPU Unit model + CPU Unit version • CPU Model: (Example) NX-CSG320 • CPU Version: (Example) Ver.1.0
sysObjectID	[(2) RO] Vendor OID. It indicates where in the private MIB this equipment information was assigned.	Supported	1.3.6.1.4.1.16838.1.1025.5
sysUpTime	[(3) RO] The time elapsed since the system was started (unit: 1/100 s).	Supported	According to the standard.
sysContact	[(4) RW] Administrator contact and information.	Supported	Set by the user.
sysName	[(5) RW] The name for management. Specify a full domain name of the equipment.	Supported	Communication Control Unit name
sysLocation	[(6) RW] The physical location of the device.	Supported	Set by the user.
sysServices	[(7) RO] The value of the provided service.	Supported	64

Interfaces Group

Subtree name	Standard [(identifier) attribute]	Support	Specifications of implementation
ifNumber	[(1) RO] The number of network interfaces.	Supported	3

Subtree name	Standard [(identifier) attribute]	Support	Specifications of implementation
ifTable	[(2) NA] Interface entity table	---	---
ifEntry	[(1) NA] Row data for interface information The index is *ifIndex*.	---	---
ifIndex	[(1) RO] A number used to identify the interface.	Supported	1 to 3
ifDescr	[(2) RO] Information related to the interface (includes manufacturer name, product name, and hardware interface version).	Supported	10/100M Fast Ethernet Port
ifType	[(3) RO] The type of interface classified according to the physical/link layer protocol directly under the network layer of the protocol stack.	Supported	ethernet-csmacd (6)
ifMtu	[(4) RO] MTU value The maximum size (in octets) of datagrams that can be sent and received through this interface.	Supported	1500
ifSpeed	[(5) RO] Estimated bandwidth If a stable, accurate value cannot be obtained for the bandwidth, a nominal value is set instead.	Supported	10000000/100000000
ifPhysAddress	[(6) RO] MAC address The physical address directly under the network layer of this interface	Supported	The MAC address of the EtherNet/IP port
ifAdminStatus	[(7) RW] The preferred status of the interface. You cannot send normal packets in the testing state. up (1) down (2) testing (3)	Supported	According to the standard.
ifOperStatus	[(8) RO] The current status of the interface. You cannot send normal packets in the testing state. up (1) down (2) testing (3)	Supported	According to the standard.
ifLastChange	[(9) RO] The sysUpTime (in 0.01 seconds) at the last change in ifOperStatus for this interface.	Supported	According to the standard.
ifInOctets	The number of octets received through this interface. This includes framing characters.	Supported	According to the standard.
ifInUcastPkts	[(11) RO][(10) RO] The number of unicast packets reported to a higher level protocol.	Supported	According to the standard.

Subtree name			Standard [(identifier) attribute]	Support	Specifications of implementation
		ifInNUcastPkts	[(10) RO[(12) RO] The number of non-unicast packets (broadcast or multicast packets) reported to a higher level protocol.	Supported	According to the standard.
		ifInDiscards	[(13) RO] The number of packets that had no errors but could not be passed to a higher level protocol (i.e., the number of packets received but discarded due to a buffer overflow).	Supported	According to the standard.
		ifInErrors	[(14) RO] The number of packets discarded because they contained errors.	Supported	According to the standard.
		ifInUnknown-Protos	[(15) RO] The number of packets received, but discarded because they were of an illegal or unsupported protocol. For example, Ethernet packets did not have IP set for the field that identifies their higher level protocol.	Supported	According to the standard.
		ifOutOctets	[(16) RO] The number of octets of packets sent through this interface. This includes framing characters.	Supported	According to the standard.
		ifOutUcastPkts	[(17) RO] The number of unicast packets sent by higher level protocols. Discarded and unsent packets are also included.	Supported	According to the standard.
		ifOutNU-castPkts	[(18) RO] The number of non-unicast packets sent by higher level protocols. This includes discarded packets and unsent packets.	Supported	According to the standard.
		ifOutDiscards	[(19) RO] The number of packets that had no errors but were discarded in the sending process due to a send buffer overflow, etc.	Supported	According to the standard.
		ifOutErrors	[(20) RO] The number of packets that could not be sent because of an error.	Supported	According to the standard.
		ifOutQLen	[(21) RO] The size of the send packet queue (i.e., the number of packets).	Supported	Always 0
		ifSpecific	[(22) RO] The object ID that represents a reference to the media-specific MIB for the interface. For example, for Ethernet, set the object ID of the MIB that defines Ethernet. If there is no information, set { 0.0 }.	Supported	0.0

Ip Group: Ip

Subtree name	Standard [(identifier) attribute]	Support	Specifications of implementation
ipForwarding	[(1) RW] Indicates if the device operates as a gateway. IP gateways can transfer datagrams, but IP hosts can perform only source routing. Some nodes take only one of these values. Therefore, if you try to change this object using the SNMP Manager, a badValue error is returned. Forwarding (1) Not-forwarding (2)	Supported	forwarding (1) not-forwarding (2)
IpDefaultTTL	[(2) RW] The default value set for the IP header TTL if no TTL value was given by the transport layer protocol.	Supported	64
IpInReceives	[(3) RO] The number of all IP datagrams that reached the interface, including errors.	Supported	According to the standard.
IpInHdrErrors	[(4) RO] The number of received datagrams that were discarded because of IP header errors, such as a checksum error, a version number error, a format error, a TTL error, an IP option error, etc.	Supported	According to the standard.
IpInAddrErrors	[(5) RO] The number of packets that were discarded because the destination IP address in the IP header was not valid.	Supported	According to the standard.
ipForwDatagrams	[(6) RO] The number of IP datagrams that were transferred to their final destination. If this node does not operate as an IP gateway, it is the number of datagrams that were successfully transferred by the source routing.	Supported	According to the standard.
ipInUnknownProtos	[(7) RO] The number of IP datagrams that were received but discarded because they were of an unsupported or unrecognized protocol.	Supported	According to the standard.
ipInDiscards	[(8) RO] The number of IP datagrams that were discarded due to insufficient buffer space or other problems although they will not cause interference with the subsequent processing.	Supported	According to the standard.
ipInDelivers	[(9) RO] The number of datagrams delivered to an IP user protocol (any higher level protocol, including ICMP).	Supported	According to the standard.

Subtree name	Standard [(identifier) attribute]	Support	Specifications of implementation
ipOutRequests	[(10) RO] The number of times a send request was made for an IP datagram by a local IP user protocol (any higher level protocol, including ICMP). This counter does not include *ipForwDatagrams*.	Supported	According to the standard.
ipOutDiscards	[(11) RO] The number of IP datagrams that were discarded due to insufficient buffer space or other problems although they can be sent out without problems.	Supported	According to the standard.
ipOutNoRoutes	[(12) RO] The number of IP datagrams that were discarded because there was no transmission path. This counter includes datagrams that attempted to be sent through *ipForwDatagrams*, but were discarded because they were set with no-route. This value is the number of datagrams that were not sent out because the default gateway was down.	Supported	According to the standard.
ipReasmTimeout	[(13) RO] The maximum number of seconds to wait to receive all IP datagrams for reassembly if a fragmented IP datagram is received.	Supported	60 sec
ipReasmReqds	[(14) RO] The number of IP datagrams received that require reassembly. There is a flag in the IP header that indicates if the datagram is fragmented. You can use that flag to identify fragments.	Supported	According to the standard.
ipReasmOKs	[(15) RO] The number of IP datagrams received that were successfully reassembled.	Supported	According to the standard.
ipReasmFails	[(16) RO] The number of IP datagrams received that were not successfully reassembled.	Supported	According to the standard.
ipFragOKs	[(17) RO] The number of IP datagrams that were successfully fragmented.	Supported	According to the standard.
ipFragFails	[(18) RO] The number of IP datagrams that were not successfully fragmented. (For example, because the Don’t Fragment flag was set for the IP datagram.)	Supported	According to the standard.
ipFragCreates	[(19) RO] The number of IP datagrams created as a result of fragmentation.	Supported	According to the standard.
ipAddrTable	[(20) NA] An address information table for IP addresses.	---	---

Subtree name	Standard [(identifier) attribute]	Support	Specifications of implementation
ipAddrEntry	[(1) NA] Row data of address information for IP addresses. The index is *ipAdEntAddr*.	---	---
ipAdEntAddr	[(1) RO] The IP address.	Supported	According to the standard.
ipAdEntIfIndex	[(2) RO] The index value of the interface that this entry applies to. The same value as ifIndex.	Supported	According to the standard.
ipAdEntNetMask	[(3) RO] The subnet mask for the IP address of this entry.	Supported	According to the standard.
ipAdEntBcastAddr	[(4) RO] The value of the least significant bit of the address when an IP broadcast is sent. An address represented by all 1 bits is used for broadcasting as an Internet standard. In that case, this value is always 1.	Supported	According to the standard.
ipAdEntReasmMaxSize	[(5) RO] The maximum IP packet size that can be reassembled from IP fragmented input IP datagrams received through the interface.	Supported	According to the standard.
ipRouteTable	[(21) NA] The IP routing table for this entity.	---	---
ipRouteEntry	[(1) NA] Route information for a specific destination. The index is *ipRouteDest*.	---	---
ipRouteDest	[(1) RW] The destination IP address for this route. A value of 0.0.0.0 for this entry indicates the default route.	Supported	According to the standard.
ipRouteIfIndex	[(2) RW] The ID number of the interface required to send to the next destination host in this route. This ID number is the same number as *ifIndex*, which is used to identify the interface.	Supported	According to the standard.
ipRouteMetric1	[(3) RW] The primary routing metric for this route. This value is determined based on the protocol specified in ipRouteProto. Set to −1 if you do not want to use this metric (this is also the same for ipRouteMetric 2 through 4).	Supported	According to the standard.
ipRouteMetric2	[(4) RW] The alternative routing metric for this route.	Supported	According to the standard.
ipRouteMetric3	[(5) RW] The alternative routing metric for this route.	Supported	According to the standard.
ipRouteMetric4	[(6) RW] The alternative routing metric for this route.	Supported	According to the standard.

Subtree name			Standard [(identifier) attribute]	Support	Specifications of implementation
		ipRouteNextHop	[(7) RW] The IP address of the next hop in this route (for routes connected by a broadcast or media, this is the agent address or address of that interface).	Supported	According to the standard.
		ipRouteType	[(8) RW] The type of route. other (1): Not any of the following types. invalid (2): An invalid route. direct (3): A direct connection. indirect (4): An indirect connection (not connected to LOCAL).	Supported	According to the standard.
		ipRouteProto	[(9) RO] This is the routing mechanism used to determine routes. Some values correspond to gateway routing protocols, but be aware that the host may not support those protocols. Other (1): Other than the following items. Local (2): A route set on the local machine. Netmgmt (3): A route set by network management. Icmp (4): A route set by an ICMP redirect or some other ICMP function. Egp (5): EGP The following are gateway protocols: Ggp (6): GGP Hello (7): HELLO rip (8): RIP is-is (9) es-is (10) ciscolgrp (11) bbnSpflgp (12) ospf (13): OSPF bgp (14)	Supported	According to the standard.
		ipRouteAge	[(10) RW] The elapsed time since this route was updated (in seconds).	Supported	Always 0
		ipRouteMask	[(11) RW] The subnet mask value in relation to ipRouteDest. For systems that do not support any subnet mask values, this value is determined by the address class of the ipRouteDest field. When ipRouteDest is 0.0.0.0, this value also becomes 0.0.0.0.	Supported	According to the standard.
		ipRouteMetric5	[(12) RW] The alternative routing metric.	Supported	According to the standard.
		ipRouteInfo	[(13) RO] The MIB object ID for the routing protocol used by this route. If not defined, set to {0.0}.	Supported	0.0

Subtree name	Standard [(identifier) attribute]	Support	Specifications of implementation
ipNetToMediaTable	[(22) NA] The IP address conversion table used to map IP addresses to physical addresses.	---	---
ipNetToMediaEntry	[(1) NA] Row data for the conversion table. The indices are *ipNetToMediaIfIndex* and *ipNetToMediaNetAddress*.	---	---
ipNetToMediaIfIndex	[(1) RW] The interface ID number for this entry. The value of *ifIndex* is used for this value.	Supported	According to the standard.
ipNetToMediaPhysAddress	[(2) RW] The media-dependent physical address.	Supported	According to the standard.
ipNetToMediaNetAddress	[(3) RW] The IP address that corresponds to the media-dependent physical address.	Supported	According to the standard.
ipNetToMediaType	[(4) RW] The address conversion method. Other (1): A method other than the following items. Invalid (2): An invalid value. Dynamic (3): Dynamic conversion. Static (4): Static conversion.	Supported	According to the standard.
ipRoutingDiscards	[(23) RO] The number of routing entries that were valid but discarded. For example, if there was not enough buffer space because of other routing entries.	Supported	According to the standard.

● Ip Group: Icmp

Name	Standard [(identifier) attribute]	Support	Specifications of implementation
icmpInMsgs	[(1) RO] The total number of received ICMP messages. This includes messages counted by icmpInErrors.	Supported	According to the standard.
icmpInErrors	[(2) RO] The number of received ICMP message errors, including checksum errors and frame length errors.	Supported	According to the standard.
icmpInDestUnreachs	[(3) RO] The number of Destination Unreachable messages received.	Supported	According to the standard.
icmpInTimeExcds	[(4) RO] The number of Time Exceed messages received.	Supported	According to the standard.
icmpInParmProbs	[(5) RO] The number of Parameter Problem messages received.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Specifications of implementation
icmpInSrcQuenchs	[(6) RO] The number of Source Quench messages received.	Supported	According to the standard.
icmpInRedirects	[(7) RO] The number of Redirect messages received.	Supported	According to the standard.
icmpInEchos	[(8) RO] The number of Echo (request) messages received.	Supported	According to the standard.
icmpInEchoReps	[(9) RO] The number of Echo Reply messages received.	Supported	According to the standard.
icmpInTimestamps	[(10) RO] The number of Timestamp messages received.	Supported	According to the standard.
icmpInTimestampReps	[(11) RO] The number of Timestamp Reply messages received.	Supported	According to the standard.
icmpInAddrMasks	[(12) RO] The number of Address Mask Request messages received.	Supported	According to the standard.
icmpInAddrMaskReps	[(13) RO] The number of Address Mask Reply messages received.	Supported	According to the standard.
icmpOutMsgs	[(14) RO] The total number of ICMP messages sent. This includes messages counted by *icmpOutErrors*.	Supported	According to the standard.
icmpOutErrors	[(15) RO] The number of ICMP messages that could not be sent because of an error.	Supported	According to the standard.
icmpOutDestUnreachs	[(16) RO] The number of Destination Unreachable messages sent.	Supported	According to the standard.
icmpOutTimeExcds	[(17) RO] The number of Time Exceed messages sent.	Supported	According to the standard.
icmpOutParmProbs	[(18) RO] The number of Parameter Problem messages sent.	Supported	According to the standard.
icmpOutSrcQuenchs	[(19) RO] The number of Source Quench messages sent.	Supported	According to the standard.
icmpOutRedirects	[(20) RO] The number of Redirect messages sent.	Supported	According to the standard.
icmpOutEchos	[(21) RO] The number of Echo (request) messages sent.	Supported	According to the standard.
icmpOutEchoReps	[(22) RO] The number of Echo Reply messages sent.	Supported	According to the standard.
icmpOutTimestamps	[(23) RO] The number of Timestamp messages sent.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Specifications of implementation
icmpOutTimestampReps	[(24) RO] The number of Timestamp Reply messages sent.	Supported	According to the standard.
icmpOutAddrMasks	[(25) RO] The number of Address Mask Request messages sent.	Supported	According to the standard.
icmpOutAddrMaskReps	[(26) RO] The number of Address Mask Reply messages sent.	Supported	According to the standard.

● Ip Group: Tcp

Name	Standard [(identifier) attribute]	Support	Specifications of implementation
tcpRtoAlgorithm	[(1) RO] The algorithm used to determine the timeout value for resending. Other (1): Other than the following items. Constant (2): A constant RTO value. Rsre (3): The algorithm specified by the MIL-STD-1778 standard. Vanj (4): The Van Jacobson algorithm.	Supported	According to the standard.
tcpRtoMin	[(2) RO] The minimum resend timeout value (in 0.01 s). This value depends on the algorithm used to determine the resend timeout value.	Supported	According to the standard.
tcpRtoMax	[(3) RO] The maximum resend timeout value (in 0.01 s). This value depends on the algorithm used to determine the resend timeout value.	Supported	According to the standard.
tcpMaxConn	[(4) RO] The total number of supported TCP connections. If the maximum number of connections is dynamic, this value is -1.	Supported	According to the standard.
tcpActiveOpens	[(5) RO] The number of times the TCP connection changed from the CLOSE state directly to the SYN-SENT state. (Active connection established)	Supported	According to the standard.
tcpPassiveOpens	[(6) RO] The number of times the TCP connection changed from the LISTEN state directly to the SYN-RCVD state. (Passive connection established)	Supported	According to the standard.
tcpAttemptFails	[(7) RO] The total number of times the TCP connection changed from the SYN-SENT or SYN-RCVD state directly to the CLOSE state and from the SYN-RCVD state directly to the LISTEN state.	Supported	According to the standard.

Name	Standard [(identifier) attribute]	Support	Specifications of implementation
tcpEstabResets	[(8) RO] The number of times the TCP connection changed from the ESTABLISHED or the CLOSE-WAIT state directly to the CLOSE state.	Supported	According to the standard.
tcpCurrEstab	[(9) RO] The total number of TCP connections currently in the ESTABLISHED or the CLOSE-WAIT state.	Supported	According to the standard.
tcpInSegs	[(10) RO] The total number of received segments. This includes the number of error segments.	Supported	According to the standard.
tcpOutSegs	[(11) RO] The total number of sent segments. This includes the number of segments for the current connection, but does not include the number of segments for resent data only.	Supported	According to the standard.
tcpRetransSegs	[(12) RO] The total number of resent segments.	Supported	According to the standard.
tcpConnTable	[(13) NA] The information table specific to the TCP connection.	---	---

Name	Standard [(identifier) attribute]	Support	Specifications of implementation
tcpConnEntry	[(1) NA] Entry information related to a specific TCP connection. This value is deleted when the connection changes to the CLOSE state. The indices are *tcpConnLocalAddress*, *tcpConnLocalPort*, *tcpConnRemAddress*, and *tcpConnRemPort*.	---	---
tcpConnState	[(1) RW] The status of the TCP connection. closed (1) listen (2) synSent (3) synReceived (4) established (5) finWait1 (6) finWait2 (7) closeWait (8) lastAck (9) closing (10) timeWait (11)	Supported	According to the standard.
tcpConnLocalAddress	[(2) RO] The local IP address of this TCP connection. A value of 0.0.0.0 is used for connections in the LISTEN state that accept connections from any IP interface related to the node.	Supported	According to the standard.
tcpConnLocalPort	[(3) RO] The local port number for this TCP connection.	Supported	According to the standard.
tcpConnRemAddress	[(4) RO] The remote IP address for this TCP connection.	Supported	According to the standard.
tcpConnRemPort	[(5) RO] The remote port number for this TCP connection.	Supported	According to the standard.
tcpInErrs	[(14) RO] The total number of error segments received such as TCP checksum errors	Supported	According to the standard.
tcpOutRsts	[(15) RO] The number of segments sent with the RST flag (the number of times the TCP connection was reset).	Supported	According to the standard.

● Ip Group: Udp

Each object can be used for read only.

Object name	(Identifier) Standard specifications	Support	Implementation specifications
udpInDatagrams	(1) The total number of UDP datagrams (i.e., the number of packets) sent to the UDP user.	○	According to the standard.

Object name	(Identifier) Standard specifications	Support	Implementation specifications
udpNoPorts	(2) The number of UDP datagrams that were received but did not start an application at the destination port.	○	According to the standard.
udpInErrors	(3) The number of UDP datagrams that were not sent to a higher level protocol for a reason other than udpNoPorts.	○	According to the standard.
udpOutDatagrams	(4) The total number of sent UDP datagrams.	○	According to the standard.
udpTable	(5) The information table for the UDP listener.	---	---
udpEntry	(1) An entry related to a specific UDP listener. The indices are *udpLocalAddress* and *udpLocalPort*.	---	---
udpLocalAddress	(1) The local IP address of this UDP listener. A value of 0.0.0.0 is used for UDP listeners that accept datagrams from any IP interface related to the node.	○	According to the standard.
udpLocalPort	(2) The local port number for this UDP listener.	○	According to the standard.

● Ip Group: Snmp

Each object can be used for read only.

Object name	(Identifier) Standard specifications	Support	Implementation specifications
snmpInPkts	(1) The total number of SNMP messages received.	○	According to the standard.
snmpOutPkts	(2) The total number of SNMP messages sent.	○	According to the standard.
snmpInBadVersions	(3) The total number of messages received of an unsupported version.	○	According to the standard.
snmpInBadCommunityNames	(4) The total number of messages received from an unregistered community.	○	According to the standard.
snmpInBadCommunityUses	(5) The total number of messages received that specify an operation that is not allowed by that community.	○	According to the standard.
snmpInASNParseErrs	(6) The total number of messages received that resulted in an ASN.1 error or BER error during decoding.	○	According to the standard.
snmpInTooBigs	(8) The total number of PDUs received with an error status of tooBig.	○	According to the standard.

Object name	(Identifier) Standard specifications	Sup-port	Implementation specifications
snmpInNoSuchNames	(9) The total number of PDUs received with an error status of noSuchName.	○	According to the standard.
snmpInBadValues	(10) The total number of PDUs received with an error status of badValue.	○	According to the standard.
snmpInReadOnlys	(11) The total number of PDUs received with an error status of readOnly.	○	According to the standard.
snmpInGenErrs	(12) The total number of PDUs received with an error status of genErr.	○	According to the standard.
snmpInTotalReqVars	(13) The total number of MIB objects read normally after receiving GetRequest or GetNextRequest.	○	According to the standard.
snmpInTotalSetVars	(14) The total number of MIB objects updated normally after receiving SetRequest.	○	According to the standard.
snmpInGetRequests	(15) The total number of GetRequest PDUs received.	○	According to the standard.
snmpInGetNexts	(16) The total number of GetNextRequest PDUs received.	○	According to the standard.
snmpInSetRequests	(17) The total number of SetRequest PDUs received.	○	According to the standard.
snmpInGetResponses	(18) The total number of GetResponse PDUs received.	○	According to the standard.
snmpInTraps	(19) The total number of trap PDUs received.	○	According to the standard.
snmpOutTooBigs	(20) The total number of PDUs sent with an error status of tooBig.	○	According to the standard.
snmpOutNoSuch-Names	(21) The total number of PDUs sent with an error status of noSuchName.	○	According to the standard.
snmpOutBadValues	(22) The total number of PDUs sent with an error status of badValue.	○	According to the standard.
snmpOutGenErrs	(24) The total number of PDUs sent with an error status of genErr.	○	According to the standard.
snmpOutGetRequests	(25) The total number of GetRequest PDUs sent.	○	According to the standard.
snmpOutGetNexts	(26) The total number of GetNextRequest PDUs sent.	○	According to the standard.
snmpOutSetRequests	(27) The total number of SetRequest PDUs sent.	○	According to the standard.

Object name	(Identifier) Standard specifications	Sup- port	Implementation specifications
snmpOutGetResponses	(28) The total number of GetResponse PDUs sent.	○	According to the standard.
snmpOutTraps	(29) The total number of trap PDUs sent.	○	According to the standard.
snmpEnableAuthen-Traps	(30) Determines if the agent generates verification failed traps. enabled (1) disabled (2)	○	According to the standard.

10-2 Procedure to Use the SNMP Agent

10-2-1 Procedures

1. Select **Controller Setup - Built-in EtherNet/IP Port Settings** on the Sysmac Studio.
   Make the following settings on the **SNMP Settings** Display or the **SNMP Trap Settings** Display.
   - SNMP Service
   - Recognition 1
   - Recognition 2
2. Select **Transfer to Controller** from the **Controller** Menu and click the **Yes** Button. The built-in EtherNet/IP port settings are transferred to the Communication Control Unit.

10-2-2 Settings Required for the SNMP Agent

The following Built-in EtherNet/IP Port Settings are made from the Sysmac Studio to use the SNMP agent.

Tab page	Setting		Setting conditions	Reference
SNMP Settings	SNMP service		Required.	page A-9
	Port No.		Specified by user. Required to change from the default value of 161.	
	Contact, location		Specified by user.	
	Send a recognition trap		Specified by user. Select this check box to send a recognition trap if there is access from an SNMP manager that is not specified (Access other than Recognition 1 and 2).	
	Recognition 1 and Recognition 2		Specified by user. Make these settings to permit access by only certain SNMP managers.	page A-10
		IP address		
		Host name		
		Community name		
SNMP Trap Settings	SNMP trap		Required	page A-11
	Port No.		Specified by user. Required to change from the default value of 162.	
	Trap 1 and trap 2			page A-12
		IP address	Required Set an IP address or a host name as the SNMP trap destination.	
		Host name		
		Community name	Specified by user.	
		Version	Required Set the version of the SNMP manager.	

Additional Information

Make the settings in the **SNMP Settings** Display and the **SNMP Trap Settings** Display if the SNMP agent is used.
Refer to *A-1-5* ***SNMP Settings*** *Display* on page A-9 for information on the **SNMP Settings** Dialog Box. Refer to *A-1-6* ***SNMP Trap Settings*** *Display* on page A-11 for information on the **SNMP Trap** Dialog Box.

A

Appendices

The appendices provide the built-in EtherNet/IP port settings, variable memory allocation methods, specifications for individual system-defined variables, and other supplemental information for the body of this manual.

A-1 Sysmac Studio Settings for the Built-in EtherNet/IP Port A-2
A-1-1 **TCP/IP Settings** Display A-2
A-1-2 **LINK Settings** Display A-6
A-1-3 **FTP Settings** Display A-7
A-1-4 **NTP Settings** Display A-8
A-1-5 **SNMP Settings** Display A-9
A-1-6 **SNMP Trap Settings** Display A-11
A-1-7 **TCP/UDP Message Service Settings** Display A-13

A-2 Testing Communications A-14
A-2-1 PING Command A-14
A-2-2 Using the PING Command A-14
A-2-3 Host Computer Operation A-14

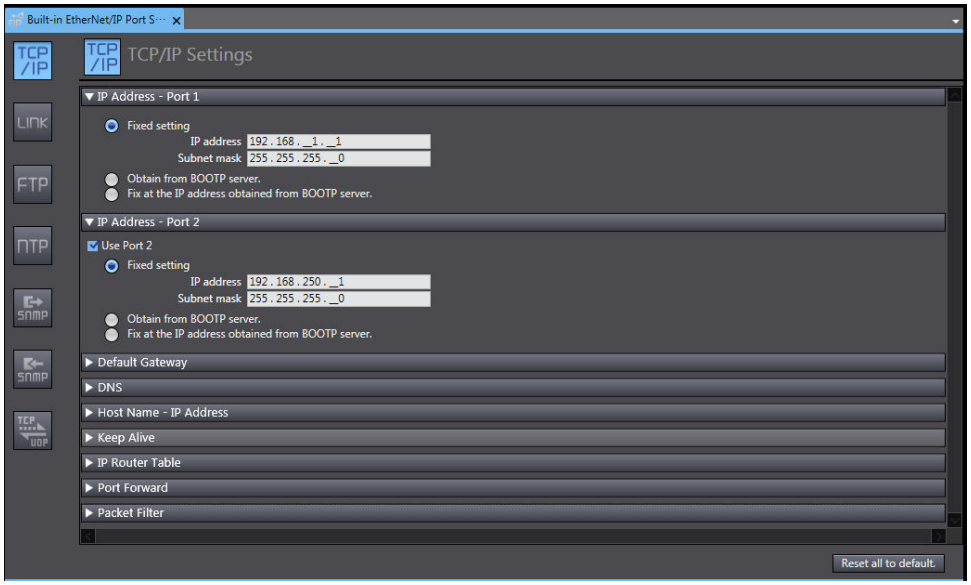
A-3 Variable Memory Allocation Methods A-16
A-3-1 Data Type Alignment and Memory Allocation Amounts A-16
A-3-2 Basic Data Types A-18
A-3-3 Arrays A-20
A-3-4 Structures A-21
A-3-5 Unions A-23

A-4 System-defined Variables A-25
A-4-1 System-defined Variables for the Overall Controller (No Category) A-26
A-4-2 PLC Function Module, Category Name: _PLC A-28
A-4-3 NX Bus Function Module, Category Name: _NXB A-29
A-4-4 EtherNet/IP Function Module, Category Name: _EIP A-31
A-4-5 Meanings of Error Status Bits A-51

A-5 Specifications for Individual System-defined Variables A-53
A-5-1 System-defined Variables for the Overall Controller (No Category) A-53
A-5-2 PLC Function Module, Category Name: _PLC A-56
A-5-3 NX Bus Function Module, Category Name: _NXB A-57
A-5-4 EtherNet/IP Function Module, Category Name: _EIP A-59

A-1 Sysmac Studio Settings for the Built-in EtherNet/IP Port

A-1-1 TCP/IP Settings Display



● IP Address - Port 1

Set an IP address for the built-in EtherNet/IP port 1.

Setting	Description	Default
IP address setting method	Select one of the following IP address setting methods for the built-in EtherNet/IP port 1. • Fixed setting • Obtain from BOOTP server. • Fix at the IP address obtained from BOOTP server.	Fixed setting
IP address*1	Set the IP address for the built-in EtherNet/IP port 1. *2	192.168.1.1
Subnet mask*2	Set the subnet mask for the built-in EtherNet/IP port 1.	255.255.255.0

*1. These settings are required if you set IP address setting method to **Fixed setting**.

*2. Refer to the *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)* for details on the IP address setting.

● IP Address - Port 2

Set an IP address for the built-in EtherNet/IP port 2.

Setting	Description	Default
Use Port 2	Select the check box to use the built-in EtherNet/IP port 2.	Selected (use)
IP address setting method	Select one of the following IP address setting methods for the built-in EtherNet/IP port 2. • Fixed setting • Obtain from BOOTP server. • Fix at the IP address obtained from BOOTP server.	Fixed setting

Setting	Description	Default
IP address*1	Set the IP address for the built-in EtherNet/IP port 2. *2	192.168.250.1
Subnet mask*2	Set the subnet mask for the built-in EtherNet/IP port 2.	255.255.255.0

*1. These settings are required if you set IP address setting method to **Fixed setting**.

*2. Refer to the *NX-series Safety Control Unit / Communication Control Unit User's Manual (Cat. No. Z395)* for details on the IP address setting.

Precautions for Correct Use

You cannot set IP addresses that make two built-in EtherNet/IP ports belong to the same network.

● DNS

Setting	Description	Default
DNS	Select the **Use** Option for DNS when a host name is used to specify remote nodes, such as for the NTP server settings. A DNS server is required to use DNS.	Do not use
Priority DNS server*1	Set the IP address of the DNS server. You can set priority and secondary IP addresses.	None
Secondary DNS server		None
Domain name*1	Set the domain name of the domain to which the built-in EtherNet/IP port belongs. (Single-byte alphanumeric characters, dots, and hyphens: 48 characters max.)	None

*1. These settings are required when the **Use** Option is selected for **DNS**.

● Host Name - IP Address

Setting	Description	Default
Host Name	Addresses are converted according to this setting when a host name is used to specify remote communications nodes. Host names can be set whether DNS is used or not. You can set up to six host names. (Single-byte alphanumeric characters, dots, and hyphens: 200 characters max. with up to 63 single-byte alphanumeric characters between dots.)	None
IP Address	Set the IP address of the registered host name.	None

Keep Alive

Setting	Description	Default
Keep Alive	For each connection number, set whether to use the Keep Alive function to check if the connected client nodes, such as FTP server functions, Sysmac Studio, TCP/UDP message service (TCP only), are communicating. If the **Keep Alive** function is set to **Use**, and a remote node does not respond during the monitoring time set in the **Keep Alive monitoring time** setting, the connection to the remote node is disconnected. The connection to a remote node is left open if the power supply to the remote node is turned OFF without warning. **Use** the Keep Alive function whenever possible. • Use • Do not use	Use
Keep Alive monitoring time	If the **Keep Alive** function is set to **Use**, and a remote node does not respond during the monitoring time set in the **Keep Alive monitoring time** setting, the connection to the remote node is disconnected. Setting range: 1 to 65,535 [sec]	300
Linger option	Set whether to specify the **Linger Option** when you connect to the TCP/UDP message service (TCP only). If the **Linger Option** is specified, the port number is immediately opened even before the port number is released after the TCP connection closes (approx. one minute). • Specify • Do not specify	Do not specify

Default Gateway

Setting	Description	Default
Default gateway*1	Set the IP address of the default gateway for the built-in EtherNet/IP port. *2 This setting is not required when the default gateway is not used.	None

*1. When the IP address setting method is set to **Obtain from BOOTP server** or **Fix at the IP address obtained from BOOTP server**, the default gateway obtained from a BOOTP server is enabled.

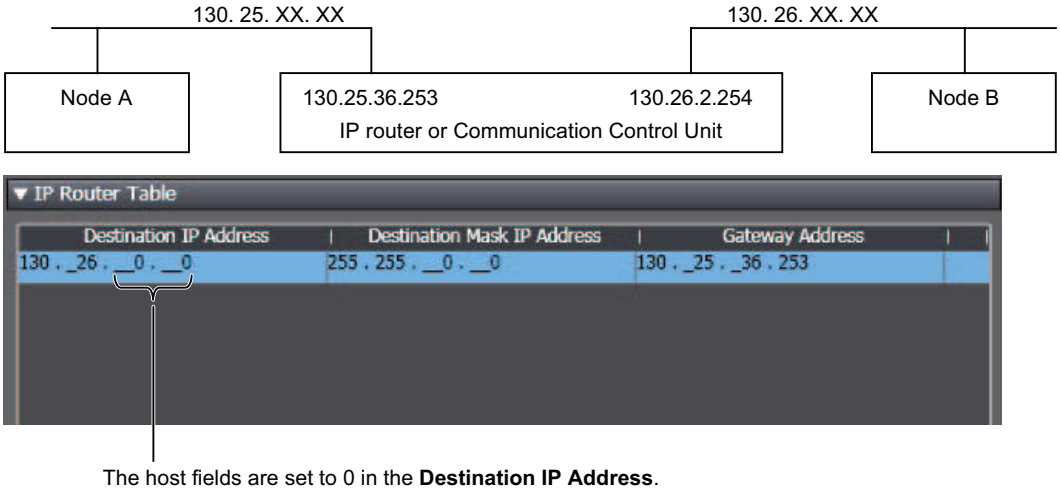
*2. Even if you are using both of port 1 and port 2, you can only set the default gateway for one of the ports.

IP Router Table

Setting	Description	Default
Destination IP Address	Set these settings when the built-in EtherNet/IP port is used for tag data links or CIP message communications with nodes on other IP network segments via an IP router. Accordingly, set these settings when you use a Communication Control Unit as an IP router using the IP routing function for the built-in EtherNet/IP port. You can set up to 64 combinations of IP addresses and gateway addresses. Specify 0 for the host portions of the IP addresses.	None
Destination Mask IP Address		
Gateway Address		None

Additional Information

IP Router Table Setting Example
Set the following IP router table in node A to use tag data links or CIP message communications between node A and node B through the IP router.
When you set the IP router table, node A sends packets to the gateway IP address (130.25.36.253) if communications instructions are executed on node A and addressed to node B.



Port Forward

Setting	Meaning	Default
IP Forward	Select whether to transfer IP packets between communications ports.	Use

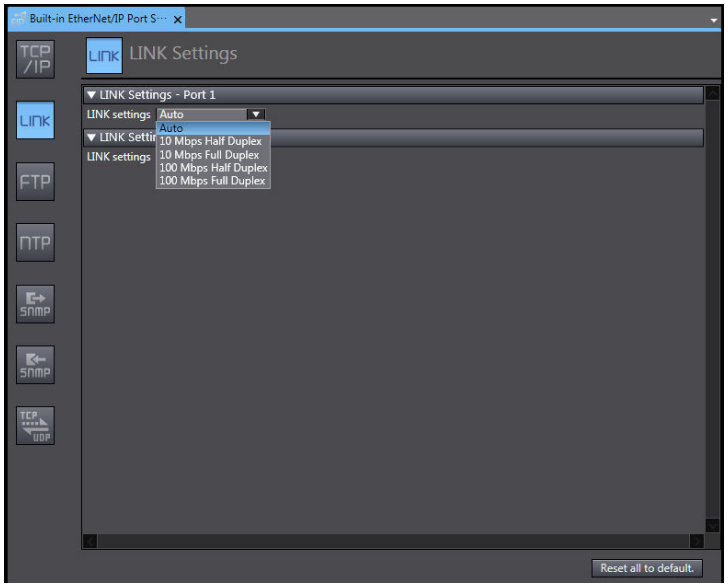
Packet Filter

Setting		Description	Default
Packet Filter		Select whether or not to set conditions for incoming IP packets received at the built-in EtherNet/IP port.	Do not use*1
Pass Frame		Set the following settings to define conditions for incoming IP packets permitted at the built-in EtherNet/IP port. You can specify conditions for up to 32 incoming IP packets that are permitted. These settings are enabled only when the **Packet Filter** setting is set to **Use**.	Port1: any Port2: any
	Port	Specify a port that is permitted to receive incoming packets. • Port1 • Port2	Port1
	Specification Method	Select the method of filtering incoming IP packets that are permitted. • IP address specification*2 • any	IP address specification
	IP Address*3	Specify an IP address that is permitted to receive incoming packets.	None

Setting		Description	Default
	Subnet mask*3	Specify a subnet mask of the IP address that is permitted to receive incoming packets.	None

*1. HTTP (TCP: 80) is the only protocol to be filtered. The other protocols are not filtered.
*2. Specify the IP address settings in **IP address** and **Subnet mask**.
*3. These settings are required only when **IP address** is selected for **Specification Method**.

A-1-2 LINK Settings Display

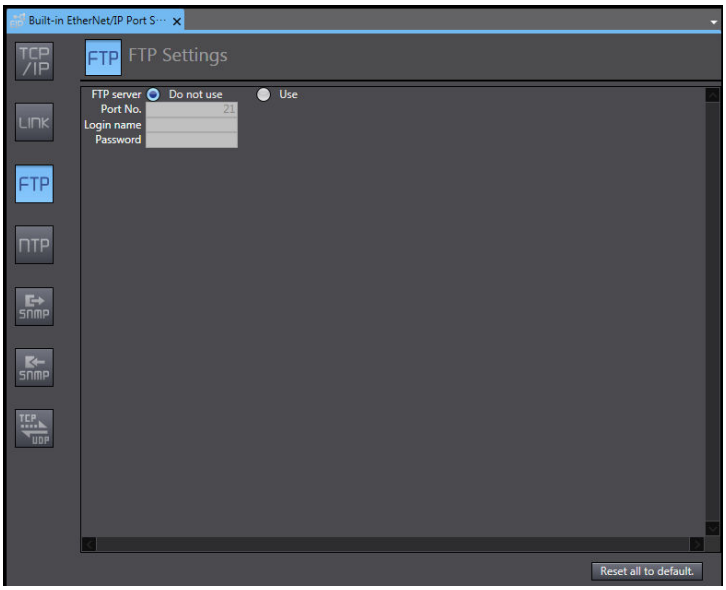


● Link Settings - Port 1 and Port 2

Set for each built-in EtherNet/IP port.

Setting	Description	Default
LINK settings	Set the baud rate for the built-in EtherNet/IP port. • Auto • 10 Mbps Half Duplex • 10 Mbps Full Duplex • 100 Mbps Half Duplex • 100 Mbps Full Duplex For Port 2, you can select Auto only.	Auto

A-1-3 FTP Settings Display



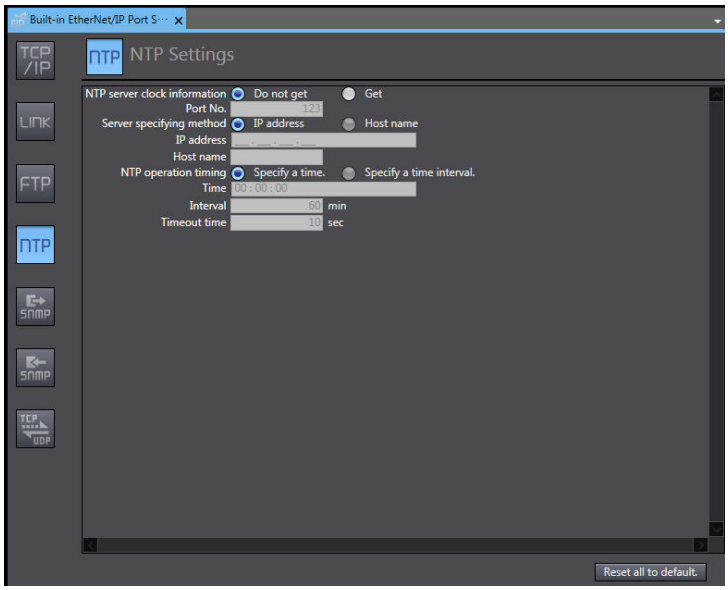
Setting	Description	Default
FTP server	Specify whether to use the FTP server. FTP connections from external devices will not be possible if the **Do not use** Option is selected.	Do not use
Port No. *1 *2	Set the FTP port number of the built-in EtherNet/IP port. It is normally not necessary to change this setting. The FTP control port is set here. The FTP data transfer port is always port 20.	21
Login name *1	Set the login name to externally connect to the built-in EtherNet/IP port via FTP. (You can use up to 12 alphanumeric characters.)*3	None
Password*1	Set the password to externally connect to the built-in EtherNet/IP port via FTP. (You can use 8 to 32 alphanumeric characters.)*3	None

*1. These settings are required when the **Use** Option is selected for the **FTP server**.
*2. The following ports are used by the system and cannot be set by the user: 20, 23, 25, 80, 110, 9610, and 44818.
*3. The login name and password are case sensitive.

Additional Information

Refer to *4-3 FTP Server* on page 4-6 for details on the FTP server.

A-1-4 NTP Settings Display



Setting	Description	Default
NTP server clock information	Set whether to obtain clock information from the NTP server to update the clock in the Communication Control Unit.	Do not get
Port No. *1 *2	Set the port number to use to connect to the NTP server to obtain clock information. It is normally not necessary to change this setting.	123
Server specifying method*1	Set the method to use to specify the NTP server to obtain clock information. • IP address • Host name	IP address
IP address	Set the IP address of the NTP server. Specify this setting if the **server specifying method** is set to the **IP address** Option.	None
Host name	Set the host name of the NTP server (i.e., the domain name of the host). Specify this setting if the **server specifying method** is set to the **Host name** Option. (Single-byte alphanumeric characters, dots, and hyphens: 200 characters max. with up to 63 single-byte alphanumeric characters between dots.)	None
NTP operation timing*1	Set the time at which the NTP server is accessed to synchronize the clocks. • Specify a time • Specify a time interval	Specify a time
Time [hours:minutes:seconds]	The NTP server is accessed at the specified time. (Setting range: 00:00:00 to 23:59:59) Specify this setting if the **NTP operation timing** is set to the **Specify a time** Option.	00:00:00
Interval [minutes]	The NTP server is accessed when the specified period of time has passed. (Setting range: 1 to 1,440 minutes) Specify this setting if the **NTP operation timing** is set to the **Specify a time interval** Option.	60 minutes

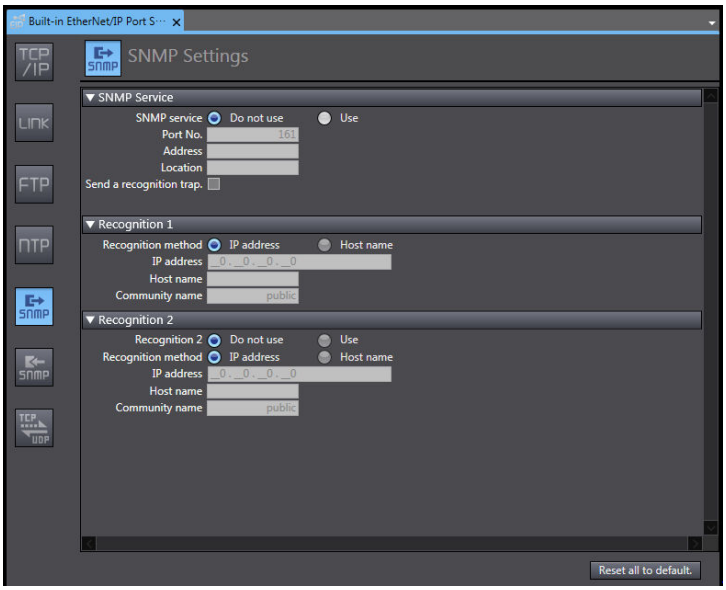
Setting	Description	Default
Timeout time (seconds)*1	Set the timeout detection time. (Setting range: 1 to 255 seconds) If the remote host does not respond, retry processing is performed four times within the time interval that is set here. If the **Specify a time interval** Option is selected for the **NTP operation timing**, timing for the next execution of the NTP operation starts when the fourth retry processing times out.	10 seconds

*1. This setting is required when the **Get** Option is selected for the **NTP server clock information**.
*2. The following ports are used by the system and cannot be set by the user: 25, 53, 68, 110, 2222, 2223, 2224, 9600, and 44818.

Additional Information

Refer to *Section 2 Automatic Clock Adjustment* on page 2-1 for details on obtaining clock information from the NTP server.

A-1-5 SNMP Settings Display



● SNMP

Setting	Description	Default
SNMP service	Specify whether to use the SNMP monitor service. If the **Do not use** Option is selected, an SNMP manager cannot connect from an external device.	Do not use

Setting	Description	Default
Port No.*1	Set the port number to use to connect to the SNMP server that is used to connect from an SNMP manager. It is normally not necessary to change this setting.	161
Address	Set the communications device administrator's name and installation location as text information. You do not necessarily have to input all items. This information is read by the SNMP manager. (You can input up to 255 single-byte alphanumeric characters for each item.)	None
Location		None
Send a recognition trap	Set whether to send a recognition trap. If you select **Send a recognition trap** and there is access from an SNMP manager that is not set in Recognition 1 or Recognition 2, a recognition trap is sent to the SNMP manager. If you select **Send a recognition trap**, specify the SNMP trap settings on the **SNMP Trap** Tab.	Not selected

*1. The following ports are used by the system and cannot be set by the user: 25, 53, 68, 110, 2222, 2223, 2224, 9600, and 44818.

Additional Information

Refer to *Section 10 SNMP Agent* on page 10-1 for details on the SNMP service.

Recognition 1

If the **Use** Option is selected for **SNMP service**, you need to make the following settings.

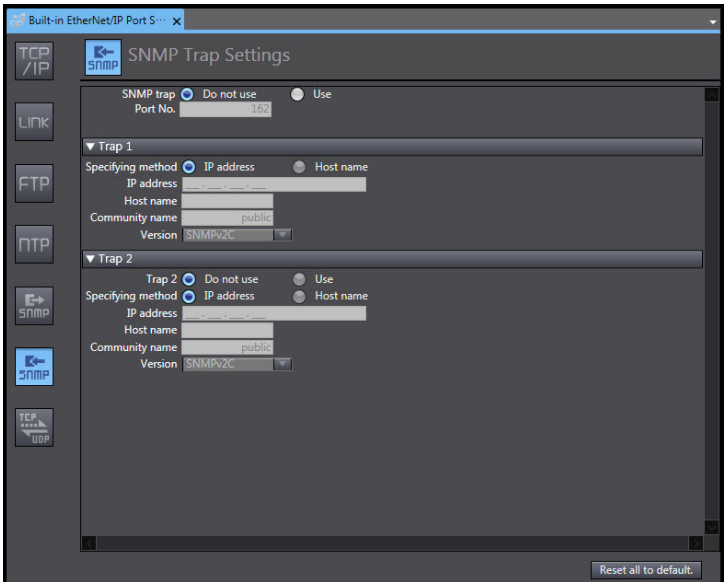
Setting	Description	Default
Recognition method	Set the method to use to specify SNMP managers for which access is permitted. • IP address • Host name Make these settings to permit access by only certain SNMP managers. Access is not allowed unless an IP address or host name is set.	IP address
IP address	Set the IP address of the SNMP manager. If the default setting of 0.0.0.0 is used, access is permitted from all SNMP managers. (Set this setting if the **Recognition method** in Recognition 1 settings is set to the **IP address** Option.)	None
Host name	Set the host name of the SNMP manager. (Set this setting if the **Recognition method** in Recognition 1 settings is set to the **Host name** Option.) (You can use up to 200 single-byte alphanumeric characters, dots, and hyphens with up to 63 single-byte alphanumeric characters between dots.)	None
Community name	Set the community name to enable the SNMP manager to access information from the built-in EtherNet/IP port. (Single-byte alphanumeric characters, dots, and hyphens: 255 characters max.)	public

Recognition 2

If the **Use** Option is selected for **SNMP service**, you need to make the following settings.

Setting	Description	Default
Recognition 2	Specify whether to use the recognition 2 settings. • Use • Do not use	Do not use
Recognition method	Set the method to use to specify SNMP managers for which access is permitted. • IP address • Host name Make these settings to permit access by only certain SNMP managers. Access is not allowed unless an IP address or host name is set.	IP address
IP address	Set the IP address of the SNMP manager. If the default setting of 0.0.0.0 is used, access is permitted from all SNMP managers. (Set this setting if the **Recognition method** in Recognition 2 settings is set to the **IP address** Option.)	None
Host name	Set the host name of the SNMP manager. (Set this setting if the **Recognition method** in Recognition 2 settings is set to the **Host name** Option.) (You can use up to 200 single-byte alphanumeric characters, dots, and hyphens with up to 63 single-byte alphanumeric characters between dots.)	None
Community name	Set the community name to enable the SNMP manager to access information from the built-in EtherNet/IP port. (Single-byte alphanumeric characters, dots, and hyphens: 255 characters max.)	public

A-1-6 SNMP Trap Settings Display



SNMP Trap

Setting	Description	Default
SNMP trap	Specify whether to use the SNMP trap (network error detection).*1 If the **Do not use** Option is selected for SNMP trap, SNMP traps are not sent to the SNMP manager	Do not use
Port No.*2	Set the port number to use to connect to the SNMP server. It is normally not necessary to change this setting.	162

*1. If you specify to use the SNMP trap, you also have to set Trap 1 and Trap 2 as described below.

*2. The following ports are used by the system and cannot be set by the user: 25, 53, 68, 110, 2222, 2223, 2224, 9600, and 44818.

Additional Information

Refer to *10-1-1 Overview* on page 10-2 for details on the SNMP trap.

Trap 1

If the **Use** Option is selected for **SNMP trap**, you need to make the following settings.

Setting	Description	Default
Recognition method	Set the specifying method for the SNMP manager destination for SNMP traps. • IP address • Host name	IP address
IP address	Set the IP address of the SNMP manager. (Set this setting if the **Recognition method** in the Trap 1 settings is set to the **IP address** Option.)	None
Host name	Set the host name of the SNMP manager. (Set this setting if the **Recognition method** in the Trap 1 settings is set to the **Host name** Option.) (You can use up to 200 single-byte alphanumeric characters, dots, and hyphens with up to 63 single-byte alphanumeric characters between dots.)	None
Community name	Set the community name. (You can use up to 255 single-byte alphanumeric characters.)	public
Version	Set the version of the SNMP manager. • SNMPv1 • SNMPv2C	SNMPv2C

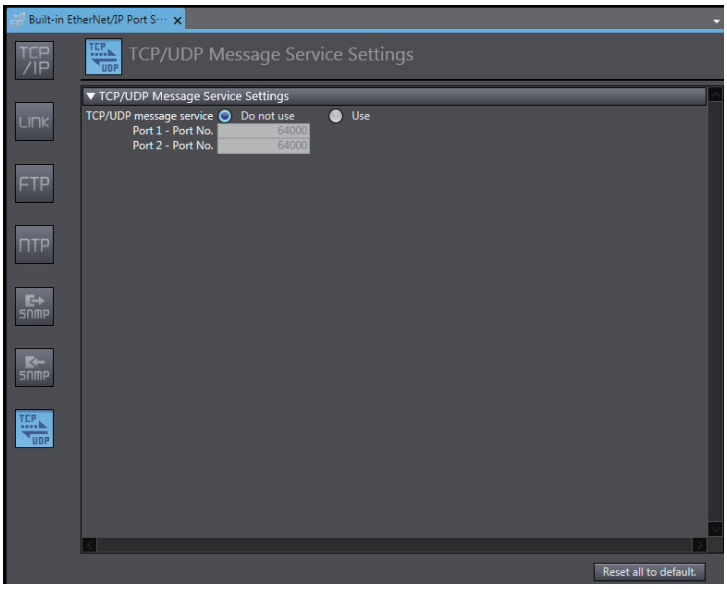
Trap 2

If the **Use** Option is selected for **SNMP trap**, you need to make the following settings.

Setting	Description	Default
Trap 2	Specify whether to use the Trap 2 settings. • Use • Do not use	Do not use
Recognition method	Set the specifying method for the SNMP manager destination for SNMP traps. • IP address • Host name	IP address

Setting	Description	Default
IP address	Set the IP address of the SNMP manager. (Set this setting if the **Recognition method** in the Trap 2 settings is set to the **IP address** Option.)	None
Host name	Set the host name of the SNMP manager. (Set this setting if the **Recognition method** in the Trap 2 settings is set to the **Host name** Option.) (You can use up to 200 single-byte alphanumeric characters, dots, and hyphens with up to 63 single-byte alphanumeric characters between dots.)	None
Community name	Set the community name. (You can use up to 255 single-byte alphanumeric characters.)	public
Version	Set the version of the SNMP manager. • SNMPv1 • SNMPv2C	SNMPv2C

A-1-7 TCP/UDP Message Service Settings Display



● TCP/UDP Message Service Settings

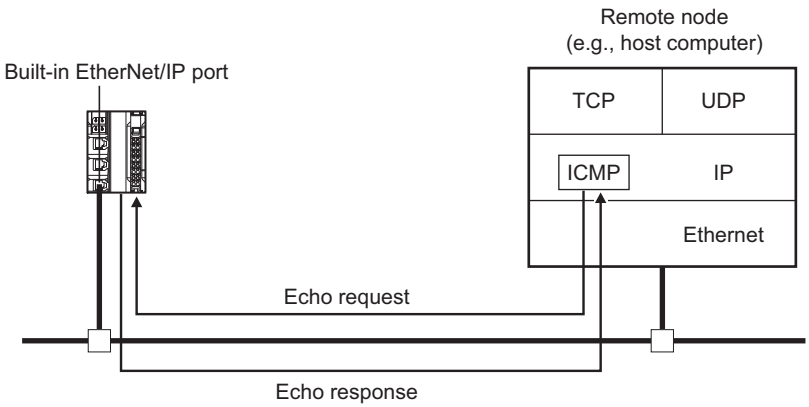
Setting	Description	Default
TCP/UDP message service	Specify whether to use the TCP/UDP message service function. When you select **Do not use** Option, you cannot use TCP/UDP message to establish a connection from an external device.	Do not use
Port 1 - Port No.	Specify a TCP/IP port number or a UDP/IP port number used for port 1. For the details on the port number range, refer to *9-3 TCP/UDP Message Service Specifications* on page 9-4.	64000
Port 2 - Port No.	Specify a TCP/IP port number or a UDP/IP port number used for Port 2. For the details on the port number range, refer to *9-3 TCP/UDP Message Service Specifications* on page 9-4.	64000

A-2 Testing Communications

If the basic settings, particularly the IP address and subnet mask, have been made correctly for the built-in EtherNet/IP port, then it is possible to communicate with nodes on the EtherNet/IP network. This section describes how to use the PING command to test communications with the built-in EtherNet/IP port.

A-2-1 PING Command

The PING command sends an echo request packet to a remote node and receives an echo response packet to confirm that the remote node communications are normal. The PING command uses the ICMP echo request and response. The echo response packet is automatically returned in the ICMP. The PING command is normally used to check the connections of remote nodes when you set up a network. The built-in EtherNet/IP port supports both the ICMP echo request and response functions. If the remote node returns a normal response to the PING command, then the node is physically connected correctly and Ethernet node settings are correct.



A-2-2 Using the PING Command

The built-in EtherNet/IP port automatically returns an echo response packet in response to an echo request packet with the PING command sent by another node (e.g., host computer).

A-2-3 Host Computer Operation

The PING command can be executed from the host computer to send an echo request packet to a built-in EtherNet/IP port.
The following example shows how to use the PING command in the host computer.

Application Method

Input the following command at the host computer's prompt ($):

$ ping IP_address (host_name)

The destination is specified by its IP address or host name.

Additional Information

The PING command is not supported by some host computers.

Application Example

In this example, a PING command is sent to the node at IP address 130.25.36.8.
The "$" in the example represents the host computer prompt.

● Normal Execution

```
$ ping   130.25.36.8                                        ← Executes the PING command.
PING   130.25.36.8: 56   data   bytes
64   bytes   from   130.25.36.8:   icmp_seq=0.   time=0. ms
64   bytes   from   130.25.36.8:   icmp_seq=1.   time=0. ms
              :              :              :              :              :
64   bytes   from   130.25.36.8:   icmp_seq=8.   time=0. ms
                                                            ← Press the Ctrl+C Keys to cancel execution.
---- 130.25.36.8   PING   Statistics ----
9 packets   transmitted,   9 packets   received,   0% packet   loss
round-trip   (ms)      min/avg/max   = 0/0/0
$
```

● Error

```
$ ping   130.25.36.8                                        ← Executes the PING command.
PING   130.25.36.8: 56   data   bytes
                                                            ← Press the Ctrl+C Keys to cancel execution.
---- 130.25.36.8   PING   Statistics ----
9 packets   transmitted,   0 packets   received,   100% packet   loss
$
```

Refer to the command reference manual for your computer's OS for details on using the PING command.

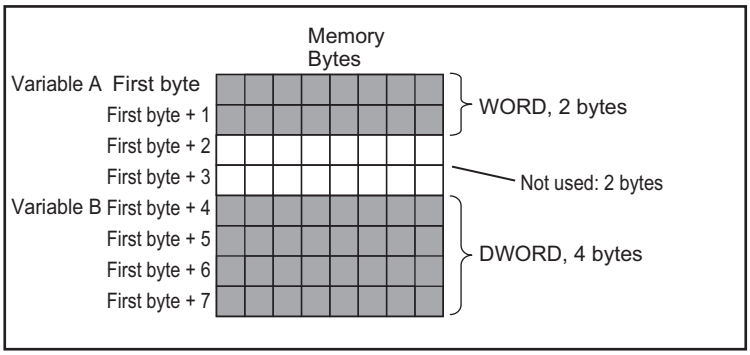
A-3 Variable Memory Allocation Methods

You must be aware of the way in which memory is allocated to variables to align the memory locations of the members of structure or union variables with variables in other devices. Adjustments are necessary mainly when structure variables are used in the communications with other devices.

The amount of memory and the memory locations that are allocated for a variable depend on the data type of the variable. The amount of memory and the memory locations that are allocated for array elements, structure members, and union members depend on the data types, but also on the declarations that are made for the arrays, structures, and unions.

A-3-1 Data Type Alignment and Memory Allocation Amounts

The data size is determined for each data type. The data size is the minimum amount of memory that is required to store the value or values of that data type.
On the other hand, memory for variables is automatically structured by the Communication Control Unit for the most efficient access. Therefore, the total amount of memory that is required for variables is not necessarily the total of the data sizes of the variables. For example, if WORD and DWORD variables are declared, the total of the data sizes is six bytes, but eight bytes are allocated in memory, as shown in the following figure.



Variable Table

Name	Data type
A	WORD
B	DWORD

This information for determining the location of a variable in memory is called the alignment. The alignment is determined for each data type. The amount of memory and the memory locations for the variables are given below.

Item	Specification
Amount of memory that is allocated	An integral multiple of the alignment. However, the minimum amount of memory is the data size.
Locations in memory	At an integral multiple of the alignment starting from the start of the variable in memory.

The alignments and the amounts of memory that are allocated for the basic data types and enumerations are given below.

Data type	Alignment [bytes]	Amount of memory that is allocated [bytes]
BOOL	2	2
BYTE, USINT, or SINT	1	1

Data type	Alignment [bytes]	Amount of memory that is allocated [bytes]
WORD, UINT, or INT	2	2
DWORD, UDINT, or DINT	4	4
LWORD, ULINT, or LINT	8	8
REAL	4	4
LREAL	8	8
TIME, DATE, TIME_OF_DAY, or DATE_AND_TIME	8	8
STRING[N+1]*1	1	N+1
Enumerations	4	4

*1. N is the maximum number of characters handled. For example, if a maximum of 10 single-byte characters are handled, the NULL character is added, so memory for 11 characters must be reserved.

The elements of arrays and the members of structures and unions are located in memory for the most efficient access. The alignments and the amounts of memory that are allocated for arrays, structures, and unions are determined by the variable declarations, as described below.

Data type	Alignment	Amount of memory that is allocated
Array	Same as alignment of the data type of the elements	(Amount of memory that is allocated for the data type of the elements) × Number of elements*1
Structure	The largest alignment of all of the members	The integral multiple of the alignment that is larger than the total amount of memory that is allocated when the members are arranged in order at integral multiples of the alignment of the data types of the members
Union	The largest alignment of all of the members	The largest amount of memory that is allocated for any of the members

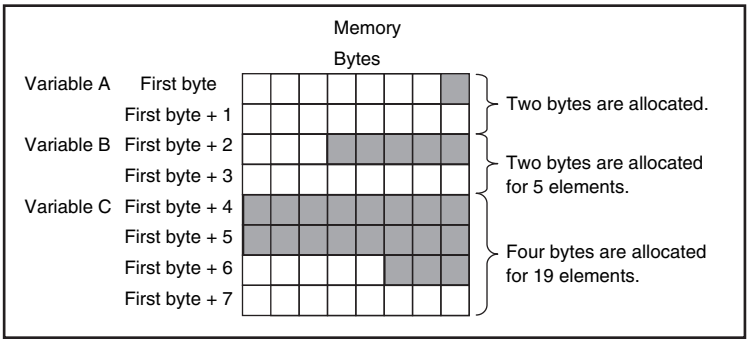
*1. BOOL arrays are an exception. Refer to Precautions for Correct Use, below, for the amount of memory that is allocated for BOOL arrays.

Precautions for Correct Use

Amount of Memory That Is Allocated for BOOL Arrays

Two bytes are allocated in memory for individual BOOL variables, BOOL structure members, and BOOL union variables.

However, for a BOOL array, two bytes of memory are not allocated for each element. One bit is allocated in order for each element. For the entire array, a multiple of two bytes of memory is allocated (including unused bits).



Variable Table

Name	Data type
A	BOOL
B	ARRAY[1..5]OF BOOL
C	ARRAY[0..18]OF BOOL

Therefore, the following formula gives the amount of memory that is allocated for a BOOL array. For 1 to 16 elements, 2 bytes are allocated. For 17 to 32 elements, 4 bytes are allocated.

$$\text{Amount of memory} = 2\left[\frac{\text{Number of elements} - 1}{16}\right] + 2$$

Truncate the decimal portion of the result of the calculation in brackets.

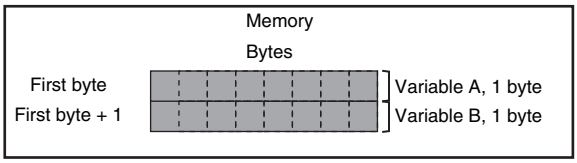
Specific examples of the rules for memory allocation for variables of each data type are given below.

A-3-2 Basic Data Types

Variables with One-Byte Alignments (e.g., BYTE)

One byte of memory is allocated for the one-byte alignment.

Example: Two consecutive BYTE variables



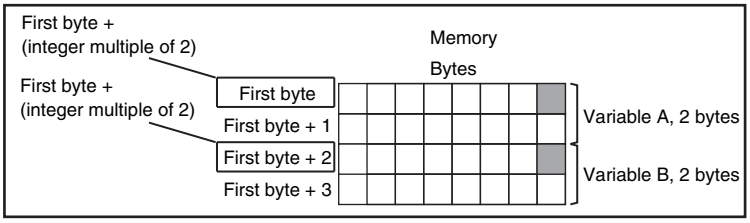
Variable Table

Name	Data type
A	BYTE
B	BYTE

Variables with Two-byte Alignments (e.g., BOOL and WORD)

Two bytes of memory are allocated for the two-byte alignment.

Example: Two consecutive BOOL variables

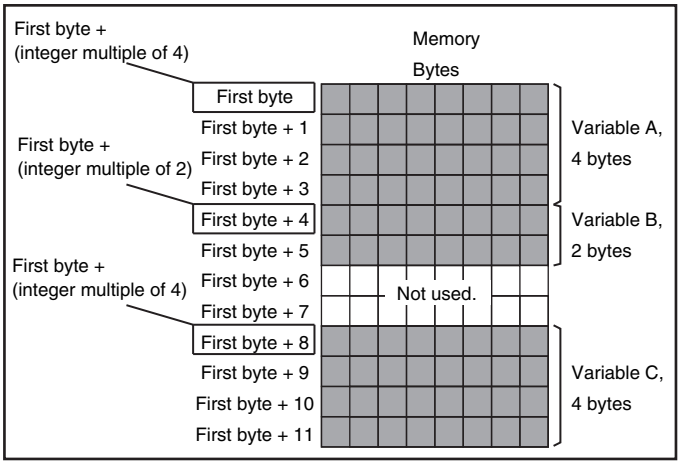


Variable Table

Name	Data type
A	BOOL
B	BOOL

Variables with Four-byte Alignments (e.g., DWORD)

Four bytes of memory are allocated for the four-byte alignment.
The location of the first byte of data in memory is an integer multiple of four bytes. Therefore, if a variable with a two-byte alignment, such as WORD data, is inserted, two bytes of unused memory will remain.
Example: Consecutive variables in the following order: DWORD, WORD, and DWORD

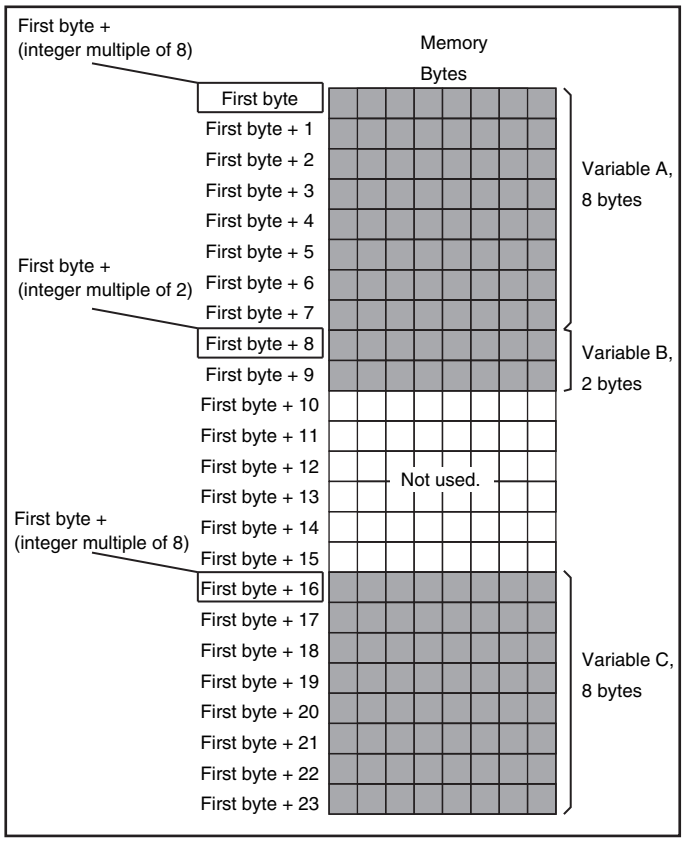


Variable Table

Name	Data type
A	DWORD
B	WORD
C	DWORD

Variables with Eight-byte Alignments (e.g., LWORD)

Eight bytes of memory are allocated for the eight-byte alignment.
The location of the first byte of data in memory is an integer multiple of eight bytes. Therefore, if a variable with a two-byte alignment, such as WORD data, is inserted, six bytes of unused memory will remain. If a variable with a four-byte alignment, such as DWORD data, is inserted, four bytes of unused memory will remain.
Example: Consecutive variables in the following order: LWORD, WORD, and LWORD



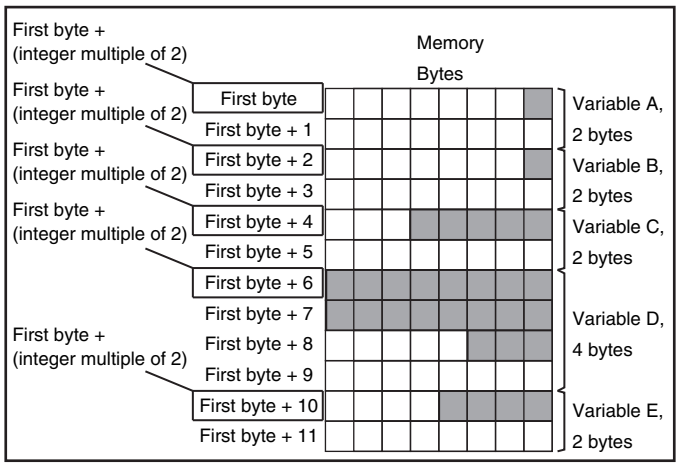
Variable Table

Name	Data type
A	LWORD
B	WORD
C	LWORD

A-3-3 Arrays

A continuous section of memory is allocated for the elements of the array based on the data size of the data type of the array variable. The alignment of an array is the same as alignment of the data type of the elements.

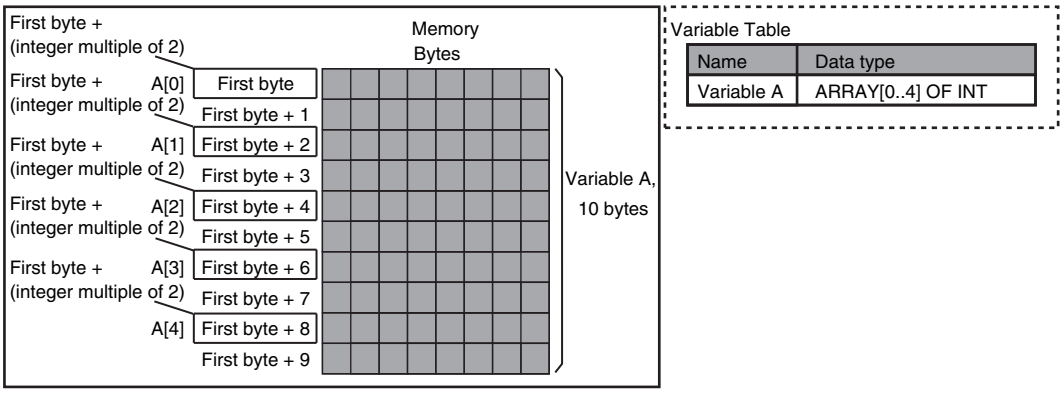
Example: Continuous variables in the following order: two BOOL variable, one BOOL array with five elements, one BOOL array with 19 elements, and one BOOL array with four elements



Variable Table

Name	Data type
A	BOOL
B	BOOL
C	ARRAY[1..5]OF BOOL
D	ARRAY[0..18]OF BOOL
E	ARRAY[5..8]OF BOOL

Example: INT array with five elements

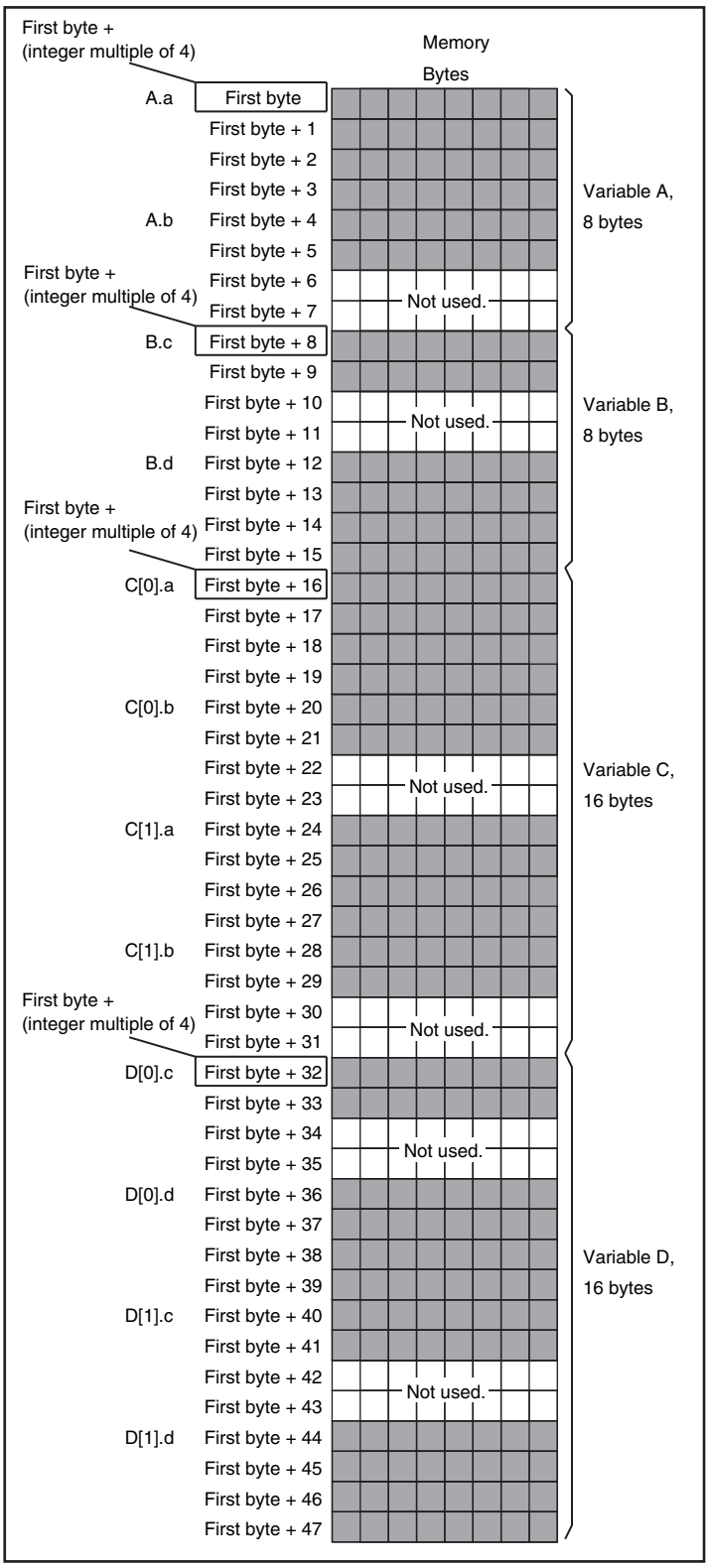


A-3-4 Structures

For a structure variable, the members are located in memory in the order that they are declared. Each member is located at an integer multiple of the alignment of the data type of the member. Therefore, there can be unused memory between members or at the end of members.
The alignment of a structure is the largest alignment of all of the members. The amount of memory that is allocated is the integral multiple of the alignment that is larger than the total amount of memory that is allocated when the members are arranged in order at integral multiples of the alignment of the data types of the members.

Example: The alignments and the amounts of memory that are allocated for the four variable declarations given in the following figure are given in the following table.

Variable	Alignment [bytes]	Amount of memory that is allocated [bytes]
A	4	8
B	4	8
C	4	16
D	4	16



Data Type Definitions

Name	Data type
Structure *STR_A*	STRUCT
a	DINT
b	INT

Name	Data type
Structure *STR_B*	STRUCT
c	INT
d	DINT

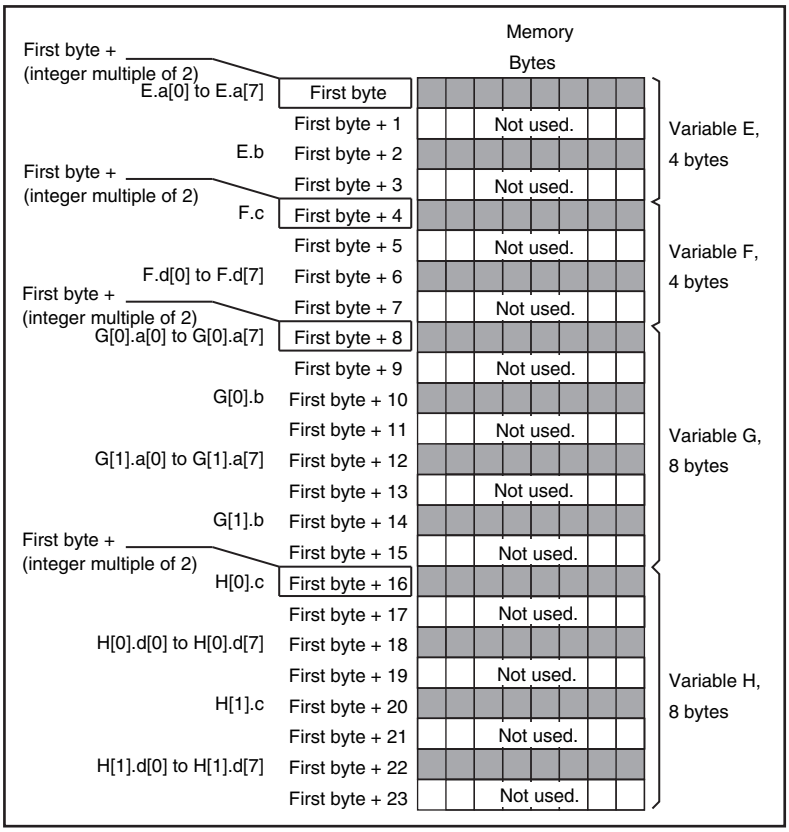
Variable Table

Name	Data type
Variable A	Structure *STR_A*
Variable B	Structure *STR_B*
Variable C	ARRAY[0..1] OF STR_A
Variable D	ARRAY[0..1] OF STR_B

Example: The alignments and the amounts of memory that are allocated for the four variable declarations given in the following figure are given in the following table.

Variable	Alignment [bytes]	Amount of memory that is allocated [bytes]
E	2	4
F	2	4
G	2	8

Variable	Alignment [bytes]	Amount of memory that is allocated [bytes]
H	2	8



Data Type Definitions

Name	Data type
Structure *STR_C*	STRUCT
a	ARRAY[0..7] OF BOOL
b	BYTE

Name	Data type
Structure *STR_D*	STRUCT
c	BYTE
d	ARRAY[0..7] OF BOOL

Variable Table

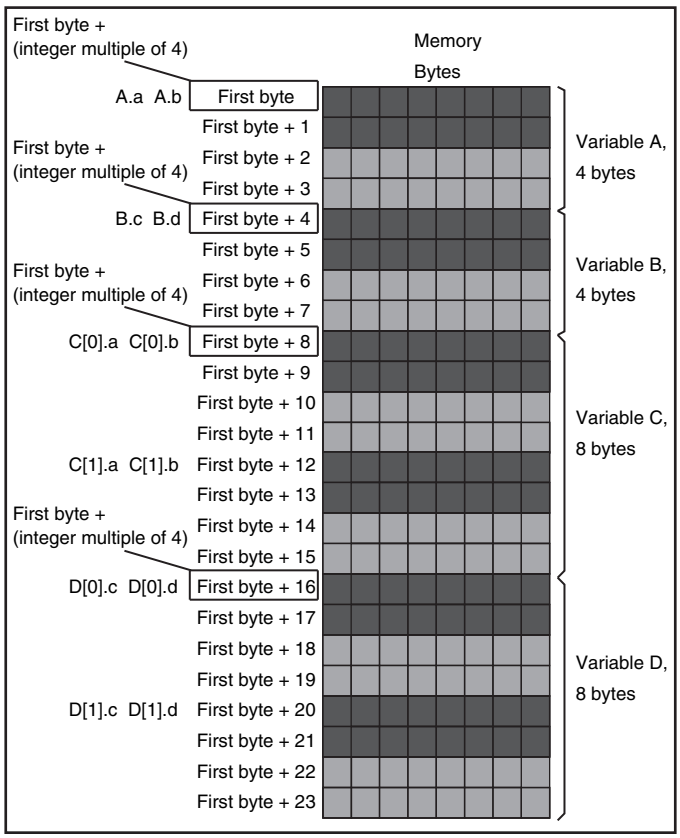
Name	Data type
Variable E	Structure *STR_C*
Variable F	Structure *STR_D*
Variable G	ARRAY[0..1] OF STR_C
Variable H	ARRAY[0..1] OF STR_D

A-3-5 Unions

For a union variable, the members overlap in the same memory locations.
The alignment of a union is largest alignment of all of the members. The amount of memory that is allocated is the largest amount of memory that is allocated for any of the members.

Example: The alignments and the amounts of memory that are allocated for the four variable declarations given in the following figure are given in the following table.

Variable	Alignment [bytes]	Amount of memory that is allocated [bytes]
A	4	4
B	4	4
C	4	8
D	4	8



Data Type Definitions

Name	Data type
Union *UNI_A*	UNION
a	DWORD
b	WORD

Name	Data type
Union *UNI_B*	UNION
c	WORD
d	DWORD

Variable Table

Name	Data type
Variable A	Union *UNI_A*
Variable B	Union *UNI_B*
Variable C	ARRAY[0..1] OF UNI_A
Variable D	ARRAY[0..1] OF UNI_B

A-4 System-defined Variables

System-defined variables are assigned specific functions by the system.
They are registered in the global variable table, or the local variable table for each POU, in advance.
These variables cannot be changed. Some of the variables start with an underbar and some start with ”P_”.

Some of the system-defined variables are read-only and some are read/write.

You read and write the variables with communications from external devices, with the Sysmac Studio, or with an NS/NA-series PT.
Basically, system-defined variables are classified according to the function modules.
The variables start with the following category names.

Function module	Category name
System-defined variables for the overall Safety Network Controller	_ (None)
PLC Function Module	_PLC
NX Bus Function Module	_NXB
EtherNet/IP Function Module	_EIP, _EIP1, and _EIP2

The variables are described in the tables of this appendix as shown below.

Variable name	Meaning	Function	Data type	Range of values	Reference
This is the system-defined variable name. The prefix gives the category name.	This is the meaning of the variable.	The function of the variable is described.	The data type of the variable is given.	The range of values that the variable can take is given.	The page of the individual system-defined variable specifications table is given.

Precautions for Correct Use

There are system-defined variables that are not supported or differ in specifications, such as the number of arrays, depending on the series of the Communication Control Unit. Refer to *A-5 Specifications for Individual System-defined Variables* on page A-53 for details on the specifications for individual system-defined variables.

A-4-1 System-defined Variables for the Overall Controller (No Category)

● Functional Classification: Clock

Variable name	Meaning	Function	Data type	Range of values	Reference
_CurrentTime	System Time	Contains the Communication Control Unit's clock data.	DATE_AND_TIME	DT#1970-01-01-00:00:00 to DT#2069-12-31-23:59:59	page A-53

● Functional Classification: Errors

Variable name	Meaning	Function	Data type	Range of values	Reference
_ErrSta	Controller Error Status	TRUE if there is a Controller error. FALSE if there is no Controller error. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#C0F0	page A-53
_AlarmFlag	User-defined Error Status	The bit corresponding to the event level is TRUE while there is a user-defined error. Bits 00 to 07 correspond to user fault levels 1 to 8. This variable contains 0000 hex when there is no user-defined error.	WORD	16#0000 to 16#00FF	page A-53

● Functional Classification: SD Memory Card

Variable name	Meaning	Function	Data type	Range of values	Reference
_Card1Ready	SD Memory Card Ready Flag	TRUE when the SD Memory Card is recognized. FALSE when the SD Memory Card is not recognized. TRUE: Can be used. FALSE: The Card cannot be used.	BOOL	TRUE or FALSE	page A-54
_Card1Protect	SD Memory Card Write Protected Flag	TRUE when the SD Memory Card is write-protected with the LOCK switch. TRUE: Write protected. FALSE: Not write protected.	BOOL	TRUE or FALSE	page A-54
_Card1Err	SD Memory Card Error Flag	TRUE when an unusable SD Memory Card is inserted or a format error occurs. TRUE: There is an error FALSE: There is no error	BOOL	TRUE or FALSE	page A-54
_Card1Access	SD Memory Card Access Flag	TRUE during SD Memory Card access. TRUE: Card is being accessed. FALSE: Card is not being accessed. The system updates the flag every 100 ms. Because of this, access to the SD Memory Card is shown by this flag with a delay of up to 100 ms.	BOOL	TRUE or FALSE	page A-54

Variable name	Meaning	Function	Data type	Range of values	Reference
_Card1Deteriorated	SD Memory Card Life Warning Flag	TRUE when the life of the SD Memory Card is exceeded. TRUE: The life of the Card has been exceeded. FALSE: The Card can still be used.	BOOL	TRUE or FALSE	page A-54
_Card1PowerFail	SD Memory Card Power Interruption Flag	TRUE when the power supply to the Communication Control Unit was interrupted during access to the SD Memory Card. TRUE: Power was interrupted during SD Memory Card access. FALSE: Normal	BOOL	TRUE or FALSE	page A-55

● Functional Classification: Backup

Variable name	Meaning	Function	Data type	Range of values	Reference
_BackupBusy	Backup Function Busy Flag	TRUE when a backup, restoration, or verification is in progress.	BOOL	TRUE or FALSE	page A-55

● Functional Classification: Power Supply

Variable name	Meaning	Function	Data type	Range of values	Reference
_PowerOnHour	Total Power ON Time	Contains the total time that the power has been ON. Contains the total time that the Communication Control Unit has been ON in 1-hour increments. To reset this value, overwrite the current value with 0. The value is not updated after it reaches 4294967295. This variable is not initialized at startup.	UDINT	0 to 4294967295	page A-55
_PowerOnCount	Power Interruption Count	Contains the number of times that the power supply has been interrupted. The value is incremented by 1 each time the power supply is interrupted after the first time that the power to the Communication Control Unit was turned ON. To reset this value, overwrite the current value with 0. The value is not updated after it reaches 4294967295. This variable is not initialized at startup.	UDINT	0 to 4294967295	page A-55
_RetainFail	Retention Failure Flag	TRUE at the following time (failure of retention during power interruptions). • When an error is detected in the battery-backup memory check at startup. FALSE at the following times (no failure of retention during power interruptions). • When no error is detected in the battery-backup memory check at startup. • When the Clear All Memory operation is performed.	BOOL	TRUE or FALSE	page A-55

● Functional Classification: Version

Variable name	Meaning	Function	Data type	Range of values	Reference
_UnitVersion	Unit Version	Contains the unit version of the Communication Control Unit. The integer part of the unit version is stored in element number 0. The fractional part of the unit version is stored in element number 1. Example 1) If the unit version is 1.08, “1” is stored in element number 0 and “8” is stored in element number 1. Example 2) If the unit version is 1.10, “1” is stored in element number 0 and “10” is stored in element number 1.	ARRAY[0..1] OF USINT	0 to 99	page A-56
_HardwareRevision	Hardware Revision	Contains the hardware revision of the Communication Control Unit. Contains - if the hardware revision is in blank, and A to Z for other cases.	STRING[2]	- or A to Z	page A-56

● Functional Classification: PLC Built-in

Variable name	Meaning	Function	Data type	Range of values	Reference
_DeviceOutHoldCfg	Device Output Hold Configuration	It is 16#A5A5 if you retain the target device output when downloaded. In the case other than 16#A5A5, the target device output is initialized when downloaded.	WORD	16#0000 to 16#FFFF	page A-56
_DeviceOutHoldStatus	Device Output Hold Status	It is TRUE if the target device output is retained when downloaded. When the device output hold configuration is other than 16#A5A5, or when a major fault level Controller error occurs, the target device output is initialized and changes to FALSE.	BOOL	TRUE or FALSE	page A-56

A-4-2 PLC Function Module, Category Name: _PLC

● Functional Classification: Errors

Variable name	Meaning	Function	Data type	Range of values	Reference
_PLC_ErrSta	PLC Function Module Error Status	TRUE when there is a Controller error that involves the PLC Function Module. FALSE when there is no Controller error that involves the PLC Function Module. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-56

● Functional Classification: Safety Data Logging

Variable name / Member name	Meaning	Function	Data type	Range of values	Reference
_PLC_SFLogSta	Safety Data Logging Status	Stores the status of safety data logging. Element number 0 corresponds to Logging Setting Number 1. Element number 1 corresponds to Logging Setting Number 2.	ARRAY[0..1] OF _sSFLOG_STA		page A-57
.IsStart	Safety Data Logging Busy Flag	TRUE when safety data logging starts.	BOOL	TRUE or FALSE	
.IsComplete	Safety Data Logging Completed Flag	TRUE when logging stops. FALSE when the next logging starts. When this flag is TRUE, it means that the logging has completed.	BOOL	TRUE or FALSE	
.IsOutput	Log File Output Completed Flag	TRUE when the log file is output. FALSE when the next logging starts.	BOOL	TRUE or FALSE	

A-4-3 NX Bus Function Module, Category Name: _NXB

● Functional Classification: NX Bus Function Module Status

Variable name	Meaning	Function	Data type	Range of values	Reference
_NXB_MaxUnitNo	Largest Unit Number	Contains the largest NX Unit number of the NX Units on the Communication Control Unit that are detected by the NX Bus Function Module. If the Unit configuration information is registered by the Sysmac Studio, the value will be the largest NX Unit number of the registered Unit configuration. Units that are set as unmounted Units are also included. If the Unit configuration information is not registered by the Sysmac Studio, the value will be the largest Unit number of an actual Unit configuration.	UINT	0 to 32 0: No NX Unit mounted.	page A-57
_NXB_UnitIOActiveTbl	NX Unit I/O Data Active Status	Indicates whether the I/O data in the NX Units on the Communication Control Unit is valid. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of 0 indicates the NX Bus Function Module and it is always TRUE. TRUE: The I/O data in the NX Unit is valid. FALSE: The I/O data in the NX Unit is invalid. The status is FALSE for NX Units that are set as unmounted Units.	ARRAY [0..32] OF BOOL	TRUE or FALSE	page A-58

Variable name	Meaning	Function	Data type	Range of values	Reference
_NXB_UnitMsgActiveTbl	NX Unit Message Enabled Status	Indicates whether the NX Units on the Communication Control Unit can process message communications. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of 0 indicates the NX Bus Function Module and it is always TRUE. TRUE: Message communications possible. FALSE: Message communications not possible. The status is FALSE for NX Units that are set as unmounted Units.	ARRAY [0..32] OF BOOL	TRUE or FALSE	page A-58
_NXB_UnitRegTbl	NX Unit Registration Status	Indicates whether the NX Units on the Communication Control Unit are registered in the Unit configuration. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of 0 indicates the NX Bus Function Module. TRUE: Registered. FALSE: Not registered. If the Unit configuration information is not registered by the Sysmac Studio, the status is FALSE for all Units. The status is TRUE for NX Units that are set as unmounted Units.	ARRAY [0..32] OF BOOL	TRUE or FALSE	page A-58

● Functional Classification: NX Bus Function Module Errors

Variable name	Meaning	Function	Data type	Range of values	Reference
_NXB_ErrSta	NX Bus Function Module Error Status	Gives the NX Bus Function Module error status. This system-defined variable provides the collective status of the NX Bus Function Module Master Error Status and NX Bus Function Module Unit Error Status for all NX Units. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#40F2	page A-58
_NXB_MstrErrSta	NX Bus Function Module Master Error Status	Gives the status of errors that are detected in the NX Bus Function Module of the Communication Control Unit. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#40F2	page A-58

Variable name	Meaning	Function	Data type	Range of values	Reference
_NXB_UnitErrStaTbl	NX Bus Function Module Unit Error Status	Gives the status of errors that are detected in the NX Bus Function Module of the Communication Control Unit. This status is given as an array of WORD data. The subscript of the array corresponds to the NX Unit number. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	ARRAY [1..32] OF WORD	16#0000 to 16#40F2	page A-59
_NXB_UnitErr-FlagTbl	NX Unit Error Status	Indicates whether errors occurred in the NX Unit on the Communication Control Unit. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of "0" indicates the NX Bus Function Module and whether an event occurred that is detected by the NX Bus Function Module. TRUE: Error. FALSE: No error. The status is "FALSE" for NX Units that are set as unmounted Units.	ARRAY [0..32] OF BOOL	TRUE or FALSE	page A-59

A-4-4 EtherNet/IP Function Module, Category Name: _EIP

● Functional Classification: EtherNet/IP Communications Errors

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_ErrSta	EtherNet/IP Error	This is the error status variable for the built-in EtherNet/IP port. Represents the collective status of the following error flags. • _EIP1_PortErr (Communications Port1 Error) • _EIP2_PortErr (Communications Port2 Error) • _EIP1_CipErr (CIP Communications1 Error) • _EIP2_CipErr (CIP Communications2 Error) • _EIP_TcpAppErr (TCP Application Communications Error) **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-59

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_PortErr	Communications Port Error	This is the error status variable for the communications port. Represents the collective status of the following error flags. • _EIP1_MacAdrErr (Port1 MAC Address Error) • _EIP1_LanHwErr (Port1 Communications Controller Error) • _EIP1_EtnCfgErr (Port1 Basic Ethernet Setting Error) • _EIP1_IPAdrCfgErr (Port1 IP Address Setting Error) • _EIP1_IPAdrDupErr (Port1 IP Address Duplication Error) • _EIP1_BootpErr (Port1 BOOTP Server Error) • _EIP_DNSCfgErr (DNS Setting Error) • _EIP_DNSSrvErr (DNS Server Connection Error) • _EIP_IPRTblErr (IP Route Table Error) **Note** If a *Link OFF Detected* or *EtherNet/IP Error* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-60

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP1_PortErr	Communications Port1 Error	This is the error status variable for the communications port 1. Represents the collective status of the following error flags. • _EIP1_MacAdrErr (Port1 MAC Address Error) • _EIP1_LanHwErr (Port1 Communications Controller Error) • _EIP1_EtnCfgErr (Port1 Basic Ethernet Setting Error) • _EIP1_IPAdrCfgErr (Port1 IP Address Setting Error) • _EIP1_IPAdrDupErr (Port1 IP Address Duplication Error) • _EIP1_BootpErr (Port1 BOOTP Server Error) • _EIP_DNSCfgErr (DNS Setting Error) • _EIP_DNSSrvErr (DNS Server Connection Error) • _EIP_IPRTblErr (IP Route Table Error) **Note** If a *Link OFF Detected* or *EtherNet/IP Error* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-60

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP2_PortErr	Communications Port2 Error	This is the error status variable for the communications port 2. Represents the collective status of the following error flags. • _EIP2_MacAdrErr (Port2 MAC Address Error) • _EIP2_LanHwErr (Port2 Communications Controller Error) • _EIP2_EtnCfgErr (Port2 Basic Ethernet Setting Error) • _EIP2_IPAdrCfgErr (Port2 IP Address Setting Error) • _EIP2_IPAdrDupErr (Port2 IP Address Duplication Error) • _EIP2_BootpErr (Port2 BOOTP Server Error) • _EIP_DNSCfgErr (DNS Setting Error) • _EIP_DNSSrvErr (DNS Server Connection Error) • _EIP_IPRTblErr (IP Route Table Error) **Note** If a *Link OFF Detected* or *EtherNet/IP Error* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-61
_EIP_CipErr	CIP Communications Error	This is the error status variable for CIP communications. Represents the collective status of the following error flags. • _EIP1_IdentityErr (CIP Communications1 Identity Error) • _EIP1_TDLinkCfgErr (CIP Communications1 Tag Data Link Setting Error) • _EIP1_TDLinkOpnErr (CIP Communications1 Tag Data Link Connection Failed) • _EIP1_TDLinkErr (CIP Communications1 Tag Data Link Communications Error) • _EIP1_TagAdrErr (CIP Communications1 Tag Name Resolution Error) • _EIP1_MultiSwONErr (CIP Communications1 Multiple Switches ON Error) **Note** If a *Tag Name Resolution Error* occurs, it is recorded in the event log and this variable changes to TRUE. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-61

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP1_CipErr	CIP Communications1 Error	This is the error status variable for CIP communications 1. Represents the collective status of the following error flags. • _EIP1_IdentityErr (CIP Communications1 Identity Error) • _EIP1_TDLinkCfgErr (CIP Communications1 Tag Data Link Setting Error) • _EIP1_TDLinkOpnErr (CIP Communications1 Tag Data Link Connection Failed) • _EIP1_TDLinkErr (CIP Communications1 Tag Data Link Communications Error) • _EIP1_TagAdrErr (CIP Communications1 Tag Name Resolution Error) • _EIP1_MultiSwONErr (CIP Communications1 Multiple Switches ON Error) **Note** If a Tag Name Resolution Error occurs, it is recorded in the event log and this variable changes to TRUE. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-61
_EIP2_CipErr	CIP Communications2 Error	This is the error status variable for CIP communications 2. Represents the collective status of the following error flags. • _EIP2_IdentityErr (CIP Communications2 Identity Error) • _EIP2_TDLinkCfgErr (CIP Communications2 Tag Data Link Setting Error) • _EIP2_TDLinkOpnErr (CIP Communications2 Tag Data Link Connection Failed) • _EIP2_TDLinkErr (CIP Communications2 Tag Data Link Communications Error) • _EIP2_TagAdrErr (CIP Communications2 Tag Name Resolution Error) • _EIP2_MultiSwONErr (CIP Communications2 Multiple Switches ON Error) **Note** If a *Tag Name Resolution Error* occurs, it is recorded in the event log and this variable changes to TRUE. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-62

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_TcpAppErr	TCP Application Communications Error	This is the error status variable for TCP application communications. Represents the collective status of the following error flags. • _EIP_TcpAppCfgErr (TCP Application Setting Error) • _EIP_NTPSrvErr (NTP Server Connection Error) **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.	WORD	16#0000 to 16#00F0	page A-62
_EIP_MacAdrErr	MAC Address Error	Indicates that an error occurred when the MAC address was read on the communications port 1 at startup. TRUE: Error FALSE: Normal	BOOL	TRUE or FALSE	page A-62
_EIP1_MacAdrErr	Port1 MAC Address Error	Indicates that an error occurred when the MAC address was read on the communications port 1 at startup. TRUE: Error FALSE: Normal	BOOL	TRUE or FALSE	page A-62
_EIP2_MacAdrErr	Port2 MAC Address Error	Indicates that an error occurred when the MAC address was read on the communications port 2 at startup. TRUE: Error FALSE: Normal	BOOL	TRUE or FALSE	page A-62
_EIP_LanHwErr	Communications Controller Error	Indicates that a Communications Controller failure occurred on the communications port 1. TRUE: Failure FALSE: Normal	BOOL	TRUE or FALSE	page A-63
_EIP1_LanHwErr	Port1 Communications Controller Error	Indicates that a Communications Controller failure occurred on the communications port 1. TRUE: Failure FALSE: Normal	BOOL	TRUE or FALSE	page A-63
_EIP2_LanHwErr	Port2 Communications Controller Error	Indicates that a Communications Controller failure occurred on the communications port 2. TRUE: Failure FALSE: Normal	BOOL	TRUE or FALSE	page A-63
_EIP_EtnCfgErr	Basic Ethernet Setting Error	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 1 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-63
_EIP1_EtnCfgErr	Port1 Basic Ethernet Setting Error	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 1 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-63

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP2_EtnCfgErr	Port2 Basic Ethernet Setting Error	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 2 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-63
_EIP_IPAdrCfgErr	IP Address Setting Error	Indicates the IP address setting errors for the communications port 1. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal	BOOL	TRUE or FALSE	page A-64
_EIP1_IPAdrCfgErr	Port1 IP Address Setting Error	Indicates the IP address setting errors for the communications port 1. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal	BOOL	TRUE or FALSE	page A-64
_EIP2_IPAdrCfgErr	Port2 IP Address Setting Error	Indicates the IP address setting errors for the communications port 2. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal	BOOL	TRUE or FALSE	page A-64
_EIP_IPAdrDupErr	IP Address Duplication Error	Indicates that the same IP address is assigned to more than one node for the communications port 1. TRUE: Duplication occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-64
_EIP1_IPAdrDupErr	Port1 IP Address Duplication Error	Indicates that the same IP address is assigned to more than one node for the communications port 1. TRUE: Duplication occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-64
_EIP2_IPAdrDupErr	Port2 IP Address Duplication Error	Indicates that the same IP address is assigned to more than one node for the communications port 2. TRUE: Duplication occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-65
_EIP_DNSCfgErr	DNS Setting Error	Indicates that the DNS or hosts settings are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-65

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_BootpErr	BOOTP Server Error	Indicates that a BOOTP server connection failure occurred on the communications port 1. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.	BOOL	TRUE or FALSE	page A-65
_EIP1_BootpErr	Port1 BOOTP Server Error	Indicates that a BOOTP server connection failure occurred on the communications port 1. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.	BOOL	TRUE or FALSE	page A-65
_EIP2_BootpErr	Port2 BOOTP Server Error	Indicates that a BOOTP server connection failure occurred on the communications port 2. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.	BOOL	TRUE or FALSE	page A-65
_EIP_IPRTblErr	IP Route Table Error	Indicates that the default gateway settings or IP router table settings are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-65
_EIP_IdentityErr	Identity Error	Indicates that the identity information for CIP communications 1 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-66
_EIP1_IdentityErr	CIP Communications1 Identity Error	Indicates that the identity information for CIP communications 1 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-66
_EIP2_IdentityErr	CIP Communications2 Identity Error	Indicates that the identity information for CIP communications 2 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-66
_EIP_TDLinkCfgErr	Tag Data Link Setting Error	Indicates that the tag data link settings for CIP communications 1 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-66

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP1_TDLinkCfgErr	CIP Communications1 Tag Data Link Setting Error	Indicates that the tag data link settings for CIP communications 1 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-66
_EIP2_TDLinkCfgErr	CIP Communications2 Tag Data Link Setting Error	Indicates that the tag data link settings for CIP communications 2 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-66
_EIP_TDLinkOpnErr	Tag Data Link Connection Failed	Indicates that establishing a tag data link connection for CIP communications 1 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-67
_EIP1_TDLinkOpnErr	CIP Communications1 Tag Data Link Connection Failed	Indicates that establishing a tag data link connection for CIP communications 1 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-67
_EIP2_TDLinkOpnErr	CIP Communications2 Tag Data Link Connection Failed	Indicates that establishing a tag data link connection for CIP communications 2 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-67
_EIP_TDLinkErr	Tag Data Link Communications Error	Indicates that a timeout occurred in a tag data link connection for CIP communications 1. TRUE: A timeout occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-67

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP1_TDLinkErr	CIP Communications1 Tag Data Link Communications Error	Indicates that a timeout occurred in a tag data link connection for CIP communications 1. TRUE: A timeout occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-67
_EIP2_TDLinkErr	CIP Communications2 Tag Data Link Communications Error	Indicates that a timeout occurred in a tag data link connection for CIP communications 2. TRUE: A timeout occurred. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-68
_EIP_TagAdrErr	Tag Name Resolution Error	Indicates that the tag resolution for CIP communications 1 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Communication Control Unit. • There is no network variable in the Communication Control Unit that corresponds to the tag setting. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-68
_EIP1_TagAdrErr	CIP Communications1 Tag Name Resolution Error	Indicates that the tag resolution for CIP communications 1 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Communication Control Unit. • There is no network variable in the Communication Control Unit that corresponds to the tag setting. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-68

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP2_TagAdrErr	CIP Communications2 Tag Name Resolution Error	Indicates that the tag resolution for CIP communications 2 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Communication Control Unit. • There is no network variable in the Communication Control Unit that corresponds to the tag setting. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-68
_EIP_MultiSwONErr	Multiple Switches ON Error	Indicates that more than one switch turned ON at the same time in CIP communications 1. TRUE: More than one data link start/stop switch changed to TRUE at the same time. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-69
_EIP1_MultiSwONErr	CIP Communications1 Multiple Switches ON Error	Indicates that more than one switch turned ON at the same time in CIP communications 1. TRUE: More than one data link start/stop switch changed to TRUE at the same time. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-69
_EIP2_MultiSwONErr	CIP Communications2 Multiple Switches ON Error	Indicates that more than one switch turned ON at the same time in CIP communications 2. TRUE: More than one data link start/stop switch changed to TRUE at the same time. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-69
_EIP_TcpAppCfgErr	TCP Application Setting Error	TRUE: At least one of the set values for a TCP application (FTP, NTP, SNMP) is incorrect. Or, a read operation failed. FALSE: Normal	BOOL	TRUE or FALSE	page A-69
_EIP_NTPSrvErr	NTP Server Connection Error	TRUE: The NTP client failed to connect to the server (timeout). FALSE: NTP is not set. Or, NTP is set and the connection was successful.	BOOL	TRUE or FALSE	page A-69
_EIP_DNSSrvErr	DNS Server Connection Error	TRUE: The DNS client failed to connect to the server (timeout). FALSE: DNS is not enabled. Or, DNS is enabled and the connection was successful.	BOOL	TRUE or FALSE	page A-69
_EIP_ChgIpSwErr	IP Address Switch Change during Operation Error	TRUE: It shows IP address switch of Port1 was changed during operation. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-70

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP1_ChgIpSwErr	Port1 IP Address Switch Change during Operation Error	TRUE: It shows IP address switch of Port1 was changed during operation. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-70
_EIP2_ChgIpSwErr	Port2 IP Address Switch Change during Operation Error	TRUE: It shows IP address switch of Port2 was changed during operation. FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-70

Hierarchical Relationship of System-defined Variables Related to EtherNet/IP Errors

The system-defined variables that are related to EtherNet/IP errors have the following hierarchical relationship. For example, if the value of any of the _EIP1_PortErr, _EIP2_PortErr, EIP1_CipErr, _EIP2_CipErr, and _EIP_TcpAppErr variables in the second level is TRUE, then the _EIP_ErrSta variable in the first level also changes to TRUE. Therefore, you can check the values of system-defined variables in a higher level to see if an error has occurred for a variable in a lower level.

Level 1		Level 2		Level 3	
Variable	Name	Variable	Name	Variable	Name
_EIP_ErrSta	EtherNet/IP Error	_EIP1_PortErr	Communications Port1 Error	_EIP1_MacAdrErr	Port1 MAC Address Error
				_EIP1_LanHwErr	Port1 Communications Controller Error
				_EIP1_EtnCfgErr	Port1 Basic Ethernet Setting Error
				_EIP1_IPAdrCfgErr	Port1 IP Address Setting Error
				_EIP1_IPAdrDupErr	Port1 IP Address Duplication Error
				_EIP1_BootpErr	Port1 BOOTP Server Error
				_EIP_DNSCfgErr	DNS Setting Error
				_EIP_DNSSrvErr	DNS Server Connection Error
				_EIP_IPRTblErr	IP Route Table Error
		_EIP2_PortErr	Communications Port2 Error	_EIP2_MacAdrErr	Port2 MAC Address Error
				_EIP2_LanHwErr	Port2 Communications Controller Error
				_EIP2_EtnCfgErr	Port2 Basic Ethernet Setting Error
				_EIP2_IPAdrCfgErr	Port2 IP Address Setting Error
				_EIP2_IPAdrDupErr	Port2 IP Address Duplication Error
				_EIP2_BootpErr	Port2 BOOTP Server Error
				_EIP_DNSCfgErr	DNS Setting Error
				_EIP_DNSSrvErr	DNS Server Connection Error
				_EIP_IPRTblErr	IP Route Table Error

Level 1		Level 2		Level 3	
Variable	Name	Variable	Name	Variable	Name
		_EIP1_CipErr	CIP Communications1 Error	_EIP1_IdentityErr	CIP Communications1 Identity Error
				_EIP1_TDLinkCfgErr	CIP Communications1 Tag Data Link Setting Error
				_EIP1_TDLinkOpnErr	CIP Communications1 Tag Data Link Connection Failed
				_EIP1_TDLinkErr	CIP Communications1 Tag Data Link Communications Error
				_EIP1_TagAdrErr	CIP Communications1 Tag Name Resolution Error
				_EIP1_MultiSwONErr	CIP Communications1 Multiple Switches ON Error
		_EIP2_CipErr	CIP Communications2 Error	_EIP2_IdentityErr	CIP Communications2 Identity Error
				_EIP2_TDLinkCfgErr	CIP Communications2 Tag Data Link Setting Error
				_EIP2_TDLinkOpnErr	CIP Communications2 Tag Data Link Connection Failed
				_EIP2_TDLinkErr	CIP Communications2 Tag Data Link Communications Error
				_EIP2_TagAdrErr	CIP Communications2 Tag Name Resolution Error
				_EIP2_MultiSwONErr	CIP Communications2 Multiple Switches ON Error
		_EIP_TcpAppErr	TCP Application Communications Error	_EIP_TcpAppCfgErr	TCP Application Setting Error
				_EIP_NTPSrvErr	NTP Server Connection Error

Note You can access the same values of the system-defined variables whose variable names with *_EIP1* and the system-defined variables whose variable names with *_EIP*. For example, you can access the same values of _EIP1_PortErr (Communications Port1 Error) and _EIP_PortErr (Communications Port Error).

● Functional Classification: EtherNet/IP Communications Status

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_EtnOnlineSta	Online	Indicates that the built-in EtherNet/IP port's communications can be used via the communications port 1 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The built-in EtherNet/IP port's communications can be used. FALSE: The built-in EtherNet/IP port's communications is disabled due to an error in initial processing, restart processing, or link OFF status.	BOOL	TRUE or FALSE	page A-70

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP1_EtnOnlineSta	Port1 Online	Indicates that the built-in EtherNet/IP port's communications can be used via the communications port 1 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The built-in EtherNet/IP port's communications can be used. FALSE: The built-in EtherNet/IP port's communications is disabled due to an error in initial processing, restart processing, or link OFF status.	BOOL	TRUE or FALSE	page A-70
_EIP2_EtnOnlineSta	Port2 Online	Indicates that the built-in EtherNet/IP port's communications can be used via the communications port 2 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The built-in EtherNet/IP port's communications can be used. FALSE: The built-in EtherNet/IP port's communications is disabled due to an error in initial processing, restart processing, or link OFF status.	BOOL	TRUE or FALSE	page A-71
_EIP_TDLinkRunSta	Tag Data Link Communications Status	Indicates that at least one connection is in normal operation in CIP communications 1. TRUE: Normal operation FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-71
_EIP1_TDLinkRunSta	CIP Communications1 Tag Data Link Communications Status	Indicates that at least one connection is in normal operation in CIP communications 1. TRUE: Normal operation FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-71
_EIP2_TDLinkRunSta	CIP Communications2 Tag Data Link Communications Status	Indicates that at least one connection is in normal operation in CIP communications 2. TRUE: Normal operation FALSE: Other than the above.	BOOL	TRUE or FALSE	page A-71
_EIP_TDLinkAllRunSta	All Tag Data Link Communications Status	Indicates that all tag data links are communicating in CIP communications 1. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.	BOOL	TRUE or FALSE	page A-71
_EIP1_TDLinkAllRunSta	CIP Communications1 All Tag Data Link Communications Status	Indicates that all tag data links are communicating in CIP communications 1. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.	BOOL	TRUE or FALSE	page A-72
_EIP2_TDLinkAllRunSta	CIP Communications2 All Tag Data Link Communications Status	Indicates that all tag data links are communicating in CIP communications 2. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.	BOOL	TRUE or FALSE	page A-72

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_RegTargetSta	Registered Target Node Information	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 1. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-72
_EIP1_RegTargetSta	CIP Communications1 Registered Target Node Information	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 1. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-72
_EIP2_RegTargetSta	CIP Communications2 Registered Target Node Information	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 2. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-72
_EIP_EstbTargetSta	Normal Target Node Information	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 1. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-73
_EIP1_EstbTargetSta	CIP Communications1 Normal Target Node Information	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 1. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-73

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP2_EstbTargetSta	CIP Communications2 Normal Target Node Information	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 2. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-73
_EIP_TargetPLCModeSta	Target PLC Operating Mode	Shows the operating status of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-73
_EIP1_TargetPLCModeSta	CIP Communications1 Target PLC Operating Mode	Shows the operating status of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-73
_EIP2_TargetPLCModeSta	CIP Communications2 Target PLC Operating Mode	Shows the operating status of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-74

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_TargetPLCErr	Target PLC Error Information	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-74
_EIP1_TargetPLCErr	CIP Communications1 Target PLC Error Information	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-74
_EIP2_TargetPLCErr	CIP Communications2 Target PLC Error Information	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-74

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_TargetNodeErr	Target Node Error Information	Indicates that the connection for the Registered Target Node Information for CIP communications 1 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-75
_EIP1_TargetNodeErr	CIP Communications1 Target Node Error Information	Indicates that the connection for the Registered Target Node Information for CIP communications 1 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-75

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP2_TargetNodeErr	CIP Communications2 Target Node Error Information	Indicates that the connection for the Registered Target Node Information for CIP communications 2 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).	ARRAY [0..255] OF BOOL	TRUE or FALSE	page A-75
_EIP_NTPResult	NTP Operation Information	Use the GetNTPStatus instruction to read the NTP operation information from the user program. Direct access is not possible.	_sNTP_RESULT		page A-75
.ExecTime	NTP Last Operation Time	Gives the last time that NTP processing ended normally. The time that was obtained from the NTP server is stored when the time is obtained normally. The time is not stored if it is not obtained from the NTP server normally.	DATE_AND_TIME	Depends on data type.	page A-76
.ExecNormal	NTP Operation Result	TRUE: Indicates an NTP normal end. FALSE: Indicates that NTP operation ended in an error or has not been executed even once.	BOOL	TRUE or FALSE	page A-76

Precautions for Correct Use

Communications Status with Target Node

The communications status of the Communication Control Unit and the target node is shown by the combination of the values of the following four system-defined variables.

- _EIP_RegTargetSta (Registered Target Node Information)
- _EIP_EstbTargetSta (Normal Target Node Information)
- _EIP_TargetPLCErr (Target PLC Error Information)
- _EIP_TargetNodeErr (Target Node Error Information)

Value of *_EIP_RegTarget-Sta*	Value of *_EIP_EstbTar-getSta*	Value of *_EIP_Tar-getPLCErr*	Value of *_EIP_Target-NodeErr*	Communications status with target node
TRUE	TRUE	FALSE	FALSE	A connection with the target node was established normally and there is no error in the target PLC.
		TRUE	TRUE	A connection with the target node was established but there is an error in the target PLC.
	FALSE	---	TRUE	A connection with the target node was not established normally.
FALSE	---	---	---	The information is not valid because the target node is not registered.

The communications status of CIP communications 1 and CIP communications 2 is shown by the combination of the values of four system-defined variables in the same way as shown in the above table.

- CIP Communications 1
  - _EIP1_RegTargetSta (CIP Communications1 Registered Target Node Information)
  - _EIP1_EstbTargetSta (CIP Communications1 Normal Target Node Information)
  - _EIP1_TargetPLCErr (CIP Communications1 Target PLC Error Information)
  - _EIP1_TargetNodeErr (CIP Communications1 Target Node Error Information)
- CIP Communications 2
  - _EIP2_RegTargetSta (CIP Communications2 Registered Target Node Information)
  - _EIP2_EstbTargetSta (CIP Communications2 Normal Target Node Information)
  - _EIP2_TargetPLCErr (CIP Communications2 Target PLC Error Information)
  - _EIP2_TargetNodeErr (CIP Communications2 Target Node Error Information)

● Functional Classification: EtherNet/IP Communications Switches

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP_TDLink-StartCmd	Tag Data Link Communications Start Switch	Change this variable to TRUE to start tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation starts. **Note** Do not force this switch to change to FALSE from the Sysmac Studio or other means before it automatically changes to FALSE.	BOOL	TRUE or FALSE	page A-76

Variable name	Meaning	Function	Data type	Range of values	Reference
_EIP1_TDLink-StartCmd	CIP Communications1 Tag Data Link Communications Start Switch	Change this variable to TRUE to start tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation starts. **Note** Do not force this switch to change to FALSE from the Sysmac Studio or other means before it automatically changes to FALSE.	BOOL	TRUE or FALSE	page A-76
_EIP2_TDLink-StartCmd	CIP Communications2 Tag Data Link Communications Start Switch	Change this variable to TRUE to start tag data links for CIP communications 2. It automatically changes back to FALSE after tag data link operation starts. **Note** Do not force this switch to change to FALSE from the Sysmac Studio or other means before it automatically changes to FALSE.	BOOL	TRUE or FALSE	page A-76
_EIP_TDLink-StopCmd	Tag Data Link Communications Stop Switch	Change this variable to TRUE to stop tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation stops. **Note** Do not force this switch to change to FALSE from the Sysmac Studio or other means before it automatically changes to FALSE.	BOOL	TRUE or FALSE	page A-77
_EIP1_TDLink-StopCmd	CIP Communications1 Tag Data Link Communications Stop Switch	Change this variable to TRUE to stop tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation stops. **Note** Do not force this switch to change to FALSE from the Sysmac Studio or other means before it automatically changes to FALSE.	BOOL	TRUE or FALSE	page A-77
_EIP2_TDLink-StopCmd	CIP Communications2 Tag Data Link Communications Stop Switch	Change this variable to TRUE to stop tag data links for CIP communications 2. It automatically changes back to FALSE after tag data link operation stops. **Note** Do not force this switch to change to FALSE from the Sysmac Studio or other means before it automatically changes to FALSE.	BOOL	TRUE or FALSE	page A-77

A-4-5 Meanings of Error Status Bits

The meanings of the individual bits in the following error status are the same.

- *_ErrSta* (Controller Error Status)
- *_PLC_ErrSta* (PLC Function Module Error Status)
- *_NXB_ErrSta* (NX Bus Function Module Error Status)
- *_NXB_MstrErrSta* (NX Bus Function Module Master Error Status)
- *_NXB_UnitErrStaTbl* (NX Bus Function Module Unit Error Status)

- *_EIP_ErrSta* (EtherNet/IP Error)
- *_EIP1_PortErr* (Communications Port1 Error), *_EIP2_PortErr* (Communications Port2 Error)
- *_EIP1_CipErr* (CIP Communications1 Error), *_EIP2_CipErr* (CIP Communications2 Error)
- *_EIP_TcpAppErr* (TCP Application Communications Error)

The meanings of the bits are shown in the following table.

Bit:	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
WORD			-	-	-	-	-	-					-	-	-	-

Bit	Description
15	Master-detected error: This bit indicates whether the master detected a Controller error in the Unit for the error status of the Controller error. TRUE: The master detected a Controller error. FALSE: The master has not detected a Controller error.
14	Collective slave error status: This bit indicates if a Controller error was detected for levels (e.g., a Unit) that are lower than the event source (i.e., a function module). TRUE: A Controller error has occurred at a lower level. FALSE: A Controller error has not occurred at a lower level.
13 to 8	Reserved.
7	This bit indicates whether a major fault level Controller error has occurred. TRUE: A major fault level Controller error has occurred. FALSE: A major fault level Controller error has not occurred.
6	This bit indicates whether a partial fault level Controller error has occurred. TRUE: A partial fault level Controller error has occurred. FALSE: A partial fault level Controller error has not occurred.
5	This bit indicates whether a minor fault level Controller error has occurred. TRUE: A minor fault level Controller error has occurred. FALSE: A minor fault level Controller error has not occurred.
4	This bit indicates whether an observation level Controller error has occurred. TRUE: An observation level Controller error has occurred. FALSE: An observation level Controller error has not occurred.
3 to 0	Reserved.

A-5 Specifications for Individual System-defined Variables

The specifications for each system-defined variable are given as described below.

Variable name	This is the system-defined variable name. The prefix gives the category name.			**Members (for structures)**	The member names are given for structure variables only.
Meaning	This is the meaning of the variable.			**Global/local**	Global: Global variable, Local: Local variable
Function	The function of the variable is described.				
Data type	The data type of the variable is given.			**Range of values**	The range of values that the variable can take is given.
R/W access	R: Read only, RW: Read/write	**Retained**	The Retain attribute of the variable is given.	**Network Publish**	The Network Publish attribute of the variable is given.

A-5-1 System-defined Variables for the Overall Controller (No Category)

● Functional Classification: Clock

Variable name	_CurrentTime				
Meaning	System Time			**Global/local**	Global
Function	Contains the Communication Control Unit's clock data.				
Data type	DATE_AND_TIME			**Range of values**	DT#1970-01-01-00:00:00 to DT#2106-02-06-23:59:59
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

● Functional Classification: Errors

Variable name	_ErrSta				
Meaning	Controller Error Status			**Global/local**	Global
Function	TRUE if there is a Controller error. FALSE if there is no Controller error. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#C0F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_AlarmFlag				
Meaning	User-defined Error Status			**Global/local**	Global
Function	The bit corresponding to the event level is TRUE while there is a user-defined error. Bits 00 to 07 correspond to user fault levels 1 to 8. This variable contains 0000 hex when there is no user-defined error.				
Data type	WORD			**Range of values**	16#0000 to 16#00FF
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

● Functional Classification: SD Memory Card

Variable name	_Card1Ready				
Meaning	SD Memory Card Ready Flag			**Global/local**	Global
Function	TRUE when the SD Memory Card is recognized. FALSE when the SD Memory Card is not recognized. TRUE: The Card can be used. FALSE: The Card cannot be used.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_Card1Protect				
Meaning	SD Memory Card Write Protected Flag			**Global/local**	Global
Function	TRUE when the SD Memory Card is write-protected with the LOCK switch. TRUE: Write protected. FALSE: Not write protected.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_Card1Err				
Meaning	SD Memory Card Error Flag			**Global/local**	Global
Function	TRUE when an unusable SD Memory Card is inserted or a format error occurs. TRUE: There is an error FALSE: There is no error				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_Card1Access				
Meaning	SD Memory Card Access Flag			**Global/local**	Global
Function	TRUE during SD Memory Card access. TRUE: Card is being accessed. FALSE: Card is not being accessed. The system updates the flag every 100 ms. Because of this, access to the SD Memory Card is shown by this flag with a delay of up to 100 ms.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_Card1Deteriorated				
Meaning	SD Memory Card Life Warning Flag			**Global/local**	Global
Function	TRUE when the life of the SD Memory Card is exceeded. If this variable changed to TRUE, replace the SD Memory Card. Read/write operation may fail if the SD Memory Card is not replaced. TRUE: The life of the Card has been exceeded. FALSE: The Card can still be used.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

(You can use the SD Memory Card life expiration detection function on some specific SD Memory Cards. Refer to *4-2 Specifications of Supported SD Memory Cards, Folders, and Files* on page 4-3.)

Variable name	_Card1PowerFail				
Meaning	SD Memory Card Power Interruption Flag			**Global/local**	Global
Function	TRUE when the power supply to the Communication Control Unit was interrupted during access to the SD Memory Card. TRUE: Power was interrupted during SD Memory Card access. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	RW	**Retained**	Retained.*1	**Network Publish**	Published.

*1. This system-defined variable is not applicable for the data backup function even with a Retain attribute.

● Functional Classification: Backup

Variable name	_BackupBusy				
Meaning	Backup Function Busy Flag			**Global/local**	Global
Function	TRUE when a backup, restoration, or verification is in progress.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

● Functional Classification: Power Supply

Variable name	_PowerOnHour				
Meaning	Total Power ON Time			**Global/local**	Global
Function	Contains the total time that the power has been ON. Contains the total time that the Communication Control Unit has been ON in 1-hour increments. To reset this value, overwrite the current value with 0. The value is not updated after it reaches 4294967295. This variable is not initialized at startup.				
Data type	UDINT			**Range of values**	0 to 4294967295
R/W access	RW	**Retained**	Retained.*1	**Network Publish**	Published.

*1. This system-defined variable is not applicable for the data backup function even with a Retain attribute.

Variable name	_PowerOnCount				
Meaning	Power Interruption Count			**Global/local**	Global
Function	Contains the number of times that the power supply has been interrupted. The value is incremented by 1 each time the power supply is interrupted after the first time that the power to the Communication Control Unit was turned ON. To reset this value, overwrite the current value with 0. The value is not updated after it reaches 4294967295. This variable is not initialized at startup.				
Data type	UDINT			**Range of values**	0 to 4294967295
R/W access	RW	**Retained**	Retained.*1	**Network Publish**	Published.

*1. This system-defined variable is not applicable for the data backup function even with a Retain attribute.

Variable name	_RetainFail				
Meaning	Retention Failure Flag			**Global/local**	Global
Function	TRUE at the following time (failure of retention during power interruptions). • When an error is detected in the battery-backup memory check at startup. FALSE at the following times (no failure of retention during power interruptions). • When no error is detected in the battery-backup memory check at startup. • When the Clear All Memory operation is performed.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Not published.

● Functional Classification: Version

Variable name	_UnitVersion				
Meaning	Unit Version			**Global/local**	Global
Function	Contains the unit version of the Communication Control Unit. The integer part of the unit version is stored in element number 0. The fractional part of the unit version is stored in element number 1. Example 1) If the unit version is 1.08, “1” is stored in element number 0 and “8” is stored in element number 1. Example 2) If the unit version is 1.10, “1” is stored in element number 0 and “10” is stored in element number 1.				
Data type	ARRAY[0..1] OF USINT			**Range of values**	0 to 99
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_HardwareRevision				
Meaning	Hardware Revision			**Global/local**	Global
Function	Contains the hardware revision of the Communication Control Unit. Contains - if the hardware revision is in blank, and A to Z for other cases.				
Data type	STRING[2]			**Range of values**	- or A to Z
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

● Functional Classification: PLC Built-in

Variable name	_DeviceOutHoldCfg				
Meaning	Device Output Hold Configuration			**Global/local**	Global
Function	It is 16#A5A5 if you retain the target device output when downloaded. In the case other than 16#A5A5, the target device output is initialized when downloaded.				
Data type	WORD			**Range of values**	16#0000 to 16#FFFF
R/W access	RW	**Retained**	Retained.	**Network Publish**	Published.

Variable name	_DeviceOutHoldStatus				
Meaning	Device Output Hold Status			**Global/local**	Global
Function	It is TRUE if the target device output is retained when downloaded. When the device output hold configuration is other than 16#A5A5, or when a major fault level Controller error occurs, the target device output is initialized and changes to FALSE.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

A-5-2 PLC Function Module, Category Name: _PLC

● Functional Classification: Errors

Variable name	_PLC_ErrSta				
Meaning	PLC Function Module Error Status			**Global/local**	Global
Function	TRUE when there is a Controller error that involves the PLC Function Module. FALSE when there is no Controller error that involves the PLC Function Module. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

● Functional Classification: Safety Data Logging

Variable name	_PLC_SFLogSta				
Meaning	Safety Data Logging Status			**Global/local**	Global
Function	Stores the status of safety data logging. Element number 0 corresponds to Logging Setting Number 1. Element number 1 corresponds to Logging Setting Number 2.				
Data type	ARRAY[0..1] OF _sSFLOG_STA			**Range of values**	---
R/W access	R	**Retained**	Not retained.	**Network Publish**	Not published.

Variable name	_PLC_SFLogSta			**Member name**	.IsStart
Meaning	Safety Data Logging Busy Flag			**Global/local**	Global
Function	TRUE when safety data logging starts.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Not published.

Variable name	_PLC_SFLogSta			**Member name**	.IsComplete
Meaning	Safety Data Logging Completed Flag			**Global/local**	Global
Function	TRUE when logging stops. FALSE when the next logging starts. When this flag is TRUE, it means that the logging has completed.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Not published.

Variable name	_PLC_SFLogSta			**Member name**	.IsOutput
Meaning	Log File Output Completed Flag			**Global/local**	Global
Function	TRUE when the log file is output. FALSE when the next logging starts.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Not published.

A-5-3 NX Bus Function Module, Category Name: _NXB

● Functional Classification: NX Bus Function Module Status

Variable name	_NXB_MaxUnitNo				
Meaning	Largest Unit Number			**Global/local**	Global
Function	Contains the largest NX Unit number of the NX Units on the Communication Control Unit that are detected by the NX Bus Function Module. If the Unit configuration information is registered by the Sysmac Studio, the value will be largest NX Unit number of the registered Unit configuration. Units that are set as unmounted Units are also included. If the Unit configuration information is not registered by the Sysmac Studio, the value will be the largest Unit number of an actual Unit configuration.				
Data type	UINT			**Range of values**	0 to 32 0: No NX Unit mounted.
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_NXB_UnitIOActiveTbl				
Meaning	NX Unit I/O Data Active Status			**Global/local**	Global
Function	Indicates whether the I/O data in the NX Units on the Communication Control Unit is valid. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of 0 indicates the NX Bus Function Module and it is always TRUE. TRUE: The I/O data in the NX Unit is valid. FALSE: The I/O data in the NX Unit is invalid. The status is FALSE for NX Units that are set as unmounted Units.				
Data type	ARRAY [0..32] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_NXB_UnitMsgActiveTbl				
Meaning	NX Unit Message Enabled Status			**Global/local**	Global
Function	Indicates whether the NX Units on the Communication Control Unit can process message communications. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of 0 indicates the NX Bus Function Module and it is always TRUE. TRUE: Message communications possible. FALSE: Message communications not possible. The status is FALSE for NX Units that are set as unmounted Units.				
Data type	ARRAY [0..32] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_NXB_UnitRegTbl				
Meaning	NX Unit Registration Status			**Global/local**	Global
Function	Indicates whether the NX Units on the Communication Control Unit are registered in the Unit configuration. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of 0 indicates the NX Bus Function Module. TRUE: Registered. FALSE: Not registered. If the Unit configuration information is not registered by the Sysmac Studio, the status is FALSE for all Units. The status is TRUE for NX Units that are set as unmounted Units.				
Data type	ARRAY [0..32] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

● Functional Classification: NX Bus Function Module Errors

Variable name	_NXB_ErrSta				
Meaning	NX Bus Function Module Error Status			**Global/local**	Global
Function	Gives the NX Bus Function Module error status. This system-defined variable provides the collective status of the NX Bus Function Module Master Error Status and NX Bus Function Module Unit Error Status for all NX Units. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#40F2
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_NXB_MstrErrSta				
Meaning	NX Bus Function Module Master Error Status			**Global/local**	Global
Function	Gives the status of errors that are detected in the NX Bus Function Module of the Communication Control Unit. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#40F2
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_NXB_UnitErrStaTbl				
Meaning	NX Bus Function Module Unit Error Status			**Global/local**	Global
Function	Gives the status of errors that are detected in the NX Bus Function Module of the Communication Control Unit. This status is given as an array of WORD data. The subscript of the array corresponds to the NX Unit number. **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	ARRAY [1..32] OF WORD			**Range of values**	16#0000 to 16#40F2
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_NXB_UnitErrFlagTbl				
Meaning	NX Unit Error Status			**Global/local**	Global
Function	Indicates whether errors occurred in the NX Unit on the Communication Control Unit. This status is given as an array of BOOL data. The subscript of the array corresponds to the NX Unit number. A subscript of "0" indicates the NX Bus Function Module and whether an event occurred that is detected by the NX Bus Function Module. TRUE: Error. FALSE: No error. The status is "FALSE" for NX Units that are set as unmounted Units.				
Data type	ARRAY [0..32] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

A-5-4 EtherNet/IP Function Module, Category Name: _EIP

● Functional Classification: EtherNet/IP Communications Errors

Variable name	_EIP_ErrSta				
Meaning	EtherNet/IP Error			**Global/local**	Global
Function	This is the error status variable for the built-in EtherNet/IP port. It represents the collective status of the following error flags. • _EIP1_PortErr (Communications Port1 Error) • _EIP2_PortErr (Communications Port2 Error) • _EIP1_CipErr (CIP Communications1 Error) • _EIP2_CipErr (CIP Communications2 Error) • _EIP_TcpAppErr (TCP Application Communications Error) **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_PortErr				
Meaning	Communications Port Error			**Global/local**	Global
Function	This is the error status variable for the communications port. It represents the collective status of the following error flags. • _EIP1_MacAdrErr (Port1 MAC Address Error) • _EIP1_LanHwErr (Port1 Communications Controller Error) • _EIP1_EtnCfgErr (Port1 Basic Ethernet Setting Error) • _EIP1_IPAdrCfgErr (Port1 IP Address Setting Error) • _EIP1_IPAdrDupErr (Port1 IP Address Duplication Error) • _EIP1_BootpErr (Port1 BOOTP Server Error) • _EIP_DNSCfgErr (DNS Setting Error) • _EIP_DNSSrvErr (DNS Server Connection Error) • _EIP_IPRTblErr (IP Route Table Error) **Note** If a *Link OFF Detected* or *EtherNet/IP Error* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_PortErr				
Meaning	Communications Port1 Error			**Global/local**	Global
Function	This is the error status variable for the communications port 1. It represents the collective status of the following error flags. • _EIP1_MacAdrErr (Port1 MAC Address Error) • _EIP1_LanHwErr (Port1 Communications Controller Error) • _EIP1_EtnCfgErr (Port1 Basic Ethernet Setting Error) • _EIP1_IPAdrCfgErr (Port1 IP Address Setting Error) • _EIP1_IPAdrDupErr (Port1 IP Address Duplication Error) • _EIP1_BootpErr (Port1 BOOTP Server Error) • _EIP_DNSCfgErr (DNS Setting Error) • _EIP_DNSSrvErr (DNS Server Connection Error) • _EIP_IPRTblErr (IP Route Table Error) **Note** If a *Link OFF Detected* or *EtherNet/IP Error* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_PortErr				
Meaning	Communications Port2 Error			**Global/local**	Global
Function	This is the error status variable for the communications port 2. It represents the collective status of the following error flags. • _EIP2_MacAdrErr (Port2 MAC Address Error) • _EIP2_LanHwErr (Port2 Communications Controller Error) • _EIP2_EtnCfgErr (Port2 Basic Ethernet Setting Error) • _EIP2_IPAdrCfgErr (Port2 IP Address Setting Error) • _EIP2_IPAdrDupErr (Port2 IP Address Duplication Error) • _EIP2_BootpErr (Port2 BOOTP Server Error) • _EIP_DNSCfgErr (DNS Setting Error) • _EIP_DNSSrvErr (DNS Server Connection Error) • _EIP_IPRTblErr (IP Route Table Error) **Note** If a *Link OFF Detected* or *EtherNet/IP Error* occurs, it is recorded in the event log and then the corresponding bit turns ON. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_CipErr				
Meaning	CIP Communications Error			**Global/local**	Global
Function	This is the error status variable for CIP communications. It represents the collective status of the following error flags. • _EIP1_IdentityErr (CIP Communications1 Identity Error) • _EIP1_TDLinkCfgErr (CIP Communications1 Tag Data Link Setting Error) • _EIP1_TDLinkOpnErr (CIP Communications1 Tag Data Link Connection Failed) • _EIP1_TDLinkErr (CIP Communications1 Tag Data Link Communications Error) • _EIP1_TagAdrErr (CIP Communications1 Tag Name Resolution Error) • _EIP1_MultiSwONErr (CIP Communications1 Multiple Switches ON Error) **Note** If a Tag Name Resolution Error occurs, it is recorded in the event log and this variable changes to TRUE. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_CipErr				
Meaning	CIP Communications1 Error			**Global/local**	Global
Function	This is the error status variable for CIP communications 1. It represents the collective status of the following error flags. • _EIP1_IdentityErr (CIP Communications1 Identity Error) • _EIP1_TDLinkCfgErr (CIP Communications1 Tag Data Link Setting Error) • _EIP1_TDLinkOpnErr (CIP Communications1 Tag Data Link Connection Failed) • _EIP1_TDLinkErr (CIP Communications1 Tag Data Link Communications Error) • _EIP1_TagAdrErr (CIP Communications1 Tag Name Resolution Error) • _EIP1_MultiSwONErr (CIP Communications1 Multiple Switches ON Error) **Note** If a Tag Name Resolution Error occurs, it is recorded in the event log and this variable changes to TRUE. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_CipErr				
Meaning	CIP Communications2 Error			**Global/local**	Global
Function	This is the error status variable for CIP communications 2. It represents the collective status of the following error flags. • _EIP2_IdentityErr (CIP Communications2 Identity Error) • _EIP2_TDLinkCfgErr (CIP Communications2 Tag Data Link Setting Error) • _EIP2_TDLinkOpnErr (CIP Communications2 Tag Data Link Connection Failed) • _EIP2_TDLinkErr (CIP Communications2 Tag Data Link Communications Error) • _EIP2_TagAdrErr (CIP Communications2 Tag Name Resolution Error) • _EIP2_MultiSwONErr (CIP Communications2 Multiple Switches ON Error) **Note** If a Tag Name Resolution Error occurs, it is recorded in the event log and this variable changes to TRUE. Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TcpAppErr				
Meaning	TCP Application Communications Error			**Global/local**	Global
Function	This is the error status variable for TCP application communications. It represents the collective status of the following error flags. • _EIP_TcpAppCfgErr (TCP Application Setting Error) • _EIP_NTPSrvErr (NTP Server Connection Error) **Note** Refer to *A-4-5 Meanings of Error Status Bits* on page A-51 for the meanings of the error status bits.				
Data type	WORD			**Range of values**	16#0000 to 16#00F0
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_MacAdrErr				
Meaning	MAC Address Error			**Global/local**	Global
Function	Indicates that an error occurred when the MAC address was read on the communications port 1 at startup. TRUE: Error FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_MacAdrErr				
Meaning	Port1 MAC Address Error			**Global/local**	Global
Function	Indicates that an error occurred when the MAC address was read on the communications port 1 at startup. TRUE: Error FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_MacAdrErr				
Meaning	Port2 MAC Address Error			**Global/local**	Global
Function	Indicates that an error occurred when the MAC address was read on the communications port 2 at startup. TRUE: Error FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_LanHwErr				
Meaning	Communications Controller Error			**Global/local**	Global
Function	Indicates that a Communications Controller failure occurred on the communications port 1. TRUE: Failure FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_LanHwErr				
Meaning	Port1 Communications Controller Error			**Global/local**	Global
Function	Indicates that a Communications Controller failure occurred on the communications port 1. TRUE: Failure FALSE: Normal				
Data type	BOOL			**Range of values**	TTRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_LanHwErr				
Meaning	Port2 Communications Controller Error			**Global/local**	Global
Function	Indicates that a Communications Controller failure occurred on the communications port 2. TRUE: Failure FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_EtnCfgErr				
Meaning	Basic Ethernet Setting Error			**Global/local**	Global
Function	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 1 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_EtnCfgErr				
Meaning	Port1 Basic Ethernet Setting Error			**Global/local**	Global
Function	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 1 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_EtnCfgErr				
Meaning	Port2 Basic Ethernet Setting Error			**Global/local**	Global
Function	Indicates that the Ethernet communications speed setting (Speed/Duplex) for the communications port 2 is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_IPAdrCfgErr				
Meaning	IP Address Setting Error			**Global/local**	Global
Function	Indicates the IP address setting errors for the communications port 1. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_IPAdrCfgErr				
Meaning	Port1 IP Address Setting Error			**Global/local**	Global
Function	Indicates the IP address setting errors for the communications port 1. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_IPAdrCfgErr				
Meaning	Port2 IP Address Setting Error			**Global/local**	Global
Function	Indicates the IP address setting errors for the communications port 2. TRUE: • There is an illegal IP address setting. • A read operation failed. • The IP address obtained from the BOOTP server is inconsistent. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_IPAdrDupErr				
Meaning	IP Address Duplication Error			**Global/local**	Global
Function	Indicates that the same IP address is assigned to more than one node for the communications port 1. TRUE: Duplication occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_IPAdrDupErr				
Meaning	Port1 IP Address Duplication Error			**Global/local**	Global
Function	Indicates that the same IP address is assigned to more than one node for the communications port 1. TRUE: Duplication occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_IPAdrDupErr				
Meaning	Port2 IP Address Duplication Error			**Global/local**	Global
Function	Indicates that the same IP address is assigned to more than one node for the communications port 2. TRUE: Duplication occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_DNSCfgErr				
Meaning	DNS Setting Error			**Global/local**	Global
Function	Indicates that the DNS or hosts settings are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_BootpErr				
Meaning	BOOTP Server Error			**Global/local**	Global
Function	Indicates that a BOOTP server connection failure occurred on the communications port 1. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_BootpErr				
Meaning	Port1 BOOTP Server Error			**Global/local**	Global
Function	Indicates that a BOOTP server connection failure occurred on the communications port 1. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_BootpErr				
Meaning	Port2 BOOTP Server Error			**Global/local**	Global
Function	Indicates that a BOOTP server connection failure occurred on the communications port 2. TRUE: There was a failure to connect to the BOOTP server (timeout). FALSE: The BOOTP is not enabled, or BOOTP is enabled and an IP address was normally obtained from the BOOTP server.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_IPRTblErr				
Meaning	IP Route Table Error			**Global/local**	Global
Function	Indicates that the default gateway settings or IP router table settings are incorrect. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_IdentityErr				
Meaning	Identity Error			**Global/local**	Global
Function	Indicates that the identity information for CIP communications 1 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_IdentityErr				
Meaning	CIP Communications1 Identity Error			**Global/local**	Global
Function	Indicates that the identity information for CIP communications 1 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_IdentityErr				
Meaning	CIP Communications2 Identity Error			**Global/local**	Global
Function	Indicates that the identity information for CIP communications 2 (which you cannot overwrite) is incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TDLinkCfgErr				
Meaning	Tag Data Link Setting Error			**Global/local**	Global
Function	Indicates that the tag data link settings for CIP communications 1 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TDLinkCfgErr				
Meaning	CIP Communications1 Tag Data Link Setting Error			**Global/local**	Global
Function	Indicates that the tag data link settings for CIP communications 1 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TDLinkCfgErr				
Meaning	CIP Communications2 Tag Data Link Setting Error			**Global/local**	Global
Function	Indicates that the tag data link setting for CIP communications 2 are incorrect. Or, a read operation failed. TRUE: Setting incorrect or read failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TDLinkOpnErr				
Meaning	Tag Data Link Connection Failed			**Global/local**	Global
Function	Indicates that establishing a tag data link connection for CIP communications 1 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TDLinkOpnErr				
Meaning	CIP Communications1 Tag Data Link Connection Failed			**Global/local**	Global
Function	Indicates that establishing a tag data link connection for CIP communications 1 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TDLinkOpnErr				
Meaning	CIP Communications2 Tag Data Link Connection Failed			**Global/local**	Global
Function	Indicates that establishing a tag data link connection for CIP communications 2 failed. TRUE: Establishing a tag data link connection failed due to one of the following causes. • The information registered for a target node in the tag data link parameters is different from the actual node information. • There was no response from the remote node. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TDLinkErr				
Meaning	Tag Data Link Communications Error			**Global/local**	Global
Function	Indicates that a timeout occurred in a tag data link connection for CIP communications 1. TRUE: A timeout occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TDLinkErr				
Meaning	CIP Communications1 Tag Data Link Communications Error			**Global/local**	Global
Function	Indicates that a timeout occurred in a tag data link connection for CIP communications 1. TRUE: A timeout occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TDLinkErr				
Meaning	CIP Communications2 Tag Data Link Communications Error			**Global/local**	Global
Function	Indicates that a timeout occurred in a tag data link connection for CIP communications 2. TRUE: A timeout occurred. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TagAdrErr				
Meaning	Tag Name Resolution Error			**Global/local**	Global
Function	Indicates that the tag resolution for CIP communications 1 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Communication Control Unit. • There is no network variable in the Communication Control Unit that corresponds to the tag setting. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TagAdrErr				
Meaning	CIP Communications1 Tag Name Resolution Error			**Global/local**	Global
Function	Indicates that the tag resolution for CIP communications 1 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Communication Control Unit. • There is no network variable in the Communication Control Unit that corresponds to the tag setting. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TagAdrErr				
Meaning	CIP Communications2 Tag Name Resolution Error			**Global/local**	Global
Function	Indicates that the tag resolution for CIP communications 2 failed (i.e., the address could not be identified from the tag name). TRUE: Tag resolution failed (i.e., the address could not be identified from the tag name). The following causes are possible. • The size of the network variable is different from the tag settings. • The I/O direction that is set in the tag data link settings does not agree with the I/O direction of the variable in the Communication Control Unit. • There is no network variable in the Communication Control Unit that corresponds to the tag setting. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_MultiSwONErr				
Meaning	Multiple Switches ON Error			**Global/local**	Global
Function	Indicates that more than one switch turned ON at the same time in CIP communications 1. TRUE: More than one data link start/stop switch changed to TRUE at the same time. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_MultiSwONErr				
Meaning	CIP Communications1 Multiple Switches ON Error			**Global/local**	Global
Function	Indicates that more than one switch turned ON at the same time in CIP communications 1. TRUE: More than one data link start/stop switch changed to TRUE at the same time. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_MultiSwONErr				
Meaning	CIP Communications2 Multiple Switches ON Error			**Global/local**	Global
Function	Indicates that more than one switch turned ON at the same time in CIP communications 2. TRUE: More than one data link start/stop switch changed to TRUE at the same time. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TcpAppCfgErr				
Meaning	TCP Application Setting Error			**Global/local**	Global
Function	TRUE: At least one of the set values for a TCP application (FTP, NTP, SNMP) is incorrect. Or, a read operation failed. FALSE: Normal				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_NTPSrvErr				
Meaning	NTP Server Connection Error			**Global/local**	Global
Function	TRUE: The NTP client failed to connect to the server (timeout). FALSE: NTP is not set. Or, NTP is set and the connection was successful.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_DNSSrvErr				
Meaning	DNS Server Connection Error			**Global/local**	Global
Function	TRUE: The DNS client failed to connect to the server (timeout). FALSE: DNS is not enabled. Or, DNS is enabled and the connection was successful.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Global

Variable name	_EIP_ChgIpSwErr				
Meaning	IP Address Switch Change during Operation Error			**Global/local**	Global
Function	TRUE: It shows IP address switch of Port1 was changed during operation. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_ChgIpSwErr				
Meaning	Port1 IP Address Switch Change during Operation Error			**Global/local**	Global
Function	TRUE: It shows IP address switch of Port1 was changed during operation. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_ChgIpSwErr				
Meaning	Port2 IP Address Switch Change during Operation Error			**Global/local**	Global
Function	TRUE: It shows IP address switch of Port2 was changed during operation. FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

● Functional Classification: EtherNet/IP Communications Status

Variable name	_EIP_EtnOnlineSta				
Meaning	Online			**Global/local**	Global
Function	Indicates that the built-in EtherNet/IP port's communications can be used via the communications port 1 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The built-in EtherNet/IP port’s communications can be used. FALSE: The built-in EtherNet/IP port’s communications is disabled due to an error in initial processing, restart processing, or link OFF status.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_EtnOnlineSta				
Meaning	Port1 Online			**Global/local**	Global
Function	Indicates that the built-in EtherNet/IP port's communications can be used via the communications port 1 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The built-in EtherNet/IP port’s communications can be used. FALSE: The built-in EtherNet/IP port’s communications is disabled due to an error in initial processing, restart processing, or link OFF status.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_EtnOnlineSta				
Meaning	Port2 Online			**Global/local**	Global
Function	Indicates that the built-in EtherNet/IP port's communications can be used via the communications port 2 (that is, the link is ON, IP address is defined, and there are no errors.) TRUE: The built-in EtherNet/IP port's communications can be used. FALSE: The built-in EtherNet/IP port's communications is disabled due to an error in initial processing, restart processing, or link OFF status.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TDLinkRunSta				
Meaning	Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that at least one connection is in normal operation in CIP communications 1. TRUE: Normal operation FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TDLinkRunSta				
Meaning	CIP Communications1 Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that at least one connection is in normal operation in CIP communications 1. TRUE: Normal operation FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TDLinkRunSta				
Meaning	CIP Communications2 Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that at least one connection is in normal operation in CIP communications 2. TRUE: Normal operation FALSE: Other than the above.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TDLinkAllRunSta				
Meaning	All Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that all tag data links are communicating in CIP communications 1. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TDLinkAllRunSta				
Meaning	CIP Communications1 All Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that all tag data links are communicating in CIP communications 1. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TDLinkAllRunSta				
Meaning	CIP Communications2 All Tag Data Link Communications Status			**Global/local**	Global
Function	Indicates that all tag data links are communicating in CIP communications 2. TRUE: Tag data links are communicating in all connections as the originator. FALSE: An error occurred in at least one connection.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_RegTargetSta				
Meaning	Registered Target Node Information			**Global/local**	Global
Function	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 1. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_RegTargetSta				
Meaning	CIP Communications1 Registered Target Node Information			**Global/local**	Global
Function	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 1. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_RegTargetSta				
Meaning	CIP Communications2 Registered Target Node Information			**Global/local**	Global
Function	Gives a list of nodes for which EtherNet/IP connections are registered for CIP communications 2. This variable is valid only when the EtherNet/IP port is the originator. Array[x] is TRUE: The connection to the node with a target node ID of x is registered. Array[x] is FALSE: The connection to the node with a target node ID of x is not registered.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_EstbTargetSta				
Meaning	Normal Target Node Information			**Global/local**	Global
Function	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 1. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_EstbTargetSta				
Meaning	CIP Communications1 Normal Target Node Information			**Global/local**	Global
Function	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 1. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_EstbTargetSta				
Meaning	CIP Communications2 Normal Target Node Information			**Global/local**	Global
Function	Gives a list of nodes that have normally established EtherNet/IP connections for CIP communications 2. Array[x] is TRUE: The connection to the node with a target node ID of x was established normally. Array[x] is FALSE: The connection to the node with a target node ID of x was not established, or an error occurred.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TargetPLCModeSta				
Meaning	Target PLC Operating Mode			**Global/local**	Global
Function	Shows the operating status of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TargetPLCModeSta				
Meaning	CIP Communications1 Target PLC Operating Mode			**Global/local**	Global
Function	Shows the operating status of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TargetPLCModeSta				
Meaning	CIP Communications2 Target PLC Operating Mode			**Global/local**	Global
Function	Shows the operating status of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP port as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. If the corresponding Normal Target Node Information is FALSE, it indicates the previous operating status. Array[x] is TRUE: This is the operating state of the target Controller with a node address of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TargetPLCErr				
Meaning	Target PLC Error Information			**Global/local**	Global
Function	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TargetPLCErr				
Meaning	CIP Communications1 Target PLC Error Information			**Global/local**	Global
Function	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 1, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TargetPLCErr				
Meaning	CIP Communications2 Target PLC Error Information			**Global/local**	Global
Function	Shows the error status (logical OR of fatal and non-fatal errors) of the target node Controllers that are connected for CIP communications 2, with the EtherNet/IP ports as the originator. The array elements are valid only when the corresponding Normal Target Node Information is TRUE. The immediately preceding value is retained if this variable is FALSE. Array[x] is TRUE: A fatal or non-fatal error occurred in the target Controller with a target node ID of x. Array[x] is FALSE: Other than the above.				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_TargetNodeErr				
Meaning	Target Node Error Information			**Global/local**	Global
Function	Indicates that the connection for the Registered Target Node Information for CIP communications 1 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TargetNodeErr				
Meaning	CIP Communications1 Target Node Error Information			**Global/local**	Global
Function	Indicates that the connection for the Registered Target Node Information for CIP communications 1 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TargetNodeErr				
Meaning	CIP Communications2 Target Node Error Information			**Global/local**	Global
Function	Indicates that the connection for the Registered Target Node Information for CIP communications 2 was not established or that an error occurred in the target Controller. The array elements are valid only when the Registered Target Node Information is TRUE. Array[x] is TRUE: A connection was not normally established with the target node for a target node ID of x (the Registered Target Node Information is TRUE and the Normal Target Node Information is FALSE), or a connection was established with the target node but an error occurred in the target Controller. Array[x] is FALSE: The target node is not registered for a target node ID of x (the Registered Target Node Information is FALSE), or a connection was normally established with the target node (the Registered Target Node Information is TRUE and the Normal Target Node Information is TRUE). An error occurred in the target Controller (the Target PLC Error Information is TRUE).				
Data type	ARRAY [0..255] OF BOOL			**Range of values**	TRUE or FALSE
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP_NTPResult				
Meaning	NTP Operation Information			**Global/local**	Global
Function	Use the GetNTPStatus instruction to read the NTP operation information from the user program. Direct access is not possible.				
Data type	_sNTP_RESULT			**Range of values**	---
R/W access	R	**Retained**	Not retained.	**Network Publish**	Published.
Usage in user program	Not possible.	**Related instructions**	You can read the contents of this variable with the GetNTPStatus instruction.		

Variable name	_EIP_NTPResult			Member name	.ExecTime
Meaning	NTP Last Operation Time			Global/local	Global
Function	Gives the last time that NTP processing ended normally. The time that was obtained from the NTP server is stored when the time is obtained normally. The time is not stored if it is not obtained from the NTP server normally.				
Data type	DATE_AND_TIME			Range of values	Depends on data type.
R/W access	R	Retained	Not retained.	Network Publish	Published.

Variable name	_EIP_NTPResult			Member name	.ExecNormal
Meaning	NTP Operation Result			Global/local	Global
Function	This variable shows if the NTP operation ended normally. TRUE: Indicates an NTP normal end. FALSE:Indicates that NTP operation ended in an error or has not been executed even once.				
Data type	BOOL			Range of values	TRUE or FALSE
R/W access	R	Retained	Not retained.	Network Publish	Published.

● Functional Classification: EtherNet/IP Communications Switches

Variable name	_EIP_TDLinkStartCmd				
Meaning	Tag Data Link Communications Start Switch			Global/local	Global
Function	Change this variable to TRUE to start tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation starts. **Note** Do not force this switch to change to FALSE from the user program or from the Sysmac Studio. It changes to FALSE automatically.				
Data type	BOOL			Range of values	TRUE or FALSE
R/W access	RW	Retained	Not retained.	Network Publish	Published.

Variable name	_EIP1_TDLinkStartCmd				
Meaning	CIP Communications1 Tag Data Link Communications Start Switch			Global/local	Global
Function	Change this variable to TRUE to start tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation starts. **Note** Do not force this switch to change to FALSE from the user program or from the Sysmac Studio. It changes to FALSE automatically.				
Data type	BOOL			Range of values	TRUE or FALSE
R/W access	RW	Retained	Not retained.	Network Publish	Published.

Variable name	_EIP2_TDLinkStartCmd				
Meaning	CIP Communications2 Tag Data Link Communications Start Switch			Global/local	Global
Function	Change this variable to TRUE to start tag data links for CIP communications 2. It automatically changes back to FALSE after tag data link operation starts. **Note** Do not force this switch to change to FALSE from the user program or from the Sysmac Studio. It changes to FALSE automatically.				
Data type	BOOL			Range of values	TRUE or FALSE
R/W access	RW	Retained	Not retained.	Network Publish	Published.

Variable name	_EIP_TDLinkStopCmd				
Meaning	Tag Data Link Communications Stop Switch			**Global/local**	Global
Function	Change this variable to TRUE to stop tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation stops. **Note** Do not force this switch to change to FALSE from the user program or from the Sysmac Studio. It changes to FALSE automatically.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	RW	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP1_TDLinkStopCmd				
Meaning	CIP Communications1 Tag Data Link Communications Stop Switch			**Global/local**	Global
Function	Change this variable to TRUE to stop tag data links for CIP communications 1. It automatically changes back to FALSE after tag data link operation stops. **Note** Do not force this switch to change to FALSE from the user program or from the Sysmac Studio. It changes to FALSE automatically.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	RW	**Retained**	Not retained.	**Network Publish**	Published.

Variable name	_EIP2_TDLinkStopCmd				
Meaning	CIP Communications2 Tag Data Link Communications Stop Switch			**Global/local**	Global
Function	Change this variable to TRUE to stop tag data links for CIP communications 2. It automatically changes back to FALSE after tag data link operation stops. **Note** Do not force this switch to change to FALSE from the user program or from the Sysmac Studio. It changes to FALSE automatically.				
Data type	BOOL			**Range of values**	TRUE or FALSE
R/W access	RW	**Retained**	Not retained.	**Network Publish**	Published.

I

Index

I

Index

Numerics

_AlarmFlag (User-defined Error Status)..... A-26, A-53
_BackupBusy (Backup Function Busy Flag)..... A-27, A-55
_Card1Access (SD Memory Card Access Flag)... A-26, A-54
_Card1Deteriorated (SD Memory Card Life Warning Flag).... ..... A-27, A-54
_Card1Err (SD Memory Card Error Flag)..... A-26, A-54
_Card1PowerFail (SD Memory Card Power Interruption Flag)..... A-27, A-55
_Card1Protect (SD Memory Card Write Protected Flag)..... ..... A-26, A-54
_Card1Ready (SD Memory Card Ready Flag)..... A-26, A-54
_CurrentTime (System Time)..... A-26, A-53
_DeviceOutHoldCfg (Device Output Hold Configuration)..... ..... A-28, A-56
_DeviceOutHoldStatus (Device Output Hold Status)..... ..... A-28, A-56
_EIP_BootpErr (BOOTP Server Error)..... A-38, A-65
_EIP_ChgIpSwErr (IP Address Switch Change during Operation Error..... A-41
_EIP_ChgIpSwErr (IP Address Switch Change during Operation Error)..... A-70
_EIP_CipErr (CIP Communications Error)..... A-34, A-61
_EIP_DNSCfgErr (DNS Setting Error)..... A-37, A-65
_EIP_DNSSrvErr (DNS Server Connection Error) A-41, A-69
_EIP_ErrSta (EtherNet/IP Error)..... A-31, A-59
_EIP_EstbTargetSta (Normal Target Node Information)..... ..... A-45, A-73
_EIP_EtnCfgErr (Basic Ethernet Setting Error)..... A-36, A-63
_EIP_EtnOnlineSta (Online)..... A-43, A-70
_EIP_IdentityErr (Identity Error)..... A-38, A-66
_EIP_IPAdrCfgErr (IP Address Setting Error)..... A-37, A-64
_EIP_IPAdrDupErr (IP Address Duplication Error) A-37, A-64
_EIP_IPRTblErr (IP Route Table Error)..... A-38, A-65
_EIP_LanHwErr (Communications Controller Error)..... ..... A-36, A-63
_EIP_MacAdrErr (MAC Address Error)..... A-36, A-62
_EIP_MultiSwONErr (Multiple Switches ON Error)..... ..... A-41, A-69
_EIP_NTPResult (NTP Operation Information)..... A-49, A-75
_EIP_NTPResult.ExecNormal (NTP Operation Result)..... ..... A-49, A-76
_EIP_NTPResult.ExecTime (NTP Last Operation Time)..... ..... A-49, A-76
_EIP_NTPSrvErr (NTP Server Connection Error). A-41, A-69
_EIP_PortErr (Communications Port Error)..... A-32, A-60
_EIP_RegTargetSta (Registered Target Node Information).... ..... A-45, A-72
_EIP_TagAdrErr (Tag Name Resolution Error)..... A-40, A-68
_EIP_TargetNodeErr (Target Node Error Information)..... ..... A-48, A-75
_EIP_TargetPLCErr (Target PLC Error Information)..... ..... A-47, A-74
_EIP_TargetPLCModeSta (Target PLC Operating Mode)..... ..... A-46, A-73
_EIP_TcpAppCfgErr (TCP Application Setting Error)..... ..... A-41, A-69
_EIP_TcpAppErr (TCP Application Communications Error)... ..... A-36, A-62
_EIP_TDLinkAllRunSta (All Tag Data Link Communications Status)..... A-44, A-71
_EIP_TDLinkCfgErr (Tag Data Link Setting Error) A-38, A-66
_EIP_TDLinkErr (Tag Data Link Communications Error)..... ..... A-39, A-67
_EIP_TDLinkOpnErr (Tag Data Link Connection Failed)..... ..... A-39, A-67
_EIP_TDLinkRunSta (Tag Data Link Communications Status)..... A-44, A-71
_EIP_TDLinkStartCmd (Tag Data Link Communications Start Switch)..... A-50, A-76
_EIP_TDLinkStopCmd (Tag Data Link Communications Stop Switch)..... A-51, A-77
_EIP1_BootpErr (Port1 BOOTP Server Error)..... A-38, A-65
_EIP1_ChgIpSwErr (Port1 IP Address Switch Change during Operation Error)..... A-42, A-70
_EIP1_CipErr (CIP Communications1 Error)..... A-35, A-61
_EIP1_EstbTargetSta (CIP Communications1 Normal Target Node Information)..... A-45, A-73
_EIP1_EtnCfgErr (Port1 Basic Ethernet Setting Error)..... ..... A-36, A-63
_EIP1_EtnOnlineSta (Port1 Online)..... A-44, A-70
_EIP1_IdentityErr (CIP Communications1 Identity Error)..... ..... A-38, A-66
_EIP1_IPAdrCfgErr (Port1 IP Address Setting Error)..... ..... A-37, A-64
_EIP1_IPAdrDupErr (Port1 IP Address Duplication Error)..... ..... A-37, A-64
_EIP1_LanHwErr (Port1 Communications Controller Error)... ..... A-36, A-63
_EIP1_MacAdrErr (Port1 MAC Address Error)..... A-36, A-62
_EIP1_MultiSwONErr (CIP Communications1 Multiple Switches ON Error)..... A-41, A-69
_EIP1_PortErr (Communications Port1 Error)..... A-33, A-60
_EIP1_RegTargetSta (CIP Communications1 Registered Target Node Information)..... A-45, A-72
_EIP1_TagAdrErr (CIP Communications1 Tag Name Resolution Error)..... A-40, A-68
_EIP1_TargetNodeErr (CIP Communications1 Target Node Error Information)..... A-48, A-75
_EIP1_TargetPLCErr (CIP Communications1 Target PLC Error Information)..... A-47, A-74
_EIP1_TargetPLCModeSta (CIP Communications1 Target PLC Operating Mode)..... A-46, A-73
_EIP1_TDLinkAllRunSta (CIP Communications1 All Tag Data Link Communications Status)..... A-44, A-72
_EIP1_TDLinkCfgErr (CIP Communications1 Tag Data Link Setting Error)..... A-39, A-66

_EIP1_TDLinkErr (CIP Communications1 Tag Data Link Communications Error)....A-40, A-67
_EIP1_TDLinkOpnErr (CIP Communications1 Tag Data Link Connection Failed)....A-39, A-67
_EIP1_TDLinkRunSta (CIP Communications1 Tag Data Link Communications Status)....A-44, A-71
_EIP1_TDLinkStartCmd (CIP Communications1 Tag Data Link Communications Start Switch).... A-51, A-76
_EIP1_TDLinkStopCmd (CIP Communications1 Tag Data Link Communications Stop Switch).... A-51, A-77
_EIP2_BootpErr (Port2 BOOTP Server Error)..... A-38, A-65
_EIP2_ChgIpSwErr (Port2 IP Address Switch Change during Operation Error).... A-42, A-70
_EIP2_CipErr (CIP Communications2 Error)..... A-35, A-62
_EIP2_EstbTargetSta (CIP Communications2 Normal Target Node Information).... A-46, A-73
_EIP2_EtnCfgErr (Port2 Basic Ethernet Setting Error).... A-37, A-63
_EIP2_EtnOnlineSta (Port2 Online).... A-44, A-71
_EIP2_IdentityErr (CIP Communications2 Identity Error).... A-38, A-66
_EIP2_IPAdrCfgErr (Port2 IP Address Setting Error).... A-37, A-64
_EIP2_IPAdrDupErr (Port2 IP Address Duplication Error).... A-37, A-65
_EIP2_LanHwErr (Port2 Communications Controller Error).... A-36, A-63
_EIP2_MacAdrErr (Port2 MAC Address Error)..... A-36, A-62
_EIP2_MultiSwONErr (CIP Communications2 Multiple Switches ON Error)....A-41, A-69
_EIP2_PortErr (Communications Port2 Error).....A-34, A-61
_EIP2_RegTargetSta (CIP Communications2 Registered Target Node Information).... A-45, A-72
_EIP2_TagAdrErr (CIP Communications2 Tag Name Resolution Error).... A-41, A-68
_EIP2_TargetNodeErr (CIP Communications2 Target Node Error Information)....A-49, A-75
_EIP2_TargetPLCErr (CIP Communications2 Target PLC Error Information)....A-47, A-74
_EIP2_TargetPLCModeSta (CIP Communications2 Target PLC Operating Mode)....A-46, A-74
_EIP2_TDLinkAllRunSta (CIP Communications2 All Tag Data Link Communications Status).... A-44, A-72
_EIP2_TDLinkCfgErr (CIP Communications2 Tag Data Link Setting Error)....A-39, A-66
_EIP2_TDLinkErr (CIP Communications2 Tag Data Link Communications Error)....A-40, A-68
_EIP2_TDLinkOpnErr (CIP Communications2 Tag Data Link Connection Failed)....A-39, A-67
_EIP2_TDLinkRunSta (CIP Communications2 Tag Data Link Communications Status)....A-44, A-71
_EIP2_TDLinkStartCmd (CIP Communications2 Tag Data Link Communications Start Switch).... A-51, A-76
_EIP2_TDLinkStopCmd (CIP Communications2 Tag Data Link Communications Stop Switch).... A-51, A-77
_ErrSta (Controller Error Status).... A-26, A-53
_HardwareRevision (Hardware Revision).... A-28, A-56
_NXB_ErrSta (NX Bus Function Module Error Status).... A-30, A-58
_NXB_MaxUnitNo (Largest Unit Number)....A-29, A-57
_NXB_MstrErrSta (NX Bus Function Module Master Error Status)....A-30, A-58
_NXB_UnitErrFlagTbl (NX Unit Error Status).... A-31, A-59
_NXB_UnitErrStaTbl (NX Bus Function Module Unit Error Status)....A-31, A-59
_NXB_UnitIOActiveTbl (NX Unit I/O Data Active Status).... A-29, A-58
_NXB_UnitMsgActiveTbl (NX Unit Message Enabled Status).... A-30, A-58
_NXB_UnitRegTbl (NX Unit Registration Status).. A-30, A-58
_PLC_ErrSta (PLC Function Module Error Status).... A-28, A-56
_PLC_SFLogSta (Safety Data Logging Status).... A-29, A-57
_PLC_SFLogSta.IsComplete (Safety Data Logging Completed Flag).... A-29, A-57
_PLC_SFLogSta.IsOutput (Log File Output Completed Flag).... A-29, A-57
_PLC_SFLogSta.IsStart (Safety Data Logging Busy Flag).... A-29, A-57
_PowerOnCount (Power Interruption Count)....A-27, A-55
_PowerOnHour (Total Power ON Time).... A-27, A-55
_RetainFail (Retention Failure Flag)....A-27, A-55
_UnitVersion (Unit Version).... A-28, A-56

A

Address....A-10
All Tag Data Link Communications Status....A-44, A-71
append....4-15
automatic clock adjustment.... 2-2
procedure....2-4
required settings.... 2-4
specifications.... 2-2

B

Backup Function Busy Flag....A-27, A-55
Basic Ethernet Setting Error....A-36, A-63
BOOTP Server Error.... A-38, A-65
bye....4-17

C

cd....4-15
CIP Communications Error....A-34, A-61
CIP Communications1 All Tag Data Link Communications Status....A-44, A-72
CIP Communications1 Error....A-35, A-61
CIP Communications1 Identity Error.... A-38, A-66
CIP Communications1 Multiple Switches ON Error.... A-41, A-69
CIP Communications1 Normal Target Node Information.... A-45, A-73
CIP Communications1 Registered Target Node Information.. A-45, A-72
CIP Communications1 Tag Data Link Communications Error.... A-40, A-67
CIP Communications1 Tag Data Link Communications Start Switch.... A-51, A-76

I

CIP Communications1 Tag Data Link Communications Status..... A-44, A-71
CIP Communications1 Tag Data Link Communications Stop Switch..... A-51, A-77
CIP Communications1 Tag Data Link Connection Failed..... A-39, A-67
CIP Communications1 Tag Data Link Setting Error..... A-39, A-66
CIP Communications1 Tag Name Resolution Error..... A-40, A-68
CIP Communications1 Target Node Error Information..... A-48, A-75
CIP Communications1 Target PLC Error Information..... A-47, A-74
CIP Communications1 Target PLC Operating Mode..... A-46, A-73
CIP Communications2 All Tag Data Link Communications Status..... A-44, A-72
CIP Communications2 Error..... A-35, A-62
CIP Communications2 Identity Error..... A-38, A-66
CIP Communications2 Multiple Switches ON Error..... A-41, A-69
CIP Communications2 Normal Target Node Information..... A-46, A-73
CIP Communications2 Registered Target Node Information.. A-45, A-72
CIP Communications2 Tag Data Link Communications Error A-40, A-68
CIP Communications2 Tag Data Link Communications Start Switch..... A-51, A-76
CIP Communications2 Tag Data Link Communications Status..... A-44, A-71
CIP Communications2 Tag Data Link Communications Stop Switch..... A-51, A-77
CIP Communications2 Tag Data Link Connection Failed..... A-39, A-67
CIP Communications2 Tag Data Link Setting Error..... A-39, A-66
CIP Communications2 Tag Name Resolution Error..... A-41, A-68
CIP Communications2 Target Node Error Information..... A-49, A-75
CIP Communications2 Target PLC Error Information..... A-47, A-74
CIP Communications2 Target PLC Operating Mode..... A-46, A-74
CIP message communications service specifications..... 8-2
close..... 4-17
Communications Controller Error..... A-36, A-63
Communications Port Error..... A-32, A-60
Communications Port1 Error..... A-33, A-60
Communications Port2 Error..... A-34, A-61
community name..... A-10 – A-13
Controller Error Status..... A-26, A-53
Controller Object..... 8-36

D

default gateway..... A-4
delete..... 4-16
Destination IP Address..... A-4
Destination Mask IP Address..... A-4
detailed descriptions of MIB objects..... 10-5
Device Output Hold Configuration..... A-28, A-56
Device Output Hold Status..... A-28, A-56
dir..... 4-13
DNS..... A-3
DNS Server Connection Error..... A-41, A-69
DNS Setting Error..... A-37, A-65
domain names..... A-3

E

Ethernet Link Object..... 8-30
EtherNet/IP Error..... A-31, A-59

F

FTP server..... A-7
FTP server application example..... 4-10
FTP server application procedure..... 4-9
FTP server overview and specifications..... 4-6
FTP settings display..... A-7

G

Gateway Address..... A-4
get..... 4-15

H

Hardware Revision..... A-28, A-56
host names..... A-3, A-8, A-10 – A-13

I

Identity Error..... A-38, A-66
Identity Object..... 8-11
interval..... A-8
IP Address Duplication Error..... A-37, A-64
IP Address Setting Error..... A-37, A-64
IP address setting method..... A-2
IP Address Switch Change during Operation Error..... A-41, A-70
IP addresses..... A-2, A-3, A-8, A-10 – A-13
IP Route Table Error..... A-38, A-65
IP router table setting example..... A-5

K

Keep Alive..... A-4
Keep Alive monitoring time..... A-4

L

Largest Unit Number..... A-29, A-57
Linger option..... A-4
LINK settings..... A-6
location..... A-10

Log File Output Completed Flag.....A-29, A-57
Lot number.....20
ls.....4-12

M

MAC Address Error..... A-36, A-62
MAC addresses..... 20
mdelete.....4-17
mdir.....4-13
mget.....4-16
MIB groups..... 10-4
MIB system diagram.....10-4
mkdir.....4-14
mls.....4-13
mput.....4-16
Multiple Switches ON Error..... A-41, A-69

N

Normal Target Node Information..... A-45, A-73
NTP Last Operation Time.....A-49, A-76
NTP Operation Information.....A-49, A-75
NTP Operation Result..... A-49, A-76
NTP operation timing..... A-8
NTP server clock information..... A-8
NTP Server Connection Error.....A-41, A-69
NTP Settings Display..... A-8
NX Bus Function Module Error Status.....A-30, A-58
NX Bus Function Module Master Error Status.....A-30, A-58
NX Bus Function Module Unit Error Status..... A-31, A-59
NX Configuration Object.....8-14
NX Unit Error Status.....A-31, A-59
NX Unit I/O Data Active Status.....A-29, A-58
NX Unit Message Enabled Status..... A-30, A-58
NX Unit Registration Status.....A-30, A-58

O

Online..... A-43, A-70
open.....4-12
Overview of the CIP message communications service....8-2

P

passwords.....A-7
PING Command.....A-14
PLC Function Module Error Status.....A-28, A-56
Port 1 - Port No..... A-13
Port 2 - Port No..... A-13
port numbers..... A-7, A-8, A-10, A-12
Port1 Basic Ethernet Setting Error..... A-36, A-63
Port1 BOOTP Server Error.....A-38, A-65
Port1 Communications Controller Error.....A-36, A-63
Port1 IP Address Duplication Error.....A-37, A-64
Port1 IP Address Setting Error..... A-37, A-64
Port1 IP Address Switch Change during Operation Error.....
.....A-42, A-70
Port1 MAC Address Error.....A-36, A-62
Port1 Online.....A-44, A-70
Port2 Basic Ethernet Setting Error..... A-37, A-63
Port2 BOOTP Server Error.....A-38, A-65
Port2 Communications Controller Error.....A-36, A-63
Port2 IP Address Duplication Error.....A-37, A-65
Port2 IP Address Setting Error..... A-37, A-64
Port2 IP Address Switch Change during Operation Error.....
.....A-42, A-70
Port2 MAC Address Error.....A-36, A-62
Port2 Online.....A-44, A-71
Power Interruption Count.....A-27, A-55
priority DNS server.....A-3
procedure to use the SNMP agent..... 10-20
Production Information.....21
put.....4-16
pwd.....4-14

Q

quit.....4-17

R

Recognition 1 settings.....A-10
Recognition 2 settings.....A-10, A-11
Recognition method.....A-10 – A-12
Registered Target Node Information.....A-45, A-72
rename..... 4-14
Retention Failure Flag..... A-27, A-55
rmdir..... 4-14

S

Safety Data Logging Busy Flag.....A-29, A-57
Safety Data Logging Completed Flag.....A-29, A-57
Safety Data Logging Status.....A-29, A-57
SD Memory Card Access Flag..... A-26, A-54
SD Memory Card Error Flag.....A-26, A-54
SD Memory Card Life Warning Flag.....A-27, A-54
SD Memory Card Power Interruption Flag..... A-27, A-55
SD Memory Card Ready Flag..... A-26, A-54
SD Memory Card Write Protected Flag..... A-26, A-54
secondary DNS server.....A-3
send a recognition trap.....A-10
server specifying method..... A-8
Settings required for the SNMP agent.....10-20
SNMP agent..... 10-2
SNMP messages.....10-3
SNMP service..... A-9
SNMP Settings Display.....A-9
SNMP specifications.....10-3
SNMP Trap Settings Display.....A-11
SNMP traps.....10-3, A-12
subnet mask..... A-2, A-3
System Time.....1-5, A-26, A-53

T

table of commands.....4-11
Tag Data Link Communications Error.....A-39, A-67
Tag Data Link Communications Start Switch.....A-50, A-76

Tag Data Link Communications Status.....A-44, A-71
Tag Data Link Communications Stop Switch.....A-51, A-77
Tag Data Link Connection Failed.....A-39, A-67
Tag Data Link Setting Error..... A-38, A-66
Tag Name Resolution Error..... A-40, A-68
Target Node Error Information..... A-48, A-75
Target PLC Error Information.....A-47, A-74
Target PLC Operating Mode.....A-46, A-73
TCP Application Communications Error..... A-36, A-62
TCP Application Setting Error.....A-41, A-69
TCP/IP Interface Object.....8-28
TCP/IP Settings Display.....A-2
TCP/UDP message service..... A-13
TCP/UDP Message Service Settings Display..... A-13
time..... A-8
timeout time.....A-9
Total Power ON Time.....A-27, A-55
Trap 1 settings.....A-12
Trap 2 settings.....A-12
type.....4-15

U

Unit Version..... 20, A-28, A-56
user.....4-12
User-defined Error Status.....A-26, A-53

V

Version.....20, A-12, A-13

W

Write Protection Key.....4-3

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:

©OMRON Corporation 2018-2026 All Rights Reserved.
In the interest of product improvement,
specifications are subject to change without notice.

Cat. No. Z396-E1-05 1026