

DeviceNet Safety

SYSTEM CONFIGURATION MANUAL

OMRON

DeviceNet Safety System Configuration Manual

Revised September 2006

Notice:

OMRON products are manufactured for use according to proper procedures by a qualified operator and only for the purposes described in this manual. The following conventions are used to indicate and classify precautions in this manual. Always heed the information provided with them. Failure to heed precautions can result in injury to people or damage to property.

WARNING

Indicates a potentially hazardous situation which, if not avoided, will result in minor or moderate injury, or may result in serious injury or death. Additionally, there may be significant property damage.



Indicates general prohibitions for which there is no specific symbol.



Indicates general mandatory actions for which there is no specific symbol.

OMRON Product References

All OMRON products are capitalized in this manual. The word “Unit” is also capitalized when it refers to an OMRON product, regardless of whether or not it appears in the proper name of the product.

The abbreviation “PLC” means Programmable Controller.

Visual Aids

The following headings appear in the left column of the manual to help you locate different types of information.

IMPORTANT Indicates important information on what to do or not to do to prevent failure to operation, malfunction, or undesirable effects on product performance.

Note Indicates information of particular interest for efficient and convenient operation of the product.

1,2,3... Indicates lists of one sort or another, such as procedures, checklists, etc.

Trademarks and Copyrights

DeviceNet and DeviceNet Safety are registered trademarks of the ODVA. Other product names and company names in this manual are trademarks or registered trademarks of their respective companies.

© OMRON, 2005

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. 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. 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.

TABLE OF CONTENTS

Notice:	1
OMRON Product References	1
Visual Aids	1
Trademarks and Copyrights.....	1
About this Manual	9
Read and Understand this Manual	11
Warranty and Limitations of Liability	11
Application Considerations	12
Disclaimers.....	13
Network Configurator Version Upgrade	15
Unit Versions of NE1A-series Controllers	17
Precautions	25
1 Intended Audience	25
2 General Precautions	25
3 Safety Precautions.....	27
4 Precautions for Safe Use	29
Section 1 Overview.....	31
1-1 DeviceNet Safety System Overview.....	32
1-1-1 About DeviceNet Safety	32
1-2 Safety Network Controller Overview	33
1-2-1 About the NE1A-series Safety Network Controller	33
1-2-2 NE1A Series Features	34
1-2-3 Standard Models.....	35
1-3 Safety I/O Terminal Overview	36
1-3-1 About the DST1-series Safety I/O Terminals.....	36
1-3-2 Safety I/O Terminal Features.....	37
1-3-3 Standard Models.....	38
1-4 Network Configurator Overview	39
1-4-1 About the Network Configurator	39
1-4-2 Network Configurator Features.....	39
1-4-3 System Requirements.....	40
1-4-4 Standard Models.....	40
1-5 Basic System Startup Procedure	41
1-5-1 System Design and Programming	41
1-5-2 Installation and Wiring.....	42
1-5-3 Configuration.....	43
1-5-4 User Test.....	43

Section 2	Constructing a Safety Network	45
2-1	Applications.....	46
2-1-1	Establishing a New Safety Network	46
2-1-2	Changing an Established Safety Network.....	49
2-2	Allocating Network Bandwidth Usage and Calculating the Best EPI.....	53
2-2-1	Checking the Network Bandwidth Used for Safety I/O Communications	53
2-2-2	Allocating Network Bandwidth Usage Rates and Calculating Best EPI	55
2-2-3	Example of EPI Calculations.....	58
2-3	Calculating and Verifying the Maximum Reaction Time	61
2-3-1	Concept of Reaction Time	61
2-3-2	Calculating the Maximum Reaction Time	62
2-3-3	Verifying the Maximum Reaction Time	66
Section 3	Basic Operation of the Network Configurator	67
3-1	Network Configurator Startup and Main Window.....	69
3-1-1	Starting and Exiting the Network Configurator.....	69
3-1-2	Checking the Version	70
3-1-3	Main Window.....	71
3-2	Menu List	72
3-2-1	File Menu	72
3-2-2	Edit Menu	72
3-2-3	View Menu	72
3-2-4	Network Menu	73
3-2-5	Device Menu	73
3-2-6	EDS File Menu	74
3-2-7	Tools Menu	74
3-2-8	Option Menu.....	74
3-2-9	Help Menu	74
3-2-10	Main Window Display Modes	74
3-3	Connecting to the Network.....	77
3-3-1	Network Connection via USB Port.....	77
3-3-2	Network Connection via DeviceNet Interface Card	77
3-4	Creating a Virtual Network	79
3-4-1	Creating a New Virtual Network.....	79
3-4-2	Network Numbers	79
3-4-3	Adding Devices	82
3-4-4	Deleting Devices	84
3-4-5	Changing the Node Address	84
3-4-6	Changing Device Comments	84
3-5	Saving and Reading Network Configuration Files	85
3-5-1	Password Protection of the Network Configuration File	85
3-5-2	Saving the Network Configuration File.....	86

3-5-3	Reading a Network Configuration File	86
3-5-4	Protect Mode.....	87
3-6	Device Password Protection	88
3-6-1	Setting a Device Password	88
3-6-2	Forgotten Device Passwords.....	89
3-7	Device Parameters and Properties	90
3-7-1	Editing Device Parameters	90
3-7-2	Uploading Device Parameters	90
3-7-3	Downloading Device Parameters	91
3-7-4	Device Properties.....	93
3-8	Parameter Verification	96
3-8-1	Device Parameter Verification	96
3-9	Configuration Lock	99
3-9-1	Locking the Device Configuration	99
3-9-2	Unlocking the Device Configuration.....	100
3-10	Device Reset and Status Change	101
3-10-1	Reset Types.....	101
3-10-2	Resetting Devices	102
3-10-3	Reset Types and Device Status	102
3-10-4	Changing Device Status	103
Section 4 Editing Safety I/O Terminal Parameters		105
4-1	Editing Parameters	106
4-1-1	Parameter Groups	106
4-1-2	General Parameter Group	108
4-1-3	Safety Input Parameter Groups	109
4-1-4	Test Output Parameter Groups	111
4-1-5	Safety Output Parameter Groups	112
4-1-6	Operation Time Parameter Groups	113
Section 5 Editing Safety Network Controller Parameters		115
5-1	Safety Connection Settings	116
5-1-1	Registering Safety Slaves.....	116
5-1-2	Setting Safety Connection Parameters.....	119
5-1-3	Stopping/Restarting Communications after an Error	124
5-1-4	Listing and Setting Connection Parameters	125
5-2	Safety Slave Settings	126
5-2-1	Registering I/O Assemblies for Safety Slaves	126
5-2-2	Setting Assembly Data.....	127
5-3	Standard Slave Settings.....	133
5-3-1	Registering I/O Assemblies for Standard Slaves.....	133
5-3-2	Setting Slave Input Data in Idle State	134
5-3-3	Setting Assembly Data.....	134

5-4	Local I/O Settings.....	136
5-4-1	Setting Safety Inputs	136
5-4-2	Setting Test Outputs	140
5-4-3	Setting Safety Outputs	142
5-5	Setting the Operating Mode and Confirming the Cycle Time	144
5-5-1	Setting the NE1A-series Controller Operating Mode	145
5-5-2	Confirming the Cycle Time.....	145
5-5-3	Restarting a Connection Stopped due to a Communications Error...	146
Section 6 Programming the Safety Network Controller		149
6-1	Starting and Exiting the Logic Editor.....	150
6-1-1	Starting the Logic Editor.....	150
6-1-2	Exiting the Logic Editor	151
6-2	Menu Commands.....	152
6-2-1	File Menu	152
6-2-2	Edit Menu	152
6-2-3	View Menu	152
6-2-4	Function Menu	153
6-2-5	Page Menu	153
6-2-6	Function Block Menu.....	153
6-3	Programming	154
6-3-1	Workspace	154
6-3-2	Function Blocks.....	155
6-3-3	Programming Using Function Blocks.....	157
6-3-4	Programming User-defined Function Blocks	170
6-3-5	Password Protection for User-defined Function Blocks.....	181
6-3-6	Saving the Program	182
6-3-7	Password Protection for Programs	182
6-3-8	Updating the Program	184
6-3-9	Monitoring the Program.....	184
Section 7 Monitoring Devices		189
7-1	Monitoring Functions.....	190
7-1-1	Monitoring Status	190
7-1-2	Monitoring Safety Connections	192
7-1-3	Monitoring Parameters.....	194
7-1-4	Monitoring the Error History	196
7-2	Maintenance Functions of DST1-series Safety I/O Terminals.....	198
7-2-1	Network Power Supply Voltage Monitor	198
7-2-2	Monitoring the Run Hours	200
7-2-3	Last Maintenance Date	203
7-2-4	Monitoring the Contact Operation Counters	205
7-2-5	Monitoring the Total ON Times	208
7-2-6	Monitoring the Operation Time	212

7-3	Maintenance Functions (Unit Version 1.0 or Later).....	216
7-3-1	Total ON Time Monitor Function.....	216
7-3-2	Contact Operation Counter.....	219
7-4	Displaying Safety Device Status	222
Section 8 Troubleshooting.....		225
8-1	Connection Status Tables	226
8-1-1	Outline.....	226
8-1-2	Connection Status for DST1 Series.....	226
8-1-3	Connection Status for the NE1A-series Controller (Safety Slave Function).....	228
8-2	Errors When Downloading	230
8-2-1	Outline.....	230
8-2-2	Error Messages and Countermeasures.....	230
8-3	Errors When Resetting	233
8-3-1	Outline.....	233
8-3-2	Error Messages and Countermeasures.....	233
8-4	Errors When Changing Modes	234
8-4-1	Outline.....	234
8-4-2	Error Messages and Countermeasures.....	234
Appendices.....		235
A-1	Connecting to the Network via a CS/CJ-series PLC	236
A-1-1	Connecting to the DeviceNet Network.....	236
A-1-2	Specifying the Connection Interface	238
A-2	Editing CS/CJ-series DeviceNet Unit Parameters	246
A-2-1	Setting the Unit Functions.....	246
A-2-2	Master Parameter Overview	247
A-2-3	I/O Allocation Using the Parameter Wizard (Simple I/O Allocation) ..	252
A-2-4	Manual I/O Allocation.....	257
A-2-5	Advanced Settings: Connection, Communications Cycle Time, Slave Function Settings, etc.	263
A-3	EDS File Management	269
A-3-1	Installing EDS Files.....	269
A-3-2	Creating EDS Files	270
A-3-3	Deleting EDS Files.....	271
A-3-4	Saving EDS Files	271
A-3-5	Searching EDS Files.....	272
A-3-6	EDS File Properties	272
A-4	Using General-purpose Tools to Set Devices	273
A-4-1	Setting Device Parameters by Specifying Class and Instance.....	273
A-4-2	Setting the Node Addresses and Baud Rates via the Network	275
A-5	Using the Password Recovery Tool	276

Glossary..... 279

Index..... 281

Revision History..... 285

About this Manual

This manual describes the configuration of the DeviceNet Safety system. Please read this manual carefully and be sure you understand the information provided before attempting to configure a DeviceNet Safety system. Be sure to read the precautions provided in the following section.

The following manuals provide information on the DeviceNet and DeviceNet Safety.

DeviceNet Safety System Configuration Manual (this manual) (Z905)

This manual explains how to configure the DeviceNet Safety system using the Network Configurator.

DeviceNet Safety Network Controller Operation Manual (Z906)

This manual describes the specifications, functions, and usage of the NE1A-series Controllers.

DeviceNet Safety I/O Terminal Operation Manual (Z904)

This manual describes the specifications, functions, and usage of the DST1 series.

DeviceNet Operation Manual (W267)

This manual describes the construction and connection of a DeviceNet network. It provides detailed information on the installation and specifications of cables, connectors, and other peripheral equipment used in the network, and on the supply of communications power. Obtain this manual and gain a firm understanding of its contents before using a DeviceNet system.



WARNING

Failure to read and understand the information provided in this manual may result in personal injury or death, damage to the product, or product failure. Please read each section in its entirety and be sure you understand the information provided in the section and related sections before attempting any of the procedures or operations given.

Read and Understand this Manual

Please read and understand this manual before using the product. Please consult your OMRON representative if you have any questions or comments.

Warranty and Limitations of Liability

WARRANTY

OMRON's exclusive warranty is that the products are free from defects in materials and workmanship for a period of one year (or other period if specified) from date of sale by OMRON.

OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, REGARDING NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR PARTICULAR PURPOSE OF THE PRODUCTS. ANY BUYER OR USER ACKNOWLEDGES THAT THE BUYER OR USER ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE. OMRON DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED.

LIMITATIONS OF LIABILITY

OMRON SHALL NOT BE RESPONSIBLE FOR SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR COMMERCIAL LOSS IN ANY WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED ON CONTRACT, WARRANTY, NEGLIGENCE, OR STRICT LIABILITY.

In no event shall the responsibility of OMRON for any act exceed the individual price of the product on which liability is asserted.

IN NO EVENT SHALL OMRON BE RESPONSIBLE FOR WARRANTY, REPAIR, OR OTHER CLAIMS 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 OR REPAIR.

Application Considerations

SUITABILITY FOR USE

OMRON shall not be responsible for conformity with any standards, codes, or regulations that apply to the combination of products in the customer's application or use of the products.

At the customer's request, OMRON will provide applicable third party certification documents identifying ratings and limitations of use that apply to the products. This information by itself is not sufficient for a complete determination of the suitability of the products in combination with the end product, machine, system, or other application or use.

The following are some examples of applications for which particular attention must be given. This is not intended to be an exhaustive list of all possible uses of the products, nor is it intended to imply that the uses listed may be suitable for the products:

- Outdoor use, uses involving potential chemical contamination or electrical interference, or conditions or uses not described in this manual.
- Nuclear energy control systems, combustion systems, railroad systems, aviation systems, medical equipment, amusement machines, vehicles, safety equipment, and installations subject to separate industry or government regulations.
- Systems, machines, and equipment that could present a risk to life or property.

Please know and observe all prohibitions of use applicable to the products.

NEVER USE THE PRODUCTS FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCTS ARE PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

PROGRAMMABLE PRODUCTS

OMRON shall not be responsible for the user's programming of a programmable product, or any consequence thereof.

Disclaimers

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 model numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the products may be changed without any notice. When in doubt, special model numbers may be assigned to fix or establish key specifications for your application on your request. Please consult with your OMRON representative at any time to confirm actual specifications of purchased products.

DIMENSIONS AND WEIGHTS

Dimensions and weights are nominal and are not to be used for manufacturing purposes, even when tolerances are shown.

PERFORMANCE DATA

Performance data given in this manual 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 users must correlate it to actual application requirements. Actual performance is subject to the OMRON Warranty and Limitations of Liability.

ERRORS AND OMISSIONS

The information in this manual has been carefully checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical, or proofreading errors, or omissions.

Network Configurator Version Upgrade

The WS02-CFSC1-E Network Configurator has been upgraded from version 1.5□ to 1.6□. The following table lists details of the upgrade.

Item	Ver.1.5□	Ver.1.6□
Number of safety connections display	Not available.	The number of connections that are currently set is displayed.
Safety device status display update	Not available.	An update function for displaying safety device status has been added for Maintenance Mode displays, making it possible to update status displays at any time.
Upgraded device information displays	Not available.	Device lists can be displayed for basic devices (Masters and Slaves). A function has been added for opening and closing these displays.
ON/OFF delay adjustment function	Not available.	A function has been added in the NE1A-SCPU□□ setting window to adjust the ON/OFF delay based on the cycle time.

The following functions have also been added for NE1A Series unit version 1.0.

Function	Description
Logic Operation Functions	
Logic operations	A maximum of 254 function blocks and logic functions can be used in a program.
Added function blocks	<p>The following function blocks can be used.</p> <ul style="list-style-type: none"> • RS-flip-flop • Multi connector • Muting • Enable switch • Pulse generator • Counter • Comparator
Reset/restart function block reset causes	<p>The following reset causes can be selected.</p> <ul style="list-style-type: none"> • Low - High – Low ON pulse (existing function) <p>Low – High rising edge</p>
I/O Control Functions	
Data that can be used with I/O tags	<p>The following I/O tags can be used.</p> <ul style="list-style-type: none"> • Local I/O status <p>General user status</p>
Contact operation counters	The number of times each input or output is turned ON and OFF can be counted and stored in internal memory.
Total ON time monitors	The amount of time each input or output is ON can be totaled and stored in internal memory.
DeviceNet Communications Functions	
Safety Master functions	A maximum of 32 connections can be used.
Safety I/O communications operating mode for communications errors	<p>Any of the following safety I/O communications operating modes can be selected for when communications errors occur.</p> <ul style="list-style-type: none"> • Automatic recovery (existing operation) • Error connection only stopped <p>All connections stopped</p>
Safety I/O communications re-opening when stopped due to an error	When safety I/O communications are stopped due to an error, they can be re-opened by the Network Configurator or a logic program.
Remote I/O allocation	<p>The following data can be added to transmission data for a Safety Input Slave or Standard Input Slave.</p> <ul style="list-style-type: none"> • Local input <p>Local output monitor</p>
Maintenance Functions	
Maintenance function settings	Total ON time monitor and contact operation counter functions are available.
Maintenance information display	NE1A-SPU01 and NE1A-CPU02 maintenance information can be referenced using the Configurator's maintenance information display function.
Maintenance information monitoring	A maintenance information monitor function has been added to the Device Monitor Window.

Unit Versions of NE1A-series Controllers

Unit Versions

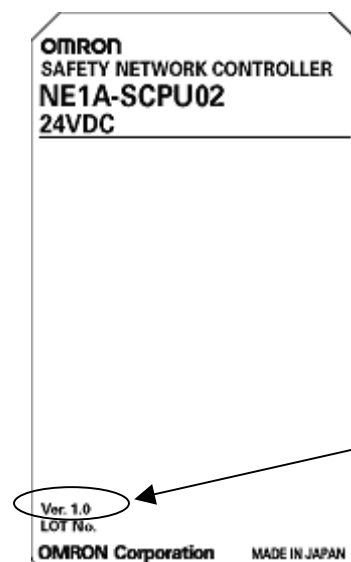
A “unit version” has been introduced to manage NEA1-series Safety Network Controllers according to differences in functionality accompanying Unit upgrades.

1) Notation of Unit Versions on Products

The unit version (Ver. □.□) is listed near the lot number on the nameplate of the products for which unit versions are being managed, as shown below.

- The unit versions of the NE1A-SCPU01 and NE1A-SCPU02 Controllers begin from Ver. 1.0.
- Controllers that do not have a unit version listed on the label are called Pre-Ver. 1.0 Controllers.

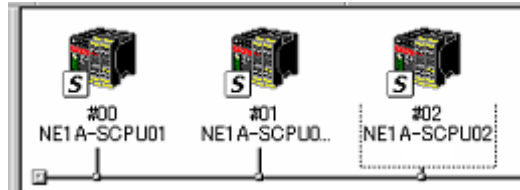
Product Nameplate



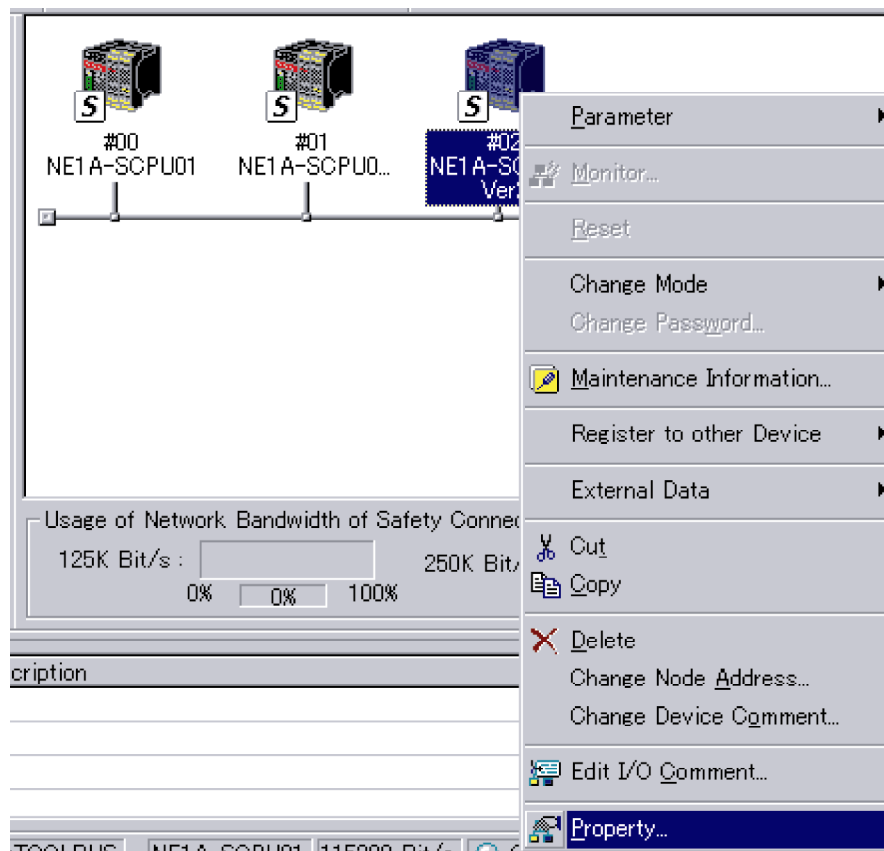
The unit version is listed here.
(Example: Ver. 1.0)

- 2) Checking the Unit Version with Support Software
The following procedure can be used to check the unit version from the Network Configurator Ver. 1.6 or higher.

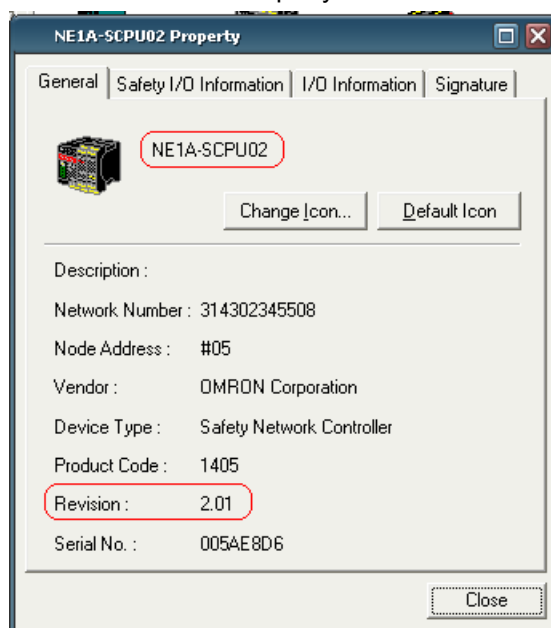
1. Upload the configuration information from the system. The device icons will be displayed, as shown in the following diagram.



2. Right-click on the Controller's icon to display the popup menu shown below.
Select **Property** from the menu.



3. The Controller's Property Window will be displayed.



The Controller's model number (device name) and revision are displayed in the Property Window. The NE1A-series Controllers supported by version 1.6□ are listed in the following table.

Model	Device name	Revision	Unit version
NE1A-SPU01	NE1A-CPU01	1.01	Pre-Ver. 1.0
NE1A-SPU01-V1	NE1A-CPU01-V1	1.01	1.0
NE1A-SPU02	NE1A-SPU02	1.01	1.0

3) Checking the Unit Version with the Unit Version Label

The following unit version labels are provided with the Controller.



These labels can be affixed to the front of earlier Controllers to differentiate between Controllers with different unit versions.

Function Support by Unit Version

Model	NE1A-SCPU01-V1		NE1A-SCPU02
Unit version	Pre-Ver. 1.0	Ver. 1.0	Ver. 1.0
Function			
Logic operations			
Maximum program size (total number of function blocks)	128	254	254
Added function blocks • RS Flip-flop • Multi Connector • Muting • Enable Switch • Pulse Generator • Counter • Comparator	---	Supported	Supported
Selection of the rising edge of the reset condition for the Reset and Restart Function Blocks	---	Supported	Supported
Use local I/O status in logic programming	---	Supported	Supported
Use the Unit's general status in logic programming	---	Supported	Supported
I/O control functions			
Contact Operation Counter	---	Supported	Supported
Total ON Time Monitor	---	Supported	Supported
DeviceNet communications functions			
Number of safety I/O connections at the Safety Master	16	32	32
Selection of operation of safety I/O communications after a communications error	---	Supported	Supported
Add local output status to send data during Slave operation.	---	Supported	Supported
Add local input monitoring to send data during Slave operation.	---	Supported	Supported
Functions supporting system startup and error recovery			
Saving non-fatal error history in non-volatile memory	---	Supported	Supported
Added function block errors to error history.	---	Supported	Supported

Unit Versions and Programming Devices

Network Configurator Ver. 1.6□ or higher must be used when using a Ver. 1.0 Safety Logic Controller. The following table shows the relationship between unit versions and Network Configurator versions.

Model number	Network Configurator		
	Ver. 1.3□	Ver. 1.5□	Ver. 1.6□
NE1A-SCPU01 Pre-Ver. 1.0	Can be used.	Can be used.	Can be used.
NE1A-SCPU01-V1 Ver. 1.0	Cannot be used.	Cannot be used.	Can be used.
NE1A-SCPU02 Ver. 1.0	Cannot be used.	Cannot be used.	Can be used.

Converting Systems to New Versions of the NE1A Controller

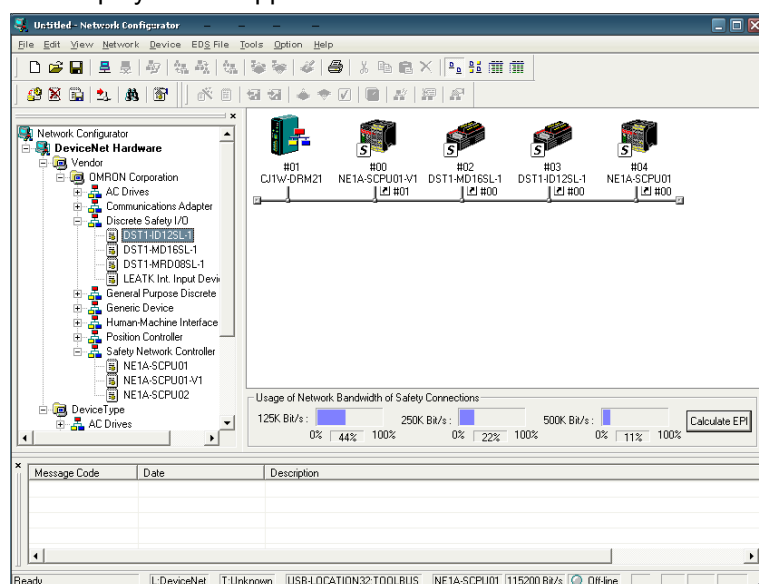
Many function have been expanded from NE1A-SCPU01 to create the NE1A-SCPU01-V1 and NE1A-SCPU02. To change from a system created with the NE1A-SCPU01 to a system that can be used with the NE1A-SCPU01-V1 or NE1A-SCPU02, the NE1A-SCPU01 configuration data must be converted to configuration data for the NE1A-SCPU01-V1 or NE1A-SCPU02. The procedure for converting configuration data is given below.

1. Read the configuration data.

Using Network Configurator version 1.6, read the configuration data using one of the following methods:

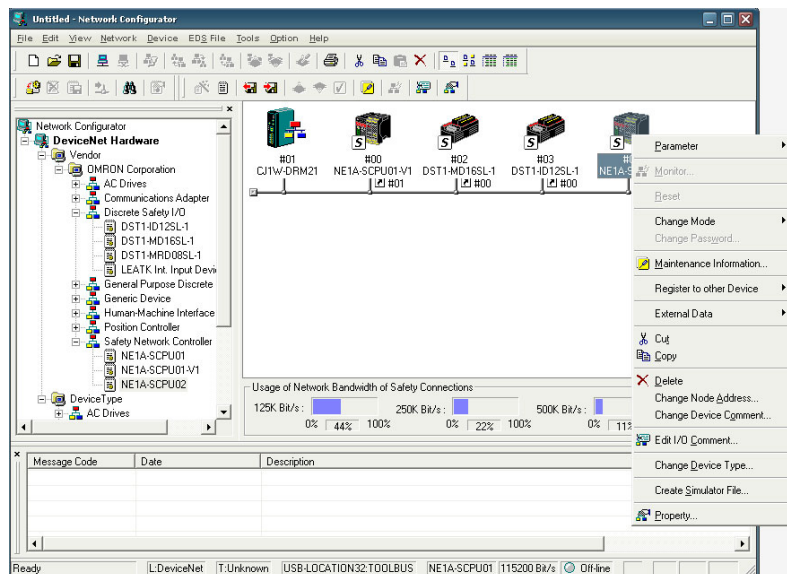
- Read configuration data that has been saved on the computer.
- Upload the configuration data from the network devices.

The display should appear as follows after then data has been read:



2. Convert the configuration data.

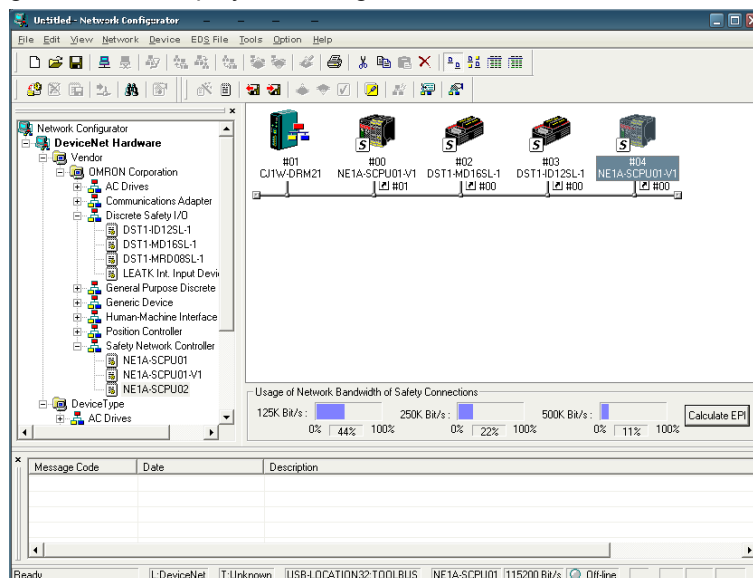
In the network configuration, right-click the NE1A-SCPU01 data to be converted to NE1A-SCPU01-V1 or NE1A-SCPU02 data and select **Change Device Type** from the pop-up menu.



Select the device to which the data is to be converted in the *New Device* Field and click the **OK** Button.



The data will be converted to configuration data for the new devices and the model given on the display will change.



3. Expansion Functions

All the configuration data for the expansion functions will be set to the default settings. Change these settings as required for any expansion functions that are to be used.

Precautions When Moving from Version 1.3□ to 1.5□

Data Compatibility

Data created using version 1.3□ can be used with version 1.5□ without any problems if converted as outlined below. Version 1.5□ data cannot be used with version 1.3□; the version 1.3□ data upload from the device will fail when loading the project file.

Procedure for Converting from Version 1.3□ to 1.5□

Version 1.5□ has improved safety check functions, so version 1.3□ programs will need to be checked for safety. Use the following procedure to check programs.

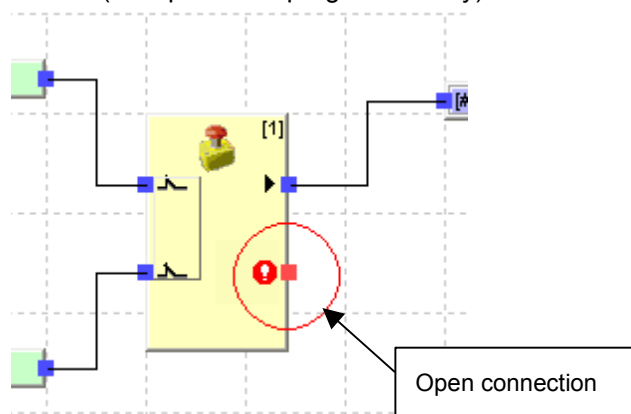
- (1) Click the **Logic** Tab on the Edit Device Parameters Window of the NE1A-series Controller and click the **Edit** Button to start the Logic Editor.
- (2) Select **Edit – Find Function Blocks with Open Connections** to check that all function block I/O have connections.
- (3) Select **File – Apply** to save the logic program then exit the editing of the logic program.
- (4) Return to the NE1A-series Controller's Edit Device Parameters Window and click the **OK** Button.

Note: Data created using version 1.3□ cannot be monitored online.
Always convert the data to version 1.5□ and download it before monitoring online.

Handling Function Blocks with Open I/O Connections

Function block outputs with open connections in version 1.3□ data could still be downloaded (see following diagram).

Download cannot be executed with version 1.5□, however, if there are outputs with open connections (to improve the program validity).



For this reason, data created using version 1.3□ cannot be downloaded as is for use with version 1.5□. If open connections exist in version 1.3□ data, use the Search Open Connection function and use the Set Output Point Tab Page in the Safety Gate Monitoring Window to disable the outputs or connect the open connections to output I/O tags.

Note: Version 1.5□ and 1.6□ have functions for creating text boxes on program screens and changing the I/O tag color. The text box and I/O color data is not saved to the NE1A-series Controller, however, during download. For this reason, text box and I/O tag color data is not restored when the program is uploaded.

Precautions

1 Intended Audience

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

- Personnel in charge of introducing FA and safety systems into production facilities
- Personnel in charge of designing FA and safety systems
- Personnel in charge of managing FA facilities
- Personnel who have the qualifications, authority, and obligation to provide safety during each of the following product phases: mechanical design, installation, operation, maintenance, and disposal

2 General Precautions

The user must operate the product according to the performance specifications described in the operation manuals.

Before using the product under conditions which are not described in the manual or applying the product to nuclear control systems, railroad systems, aviation systems, vehicles, combustion systems, medical equipment, amusement machines, safety equipment, and other systems, machines, and equipment that may have a serious influence on lives and property if used improperly, consult your OMRON representative.

Make sure that the ratings and performance characteristics of the product are sufficient for the systems, machines, and equipment, and be sure to provide the systems, machines, and equipment with double safety mechanisms.

This manual provides information for programming and operating the Unit. Be sure to read this manual before attempting to use the Unit and keep this manual close at hand for reference during operation.

WARNING

This is the *System Configuration Manual* for DeviceNet Safety Systems. Heed the following items during system construction to ensure that safety-related components are configured in a manner that allows the system functions to operate sufficiently.

● Risk Assessment

The proper use of safety devices described in this Manual as it relates to installation conditions and mechanical performance and functions is a prerequisite for their use. When selecting or using a safety device, risk assessment must be conducted with the aim of identifying potential danger factors in equipment or facilities in which the safety device is to be applied, during the development stage of the equipment or facilities. Suitable safety devices must be selected under the guidance of a sufficient risk assessment system. An insufficient risk assessment system may lead to the selection of unsuitable safety devices.

- Typical related international standards: ISO 14121, Safety of Machinery -- Principles of Risk Assessment

● Safety Measures

When using safety devices to build systems containing safety-related components for equipment or facilities, the system must be designed with the full understanding of and conformance to international standards, such as those listed below, and/or standards in related industries.

- Typical related international standards: ISO/DIS 12100, Safety of Machinery -- Basic Concepts and General Principles for Design
IEC 61508, Safety Standard for Safety Instrumented Systems (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)

● Role of Safety Devices

The safety devices are provided with safety functions and mechanisms as stipulated in relevant standards, but suitable designs must be used to allow these functions and mechanisms to operate properly inside system constructions containing safety-related components. Build systems that enable these functions and mechanisms to perform properly, based on a full understanding of their operation.

- Typical related international standards: ISO 14119, Safety of Machinery -- Interlocking Devices Associated with Guards -- Principles of Design and Selection

● Installation of Safety Devices

The construction and installation of systems with safety-related components for equipment or facilities must be performed by technicians who have received suitable training.

- Typical related international standards: ISO/DIS 12100, Safety of Machinery -- Basic Concepts and General Principles for Design
IEC 61508, Safety Standard for Safety Instrumented Systems (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems)

● Complying with Laws and Regulations

The safety devices conform to the relevant regulations and standards, but make sure that they are used in compliance with local regulations and standards for the equipment or facilities in which they are applied.

- Typical related international standards: IEC 60204, Safety of Machinery -- Electrical Equipment of Machines

● Observing Precautions for Use

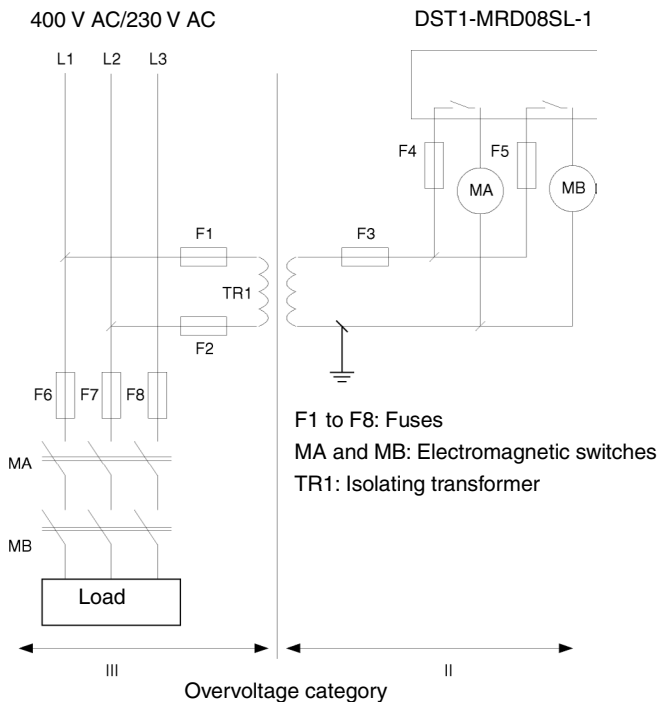
When putting the selected safety devices to actual use, heed the specifications and precautions in this Manual and those in the Operation Manuals that comes with the products. Using the products in a manner that deviates from these specifications and precautions will lead to unexpected failures in equipment or devices, and to damages that result from such failures, due to insufficient operating functions in safety-related components.

● Moving or Transferring Devices or Equipment

When moving or transferring devices or equipment, be sure to include this Manual to ensure that the person to whom the device or equipment is being moved or transferred will be able to operate the system properly.

- Typical related international standards: ISO/DIS 12100 ISO, Safety of Machinery -
- Basic Concepts and General Principles for Design IEC 61508, Safety Standard
for Safety Instrumented Systems (Functional Safety of
Electrical/Electronic/Programmable Electronic Safety-related Systems)

3 Safety Precautions

⚠ WARNING	
Safety functions may be impaired and serious injury may occasionally occur. Do not use the test outputs of the products as safety outputs.	⊘
Safety functions may be impaired and serious injury may occasionally occur. Do not use DeviceNet standard I/O data or explicit message data as safety signals.	⊘
Safety functions may be impaired and serious injury may occasionally occur. Do not use the indicators on the products for safety operations.	⊘
Serious injury may possibly occur due to breakdown of safety outputs or test outputs. Do not connect loads beyond the rated value to the safety outputs or test outputs.	⊘
Safety functions may be impaired and serious injury may occasionally occur. Wire the output lines and 24-VDC line so that they will not touch each other to prevent a load from turning ON due to a short-circuit with the 24-VDC line.	!
Safety functions may be impaired and serious injury may occasionally occur. Ground the 0-V side of the external power supply to prevent an output from turning ON due to a ground fault in a safety output or test output.	!
<p>For the DST1-MRD08SL-1, isolating transformers, such as TR1, that are used to isolate between overvoltage categories III and II must conform to IEC 60742, and the insulation between the primary input and secondary output must satisfy at least the basic insulation standards of overvoltage category III. One side of the secondary output of the isolating transformer must be grounded to prevent electrical shock in case of short-circuiting to the ground or to the frame of the isolating transformer. To protect the isolating transformer and to prevent electrical shock in case of short-circuiting to the frame, insert fuses according to transformer specifications, i.e., at points F1, F2, and F3.</p>  <p>The diagram illustrates the electrical setup for the DST1-MRD08SL-1 device. On the left, a 400 V AC/230 V AC supply is connected to three lines labeled L1, L2, and L3. These lines pass through fuses F6, F7, and F8 respectively. The output of this supply is connected to an isolating transformer TR1. The primary of TR1 is connected to the supply lines, with fuses F1 and F2 placed on the lines. The secondary of TR1 is connected to the device, with fuse F3 placed on the line. The device has two output terminals, MA and MB, which are connected to electromagnetic switches. The diagram also shows a Load connected to the output lines. A ground symbol is shown at the bottom of the device. A legend indicates: F1 to F8: Fuses; MA and MB: Electromagnetic switches; TR1: Isolating transformer. The diagram is divided into two sections by a vertical line, labeled III and II, representing different overvoltage categories.</p> <p style="text-align: center;">Overvoltage category</p>	
Safety functions may be impaired and serious injury may occasionally occur. For the DST1-MRD08SL-1, insert a fuse rated at 3.15 A or less for each output terminal to protect safety output contacts from welding. Confirm the fuse selection with the fuse manufacturer to ensure the dependability of the characteristics of the connected load.	!
Safety functions may be impaired, and serious injury may occasionally occur. Before connecting a device to the network, clear the previous configuration data.	!

⚠ WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before connecting a device to the network, configure the appropriate node address and the baud rate.



Safety functions may be impaired and serious injury may occasionally occur. Before operating the system, conduct user testing to confirm if the configuration data of all the devices and their operations are correct.



Safety functions may be impaired, and serious injury may occasionally occur. When replacing a device, confirm that the replacement device is appropriately configured and operates properly.



Serious injury may possibly occur due to loss of required safety functions. Use appropriate components or devices according to the requirements given in the following table.



Controlling devices	Requirements
Emergency stop switch	Use approved devices with a direct opening mechanism compliant with IEC/EN 60947-5-1.
Door interlocking switch or limit switch	Use approved devices with a direct opening mechanism compliant with IEC/EN 60947-5-1 and capable of switching micro-loads of 4 mA at 24 VDC.
Safety sensor	Use approved devices compliant with the relevant product standards, regulations, and rules in the country where they are used.
Relay with forcibly guided contacts	Use approved devices with forcibly guided contacts compliant with EN 50205. For feedback, use devices with contacts capable of switching micro-loads of 4 mA at 24 VDC.
Contactor	Use contactors with a forcibly guided mechanism and monitor the auxiliary NC contact to detect contactor failures. For feedback, use devices with contacts capable of switching micro-loads of 4 mA at 24 VDC.
Other devices	Evaluate whether devices used are appropriate to satisfy the requirements of the safety category level.

4 Precautions for Safe Use

● Handling

Do not drop the products or subject them to excessive vibration or impact. Doing so may result in error or malfunction.

● Installation and Storage

Do not install or store the products in the following locations:

- Locations subject to direct sunlight
- Locations subject to temperatures or humidity outside the range specified in the specifications
- Locations subject to condensation as the result of severe changes in temperature
- Locations subject to corrosive or flammable gases
- Locations subject to dust (especially iron dust) or salts
- Locations subject to water, oil, or chemicals
- Locations subject to shock or vibration outside the range specified in the specifications

Take appropriate and sufficient measures when installing systems in the following locations. Inappropriate and insufficient measures may result in malfunction.

- Locations subject to static electricity or other forms of noise
- Locations subject to strong electromagnetic fields
- Locations subject to possible exposure to radioactivity
- Locations close to power supplies

● Mounting

Confirm the operating suggestions provided in the operation manual for each product before installation and mounting.

● Wiring

- Use the following wires to connect external I/O devices to the products.

Solid wire	0.2 to 2.5 mm ² (AWG 24 to AWG 12)
Stranded (flexible) wire	0.34 to 1.5 mm ² (AWG 22 to AWG 16) Stranded wires should be prepared by attaching ferrules with plastic insulation collars (DIN 46228-4 standard compatible) before connecting them.

- Turn OFF the power supply before starting any wiring operations. Not doing so may result in unexpected operation of external devices connected to the products.
- Properly apply the specified voltage to the product inputs. Applying an inappropriate DC voltage or any AC voltage may cause reduced safety functions, damage to the products, or a fire.
- Do not wire cables for communications and I/O signals near high-voltage lines or power lines.
- Be careful not to get your fingers caught when attaching connectors to the plugs on the products.
- Tighten the DeviceNet connector to the appropriate torque (0.25 to 0.3 Nm).
- Incorrect wiring may reduce safety functions. Perform all wiring correctly and check operation prior to using the products.
- Remove the dust-preventive label after completing wiring to ensure proper heat dissipation.

- **Selecting a Power Supply**

Use a DC power supply satisfying the following requirements.

- The secondary circuits of the DC power supply must be isolated from the primary circuit by double insulation or reinforced insulation.
- The DC power supply must satisfy the requirements for class 2 circuits or limited voltage/current circuits defined in UL 508.
- The output hold time must be 20 ms or longer.

- **Periodic Inspections and Maintenance**

- Turn OFF the power supply before replacing the products. Not doing so may result in unexpected operation of external devices connected to the products.
- Do not disassemble, repair, or modify the products. Doing so may impair the safety functions.

- **Disposal**

- If you disassemble the products for disposal, be careful not to injure yourself.

Section 1

Overview

1-1	DeviceNet Safety System Overview.....	32
1-1-1	About DeviceNet Safety	32
1-2	Safety Network Controller Overview	33
1-2-1	About the NE1A Safety Network Controller	33
1-2-2	NE1A Series Features	34
1-2-3	Standard Models	35
1-3	Safety I/O Terminal Overview	36
1-3-1	About the DST1-series Safety I/O Terminals	36
1-3-2	Safety I/O Terminal Features.....	37
1-3-3	Standard Models	38
1-4	Network Configurator Overview	39
1-4-1	About the Network Configurator	39
1-4-2	Network Configurator Features.....	39
1-4-3	System Requirements.....	40
1-4-4	Standard Models.....	40
1-5	Basic System Startup Procedure	41
1-5-1	System Design and Programming	41
1-5-2	Installation and Wiring.....	42
1-5-3	Configuration.....	43
1-5-4	User Test.....	43

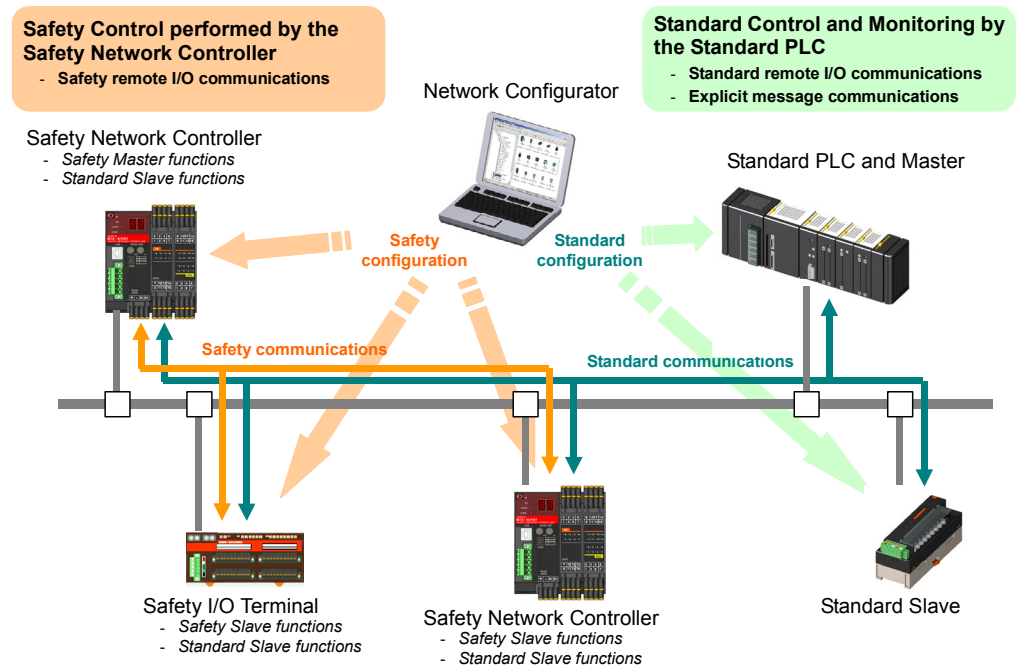
1-1 DeviceNet Safety System Overview

1-1-1 About DeviceNet Safety

DeviceNet is an open-field, multi-vendor, multi-bit network, which combines the controls in the machine and line control levels with information. The DeviceNet Safety network adds safety functions to the conventional standard DeviceNet communications protocol. The DeviceNet Safety concept has been approved by a third-party organization (TUV Rhineland).

Just as with DeviceNet, DeviceNet Safety-compliant devices from third-party vendors can be connected to a DeviceNet Safety network. Also, DeviceNet-compliant devices and DeviceNet Safety-compliant devices can be combined and connected on the same network.

By combining DeviceNet Safety-compliant products, a user can construct a safety control/network system that meets the requirements for Safety Integrity Level (SIL) 3 according to IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems) and the requirements for Safety Category 4 according to EN 954-1.



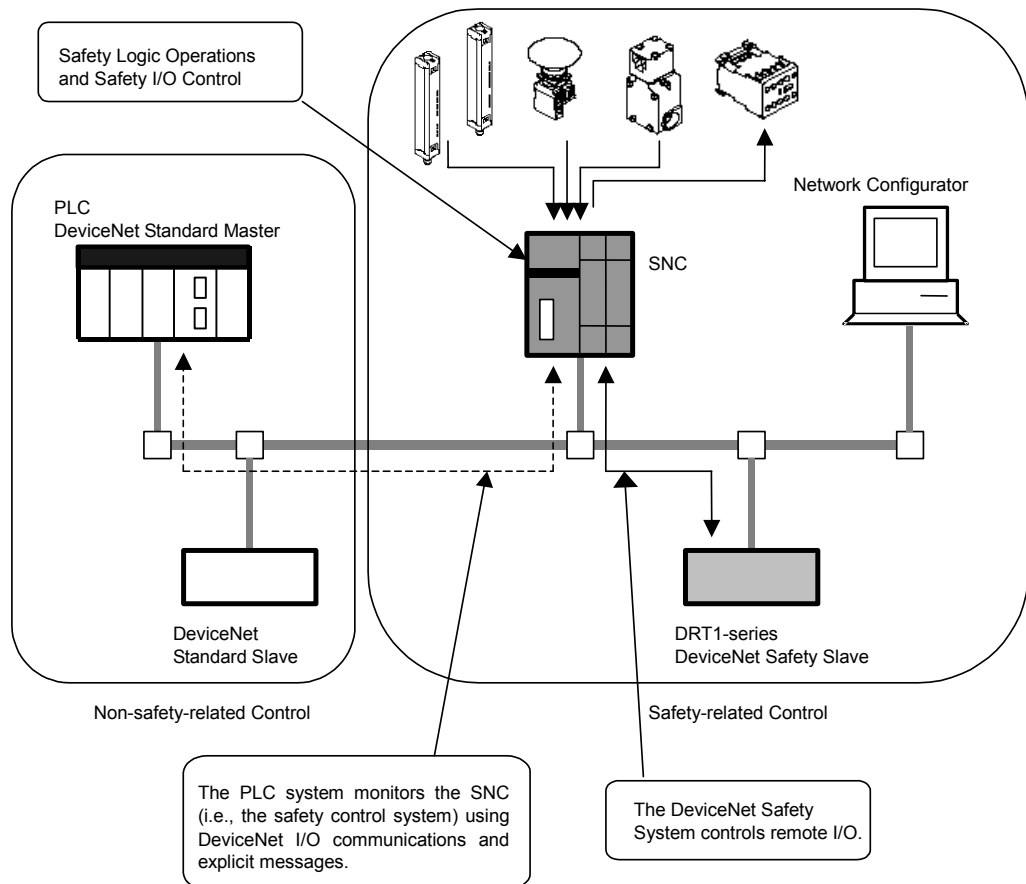
1-2 Safety Network Controller Overview

1-2-1 About the NE1A-series Safety Network Controller

The NE1A-series Safety Network Controllers provide various functions, such as safety logic operations, safety I/O control, and a DeviceNet Safety protocol. The NE1A-series Controllers allow the user to construct a safety control/network system that meets the requirements for Safety Integrity Level (SIL) 3 according to IEC 61508 (*Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems*) and the requirements for Safety Category 4 according to EN 954-1.

In the example system shown below, the safety control system implemented with the NE1A-series Controller and the monitoring system implemented with the standard PLC are realized on the same network.

- As a Safety Logic Controller, the NE1A-series Controller executes safety logic operations and controls local I/O.
- As a Safety Master, the NE1A-series Controller controls the remote I/O of Safety Slaves.
- As a Standard Slave, the NE1A-series Controller communicates with the Standard Master.



1-2-2 NE1A Series Features

Safety Logic Operations

In addition to basic logic functions, such as AND and OR, the NE1A-series Controllers also support application function blocks, such as Emergency Stop Pushbutton Monitoring and Safety Gate Monitoring, that enable various safety applications.

User-defined Function Blocks

Previously prepared logic functions and function blocks can be combined to create a user-defined function block using the Network Configurator version 1.5□ or higher. This can be used to standardize functions that are used frequently to facilitate reusing them. Passwords can also be used to protect the programming inside the function blocks by making them “black boxes.”

Local Safety I/O

- A total of 24 local safety I/O points are supported by NE1A-SCPU01(-V1): 16 input terminals and 8 output terminals.
- A total of 48 local safety I/O points are supported by NE1A-SCPU02: 40 input terminals and 8 output terminals.
- Faults in external wiring can be detected.
- Dual Channel Mode can be set for pairs of related local inputs. When Dual Channel Mode is set, the NE1A-series Controller can evaluate the input data patterns and the time discrepancy between input signals.
- Dual Channel Mode can be set for pairs of related local outputs. When Dual Channel Mode is set, the NE1A-series Controller can evaluate the output data patterns.

DeviceNet Safety Communications

- As a Safety Master, the NE1A-series Controller can perform safety I/O communications with up to 16 connections using up to 16 bytes per connection.
- As a Safety Slave, the NE1A-series Controller can perform safety I/O communications with a maximum of four connections using up to 16 bytes per connection.

DeviceNet Communications

As a Standard Slave, the NE1A-series Controller can perform standard I/O communications with one Standard Master for up to two connections using up to 16 bytes per connection.

Standalone Controller Mode

The NE1A-series Controller can be used as a Standalone Controller by disabling the NE1A-series Controller's DeviceNet communications.

Configuration with a Graphical Tool

- A graphical tool is provided for both network configuration and logic programming. It enables easy configuration and programming.
- A Logic Editor can be activated from the Network Configurator.
- Configuration data can be downloaded and uploaded, and devices can be monitored online via DeviceNet, USB, or the peripheral interface of an OMRON PLC.

System Startup and Error Recovery Support

- Error information can be checked by using the error history or the indicators on the front of the NE1A-series Controller.
- The NE1A-series Controller's internal status information can be monitored from a standard PLC by allocating the information in the Standard Master. In the same way, the information can be monitored from a safety PLC by allocating the information in the Safety Master.

Access Control with a Password

- NE1A-series Controller configuration data is protected by a password.
- Network configuration files (project files) created with the Network Configurator are also password protected.

- Programs and user-defined function blocks can be password-protected using the Network Configurator version 1.5□ or higher.

1-2-3 Standard Models

Model number	Name	Number of I/O points		
		Safety inputs	Test outputs	Safety outputs
NE1A-SCPU01	Safety Network Controller	16 inputs	4 outputs	8 outputs
NE1A-SCPU01-V1, unit version 1.0	Safety Network Controller	16 inputs	4 outputs	8 outputs
NE1A-SCPU02, unit version 1.0	Safety Network Controller	40 inputs	8 outputs	8 outputs

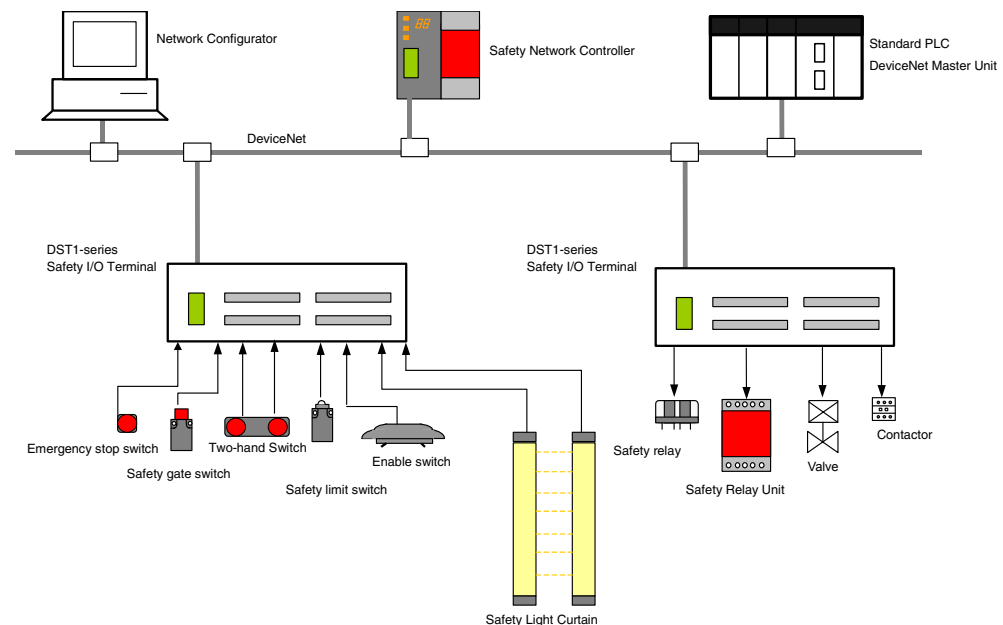
1-3 Safety I/O Terminal Overview

1-3-1 About the DST1-series Safety I/O Terminals

The Safety I/O Terminals support the DeviceNet Safety protocol and provide various functions for the Safety System. The Safety I/O Terminals allow the user to construct a safety control/network system that meets the requirements for Safety Integrity Level (SIL) 3 according to IEC 61508 (*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*) and the requirements for Safety Category 4 according to EN 954-1.

The DST1-series safety I/O data is transmitted through safety I/O communications conforming to the DeviceNet Safety Protocol, and the data processing is performed in the Safety Network Controller.

Also, the status of the safety I/O data can be monitored in a standard PLC in an existing DeviceNet network using standard I/O communications or explicit message communications.



1-3-2 Safety I/O Terminal Features

Safety Inputs

- Semiconductor output devices such as light curtains can be connected as well as contact output devices such as emergency stop switches.
- Faults in external wiring can be detected.
- Input delays (ON delays and OFF delays) can be set.
- Pairs of related local inputs can be set to Dual Channel Mode in order to be compliant with the Category 4 standards.
When Dual Channel Mode is set, the input data patterns and the time discrepancy between input signals can be evaluated.

Test Outputs

- 4 independent test outputs are available to use.
- A disconnected external indicator lamp can be detected. (Can be set for the T3 Terminal only.)
- Test outputs can be used as power supply terminals to devices such as sensors.
- Test outputs can be used as the standard output terminals for monitor outputs.

Safety Outputs

- **Semiconductor Outputs**
 - Pairs of related local outputs can be set to Dual Channel Mode in order to be compliant with the Category 4 standards.
When Dual Channel Mode is set, the output data patterns can be evaluated.
 - The rated output current is 0.5 A max. per output.
- **Relay Outputs**
 - Pairs of related output terminals can be set to Dual Channel Mode in order to be compliant with the Category 4 standards.
When Dual Channel Mode is set, the output data patterns can be evaluated.
 - The rated output current is 2 A max. per output terminal.
 - The safety relays can be replaced.

DeviceNet Safety Communications

As a Safety Slave, the Safety I/O Terminal can perform safety I/O communications with up to four connections.

DeviceNet Communications

As a Standard Slave, the Safety I/O Terminal can perform standard I/O communications with one Standard Master with up to two connections.

System Startup and Error Recovery Support

- Error information can be checked by using the error history or the indicators on the front of the Safety I/O Terminal.
- The Safety I/O Terminal's safety I/O data and internal status information can be monitored from a Standard PLC by allocating the information in the standard Master. In the same way, the information can be monitored from a safety PLC by allocating the information in the Safety Master.

Access Control with a Password

Safety I/O Terminal configuration data is protected by a password.

I/O Connector Connection/Disconnection

- The I/O Connector can be connected and disconnected.
- The I/O Connector is structured to prevent incorrect connection.

Cage Clamp Wiring

Cables can be wired without terminal screws.

Maintenance Functions

The Safety I/O Terminals are equipped with Maintenance Functions such as a contact operation counter, total ON time monitor, and operating time monitor.

1-3-3 Standard Models

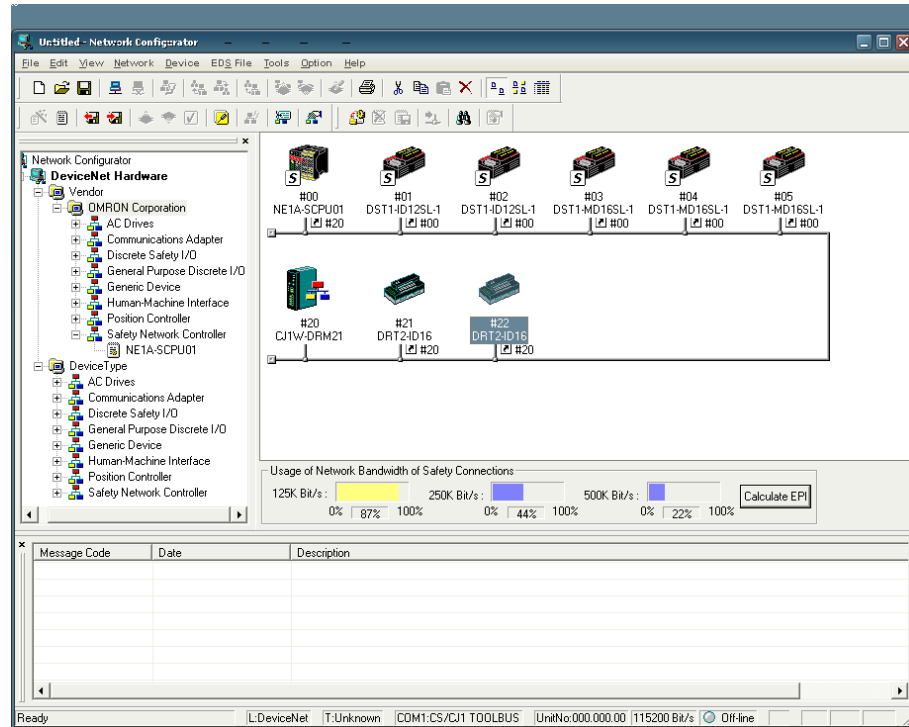
The following table shows the three models of DST1-series Safety I/O Terminals that are available: the Safety Input Terminal, Safety I/O Terminal (Semiconductor Output), and Safety Input/Output Terminal (Relay Output).

Model number	Name	Number of I/O points			
		Safety inputs	Test outputs	Safety outputs	
				Semiconductor outputs	Relay outputs
DST1-ID12SL-1	Safety Input Terminal	12 inputs	4 outputs	—	—
DST1-MD16SL-1	Safety I/O Terminal (Semiconductor Output)	8 inputs	4 outputs	8 outputs	—
DST1-MRD08SL-1	Safety I/O Terminal (Relay Output)	4 inputs	4 outputs	—	4 outputs

1-4 Network Configurator Overview

1-4-1 About the Network Configurator

The WS02-CFSC1-E Network Configurator Support Software is used to configure, set, and manage a DeviceNet Safety network with graphical window operations. The Network Configurator can be used to configure a virtual DeviceNet Safety network (in the Network Configuration Window) and monitor the configuration and parameters of each safety device and standard device.



1-4-2 Network Configurator Features

Compliant with Standard and Safety DeviceNet Networks

The Network Configurator can configure and monitor DeviceNet Safety compliant devices as well as existing standard DeviceNet devices. It can thus support building systems for standard control, safety control, or mixed standard/safety control.

Safety Network Controller Programming

The Network Configurator provides built-in programming tools for the safety logic of the NE1A-series Controller and thus enables building DeviceNet Safety applications using only the Network Configurator.

- Previously prepared function blocks can be incorporated in logic. AND/OR and other logic functions and emergency stop button/safety door/light curtain monitoring, and other previously prepared function blocks can be selected from the function block list and placed in the Workspace to create software connections in the logic of the Network Controller.
- User-defined function blocks can be easily created and reused using the Network Configurator version 1.5□ or higher. New user-defined function blocks can be created. These can be used simply by selecting them from the function block list and placing them in the Workspace. Created user-defined function blocks can be saved to file and installed on another computer to use with the Network Configurator on that computer.
- Editing of user-defined function blocks can be password-protected.

Upward Compatibility with DeviceNet Configurator

All the functions of DeviceNet Configurator are supported. Also, all of the files created by the DeviceNet Configurator can be used as they are.

1-4-3 System Requirements

The following computer specifications are required in order to use the Network Configurator.

Item	Specification
Computer	IBM PC/AT or compatible computer with 300 MHz or faster processor 256 MB RAM min. 40 MB free hard disk space Super VGA (800 x 600) or higher Display CD-ROM drive or DVD drive
OS	Windows® 2000 or Windows® XP
COM Port	One of the following COM Ports is required: <ul style="list-style-type: none">• USB Port: For an online connection via the NE1A-series Controller's USB port (USB 1.1)• DeviceNet Interface Card (3G8E2-DRM21-V1): For an online connection via DeviceNet

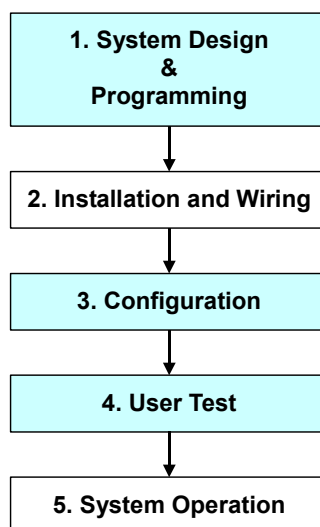
1-4-4 Standard Models

Model number	Name	Component	Compatible computer	OS
WS02-CFSC1-E	Network Configurator	Installation disk (CD-ROM)	IBM PC/AT or compatible	Windows® 2000 or Windows® XP

1-5 Basic System Startup Procedure

This manual introduces the basic steps that are needed to make the safety system operational, with particular focus on the following steps.

- System Design and Programming
- Configuration
- Testing



1-5-1 System Design and Programming

In this step, the optimum safety system is determined by the following procedures:

- (1) Based on the required safety system specifications, select and arrange the safety devices and determine the safety functions to be allocated to each device.
- (2) Configure the network system as a virtual network in the Network Configurator.
 - Register all of the devices. If the system is a mixed safety control and standard control system, register both the safety devices and standard devices.
 - Set the parameters of all the devices.
 - Check the percentage of the network bandwidth being used and review the parameters.
 - Create the program for the NE1A-series Controller.
 - Verify the system reaction time of all the safety chains.

The network bandwidth usage and the system reaction time are affected by several factors, including the network configuration, NE1A-series Controller and Safety I/O Terminal parameter settings, and NE1A-series Controller program, so repeat the steps above to determine a system configuration which meets the users' requirements.

Please refer to the following sections for the operating instructions of the Network Configurator.

- Device Registration
Refer to *3-4 Creating a Virtual Network*.
- Editing Device Parameters
Refer to *3-7 Device Parameters and Properties*.
Refer to *Section 4 Editing Safety I/O Terminal Parameters*.
Refer to *Section 5 Editing Safety Network Controller Parameters*.
- Checking the Usage Rate of Network Bandwidth
Refer to *2-2 Allocating Network Bandwidth Usage and Calculating the Best EPI*.
- Calculating the Reaction Time
Refer to *2-3 Calculating and Verifying the Maximum Reaction Time*.

IMPORTANT: Allocate a unique safety network number to each safety network or safety subnetwork.

1-5-2 Installation and Wiring

In this step, install and wire each device as shown below:

- Install all of the devices and set node addresses and baud rates.
- Connect to I/O devices.
- Wire the power supplies.
- Wire the DeviceNet.
- Wire the USB.

Please refer to the following related manuals for details:

Item	Manual name	Cat. No.
DeviceNet installation	DeviceNet Operation Manual	W267
NE1A-series Controller installation	DeviceNet Safety Network Controller Operation Manual	Z906
DeviceNet Safety I/O Terminal installation	DeviceNet Safety I/O Terminal Operation Manual	Z904
Installation of other devices	Operation manual for each device	–

WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before connecting a device to the network, clear the previous configuration data.



WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before connecting a device to the network, set the appropriate node address and baud rate.



1-5-3 Configuration

In this step, transfer the parameters for each device created by the Network Configurator to the actual device to make the system operative.

Use the Network Configurator to perform the following operations:

(1) Download

The parameters set in the Network Configurator's virtual network are transferred to the actual device and stored in each device.

(2) Verification

Verify the safety device settings.

The user confirms that the parameters and safety signatures stored in each device are correct.

Please refer to the following sections for the operating instructions of the Network Configurator.

- Download

Refer to *3-7 Device Parameters and Properties*.

- Verification

Refer to *3-8 Parameter Verification*.

- IMPORTANT:**
- After downloading the device parameters, verify the parameters to confirm that the parameters and the safety signature saved in the devices are correct.
 - When selecting Open Only in the Open Type setting for the safety connection, check that the Safety Master and Safety Slave are correctly configured.

1-5-4 User Test

In this step, the user himself confirms the program operation and performs functional tests.

Always perform the user test, because it is the user's responsibility to verify the system operation. The user test verifies the correctness of all parameters downloaded to each safety device, as well as each device's safety signature. To demonstrate that all parameters and safety signatures are correct after completing the user test, perform a Configuration Lock operation on all of the safety devices.

Refer to *3-9 Configuration Lock* for details on performing a Configuration Lock from the Network Configurator.

WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before operating the system, perform user testing to confirm that the configuration data of all the devices is correct and that they are operating correctly.



- IMPORTANT:**
- After configuring all the devices, user testing must be performed to check if the configuration data and device operation of each device are correct. User testing is performed to verify the safety signature for each device.
 - The configuration must be locked after the user testing has completed.

Section 2

Constructing a Safety Network

2-1	Applications	46
2-1-1	Establishing a New Safety Network	46
2-1-2	Changing an Established Safety Network	49
2-2	Allocating Network Bandwidth Usage and Calculating the Best EPI	53
2-2-1	Checking the Network Bandwidth Used for Safety I/O Communications	53
2-2-2	Allocating Network Bandwidth Usage Rates and Calculating Best EPI	55
2-2-3	Example of EPI Calculations	58
2-3	Calculating and Verifying the Maximum Reaction Time	61
2-3-1	Concept of Reaction Time	61
2-3-2	Calculating the Maximum Reaction Time	62
2-3-3	Verifying the Maximum Reaction Time	66

2-1 Applications

This section describes how to construct a DeviceNet Safety Network in the following two cases.

- (1) Establishing a new Safety Network
- (2) Changing an established Safety Network

2-1-1 Establishing a New Safety Network

This section describes the procedure for establishing a system by designing a new Safety Network using the Network Configurator and then downloading the parameters to the network devices.

System Design and Programming

1. Starting the Network Configurator

Start the Network Configurator.

Refer to 3-1-1 *Starting and Exiting the Network Configurator*.

2. Creating the Virtual Network

Create the virtual network by adding a device from the Hardware List. If the user is to specify the network number, set the network number as well.

Refer to 3-4 *Creating a Virtual Network*.

3. Editing and Programming Device Parameters

Set the parameters of the DST1-series I/O Terminals configured in the virtual network.

Refer to *Section 4 Editing Safety I/O Terminal Parameters* and to the *DST1 Series I/O Terminal Operation Manual (Z904)*.

Set the parameters of the NE1A-series Controller configured in the virtual network.

Refer to *Section 5 Editing Safety Network Controller Parameters* and to the *Safety Network Controller Operation Manual (Z906)*.

Program the NE1A-series Controller configured in the virtual network.

Refer to *Section 6 Programming the Safety Network Controller* and to the *Safety Network Controller Operation Manual (Z906)*.

4. Verifying the Network Bandwidth to Use

Confirm that the bandwidth used in the safety I/O communications does not exceed the acceptable bandwidth in the network. If exceeded, re-examine the procedure from network configuration in step 2.

Refer to 2-2 *Allocating Network Bandwidth and Calculating the Best EPI*.

5. Calculating and Verifying the Maximum Reaction Time

Calculate the maximum reaction time of all the safety chains and check if the requirement specifications are met. If the requirement specifications are not met, re-examine the procedure from network configuration in step 2.

Refer to 2-3 *Calculating and Verifying the Maximum Reaction Time*.

6. Saving the Network Configuration File

Save the network configuration file with the completed design.

Refer to 3-5-2 *Saving the Network Configuration File*.

7. Exiting the Network Configurator

Exit the Network Configurator.

The following operations are performed by connecting the Network Configurator to the network after the network installation and wiring.

IMPORTANT: Allocate a unique safety network number to each safety network or safety

subnetwork.

Configuration

8. Starting the Network Configurator and Connecting to the Network

Start the Network Configurator and connect it to the network via the USB port on the NE1A-series Controller or a DeviceNet Interface Card.

Refer to 3-3 *Connecting to the Network*.

9. Reading the Network Configuration File

Read the saved network configuration file with the completed design.

Refer to 3-5-3 *Reading the Network Configuration File*.

10. Resetting a Device

When changing the configuration because of user testing results or when downloading the parameters again, it is necessary to clear the previous configuration before downloading the new parameters. Reset the device by setting the reset type to *Return to the out-of-box configuration, and then emulate cycling power*.

Refer to 3-10-2 *Resetting Devices*.

11. Downloading Device Parameters

Download the parameters to all the devices.

Refer to 3-7-3 *Downloading Device Parameters*.

12. Confirming the Downloaded Device Parameters and Safety Signatures

Verify the parameters for all the devices and check if the device parameters and program that the user input have been correctly downloaded and saved in the devices.

Refer to 3-8 *Parameter Verification*.

13. Saving the Network Configuration File

Save the network configuration file in which parameter verification of all the devices has been completed.

Refer to 3-5-2 *Saving the Network Configuration File*.

14. Exiting the Network Configurator

Exit the Network Configurator.

- IMPORTANT:**
- After downloading the device parameters, verify the parameters to confirm that the parameters and the safety signature saved in the devices are correct.
 - When selecting *Open Only* in the Open Type setting for the safety connection, check that the Safety Master and Safety Slave are correctly configured.

User Testing

15. User Testing

The user himself must verify device parameters and operation to confirm that safety system requirement specifications are met.

16. Starting the Network Configurator and Connecting to the Network

Start the Network Configurator and connect it to the network via the USB port on the NE1A-series Controller or a DeviceNet Interface Card.

Refer to 3-3 *Connecting to the Network*.

17. Reading the Network Configuration File

Read the saved network configuration file with parameters that are already verified.

Refer to 3-5-3 *Reading a Network Configuration File*.

18. Configuration Lock

Lock the configuration of all the devices to indicate that they have been verified as well as to prevent parameters from being mistakenly rewritten.

Refer to 3-9-1 *Locking the Device Configuration*.

19. Saving the Network Configuration File

Save the network configuration file of the virtual network in which the configuration is locked.

Refer to 3-5-2 *Saving the Network Configuration File*.

20. Exiting the Network Configurator

Exit the Network Configurator.

⚠ WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before operating the system, perform user testing to confirm that the configuration data of all the devices is correct and that they are operating correctly.



- IMPORTANT:**
- After configuring all the devices, user testing must be performed to check if the configuration data and device operation of each device are correct. User testing is performed to verify the safety signature for each device.
 - The configuration must be locked after the user testing has completed.

Running the System**21. Running the System**

Run the system.

2-1-2 Changing an Established Safety Network

This section describes procedure to change the Safety Network after the system is running.

Changing the System

1. Stopping the System

Turn OFF the power supplies to moving parts, such as motors, and stop the system. Continue supplying power to the network and the NE1A-series Controller.

2. Starting the Network Configurator and Connecting to the Network

Start the Network Configurator and connect it to the network via the USB port on the NE1A-series Controller or a DeviceNet Interface Card.

Refer to 3-1-1 *Starting and Exiting the Network Configurator* and 3-3 *Connecting to the Network*.

3. Uploading the Network Configuration

Upload the network to obtain the current network configuration.

Refer to 3-4 *Creating a Virtual Network*.

4. Unlocking the Configurations

Unlock the configurations of all the devices to enable changing the network configuration.

Refer to 3-9-2 *Unlocking the Device Configuration*.

5. Resetting a Device

Before changing device parameters and node address, clear the configuration of the device. Reset the device by setting the reset type to *Return to the out-of-box configuration, and then emulate cycling power*.

Refer to 3-10-2 *Resetting Devices*.

6. Exiting the Network Configurator

Exit the Network Configurator.

7. Changing the System

Change the network, wiring, and node addresses and add or delete devices according to the specified system changes. Safety devices that are being newly added must be configured in advance.

Refer to 3-10-2 *Resetting Devices*.

WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before connecting a device to the network, clear the previous configuration data.



WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before connecting a device to the network, set the appropriate node address and baud rate.



Note: There is no need to use the saved network configuration file, because the purpose of this procedure is to unlock the device configurations and reset devices to the default configurations.

Redesigning the System

8. Starting the Network Configurator

Start the Network Configurator to redesign the network.

9. Reading the Network Configuration File

Read the saved network configuration file with a locked configuration.

Refer to 3-5-3 *Reading a Network Configuration File*.

10. Changing the Virtual Network

Add or delete the devices and change the node addresses according to specified changes.

Refer to 3-4 *Creating a Virtual Network*.

11. Changing the Device Parameters and Program

Set and change the parameters of the DST1-series I/O Terminals configured in the virtual network according to specified changes.

Refer to *Section 4 Editing Safety I/O Terminal Parameters* and to the *DST1 Series I/O Terminal Operation Manual (Z904)*.

Set and change the parameters of the NE1A-series Controller configured in the virtual network according to specified changes.

Refer to *Section 5 Editing Safety Network Controller Parameters* and to the *Safety Network Controller Operation Manual (Z906)*.

Create and change the program of the NE1A-series Controller configured in the virtual network according to specified changes.

Refer to *Section 6 Programming the Safety Network Controller* and to the *Safety Network Controller Operation Manual (Z906)*.

12. Verifying the Network Bandwidth to Use

Confirm that the bandwidth used in the safety I/O communications does not exceed the acceptable bandwidth in the network. If exceeded, re-examine the specified changes.

Refer to 2-2 *Allocating Network Bandwidth Usage and Calculating the Best EPI*.

13. Recalculating and Verifying the Maximum Reaction Time

Calculate the maximum reaction time of all the safety chains and check if the requirement specifications are met. If the requirement specifications are not met, re-examine the specified changes.

Refer to 2-3 *Calculating and Verifying Maximum Reaction Time*.

14. Saving the Network Configuration File

Save the network configuration file with the completed changes.

Refer to 3-5-2 *Saving the Network Configuration File*.

15. Exiting the Network Configurator

Exit the Network Configurator.

The following operations are performed by connecting the Network Configurator to the network after the actual system changes have been completed.

- IMPORTANT:**
- Allocate a unique network number when establishing a network or subnetwork.
 - If the parameters of a Safety Slave or Standard Slave are changed, the parameter information will not match in the Safety Master or Standard Master in which the Slave is registered. Therefore, a yellow [!] symbol will be displayed next to the slave icon. If this symbol is displayed, check the slave information by opening the Edit Parameter Window of the Master. Allocate a unique network number when establishing a network or subnetwork with

Safety Slaves.

Note: If device parameters with a locked configuration are changed, the color of the key icon will change to yellow.

Re-configuration

16. Starting the Network Configurator and Connecting to the Network

Start the Network Configurator and connect it to the network via the USB port of the NE1A-series Controller or a DeviceNet Interface Card.

Refer to 3-3 *Connecting to the Network*.

17. Reading the Network Configuration File

Read the saved network configuration file with the completed design changes.

Refer to 3-5-3 *Reading a Network Configuration File*.

18. Downloading Device Parameters

Download the parameters to all the devices.

Refer to 3-7-3 *Downloading Device Parameters*.

19. Confirming the Downloaded Device Parameters and Safety Signature

Verify the parameters for all devices with an icon indicating pre-verification and check if the device parameters and program that the user input are correctly downloaded and saved to the devices.

Refer to 3-8 *Parameter Verification*.

20. Saving the Network Configuration File

Save the configuration file for a network in which parameter verifications of all the devices have been completed.

Refer to 3-5-2 *Saving the Network Configuration File*.

21. Exiting the Network Configurator

Exit the Network Configurator.

- IMPORTANT:**
- After downloading the device parameters, verify the parameters to confirm that the parameters and the safety signature saved in the device are correct.
 - When selecting *Open Only* in the Open Type setting for the safety connection, check that the Safety Master and Safety Slave are correctly configured.

- Note:
- In the Network Configuration Pane, the device will be displayed as locked, but the actual device has already been unlocked. Therefore, the parameters can be downloaded.
 - If downloading to a device with a key icon color that has changed to yellow because of parameter changes, the icon must be returned to the state before verification (white [S] symbol).
 - If downloading to a device with a key icon color that has not changed because parameters have not been changed, the icon must be returned to the state indicating that verification has been completed (green [S] symbol).

Additional User Testing

22. User Testing

The user himself must verify device parameters and operation to confirm that the safety system requirement specifications are met.

23. Starting the Network Configurator and Connecting to the Network

Start the Network Configurator and connect it to the network via the USB port

on the NE1A-series Controller or a DeviceNet Interface Card.
Refer to 3-3 *Connecting to the Network*.

24. Reading the Network Configuration File

Read the saved network configuration file with verified parameters.
Refer to 3-5-3 *Reading a Network Configuration File*.

25. Configuration Lock

Lock the configuration of all the devices to indicate that they have been verified as well as to prevent parameters from being mistakenly rewritten.
Refer to 3-9-1 *Locking the Device Configuration*.

26. Saving the Network Configuration File

Save the file of a virtual network with a locked configuration.
Refer to 3-5-2 *Saving the Network Configuration File*.

27. Exiting the Network Configurator

Exit the Network Configurator.

⚠ WARNING

Safety functions may be impaired and serious injury may occasionally occur. Before operating the system, perform user testing to confirm that the configuration data of all the devices is correct and that they are operating correctly.



IMPORTANT:

- After configuring all the devices, user testing must be performed to confirm that the configuration data and operation of each device are correct. User testing is performed to verify the safety signature for each device.
- The configuration must be locked after user testing has been completed.

Restarting the System

28. Running the System

Run the system.

2-2 Allocating Network Bandwidth Usage and Calculating the Best EPI

Almost all of the DeviceNet Safety network bandwidth can be used for safety I/O and standard I/O communications.

Communications may time out, however, if the connection settings exceed the acceptable bandwidth usage for each type of communications.

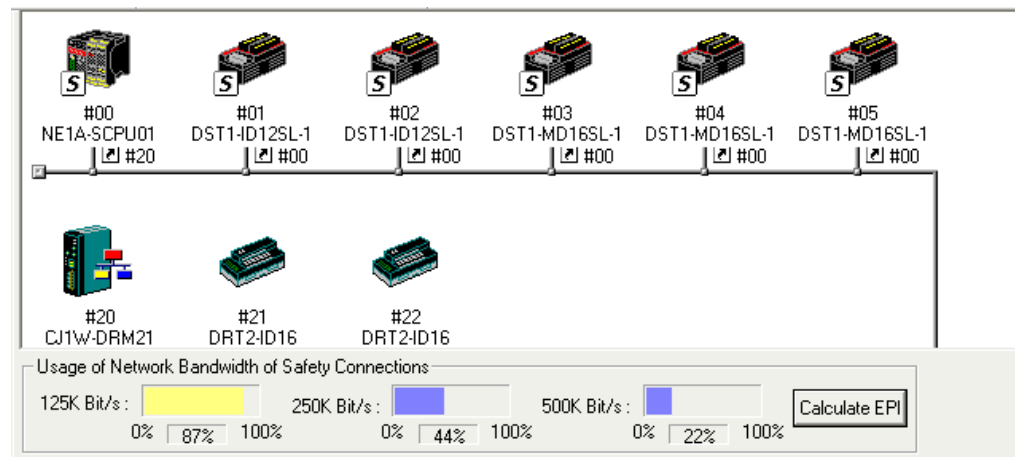
Check the connection settings and, if a setting is found to exceed the acceptable bandwidth usage rate, the setting must be changed to the value outlined in the following table.

• Safety I/O communications	EPI (Expected Packet Interval) setting for safety connections
• Standard I/O communications	Master communications cycle time

The network configuration may need to be changed if the settings exceed the acceptable bandwidth usage rate as a result of securing the required communications performance (i.e., the required network reaction time for safety I/O communications). This section describes how to check the network bandwidth used for safety I/O communications in the designed network, how to calculate the best EPI from the set bandwidth usage rate, and how to re-set the value.

2-2-1 Checking the Network Bandwidth Used for Safety I/O Communications

The actual network bandwidth usage rate for safety I/O communications for the connections set in the virtual network is displayed at the bottom of the Network Configuration Window under *Usage of Network Bandwidth for Safety Connections*. The network bandwidth usage rate is displayed for each baud rate, as shown in the following diagram.



As shown in the diagram, the faster the baud rate, the lower the bandwidth usage rate.

IMPORTANT: Keep 10% or more of the network bandwidth available for establishing connections and for explicit message communications with the Network Configurator, whether using only safety I/O communications or using both safety I/O and standard I/O communications. Even if 10% or more is available, however, safety or standard communications might time out, depending on the Network Configurator operation (e.g., monitoring or other operations that create a load on the network) or if the user application uses explicit message communications. If timeouts occur, reduce the network bandwidth usage rate (i.e., increase the unused bandwidth).

Performing Only Safety I/O Communications

When performing only safety I/O communications, there is no problem if the network bandwidth used for safety I/O communications is approximately 90%.

If the bandwidth exceeds 90%, obtain the best average EPI for all connections by referring to *2-2-2 Allocating Network Bandwidth Usage Rates and Calculating Best EPI* and change the EPI setting for each connection.

Performing Safety I/O Communications and Standard I/O Communications

When both safety I/O communications and standard I/O communications are used on one network, it is necessary to determine the network bandwidth to use for each type of communications. Problems will occur if only the network bandwidth for safety I/O communications is determined, because some network bandwidth is required for standard I/O communications.

Refer to *2-2-2 Allocating Network Bandwidth Usage and Calculating the Best EPI* and enter the network bandwidth used for each type of communications and set the best average EPI for each safety connection and the communications cycle time of the Standard Master.

2-2-2 Allocating Network Bandwidth Usage Rates and Calculating Best EPI

The average EPIs for safety I/O communications and standard I/O communications and the best communications cycle time are calculated by entering the network bandwidth usage rate for each type of communications into the Network Configurator.

Calculate the best average EPIs and the best communications cycle using the following procedure. The network configuration might need to be changed if the required communications characteristics cannot be achieved.

1. Make the required settings for the virtual network on the Network Configurator, including creating programs for the Safety Network Controller.
2. Click the **Calculate EPI** Button at the bottom of the Network Configuration Window. The Calculate EPI Dialog Box will be displayed.
3. Input the network bandwidth used in safety I/O communications and the bandwidth used in standard I/O communications.
 - If using only safety I/O communications:
Input the network bandwidth used by the safety connections as 90% or less and input 0% for the network bandwidth used by standard connections.
 - If using both safety and standard I/O communications:
Input the total network bandwidth used for safety and standard connections as 90% or less, e.g., 50% for safety connections and 40% for standard connections.

Safety and standard I/O communications will use the bandwidth based on the rates specified here.
4. Click the **Calculate** Button.
5. The best average EPI of all the connections in the safety I/O communications and the optimum Master communications cycle time in the standard I/O communications will be displayed for each baud rate.

Safety Connections	
Network Bandwidth	
Use Rate :	40 %
Best Average of EPI	
125K Bit/s :	30 ms
250K Bit/s :	15 ms
500K Bit/s :	8 ms
Update device configuration...	

Standard Connections	
Network Bandwidth	
Use Rate :	30 %
Best Average of Cycle Time	
125K Bit/s :	6 ms
250K Bit/s :	3 ms
500K Bit/s :	2 ms

Calculate Close

6. Perform the following trial calculation.
 - When using safety I/O communications only
Increase the network bandwidth for safety connections to 90%. If the desired best EPI for each safety connection cannot be calculated, try increasing the EPI for connections that need faster speeds (EPI settings, step 9 as described later).
 - When using a mixture of safety and standard I/O communications:
Try changing the network bandwidth usage rate and calculating the EPI, as described below.

- Increase the usage rate for safety connections to shorten the EPI for safety I/O communications and lengthen the communications cycle time for standard I/O communications.
- Conversely, increase the usage rate for standard communications to shorten the cycle time for standard I/O communications and increase the EPI for safety I/O communications.

7. Check the Safety Network Controller cycle time.

Next, check that the cycle times calculated in the previous steps are longer than the Safety Network Controller cycle time. If they are shorter, the Safety Network Controller cycle time will be the minimum that can be set for the EPI. The Safety Network Controller cycle time can be checked offline after creating the program, under *Cycle Time* on the Mode/Cycle Time Tab in the Edit Device Parameters Dialog Box. Refer to 5-5 *Setting the Operating Modes and Confirmation the Cycle Time*.

IMPORTANT: The minimum possible EPI setting is larger value of either the Safety Network Controller cycle time or the Safety Slave cycle time (fixed at 6 ms). The minimum possible EPI will be affected, therefore, if the Safety Network Controller cycle time is longer than 6 ms.

8. Reconsider the network configuration itself if you have performed the test calculation as outlined above and either of the following occur, i.e.,

- the desired best average EPI for each safety connection and the best communications cycle time for the Standard Master cannot be calculated, or
- the Safety Network Controller cycle time is longer than the best average EPI.

Consider adjusting the following aspects of the network configuration.

- Reducing the number of nodes or I/O points.
- Splitting the network
 - If using both safety and standard I/O communications, split the network into a DeviceNet Safety network and a standard DeviceNet network.
 - If using only safety I/O communications, split the network into two DeviceNet Safety networks.

9. Change the EPI settings for each safety connection and the Standard Master communications cycle time setting to suit the desired baud rate.

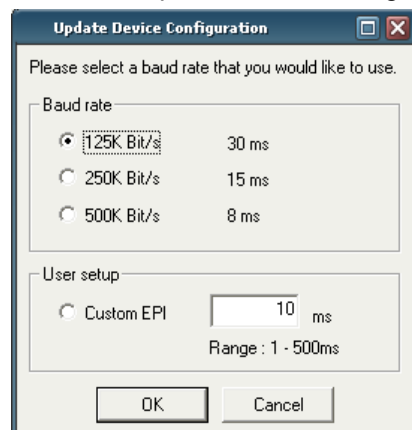
● **Changing the EPI Settings for Each Safety I/O Connection**

The best average EPI calculated is the best average of all safety connections. The following method is used for setting the calculated EPI as the EPI in the parameters for all safety connections.

- Method for batch setting the best EPI to devices

1. Click the **Update Device Configuration** Button.

The Update Device Configuration Dialog Box will be displayed.



2. Select the baud rate to be used and click the **OK** Button.

The calculated best average EPI value will be batch set as the EPI in the safety connection parameters for all devices.

3. If required, adjust the EPI settings for the whole network, making the EPI smaller for those connections that need a faster response time (e.g., for safety curtain connections) and making the EPI larger for those connections that do not need a fast response (e.g., for door switches not used in hazardous areas). Refer to the reaction time listed in the EPI field to check what the reaction time will be for each safety connection EPI setting.

Note: Set the EPI for each safety connection longer than Safety Network Controller cycle time. If the EPI is shorter, errors will occur when the safety connection parameters are downloaded and the download will fail.

- **Changing Standard Master Communications Cycle Times**

The value calculated as the best average cycle time is the best communications cycle time for the Standard Master.

Set the calculated value as the Standard Master communications cycle time.

10. Reconfirm the bandwidth usage rate.

If the EPI settings in the safety connection parameters or the Standard Master communications cycle time setting has been changed based on the calculation results, check that the network bandwidth usage when safety connections are used, displayed at the bottom of the Network Configuration Window, is less than the value input in the Calculate EPI Dialog Box.

It is particularly important to check the bandwidth usage rate if the best average EPI has been adjusted for each connection rather than applied as a batch setting.

Note: The EPI is set in 1-ms units, so the network bandwidth usage rate may be smaller than the input value if the calculation result is input directly.

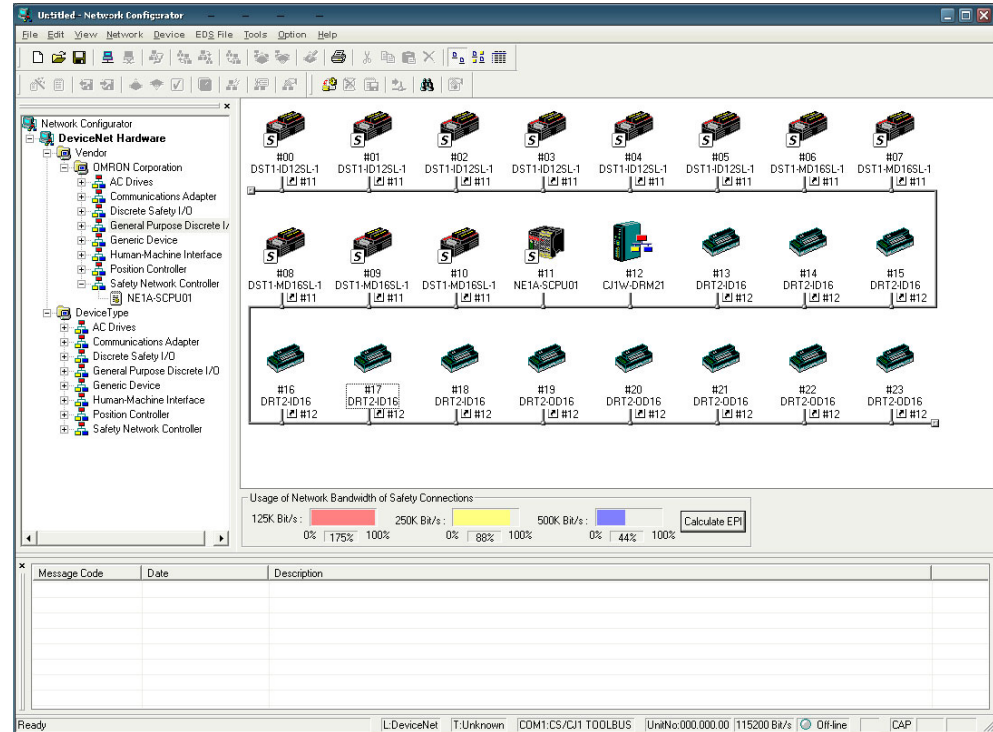
11. Perform a test to ensure that there are no problems with the set values.

2-2-3 Example of EPI Calculations

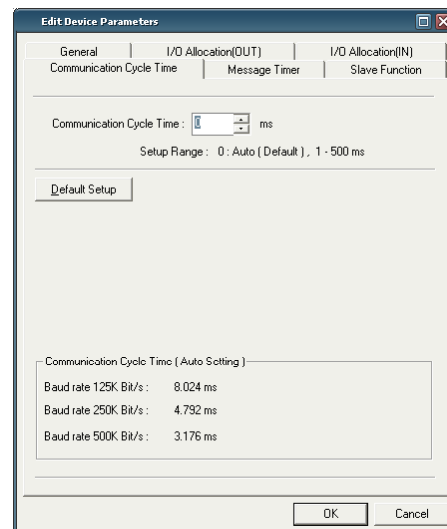
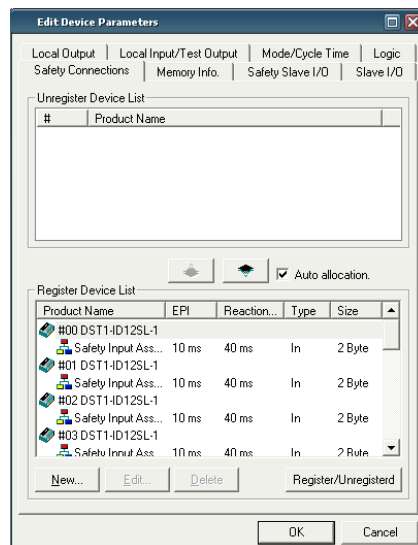
The following network configuration is used for an example of calculating the EPI.

Conditions

The baud rate is 500 Kbit/s.



- Safety I/O Communications**
 Example: The NE1A-series Controller sets safety connections between six DST1-ID12SL-1 Input Terminals and five DST1-MD16SL-1 I/O Terminals. The default set values are used for all the safety connections, and the EPI is 10 ms.
- Standard I/O Communications**
 Example: The CJ1W-DRM21 sets the standard connections between six DRT2-ID16 Input Terminals and five DRT2-OD16 Output Terminals. The default set values are used, and the communications cycle of the CJ1W-DRM21 is automatically set but it attempts to operate at a cycle time of about 3.2 ms.



Calculations

Here, we allocate 70% network bandwidth usage rate to safety connections and 20% to standard connections.

Click the **Calculate** Button and from the calculation results, you can see the EPI for the safety connections can be set to 7 ms and the communications cycle of the Standard Master can be set to 6 ms.

Safety Connections	
Network Bandwidth	
Use Rate :	70 %
Best Average of EPI	
125K Bit/s :	25 ms
250K Bit/s :	13 ms
500K Bit/s :	7 ms
Update device configuration...	

Standard Connections	
Network Bandwidth	
Use Rate :	20 %
Best Average of Cycle Time	
125K Bit/s :	22 ms
250K Bit/s :	11 ms
500K Bit/s :	6 ms

Calculate Close

Checking the Safety Network Controller Cycle Time

If, for example, the Safety Network Controller cycle time was 6 ms, it is shorter than the calculation result of 7 ms which means the result can be set as the EPI.

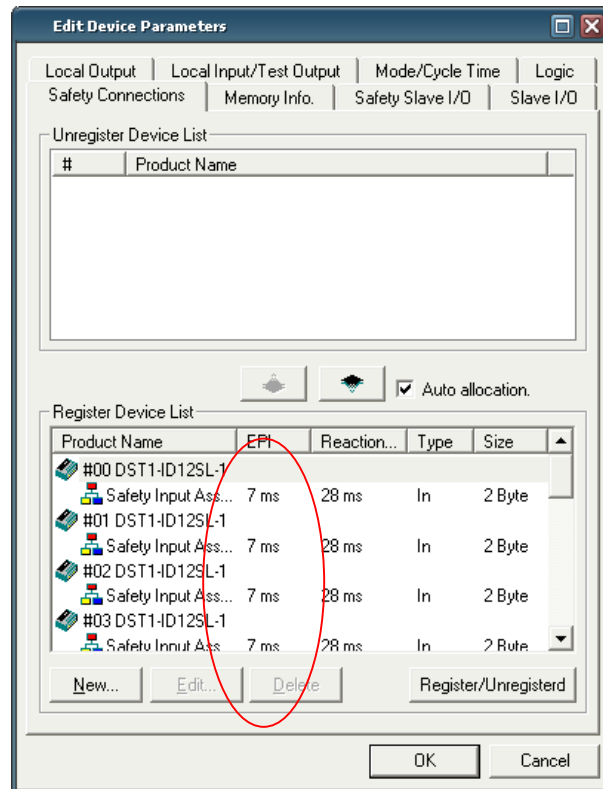
Changing Settings

Changing the EPI Settings for Each Safety I/O Connection

Set the EPI of all safety connections set in the NE1A-series Controller to 7 ms according to the calculation results.

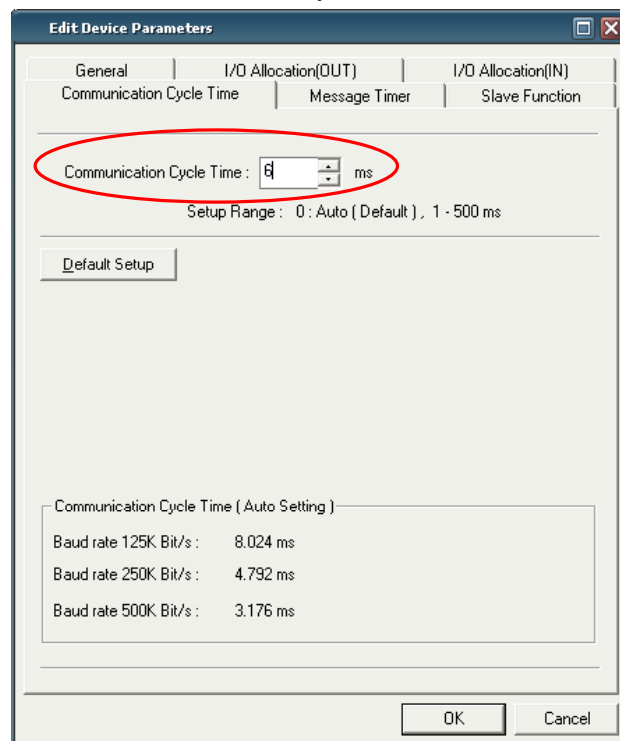
Click the **Update Device Configuration** Button to batch set the calculation result of 7 ms as the EPI for all safety connections by selecting the baud rate to be used.

Refer to 2-2-2 *Allocating Network Bandwidth Usage and Calculating the Best EPI*.



Changing Standard Master Communications Cycle Time Settings

Set the communications cycle of the CJ1W-DRM21 to 6 ms.



2-3 Calculating and Verifying the Maximum Reaction Time

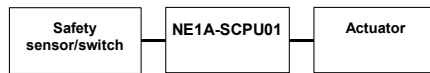
The last step in designing the network is calculating the reaction time of safety chains. The user must check that the reaction time in all the safety chains meets the requirement specifications.

2-3-1 Concept of Reaction Time

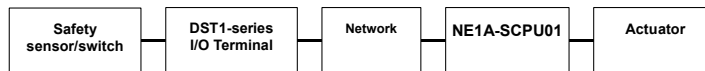
Reaction time is the worst down time among the running devices considering faults and failures in safety chains. The safety distance is calculated from reaction time.

The reaction time is calculated for each safety chain. The typical combinations of safety chains are as follows:

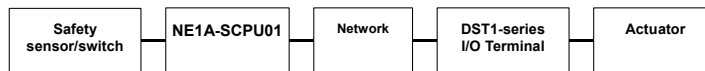
(1) NE1A-series Controller Standalone System



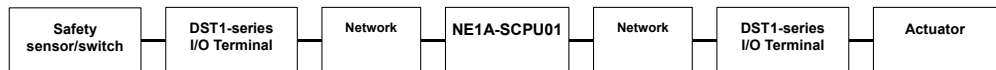
(2) Remote Input – NE1A-series Controller Output



(3) NE1A-series Controller Input – Remote Output



(4) Remote Input – Remote Output



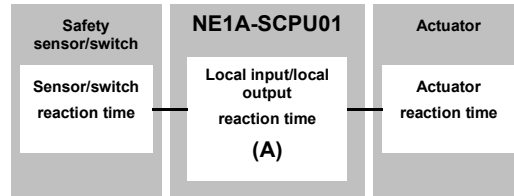
Note: Even if a fault or failure occurs in a safety chain, the output shutoff time is ensured as the maximum reaction time.

2-3-2 Calculating the Maximum Reaction Time

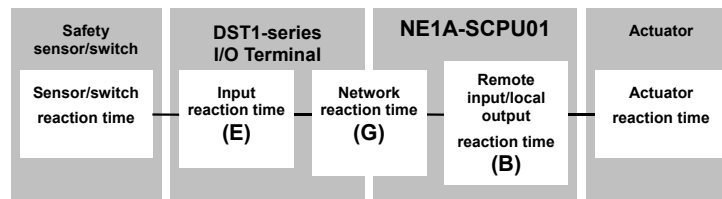
Reaction Time Components

Reaction time components are displayed for each safety chain.

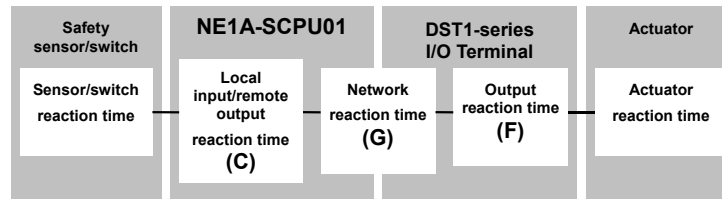
(1) NE1A-series Controller Standalone System



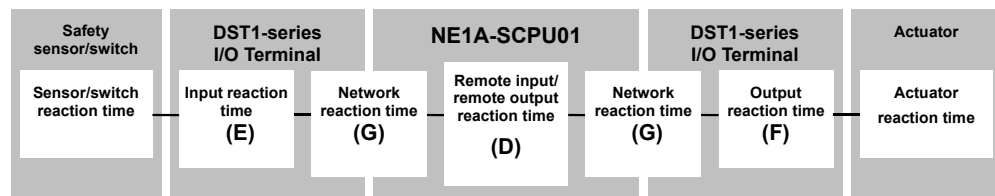
(2) Remote Input – NE1A-series Controller Output



(3) NE1A-series Controller Input – Remote Output



(4) Remote Input – Remote Output



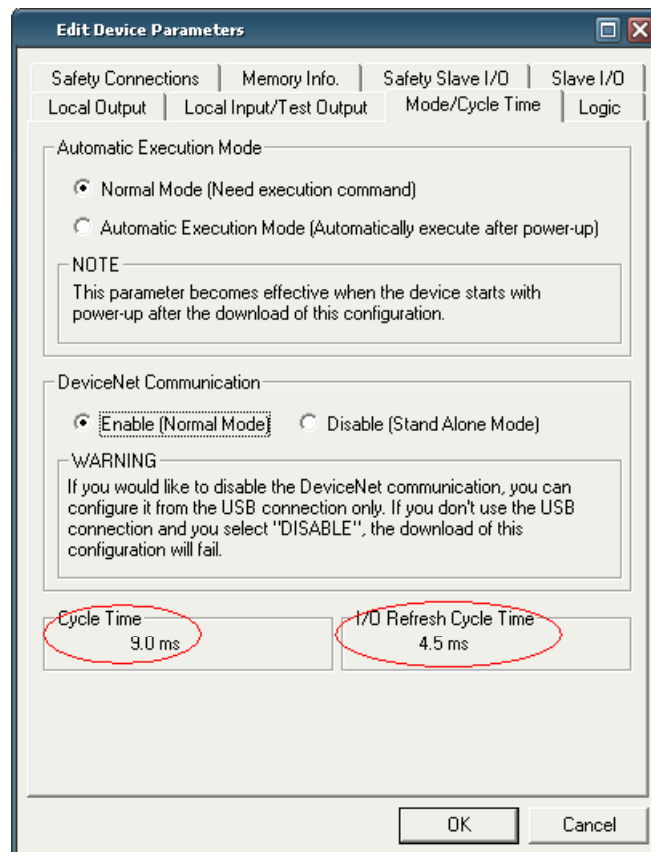
Maximum Reaction Time Formula

	Item	Formula
A	Local input/local output reaction time of the NE1A-series Controller (ms)	ON/OFF delay + I/O refresh cycle + NE1A-series Controller cycle time $\times 2 + 2.5$
B	Remote input/local output reaction time of the NE1A-series Controller (ms)	NE1A-series Controller cycle time + 2.5
C	Local input/remote output reaction time of the NE1A-series Controller (ms)	ON/OFF delay + I/O refresh cycle + NE1A-series Controller cycle time $\times 2$
D	Remote input/remote output reaction time of the NE1A-series Controller (ms)	NE1A-series Controller cycle time
E	Input reaction time of the DST1-series I/O Terminal (ms)	ON/OFF delay + 16.2
F	Output reaction time of DST1-series I/O Terminal (ms)	6.2 + Relay reaction time (DST1-MRD08SL-1 only)
G	Network reaction time (ms)	Use the Network Configurator calculation result.

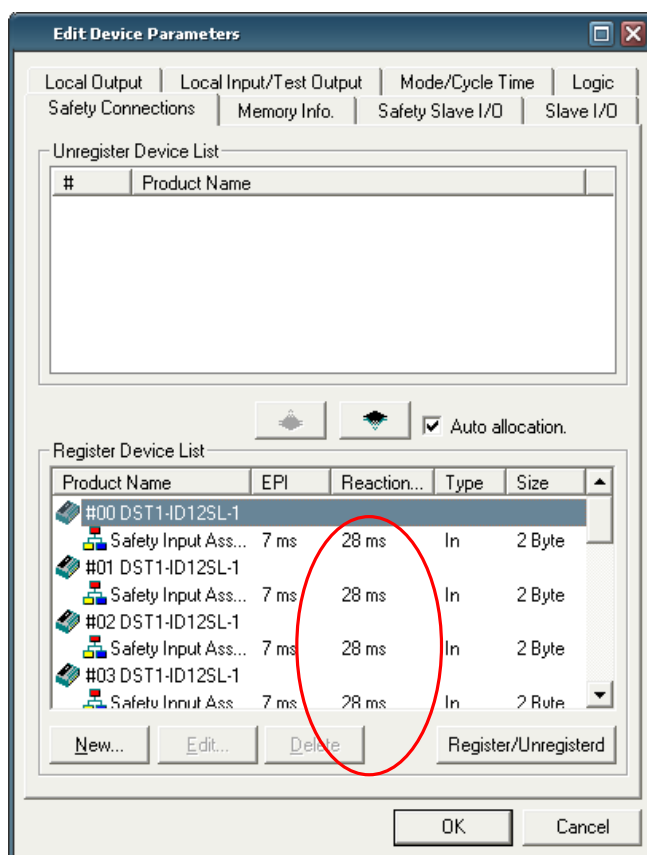
IMPORTANT: In the SNC program, add the time for the NE1A-series Controller cycle time to the reaction time of the safety chain when the output from a function block is fed back to the input side of the function block.

Check the NE1A-series Controller cycle time, I/O refresh cycle time, and network reaction time in the Network Configurator.

Check the NE1A-series Controller cycle time and I/O refresh time in **Mode/Cycle Time** Tab of the Edit Device Parameters Window.

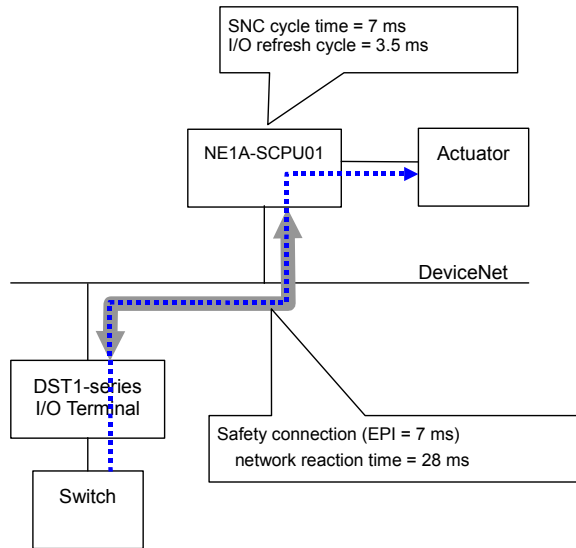


Check the network reaction time in the **Safety Connection** Tab of the Edit Device Parameters Window.



Example of Maximum Reaction Time Calculation

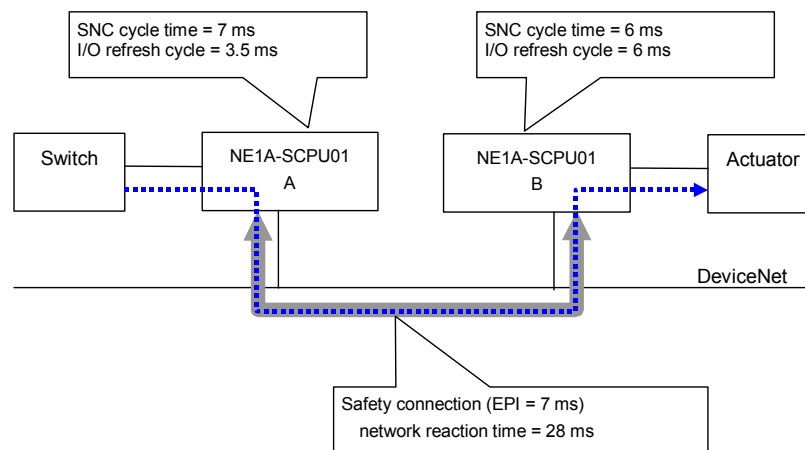
Example 1: Remote Input – NE1A-series Controller Output



Maximum reaction time (ms)

$$\begin{aligned}
 &= \text{Switch reaction time} \\
 &\quad + \text{DST1-series I/O Terminal input reaction time} \\
 &\quad + \text{Network reaction time} \\
 &\quad + \text{NE1A-series Controller remote input/local output reaction time} \\
 &\quad + \text{Actuator reaction time} \\
 &= \text{Switch reaction time} \\
 &\quad + \text{ON/OFF delay (DST1-series I/O Terminal)} + 16.2 \\
 &\quad + 28 \\
 &\quad + 7 + 2.5 \\
 &\quad + \text{Actuator reaction time} \\
 &= \underline{\underline{53.7 + \text{ON/OFF delay} + \text{Switch reaction time} + \text{Actuator reaction time}}}
 \end{aligned}$$

Example 2: Local Input – Remote Output



Maximum reaction time (ms)

$$\begin{aligned}
 &= \text{Switch reaction time} \\
 &\quad + \text{NE1A-series Controller-A local input/remote output reaction time} \\
 &\quad + \text{Network reaction time} \\
 &\quad + \text{NE1A-series Controller-B remote input/local output reaction time} \\
 &\quad + \text{Actuator reaction time} \\
 &= \text{Switch reaction time} \\
 &\quad + \text{ON/OFF delay (NE1A-series Controller)} + 3.5 + 7 \times 2 \\
 &\quad + 28 \\
 &\quad + 6 + 2.5 \\
 &\quad + \text{Actuator reaction time} \\
 &= \underline{\underline{54.0 + \text{ON/OFF delay} + \text{Switch reaction time} + \text{Actuator reaction time}}}
 \end{aligned}$$

2-3-3 Verifying the Maximum Reaction Time

Check that the calculated maximum reaction time meets the required specifications in all safety chains. If the reaction time exceeds the required specifications, re-examine the network design, taking into consideration the following points for the maximum reaction time to meet the requirement specifications:

- Shortening the EPI will shorten the network reaction time. Shortening the EPI, however, narrows the network bandwidth that can be used for other connections.
- The NE1A-series Controller cycle time is automatically calculated based on the program size, the number of connections, etc. It is also possible to use different NE1A-series Controller Controllers for safety chains that require a high-speed reaction time and other safety chains.

Section 3

Basic Operation of the Network Configurator

3-1	Network Configurator Startup and Main Window	69
3-1-1	Starting and Exiting the Network Configurator.....	69
3-1-2	Checking the Version.....	70
3-1-3	Main Window	71
3-2	Menu List.....	72
3-2-1	File Menu	72
3-2-2	Edit Menu.....	72
3-2-3	View Menu	72
3-2-4	Network Menu.....	73
3-2-5	Device Menu	73
3-2-6	EDS File Menu.....	74
3-2-7	Tools Menu	74
3-2-8	Option Menu	74
3-2-9	Help Menu.....	74
3-2-10	Main Window Display Modes.....	74
3-3	Connecting to the Network	77
3-3-1	Network Connection via USB Port.....	77
3-3-2	Network Connection via DeviceNet Interface Card	77
3-4	Creating a Virtual Network	79
3-4-1	Creating a New Virtual Network.....	79
3-4-2	Network Numbers	79
3-4-3	Adding Devices	82
3-4-4	Deleting Devices	84
3-4-5	Changing the Node Address.....	84
3-4-6	Changing Device Comments	84
3-5	Saving and Reading Network Configuration Files.....	85
3-5-1	Password Protection of the Network Configuration File	85
3-5-2	Saving the Network Configuration File	86
3-5-3	Reading a Network Configuration File	86
3-5-4	Protect Mode.....	87
3-6	Device Password Protection	88
3-6-1	Setting a Device Password	88
3-6-2	Forgotten Device Passwords.....	89
3-7	Device Parameters and Properties	90
3-7-1	Editing Device Parameters	90
3-7-2	Uploading Device Parameters	90
3-7-3	Downloading Device Parameters	91
3-7-4	Device Properties.....	93

3-8	Parameter Verification	96
3-8-1	Device Parameter Verification	96
3-9	Configuration Lock	99
3-9-1	Locking the Device Configuration	99
3-9-2	Unlocking the Device Configuration	100
3-10	Device Reset and Status Change	101
3-10-1	Reset Types	101
3-10-2	Resetting Devices	102
3-10-3	Reset Types and Device Status	102
3-10-4	Changing Device Status	103

3-1 Network Configurator Startup and Main Window

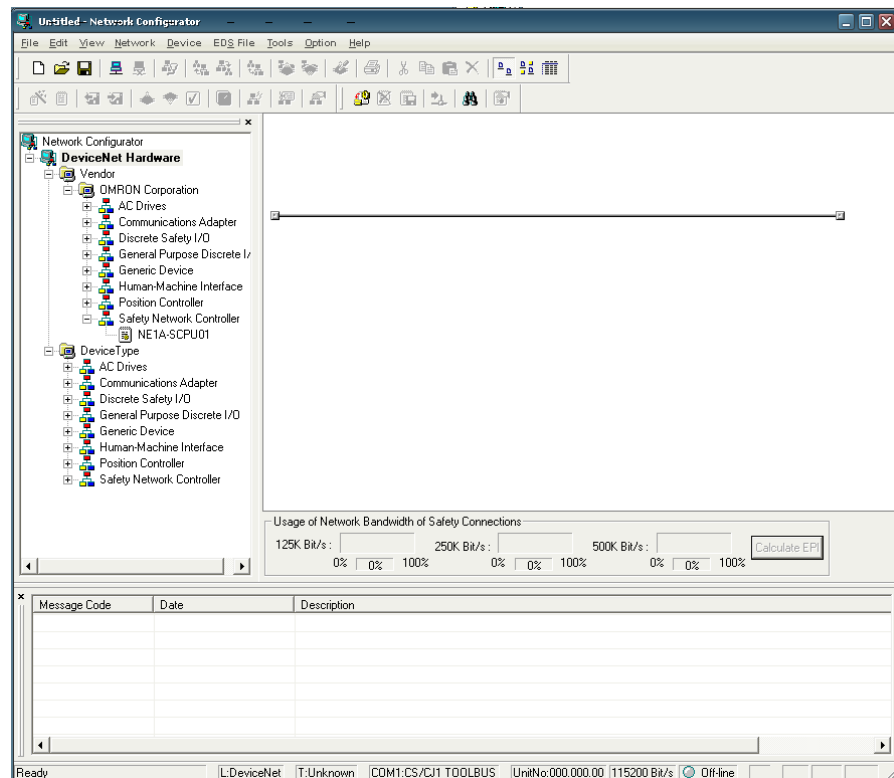
This section describes methods for starting and exiting the Network Configurator, describes how to check the Network Configurator version and describes the Main Window.

3-1-1 Starting and Exiting the Network Configurator

Starting

Select **Program -OMRON Network Configurator for DeviceNet Safety - Network Configurator** from the Windows Start Menu (when using the default program folder name).

The Network Configurator will start, and the following window will be displayed.



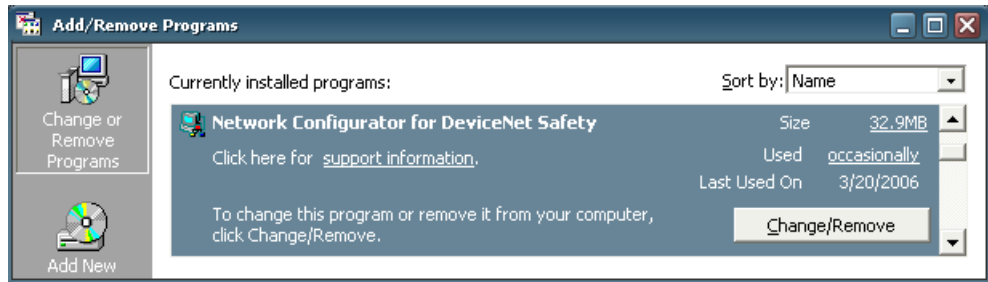
Exiting

Select **File -Exit** in the Main Window.
The Network Configurator will close.

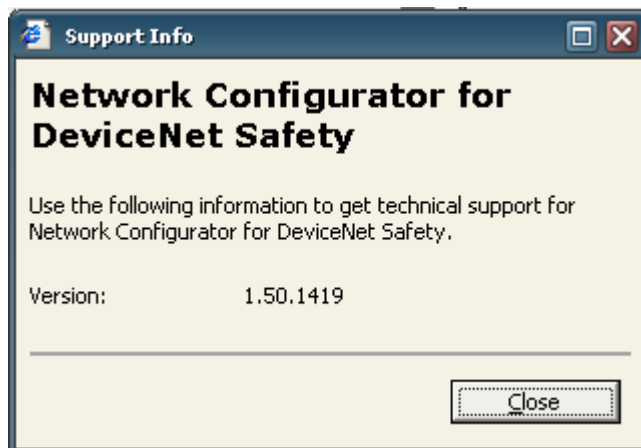
3-1-2 Checking the Version

The procedure to check the Network Configurator version is as follows:

1. Select the **Control Panel** from the Windows Start Menu.
2. Select the **Add or Remove Programs** (Windows XP) or **Add/Remove Programs** (Windows 2000).
3. Select the **Network Configurator for DeviceNet Safety** from the installed program list, and then refer to the support information by following each display.



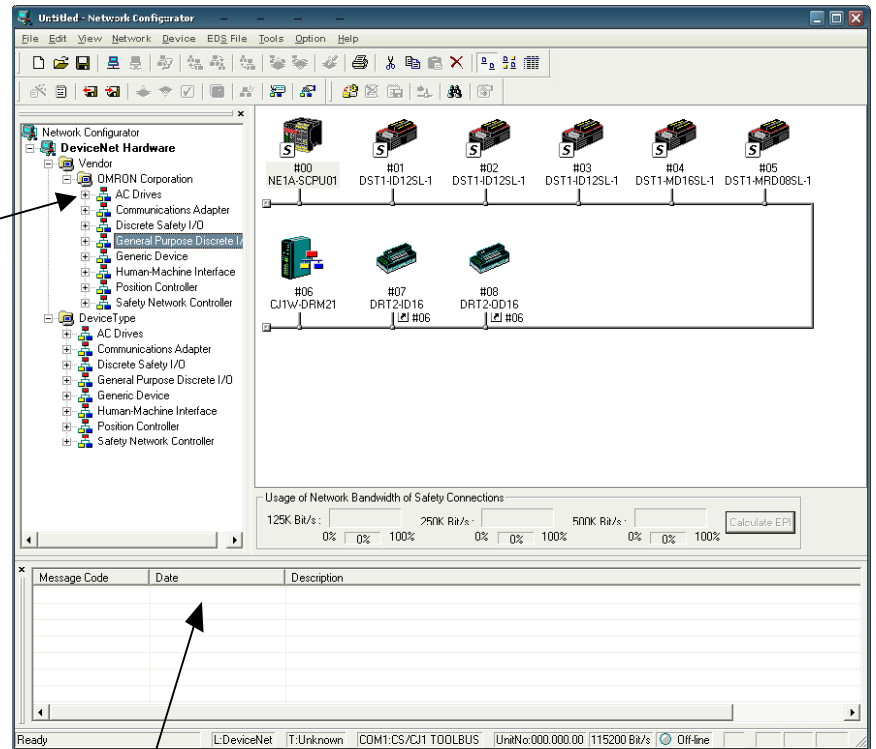
4. The version will be displayed as support information.



3-1-3 Main Window

The Main Window consists of the Hardware List, the Network Configuration Pane, and the Message Pane.

Hardware List:
Displays the devices that can be added to the network.



Message Report Pane:
Display information such as communications errors.

3-2 Menu List

This section describes the function of each menu command of the Network Configurator.

"Online" is the state in which the Network Configurator is connected to the network.

"Offline" is the state in which the Network Configurator is disconnected from the network.

3-2-1 File Menu

O: Supported ×: Not supported

Submenu		Description	Offline	Online
New		Creates a new network configuration.	O	O
Open		Opens an existing network configuration file.	O	O
Save		Saves the current network configuration to a file.	O	O
Save As		Names and saves the current network configuration.	O	O
External Data	Export	Exports in CSV format a file with the contents displayed in the detailed display.	O	O
	Import	Imports a network configuration file created in DeviceNet Configurator version 1 or version 2.	O	O
Change Password		Changes the password of the network configuration file.	O	O
Report		Creates a report on a specified device.	O	O
Print		Prints the device parameters and I/O comment list.	O	O
Setup Printer		Sets up the printer.	O	O
Exit		Exits the Configurator.	O	O

3-2-2 Edit Menu

Submenu	Description	Offline	Online
Cut	Deletes selected devices and copies them to the clipboard.	O	O
Copy	Copies selected devices to the clipboard.	O	O
Paste	Pastes a device on the clipboard to the cursor position.	O	O
Delete	Deletes selected devices.	O	O
Select All	Selects all the devices.	O	O
Clear Message Report	Clears a message in the Message Pane.	O	O

3-2-3 View Menu

Submenu	Description	Offline	Online
Toolbar	Displays or hides the toolbar.	O	O
Status Bar	Displays or hides the status bar.	O	O
Message Report	Displays or hides the Message Pane.	O	O
Large Icons	Switches to network display.	O	O
Large Icons - Maintenance Mode	Displays or hides maintenance information.	O	O
Display Mode 1	Switches to the detailed display mode 1, which displays the configuration based on the master device.	O	O
Display Mode 2	Switches to the detailed display mode 2, which displays the configuration based on the slave devices.	O	O
Hardware List	Displays or hides the Hardware List.	O	O

3-2-4 Network Menu

Submenu		Description	Offline	Online
Connect		Connects the Network Configurator to the network.	O	x
Disconnect		Disconnects the Network Configurator from the network.	x	O
Change Connect Network Port		Changes the destination network port.	x	O
Move Network		Switches the network to connect.	x	O
Wireless Network	Move to Upper Network	Displays the network one layer above the current network in the wireless networks.	x	O
	Move to Lower Network	Displays the network one layer below the current network in the wireless networks.	x	O
Upload		Uploads all the device parameters in the network to the Network Configurator.	x	O
Download		Downloads all the device parameters in the Network Configurator to the devices in the network.	x	O
Verify Structure		Verifies the current network configuration in the Network Configurator with the actual network configuration of the destination online connection.	x	O
Update Maintenance Information		Updates the maintenance information of each device to the latest information.	x	O
Update Device Status		Updates the status information for each device to the most recently updated information.	x	O
Check Connection		Checks the consistency of all the connections.	O	O
Edit All Connections		Makes batch settings for all connections in the system.	O	O
Property		Displays the network properties. The network name and safety network number can be set. This function can also get network numbers from actual networks. This function is enabled only when on online.	O	O

3-2-5 Device Menu

Submenu		Description	Offline	Online
Parameter	Wizard	Configures the device parameters in a wizard format. This function is not supported by all devices.	O	O
	Edit	Edits the device parameters.	O	O
	Read	Reads the parameters from the device parameter file.	O	O
	Save As	Saves the device parameters to a file.	O	O
	Upload	Uploads the device parameters from a device in the network.	x	O
	Download	Downloads the device parameters to a device in the network.	x	O
	Verify	Verifies the device and the device parameters in the network.	x	O
	Lock	Locks the configuration of a device in the network.	x	O
	Unlock	Unlocks the locked configuration of a device in the network.	x	O
Monitor		Monitors the parameters and status of a device in the network. Not all devices support this function.	x	O
Reset		Resets a device in the network.	x	O
Change Mode		Changes the status of a device in the network. Not all devices support this function.	x	O
Change Password		Changes the password of a device in the network.	x	O
Maintenance Information		Displays the maintenance information of a device in the network. This function is enabled only for devices that support it.	x	O
Register to Another Device		Registers a device to another device.	O	O
External Data	Export	Exports I/O comments or device parameters to another file format. Not all devices support this function.	O	O
	Import	Imports a device parameter file created with DeviceNet Configurator (version 1 or version 2). Not all devices support this function.	O	O
Change Node Address		Changes a device node address.	O	O
Change Device Comment		Changes a device name.	O	O
Change Device		Converts configuration data for the NE1A-SCPU01 to configuration data for the NE1A-SCPU01-V1 or E1A-SCPU02.	O	O
Edit I/O Comment		Edits the I/O comment.	O	O
Property		Displays the properties of a device.	O	O

Note: The Device Menu and Edit Menu can be partially displayed by right-clicking in the Network Configuration Pane.

3-2-6 EDS File Menu

Submenu	Description	Offline	Online
Install	Installs an EDS file and adds a device to the Hardware List.	○	○
Create	Creates a new EDS file and adds a device to the Hardware List.	○	○
Delete	Deletes a device from the Hardware List. The installed EDS file is also deleted.	○	○
Save As	Names and saves the EDS file of a device on the Hardware List.	○	○
Find	Searches for a specified EDS file from the Hardware List.	○	○
Add to Network	Adds a device on the Hardware List to the virtual network.	○	○
Property	Displays the properties of an EDS file.	○	○

Note: The EDS File Menu can be displayed by right-clicking in the Hardware List Window.

3-2-7 Tools Menu

Submenu	Description	Offline	Online
Setup Parameters	Sets parameters by using explicit message communications.	×	○
Setup Node Address/Baud Rate	Sets the node address and baud rate of a device in the network.	×	○

3-2-8 Option Menu

Submenu	Description	Offline	Online
Select Interface	Selects an interface for the Network Configurator to use for the network connection.	○	×
Edit Configuration File	Edits various configuration files.	○	○
Setup Monitor Refresh Timer	Sets the monitor refresh timer values (monitoring cycles in device monitoring).	○	○
Install Extend Module	Installs an Expansion Module.	○	○
Install Interface Module	Installs an Expansion Module.	○	×
Parameter Auto Update when Configuration Changed	If this option is selected, the slave I/O size registered in the Master will also be updated automatically when a slave I/O size is changed. The default is OFF (do not update). Under normal conditions, leave this option OFF.	○	○
Update Device Status automatically, when it was connected on Network	When an online connection is made, device status information can be acquired and the display can be updated.	○	×

3-2-9 Help Menu

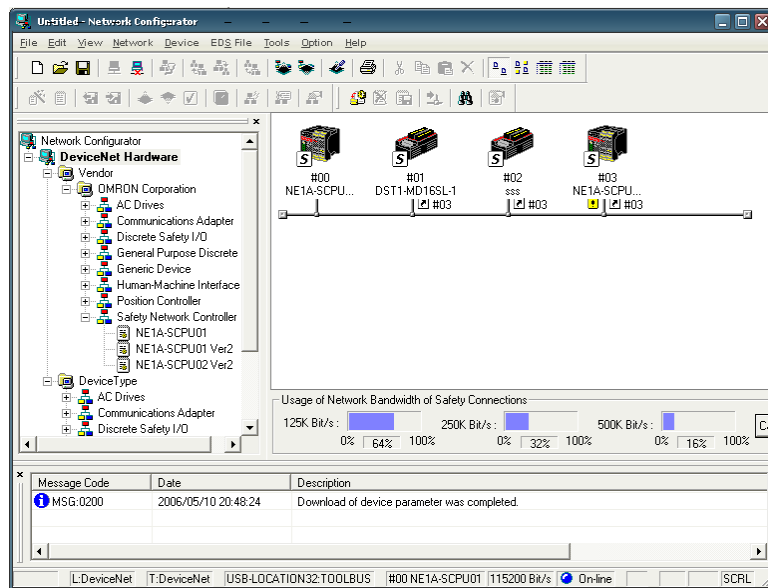
Submenu	Description	Offline	Online
Topic	Searches the help topics.	○	○
About	Displays the version information of the Network Configurator.	○	○

3-2-10 Main Window Display Modes

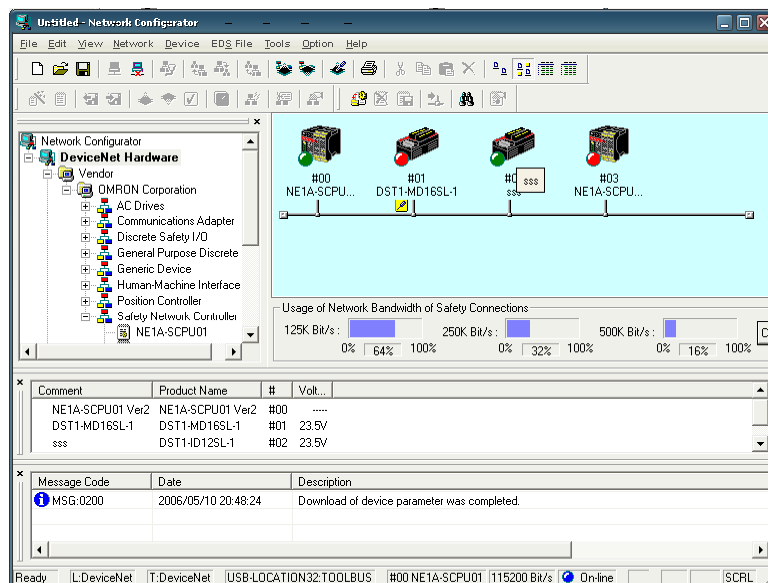
The Main Window display can be changed. Any of the following display modes can be selected: Communications Mode, Maintenance Mode, Detailed Display 1, or Detailed Display 2.

Communications Mode

This is the communications display window. A device list, node addresses, and device names are displayed.



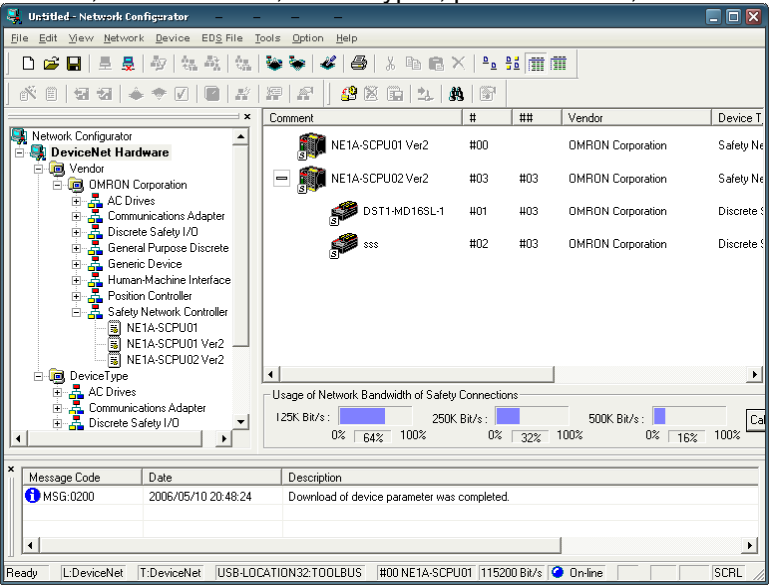
Maintenance Mode



In this mode, in addition to the information displayed in Communications Mode, the devices required for maintenance can be checked at a glance and device status can be displayed at the same time.

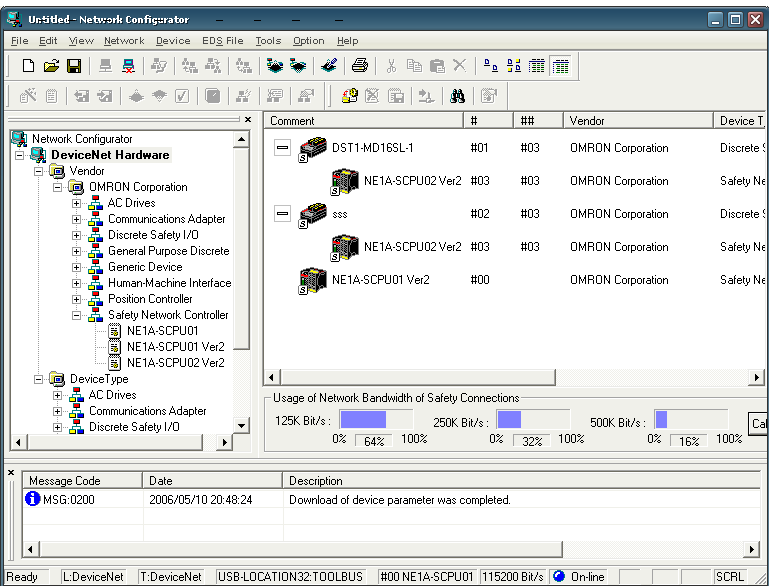
Detailed Display 1 (Based on Master Devices)

The following items are displayed in list format in this mode: Comments added to devices, device names, node addresses, device node addresses registered to master devices, header names, device types, product names, and revisions.



Detailed Display 2 (Based on Slave Devices)

The following items are displayed in list format in this mode: Comments attached to devices, device names, MAC IDs, device MAC IDs registered to slave devices, header names, device types, product names, and revisions.



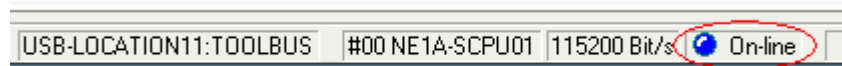
3-3 Connecting to the Network

The Network Configurator must be connected to the network to perform operations that are valid only when online, such as obtaining the network configuration from an actual network or downloading the configured device parameters to actual devices. This section describes the procedure for connecting to the network via the USB port on the NE1A-series Controller and a DeviceNet Interface Card installed in a computer. Refer to the Appendix for other network connection procedures.

3-3-1 Network Connection via USB Port

1. Turn ON the power supply to the NE1A-series Controller and connect it to a USB port on the computer.
2. Select **Option - Select Interface - NE1A USB Port** followed by the desired mode from the menu bar.
3. Select **Network - Connect** from the menu bar.

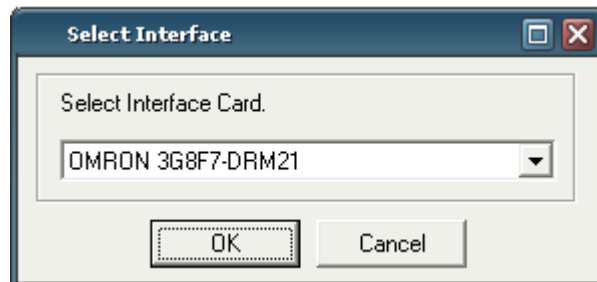
If an online connection is made normally, *On-line* will be displayed in the status bar at the bottom of the window.



3-3-2 Network Connection via DeviceNet Interface Card

1. Select **Option - Select Interface - DeviceNet I/F**.
2. Select **Network - Connect**.

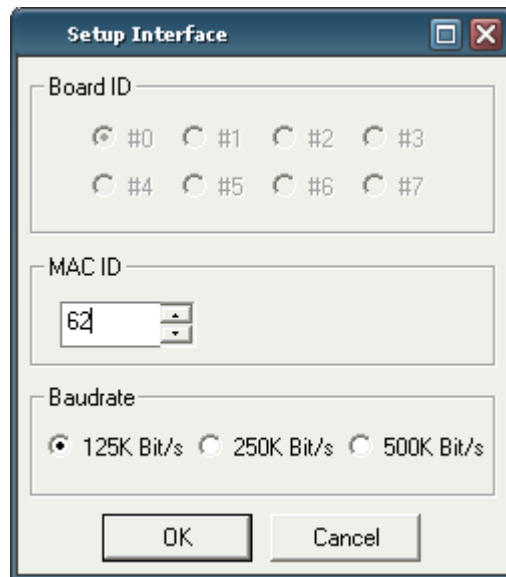
The Select Interface Dialog Box will be displayed.



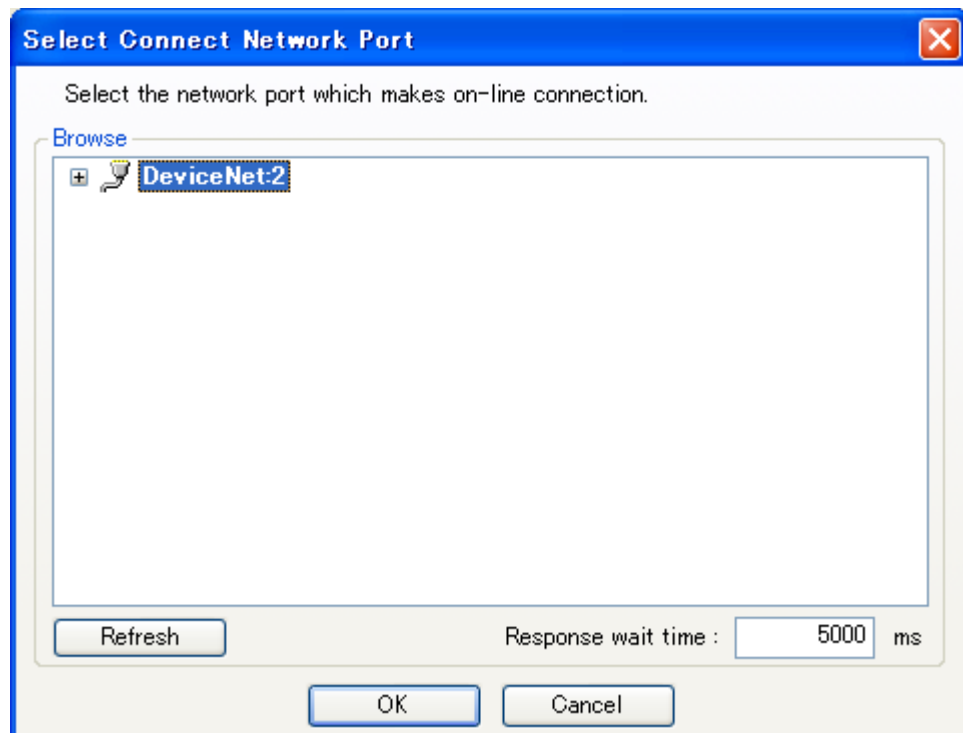
3. Select the interface card, and click the **OK** Button.

The Setup Interface Dialog Box will be displayed.

This window varies depending on the type of interface card. In this example, a DeviceNet PCMCIA Card (3G8E2-DRM21-V1) is used. If you use another interface card, refer to the operation manual for the card.



4. Set the MAC ID (node address) and baud rate, and click the **OK** Button.
The Select Connect Network Port Dialog Box will be displayed.



In the first network connection, a network search is performed automatically with this dialog box displayed. Wait until the search has been performed for all addresses. After the search, the networks that can be connected will be displayed. Automatic searching for networks will not be performed the second time or after.

5. Select the network to connect to, and click the **OK** Button.
If is online connection is made normally, *On-line* will be displayed in the status bar at the bottom of the window.

3-4 Creating a Virtual Network

To set device parameters and to program the NE1A-series Controller, create a virtual network in the Network Configurator, set the device parameters in the virtual network, and then download them the parameters to the actual devices.
This section describes how to create a virtual network.

3-4-1 Creating a New Virtual Network

When the Network Configurator is started, a new virtual network can be created. Only one virtual network can be edited simultaneously. Use one of the following methods to create another network.

- (1) Select **File - New** from the menu bar.
- (2) Click the **New** Button on the toolbar.

Note: When a new virtual network is created, the virtual network information that was displayed until then will be deleted. If the previous virtual network information is required, save the data before creating a new virtual network.

3-4-2 Network Numbers

The network number is defined under *CIP Safety*. CIP networks can be configured in multiple domains. Network numbers are used in combination with node addresses to specify unique devices and confirm communicating nodes in this kind of multi-network configuration. This value is called a TUNID (Target Unique Node Identifier) and is stored in the non-volatile memory of each device.

Setting TUNIDs

The TUNID is automatically set when parameters are first downloaded from the Network Configurator to a device in out-of-the-box configuration. (See note.)

Note: “Out-of-the-box configuration” indicates the status when a reset-type device is returned to its default status and restarted.

Users do not normally need to be aware of the existence of network numbers because they can visually identify a device on the Network Configurator.
The default network number is automatically generated based on the date and time the Network Configurator created the network configuration, but it can also be specified by the user.

Cases Where the User Needs to Specify Network Numbers

The automatically generated network numbers will be sufficient when the Network Configurator is used to set all the devices on the network. In the following cases, however, the user must set a different network number for each network.

- (1) When multiple Network Configurators are used to set individual devices:
When more than one Network Configurator is used to make settings on the same network, the same network number must be set for each device.
- (2) When more than one type of setting software is used:
When setting software other than Network Configurator is used because devices made by other manufacturers are being used, specify the same network number with each type of setting software.

Precautions When Downloading to Existing Networks

The following precautions must be heeded because parameters cannot be downloaded to devices if the new automatically generated TUNID to be transmitted is different from the TUNID in the device memory.

Always use one of the four methods listed below when downloading parameters to a device that has already had parameters downloaded to it.

If the download is executed using a different method, the download will fail because the transmitted TUNID and the TUNID in the device memory are different. A “Different TUNID” error message will appear in the error history.

Method 1: Download the parameters using the previously created network configuration file.

Method 2: Download the parameters based on the configuration obtained from a network upload.

Method 3: If using a newly created network configuration file, get the network number from the actual network (a function of Network Configurator version 1.50 or higher; see note). Make the virtual network number in Network Configurator the same as the actual network number and then download the parameters.

Note: Use the following procedure to get the network number.

1. Select **Network – Property** or right-click the Network Configuration Window and select **Property**. Click the **Get from the actual network** Button in the Network Number Area in the Network Property Dialog Box.
2. The network number of the real number that you want to download will be read to the personal computer.
3. Click the **OK** Button and update the network number. Then re-execute the download.

Method 4: If using a device that has been used in another location, reset the device to out-of-the-box configuration (see note) and download using methods 1, 2, or 3.

Note: Select **Device – Reset** or click the right mouse button and select **Reset** to display the Reset Device Dialog Box. Set the reset type to **Return to the out-of-box configuration, and then emulate cycling power** and click the **OK** Button.

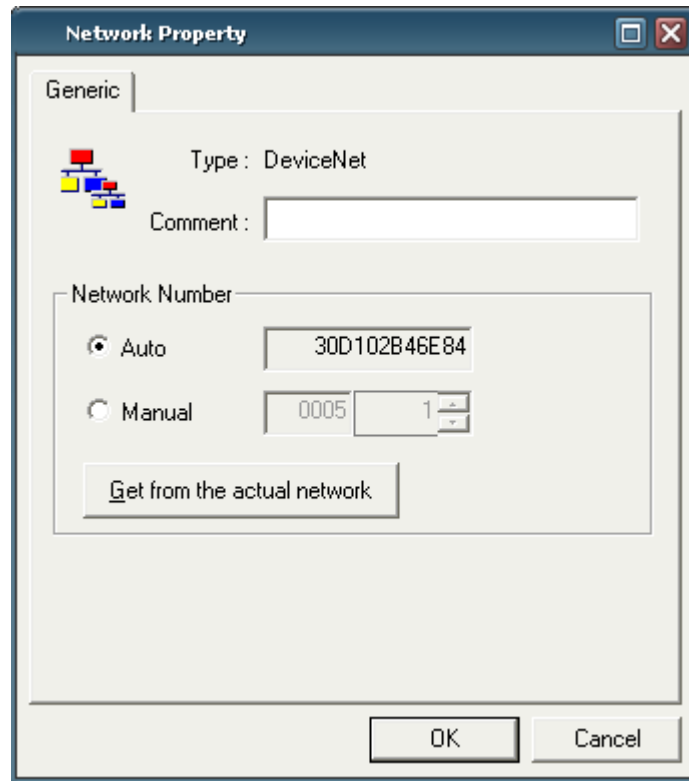
Generally, method 1 should be used, i.e., save the master network configuration file and use it to make any network configuration or parameter changes. Then download parameters using that master file.

When connecting a new device to the network, use method 4 and reset the device to initial status before downloading.

Note: When the parameters are downloaded to the devices, the network number is transferred with the parameters as the UNID and saved in the devices. Therefore, when using a device whose parameters have already been downloaded to another domain, set the reset type to *Return to the out-of-box configuration, and then emulate cycling power* and perform a reset to clear the UNID.

Use the following procedure to set the network number.

- (1) Select **Network - Property** from the menu bar.
- (2) In the Network Number Field, select the *Manual* Option and enter the value.



IMPORTANT: Always allocate a unique network number when a network or subnetwork is established.

If the network number is not set correctly, a connection may be opened to a different device. A different network number must be set for each network domain, and the same network number must be set for all the devices on the same domain.

If the network number is set by the user, click the **Get from the actual network** Button in the Network Number Field on the Network Property Dialog Box to check the network number set for the target actual network. The network number set to the target network will be read and displayed in the *Manual* Field.

3-4-3 Adding Devices

There are three ways to add a device to the virtual network.

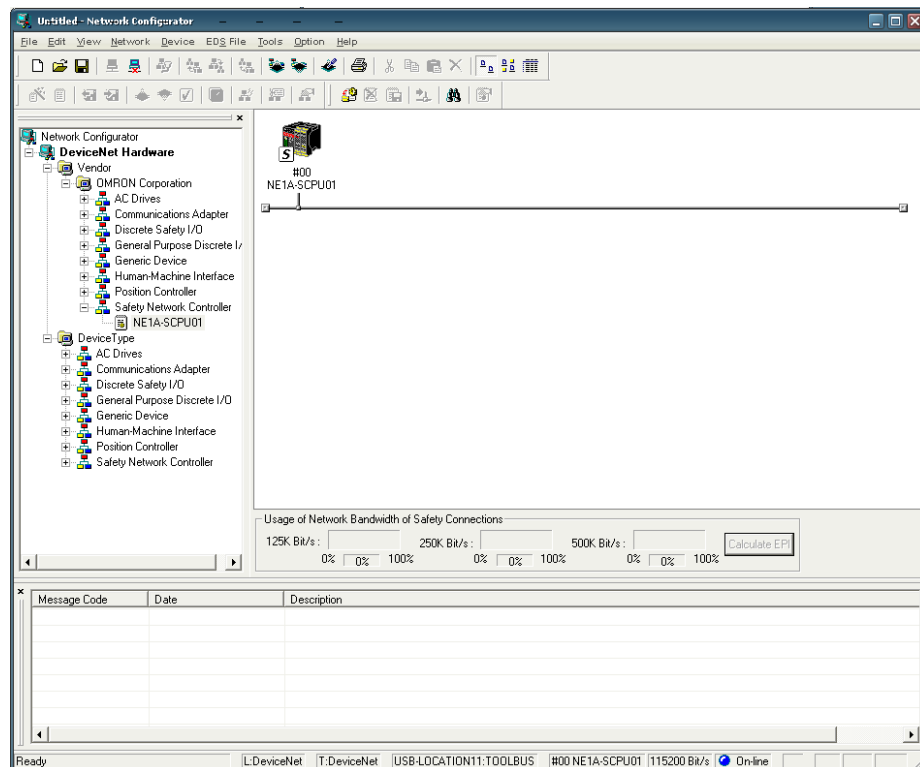
- (1) Add from the Hardware List.
- (2) Upload the network configuration from the actual network.
- (3) Select **EDS File – Add to Network** from the menu.

Adding Devices from the Hardware List

There are two ways to add a device to the virtual network from the Hardware List.

- (1) Double-click the selected device in the Hardware List.
- (2) Select the device from the Hardware List and drag it to the Network Configuration Pane.

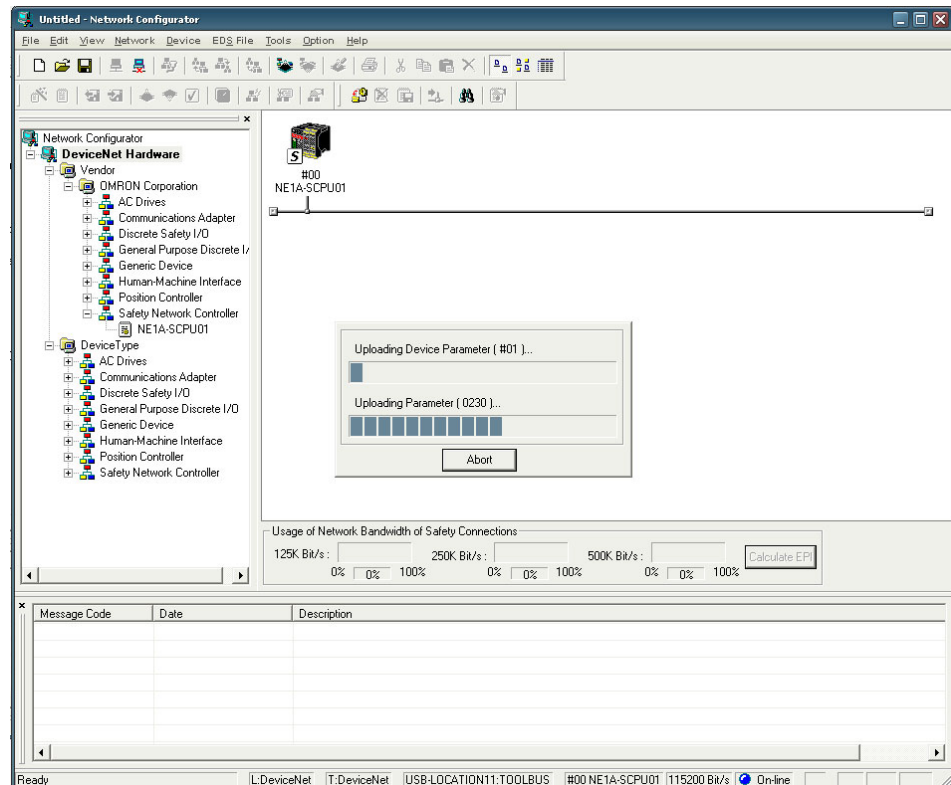
When a device has been registered, it will be displayed as follows:



Uploading the Network Configuration from the Actual Network (Network Upload)

The network configuration can be read from the actual network and to create the same configuration in the virtual network. Connect the Network Configurator to the network, and then upload the network configuration using any of the following methods.

- (1) Select **Network - Upload** from the menu bar.
- (2) Click **Upload from Network** on the toolbar. Uploading will start, and the detected devices will be displayed sequentially.
- (3) Right-click without selecting any device in the Network Configuration Pane and select **Upload**.



If there is another device that must be added after the upload has completed, add the device following the same procedure as in *Adding Devices from the Hardware List*, above.

IMPORTANT: When the CS/CJ-series DeviceNet Unit exists in the network, disable the master functionality of the CS/CJ-series DeviceNet Unit, and then do the upload. If the master functionality is enabled, uploading the device parameters may fail.

- Note:**
- When uploading the network configuration from a network, it can be uploaded as the configuration or the current network or as a new network.
 - When data is uploaded as a new network, the virtual network information that was displayed until will be deleted. If the previous virtual network information is required, save the data before the uploading the network.
 - When a network in which devices already have a set network number is uploaded, the value that is already set in the devices will be used for the network number.

3-4-4 Deleting Devices

There are three ways to delete a device from a virtual network.

- (1) Select a device, and then select **Edit - Delete** from the menu bar.
- (2) Select a device, and then click the **Delete** Button on the toolbar.
- (3) Select a device, and then right-click the selected device and select **Delete**.

A confirmation dialog box will be displayed before the deletion. Click the **Delete** Button to delete the device.

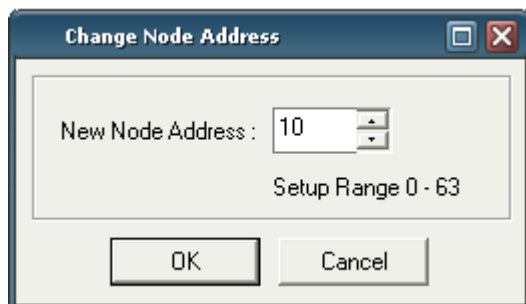
3-4-5 Changing the Node Address

When a device is added from the Device List, an unused node address from 0 to 63 is automatically allocated sequentially in the order the device is added.

There are two ways to change the allocated node address.

- (1) Select a device, and select **Device - Change Node Address** from the menu bar.
- (2) Select a device, and then right-click the device and select **Change Node Address**.

The following dialog box will be displayed. Change the node address and click the **OK** Button.

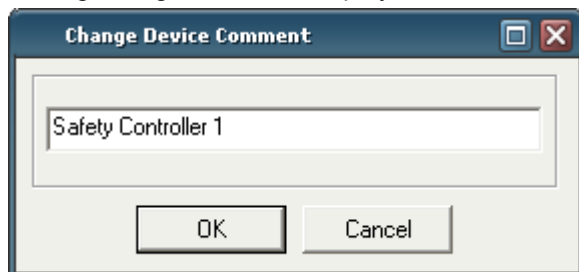


3-4-6 Changing Device Comments

When a device is added from the Device List, the displayed comment is the device type. Device comments can be set in the following two ways.

- (1) Select a device, and then select **Device - Change Device Comment** from the menu bar.
- (2) Select a device, and then right-click the device and select **Change Device Comment**.

The following dialog box will be displayed. Enter the device name and click the **OK** Button.



3-5 Saving and Reading Network Configuration Files

The created network configuration of the virtual network can be saved in a file. Also, you can open the saved file, modify it, or download it to the devices by connecting to the network.

3-5-1 Password Protection of the Network Configuration File

A password can be set for the network configuration file. The set password is encrypted and saved in the file. By setting the password for the network configuration file, the file is protected from unintended or unauthorized access.

The network configuration file password must be entered when the following operations are performed in the Network Configurator:

- Saving the network configuration file
- Reading the network configuration file
- Changing the network configuration file password

The passwords must match to save the file. If the password does not match when opening a file, Protect Mode is started. In Protect Mode, some Network Configurator operations are restricted.

The password for the network configuration file is set when the file is saved for the first time. The password must be from 6 to 16 alphanumeric characters. If you do not want to set a password, enter nothing and click the **OK** Button.

A screenshot of a Windows-style dialog box titled "Assign Password". The dialog has a title bar with a maximize button and a close button. The main text says "Please input a new password for 'Untitled'.". Below this, there are two text input fields. The first is labeled "New Password" and the second is labeled "Confirm of the New Password". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

To change the password for a network configuration file, select **File - Change Password** from the menu bar. After changing the password, however, the file and the password must be saved.

IMPORTANT:

- For security purposes, it is recommended to set a password for network for network configuration files.
- Do not forget the set password. You can open a network configuration file only in read-only mode if the password is forgotten, i.e., the file cannot be edited.

3-5-2 Saving the Network Configuration File

The network configuration can be saved using either of the following methods.

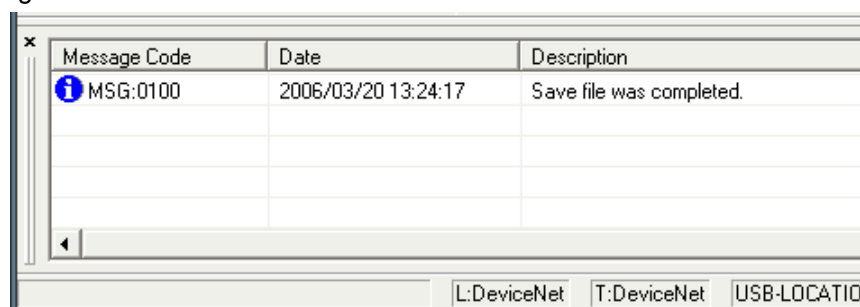
- (1) Select **File - Save** or **File - Save As** from the menu bar.
- (2) Click the **Save** Button on the toolbar.

Either way, the standard Windows dialog box for saving will be displayed. Select the saving location, name the file, and then click the **Save** Button.

When saving the file for the first time, the Assign Password Dialog Box will be displayed. Enter the password to set for the network configuration file.

When saving the second time or after, the Password Confirmation Dialog Box will be displayed. Enter the password set when the network configuration file was initially saved.

When saving has completed successfully, the following message will be displayed in the Message Pane:



3-5-3 Reading a Network Configuration File

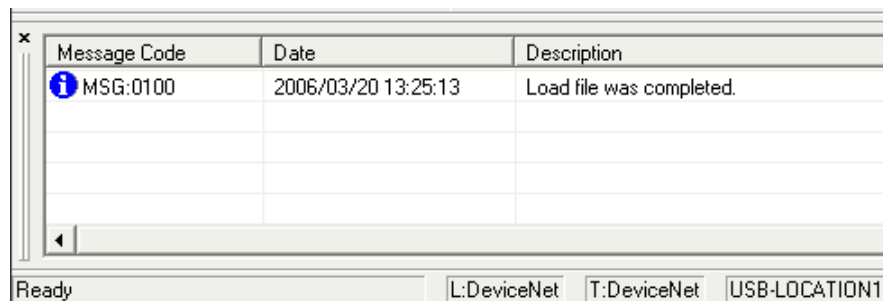
The saved network configuration file can be read for use by the Network Configurator using either of the following methods.

- (1) Select **File - Open** from the menu bar.
- (2) Click the **Open** Button on the toolbar.

Either way, the standard Windows Open File Dialog Box will be displayed. Select the file to open, and click the **Open** Button.

Next, the Check Password Dialog Box will be displayed. Enter the password set when the network configuration file was saved.

When reading has completed successfully, the following message will be displayed in the Message Pane:

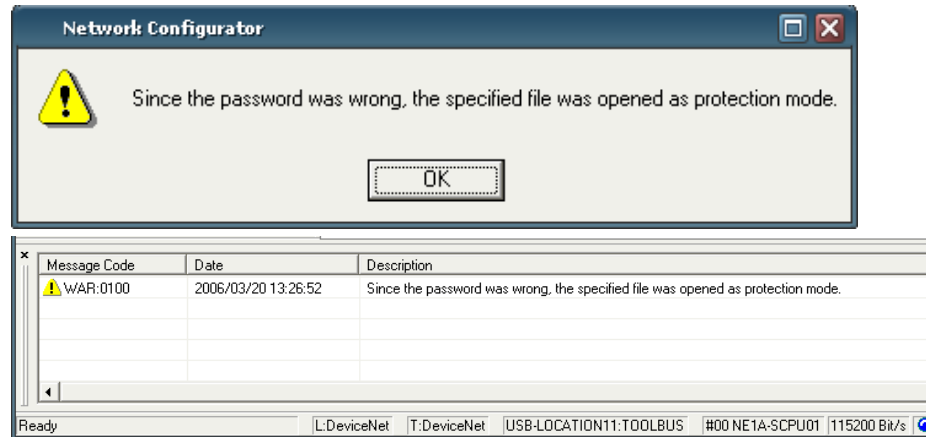


Note: If the password does not match, the Network Configurator will open the file in Protect Mode. In Protect Mode, operations such as saving the file, downloading parameters, and changing device status are prohibited. Refer to 3-5-4 *Protect Mode* for details.

3-5-4 Protect Mode

If the password does not match when opening the network configuration file, the Network Configurator will open the file in Protect Mode.

If the password does not match, the following message will be displayed in a dialog box and the Message Pane.



The following operations cannot be performed in Protect Mode.

- Saving a network configuration file
- Changing the password for the network configuration file
- Downloading the network configuration to devices in the network
- Downloading parameters to devices in the network
- Resetting devices in the network
- Changing passwords for devices in the network
- Sending explicit message requests to devices in the network
- Setting node addresses for devices in the network
- Setting the baud rate for devices in the network

3-6 Device Password Protection

A safety device can save a password internally. Setting the password in the device prevents an unauthorized person from changing the safety device parameters and status.

3-6-1 Setting a Device Password

Entering a device password is required when the following operations are performed on the Network Configurator. If the password does not match, the operations cannot be performed.

- Network downloading
- Parameter downloading
- Configuration locking
- Releasing a configuration lock
- Resetting
- Changing status
- Changing the password

A password is set for each device using either of the following methods. This function can be used only when the Network Configurator is online.

- (1) Select a device, and then select **Device - Change Password** from the menu bar.
- (2) Select a device, and then right-click the device and select **Change Password**.

The Change Password Dialog Box will be displayed as shown in the following figure. Enter the current password and a new password, and click the **OK** Button.

A password can contain from 6 to 16 alphanumeric characters.

The image shows a Windows-style dialog box titled "Change Password for Untitled". It has a standard title bar with a maximize button (disabled), a minimize button, and a close button. The dialog contains three text input fields, each with a label to its left: "Current Password", "New Password", and "Confirm of the New Password". The "New Password" and "Confirm of the New Password" fields are masked with asterisks. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Device passwords are not stored in the Network Configuration File. There is no password in the default settings. If the device is reset by setting the *Reset Type* to *Return to the out-of-box configuration, and then emulate cycling power*, it will return to the no-password setting. To reset the device, however, entering the current password is required. Therefore, do not forget the device password.

IMPORTANT: For security purposes, it is recommended to set passwords for devices.

Note: If you set the same password for multiple devices and perform an operation that requires entering a password, entering the password once can be treated as entering the password for all the devices. Select the *Use this password for all device* check box in the Password Input Dialog Box.



3-6-2 Forgotten Device Passwords

If you forget a device password, contact your OMRON Support Center. If you enter the recovery key obtained from the Support Center in the Password Recovery Tool installed in the Network Configurator, you can return the device to the no-password setting.

To obtain the recovery key, the following information is required. Use the Password Recovery Tool to obtain the information from the device. For details, refer to *Appendix 5 Using the Password Recovery Tool*.

- Vendor ID
- Serial number
- Counter information

3-7 Device Parameters and Properties

Registered device parameters can be edited on the virtual network without restrictions. Also, for parameters saved as a network configuration file, you can open the file later and download to a device or make modifications.

3-7-1 Editing Device Parameters

Device parameters can be edited using any of the following methods.

- (1) Double-click a device icon.
- (2) Select a device, and then select **Device - Parameter - Edit** from the menu bar.
- (3) Select a device, and then click the **Edit Parameter** Button on the toolbar.
- (4) Select a device, and then right-click the device and select **Parameter - Edit**.

The edit window for device parameters varies depending on the device.

Refer to *Section 4* for editing device parameters of DST1-series Safety I/O Terminals.

Refer to *Section 5* for editing device parameters of the NE1A-series Controller.

3-7-2 Uploading Device Parameters

Parameters of all the devices in the network can be uploaded from the network. Any of the following methods enables uploading parameters from one or more selected devices. This function is enabled only when the Network Configurator is online.

- (1) Select one or more devices, and then select **Device - Parameter - Upload** from the menu bar.
- (2) Select one or more devices, and then click the **Upload from Device** Button on the toolbar.
- (3) Select one or more devices, and then, right-click each device and select **Parameter - Upload**.

IMPORTANT: When the CS/CJ-series DeviceNet Unit exists in the network, disable the master functionality of the CS/CJ-series DeviceNet Unit, and then do the upload. If the master functionality is enabled, uploading the device parameters may fail.

Note: To upload the network configuration, refer to *Uploading the Network Configuration from the Actual Network (Network Upload)* in 3-4-3 Adding Devices.

3-7-3 Downloading Device Parameters

There are two ways to download parameters to a device: downloading to the selected devices and downloading sequentially to all the devices in the network. Either way is acceptable. Make sure, however, to download parameters to all the devices.

This function is enabled only when the Network Configurator is online. Downloading parameters also requires entering the device passwords.

Downloading Parameters to a Selected Device

You can download parameters to selected devices using any of the following methods.

- (1) Select one or more devices, and then select **Device - Parameter - Download** from the menu bar.
- (2) Select a device, and then click the **Download to Device** Button on the toolbar.
- (3) Select one or more devices, and then right-click each device and select **Parameter - Download**.

Next, the password input window for the device will be displayed. Enter the password for the selected devices and click the **OK** Button.

When selecting multiple devices and setting the same device password for all the devices, select the *Use this password for all device* check box in the following dialog box, and then entering passwords will no longer be necessary for each device.



Downloading Parameters to All Devices in the Network (Network Download)

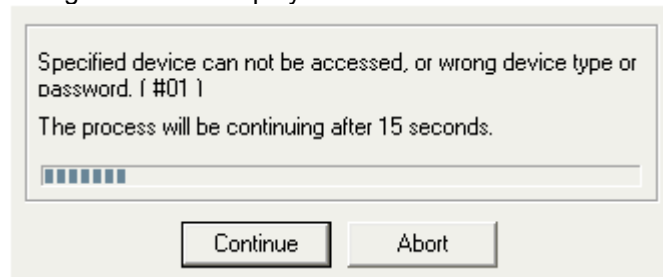
You can download parameters to all the devices in the network using any of the following methods.

- (1) Select **Network - Download** from the menu bar.
- (2) Click the **Download to Network** Button on the toolbar.
- (3) In the Network Configuration Pane, right-click without selecting any device and select **Download**.

The password input window of the devices will be displayed. As described in *Downloading Parameters to a Selected Device*, enter the password for the selected devices and then click the **OK** Button.

Errors while Downloading

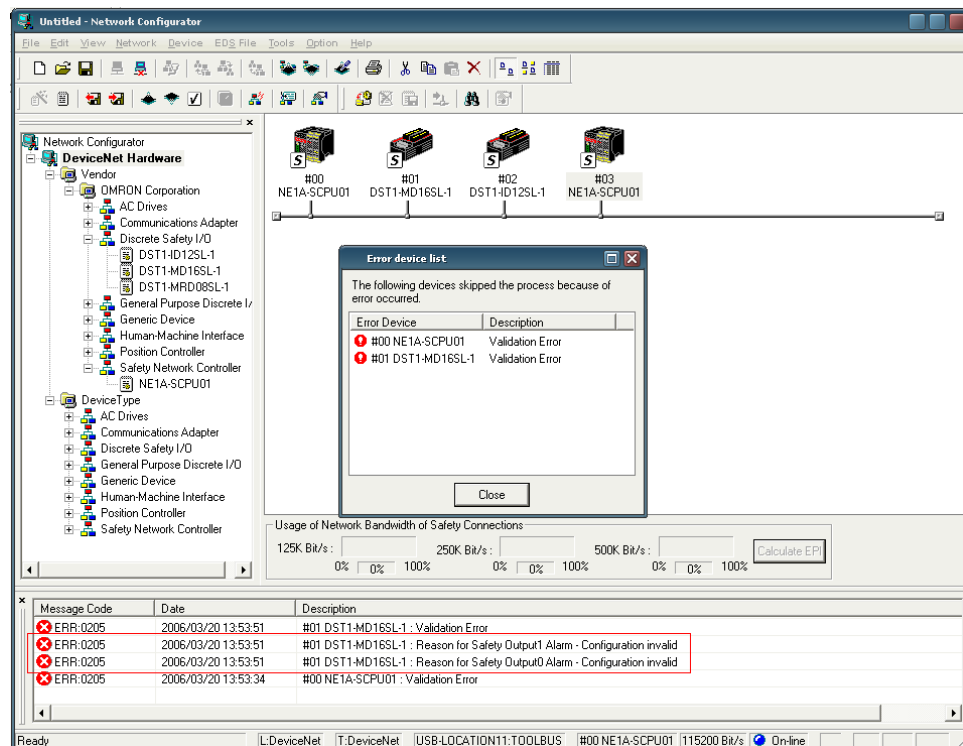
When an error occurs while downloading to multiple devices sequentially, the following dialog box will be displayed.



Downloading will continue to the next device if 15 seconds passes and neither button is clicked. If you want to perform the next download immediately, however, click the **Continue** Button.

If you click the **Abort** Button, the download process will be cancelled (and consequently, the parameters will not be downloaded to the subsequent devices).

The error that occurred will be displayed in the Message Pane and the device in which the error occurred will be displayed in the Error Device List.



The Error Device List displays by device the errors that occurred during parameter download.

- If the Error Device List shows that a parameter error has been found and if that error was caused by the I/O Terminal settings, the terminal with the error will be displayed in the Message Pane. (Refer to the outlined section in the above diagram.) No alarm will appear in the Error Device List if the error is not caused by the I/O Terminal settings and the cause must be found elsewhere.
- If the Error Device List displays an error stating that the TUNID does not match, click the **Get from the actual network** Button in the Network Number Field on the Network Property Dialog Box (see note). The network number for the actual network to be downloaded will be in the project file data. Click the **OK** Button to update the network number. Then execute the download again. Refer to 3-4-2 *Network Numbers* for details on network numbers and TUNID.

Note: Select **Network – Property** or right-click in the Network Configuration Window and select **Property** to display the Network Property Dialog Box.

Note: Refer to 8-2 *Errors When Downloading* for Error Device List errors other than those listed above, error details, and countermeasures.

Note: The download may take time if the NE1A-series Safety Master is in RUN mode. The time required for downloads can be reduced by changing to IDLE mode.

3-7-4 Device Properties

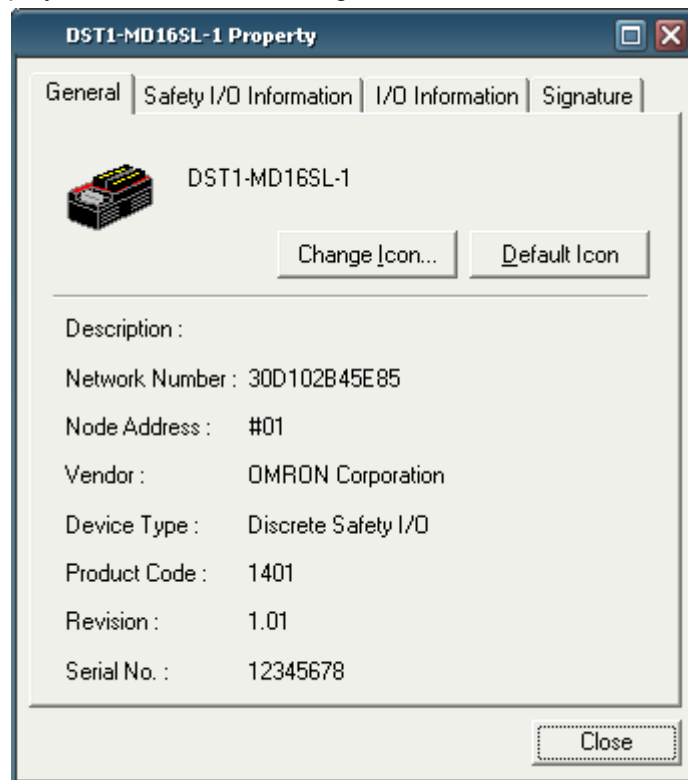
The device information, types of safety I/O and standard I/O, and safety signatures can be checked in the Device Property Dialog Box.

The Device Property Dialog Box can be displayed using any of the following methods.

- (1) Select a device, and then select **Device - Property** from the menu bar.
- (2) Select a device, and then click the **Device Property** Button on the toolbar.
- (3) Select a device, and then right-click the device and select **Property**.

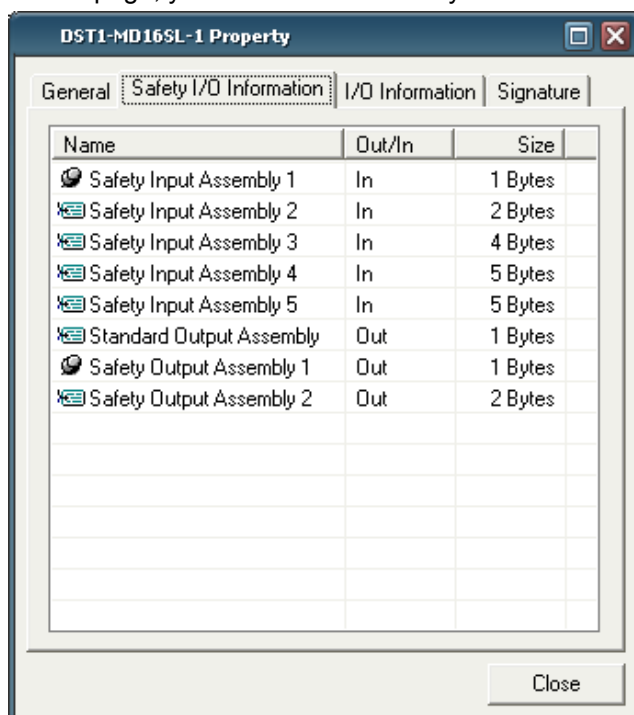
General Tab Page

In this tab page, you can check the device information and change the device icon displayed in the Network Configuration Pane.



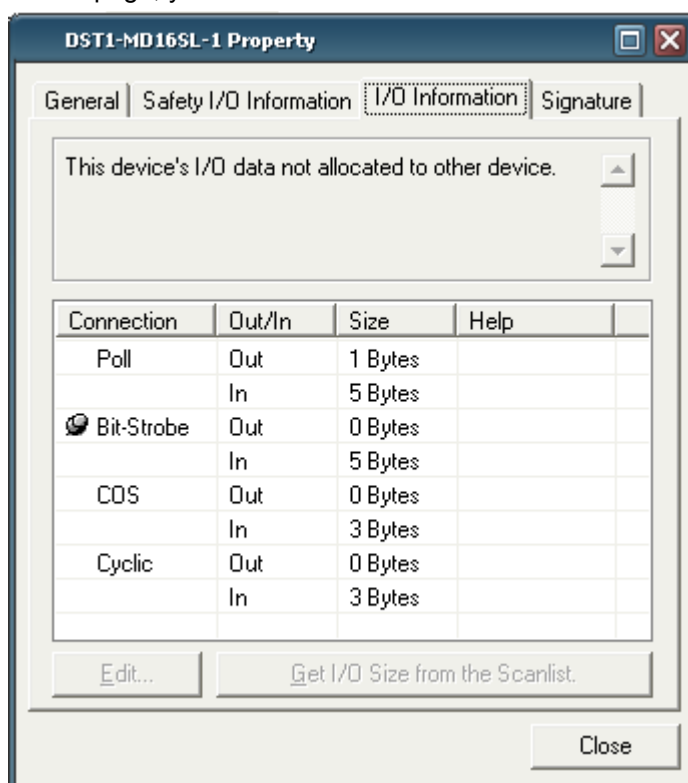
Safety I/O Information Tab Page

In this tab page, you can check the safety I/O classification information of a device.



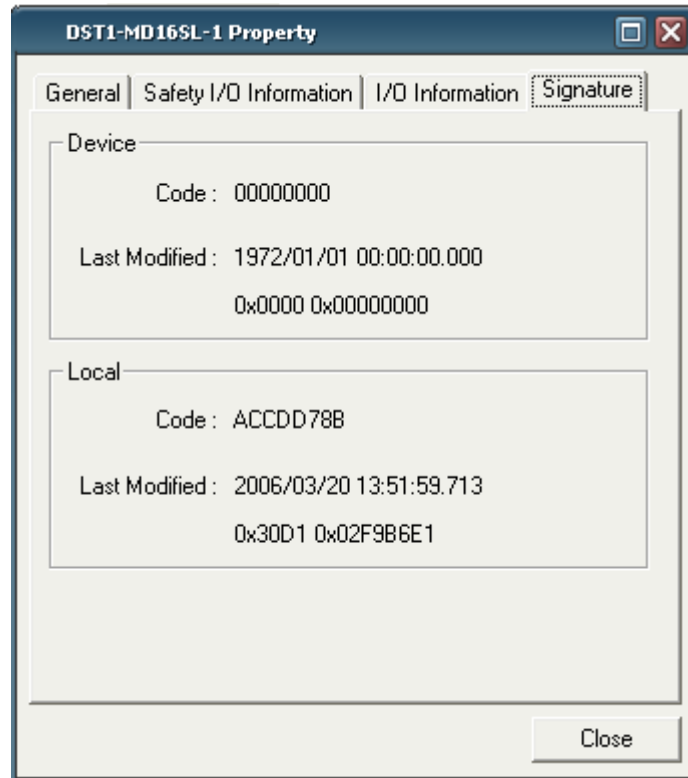
I/O Information Tab Page

In this tab page, you can check the standard I/O classification information of a device.



Signature Tab Page

In this tab page, you can check the safety signature that the Network Configurator generated and the one that the actual device has.



3-8 Parameter Verification

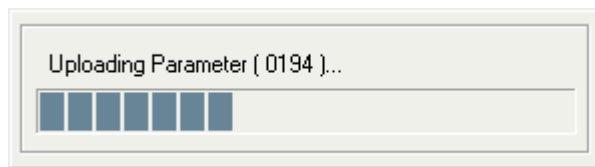
After downloading the parameters to a device, the user must perform parameter verification to check whether the parameters entered by the user were correctly downloaded to the device. The user must perform this verification for safety devices.

3-8-1 Device Parameter Verification

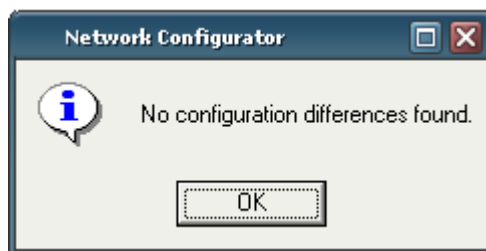
Verify the parameters using any of the following methods after downloading the parameters to devices. This function is enabled only when the Network Configurator is online.

- (1) Select a device, and then select **Device - Parameter - Verify** from the menu bar.
- (2) Select a device, and then click the **Verify Parameter** Button on the toolbar.
- (3) Select a device, and then right-click the device and select **Parameter - Verify**.

The device parameters will be uploaded.



First, the Network Configurator itself checks if the uploaded parameters are different from the parameters in the virtual network. If there are no differences, the following dialog box will be displayed.



If you click the **OK** Button, the uploaded parameters will be displayed.

Configuration Report - #01 : DST1-MD16SL-1

Save... Print... Close

Configuration Report - #01 : DST1-MD16SL-1

Generated by Network Configurator

#01 : DST1-MD16SL-1

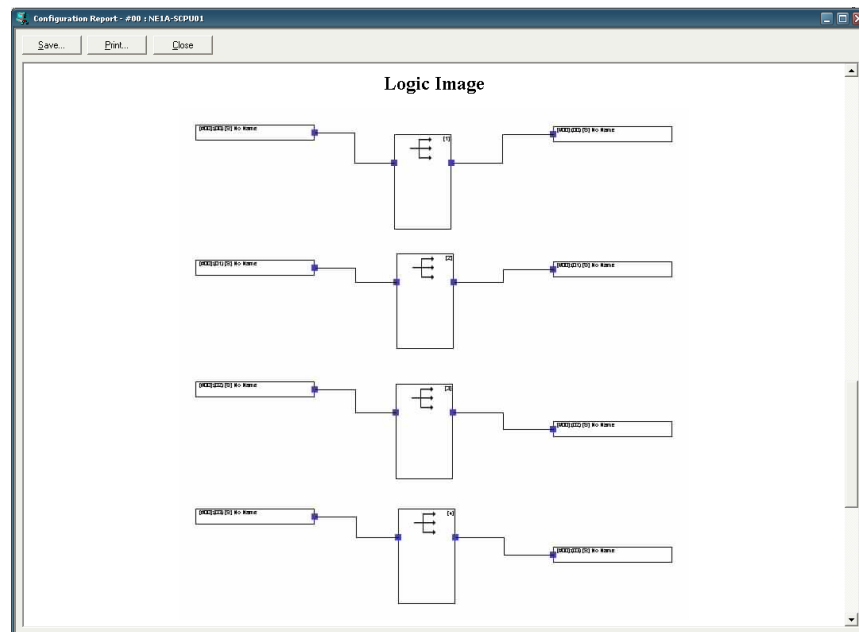
General Information

Product Name:	DST1-MD16SL-1
Description:	No Data
Node Address:	#01
Vendor:	OMRON Corporation
Device Type:	Discrete Safety I/O
Product Code:	1401
Revision:	1.01

Parameters

Signature Code:	8CFAFD80
Last Modified:	2006/03/20 14:07:10.833
	0x30D1 0x03079DF1

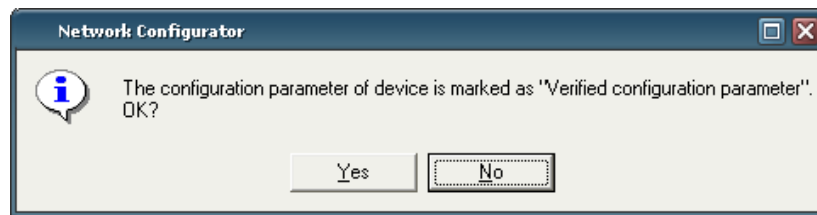
The user must check whether all the displayed parameters match the input values. If the device is the NE1A-series Controller, the Logic Program will also be displayed as in the following window. Check whether the Logic Program matches.



- Note:**
- Verification results can be saved. Click the **Save** Button at the top left of the window to save the results.
 - The displayed parameters and logic can also be printed. To print, click the **Print** Button.
 - In some cases the printout may exceed the specified size. Save the file and edit it using HTML editing software, then print the file.

After completing the verification, click the **Close** Button in the upper left to close the window.

The following window will be displayed.



If the parameters match, click the **Yes** Button.

After the verification has been completed, the safety symbol attached to the device icon in the virtual network will turn green, which indicates that verification is done.

IMPORTANT: After downloading the configuration data, verify the parameters and check whether the parameters saved in the device and the safety signature are correct.

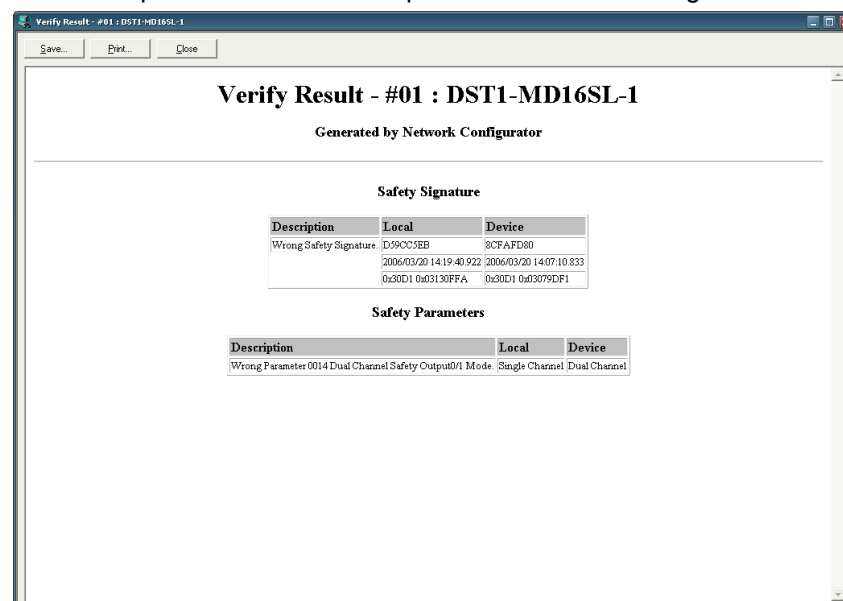
Note: Click the **Save** Button to save the configuration parameter report in HTML format. Click the **Print** Button to print the report.

- Note:
- After verifying the parameters of all the devices, make sure to save the network configuration file.
 - The *Verified configuration parameter* symbol ensures that the device parameters in the network configuration file are correct. This information is saved in the network configuration file, but not in the device itself. Therefore, the *Verified configuration parameter* symbol will not be attached even though the network configuration is obtained by network upload from a device that has been already verified.
 - If you edit parameters that have been verified, the *Verified configuration parameter* symbol will disappear. The device parameters must be verified again.

Parameter Mismatch

When the Network Configurator detects a mismatch in parameter verification, the parameter with the mismatch will be displayed with the safety signature in the window as in the following example.

Check the parameter values and perform the download again.



3-9 Configuration Lock

Perform user testing after verifying the device parameters. Checking all the operations of the device using user testing indicates that the device parameters have been verified by the user.

The configuration lock symbol indicates that the user test has completed.

3-9-1 Locking the Device Configuration

After the user testing, lock the configuration using either of the following methods. This function is enabled only when the Network Configurator is online. Also, to lock the configuration, verification of the device must have been completed already.

- (1) Select one or more devices, and then select **Device - Parameter - Lock** from the menu bar.
- (2) Select one or more devices, and then click each device and select **Parameter - Lock**.

Next, the password input window for the device will be displayed. Enter the password of the selected devices and click the **OK** Button.

When selecting multiple devices and setting the same device password for all the devices, select the *Use this password for all device* check box in the following dialog box, and then entering passwords will no longer be necessary for each device.



After the configuration lock has completed, the safety symbol attached to the device icon in the virtual network will change to a symbol of a lock, which indicates that the configuration lock has completed.



IMPORTANT: Operation of the device must be tested before lock the configuration.

- Note:
- **After performing a configuration lock for all the devices, make sure to save the network configuration file.**
 - **The symbol that indicates that the configuration lock has been done ensures that the device has been tested. This information is saved in the device itself as well as in the network configuration file.**
 - **Once the configuration lock has been performed, you cannot download the parameters to the device. To change the parameters, release the configuration lock.**
 - **When verified device parameters are edited, the *Verified configuration parameter* symbol will disappear. The device parameters must be verified again.**

3-9-2 Unlocking the Device Configuration

The configuration must be unlocked to change device parameters for which a configuration lock has been performed. Unlock the configuration for the selected devices using any of the following methods. This function is enabled only when the Network Configurator is online.

- (1) Select one or more devices, and then select **Device - Parameter - Unlock** from the menu bar.
- (2) Select one or more devices, and then right-click each device and select **Parameter - Unlock**.

Next, the password input window for the device will be displayed. As in *2–9–1 Locking the Device Configuration*, enter the password for the selected devices and click the **OK** Button.

When the configuration unlock has completed, the safety symbol attached to the device icon in the virtual network will return to the *Verified configuration parameter* symbol.

Note: **When changing the device parameters after a configuration unlock, lock the configuration after verifying the parameters again.**

3-10 Device Reset and Status Change

This section describes how to reset and change the status of safety devices. For some device types, status changes may not be supported.

3-10-1 Reset Types

There are three ways to reset a safety device.

Reset type	Description
Emulate cycling power.	Resets in the same way as cycling the power.
Return to the out-of-box configuration, and then emulate cycling power.	Returns the information stored in the device nonvolatile memory to the default settings and restarts.
Return information except for specified parameters to the out-of-box configuration, and then emulate cycling power.	Returns all information stored in the device nonvolatile memory other than specified data to the default settings, and then restarts.

The safety device stores the following information in the nonvolatile memory of the device:

Type	Default setting	Setting timing	Description
Device parameter	Not configured	Parameter download	Parameters and programs set by the user
Node address (software setting)	63	Node address change	Node address at startup with software setting enabled
Baud rate (software setting)	125 Kbit/s	Baud rate change	Baud rate at startup with software setting enabled (NE1A-series Controller only)
TUNID (Target Unique Node Identifier)	Not set	First parameter download	The identifier of the local node in the Safety Network as well as the combined values of the network number and node address
Password	No password	Password change	Password that a device has
CFUNID (Configuration Owning UNID)	Not set	First parameter download	UNID of the configuration source
OCPUNID (Output Connection Point Owning UNID)	Not set	Start of first safety communications	UNID of the Safety Master that opens a safety output connection.

The information above is stored in the nonvolatile memory of the device, and so it is not cleared by cycling the power source once it is set. To clear the information (to return to the default settings), select *Return to the out-of-box configuration, and then emulate cycling power* or *Return to the out-of-box configuration except to preserve the following parameters, and then emulate cycling power*.

WARNING

Failure to clear the previous configuration data before connecting the device to the network may result in loss of safety functions, personal injury, or death.



3-10-2 Resetting Devices

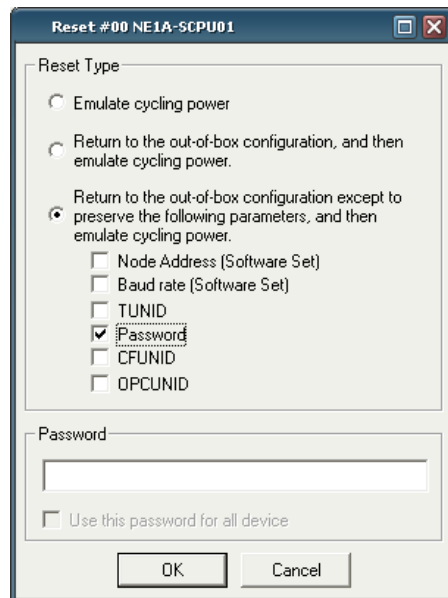
Reset devices using either of the following methods. This function is enabled only when the Network Configurator is online.

- (1) Select one or more devices, and then select **Device - Reset** from the menu bar.
- (2) Select one or more devices, and then right-click each device and select **Reset**.

The reset window of the devices will be displayed as shown in the following example.

Enter a reset type and the password and then click the **OK** Button.

For example, to keep the current password setting for multiples devices with the same password but return other information to the default, specify the setting as follows:



3-10-3 Reset Types and Device Status

Resetting may not be supported for some types of reset and device status.

Reset type	Device status			
	Safety connection being established and configuration locked.	Safety connection being established and configuration locked.	Safety connection not established and configuration locked.	Safety connection not established and configuration locked.
Emulate cycling power	Unable to reset.	Unable to reset.	Able to reset.	Able to reset.
Return to the out-of-box configuration, and then emulate cycling power.	Unable to reset.	Unable to reset.	Unable to reset.	Able to reset.
Return information except for specified parameters to the out-of-box configuration, and then emulate cycling power.	Unable to reset.	Unable to reset.	Unable to reset.	Able to reset.

3-10-4 Changing Device Status

Changing the device status is not supported by all devices.

The NE1A-series Controller can switch between IDLE mode and RUN mode. For details on NE1A-series Controller modes, refer to the *Safety Network Controller Operation Manual (Z906)*.

For DST1-series Safety I/O Terminals, there is no need to change modes.

Change the device mode using either of the following methods. This function is enabled only when the Network Configurator is online.

- (1) Select a device, and then select **Device - Change Mode** followed by the desired mode.
- (2) Select a device, and then right-click the device and select **Change Mode** followed by the desired mode.

Next, the password input window for the device will be displayed. Enter the password for the selected devices and click the **OK** Button.



Section 4

Editing Safety I/O Terminal Parameters

4-1	Editing Parameters	106
4-1-1	Parameter Groups	106
4-1-2	General Parameter Group	108
4-1-3	Safety Input Parameter Groups	109
4-1-4	Test Output Parameter Groups	111
4-1-5	Safety Output Parameter Groups	112
4-1-6	Operation Time Parameter Groups	113

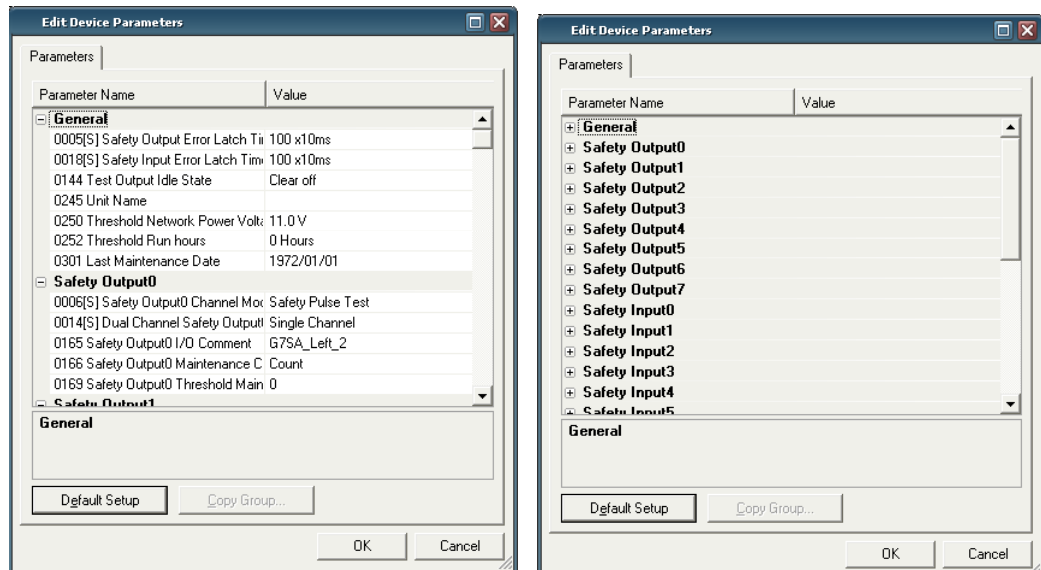
4-1 Editing Parameters

Device parameters can be edited using any of the following methods.

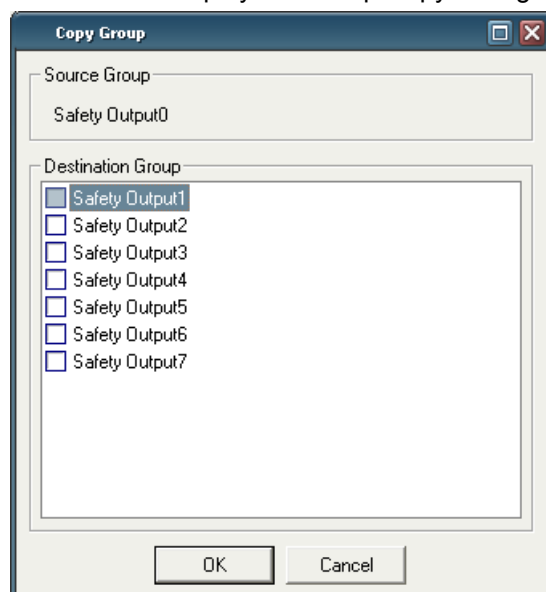
- (1) Double-click a device icon.
- (2) Select a device, and then select **Device - Parameter - Edit** from the menu bar.
- (3) Select a device, and then click the **Edit Parameter** Button on the toolbar.
- (4) Right-click the device and select **Parameter - Edit**.

4-1-1 Parameter Groups

Safety I/O Terminal parameters are classified into groups as shown in the following diagram.



- Double-click a group name or click the icon to display or hide that group. Parameter settings for a particular terminal can be batch copied to the parameters for another terminal. The **Copy Group** Button is enabled when a group name is selected and a group with a different terminal number but similar parameters exists, e.g., when safety input 0 is selected and safety input 1 or safety input 2 exists. Click the **Copy Group** Button to display the Group Copy Dialog Box shown below.

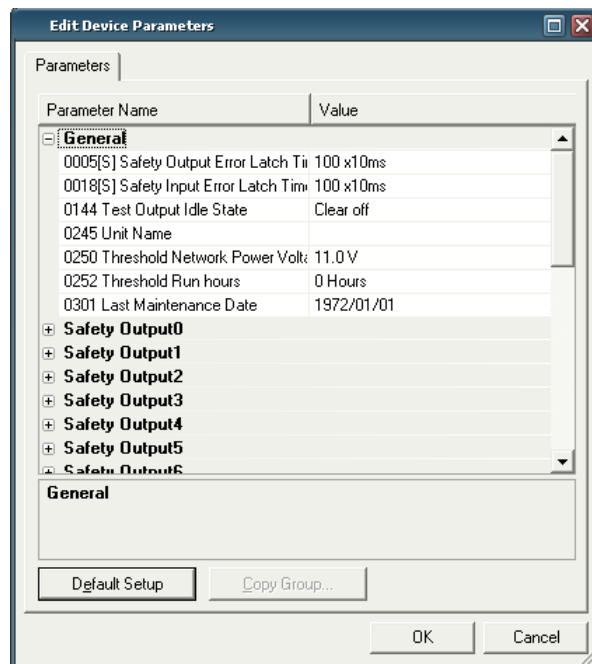


The source and destination groups will be displayed. Select the desired destination groups and then click the OK Button. The parameters will be copied.

- Parameter names with [S] in front of them are related to the safety application.
- The size of the Edit Device Parameters Window can be changed.

4-1-2 General Parameter Group

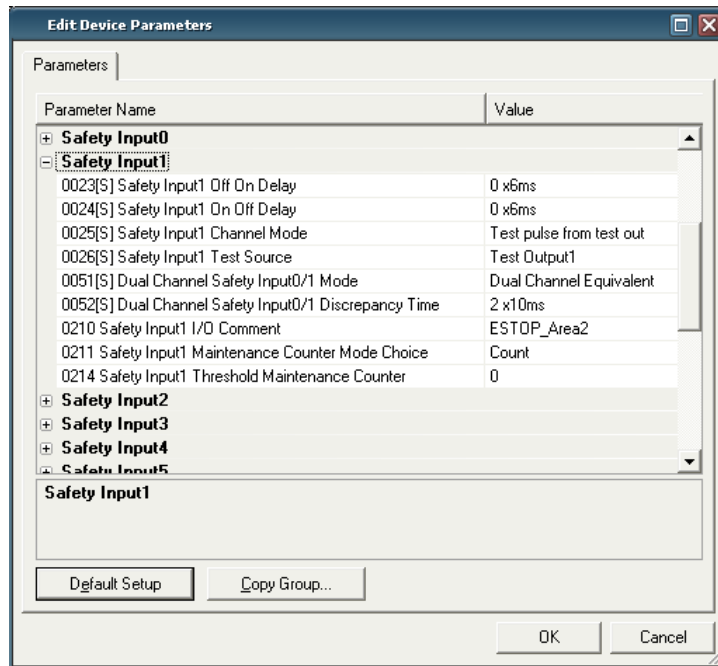
This section describes parameters in the general parameter group.



	Item	Settings	Description	Default
S	Output Error Latch Time	0 to 65,530 ms (in 10-ms increments)	This parameter is common to all the safety outputs. It sets the time to latch the error state when an error occurs in these outputs. Even when the cause of the error has been removed, the error state will remain latched for the time set here.	1,000 ms
S	Input Error Latch Time	0 to 65,530 ms (in 10-ms increments)	This parameter is common to all safety inputs and test outputs. It sets the time to latch the error state when an error occurs in these inputs/outputs. Even when the cause of the error has been removed, the error state will remain latched for the time set here.	1,000 ms
	Test Output Idle State	Clear off Keep output data	This parameter is common to all test outputs for which the Test Output Channel Mode is set to <i>Standard Output</i> . It sets the output state of the test output when idle data is received.	Clear off
	Unit Name	32 characters max.	This parameter sets a user-chosen name for the Safety I/O Terminal. The set name is saved in the Safety I/O Terminal and displayed in the network configuration.	None
	Threshold Network Power Voltage	8.0 to 30.0 V	This parameter sets the threshold of the network power voltage. When the voltage falls below the set threshold voltage, the corresponding bit in general status turns ON.	11.0 V
	Threshold Run Hours	0 to 429,496,729 hours	This parameter sets the threshold for unit operating hours. When the operating hours exceeds the set threshold, the corresponding bit in general status will turn ON.	0 hours
	Last Maintenance Date	January 1, 1972 to January 19, 2038	This parameter saves the maintenance date in the Safety I/O Terminal.	January 1, 1972

4-1-3 Safety Input Parameter Groups

This section describes parameters in the safety input parameter groups. The safety input parameters are grouped by terminal number.



	Item	Settings	Description	Default
S	Off On Delay	0 to 126 ms (in 6-ms increments)	Sets the OFF/ON delay time.	0 ms
S	Off On Delay	0 to 126 ms (in 6-ms increments)	Sets the ON/OFF delay time.	0 ms
S	Safety Input Channel Mode	Not used.	The safety input is not used. (External input device not connected.)	Not used.
		Test pulse from test out	Specifies connecting a device with a contact output in combination with a test output. When this mode is selected, select the test output to use for the test source and then set the test output mode to <i>Pulse Test Output</i> . When these settings are made, contact between the input signal line and the power supply (plus) and short circuits with other input signal lines can be detected.	
		Used as a safety input.	Specifies connecting a safety device with a semiconductor output, such as a light curtain.	
		Used as a standard input.	Specifies connecting a standard device (i.e., a non-safety device).	
S	Test Source	Not used.	If the channel mode of a safety input is set to <i>Test Pulse from Test Out</i> , the test output is selected for use in combination with the safety input. Set the channel mode of the test output selected here to <i>Pulse Test Output</i> .	Not used.
		Test Output 0		
		Test Output 1		
		Test Output 2		
		Test Output 3		
S	Dual Channel Safety Input Mode	Single Channel	Specifies using Single Channel Mode. If <i>Single Channel</i> is selected, the safety input that would be paired for the dual channel parameter will also be set to Single Channel Mode.	Dual Channel Equivalent
		Dual Channel Equivalent	Specifies using the Dual Channel Equivalent Mode with a paired safety input.	
		Dual Channel Complementary	Specifies using Dual Channel Complementary Mode with a paired safety input.	
S	Dual Channel Safety Input Discrepancy Time	0 to 65,530 ms (in 10-ms increments)	Sets the time to monitor the logic discrepancy in the dual channel input logic.	0 ms

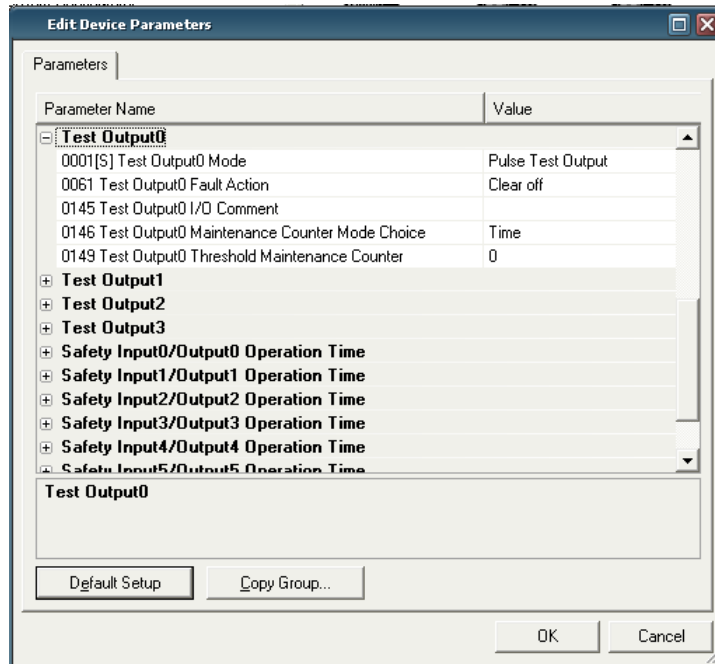
Section 4-1 Editing Parameters

	Item	Settings	Description	Default
	I/O Comment	32 characters max.	Sets an I/O comment for the safety input. The I/O comment set here is used as the I/O tag in the Logic Editor.	None
	Maintenance Counter Mode Choice	Time Count	Sets the operating mode for the maintenance counter.	Time
	Threshold Maintenance Counter	0 to 4,294,967,295 hours	Sets the threshold value for the maintenance counter.	0

IMPORTANT: When the Safety Input Channel Mode is set to *Test Pulse from Test Out*, specify the test output to use for the test source and set the Test Output Channel Mode of the test output to *Pulse Test Output*.

4-1-4 Test Output Parameter Groups

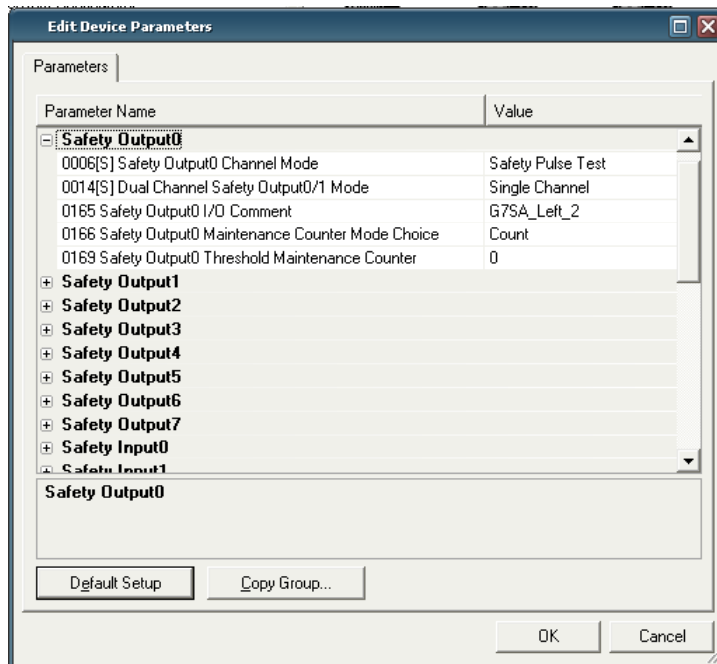
This section describes parameters in the test output groups. The test output parameters are grouped by terminal number.



	Item	Settings	Description	Default
S	Test Output Mode	Not used.	The corresponding test output is not used.	Not used.
		Standard Output	Specifies connecting to the input for a muting lamp or PLC. Used as a monitor output.	
		Pulse Test Output	Specifies connecting a device with a contact output in combination with the safety input.	
		Power Supply Output	Specifies connecting to the power supply terminal of a safety sensor. The voltages supplied to the IO power from the test output are output.	
		Muting Lamp Output (Setting supported only for T3 terminal.)	Specifies a muting lamp output. When the output is ON, disconnection of the muting lamp can be detected.	
	Fault Action	Clear off	Sets the output state of the test output when a communications error occurs. This parameter is enabled when the Test Output Channel Mode is set to <i>Standard Output</i> or <i>Muting Lamp Output</i> .	Clear off
		Hold last data		
	I/O Comment	32 characters max.	Sets an I/O comment for the test output. The I/O comment set here is used as the I/O tag in the Logic Editor.	None
	Maintenance Counter Mode Choice	Time	Sets the operating mode for the maintenance counter.	Time
		Count		
	Threshold Maintenance Counter	0 to 4,294,967,295 hours	Sets the threshold value for the maintenance counter.	0

4-1-5 Safety Output Parameter Groups

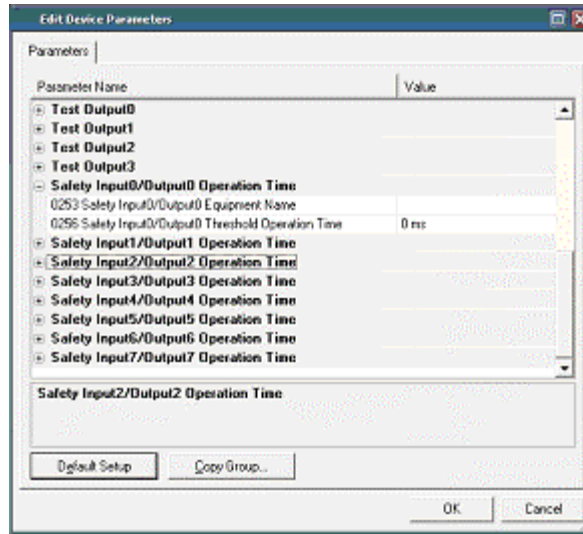
This section describes parameters in the safety output groups. The safety output parameters are grouped by terminal number.



	Item	Settings	Description	Default
S	Safety Output Channel Mode	Not used.	The safety output is not used. (External output device not connected.)	Not used.
		Safety	Specifies not outputting the test pulse when the output is ON. Contact between the output signal line and the power supply (positive) when the output is OFF and ground faults can be detected.	
		Safety Pulse Test (Setting supported only for the DST1-MD16SL-1.)	Outputs the test pulse when the output is ON. Contact between the output signal line and the power supply, and short circuits with other output signal lines can be detected.	
S	Dual Channel Safety Output Mode	Single Channel	Specifies using Single Channel Mode. When <i>Single Channel</i> is set, the safety output that would be paired for the dual channel parameter is also set to Single Channel Mode.	Dual Channel
		Dual Channel	Specifies using Dual Channel Mode. When both of the safety outputs to be paired are normal, the outputs can be turned ON.	
	I/O Comment	32 characters max.	Sets an I/O comment for the safety output. The I/O comment set here is used as the I/O tag in the Logic Editor.	None
	Maintenance Counter Mode Choice	Time	Sets the operating mode for the maintenance counter.	Time
		Count		
	Threshold Maintenance Counter	0 to 4,294,967,295 hours	Sets the threshold value for the maintenance counter.	0

4-1-6 Operation Time Parameter Groups

This section describes parameters in the safety input/output operation time groups. The operation time parameters are grouped by the terminal numbers to be paired.



	Item	Settings	Description	Default
	Equipment Name	32 characters max.	Sets a comment for the operation time to monitor.	None
	Threshold Response Time	0 to 65,535 ms (in 1-ms increments)	Sets the threshold value for the operation time.	0 ms

Section 5

Editing Safety Network Controller Parameters

5-1	Safety Connection Settings	116
5-1-1	Registering Safety Slaves	116
5-1-2	Setting Safety Connection Parameters.....	119
5-1-3	Stopping/Restarting Communications after an Error	124
5-1-4	Listing and Setting Connection Parameters	125
5-2	Safety Slave Settings	126
5-2-1	Registering I/O Assemblies for Safety Slaves	126
5-2-2	Setting Assembly Data.....	127
5-3	Standard Slave Settings	133
5-3-1	Registering I/O Assemblies for Standard Slaves.....	133
5-3-2	Setting Slave Input Data in Idle State	134
5-3-3	Setting Assembly Data.....	134
5-4	Local I/O Settings	136
5-4-1	Setting Safety Inputs.....	136
5-4-2	Setting Test Outputs	140
5-4-3	Setting Safety Outputs	142
5-5	Setting the Operating Modes and Confirming the Cycle Time	144
5-5-1	Setting the NE1A-series Controller Operating Modes	145
5-5-2	Confirming the Cycle Time.....	145
5-5-3	Restarting a Connection Stopped due to a Communications Error...	146

5-1 Safety Connection Settings

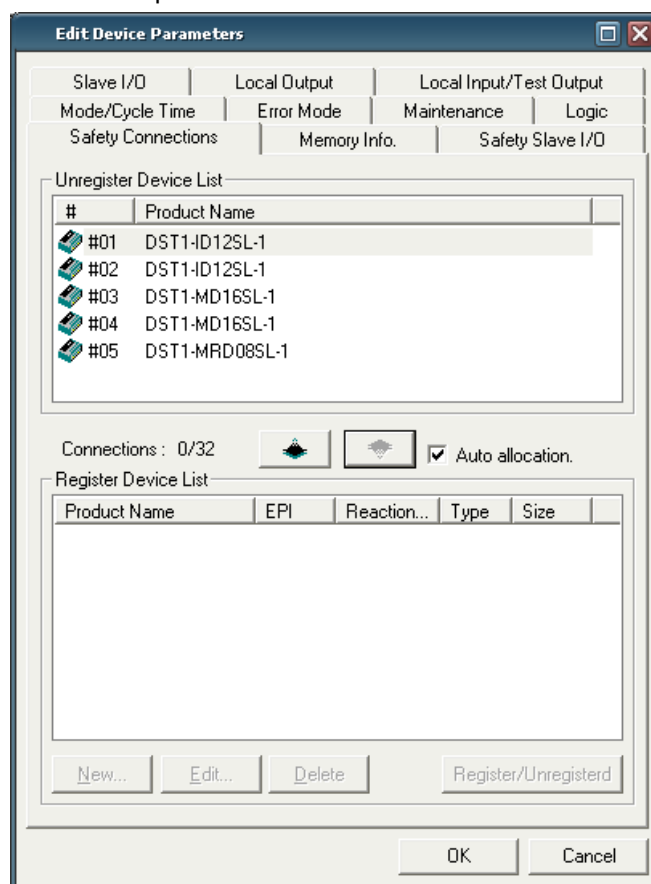
Open the Edit Device Parameter Window of the NE1A-series Controller and click the **Safety Connections** Tab to display the Safety Connection Setting Window. In this window, you can register the Safety Slaves, such as the DST1-series Safety I/O Terminals, that perform the safety communications and set the communications parameters.


Note: Setting parameters in this window is not necessary when the NE1A-series Controller is used in Standalone Mode.

5-1-1 Registering Safety Slaves

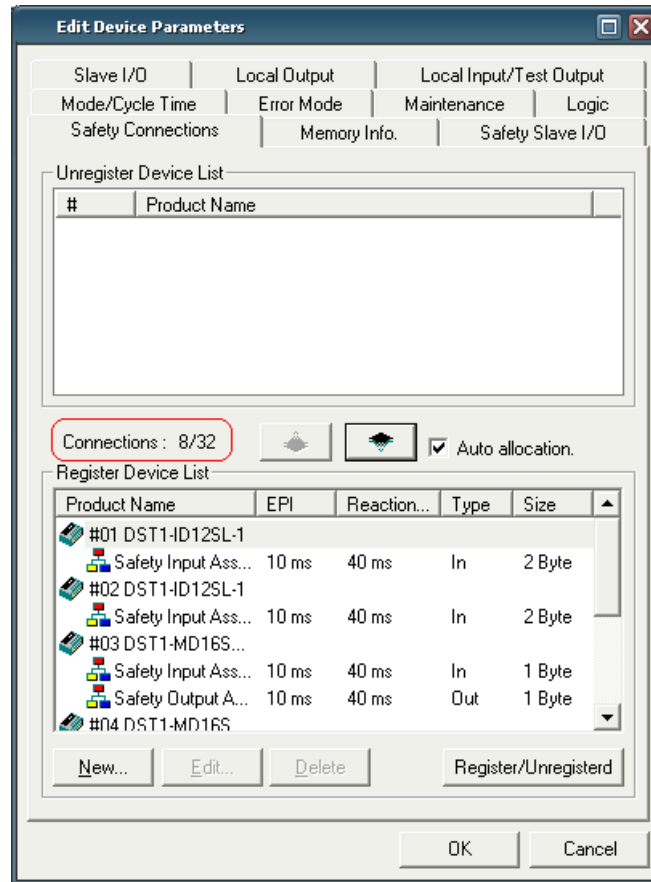
Use the following procedure to register Safety Slaves as communications destinations.

1. Unregistered devices are listed in the upper pane, and registered devices are listed in the lower pane.



2. Select a Safety Slave to register in the Unregister Device List and click the  Button.

3. The Safety Slave selected in step 2 will be registered.
If the *Auto Allocation* Check Box is selected at this point, the default connections and the parameters are will be automatically allocated as shown in the following figure.




In addition, the number of connections used and the number of connections that can be used are displayed in the window.

The following information is displayed in the Register Device List.

Item	Information displayed
Product Name	The name of the registered Safety Slave (icon) or I/O assembly used in the safety connection (icon) is displayed.
EPI	The EPI for the safety connection is displayed. For details on EPI, refer to <i>5-1-2 Setting Safety Connection Parameters</i> .
Reaction Time	The network reaction time for the safety connection is displayed.
Type	The type of the I/O assembly used in the safety connection is displayed.
Size	The data size of the I/O assembly used in the safety connection is displayed.

4. In the Register Device List, you can add and delete connections and edit the connection parameters.
 - To add a connection, select the Safety Slave that you want to add the connection to and click the **New** Button. Refer to *5-1-2 Setting Safety Connection Parameters* to set the parameters.
 - To delete a connection, select the connection you want to delete and click the **Delete** Button.
 - To edit connection parameters, select the connection you want to edit and click the **Edit** Button. The parameters of the selected connection will be displayed. Refer to *5-1-2 Setting Safety Connection Parameters* to change the parameters.
 - Select the Safety Slave and click the **Register/Unregister** Button. If connections are already set, the button cancels all the connections and if not, it allocates the default connection and parameters.

- Note:**
- To delete a Safety Slave from the Register Device List, select the Safety Slave you want to delete and click the  Button.
 - Also, when either of the following operations is performed in the Network Configuration Window, the Safety Slave will be registered using auto-allocation.
 - (1) Dragging a slave device to the NE1A-series Controller.
 - (2) Selecting a slave device and specifying the destination as the NE1A-series Controller by selecting Device and then *Register to Other Device* from the menu bar.

IMPORTANT: Changing safety connection settings may affect the program. After changing any setting, always open the Logic Editor and check the program.

5-1-2 Setting Safety Connection Parameters

This section describes how to set safety connection parameters.

I/O Connections

Select the assembly to use from the I/O assemblies that the destination Safety Slave supports.

- Note:
- Refer to the **DST1-Series Safety I/O Terminals Operation Manual (3-2 Remote I/O Allocations)** for I/O assemblies that the DST1-series Safety I/O Terminals support.
 - When the Safety Slave function of the NE1A-series Controller is used, the I/O assembly must be set in the Safety Slave I/O Window. Refer to 5-2 Safety Slave Settings.

Output Connection Owner

To prevent safety outputs from an unintended Safety Master, the Safety Slave stores data in non-volatile memory to show that the Safety Master that last established an output connection (see note 1) is the owner of the output connection. The Safety Master data that is stored is the TUNID (see note 2). Other Safety Masters cannot open that output connection while the Safety Slave has an output connection owner TUNID stored.

If an attempt is made, the 7-segment display on the NE1A-series Safety Master will show "d6" and the status code (see note 3)(error code) shown on the Safety Connection Tab of the Device Monitor Window will be "01:0106".

Reset the Safety Slave to the default settings to clear the output connection owner data.

Note 1: The DST1 is displayed as "Safety Output Assembly" and the NE1A-series Controller is displayed as "Safety Output."

2: Refer to 3-4-2 Network Numbers for information on TUNIDs.

3: Refer to *7-1-2 Monitoring Safety Connections* for information on status codes.

- Note:**
- Reset the Safety Slave to default settings before opening an output connection from another Safety Master.
 - The error referred to earlier will occur if the Safety Master TUNID changes as a result of node address or network number changes and the output connection owner no longer matches.

Open Type

Select the type of open processing to be performed when the NE1A-series Controller establishes a connection with the Safety Slave.

Open Type	Description
Configure the target device	The Safety Slave is configured when the connection is established. The parameters that can be set are limited to the parameters relevant to the safety application. Do not use this open type under normal conditions.
Check the safety signature	The NE1A-series Controller sends the safety signature of the slave when the connection is established. The safety signature is checked in the Safety Slave that receives a connection is established. Specify this open type when establishing a connection with DST1-series Safety I/O Terminals.
Open only	The NE1A-series Controller does not send the safety signature of the slave when a connection is established. The Safety Slave establishes the connection without checking the safety signature. To use the slave function of the NE1A-series Controller, it is necessary to configure the Safety Slave correctly from the Network Configurator. If it is not correctly configured, a connection will not be established, so there is no need to send the safety signature from the Safety Master for checking.

IMPORTANT: Check that the Safety Master and the Safety Slave are configured correctly when selecting *Open only* as the safety connection open type.

- Note:** If the Safety Slave is not configured when *Configure the target device* is specified, the NE1A-series Controller configures the Safety Slave and then establishes a connection. Therefore, the communications can be started again just by connecting the slave to the network without the Network Configurator when the Safety Slave is replaced. In the current version, however, the parameters to be set are only those related to the safety application. When standard parameters do not need to be set, this open type can be specified. The ability to set standard parameters is planned for future development.

Configuration Owner

To prevent configuration from an unintended source, Safety Slaves store data in non-volatile memory to show that the node that performed configuration last time is the configuration owner. The Safety Slave stores data in memory to show if the configuration was performed by the Network Configurator or a similar software tool (see note 1) and, if the configuration was performed by a Safety Master, the Safety Slave stores the TUNID (see note 2). The Safety Slave cannot be configured from another source while it has data on the configuration owner.

If the configuration owner does not match, the following will occur.

- A) If a download is attempted using the Network Configurator, an error message will be displayed to indicate that configuration is not possible until the Safety Slave is reset because the Safety Slave has been configured by another device.
- B) If **Configure Target Device** is specified, the NE1A-series Safety Master 7-segment display will show “d6” and the status code (see note 3) (error code) shown on the Safety Connection Tab in the Monitor Device Window will be “01:0105”.

The configuration owner is cleared when the Safety Slave is reset to default

settings.

- Note 1:** No distinction is made between Support Software, so other Network Configurators can be used to configure the Safety Slave.
- 2:** Refer to 3-4-2 *Network Numbers* for information on TUNIDs.
- 3:** Refer to 7-1-2 *Monitoring Safety Connections* for information on status codes.

- Note:
- **Reset the Safety Slave to default settings to configure from a different configuration owner.**
 - **The configuration owner will not match and the error listed above will occur if the Safety Master TUNID changes because the node address or network number has changed.**

Connection Type

Select the connection type to use between the NE1A-series Controller and Safety Slave.

Connection Type	Description
Multi-cast connection	This connection type can be selected only with a Safety Input Slave. When a multi-cast connection is selected, a Safety Input Slave can transmit the input data to a maximum of 15 NE1A-series Controllers via a multi-cast connection. These NE1A-series Controllers are classified as the same multi-cast group when multiple NE1A-series Controllers establish a multi-cast connection with one Safety Slave and the I/O assembly and EPI values specified in I/O Connection are the same. This connection type can be selected even for one NE1A-series Controller.
Single-cast connection	This connection type can be selected for an input connection or output connection. The NE1A-series Controller and the Safety Slave establish a 1:1 connection and send safety data.

EPI (Expected Packet Interval)

The EPI is the interval at which the Safety Controller and Safety Slave communicate safety data. The minimum set value is the greater of the destination Safety Slave cycle time and Safety Controller cycle time.

- The cycle time of DST1-series Safety Slaves is always 6 ms.
- The Safety Controller cycle time is 4 ms if no programming has been created (default status). The cycle time will be longer if safety logic programming has been created and will depend on the size of the programming. (Refer to 9-2 *Operational Flow and Cycle Times* in the *Safety Network Controller Operation Manual* (Cat. No. Z906). The Safety Controller cycle time can be checked under *Cycle Time* on the Mode/Cycle Time Tab in the Edit Device Parameters Dialog Box, once all parameters have been set and programming completed. (Refer to 5-5 *Setting the Operating Mode and Confirming the Cycle Time*.)

The EPI set here affects the network bandwidth usage rate and the network reaction time.

- **Network Reaction Time:**
Displayed under *Reaction Time* in the *Data Expected Packet Interval* (EPI) Field. Refer to 2-3 *Calculating and Verifying the Maximum Reaction Time* and 9-4 *Reaction Time* in the *Safety Network Controller Operation Manual* (Cat. No. Z906) for information on the network reaction time.
- **Network Bandwidth Usage Rate:**
Displayed under *Usage of Network Bandwidth for Safety Connections* at the bottom of the Network Configuration Window.

The network configuration may need to be reconsidered if the acceptable network

bandwidth usage rate (must be 90% or less overall) cannot be obtained with the EPI setting required to achieve the required network reaction time. Refer to 2-2-2 *Allocating Network Bandwidth Usage and Calculating the Best EPI* for details.

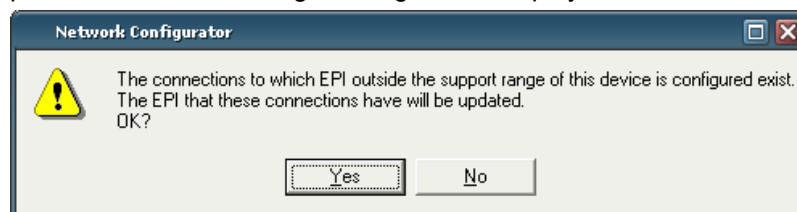
IMPORTANT: Set the EPI for each safety connection longer than the Safety Network Controller cycle time. An error will occur when the safety connection parameters are downloaded if the EPI is shorter, and the download will fail.

Note: **Calculate the best average EPI for all connections using the following procedure and batch set the EPI to all devices.**

1. Click the **Calculate EPI** Button under *Usage of Network Bandwidth for Safety Connections* at the bottom of the Network Configuration Window.
2. Input the network bandwidth to be used in the *Safety Connections* Field and click the **Calculate** Button.
3. The best average EPI for all connections will be displayed under Best Average EPI.
4. Click the **Update Device Configuration** Button.
5. Select the baud rate to be used in the Update Device Configuration Dialog Box and click the **OK** Button.

The best average EPI for all connections will be batch set as the EPI in the safety connection parameters for all devices.

Configurator version 1.6□ has an automatic EPI adjustment function. The EPI that is set in the device parameters is compared to the actual cycle time. If the EPI setting is shorter, it will be automatically updated. If the EPI is shorter than the device parameters, the following warning will be displayed.



Click the **Yes** Button in the above dialog box. The EPI for the applicable connection will be automatically changed to the device cycle time.

It can prevent errors from occurring during downloads.

Note: **If the communications partner is an NE1A-series Controller in slave operation, the cycle time of the communications partner is not checked. Confirm that the EPI setting is greater than the cycle time of the communications partner.**

Expand Setting

The **Advanced** Button enables changing more detailed communications parameters. The Timeout Multiplier, Network Delay Multiplier, and ID Allocation can be set in the Under normal operation conditions, it is not necessary to change one of these parameters.

In some cases, it may be necessary to change the “Timeout Multiplier,” “Network Delay Multiplier,” or “ID Allocation” to cover the requirements in special installation environments.

IMPORTANT: “Timeout Multiplier” and “Network Delay Multiplier” affect reaction time of the safety system. If one or both parameters are changed, there will be an increase in safety reaction time.

“Timeout Multiplier”

This parameter is used to set up Time Out count.

Safety Device will judge the Communication Error based on this parameter. If this parameter is set to “3”, Safety Device accepts communication time out twice and this parameter also affects reaction time of safety system. There will be an increase in safety reaction time.

“Network Delay Multiplier”:

This parameter is used for Calculation of Reaction Time and this parameter also affects reaction time of safety system. There will be an increase in safety reaction time.

“ID Allocation”:

One connection (e.g., NE1A-SCPU01 and DST1-ID12SL-1) uses one ID and each Device has 12 IDs.

If the connection has established, either Master D or Slave ID will be consumed.

The radio button shows two possibilities to choose from:

Set to “Allocate the ID for produced connections” uses ID master device has.

Set to “Ask the slave for produced Ids” uses ID slave device has.

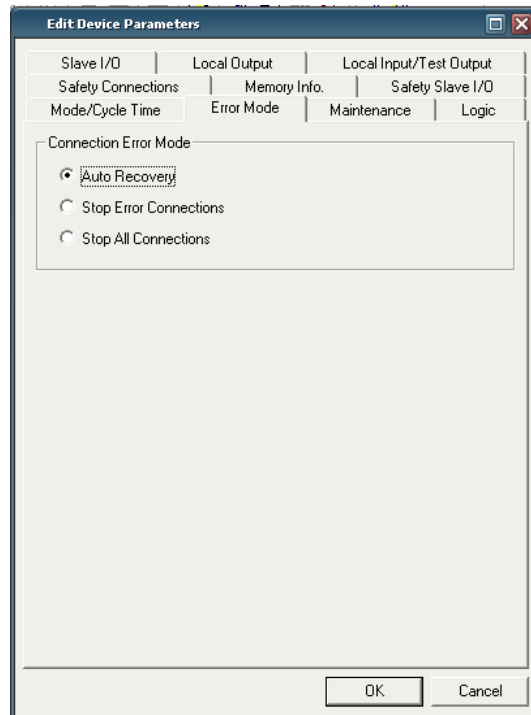
Under normal conditions, it will be set by Network Configurator automatically.

5-1-3 Stopping/Restarting Communications after an Error

With Ver. 1.0 and higher Controllers, the user can specify whether to stop or continue I/O communications after the connection times out during safety I/O communications with the safety slave. If I/O communications are stopped because of a timeout error, the communications can be restarted from the logic program or a Programming Device.

Setting the Operating Mode after a Communications Error

One of the following modes can be selected to specify the Controller's operation when there is a connection timeout during safety I/O communications with the safety slave.



Mode after communications error	Description
Automatic reset	Specify this mode to re-establish the safety I/O connection with a safety slave after a safety I/O communications error has occurred with the slave. If the cause of the communications error is eliminated, safety I/O communications will restart automatically.
Stop only the connection where the error occurred.	Specify this mode to keep safety I/O communications with a safety slave stopped after a safety I/O communications error has occurred with the slave. To restart safety I/O communications with the safety slave after I/O communications have been stopped, use the Network Configurator to send a command to restart communications. It is also possible to write a logic routine in the logic program in advance to turn ON the Safety I/O Communications Restart Flag and restart communications with a specified trigger bit.
Stop all connections	Specify this mode to stop safety I/O communications with all safety slaves stopped after a safety I/O communications error has occurred. To restart safety I/O communications with the safety slaves after I/O communications have been stopped, use the Network Configurator to send a command to restart communications. It is also possible to write a logic routine in the logic program in advance to turn ON the Safety I/O Communications Restart Flag and restart communications with a specified trigger bit.

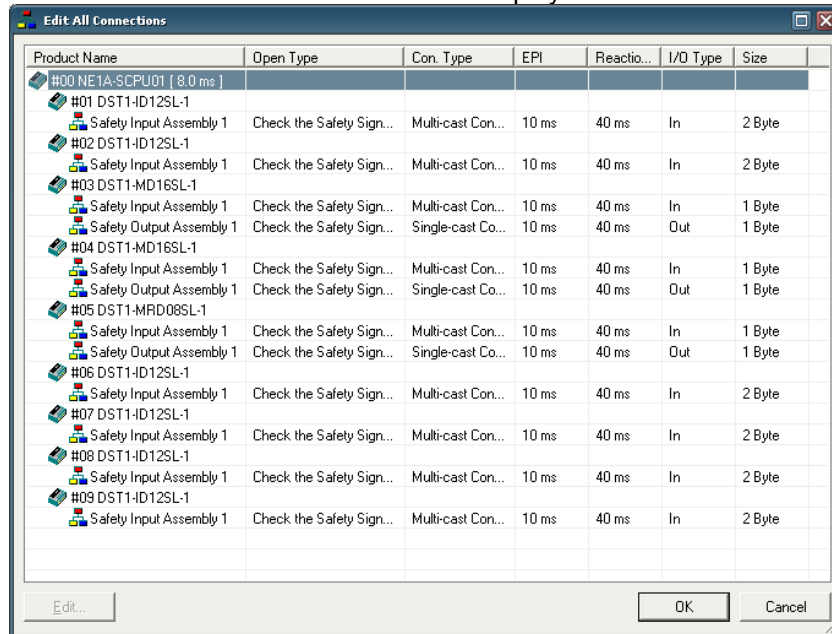
5-1-4 Listing and Setting Connection Parameters

The connection data currently set for all devices can be displayed in the Edit All Connection Window and parameters can be changed. New connections, however, cannot be created and existing connections cannot be deleted.

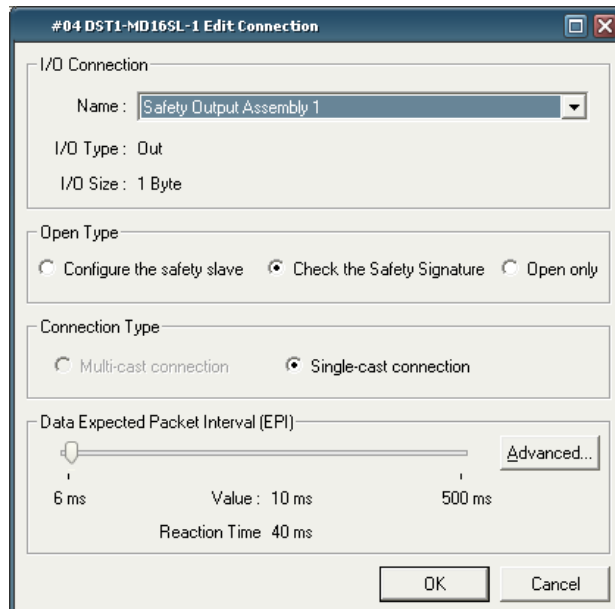
Connection parameters can be efficiently changed from the Edit All Connection Window.

1 Select **Network – Edit All Connection**.

The Edit All Connection Window will be displayed.



2 Double-click the connection in the list for which the settings are to be changed.
The Edit Connection Dialog Box will be displayed.



Refer to 5-1-2 *Setting Safety Connection Parameters* for information on how to use the Allocate Connections Dialog Box.

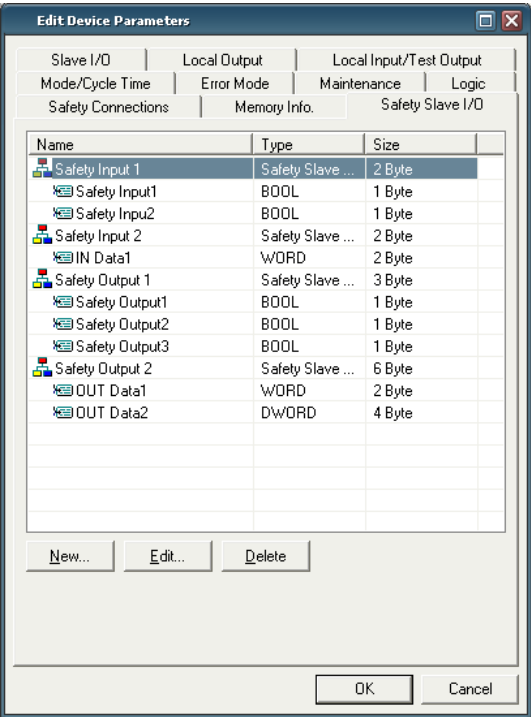
5-2 Safety Slave Settings

Clicking the **Safety I/O Target** Tab displays the setting window of the I/O assembly for the Safety Slave that is necessary to operate the NE1A-series Controller as a Safety Slave. The I/O assembly set here is displayed and can be selected in the Connection Setting Window of the NE1A-series Controller that is functioning as a Safety Master. The I/O tags can be used in the Logic Editor.



Note: **When the NE1A-series Controller is not used as a Safety Slave, it is not necessary to set the parameters in this window.**

5-2-1 Registering I/O Assemblies for Safety Slaves

Register the I/O assemblies for the Safety Slave to be used when the NE1A-series Controller functions as a Safety Slave.



The following information is displayed in this window.

Item	Information Displayed
Name	The registered I/O assembly name ( icon) and the I/O tags name defined in the assembly ( icon) are displayed.
Type	The input/output type for the I/O assembly and the data types for the I/O tags are displayed.
Size	The I/O assembly size and the sizes of the I/O tags are displayed.

You can add, change, and delete I/O assemblies for the Safety Slave in this window. Up to four I/O assemblies can be registered.

- To add an I/O assembly, click the **New** Button. The I/O Assembly Setting Window will be displayed. Define the I/O assembly data referring to 5-2-2 *Setting Assembly Data*.
- To change the data of the I/O assembly, select the I/O assembly you want to change and click the **Edit** Button. The I/O Assembly Setting Window will be displayed. Change the I/O assembly data referring to 5-2-2 *Setting Assembly Data*.
- To delete the I/O assembly, select the I/O assembly you want to delete and click the **Delete** Button.

5-2-2 Setting Assembly Data

This section describes how to define I/O assembly data.

Edit Safety Slave I/O

I/O Type

☒ Safety Slave Input ☐ Safety Slave Output

I/O Tag

Name	Type	Size

New... Edit... Delete...

Status

☐ General Status ☐ Local Input Status

☐ Local Output Status ☐ Test Output / Muting Lamp Status

OK Cancel

I/O Type

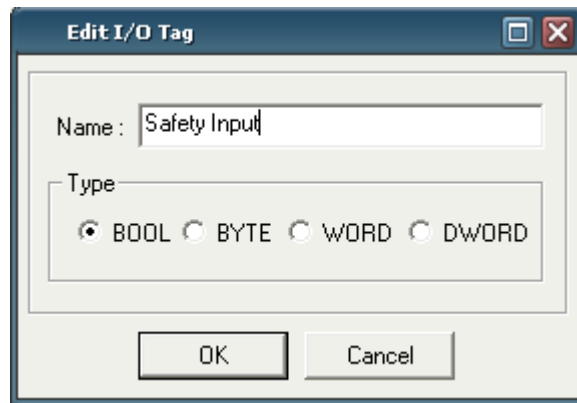
Select the data type to set. The transmission directions for the safety data are as follows:

Safety Slave Input: NE1A-series Controller (Safety Slave) → Safety Master
 Safety Slave Output: Safety Master → NE1A-series Controller (Safety Slave)

I/O Tag

Multiple I/O tags can be defined in an I/O assembly. The I/O tags defined here can be used in the Logic Editor.

- Click the **New** Button and set a tag name and data type when defining a new I/O tag. I/O tags for up to 16 bytes can be defined in each I/O assembly.



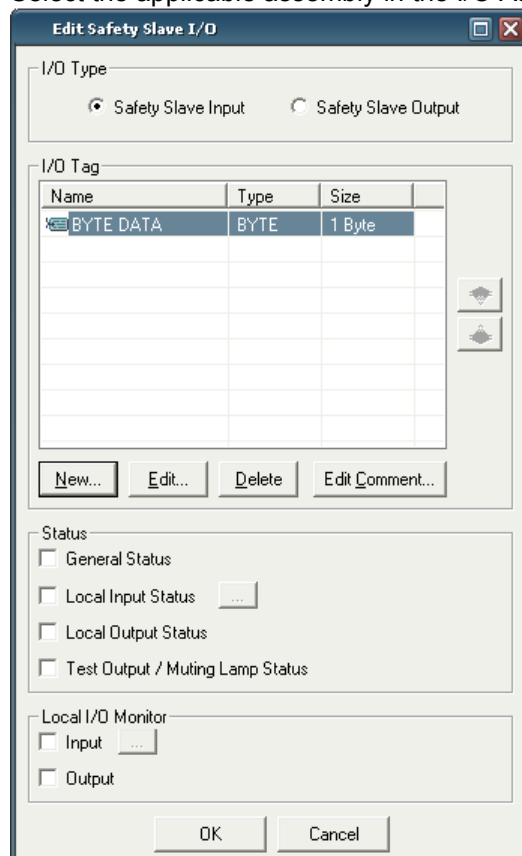
- To change an I/O tag that has already been defined, select the I/O tag you want to change and click the **Edit I/O Tag** Button.
- To delete an I/O tag that has already been defined, select the I/O tag you want to delete and click the **Delete** Button.

Note: BOOL (Boolean) data is 1 byte.

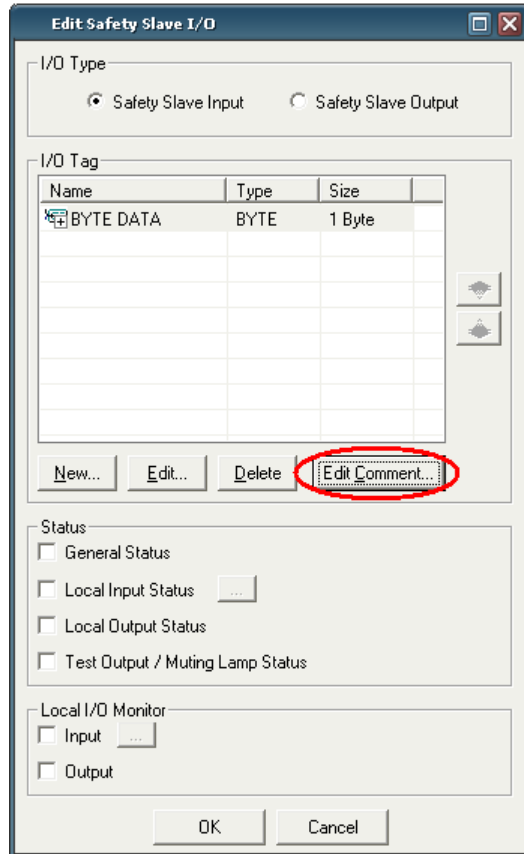
Setting Tag Names by Bit

A tag can be set for each bit with the NE1A series with unit version 1.0 or higher.

Select the applicable assembly in the I/O Assembly Setting Window.



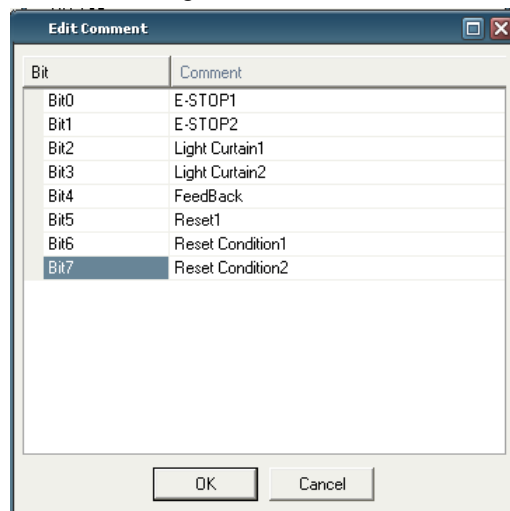
Click the **Edit Comment** Button.



The **Edit Safety Slave I/O** dialog box is shown. It has a title bar with a close button. The **I/O Type** section has two radio buttons: **Safety Slave Input** (selected) and **Safety Slave Output**. The **I/O Tag** section contains a table with columns **Name**, **Type**, and **Size**. The first row is **BYTE DATA**, **BYTE**, and **1 Byte**. Below the table are buttons for **New...**, **Edit...**, **Delete**, and **Edit Comment...** (which is circled in red). The **Status** section has checkboxes for **General Status**, **Local Input Status** (with a button), **Local Output Status**, and **Test Output / Muting Lamp Status**. The **Local I/O Monitor** section has checkboxes for **Input** (with a button) and **Output**. At the bottom are **OK** and **Cancel** buttons.

Name	Type	Size
BYTE DATA	BYTE	1 Byte

1. Edit the I/O Tag.

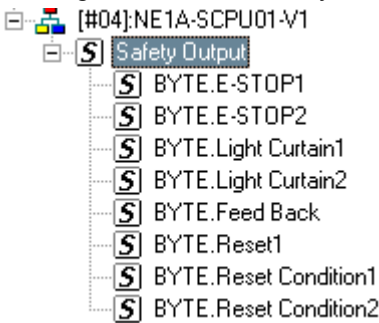


The **Edit Comment** dialog box is shown. It has a title bar with a close button. It contains a table with columns **Bit** and **Comment**. The rows are:

Bit	Comment
Bit0	E-STOP1
Bit1	E-STOP2
Bit2	Light Curtain1
Bit3	Light Curtain2
Bit4	FeedBack
Bit5	Reset1
Bit6	Reset Condition1
Bit7	Reset Condition2

At the bottom are **OK** and **Cancel** buttons.

I/O Tags created in this way will be displayed as follows by the Logic Editor:



Status

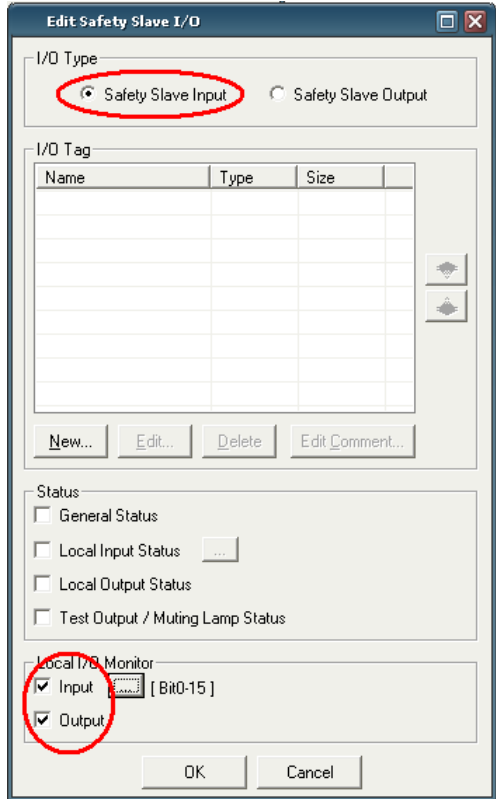
When the I/O type is *Target Input*, the NE1A-series Controller status information can be included in the I/O assembly. The following tag names are automatically used for the status information:

Status	Tag name
General Status	General Status
Safety Input Status	Safety Input Status
Safety Output Status	Safety Output Status
Test Output/Muting Lamp Status	Test Output/Muting Lamp Status

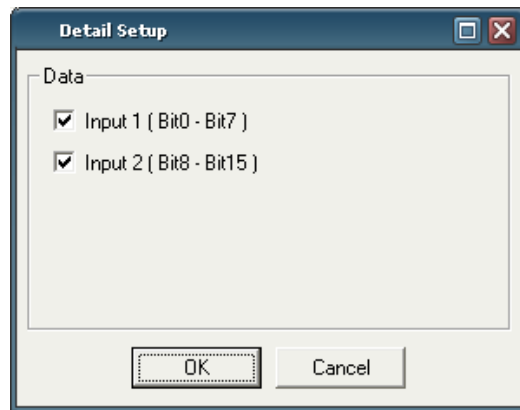
Local I/O Monitor

When the I/O type is *Input*, the NE1A-SCPU01's local I/O information can be included in the I/O assembly.
Use the following procedure.

Check Box in the *Local I/O Monitor* Area.

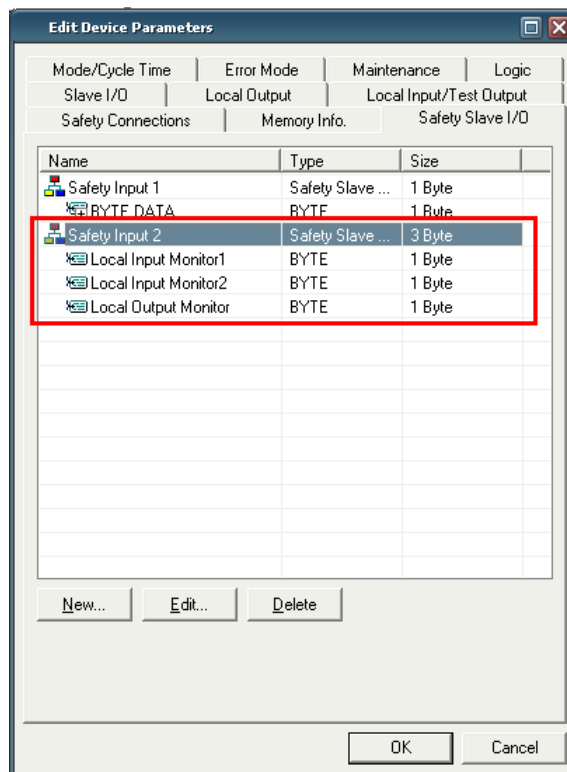


A button will be displayed next to the Input Check Box. The button will be labeled according to the number of input points ("Bit0-15" in the example display). Click this button. The following dialog box will be displayed.

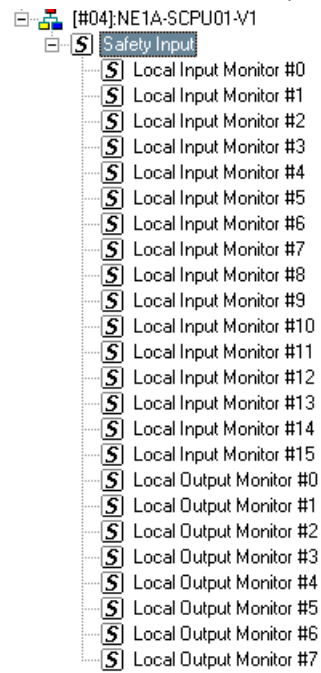


The check boxes that are displayed can be used to specify the data to include in the assembly data.

The local I/O data that has been specified to be included in the assembly data is displayed as shown below.



The local I/O data is displayed in the Program Window as shown below.



5-3 Standard Slave Settings

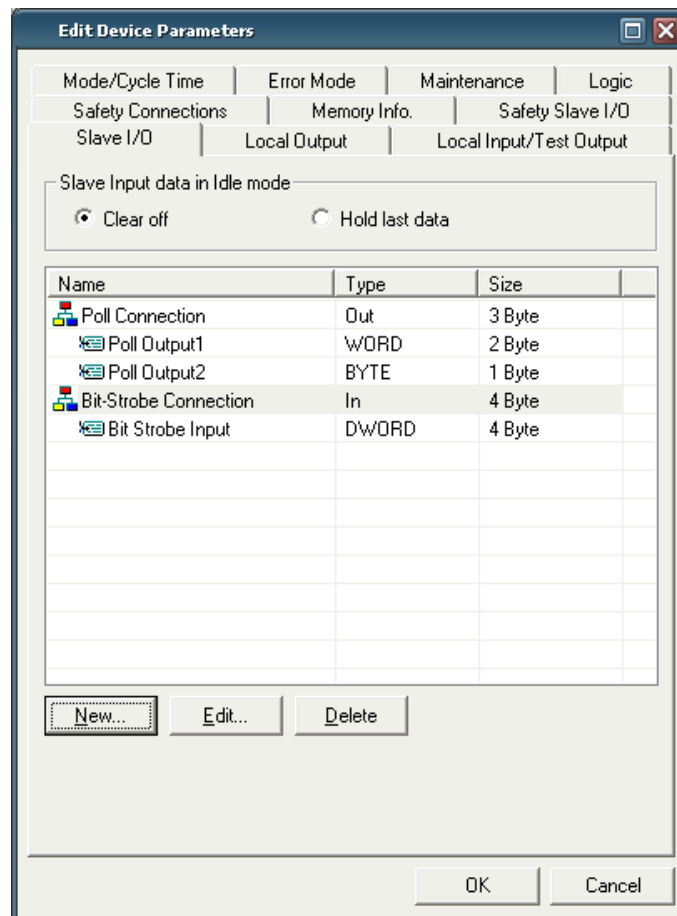
Clicking the **Slave I/O** Tab displays the window for setting a Standard Slave I/O assembly that is necessary for operating the NE1A-series Controller as a Standard Slave. The I/O assembly set here is displayed and can be selected in the Connection Setting Window of, for example, the DeviceNet Unit for a CS/CJ-series PLC that is a Standard Master.

The I/O tags defined in the I/O assembly can be used in the Logic Editor.



Note: When the NE1A-series Controller is not used as a Standard Slave, it is not necessary to set the parameters in this window.

5-3-1 Registering I/O Assemblies for Standard Slaves

Register the I/O assemblies for the Standard Slave to be used when the NE1A-series Controller functions as a Standard Slave.



The following information is displayed in this window.

Item	Information Displayed
Name	The registered I/O assembly name ( icon) and I/O tags name defined in the assembly ( icon) are displayed.
Type	The input/output type for the I/O assembly and data types for the I/O tags are displayed.
Size	I/O assembly size and the sizes of I/O tags are displayed.

You can add, change, and delete I/O assemblies for a Standard Slave in this window. Input assemblies and output assemblies can be registered for each standard connection.

- To add an I/O assembly, click the **New** Button. The I/O Assembly Setting Window will be displayed. Refer to 5-3-3 *Setting Assembly Data* to define the I/O assembly data.
- To change the I/O assembly data, select the I/O assembly you want to change and click the **Edit** Button. The I/O Assembly Setting Window will be displayed. Refer to 5-3-3 *Setting Assembly Data* to define the I/O assembly data.
- To delete the I/O assembly, select the I/O assembly you want to delete and click the **Delete** Button.

5-3-2 Setting Slave Input Data in Idle State

Set to hold or clear the last data for an input assembly that the NE1A-series Controller transmits to the Standard Master in either of the following conditions:

- When changing the NE1A-series Controller from the RUN state to the IDLE state.
- When detecting an error, such as a communications error in a safety chain, that sets the data to an I/O tag in an input assembly.

5-3-3 Setting Assembly Data

This section describes how to define I/O assembly data.

Name	Type	Size

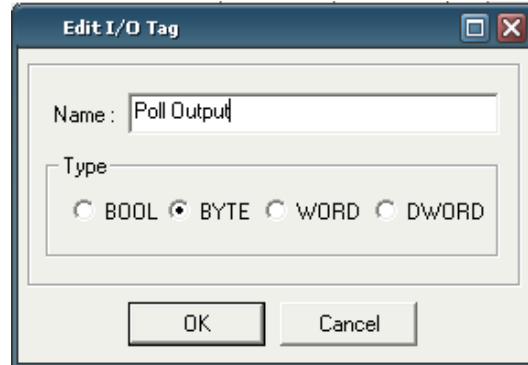
I/O Type

Select the connection type to use for the I/O assembly. Input assemblies and output assemblies can be registered for each connection. Output assemblies cannot be registered, however, when *Bit-Strobe* is selected as the connection type, because the data cannot be output by the Standard Master.

I/O Tag

Multiple I/O tags can be defined in an I/O assembly. The I/O tags defined here can be used in the Logic Editor.

- Click the **New** Button and set a tag name and data type when defining a new I/O tag. I/O tags for up to 16 bytes can be defined in each I/O assembly.



- To change an I/O tag that has already been defined, select the I/O tag you want to change and click the **Edit I/O Tag** Button.
- To delete an I/O tag that has already been defined, select the I/O tag you want to delete and click the **Delete** Button.

Status

When the I/O type is *Input*, the NE1A-series Controller status information can be included in the I/O assembly. The following tag names are automatically used for the status information:

Status	Tag Name
General Status	General Status
Safety Input Status	Safety Input Status
Safety Output Status	Safety Output Status
Test Output/Muting Lamp Status	Test Output/Muting Lamp Status

Setting Bit Tags

With NE1A-series Controllers with unit version 1.0 or later, tags can be set for each bit in the standard assembly, just like they can be for safety assembly.

Local I/O Data

When the I/O type is *Input*, local I/O data for the NE1A-SCPU01 can be included in the I/O assembly, just like it can be in the safety I/O assembly.

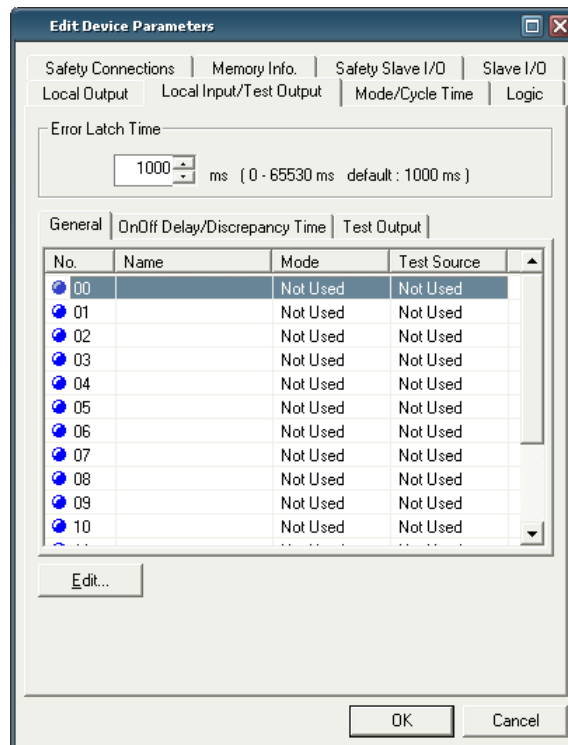
5-4 Local I/O Settings

Click the **Local OUT** Tab or **Local IN/Test Output** Tab to display the NE1A-series Controller's I/O Setting Window.

Note: **All I/O are in the *Not Used* state in the default settings. If you do not use the I/O of the NE1A-series Controller, it is not necessary to set the parameters in this window.**

5-4-1 Setting Safety Inputs

Click the **Local IN/Test Output** Tab and then click the **General** Tab in the window. To configure the safety inputs.



Note: **There are many settings for safety inputs. The display window is thus separated into the General Tab Page and On-Off Delay/Discrepancy Time Tab Page. Safety input scan are set from both tab pages.**

Error Latch Time

This parameter applies to all safety inputs and test outputs. It sets the time to latch the error state when an error occurs in an input or output.

Even if cause of the cause of the error has been removed, the error state is always latched for this time. It can be set between 0 and 65,530 ms in 10-ms increments.

Settings for Individual Safety Inputs

Double-click the row of the safety input to set or select the row and click the **Edit** Button.

Terminal Name

A terminal name can be set for a safety input. The terminal name set here is used as the I/O tag in the Logic Editor.

Channel Mode

Set the Channel Mode for the safety input.

Channel Mode	Description
Not Used	The corresponding safety input will not be used. (It does not connect to an external input device.)
Test pulse from test out	Specifies connecting a device with a contact output in combination with a test output. When this mode is selected, select the test output to use for the <i>Test Source</i> and then set the test output mode to <i>Pulse Test Output</i> . When these settings are made, contact between the input signal line and the power supply (plus) and short circuits with other input signal lines can be detected.
Used as safety input	Specifies connecting a safety device with a semiconductor output, such as a light curtain.
Used as standard input	Specifies connecting a standard device (i.e., a non-safety device).

Test Source

When the channel mode of a safety input is set to *Test pulse from test out*, select the test output to use in combination with the safety input.

The channel mode for the test output selected here is automatically set to *Pulse Test Output*.

Note: **The channel mode of the test output selected here automatically becomes *Pulse Test Output*.**

ON Delay Time and OFF Delay Time

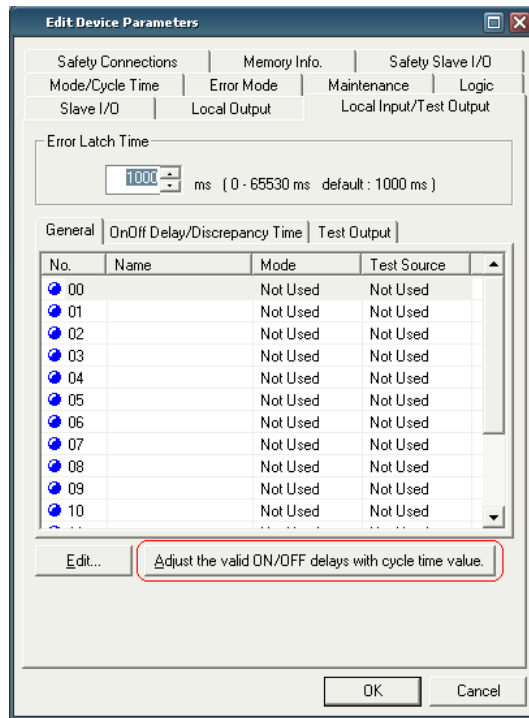
These parameters set the ON delay time and OFF delay time for the safety input. The setting range is 0 to 128 ms, but it must be a multiple of the NE1A-series Controller cycle time. Check the displayed NE1A-series Controller cycle time and determine the set value.

- IMPORTANT:
- **The optimum value for the NE1A-series Controller cycle time is automatically calculated based on the parameter settings and the programs. Therefore, the ON delay time and OFF delay time must be set last.**
 - **Set integral multiples of the cycle time for the ON delay time and OFF delay time. Otherwise, an error will be displayed when the Edit Device Parameters Window is closed.**
 - **Automatic adjustment of ON and OFF delay times can be used with Network Configurator version 1.6□ or higher, as described below.**

Automatic Adjustment of ON and OFF Delay Times

If parameters that affect the cycle time are changed after the ON and OFF delays have been set, it may become impossible to close the Edit Device Parameters Dialog Box due to an error in the parameter settings. If this occurs, the ON and OFF delay times can be readjusted based on the cycle time.

As shown in the illustration below, there is a button on the **Local Input/Test Output** Tab Page for adjusting the effective ON/OFF delay time based on the cycle time. Pressing this button sets all values to be automatically adjusted as a multiple of the cycle time.



Dual Channel Safety Input Mode

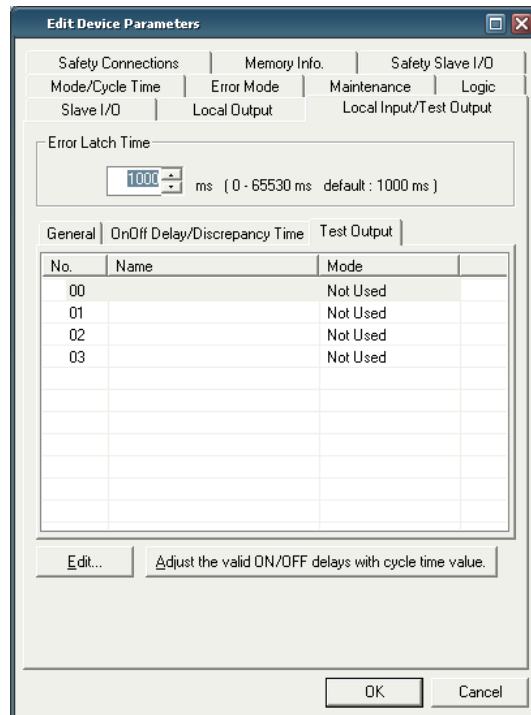
Set the Dual Channel Safety Input Mode and the discrepancy time. The combinations that can be used in Dual Channel Mode are pre-defined.

The discrepancy time can be set between 0 and 65,530 ms in 10-ms increments.

Channel Mode	Description
Single Channel	Specifies using Single Channel Mode. If <i>Single Channel</i> is selected, the Safety Input Terminal to be paired in the Dual Channel setting will also be set to Single Channel Mode.
Dual Channel Equivalent	Specifies using the Dual Channel Equivalent Mode with a paired Safety Input Terminal.
Dual Channel Complementary	Specifies using Dual Channel Complementary Mode with a paired Safety Input.

5-4-2 Setting Test Outputs

Click the **Local IN/Test Output** Tab and then **Test Output** Tab in the window to set the test outputs.

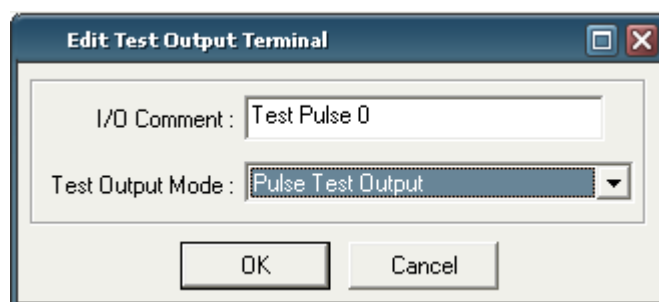


Error Latch Time

The test output is used in combination with a safety input. The same error latch time setting is thus used for all safety inputs. Refer to *Error Latch Time* in 5-4-1 *Setting Safety Inputs*.

Settings for Individual Test Outputs

Double-click the row of the test output number to set, or select the row and click the **Edit** Button.



Terminal Name

Set the terminal name for the test output. The terminal name set here is used as the I/O tag in the Logic Editor.

Test Output Mode

Set the Channel Mode for the test output.

Channel Mode	Description
Not Used	The corresponding Test Output is not used.
Standard Output	Specifies connecting to the input for a muting lamp or PLC. Used as a Monitor Output.
Pulse Test Output	Specifies connecting a device with a contact output in combination with a safety input.
Power Supply Output	Specifies connecting to the power supply terminal of a Safety Sensor. The voltage supplied from the Test Output Terminal to the I/O power supply (V, G) is output.
Muting Lamp Output	Specifies a muting lamp output. (Setting supported only for T3 Terminal.) When the output is ON, disconnection of the muting lamp can be detected.

5-4-3 Setting Safety Outputs

Click the **Local OUT** Tab to set the safety outputs.

Edit Device Parameters

Mode/Cycle Time | Error Mode | Maintenance | Logic
 Safety Connections | Memory Info. | Safety Slave I/O
 Slave I/O | **Local Output** | Local Input/Test Output

Error Latch Time
 1000 ms (0 - 65530 ms default : 1000 ms)

General

No.	Name	Mode
<input checked="" type="radio"/> 00		Not Used
<input checked="" type="radio"/> 01		Not Used
<input checked="" type="radio"/> 02		Not Used
<input checked="" type="radio"/> 03		Not Used
<input checked="" type="radio"/> 04		Not Used
<input checked="" type="radio"/> 05		Not Used
<input checked="" type="radio"/> 06		Not Used
<input checked="" type="radio"/> 07		Not Used

Edit...

OK Cancel

Error Latch Time

This parameter applies to all the safety outputs. It sets the time to latch the error state if an error occurs in a safety output. Even if the cause of the error is removed, the error state will be latched for the time set here. It can be set between 0 and 65,530 ms in 10-ms increments.

Settings for Individual Safety Outputs

Double-click the row of the safety output number to set, or select the row and click the **Edit** Button.

Terminal Name

Set a terminal name for a safety output. The terminal name set here is used as the I/O tag in the Logic Editor.

Safety Output Channel Mode

Set the Channel Mode for the safety output.

Channel Mode	Description
Not Used	The Safety Output Terminal is not used. (External output device not connected.)
Safety	Specifies not outputting the test pulse when the output is ON. Contact between the output signal line and the power supply (positive) when the output is OFF and ground faults can be detected.
Safety Pulse Test	Outputs the test pulse when the output is ON. Contact between the output signal line and the power supply, and short circuits with other output signal lines can be detected.

Dual Channel Safety Output Mode

Set the Dual Channel Safety Output Mode. The combinations that can be used in the Dual Channel Mode are pre-defined.

Channel Mode	Description
Single Channel	Specifies using Single Channel Mode. When <i>Single Channel</i> is set, the Safety Output to be paired in the Dual Channel Mode is also set to Single Channel Mode.
Dual Channel	Specifies using Dual Channel Mode. When both of the Safety Outputs to be paired are normal, the outputs can be turned ON.

5-5 Setting the Operating Mode and Confirming the Cycle Time

Click the **Mode/Cycle Time** Tab to display the NE1A-series Controller operating mode settings and the cycle time.

The screenshot shows the 'Edit Device Parameters' dialog box with the 'Mode/Cycle Time' tab selected. The dialog has a tabbed interface with the following tabs: Safety Connections, Memory Info., Safety Slave I/O, Slave I/O, Local Output, Local Input/Test Output, Mode/Cycle Time (selected), Error Mode, Maintenance, and Logic.

Under the 'Automatic Execution Mode' section, there are two radio buttons:
• **Normal Mode (Need execution command)** (selected)
• Automatic Execution Mode (Automatically execute after power-up)

Below this is a 'NOTE' box:
NOTE
This parameter becomes effective when the device starts with power-up after the download of this configuration.

Under the 'DeviceNet Communication' section, there are two radio buttons:
• **Enable (Normal Mode)** (selected)
• Disable (Stand Alone Mode)

Below this is a 'WARNING' box:
WARNING
If you would like to disable the DeviceNet communication, you can configure it from the USB connection only. If you don't use the USB connection and you select "DISABLE", the download of this configuration will fail.

At the bottom, there are two input fields:
Cycle Time: 7.0 ms
I/O Refresh Cycle Time: 3.5 ms
A 'Change Mode...' button is located to the right of the I/O Refresh Cycle Time field.

At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

5-5-1 Setting the NE1A-series Controller Operating Mode

Automatic Execution Mode

Set the NE1A-series Controller automatic execution mode only after the system has been configured (i.e., after downloading device parameters).

Automatic Execution Mode	Description
Normal Mode	The unit starts in IDLE Mode after the power supply is turned ON. To change to RUN Mode, the operating mode must be changed from the Network Configurator. Use this mode until device parameters have been verified.
Automatic Execution Mode	If this mode is selected and the following conditions exist, the Controller will start in RUN Mode after the power supply is turned ON: <ul style="list-style-type: none"> • The configuration has been locked. • The operating mode before the power was turned OFF was RUN Mode.

IMPORTANT: Even when Automatic Execution Mode is selected and the configuration has been locked, the next startup will not be performed in RUN Mode if the power is turned OFF in IDLE Mode. Turn OFF the power in RUN Mode to use automatic execution.

Setting DeviceNet Communications

When the NE1A-series Controller is used in Standalone Mode, DeviceNet communications can be disabled. If DeviceNet communications are disabled, the cycle time of the NE1A-series Controller will be shortened, but none of the DeviceNet communications functions can be used.

IMPORTANT: When disabling DeviceNet communications, connect the Network Configurator via the NE1A-series Controller's USB port. If the parameters that disabled DeviceNet communications are downloaded while connected via a DeviceNet Interface Card, an error will occur in the Network Configurator because the DeviceNet communications of the NE1A-series Controller will stopped.

5-5-2 Confirming the Cycle Time

Cycle Time

The NE1A-series Controller cycle time is automatically calculated and displayed based on the set parameters and programs created in the Logic Editor. The cycle time is used in calculating the reaction time and the ON/OFF delay time settings. Check the value after all the parameters and programs have been set.

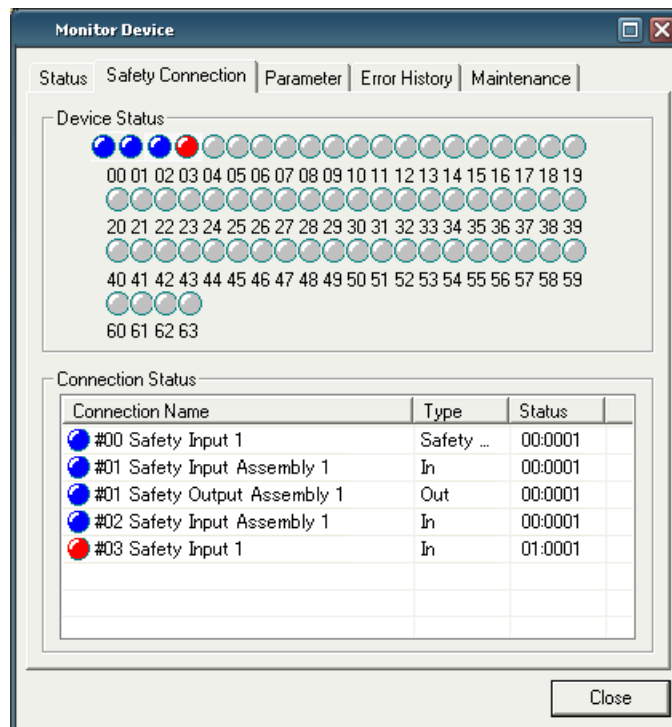
I/O Refresh Cycle

The I/O refresh cycle is used to refresh local I/O. It is automatically calculated with the cycle time and displayed.
The I/O refresh cycle time is used in calculating the reaction time.
Check the value after all the parameters and programs have been set.

5-5-3 Restarting a Connection Stopped due to a Communications Error

When I/O communications have stopped in a connection due to a connection timeout, I/O communications can be restarted in the stopped connection by turning ON the Communications Restart Flag from the logic program or sending a Communications Restart command from the Network Configurator. If the Controller communications mode is set to stop all connections after a communications error, communications cannot be restarted in a specified stopped connection. In this case, restart communications in all connections.

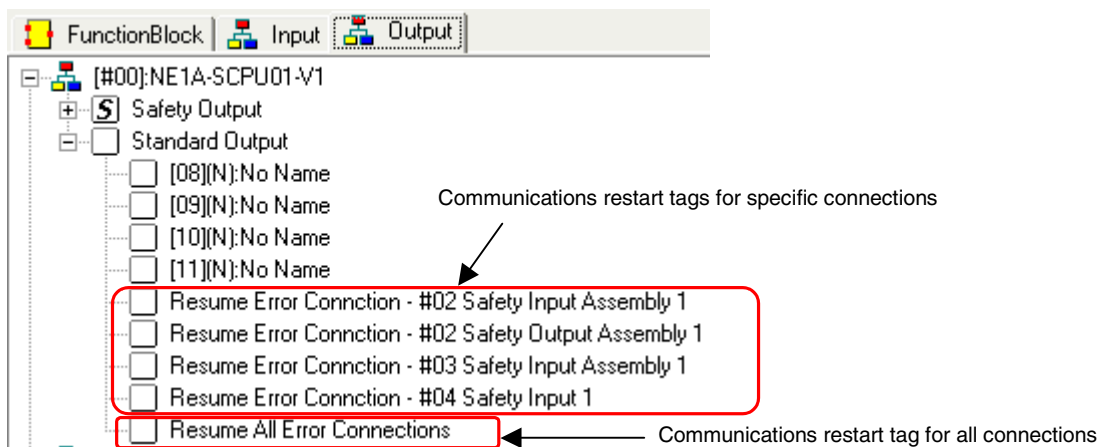
- (1) Restarting I/O Communications from the Network Configurator
After connecting online with the Network Configurator, select the Safety Master, right-click to display the popup menu, and select **Monitor** to display the Monitor Device Window. The following window will appear when the safety connection is selected.



Communications can be restarted in a connection where an error occurred (evident from the connection status) by selecting that connection and clicking the **Resume** Button. If the **Resume All** Button is clicked, I/O communications will restart in all Slaves with which communications were stopped. Retries will be made until communications are restarted.

(2) Restarting I/O Communications from the Logic Program

When the safety connection is set, the following logic program output tags will be displayed for the connection.



When these tags have been set in the logic program in advance as I/O communications restart conditions, I/O communications can be restarted with these tags by turning ON (OFF → ON) the specified condition.

Section 6

Programming the Safety Network Controller

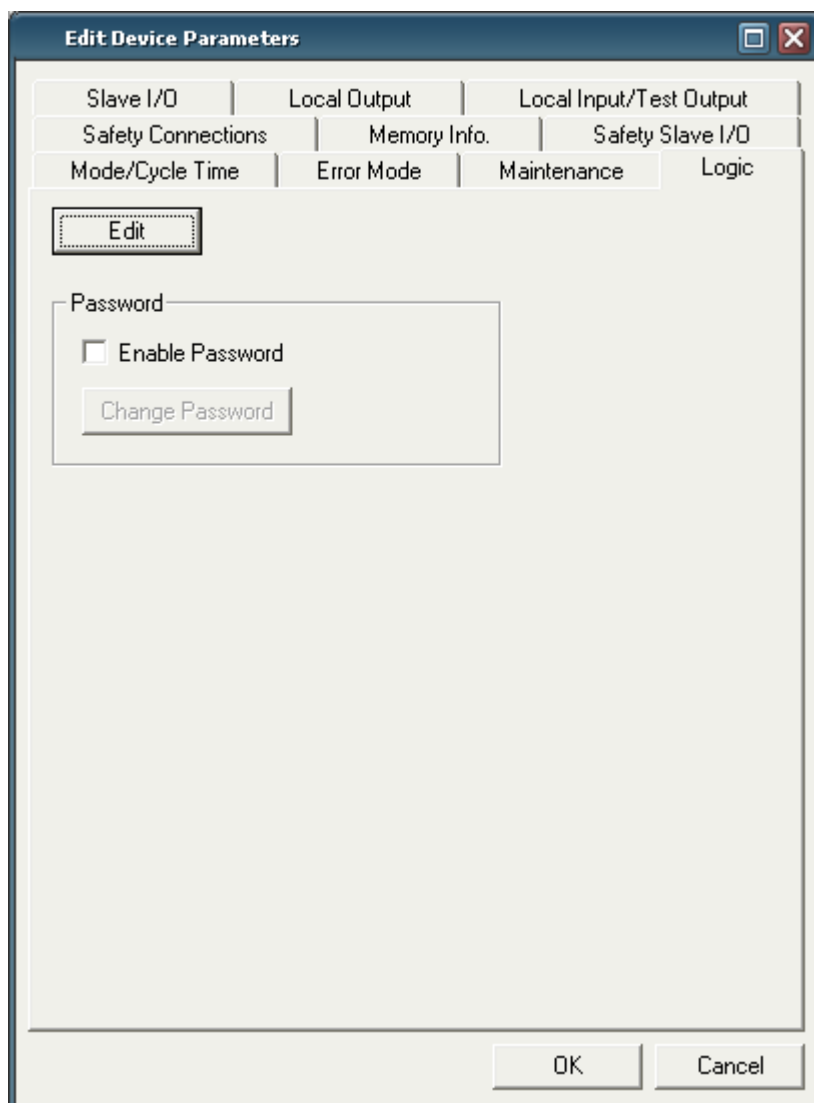
6-1	Starting and Exiting the Logic Editor	150
6-1-1	Starting the Logic Editor.....	150
6-1-2	Exiting the Logic Editor	151
6-2	Menu Commands	152
6-2-1	File Menu	152
6-2-2	Edit Menu	152
6-2-3	View Menu	152
6-2-4	Function Menu	153
6-2-5	Page Menu.....	153
6-2-6	Function Block Menu	153
6-3	Programming	154
6-3-1	Workspace	154
6-3-2	Function Blocks.....	155
6-3-3	Programming Using Function Blocks.....	157
6-3-4	Programming User-defined Function Blocks	170
6-3-5	Password Protection for User-defined Function Blocks	181
6-3-6	Saving the Program	182
6-3-7	Password Protection for Programs	182
6-3-8	Updating the Program.....	184
6-3-9	Monitoring the Program	184

6-1 Starting and Exiting the Logic Editor

6-1-1 Starting the Logic Editor

Use the Logic Editor to program the NE1A-series Controller.
Use the following procedure to start the Logic Editor.

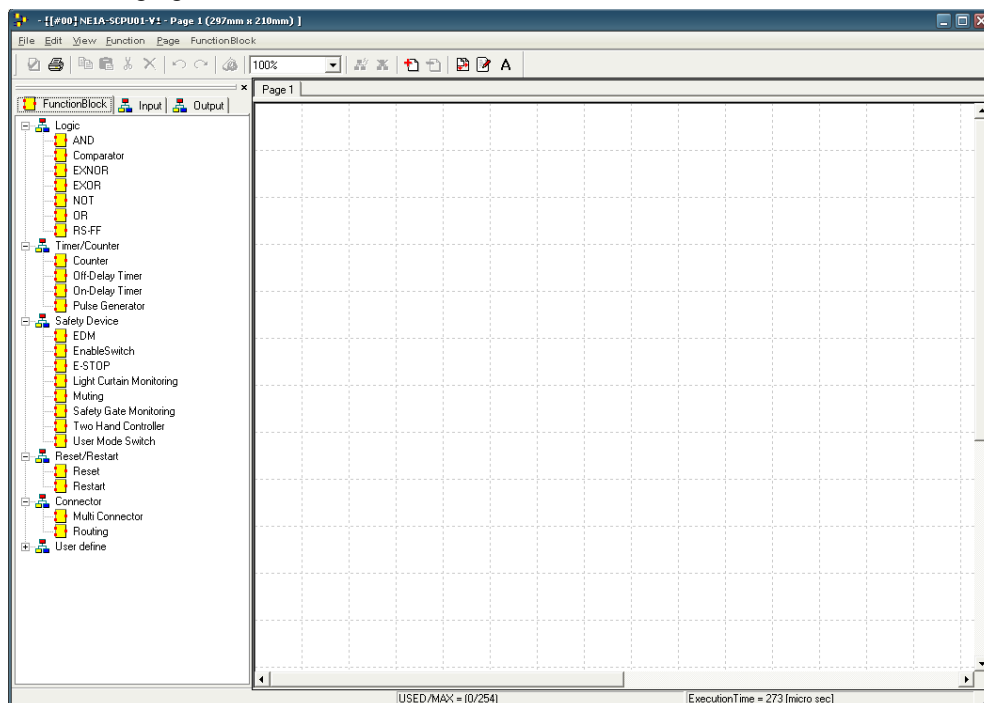
1. Click the **Logic** Tab in the Edit Device Parameters Window of the NE1A-series Controller.



2. Click the **Edit** Button.

The Logic Editor will start, as shown in the following figure.

The Logic Editor consists of the Object List and the Workspace, as shown in the following figure.



6-1-2 Exiting the Logic Editor

Use the following procedure to exit the Logic Editor.

1. Select **Exit** from the File Menu of the Logic Editor.

The Logic Editor will close

2. Click the **OK** Button in the Edit Device Parameters Window.

IMPORTANT:

- To save the program and exit, the user must click the **OK** Button in the Edit Device Parameters Dialog Box when exiting the Logic Editor.
- If the user clicks the **Cancel** Button, none of the parameters entered until then, including the program, will be saved. Any programming saved temporarily by selecting **File - Apply** will also be deleted.

6-2 Menu Commands

The following tables describe the commands in the Logic Editor menus.

6-2-1 File Menu

Command	Description	Online	Offline
Apply	Temporarily saves the current program in the Configurator.	OK	OK
Import	Reads a file saved using the Export Command.	OK	OK
Export	Saves the current program to a file. The user can use the saved file by importing it via another NE1A-series Controller. Connections between I/O tags and function blocks, however, are not saved.	OK	OK
Print	Prints the program.	OK	OK
Page Setup	Sets the page.	OK	OK
Program Title	Sets the title and creator of the program. This information is added when the program is printed.	OK	OK
Exit	Exits the Logic Editor.	OK	OK

6-2-2 Edit Menu

Command	Description	Online	Offline
Cut	Cuts the selected function block and copies it to the clipboard.	OK	OK
Copy	Copies the selected function block to the clipboard.	OK	OK
Paste	Pastes the function block on the clipboard to the Workspace.	OK	OK
Undo	Undoes the previous operation.	OK	OK
Redo	Redoes the undone operation.	OK	OK
Select All	Selects all items.	OK	OK
Delete	Deletes the selected item.	OK	OK
Properties	Displays the property window of the selected function block.	OK	OK
Create Comment	Used to create any size text box by dragging the mouse.	OK	OK
Search Open Connection	Lists function blocks that have open connections. Double-click a function block to display and edit it with the list still displayed. Note: If an error occurs when a program created using version 1.3□ is opened or edited with version 1.5□, use this function to check and make corrections.	OK	OK

6-2-3 View Menu

Command	Description	Online	Offline
Function List	Display or hides the Function List.	OK	OK
Status	Display or hides the status bar.	OK	OK
Tool Bar	Displays or hides the toolbar.	OK	OK
Grid	Used to make grid settings such as display/hide grid, enable/disable grid alignment, and grid width settings. If grid display and alignment are enabled, a grid will appear on the Workspace and function blocks and I/O tags will be grid-aligned when pasted to the Workspace.	OK	OK

6-2-4 Function Menu

Command		Description	Online	Offline
Transmission Message Setting		Sets the explicit message send function.	OK	OK
Monitoring		Monitors I/O tag values and signal states of all the connection lines in the Logic Editor.	OK	---
Jump Address	Make New Jump Address	Creates a new jump address (jump source).	OK	OK
	Select Jump Address	Pastes the destination of the jump address in the Workspace.	OK	OK

6-2-5 Page Menu

Command	Description	Online	Offline
Add Page	Adds a new page after the last page.	OK	OK
Insert Page	Inserts a new page immediately after the currently displayed page.	OK	OK
Delete Current Page	Deletes the currently displayed page.	OK	OK
Change Page Title	Changes the title of the currently displayed page.	OK	OK

6-2-6 Function Block Menu

Command	Description	Online	Offline
Import	Imports a user-defined function block from a function block file (*.fbd).	OK	OK
Export	Exports a user-defined function block to a function block file (*.fbd).	OK	OK
Export All Function Blocks	Groups all user-defined function blocks and exports to multiple function block files (*.fbd).	OK	OK
Create	Creates a new user-defined function block.	OK	OK
Edit	Edits user-defined function blocks.	OK	OK
Delete	Deletes imported user-defined function blocks.	OK	OK
Validate	Checks user-defined function blocks.	OK	OK
Property	Displays/edits user-defined function blocks.	OK	OK

6-3 **Programming**

6-3-1 **Workspace**

First, set the size of the Workspace. Select **File - Page Setup** from the menu bar. The Workspace will consist of pages of the specified size. Pages can be added or deleted as required. When printing the program, each page will be printed at the specified size.

IMPORTANT: The page setup cannot be changed if there are any items in the Workspace. Set the size of the Workspace first using **Page Setup**.

Programming Restrictions

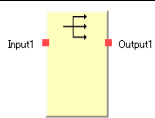
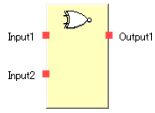
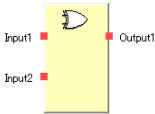
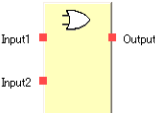
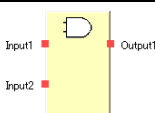

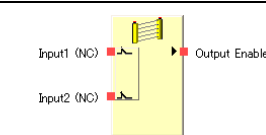
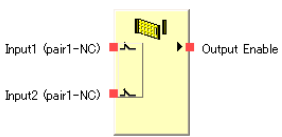
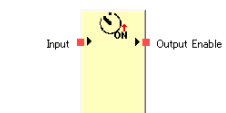
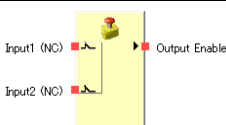
Items, such as I/O tags and function blocks can be used on each page. The following restrictions apply.

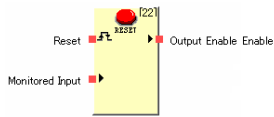
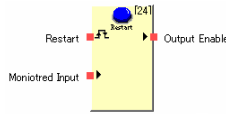
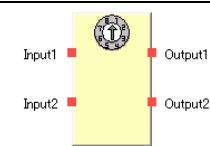
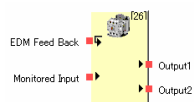
- The same input tag can be placed on more than one page. The same input tag, however, can be used only once on each page.
- Each output tag can be used only once, even on different pages.
- When a function block is pasted, it is placed in the same position as the function block that was copied. When pasting a function block on the same page, move the source function block.
- A maximum of 128 function blocks can be used with Pre-Ver. 1.0 NE1A-SCPU01 Controllers and a maximum of 254 function blocks can be used with NE1A-series Controllers with unit version 1.0 or later.
- A maximum of 128 number jump addresses can be used.
- A maximum of 32 of pages can be used.
- A maximum of 128 text boxes (comments) can be created.

6-3-2 Function Blocks

The Network Configurator can create Safety Logic by combining any logic functions and function blocks supported by the NE1A-series Safety Network Controller. These are listed below.

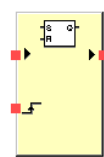
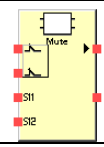
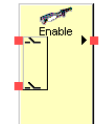
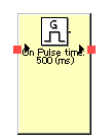
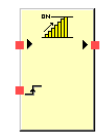
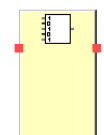
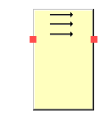
Function Blocks

Name	Notation on Function List	Display on the Network Configurator Logic Editor Screen	Details
Routing	Routing		Allocates an input signal to up to 8 signals. Used for signal outputs to multiple physical addresses (output I/O tags).
Exclusive NOR	EXNOR		Outputs the exclusive NOR of the input conditions.
Exclusive OR	EXOR		Outputs the exclusive OR of the input conditions.
OR	OR		Outputs the logical OR of the input conditions.
AND	AND		Outputs the logical AND of the input conditions.
NOT	NOT		Outputs the logical complement of the input condition.
Two Hand Controller	Two Hand Controller		Monitors Two-hand Switch status.
Light Curtain Monitoring	Light Curtain Monitoring		Monitors Type 4 Safety Light Curtains.
Safety Gate Monitoring	Safety Gate Monitoring		Monitors the safety gate status. The safety gate status is monitored using input signals from safety door switches, safety limit switches, and other switches mounted to the gate.
Off-Delay Timer	Off-Delay Timer		Operates an OFF-delay timer set in 10-ms units.
On-Delay Timer	On-Delay Timer		Operates an ON-delay timer set in 10-ms units.
Emergency Stop Switch Monitoring	E-STOP		Monitors the status of the emergency stop switch.

Reset	Reset		Turns ON the Output Enable signal when the reset signal is correctly input while the input condition for the Reset function block is ON.
Restart	Restart		Turns ON the Output Enable signal when the restart signal is correctly input while the input condition for the Restart function block is ON.
User Mode Switch Monitoring	User Mode Switch		Monitors the operating mode switch for the user system or device.
External device Monitoring	EDM		Evaluates the input signal and external device status and sends a safety output to the external device.

Function Blocks Supported by NE1A-series Controllers with Unit Version

1.0 or Later

Reset Set Flip-Flop	RS-FF		When Input 1 turns ON, RS-FF holds the ON status in the function block and connects to Output 1 for output. Because the ON status is held in the function block, the ON status continues to be output even when Input 1 turns from ON to OFF. When Input 2 is turns ON, the signal held in the function block turns OFF.
Muting	Muting		Temporarily disables the light curtain detection operation when the muting sensor is detected.
Enable Switch	Enable Switch		Monitors enable switch device inputs.
Pulse Generator	Pulse Generator		Outputs ON/OFF pulses on Output 1 while Input 1 is ON.
Counter	Counter		Counts the number of input signals and turns ON Output 1 hen the count reaches the number set in the configuration data.
Comparator	Comparator		Compares input signals (8 max.) with the comparison value set in the configuration, and turns ON Output 1 when all the input signals match the set values.
Multi Connector	Multi Connector		Outputs input signals (8 max.) to output signals (8 max.). The input and output signals correspond 1:1 from 1 to 8 respectively, and are not affected by the status of other input signals.

6-3-3 Programming Using Function Blocks

Improved Operability with Version Upgrade (Version 1.5 or Higher)

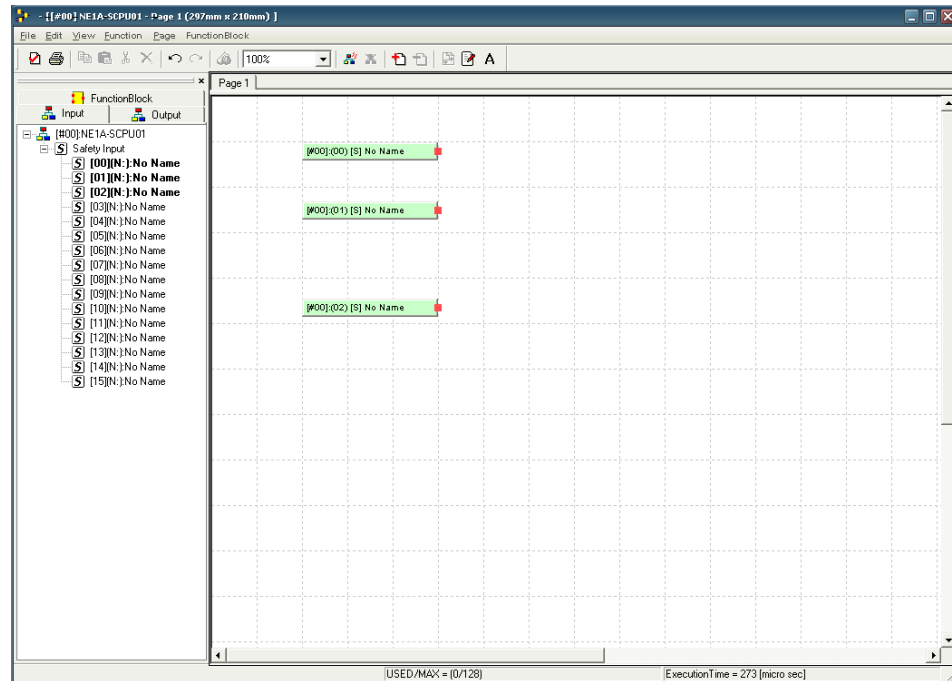
The following operations are possible with Network Configurator version 1.5 or higher.

- Undo/Redo (Edit Menu)
- Copying and Pasting I/O tags, connections, and text boxes (comments) (only function block copying and pasting was possible with earlier versions).
- Cutting I/O tags, connections, text boxes, and jump addresses (only function blocks could be cut with earlier versions).
- Copying function blocks to a location by selecting the function block, holding the Ctrl Key, and drag-and-dropping the function block to that location.
- Select All command added to the Edit Menu.
- Searching I/O tags being used
I/O tags being used in programs can be searched. Double-click the highlighted item in the I/O list in the Object List to display the page in the program where the I/O tag is being used and the I/O tag will appear flashing in red.
- Linking jump addresses
Double-click a jump address to change the display to the corresponding jump address.
- Adding pages after the currently displayed page (pages could be added only after the last page with earlier versions). (Use the Page Menu or right-click the Page Tab.)
- Deleting pages other than the last page (only the last page could be deleted with earlier versions). (Use the Page Menu or right-click the Page Tab.)
- Aligning function blocks, I/O tags, and other object on a grid when pasting. (Select **View – Grid**.)
- Placing text boxes (comments) in the Workspace. (Select **Edit – Create Text Box** then drag the mouse to create the text box area. Double-click the created text box to display the Edit Text Box Dialog Box. Input the comment and click the **OK** Button to write a comment in the text box. To change the comment, double-click the text box to display the Edit Text Box Dialog Box and change the comment in the text box.)
- Displaying function block help. (Right-click the function block in the Object List or the Workspace and select **Help**.)
- Changing the I/O tag color.
Right-click the I/O tag in the Object List or Workspace to display the pop-up menu. Select **Change Color** to change the color.

Note: The Undo command can be used to undo up to the last 5 operations.

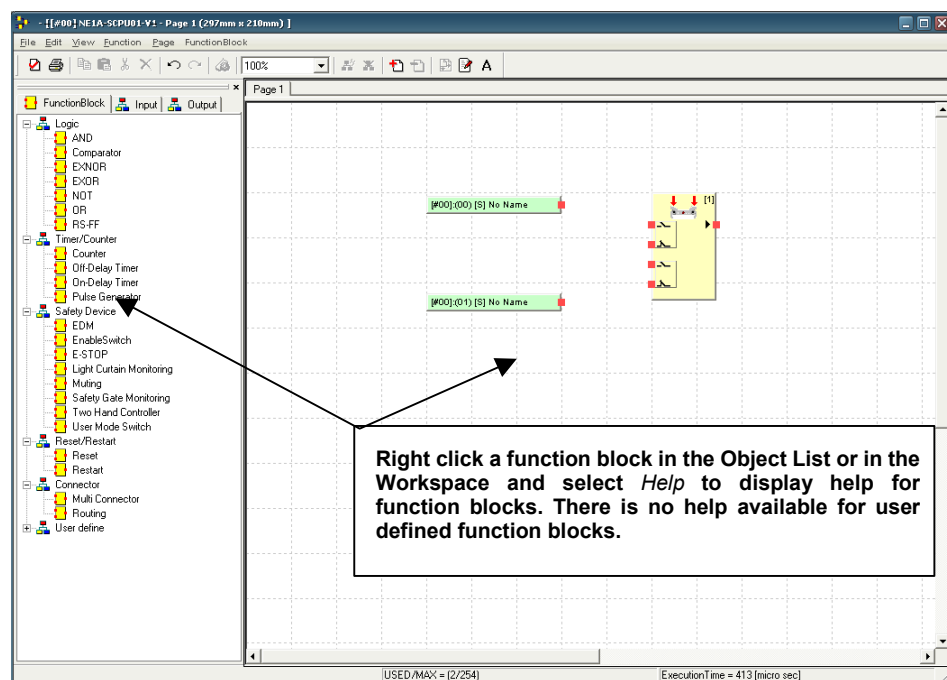
Input I/O Tag Placement

- 1 Click the **Input** Tab in the Object List.
- 2 Select the input I/O tag to be used and drag-and-drop it to the desired location in the Workspace. More than one I/O tag can be selected and drag-and-dropped to the Workspace.



Function Block Placement

1. Click the **Function Block** Tab in the Object List.
2. Select the Function Block to use, drag it to the Workspace, and drop it where you want to position it.

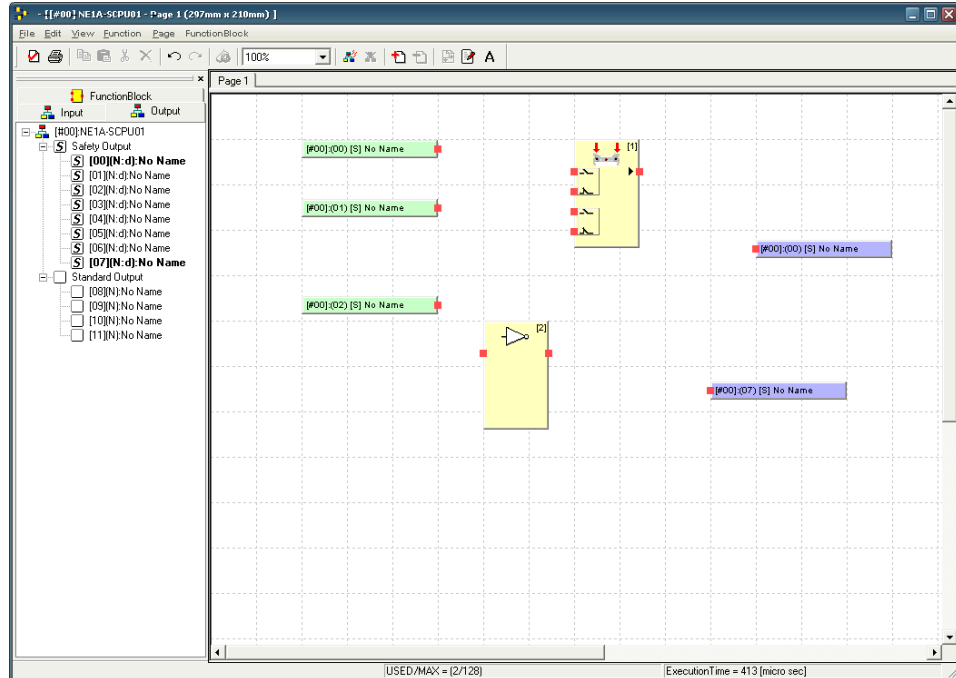


Note: Help can be displayed for function blocks. (Right-click a function block in the Object List or in the Workspace and select **Help**).

Output Tag Placement

1. Click the **Output** Tab in the Object List.
2. Select the output tag to use, drag it to the Workspace, and then drop it where you want to position it.

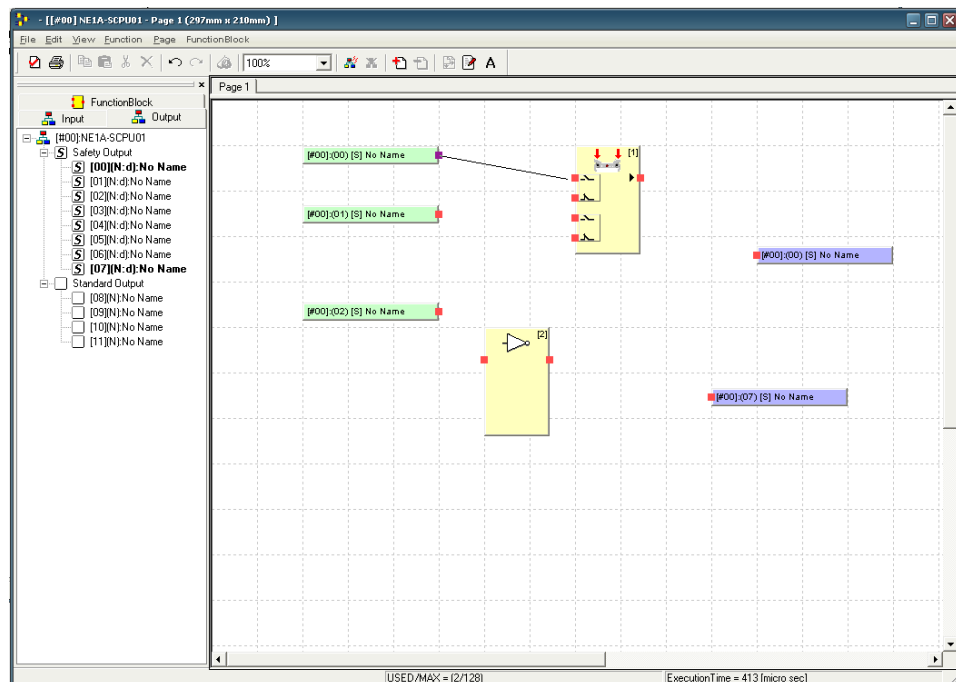
The user can select multiple output tags and position them at the same time.



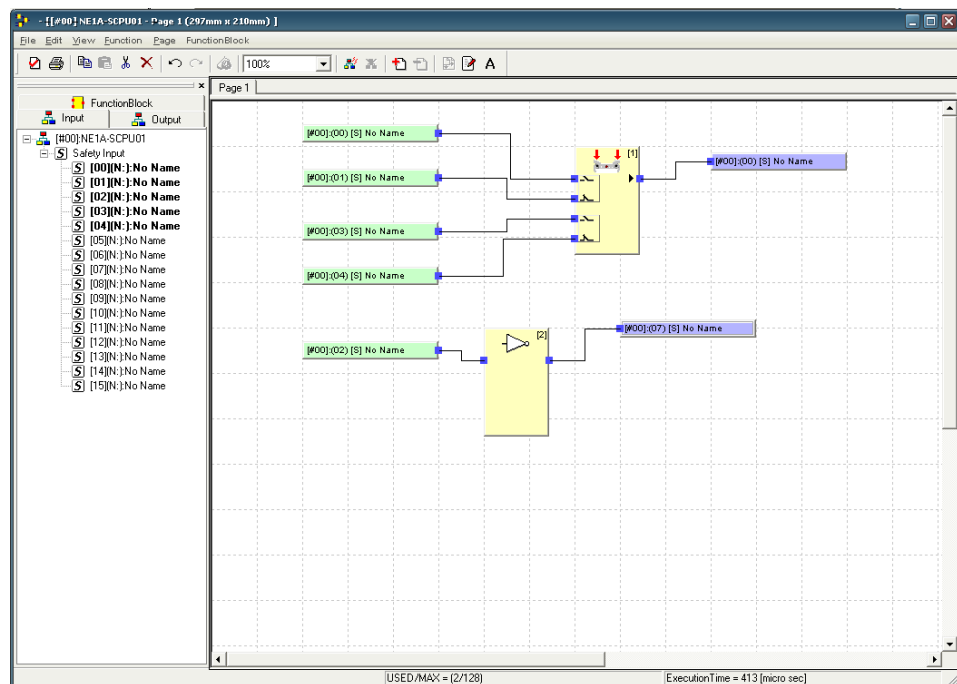
Connections

Connect the I/O tags and the function block.

1. Click the source connector (■) and drag it to the destination connector.



2. Repeat this operation to create the program.



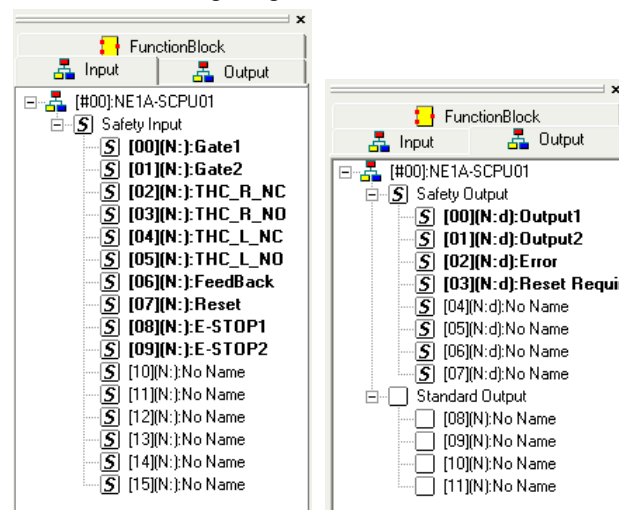
Using I/O Tags

I/O tags can be used for the following when programming.

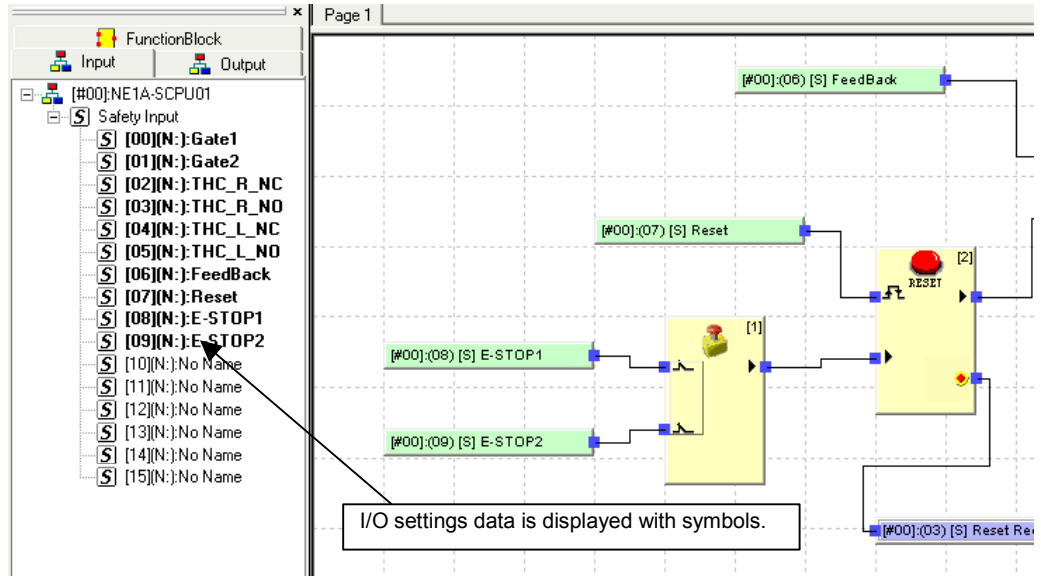
- Local terminals on the local Safety Network Controller (I/O tags set in advance)
- Local terminals for Safety I/O Terminals registered as communications partners (I/O tags set beforehand).
- Local terminals on the local Safety Network Controller (Safety Slaves) for accessing another Safety Master on the network (user-defined I/O tags for assembly data settings)
- Local terminals on the local Safety Network Controller (Standard Slaves) for accessing another Standard Master on the network (user-defined I/O tags for assembly data settings)

The following useful functions for I/O tags are supported in the version upgrade.

- The I/O tags used in the program are highlighted in the Object List, as shown in the following diagram.



- I/O settings are displayed with symbols with the I/O tags in the Object List.



The meanings of the symbols are given in the following tables.

Input mode	Display	Channel mode	Display
Not Used	N	Single	None
Test pulse from Test out	P	Dual Channel Equivalent	e
Used as safety input	S	Dual Channel Complementary	c
Used as standard input	ST	—	—

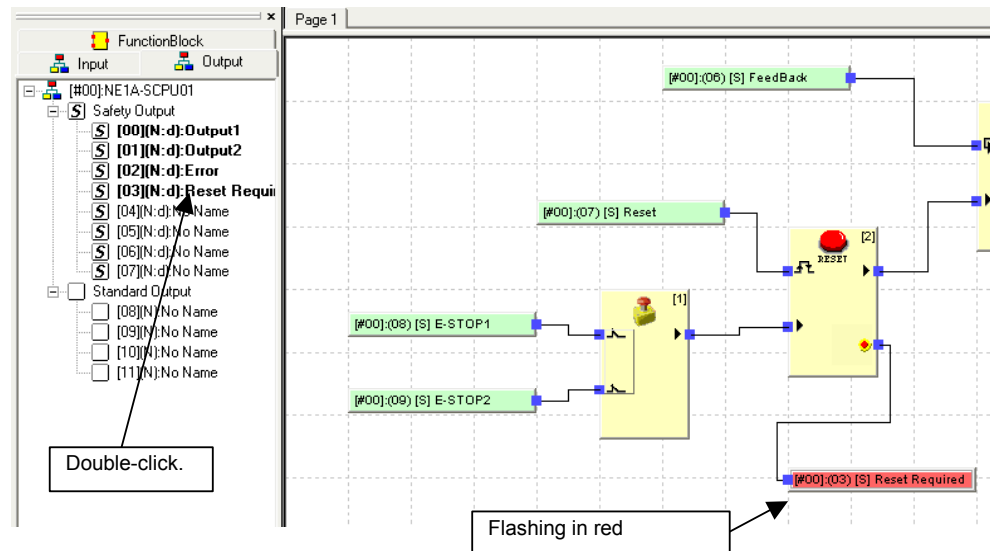
Output mode	Display	Channel mode	Display
Not Used	N	Single	None
Safety	S	Dual	d
Safety Pulse Test	P	—	—

Test Output mode	Display
Not Used	N
Standard input	ST
Pulse Test	P
Power Supply Output	PW
Muting Lamp Output	ML

Note: I/O tags in the program do not have I/O settings data displayed, just whether they are safety I/O or standard I/O.

	Display
Safety I/O	S
Standard I/O	None

- Double-click the I/O tag in the Object List to display the location in the program it is being used.



Note: If an input I/O tag is being used on more than one page, keep double-clicking to change the display to the next page. Click the Workspace or perform any another operation to return to the first page.

Deleting Items

Use any of the following methods to delete I/O tags, function blocks, or connections.

- (1) Select the item to delete and then select **Edit - Delete** from the menu bar.
- (2) Select the item to delete and then click the **Delete** Button on the toolbar.
- (3) Right-click the item to delete and then select **Delete** form the pop-up menu.
- (4) Select the item to delete and then press the **Delete** Key or **Backspace** Key.

Adding and Deleting a Page

Inserting a Page (Adding a New Page between Pages)

Pages can be inserted using either of the following methods. A new page will be added between other pages.

- (1) Select **Page - Insert Page** from the menu bar.
- (2) Right-click the **Page** Tab and select **Insert Page**.

Adding a Page

To add a page, use either of the following methods. A new page will be added after the last page.

- (1) Select **Page - Add Page** from the menu bar.
- (2) Click the **Add Page** Button on the toolbar.

Deleting a Page

To delete a page, use either of the following methods. The currently displayed page will be deleted.

- (1) Select **Page - Delete Last Page** from the menu bar.
- (2) Click the **Delete Page** Button on the toolbar.
- (3) Right-click the **Page** Tab and select **Delete Page**.

Page Title

The user can enter a title for each page. The title can be entered when adding a page, or it can also be entered using either of the following methods:

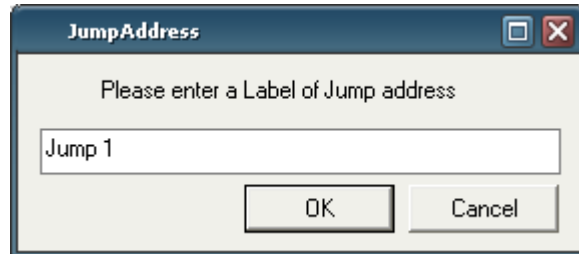
- (1) Display the page for which the title is to be changed and select **Page - Change Page Title** from the menu bar.
- (2) Display the page for which the title is to be changed and right-click the **Page** Tab and select **Change Page Title**.

Jump Addresses

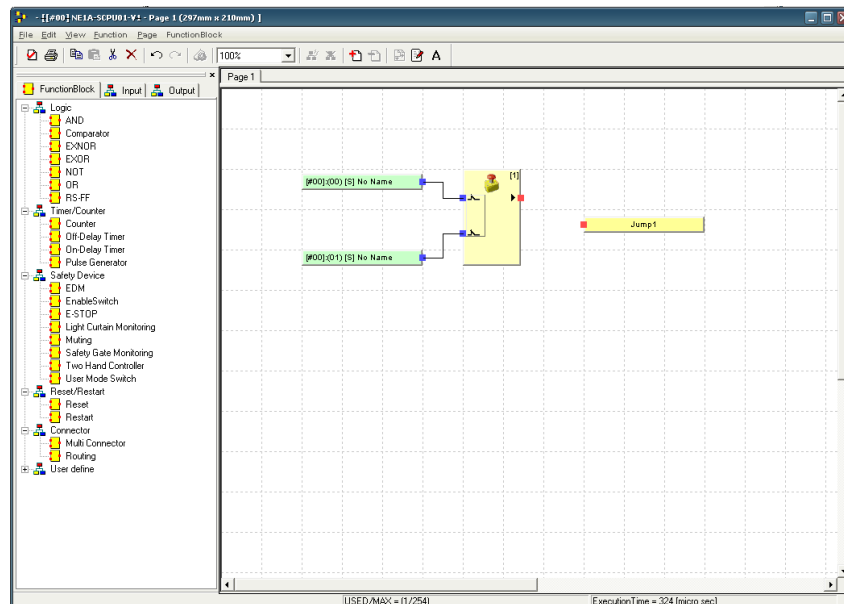
The *Jump Address* menu commands can be used when the program is complex or when it spans multiple pages.

1. First, set the source jump address using either of the following methods:

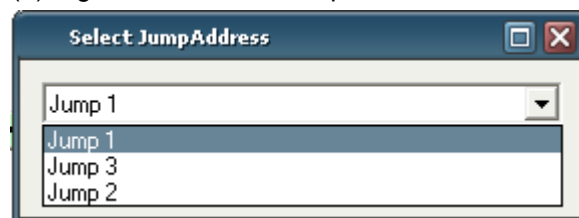
- (1) Select **Function - Jump Address - New** from the menu bar.
- (2) Right-click in Workspace and select **Jump Address**.



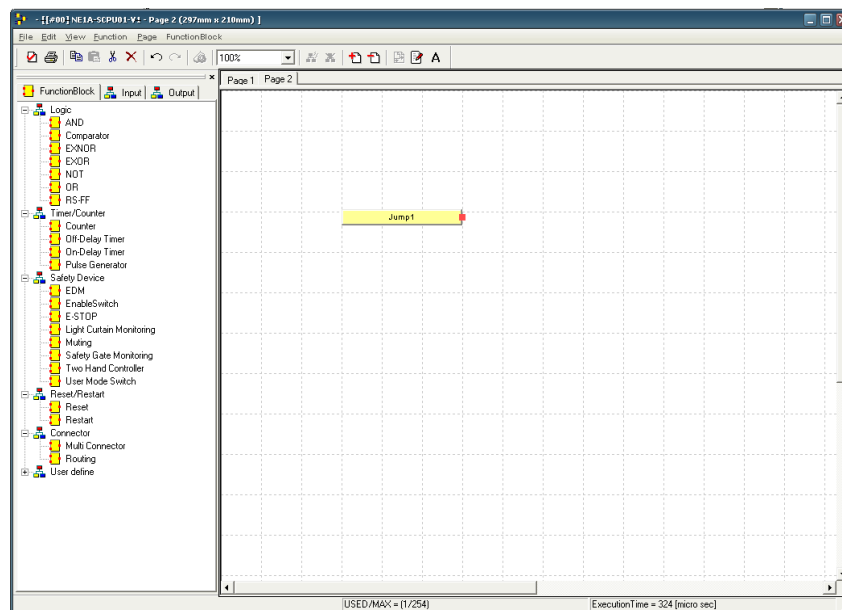
2. Enter a name for the jump address and click the **OK** Button.
The jump address will be displayed as follows:



3. Enter the jump destination using either of the following methods:
 - (1) Select **Menu - Jump Address - Select** from the menu bar.
 - (2) Right-click in the Workspace and select **Select Jump Address**.



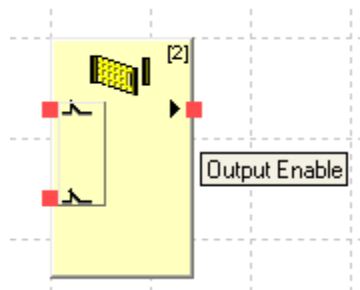
4. Select the name of the jump source and click the **OK** Button.
The jump address will be displayed as follows:



Note: Double-click a jump address to change the display to the corresponding jump address.


Function Block I/O Information

The input and output descriptions for a function block are displayed when the mouse cursor is placed on the corresponding I/O point on the screen.



Editing Function Block Parameters

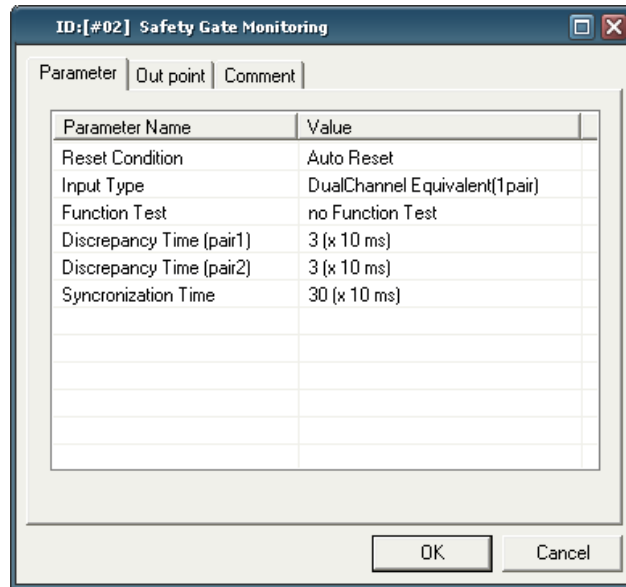
To edit the parameters of a function block, use any of the following methods to display the Parameter Edit Window.

- (1) Double-click the function block.
- (2) Select the function block and then select **Edit - Properties** from the menu bar.
- (3) Right-click the function block and the select **Edit** from the pop-up menu.
- (4) Select the function block and then click  **Property** on the toolbar.

Note: The parameters that can be edited depend on the function block. For details, refer to the *Safety Network Controller Operation Manual (Z906)*.

Parameters

Click the **Parameter** Tab to set the parameters of the function block.

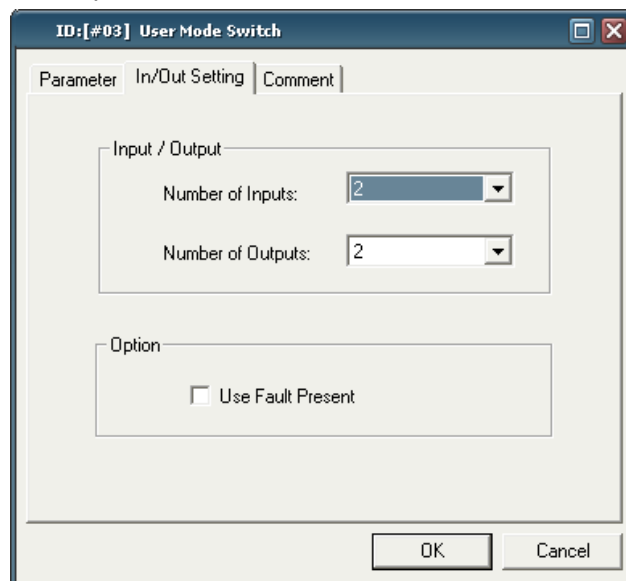


Parameter Name	Value
Reset Condition	Auto Reset
Input Type	DualChannel Equivalent(1pair)
Function Test	no Function Test
Discrepancy Time (pair1)	3 (x 10 ms)
Discrepancy Time (pair2)	3 (x 10 ms)
Synchronization Time	30 (x 10 ms)

OK Cancel

Input/Output Settings

Click the **In/Out Setting** Tab to set the number of inputs or outputs and the *Fault Present* Option.



Input / Output

Number of Inputs: 2

Number of Outputs: 2

Option

☐ Use Fault Present

OK Cancel

Setting Output Points

Click the **Set Output Point** Tab and set whether or not to use the different output point functions for function blocks.

Dialog box: ID: [#04] Two Hand Controller

Parameter | Out point | Comment

Use / Not Use

☒ Output Enable

☐ Discrepancy Error (Pair1)

☐ Discrepancy Error (Pair2)

☐ Fault Present

OK Cancel

Setting Comments

Click the **Comment** Tab to enter names for the function block or I/O signals. The names of I/O signals are not displayed in the window, but the name of the function block is displayed under the function block in the window. The user can select to display or hide all the names entered in this window when the program is printed.

Dialog box: ID: [#05] Restart

Parameter | In/Out Setting | Out point | Comment

Text for FB:

In1: Out1:

In2:

OK Cancel

Sending Explicit Messages

An explicit message can be set in advance and then sent when an output tag turns ON as a trigger. One explicit message can be set for the entire program. Select *Function - User EM* from the menu bar.

Transmission Message

TriggerAddress: [#00]:NE1A-SCPU01 (Bit:00): Output1

Function: ExplicitMessage Client

Retry Count: 52208

Send Message

TargetNode: 00 (Hex) ServiceCode: 00 (Hex)

ClassID: 0000 (Hex) Instance: 0000 (Hex)

Service Data(Hex)

OK Cancel Delete

Trigger Address

Select the output tag to function as the trigger for sending the explicit message. Every time the specified output tag changes from OFF to ON, the explicit message set as the send message will be sent.

Retry Count

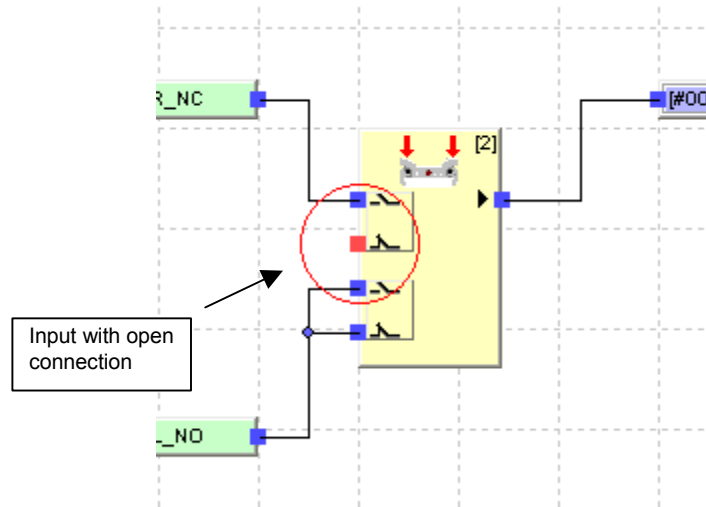
Set the number times sending will be retried if explicit message transmission fails.
Set to 0 for no retries.

Send Message

- **Target Node**
Set in hexadecimal the destination node address to which to send the explicit message.
- **Service Code**
Set the service code of the explicit message in hexadecimal.
- **Class ID**
Set the class ID of the explicit message in hexadecimal.
- **Instance ID**
Set the instance ID of the explicit message in hexadecimal.
- **Service Data**
Set any service data in hexadecimal.

Finding Function Blocks with Open Connections

Newly created programs containing function blocks with open inputs or outputs (see diagram) cannot be downloaded. For this reason, all I/O must be used.



The 'Transmission Message' dialog box has a blue title bar with a close button. It contains the following fields and controls:

- TriggerAddress:** A dropdown menu showing '[#00]:NE1A-SCPU01 (Bit:11): No Name'.
- Function:** A dropdown menu showing 'ExplicitMessage Client'.
- Retry Count:** A text box containing '0'.
- Send Message:** A section with four text boxes:
 - TargetNode:** '00' (Hex)
 - ServiceCode:** '00' (Hex)
 - ClassID:** '0000' (Hex)
 - Instance:** '0000' (Hex)
- Service Data(Hex):** A large text area for entering hex data.
- Buttons:** 'OK', 'Cancel', and 'Delete' at the bottom.

Select **Search Open Connection**. The following dialog box will be displayed.

6-3-4 Programming User-defined Function Blocks

User-defined function blocks are created and used using the following steps.

- Create a user-defined function block.
- Create a program that uses the user-defined function block.
- Check operation of the program that includes the user-defined function block.

User-defined function blocks can be imported and exported and used by other users by following these steps.

- Export/import the user-defined function block.
- Re-use the user-defined function block.

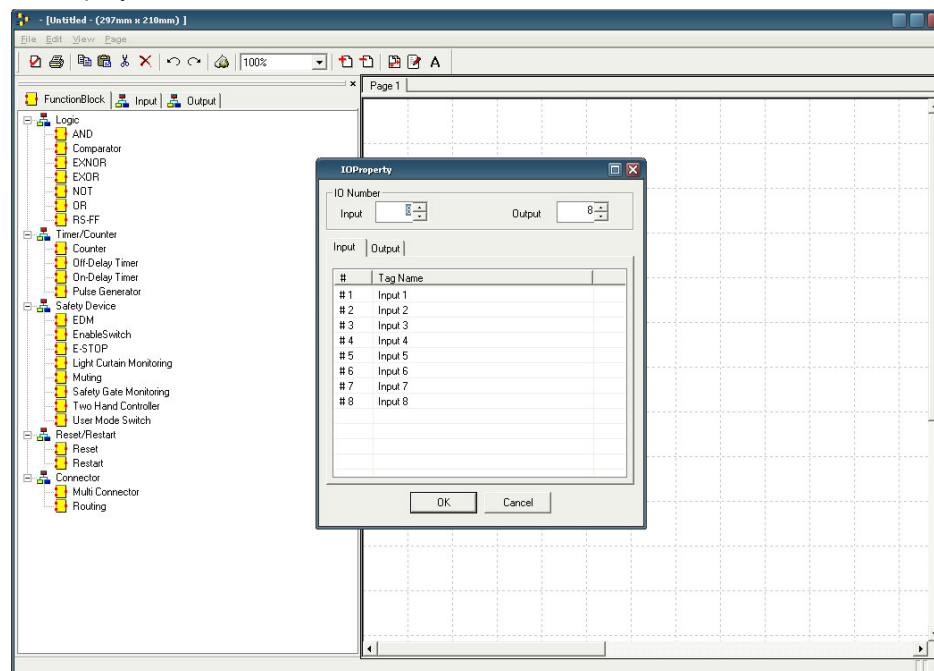
The procedure is described in detail below.

Creating User-defined Function Blocks

Creating a New User-defined Function Block

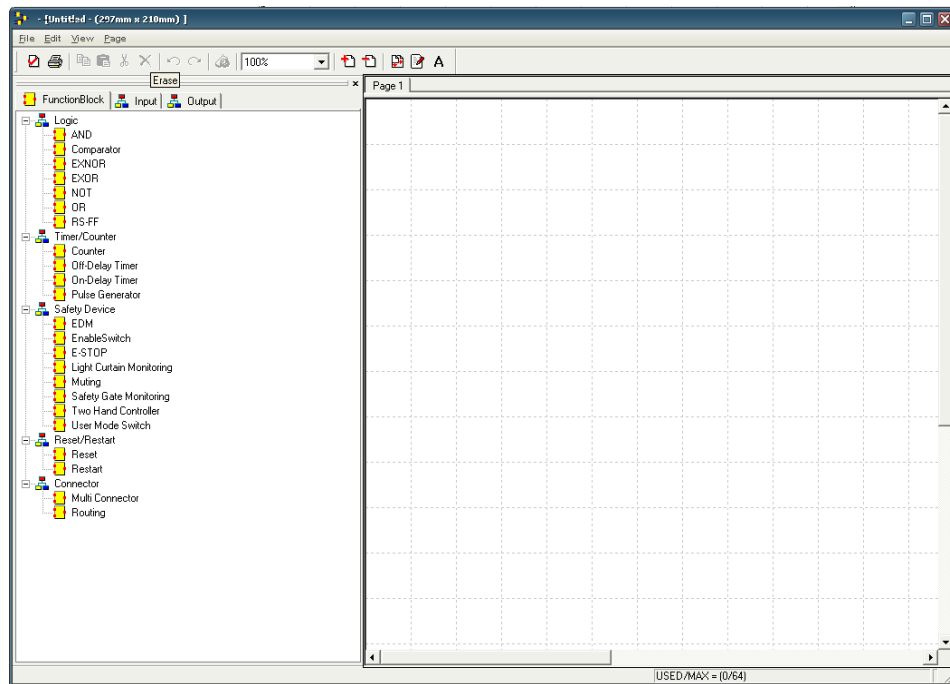
- 1 Select **Function Block – Create** from the Logic Editor Function Block Menu.

The Logic Editor for creating a function block and the IO Settings Dialog Box will be displayed.



- 2 The number of inputs and outputs and the tag name are set in the IO Settings Dialog Box. The tag name can also be set later.

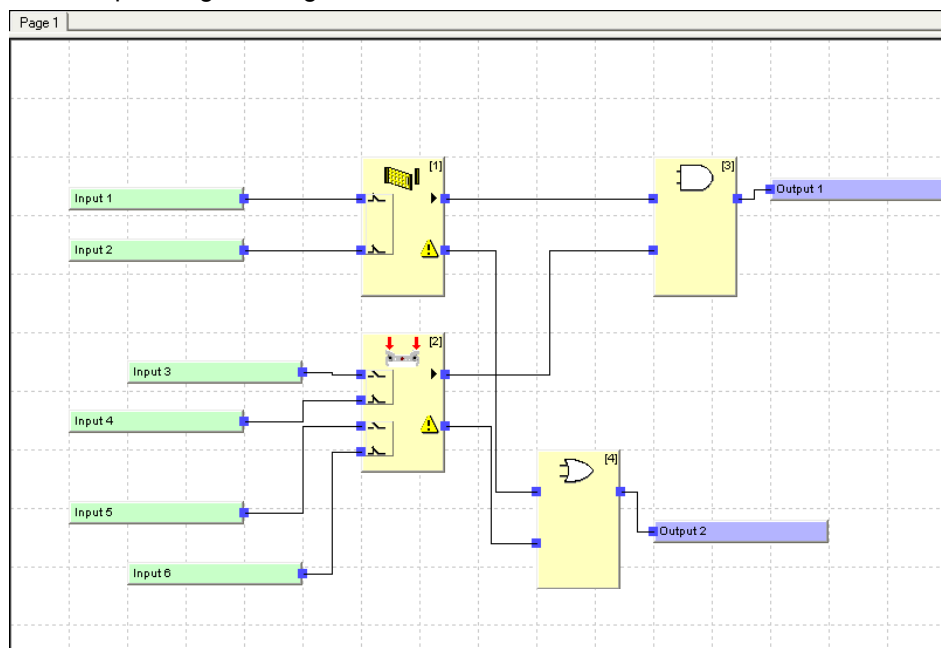
The Logic Editor for creating a function block will be displayed.



- 3 Create the program by placing and connecting function blocks, input tags, and output tags.

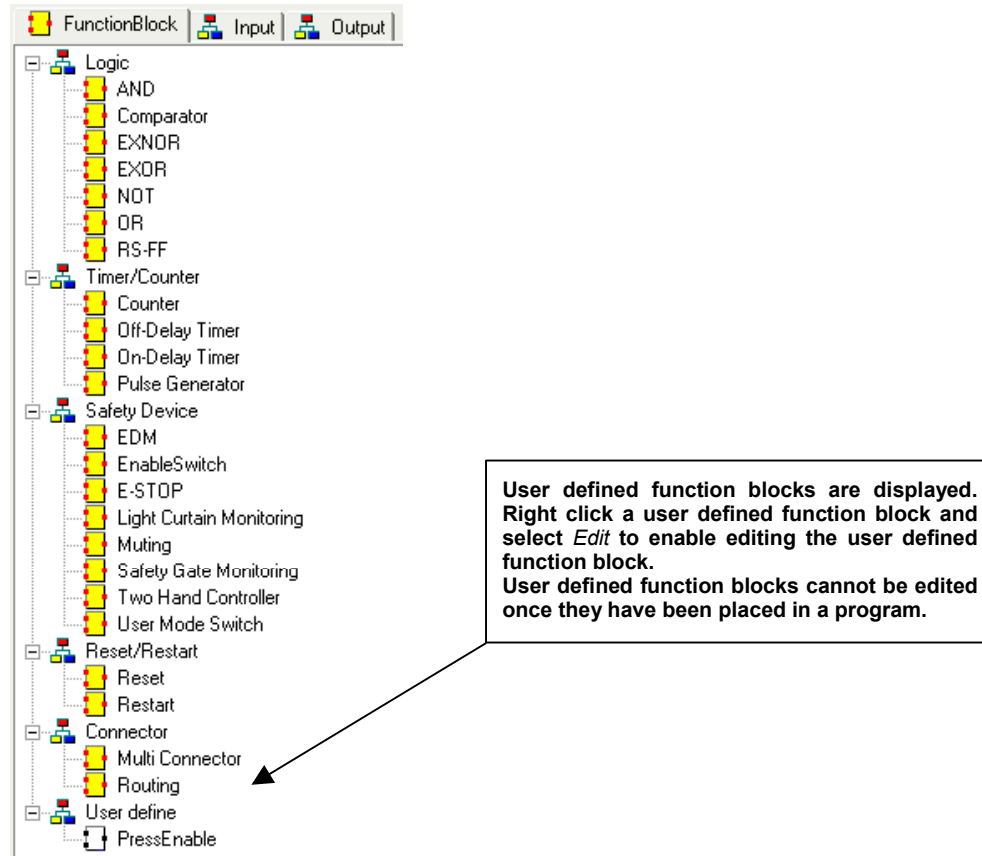
Refer to 6-3-3 *Programming Using Function Blocks* for information on how to use the Logic Editor.

Example Programming a User-defined Function Block:



- 4 Save the user-defined function block.
 - Select **File – Apply** from the Logic Editor menu for creating a user-defined function block.
 - Set the user-defined function block name in the Function Block Name Dialog Box and click the **OK** Button.

The saved user-defined function block will appear on the Logic Editor Object List.
Example screen:

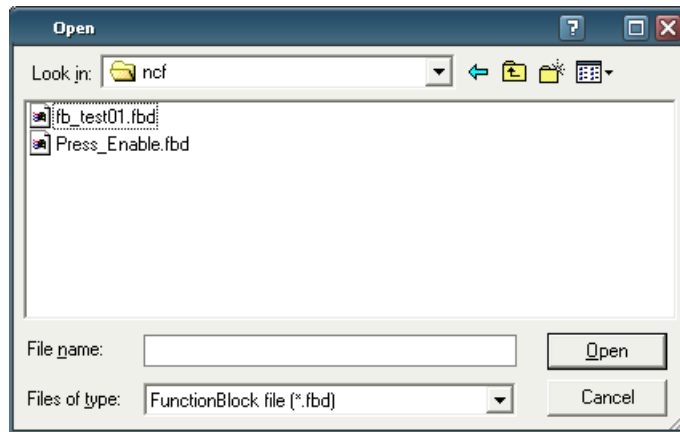


Creating Programs Using User-defined Function Blocks

Importing User-defined Function Blocks

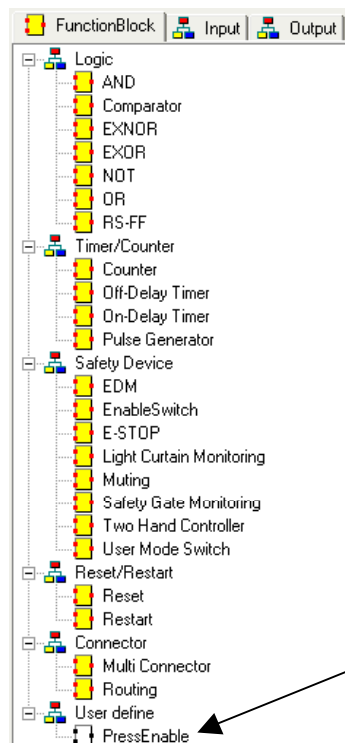
User-defined function blocks must be imported before they can be used in a program. (They do not need to be imported if they are already present.)

- 1 Use the Network Configurator to allocate a new NE1A-series Controller to the network and open the Logic Editor.
- 2 Select **Function Block – Import** from the main Logic Editor menu. The Open File Dialog Box will be displayed.



- 3 Select the file and click the **Open** Button. The imported user-defined function block will be displayed in the Logic Editor Object List.

Example Screen:

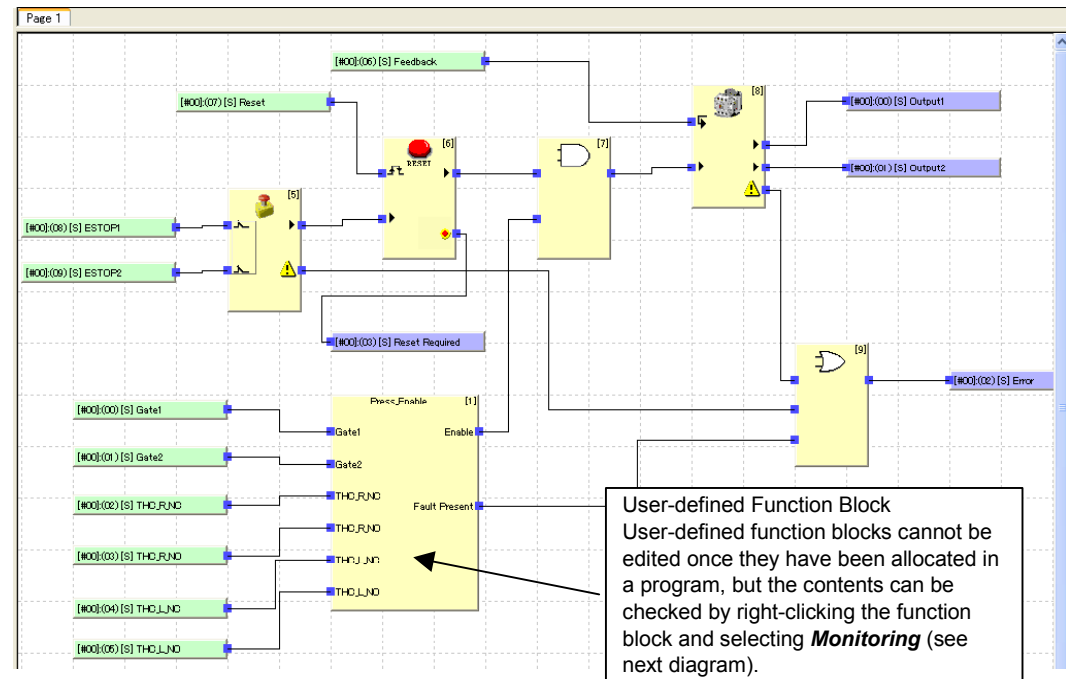


User defined function blocks are displayed. Right click a user defined function block and select *Edit* to enable editing the user defined function block. User defined function blocks cannot be edited once they have been placed in a program.

Allocating User-defined Function Blocks

Imported user-defined function blocks can, like normal function blocks, be selected from the Logic Editor Object List and drag-and-dropped to the Workspace and used.

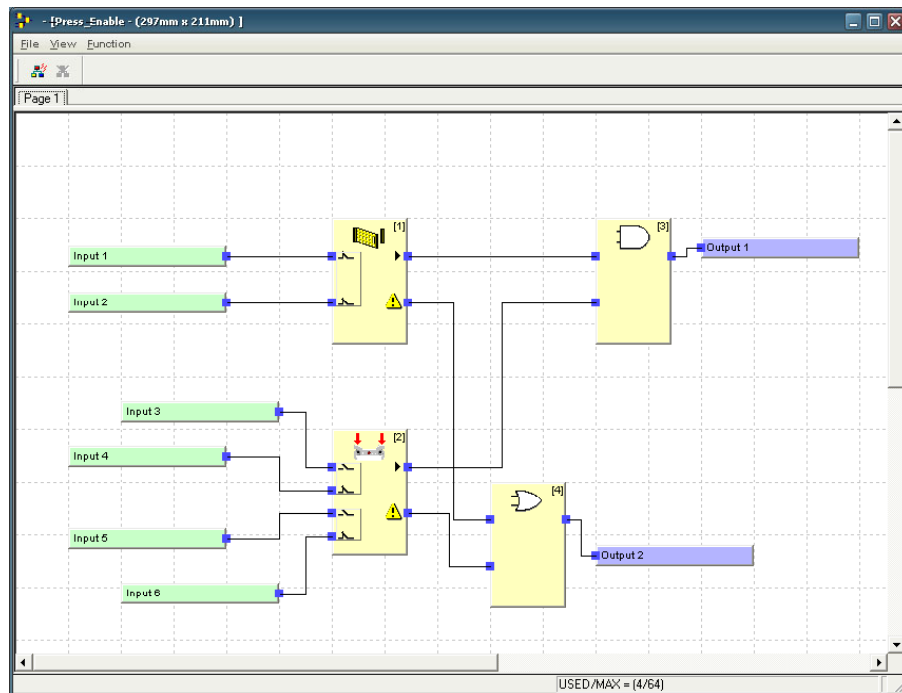
Example of Using User-defined Function Block:



Precautions When Using User-defined Function Blocks

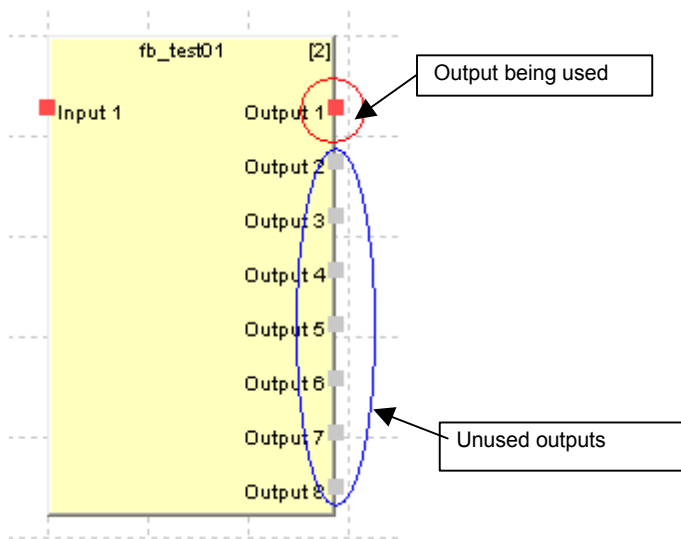
User-defined function blocks cannot be edited once they have been allocated in a program. Editing must be performed while the function block is not being used in a program. To check the contents after allocation, right-click the user-defined function block in the program and select **Monitoring** (see next diagram).

Example Screen Display When User-defined Function Block Is Right-clicked and **Monitoring** Is Selected:



Note: The values for I/O tags in function blocks and the status of signal connections with function blocks can be monitored online if the Network Configurator is online and the NE1A-series Controller is in RUN mode.

The following diagram shows how I/O that are not used in user-defined function blocks are displayed on screen. Used outputs are indicated in red and unused outputs are indicated in gray. Unused I/O connections cannot be connected.



Checking Operation of Programs with User-defined Function Blocks

Always download programs with user-defined function blocks to the NE1A-series Controller and check operation before using them in an application.

Reusing User-defined Function Block Files

Project files (*.ncf files) and user-defined function block files (*.fbd files) exist as separate files. This allows a user to reuse user-defined function blocks created by a different user when creating programs. The procedure to reuse user-defined function blocks is described below.

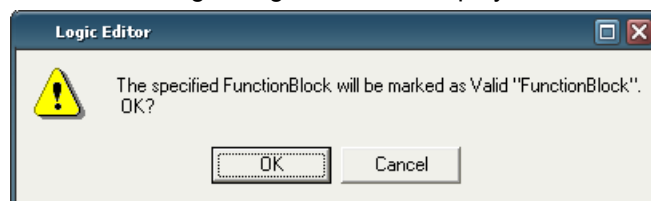
Creating User-defined Function Blocks

Refer to 6-3-3 Programming Using Function Blocks.

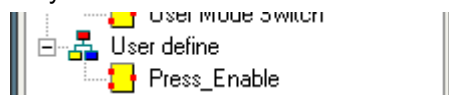
Checking User-defined Function Blocks

Before distributing user-defined function blocks, check the operation and change the user-defined function block status to **Validated**.

- 1 Right-click the imported user-defined function block in the Logic Editor Object List and select **Edit**.
The Logic Editor for creating function blocks will start and the user-defined function block will be displayed.
- 2 Check the user-defined function block program and, if there are no problems, close the Logic Editor (**File – Close**).
- 3 Right-click the imported user-defined function block in the Logic Editor Object List and select **Validate**.
The following dialog box will be displayed.



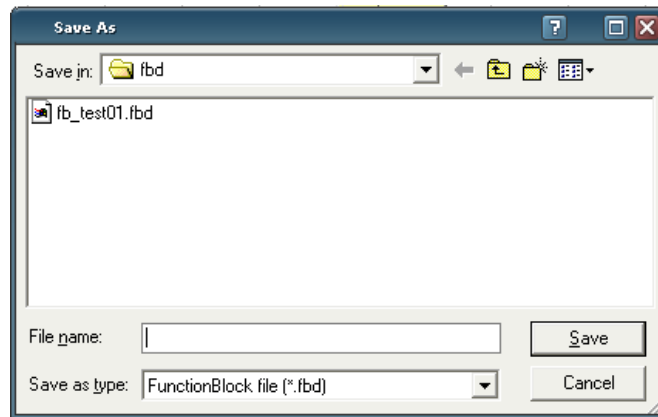
- 4 Click the **OK** Button.
The icon for the checked user-defined function block will change from white to yellow.



Exporting User-defined Function Blocks

A user-defined function block can be exported (i.e., saved as a user-defined function block file).

- 1 Click the saved user-defined function block in the Logic Editor Object List to select it.
- 2 Select **Function Block – Export** from the Logic Editor main menu.
The Save As Dialog Box will be displayed.



- 3 Enter the file name and click the **Save** Button.
The user-defined function block will be saved in a user-defined function block file (*.fbd).

Note: Select **Function Block – Batch Export** to export all user-defined function blocks in a group.

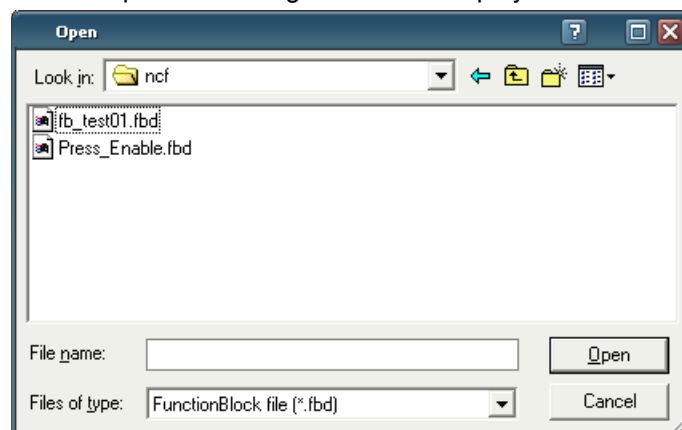
Distributing User-defined Function Block Files

Once the file has been exported, move the saved file to the personal computers on which it is to be reused.

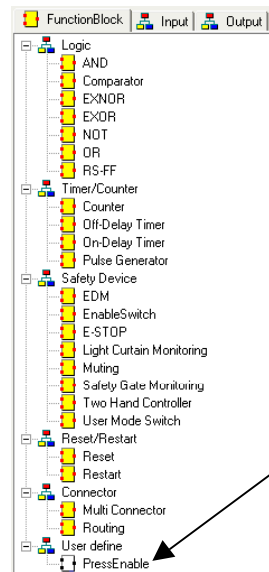
Importing User-defined Function Blocks

A user-defined function block must first be imported before it can be used in a program.

- 1 Use the Network Configurator to allocate a new NE1A-series Controller to the network and open the Logic Editor.
- 2 Select **Function Block – Import** from the Logic Editor main menu.
The Open File Dialog Box will be displayed.



- 3 Select the file and click the **Open** Button.
The imported user-defined function block will be displayed in the Logic Editor Object List.



User-defined function blocks that are no longer required can be deleted.

- 1 Click the user-defined function block to be deleted on the Logic Editor Object List.
- 2 Select **Function Block – Delete** from the Logic Editor main menu.

Note: Deleted user-defined function blocks cannot be restored. Be sure you do not need the function block before deleting it.

Precautions When Using User-defined Function Block Files

Project files (*.ncf files) and user-defined function block files (*.fbd files) exist as separate files. This section describes the relationship between project files and user-defined function block files.

Saving Programs

Apply the program (select **File – Apply**) in Logic Editor to temporarily save data for all function blocks used in a program (including those used inside user-defined function blocks) (see note). This data will include all data required for NE1A-series Controller operation.

Note: Once you exit Logic Editor and click the **OK** Button in the NE1A-series Controllers' Edit Device Parameters Dialog Box, the data will be saved to a project file.

Reading Project Files

Project files can still be read normally even if there are no user-defined function block files.

Downloading Programs

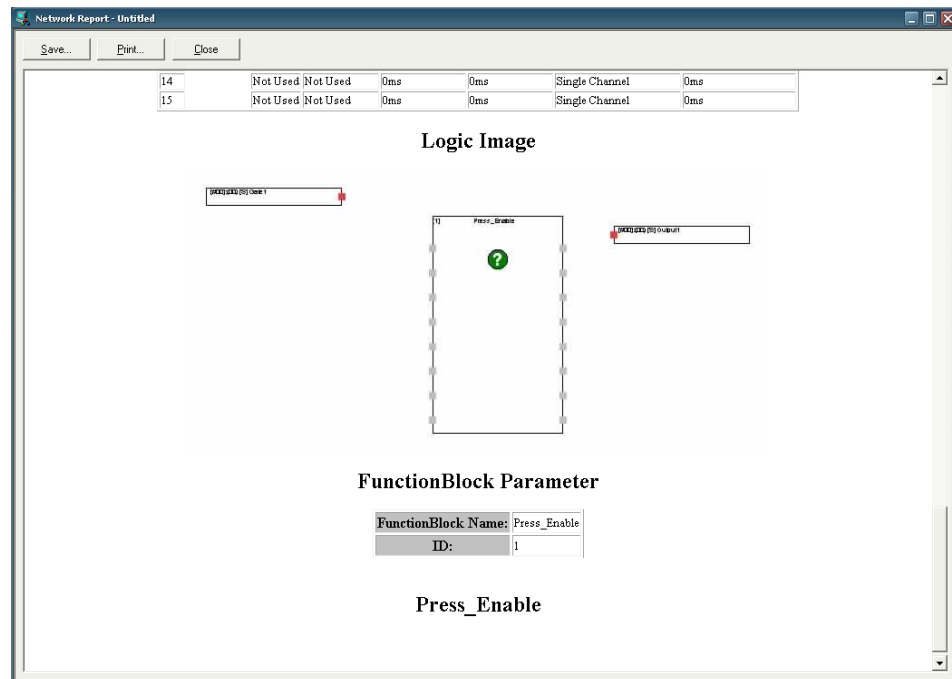
Configurator data can still be downloaded normally even if there are no user-defined function block files.

Uploading Programs

Once programs that include user-defined function blocks have been downloaded to the NE1A-series Controller, they can still be uploaded normally even if there are no user-defined function block files.

Displaying Program Reports

Always import the user-defined function block file before displaying reports. The reports can still be displayed without the user-defined function blocks, but the user-defined function block for that report will appear as a question mark (?), as shown below, and the contents cannot be checked.

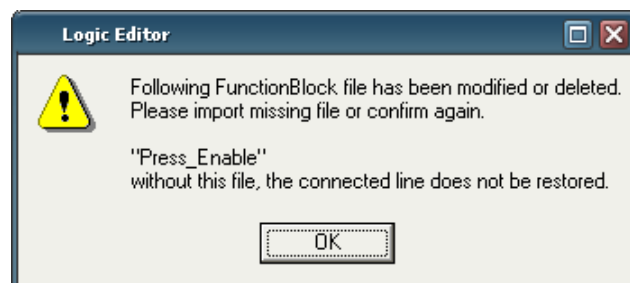


Verifying Programs

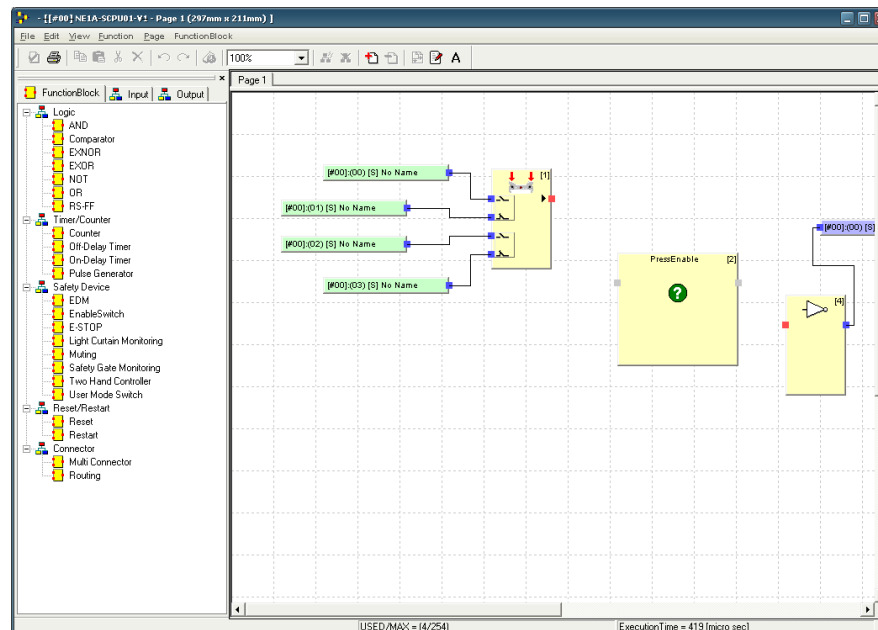
Always import the user-defined function block file before verification. Program verification can be completed even without user-defined function blocks once the program with user-defined function blocks is downloaded to the NE1A-series Controller, but the user-defined function block for that report will appear as a question mark (?) and the contents cannot be checked.

Editing Programs

Programs cannot be edited without the user-defined function block file. Always import the user-defined function blocks before editing. A warning message like the one shown below will appear if the Logic Editor is started without the user-defined function block file.



The following diagram shows how the program will appear if the Logic Editor is started in this status.



A user-defined function block without a file will appear as a question mark (?) and the connections will be deleted. Editing operations (copy, paste, undo, redo, etc.) cannot be used for the user-defined function block. Also, the program cannot be saved or downloaded after editing.

If the user-defined function block file is missing, import the user-defined function block. The program will not be automatically updated, however, if the user-defined function block is imported with the program open. Close the program and open it again to correctly display the user-defined function block.

The following table shows which functions require user-defined function block files and what will happen if the function is executed without the file.

Function	File	Operation
Download	Not required	Operates normally.
Upload	Not required	Operates normally.
Save project file	Not required	Operates normally.
Load project file	Not required	Operates normally.
Verify device	Required	The corresponding user-defined function block image will appear as a question mark (?).
Display report	Required	The corresponding user-defined function block image will appear as a question mark (?).
Edit program	Required	The Edit Program Screen will be displayed but the editing operations (copy, paste, undo, redo, etc.) cannot be executed.
Apply program	Required	Cannot be executed.

Editing User-defined Function Blocks After Creating a Program

If, for example, a user-defined function block called “Sample” was created and used in a new program, and that user-defined function block was edited after the project file containing the new program was saved, the program would not be updated with the edited “Sample” data.

Always check the original program after editing user-defined function blocks.

It is recommended that a password is set for user-defined function blocks to prevent unintended changes.

Note: User-defined function blocks cannot be imported, saved, deleted, checked, or edited by any user (e.g., by a guest account) other than the Windows administrator. Perform these operations immediately after logging in to Windows as the administrator.

6-3-5 Password Protection for User-defined Function Blocks

Passwords can be set for user-defined function block files. The password protection applies to editing and deleting of user-defined function block files. Verify, Report, and Print operations are not password protected.

- 1 Select **File – Change Password**.

The Change Password Dialog Box will be displayed.

A screenshot of a 'Change Password' dialog box. The dialog has a title bar with the text 'Change Password' and standard window control buttons (minimize, maximize, close). Inside the dialog, there are three text input fields labeled 'Current Password', 'New Password', and 'Confirm Password'. The 'Current Password' field is empty. The 'New Password' and 'Confirm Password' fields are also empty. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

- 2 Enter the password in the New Password field (up to 6 alphanumeric characters).
 - 3 Re-enter the password in the Confirm Password field.
 - 4 Click the **OK** Button.
- The program password is now set.

From now on a dialog box requesting the password will be displayed whenever **Function Block – Edit** is selected from the function block list. Unless the set password is entered, the screen for creating user-defined function blocks will not be displayed and the function blocks cannot be edited.

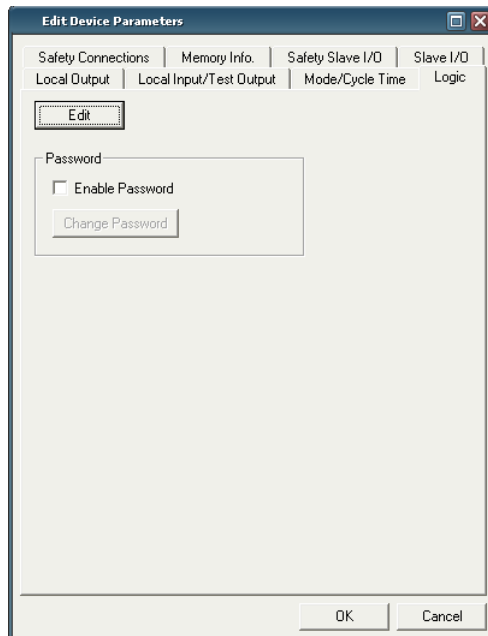
The contents of user-defined function blocks can, however, be browsed. The program must be password protected to prevent browsing of user-defined function blocks (refer to 6-3-7 *Password Protection for Programs*).

Note: It is recommended that passwords be set for user-defined function blocks for which user tests have been completed so that unintentional changes are not made after the function block has been allocated in a program.

6-3-6 Saving the Program

Use the following procedure to save the program.

1. Select *File - Apply*.
The program is saved temporarily in the Network Configurator. The data is also saved temporarily in the same way when the user exits the Logic Editor.
2. After exiting the Logic Editor, click the **OK** Button in the Edit Device Parameters Dialog Box.



3. To save the file, select *File* and *Save* or *Save As* in the Main Window of the Network Configurator.

- IMPORTANT:**
- To save the program and exit, the user must click the **OK** Button in the Edit Device Parameters Dialog Box when exiting the Logic Editor.
 - If the user clicks the **Cancel** Button, none of the parameters entered until then, including the program, will be saved. Any programming saved temporarily by applying the program (selecting *File – Apply*) will also be deleted.

6-3-7 Password Protection for Programs

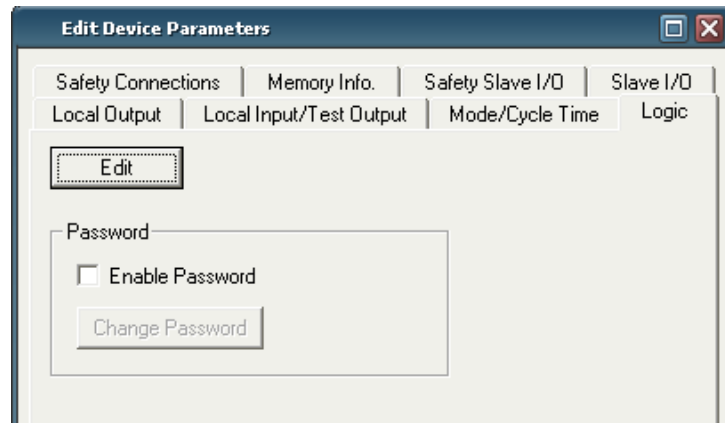
Passwords can be registered to protect editing, verification, and printing of programs.

Note: There is no recovery mechanism if the program password is forgotten.

When password-protecting programs, keep two copies of the network configuration file, one with a password and one without a password.

Download the file with the password to the Safety Network Controller.

- 1 Select **Enable Password** on the Logic Tab Page of the Edit Device Parameters Dialog Box shown below.



The Change Password Dialog Box will be displayed.



- 2 Enter the password in the New Password Field (up to 6 alphanumeric characters).
- 3 Re-enter the password in the Confirm Password Field.
- 4 Click the **OK** Button.

The program password is now set. A dialog box requesting the password will be displayed whenever the Edit Button is clicked to start the Logic Editor. Program edit/verification and report/print functions will not be available if the set password is not entered. Program can be uploaded and downloaded but the program contents cannot be displayed.

To change the password, click the **Change Password** Button on the Logic Tab in the Edit Device Parameters Dialog Box.

Note: Passwords can be set only for programs created using version 1.3□ by clicking the **Edit** Button to start the Logic Editor first.

6-3-8 Updating the Program

If the I/O tags of the Safety Slaves that configure the NE1A-series Controller's local I/O and connections are changed (e.g., by adding or deleting I/O tags), the user must start the Logic Editor and check the program.

If the user downloads the parameters to the NE1A-series Controller without starting the Logic Editor, a download error will occur in the Logic Editor because of data inconsistency. If this error occurs, start the Logic Editor and check the program, making any required modifications.

6-3-9 Monitoring the Program

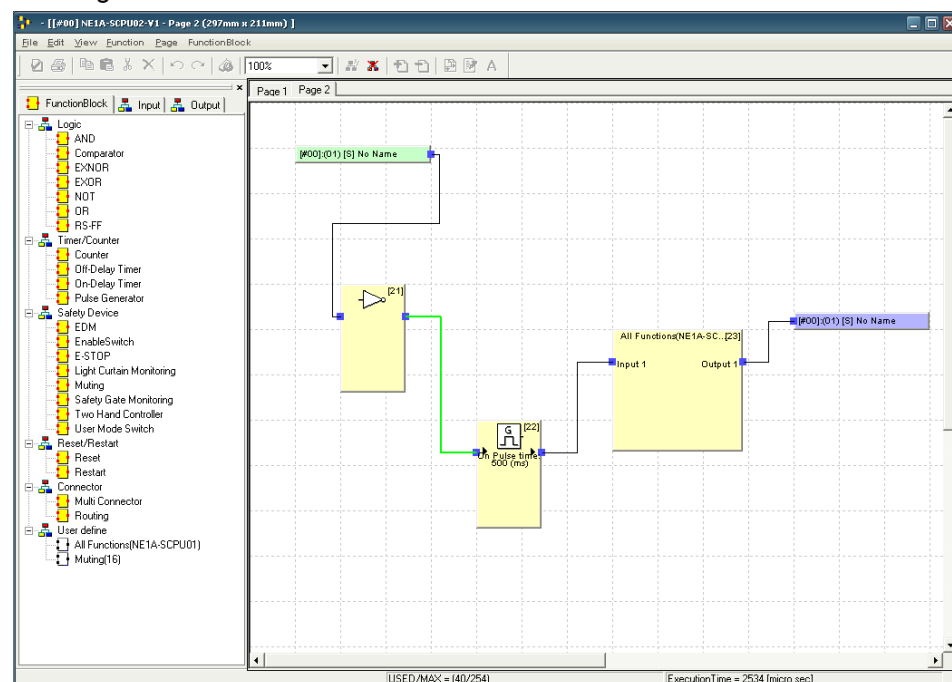
The I/O tag values and signal states of connections with function blocks can be monitored online in the Logic Editor Window. Make sure that the Network Configurator is connected to the network and that the NE1A-series Controller being monitored is in RUN state before starting online program monitoring.

Starting Online Monitoring

Start online monitoring using either of the following methods:

- (1) Select **Function - Monitoring** from the menu bar.
- (2) Click the **Monitoring** Button on the toolbar.

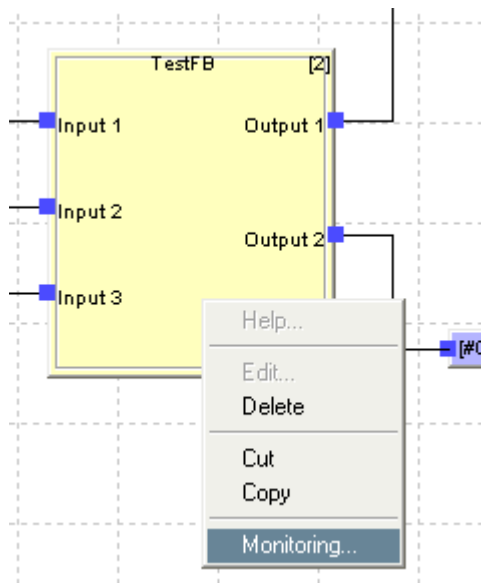
During monitoring, the I/O tags or connections that are ON will be displayed in a darker green color.



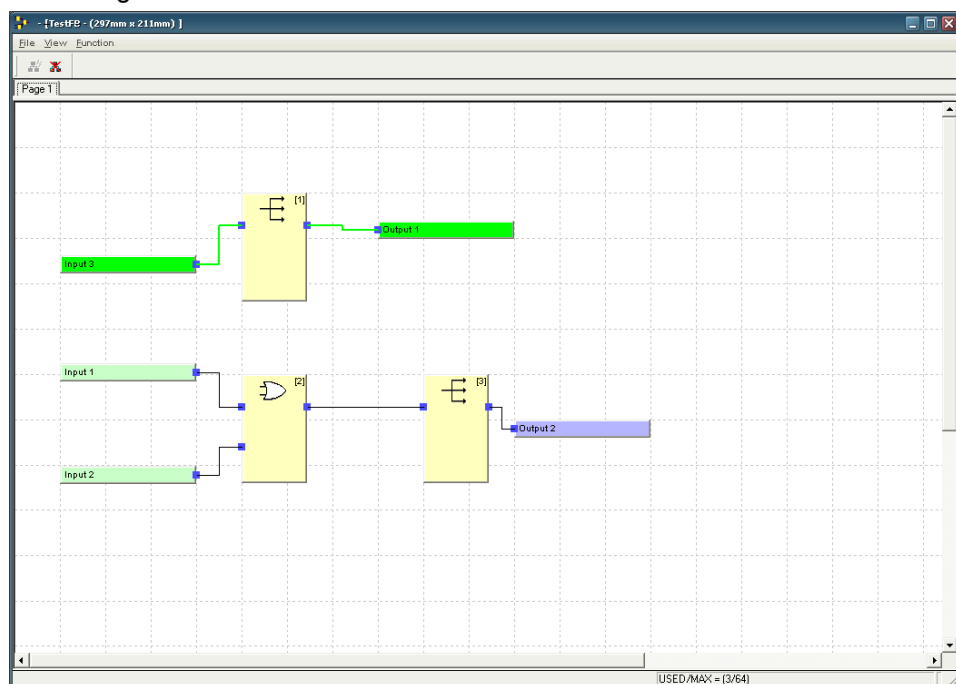
User-defined function block contents can be monitored.

Use the following procedure to start online monitoring.

- 1 Right-click the user-defined function block displayed on the screen and select **Monitoring** from the pop-up menu.



- 2 The Monitoring Screen will be displayed.
- 3 Click the **Monitoring** Button on the toolbar.
During monitoring, the I/O tags or connections that are ON will be displayed in dark green.



Stopping Online Monitoring

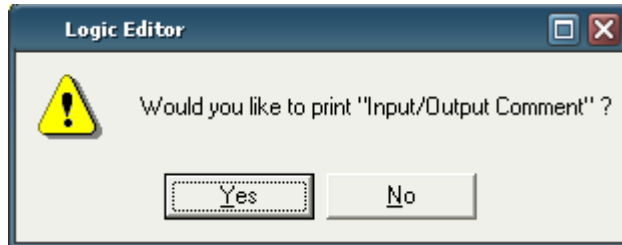
Click the **Stop Monitoring** Button on the toolbar to stop online monitoring.

Printing Programs

Programs can be printed.

- 1 Use one of the following methods to print the program
 - (1) Select **File – Print** from the menu bar.
 - (2) Click the **Print** Button on the toolbar.

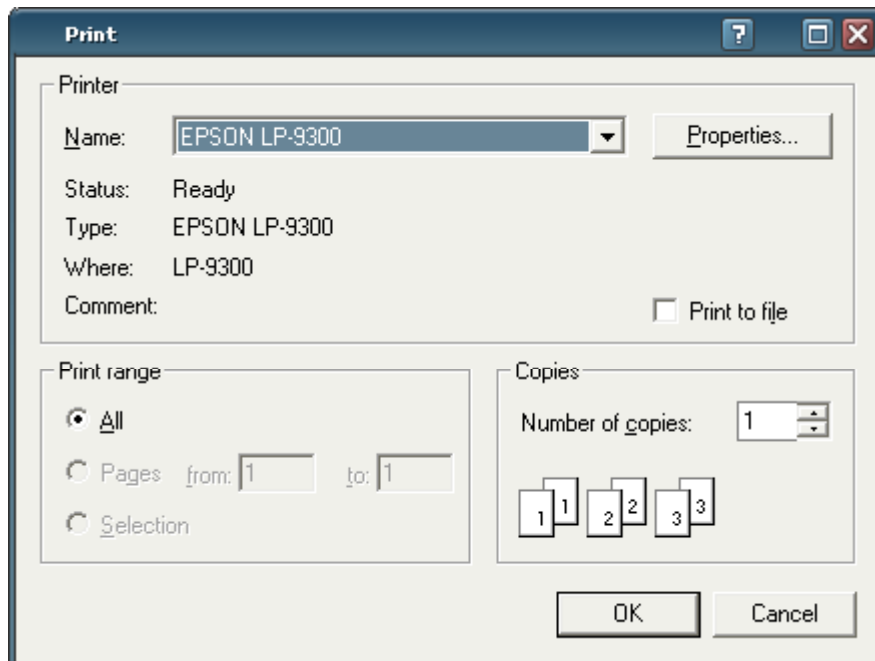
The following dialog box will be displayed.



- 2 Click the **Yes** Button to also print the function block I/O comments when printing the program.

A Print Dialog Box like the one shown below will be displayed.

(The screen may differ depending on the printer set for the personal computer being used.)



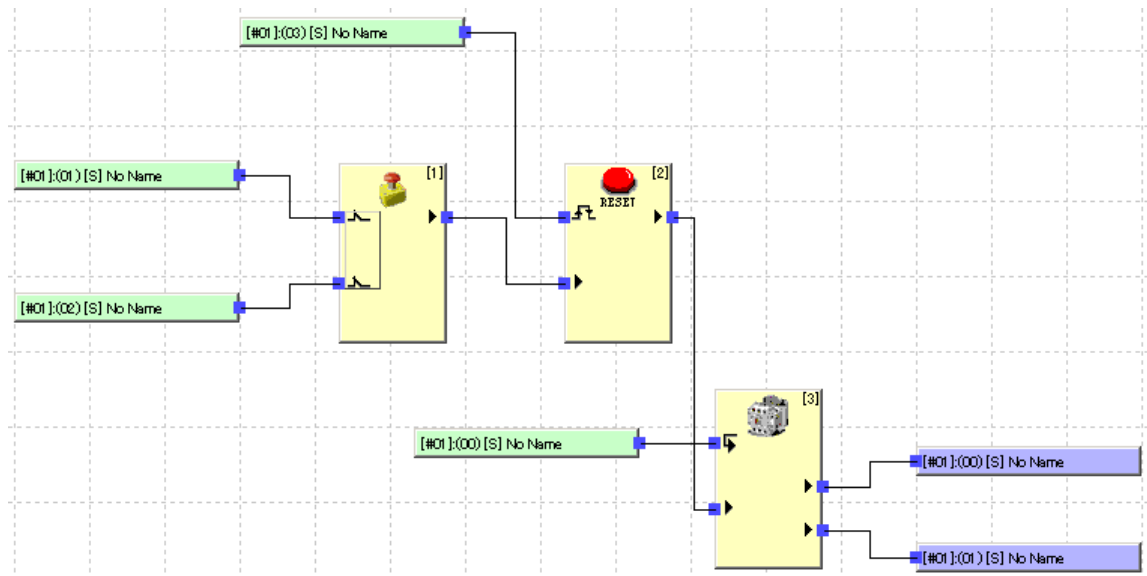
- 3 Click the **OK** Button.
The program will start printing.

Note: The diagram frames will be printed with version 1.5□. Function blocks at the edges of program screens in data created using version 1.3□ may overlap with diagram frames when the program is printed. Do not place function blocks at the edges of the program screen.

Program Execution Sequence

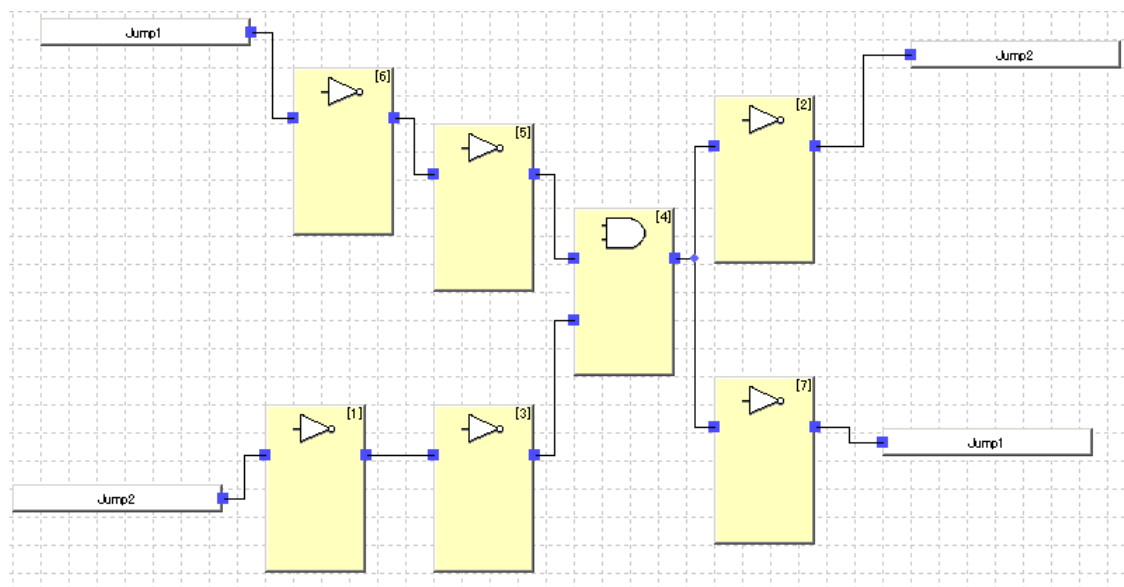
The order of execution of function blocks is automatically set by the Logic Editor and displayed in the upper right corner of each function block. The execution order would be as follows in the following example:

- 1: E-STOP
- 2: Reset
- 3: EDM



Execution Sequence of Programs with Loopbacks

Jump addresses can be used in programs to create loopbacks. If a program contains more than one loopback (e.g., Jump 1 to Jump 1 and Jump 2 to Jump 2 in the following example), the sequence of execution will be in the order that the function blocks are positioned. Carefully test all programs containing more than one loopback in the actual application to be sure they execute properly.



Section 7

Monitoring Devices

7-1	Monitoring Functions	190
7-1-1	Monitoring Status	190
7-1-2	Monitoring Safety Connections	192
7-1-3	Monitoring Parameters	194
7-1-4	Monitoring the Error History	196
7-2	Maintenance Functions of DST1-series Safety I/O Terminals	198
7-2-1	Network Power Supply Voltage Monitor	198
7-2-2	Monitoring the Run Hours	200
7-2-3	Last Maintenance Date	203
7-2-4	Monitoring the Contact Operation Counters	205
7-2-5	Monitoring the Total ON Times	208
7-2-6	Monitoring the Operation Time	212
7-3	Maintenance Functions (Unit Version 1.0 or Later)	216
7-3-1	Total ON Time Monitor Function	216
7-3-2	Contact Operation Counter	219
7-4	Displaying Safety Device Status	222

7-1 Monitoring Functions

Devices supporting DeviceNet Safety hold a variety of status information internally. This information can be monitored using the Network Configurator.

7-1-1 Monitoring Status

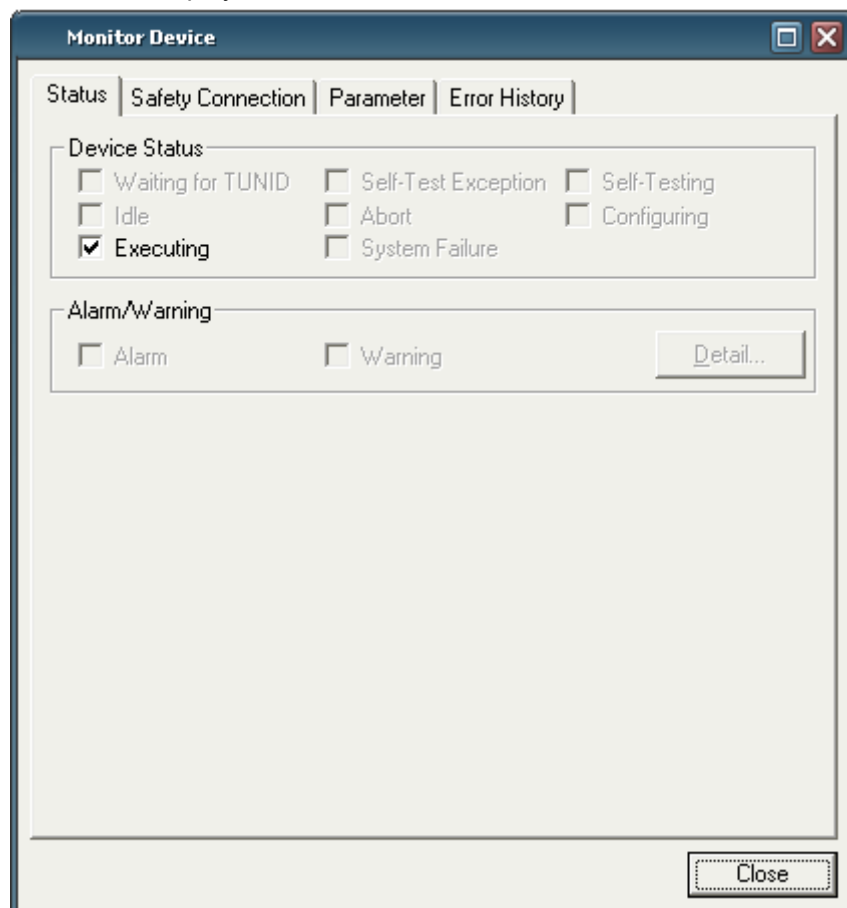
Description

The status of the NE1A-series Controller and DST1-series Safety I/O Terminals can be monitored using the Network Configurator. If an error occurs in a device, detailed information about the error can be accessed.

Monitoring Status Using the Network Configurator

The user can monitor the status using any of the following methods:

- (1) Select a device and select **Device - Monitor** from the menu bar. Click the **Status** Tab in the displayed window.
- (2) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Status** Tab in the displayed window.
- (3) Right-click a device and select **Monitor** from the pop-up menu. Click the **Status** Tab in the displayed window.





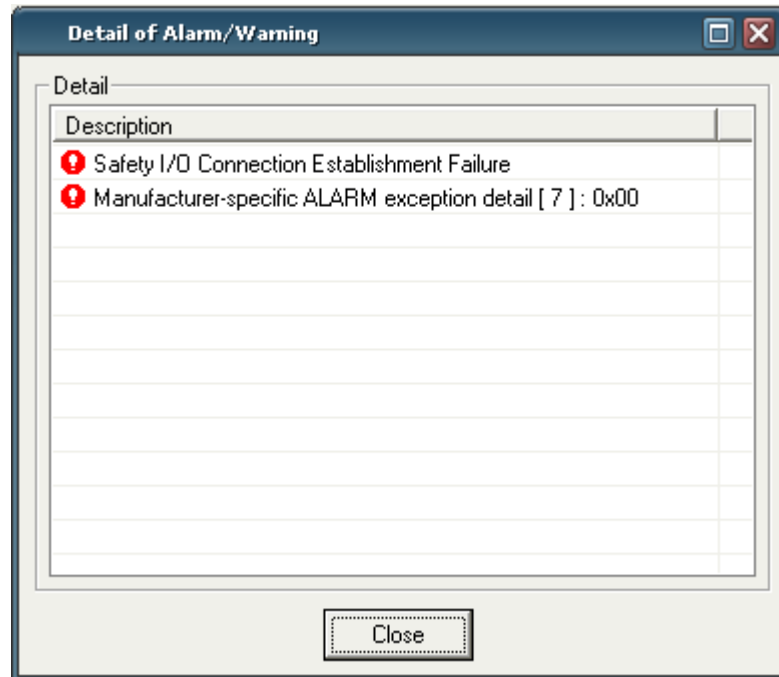
Device Status

The device status is displayed.

Alarm/Warning

Errors and warning that have occurred in the device are displayed.

Click the **Detail** Button to identify the error. The  icon will be displayed for alarms and the  icon for warnings.



7-1-2 Monitoring Safety Connections

Description

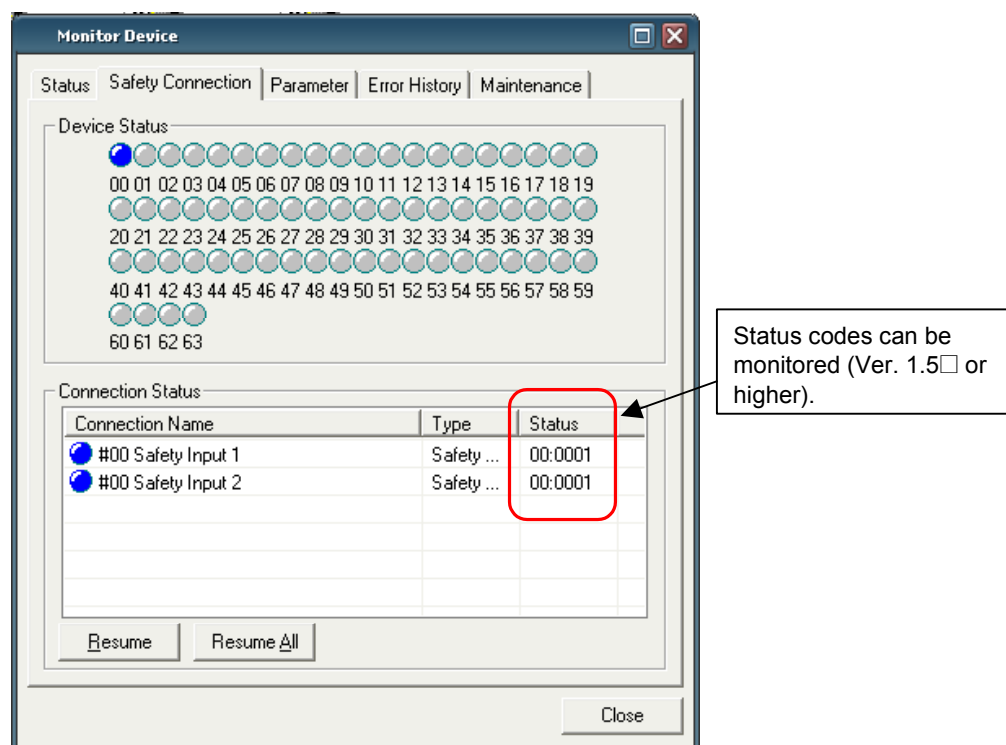
The safety connection status of the NE1A-series Controller can be monitored using the Network Configurator. This enables the user to specify with which device an error is occurring in the safety communications and in which safety connection the error is occurring. Connection information of the DST1-series Safety I/O Terminals cannot be monitored.

Monitoring Using the Network Configurator

The user can monitor the safety connection status using any of the following methods:

- (1) Select the NE1A-series Controller and select **Device - Monitor** from the menu bar. Click the **Safety Connection** Tab in the displayed window.
- (2) Select the NE1A-series Controller and click the **Monitor Device** Button on the toolbar. Click the **Safety Connection** Tab in the displayed window.
- (3) Right-click the NE1A-series Controller and select **Monitor** from the pop-up menu. Click the **Safety Connection** Tab in the displayed window.

The connection status of the Safety Slave is displayed for the local node address. For the other node addresses, the status of the safety connections configured for the device parameters is displayed.



Status codes (error codes) can be monitored (version 1.5 or higher).

This is useful when a connection cannot be established, because the status code returned by the target device can be used to check the cause of the error. Refer to *8-1 Connection Status Tables* in *Section 8 Troubleshooting* for details of status codes.

The connection status of the Safety Slave is displayed for the local node address. For the other node addresses, the status of the safety connections configured for the device parameters is displayed.

Device Status

The connection status can be checked for each node address in the *Device Status* Field. The connection status is indicated by the following colors.

Color	Status
Gray	Unregistered device.
Green	All the connections are sending idle data.
Blue	All the connections are communicating normally.
Yellow	At least one connection is not connected or sending idle data. (An error has occurred and there is no connection.)
Red	An error has occurred in at least one connection.

For the local node address (i.e., the node address of the Safety Slave), the color gray indicates that there are no connections or that an error has occurred in a connection. The color blue indicates that normal communications are being performed in one or more connections.

Connection Status

The status can be checked for each safety connection in the *Connection Status* Field. The connection status is indicated by the following colors.

Color	Status
Gray	Connection is not connected.
Green	Idle data is being transmitted.
Blue	Normal communications are being performed.
Red	Connection error has occurred.

For the local node address (i.e., the node address of the Safety Slave), the color gray indicates that there is no connection or that an error has occurred in the connection. The color blue indicates normal communications.

7-1-3 Monitoring Parameters

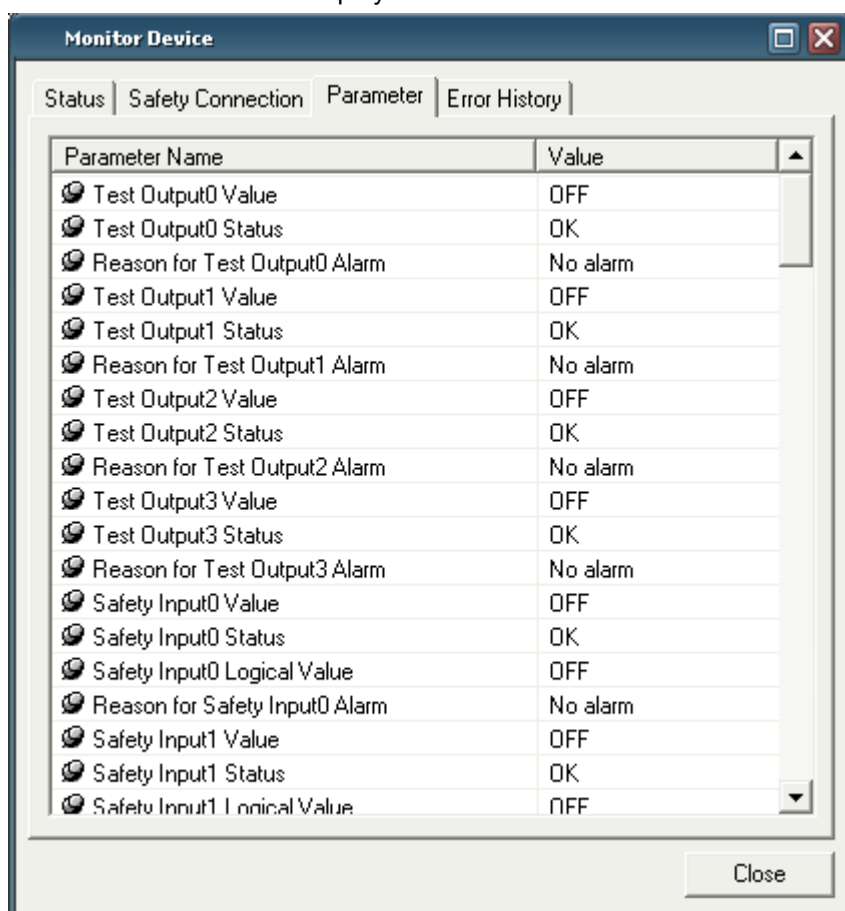
Description

The I/O status of a NE1A-series Controller or DST1-series Safety I/O Terminal can be monitored using the Network Configurator. If the configuration fails or if an error occurs in any I/O, monitoring this information enables the user to determine the cause of the error.

Monitoring Using the Network Configurator

The user can monitor the parameters using any of the following methods:

- (1) Select a device and select **Device – Monitor** from the menu bar. Click the **Parameters** Tab in the displayed window.
- (2) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Parameters** Tab in the displayed window.
- (3) Right-click a device and select **Monitor** from the pop-up menu. Click the **Parameters** Tab in the displayed window.



Test Output Terminal Status

Item	Description
Test Output Value	Output value of the test output.
Test Output Status	Evaluation result of the test output. "Alarm" is displayed if an error occurs.
Reason for Test Output Alarm	The cause of the error is displayed.

Safety Input Terminal Status

Item	Description
Safety Input Value	Input value to the safety input.
Safety Input Status	Evaluation result of the single-channel safety input. "Alarm" is displayed if an error occurs.
Safety Input Logical Value	Logical value from the evaluation result
Reason for Safety Input Alarm	The cause of the error is displayed.

Safety Output Terminal Status

Item	Description
Safety Output Value	Output value of the safety output.
Safety Output Monitor Value	Monitoring value of the output for the safety output.
Safety Output Status	Evaluation result of the single-channel safety output. "Alarm" is displayed if an error occurs.
Reason for Safety Output Alarm	The cause of the error is displayed.

Dual Channel Safety Input Status

Item	Description
Dual Channel Safety Input Evaluation	Evaluation result of the dual-channel safety input. "Alarm" is displayed if an error occurs.

7-1-4 Monitoring the Error History

Description

The error history of a NE1A-series Controller or DST1-series Safety I/O Terminal can be monitored using the Network Configurator.

Twenty error history records can be saved internally in a Pre-Ver. 1.0 NE1A-series Controller, 100 records in an NE1A-SCPU01 Controller with unit version 1.0 or an NE1A-SCPU02 Controller, and ten records in a DST1-series Safety I/O Terminal.

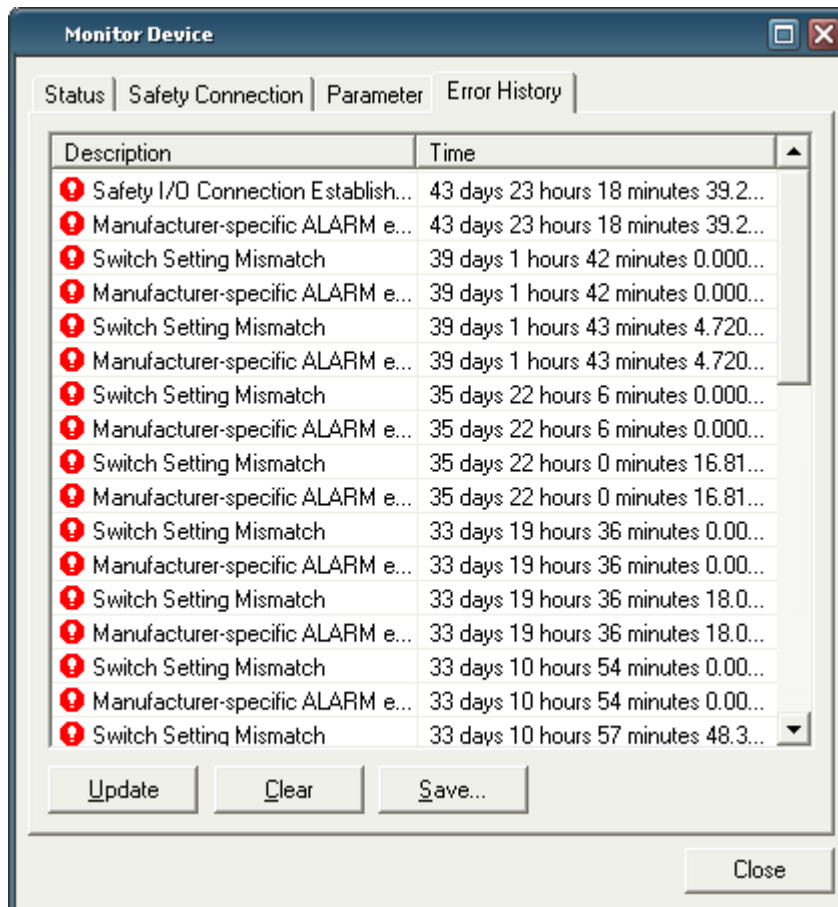
When the number of errors exceeds the number of records, the oldest records will be deleted.

Depending on the error type, some errors are saved in non-volatile memory and not cleared when the power is turned OFF. Other errors are saved in RAM and cleared when the power is turned OFF. Refer to the relevant operation manual for details.

Monitoring Using the Network Configurator

The user can monitor the error history using any of the following methods:

- (1) Select a device and select **Device – Monitor** from the menu bar. Click the **Error History** Tab in the displayed window.
- (2) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Error History** Tab in the displayed window.
- (3) Right-click a device and select **Monitor** from the pop-up menu. Click the **Error History** Tab in the displayed window.



Error History Display Items

Item	Description
Description	Provides error details.
Time	The total device operation time when the error occurred. DST1-series Safety I/O Terminals do not support this function and 0 will always be displayed.

Saving the Error History

The error history information can be saved in CSV format. Click the **Save** Button to save the information.

Clearing the Error History

Click the **Clear** Button to clear the error history saved internally in the NE1A-series Controller or DST1-series Safety I/O Terminal.

Updating the Error History

Click the **Update** Button to access the most recent error history.

7-2 Maintenance Functions of DST1-series Safety I/O Terminals

DST1-series Safety I/O Terminals support the same maintenance functions as DRT2-series Smart Slaves, which are Standard Slaves.

7-2-1 Network Power Supply Voltage Monitor

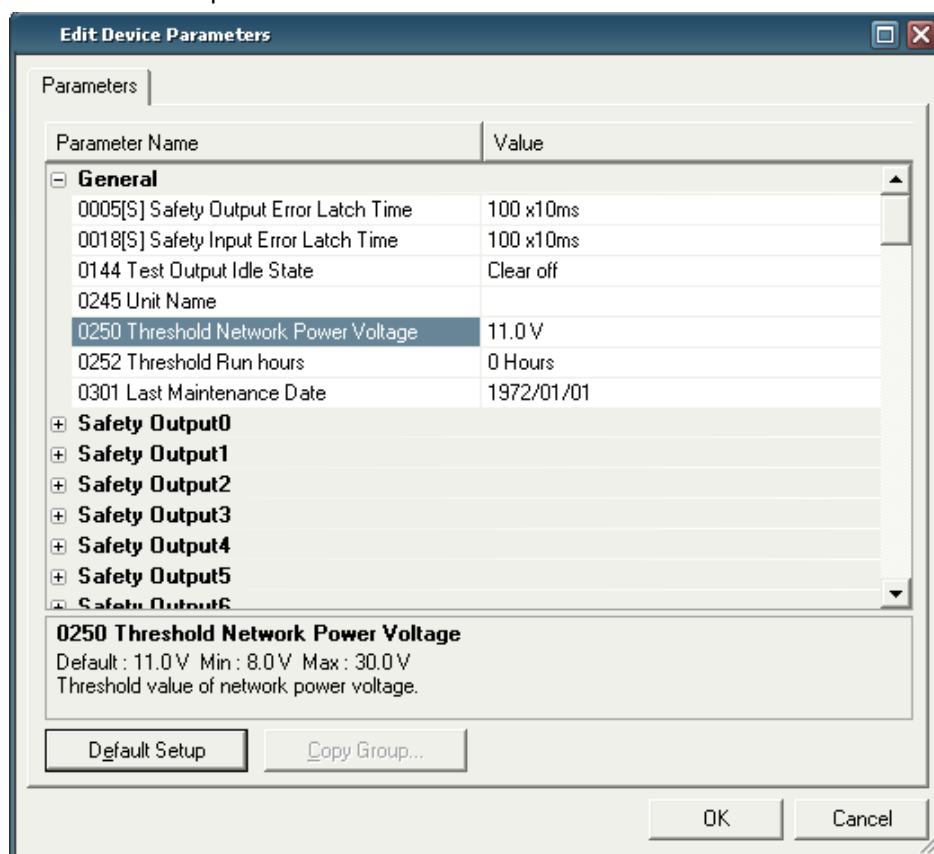
Description

DST1-series Safety I/O Terminals always monitor the present, minimum, and maximum values of the network power supply voltage. If the voltage falls below the set threshold voltage (11 V in the default settings), the Threshold Network Power Voltage Error Flag will be turned ON in the General Status. The user can monitor this information using the Network Configurator and explicit messages.

- Note:
- The minimum communications power voltage of the DeviceNet is 11 V. If the voltage falls below 11 V, the Configurator may not be able to read measured values.
 - The present, maximum, and minimum values of the network power supply voltage are cleared when the power supply to the DST1-series Safety I/O Terminal (network power) is turned OFF.

Setting the Threshold Network Power Supply Voltage Using the Network Configurator

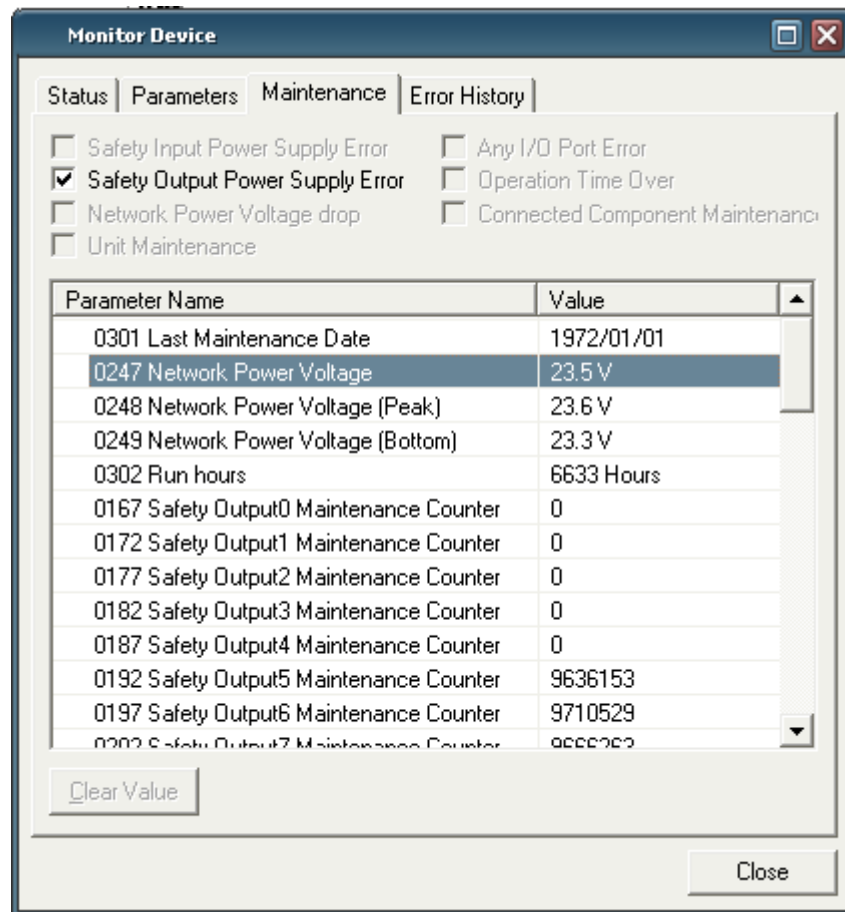
Set the threshold voltage in the *Threshold Network Power Voltage* Field in the General Parameter Group.



Monitoring Using the Network Configurator

The user can monitor the present, maximum, and minimum values of the network power voltage in the General Status using any of the following methods:

- (1) Select a device and select **Device - Maintenance Information** from the menu bar.
- (2) Select a device and click the **Maintenance Information** Button on the toolbar.
- (3) Right-click a device and select **Maintenance Information** from the pop-up menu.
- (4) Select a device and select **Device - Monitor** from the menu bar. Click the **Maintenance** Tab in the displayed window.
- (5) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Maintenance** Tab in the displayed window.
- (6) Right-click a device and select **Monitor** from the pop-up menu. Click the **Maintenance** Tab in the displayed window.



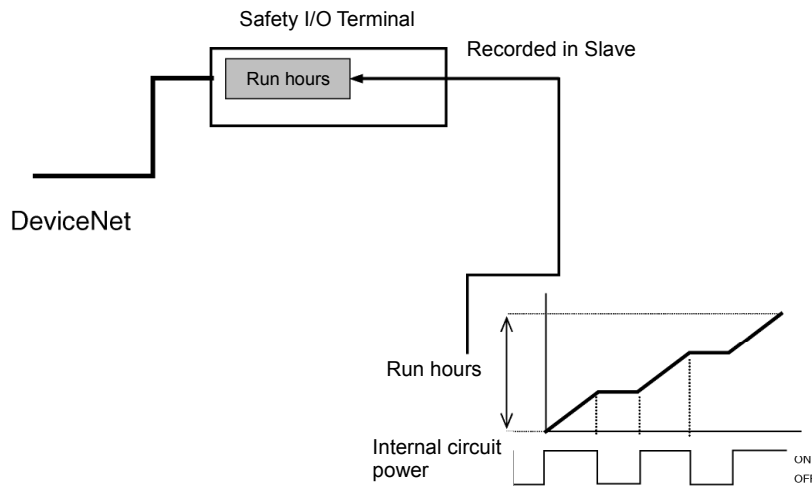
The maximum and minimum values of the network power voltage can be cleared. Select the maximum or minimum value and click the **Clear Value** Button.

7-2-2 Monitoring the Run Hours

Description

A DST1-series Safety I/O Terminal totals the number of hours the internal circuit power is supplied and internally saves it in non-volatile memory. If the cumulative time reaches the set threshold value, the Unit Maintenance Flag will turn ON in the General Status.

- Measurement time: 0 to 429,496,729.5 hours
(stored data: 0000 0000 to FFFF FFFF hex)
- Measurement unit: 0.1 hour

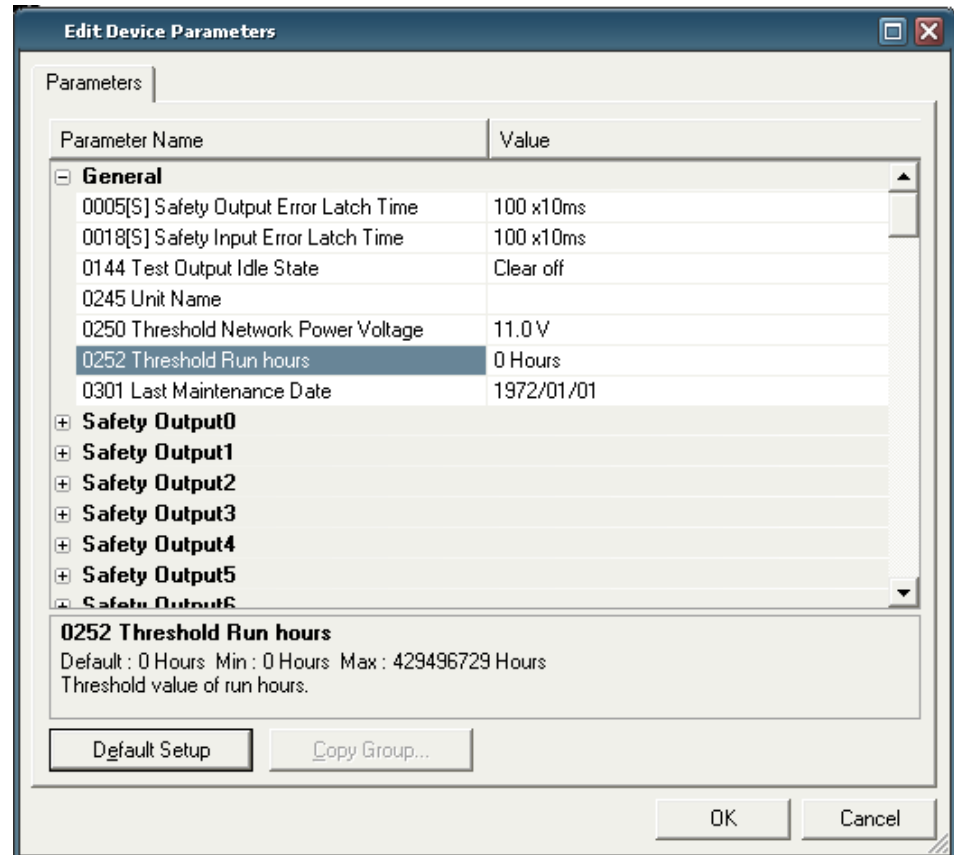


The user can monitor this information using the Network Configurator and explicit messages.

- Note:
- **The run hours monitoring function totals the time when the power supply to the DST1-series Safety I/O Terminal (network power) is ON. This does not include the time when the power is OFF.**
 - **The DST1-series Safety I/O Terminals measure time internally in 0.1-hour increments. When the Threshold Run Hours parameter is set on the Network Configurator and when the run hours are monitored, however, the time will be in 1-hour increments.**

Setting the Threshold Run Hours Using the Network Configurator

Set the threshold value in the *Threshold Run hours* Field of the *General* Parameter Group.



If the threshold value is set to 0, the threshold value will not be checked.

Monitoring Using the Network Configurator

The user can monitor run hours in the General Status using any of the following methods:

- (1) Select a device and select **Device - Maintenance Information** from the menu bar.
- (2) Select a device and click the **Maintenance Information** Button on the toolbar.
- (3) Right-click a device and select **Maintenance Information** from the pop-up menu.
- (4) Select a device and select **Device - Monitor** from the menu bar. Click the **Maintenance** Tab in the displayed window.
- (5) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Maintenance** Tab in the displayed window.
- (6) Right-click a device and select **Monitor** from the pop-up menu. Click the **Maintenance** Tab in the displayed window.

Parameter Name	Value
0301 Last Maintenance Date	1972/01/01
0247 Network Power Voltage	23.5 V
0248 Network Power Voltage (Peak)	23.6 V
0249 Network Power Voltage (Bottom)	23.3 V
0302 Run hours	6634 Hours
0167 Safety Output0 Maintenance Counter	0
0172 Safety Output1 Maintenance Counter	0
0177 Safety Output2 Maintenance Counter	0
0182 Safety Output3 Maintenance Counter	0
0187 Safety Output4 Maintenance Counter	0
0192 Safety Output5 Maintenance Counter	9636153
0197 Safety Output6 Maintenance Counter	9710529
0202 Safety Output7 Maintenance Counter	9888262

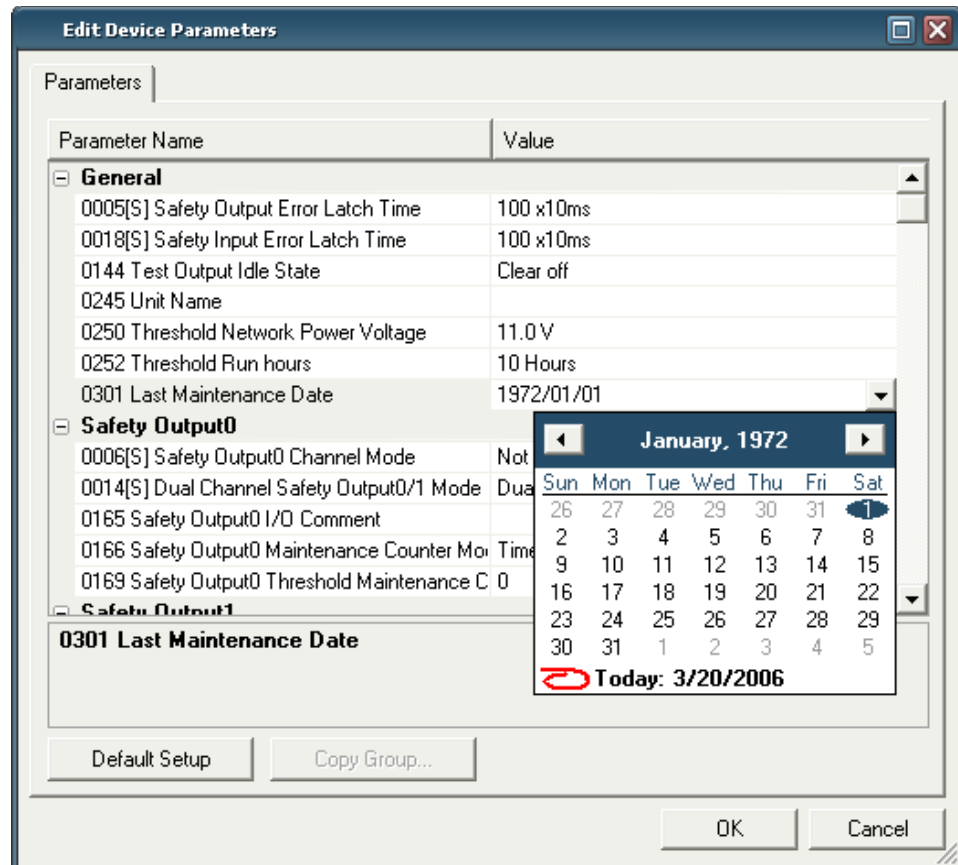
7-2-3 Last Maintenance Date

Description

With a DST1-series Safety I/O Terminal the last maintenance date can be recorded internally in non-volatile memory. This enables the user to easily decide the time for the next maintenance. The recorded maintenance date can be monitored using the Network Configurator or explicit messages.

Recording the Maintenance Date Using the Network Configurator

Record the data using the Last Maintenance Date Parameter in the *General* Parameter Group.



Monitoring Using the Network Configurator

The user can monitor the maintenance date using any of the following methods:

- (1) Select a device and select **Device - Maintenance Information** from the menu bar.
- (2) Select a device and click the **Maintenance Information** Button on the toolbar.
- (3) Right-click a device and select **Maintenance Information**.
- (4) Select a device and select **Device - Monitor** from the menu bar. Click the **Maintenance** Tab in the displayed window.
- (5) Select a device and click the **Monitor Device** Button. Click the **Maintenance** Tab in the displayed window.
- (6) Right-click a device and select **Monitor** from the pop-up menu. Click the **Maintenance** Tab in the displayed window.

Monitor Device

☐ Safety Input Power Supply Error
 ☐ Any I/O Port Error
☒ Safety Output Power Supply Error
 ☐ Operation Time Over
☐ Network Power Voltage drop
 ☐ Connected Component Maintenance
☒ Unit Maintenance

Parameter Name	Value
0301 Last Maintenance Date	2006/03/20
0247 Network Power Voltage	23.5 V
0248 Network Power Voltage (Peak)	23.6 V
0249 Network Power Voltage (Bottom)	23.3 V
0302 Run hours	6634 Hours
0167 Safety Output0 Maintenance Counter	0
0172 Safety Output1 Maintenance Counter	0
0177 Safety Output2 Maintenance Counter	0
0182 Safety Output3 Maintenance Counter	0
0187 Safety Output4 Maintenance Counter	0
0192 Safety Output5 Maintenance Counter	9636153
0197 Safety Output6 Maintenance Counter	9710529
0202 Safety Output7 Maintenance Counter	9999999

Clear Value

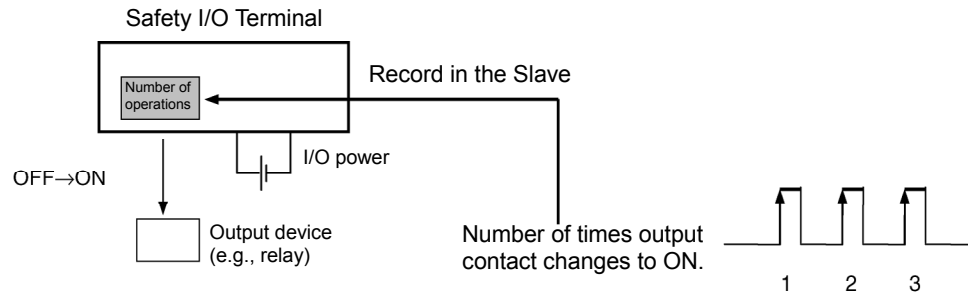
Close

7-2-4 Monitoring the Contact Operation Counters

Description

A DST1-series Safety I/O Terminal totals the number of times each safety input contact, test output contact, and safety output contact turns ON and internally saves the data in non-volatile memory. If the value of a counter reaches the threshold value, the Connected Component Maintenance Flag in General Status will turn ON.

- Measurement count: 0 to 4,294,967,295 counts
(stored data: 0000 0000 to FFFF FFFF hex)
- Measurement unit: Operations
- Maximum resolution: 166.7 Hz



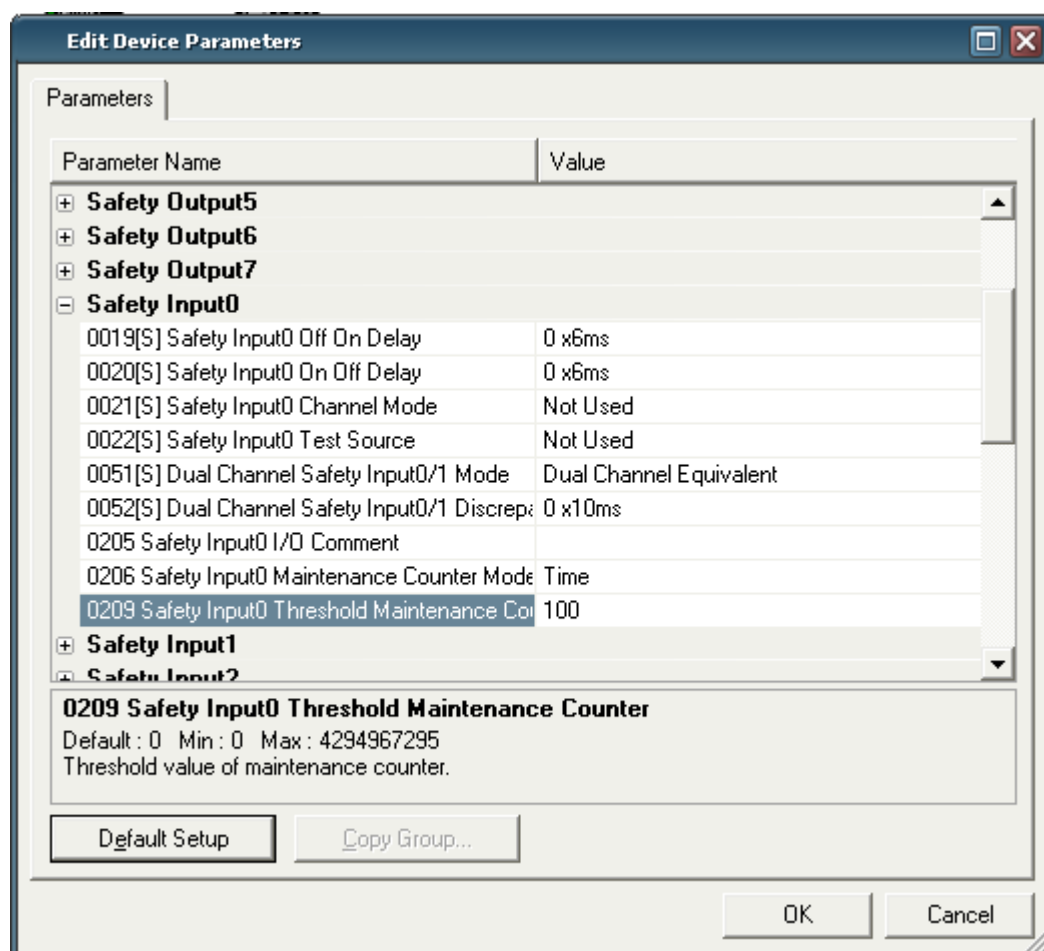
The user can monitor this information using the Network Configurator and explicit messages.

- Note:
- **One contact cannot be used at the same time for both the time and count monitoring functions. Select only one of these in the *Maintenance Counter Mode Choice*.**
 - If the *Maintenance Counter Mode Choice* is changed, the counter or time data saved internally will be cleared.
 - This function does not operate when the I/O power supply is OFF.

Setting the Contact Operation Counter Threshold Using the Network

Configurator

Set the Maintenance Counter Mode Choice Parameter and Threshold Maintenance Counter Parameter for each I/O of the safety input group, test output group, and safety output group.

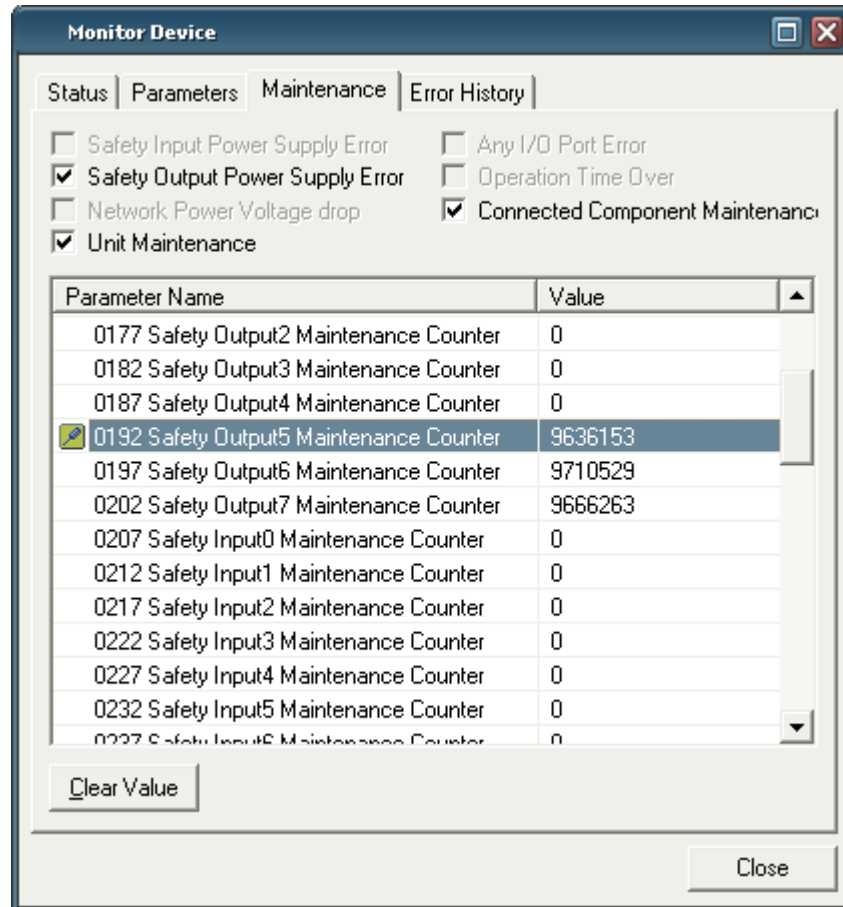


When the Threshold Maintenance Counter is set to 0, the threshold value will not be checked.

Monitoring Using the Network Configurator

The user can monitor the counts for safety input status, test output status, and safety output status using any of the following methods:

- (1) Select a device and select **Device - Maintenance Information** from the menu bar.
- (2) Select a device and click the **Maintenance Information** Button on the toolbar.
- (3) Right-click a device and select **Maintenance Information** from the pop-up menu.
- (4) Select a device and select **Device - Monitor** from the menu bar. Click the **Maintenance** Tab in the displayed window.
- (5) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Maintenance** Tab in the displayed window.
- (6) Right-click a device and select **Monitor** from the pop-up menu. Click **Maintenance** Tab in the displayed window.



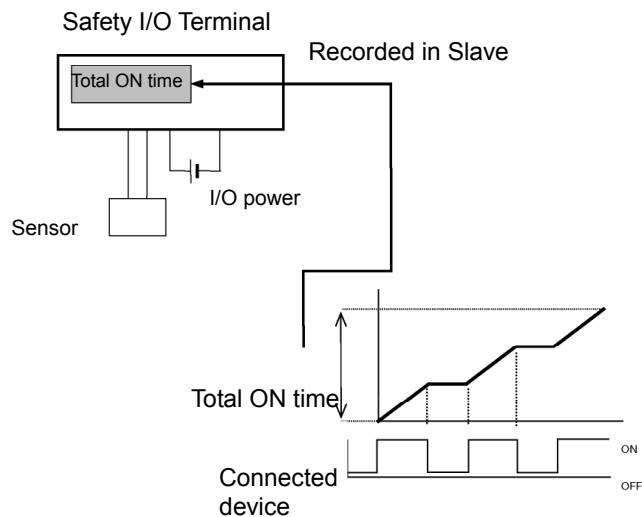
Each counter can be cleared. Select the counter to clear and click the **Clear Value** Button.

7-2-5 Monitoring the Total ON Times

Description

A DST1-series Safety I/O Terminal totals the time each safety input contact, test output contact, and safety output contact is ON, and saves it internally in non-volatile memory. If a cumulative time reaches the threshold value, the Connected Component Maintenance Flag in General Status will turn ON.

- Measurement time: 0 to 4,294,967,295 seconds
(stored data: 0000 0000 to FFFF FFFF hex)
- Measurement unit: Seconds



The user can monitor this information using the Network Configurator and explicit messages.

Note:

- One contact cannot be used at the same time for both the time and count monitoring functions. Select only one of these in the *Maintenance Counter Mode Choice*.
- If the *Maintenance Counter Mode Choice* is changed, the counter or time data saved internally will be cleared.
- This function does not operate when the I/O power supply is OFF.
- The time monitor checks if the connected component is ON approximately every second. This should be noted when the time is measured in increments of 1 second or less.

Measuring 0.5-second ON Time

In *Figure A*, the actual ON time is 0.5 seconds x 3, or 1.5 seconds. Operation is ON only once when measurements are made, however, so the time is measured as 1 second.

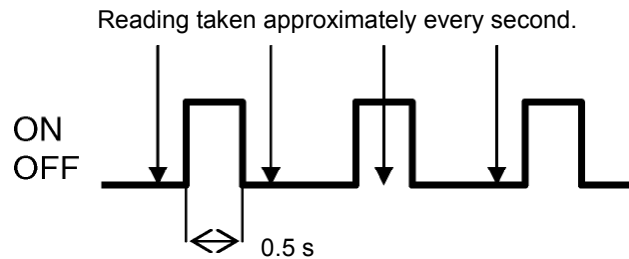


Figure A

In *Figure B*, the actual ON time is 0.5 seconds x 3, or 1.5 seconds. Operation is ON twice when measurements are made, however, so the time is measured as 2 seconds.

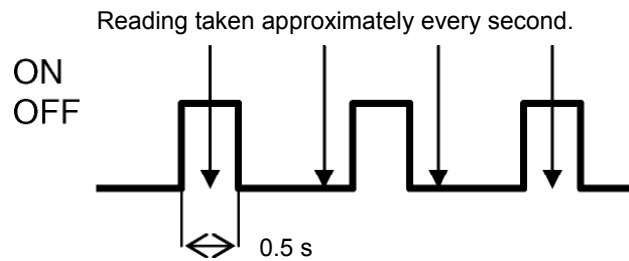


Figure B

Measuring 1.5-second ON Time

In *Figure C*, the actual ON time is 1.5 seconds x 2, or 3 seconds. Operation is ON four times when measurements are made, however, so the time is measured as 4 seconds.

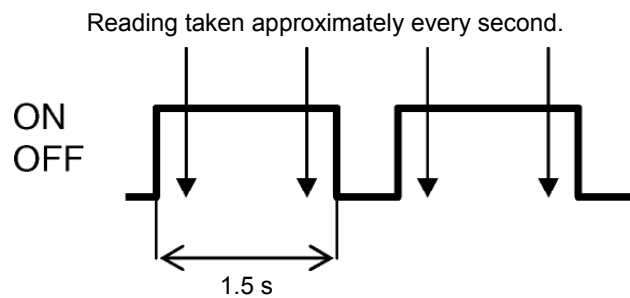


Figure C

Setting the Threshold Value for Total ON Time Using the Network

Configurator

Set the Maintenance Counter Mode Choice Parameter and Threshold Maintenance Counter Parameter for each contact of the safety input group, test output group, and safety output group.

The screenshot shows the 'Edit Device Parameters' dialog box with the 'Parameters' tab selected. It displays a list of parameters for Safety Output5, Output6, and Output7. The parameter '0191 Safety Output5 Maintenance Counter Mode Choice' is highlighted, showing a value of 'Time'. Below the list, there is a section titled '0191 Safety Output5 Maintenance Counter Mode Choice' with a default value of 'Time' and a description: 'Select the action of the maintenance counter. The time mode is the mode to estimate the time during the output is ON. The count mode is the mode to count the number that the output changes from.' At the bottom, there are buttons for 'Default Setup', 'Copy Group...', 'OK', and 'Cancel'.

Parameter Name	Value
0189 Safety Output4 Threshold Maintenance C	0
Safety Output5	
0011[S] Safety Output5 Channel Mode	Not Used
0016[S] Dual Channel Safety Output4/5 Mode	Dual Channel
0190 Safety Output5 I/O Comment	
0191 Safety Output5 Maintenance Counter Mode Choice	Time
0194 Safety Output5 Threshold Maintenance C	100
Safety Output6	
0012[S] Safety Output6 Channel Mode	Not Used
0017[S] Dual Channel Safety Output6/7 Mode	Dual Channel
0195 Safety Output6 I/O Comment	
0196 Safety Output6 Maintenance Counter Mode Choice	Time
0199 Safety Output6 Threshold Maintenance C	0
Safety Output7	
0013[S] Safety Output7 Channel Mode	Not Used

0191 Safety Output5 Maintenance Counter Mode Choice
 Default : Time
 Select the action of the maintenance counter. The time mode is the mode to estimate the time during the output is ON. The count mode is the mode to count the number that the output changes from.

Buttons: Default Setup, Copy Group..., OK, Cancel

If the Threshold Maintenance Counter is set to 0, the threshold value will not be checked.

Monitoring Using the Network Configurator

The user can monitor the times for safety input status, test output status, and safety output status using any of the following methods:

- (1) Select a device and select **Device - Maintenance Information** from the menu bar.
- (2) Select a device and click the **Maintenance Information** Button on the toolbar.
- (3) Right-click a device and select **Maintenance Information** from the pop-up menu.
- (4) Select a device and select **Device - Monitor** from the menu bar. Click the **Maintenance** Tab in the displayed window.
- (5) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Maintenance** Tab in the displayed window.
- (6) Right-click a device and select **Monitor** from the pop-up menu. Click the **Maintenance** Tab in the displayed window.

Parameter Name	Value
0187 Safety Output4 Maintenance Counter	0
0192 Safety Output5 Maintenance Counter	9636153
0197 Safety Output6 Maintenance Counter	9710529
0202 Safety Output7 Maintenance Counter	9666263
0207 Safety Input0 Maintenance Counter	0
0212 Safety Input1 Maintenance Counter	0
0217 Safety Input2 Maintenance Counter	0
0222 Safety Input3 Maintenance Counter	0
0227 Safety Input4 Maintenance Counter	0
0232 Safety Input5 Maintenance Counter	0
0237 Safety Input6 Maintenance Counter	0
0242 Safety Input7 Maintenance Counter	62156
0147 Test Output0 Maintenance Counter	0

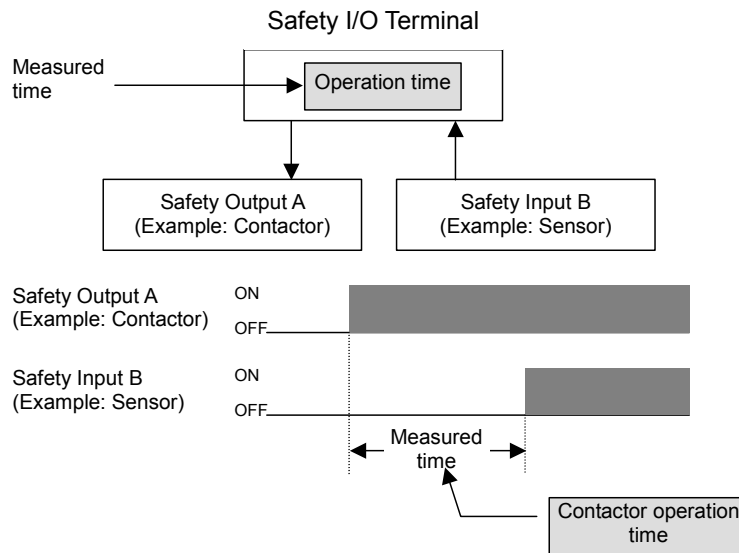
Each time value can be cleared. Select the time to clear and click the **Clear Value** Button.

7-2-6 Monitoring the Operation Time

Description

A DST1-series Safety I/O Terminal measures the time from when a safety output turns ON until the safety input turns ON and internally saves the data in non-volatile memory. If the value of the operation time reaches the threshold value, the Threshold Response Time Flag in General Status will turn ON.

- Measurement time: 0 to 65,535 ms (stored data: 0000 to FFFF hex)
- Measurement unit: ms



The input reaction time and the output reaction time of the DST1-series Safety I/O Terminal are added to monitor the operation time.

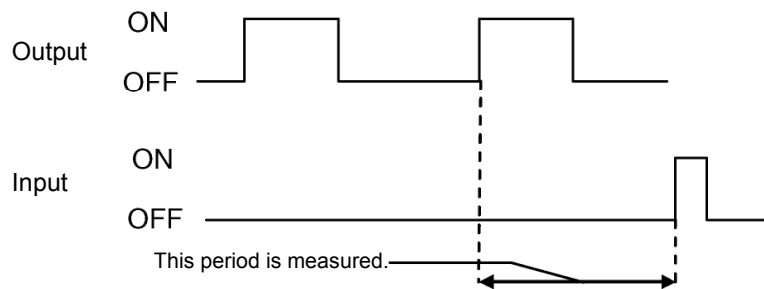
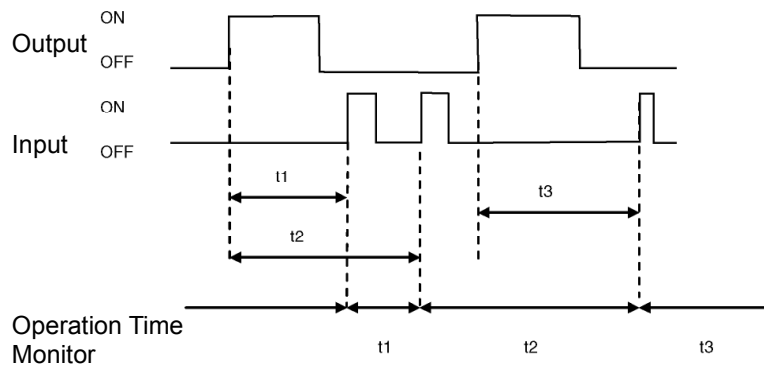
Maximum input reaction time of the DST1-series Safety I/O Terminal
= 16.2 ms + ON/OFF delay

Maximum output reaction time of the DST1-series Safety I/O Terminal
= 6.2 ms + Relay reaction time (DST1-MRD08SI-1 only)

The measurement is accurate to ± 6 ms.

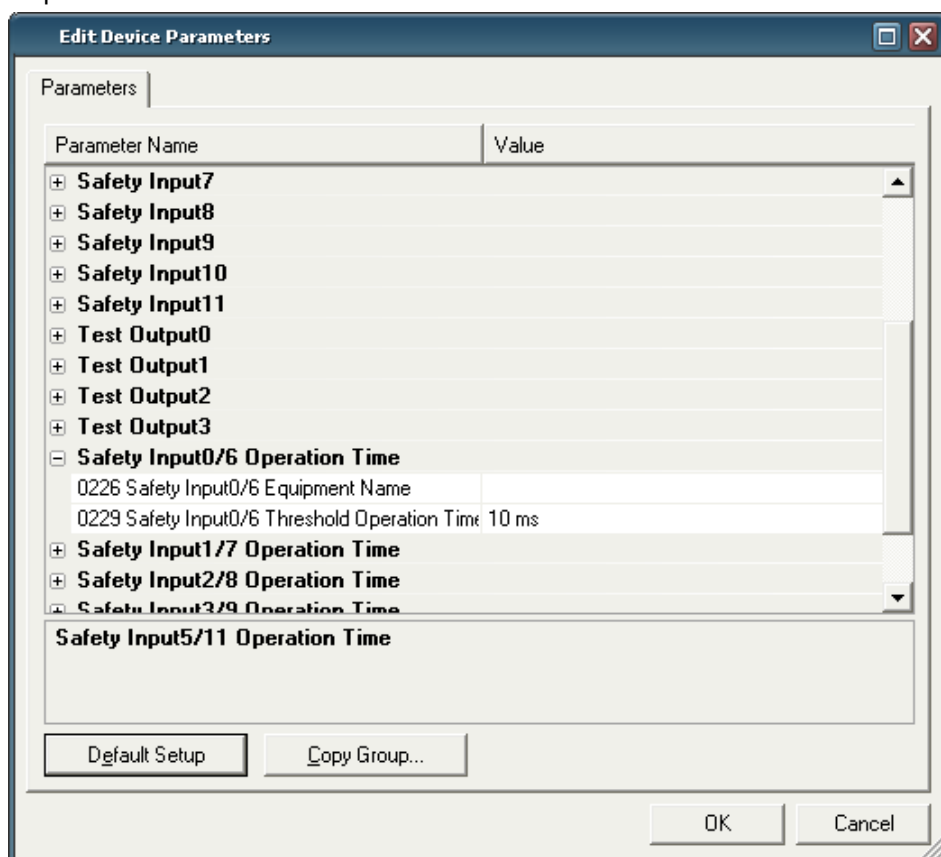
The user can monitor this information using the Network Configurator and explicit messages.

- Note:
- In the DST1-MD16SL-1 or DST1-MRD08SL-1, the time is measured from when a safety output turns ON until the safety input turns ON for the safety input and safety output with the same number (e.g., Safety Input 0 and Safety Output 0).
 - In the DST1-ID12SL-1, the time is measured between two safety inputs turning ON (e.g., Safety Input 0 and Safety Input 6).
 - The operation time is stored when the time from an output turning ON to an input turning ON is measured. The measurement, however, continues internally until the next time the output turns ON. If the input turns ON again before the output turns ON, the measurement time will be updated. If an input occurs in the middle of the operating range of reciprocating motion, like a cylinder, the measurement value of operation (outward path) may be updated when returning (return path).
 - When an output turns ON two consecutive times before the input turns ON, the time will be measured from the second time the output turned ON until the time the input turned ON.



Setting the Threshold Response Time Using the Network Configurator

The Threshold Response Time is set for each pair in the *Operation Time* Parameter Group.

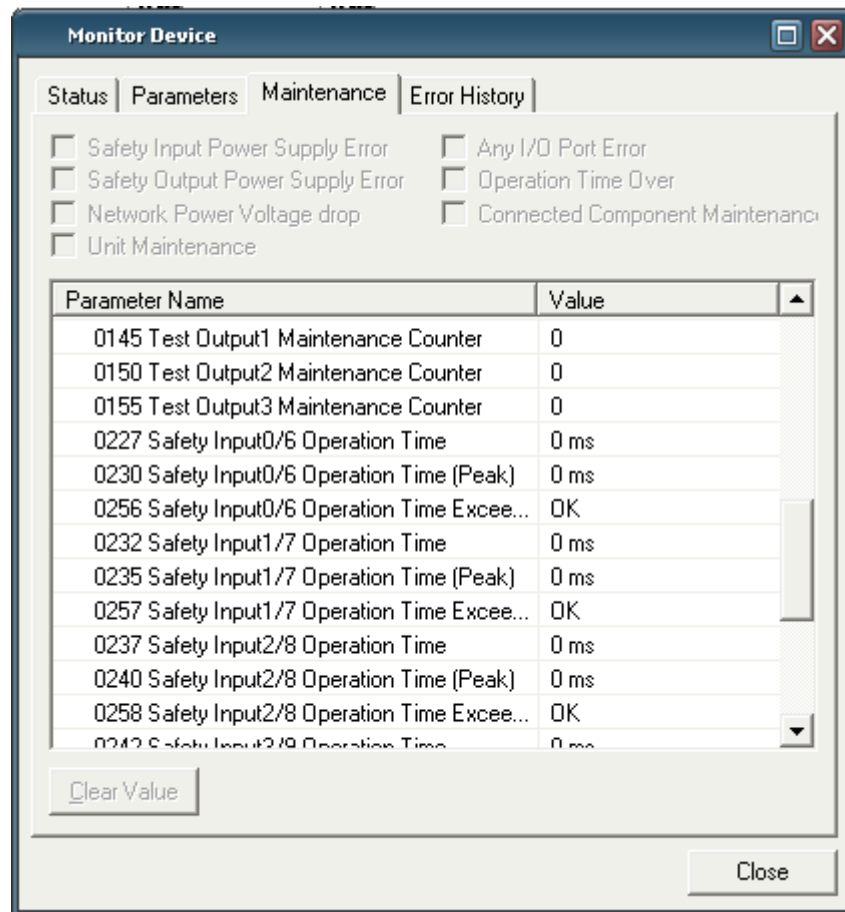


If the threshold value is set to 0, the threshold value will not be checked.

Monitoring Using the Network Configurator

The user can monitor the operation time using any of the following methods:

- (1) Select a device and select **Device - Maintenance Information** from the menu bar.
- (2) Select a device and click the **Maintenance Information** Button on the tool bar.
- (3) Right-click a device and select **Maintenance Information** from the pop-up menu.
- (4) Select a device and select **Device - Monitor** from the menu bar. Click the **Maintenance** Tab in the displayed window.
- (5) Select a device and click the **Monitor Device** Button on the toolbar. Click the **Maintenance** Tab in the displayed window.
- (6) Right-click a device and select **Monitor** from the pop-up menu. Click the **Maintenance** Tab in the displayed window.



- The present value of the operation time is displayed for the *Operation Time*.
- The slowest value of the operation time is displayed for the *Operation Time (Peak)*.
- If the Threshold Response Time is set and the value exceeds the threshold value even once, "Alarm" will be displayed for the *Operation Time Exceed Hold*.

The user can clear the *Operation Time (peak)* and *Operation Time Exceed Hold* values. Select an item to clear and click the **Clear Value** Button.

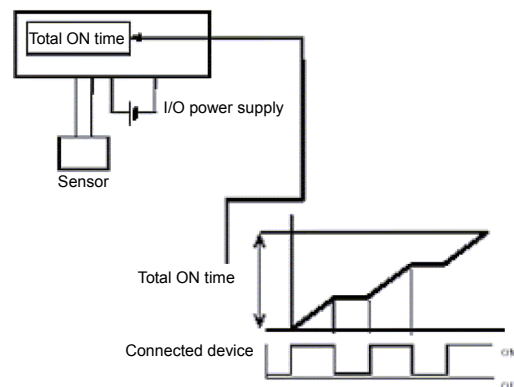
7-3 Maintenance Functions (Unit Version 1.0 or Later)

7-3-1 Total ON Time Monitor Function

Overview

In NE1A-series Controllers with unit version 1.0 or later, this function times how long a local input, test output, or local output is ON and stores that total ON time internally in non-volatile memory.

- Count range: 0 to 4,294,967,295 s (stored as 00000000 to FFFFFFFF Hex)
- Count units: Seconds



This information can be monitored using the Network Configurator or explicit messaging.

- Note 1:** The Total ON Time Monitor function (Time) and Contact Operation Counter function (Count) cannot be used simultaneously on one bit. Select one of these functions with the Maintenance Counter Mode Choice setting.
- 2:** When the Maintenance Counter Mode Choice setting is changed, the collected data (operations count or total ON time) will be cleared.
- 3:** These functions do not operate when the I/O power supply is OFF.
- 4:** The Total ON Time Monitor function checks whether the connected device is ON at about 1-s intervals. This function may not count the total ON time precisely if the device is ON for intervals of less than 1 second.

Calculating the Total ON Time with 0.5-s ON Pulses

In figure A, the bit is actually ON for $0.5 \text{ s} \times 3 = 1.5 \text{ s}$, but the bit is ON just once when the status is checked, so the total ON time is measured as 1 s.

In figure B, the bit is actually ON for $0.5 \text{ s} \times 3 = 1.5 \text{ s}$, but the bit is ON twice when the status is checked, so the total ON time is measured as 2 s.

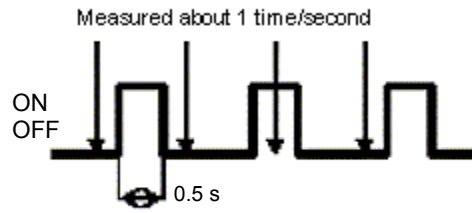


Figure A

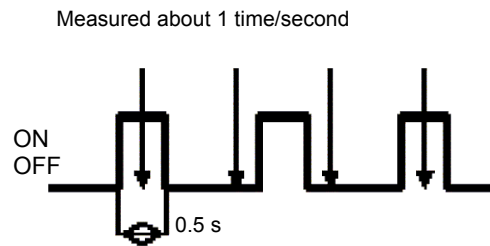


Figure B

Calculating the Total ON Time with 1.5-s ON Pulses

In figure C, the bit is actually ON for $1.5 \text{ s} \times 2 = 3 \text{ s}$, but the bit is ON four times when the status is checked, so the total ON time is measured as 4 s.

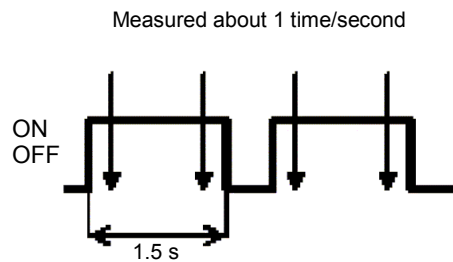
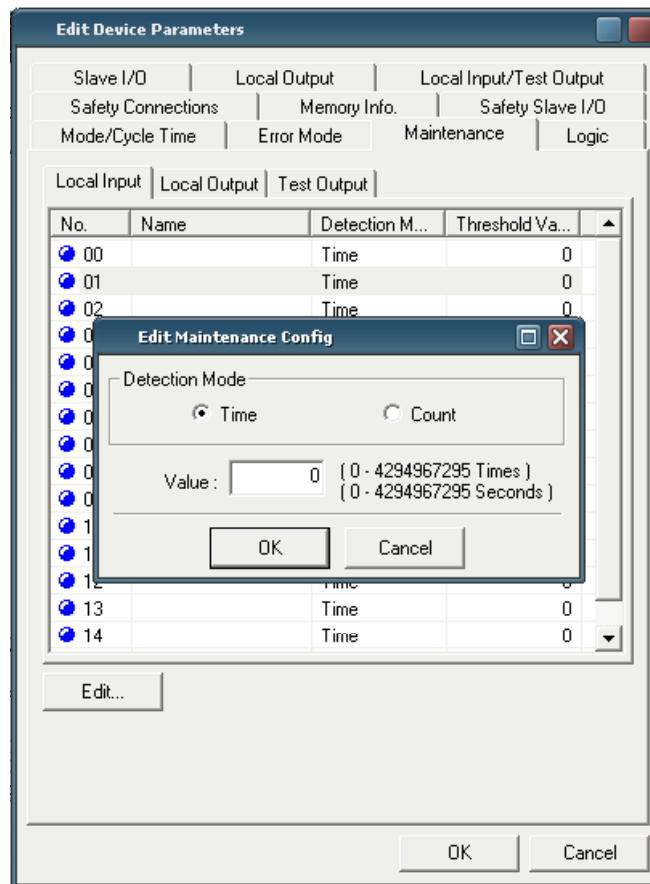


Figure C

Setting the Total ON Time Alarm Threshold with the Network Configurator

The maintenance mode (Maintenance Counter Mode Choice) and alarm threshold (Threshold Maintenance Counter) can be set for each local input, test output, and local output terminal.

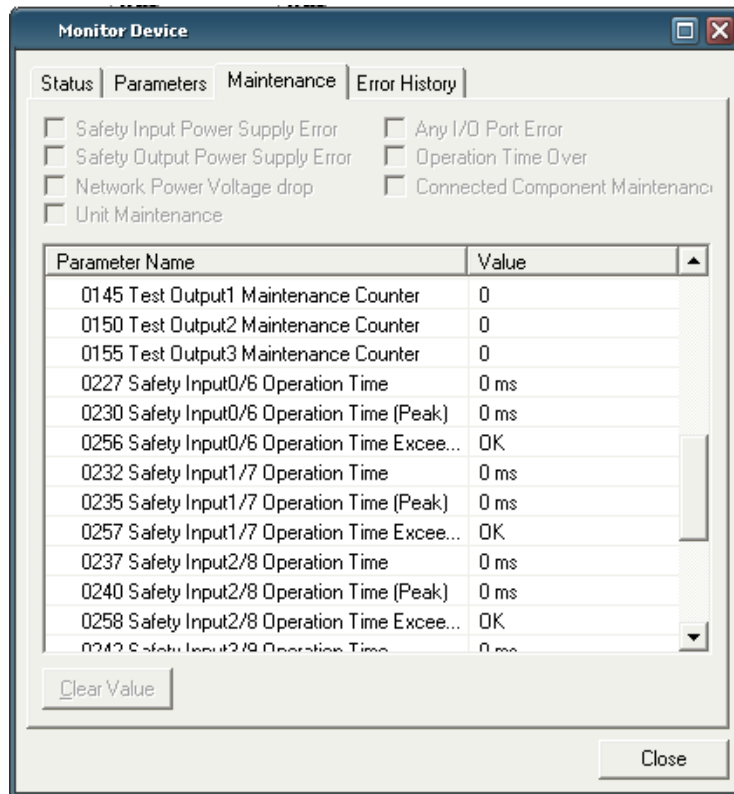


If the alarm threshold (Threshold Maintenance Counter) is set to 0, the Controller will not compare the count or time PV to the alarm threshold SV.

Monitoring the Total ON Time from the Network Configurator

Any of the following methods can be used to monitor the total ON time in the local input status, test output status, or local output status.

- (1) Select the device and select **Device – Maintenance information** from the menu bar.
- (2) Select the device and click the toolbar's **Maintenance** Button.
- (3) Select the device, right-click that device, and select **Maintenance information** from the popup menu.
- (4) Select the device, select **Device – Monitor** from the menu bar, and click the **Maintenance** Tab in the displayed window.
- (5) Select the device, click the toolbar's **Device Monitor** Button, and click the **Maintenance** Tab in the displayed window.
- (6) Select the device, right-click that device, select **Monitor** from the popup menu, and click the **Maintenance** Tab in the displayed window.



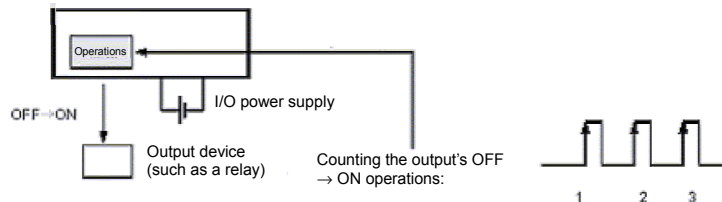
Each I/O point's accumulated total ON time can be cleared. To clear the time, select the total ON time to be cleared and click the **Clear Value** Button.

7-3-2 Contact Operation Counter

Overview

In Ver. 1.0 and higher NE1A-series Controllers, this function counts the number of OFF → ON operations at a local input, test output, or local output and stores the count internally in non-volatile memory.

- Count range: 0 to 4,294,967,295 operations (stored as 00000000 to FFFFFFFF Hex)
- Count units: Operations
- Resolution: Depends on the cycle time.



This information can be monitored using the Network Configurator or explicit messaging.

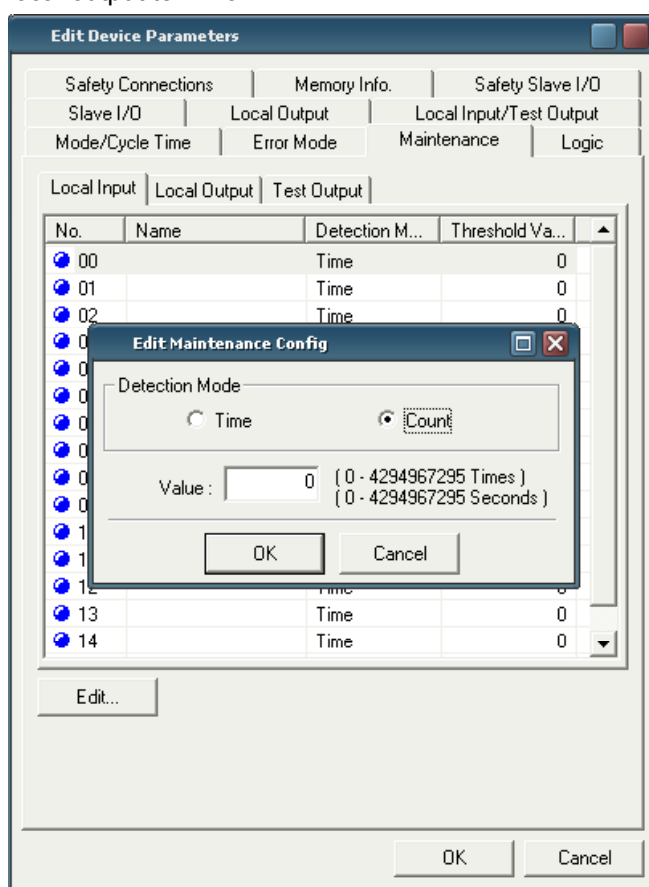
Note 1: The Contact Operation Counter function (Count) and Total ON Time Monitor function (Time) cannot be used simultaneously on one bit. Select one of these functions with the Maintenance Counter Mode Choice setting.

2: When the Maintenance Counter Mode Choice setting is changed, the collected data (operations count or total ON time) will be cleared.

3: These functions do not operate when the I/O power supply is OFF.

Setting the Contact Operations Alarm Threshold with the Network Configurator

The maintenance mode (Maintenance Counter Mode Choice) and alarm threshold (Threshold Maintenance Counter) can be set for each local input, test output, and local output terminal.

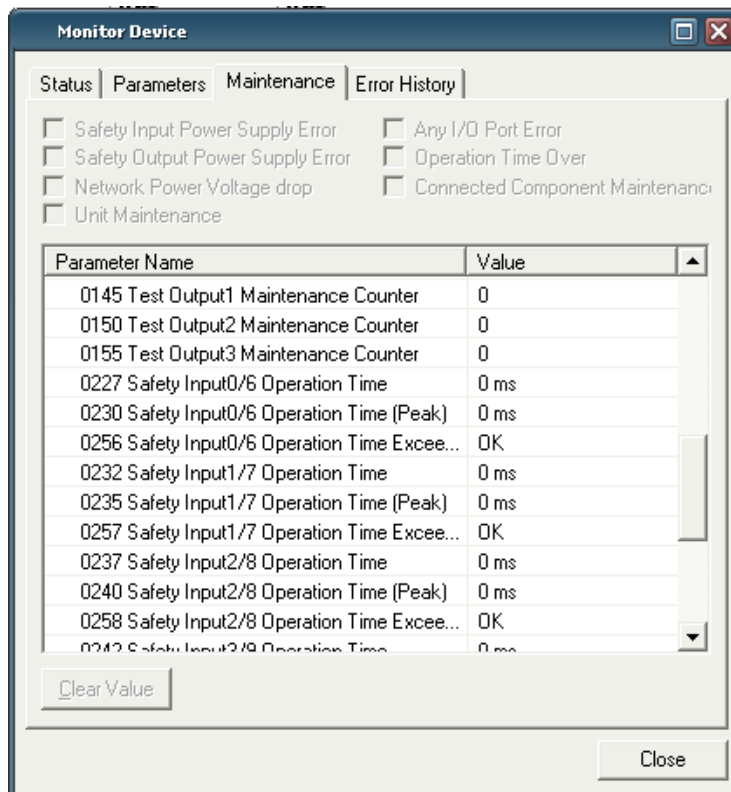


If the alarm threshold (Threshold Maintenance Counter) is set to 0, the Controller will not compare the count or time PV to the alarm threshold SV.

Monitoring Operations from the Network Configurator

Any of the following methods can be used to monitor the number of contact operations in the local input status, test output status, or local output status.

- (1) Select the device and select **Device – Maintenance information** from the menu bar.
- (2) Select the device and click the toolbar's **Maintenance** Button.
- (3) Select the device, right-click that device, and select **Maintenance information** from the popup menu.
- (4) Select the device, select **Device – Monitor** from the menu bar, and click the **Maintenance** Tab in the displayed window.
- (5) Select the device, click the toolbar's **Device Monitor** Button, and click the **Maintenance** Tab in the displayed window.
- (6) Select the device, right-click that device, select **Monitor** from the popup menu, and click the **Maintenance** Tab in the displayed window.

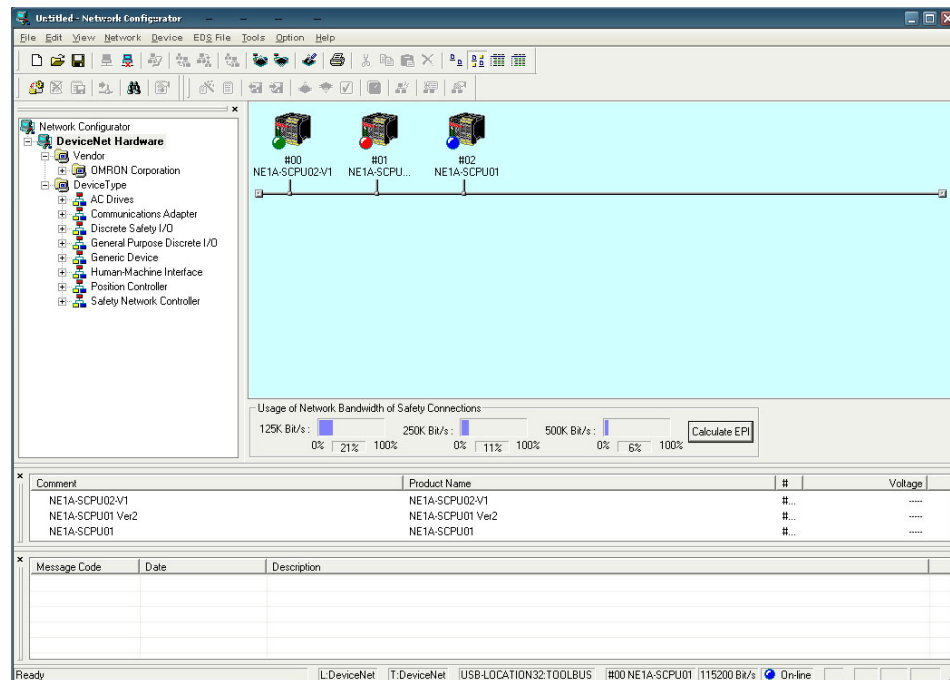


Each I/O point's accumulated contact operations count can be cleared. To clear the count, select the contact operations count to be cleared and click the **Clear Value** Button.

7-4 Displaying Safety Device Status

Device Status Display

Safety information for safety devices (NE1A-SCPU and DST1 Series) can be displayed in Maintenance Mode. An example is shown below.



Moving to Maintenance Mode

The icons that appear in the Maintenance Mode display indicate the status shown in the following table.

Icon (diagram)	Status
Gray with white border	Offline
Gray with green border	Default status (Not set in configuration.)
Green	Idle state
Blue	Normal execution
Yellow	Warning
Red	Alarm

Updating Device Status Displays

Device status displays are automatically updated when the following operations are executed using the Network Configurator.

- Uploading networks
- Downloading networks
- Downloading parameters
- Updating maintenance information
- Uploading device modes (RUN/IDLE)
- Resetting devices

In addition, while online, the display can be updated at any time by selecting **Network –Update Device Status**.

Automatic Updates of Device Status Displays

When the Network Configurator is connected to the system and online, device information can be automatically acquired and the status displayed. To have device status updated and displayed automatically when an online connection is made, select ***Options – Update Device Status automatically, when it was connected on Network.***

Option	Help
Select Interface	▶
Edit Configuration File	▶
Setup Monitor Refresh Timer	
Install Plugin Module	
Install Interface Module	
Update Parameter automatically, when Configuration was changed	
Update Device Status automatically, when it was connected on Network	

Section 8

Troubleshooting

8-1	Connection Status Tables	226
8-1-1	Outline.....	226
8-1-2	Connection Status for DST1 Series	226
8-1-3	Connection Status for the NE1A-series Controller (Safety Slave Function).....	228
8-2	Errors When Downloading	230
8-2-1	Outline.....	230
8-2-2	Error Messages and Countermeasures	230
8-3	Errors When Resetting	233
8-3-1	Outline.....	233
8-3-2	Error Messages and Countermeasures	233
8-4	Errors When Changing Modes	234
8-4-1	Outline.....	234
8-4-2	Error Messages and Countermeasures	234

8-1 Connection Status Tables

8-1-1 Outline

If an error occurs when the NE1A-series Controller tries to establish a safety connection with a DST1-series Safety I/O Terminal or an NE1A-series Controller set as a Slave, the 7-segment display will display the error code "d6".

Check the status code (error code) shown on the Safety Connection Tab Page in the Monitor Device Window and take the corresponding countermeasure.

8-1-2 Connection Status for DST1 Series

Status	Countermeasure
00:0001 Normal communications	The Safety I/O connection status is normal.
01:0001 Safety I/O Connection Timeout	The Safety I/O connection has timed out. Check the following items. <ul style="list-style-type: none"> • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise? • Is the network bandwidth allocation suitable?
01:0105 Configuration Owner Error	The Safety Slave was configured from a configuration tool or Safety Master at a different node address last time. Reset the Safety Slave to the default settings and download the device parameters again. Refer to 5-1-2 <i>Setting Safety Connection Parameters</i> for information on configuration owners.
01:0106 Output Connection Owner Error	The Safety Slave established output safety I/o connections with a Safety Master at a different node address last time. Reset the Safety Slave to the default settings and download the device parameters again. Refer to 5-1-2 <i>Setting Safety Connection Parameters</i> for information on output connection owners.
01:0110 Device Not Configured	The Safety Slave has not been configured. Download the device parameters to the Safety Slave.
01:0113 No. of Connections Error	The setting for the number of safety I/O connections exceeds the upper limit supported by the Safety Slave. Adjust the Safety Connection setting for the relevant Safety Master.
01:0114 Vendor ID or Program Code Error	The device data (vendor ID or product code) for the device on the Configurator and the device used in the actual system does not match. <ul style="list-style-type: none"> • Use Safety Slave Verification (Device – Parameter – Verify) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0115 Device Type Error	The device data (device type) for the device on the Configurator and the device used in the actual system does not match. <ul style="list-style-type: none"> • Use Safety Slave Verification (Device – Parameter – Verify) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0116 Revision Error	The device data (revision) for the device on the Configurator and the device used in the actual system does not match. <ul style="list-style-type: none"> • Use Safety Slave Verification (Device – Parameter – Verify) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.

Status		Countermeasure
01:0117	Connection Path Error	<p>1: Two or more output safety I/O connections have been set for the Safety Slave.</p> <ul style="list-style-type: none"> Change the Safety Connection setting for the Safety Master so there is only one connection. Then reset the Safety Slave to default settings and download the device parameters to the Safety Slave again. <p>2: The same output assembly number for a Safety Slave has been used for both a Safety Master and a Standard Master.</p> <ul style="list-style-type: none"> Input assembly numbers can be duplicated but output assembly numbers cannot. Check the Safety Connection setting for both the Safety Master and the Standard Master then return the Safety Slave to default settings and download the device parameters to the Safety Slave again. If the error remains even after the above countermeasure has been performed, delete and re-register the connections registered to the Safety Master.
01:031E	No. of Connections Error	The setting for the number of safety I/O connections exceeds the upper limit supported by the Safety Slave. Adjust the Safety Connection setting for the relevant Safety Master. In particular, check that no more than 15 Safety Masters are set for each Multi-cast connection, with a maximum total of 30.
01:031F	Connection ID Resource Error	<p>The maximum number of connection IDs for one Safety Master (12) has been exceeded.</p> <p>Change the ID allocation under Edit Safety Connection – Expansion Connection Setting to “Check Produced IDs in the Safety Slave” in the corresponding Safety I/O Connection (Safety Input Assembly) setting, then download the device parameters to the Safety Master again.</p>
01:07FF	Non-existent Safety Slave	<p>The Safety Slave may not have been added to the network correctly. Check that the corresponding Safety Slave is online (i.e., the NS indicator is flashing green or lit green.) If the Safety Slave is not online, check the following items.</p> <ul style="list-style-type: none"> Is the node address for the Safety Slave correct? Do all nodes have the same baud rate? Is the cable length correct (trunk lines and branch lines)? Is the cable disconnected or slack? Is the terminating resistance only on both ends of the main line? Is there a lot of noise?
01:080C	Safety Signature Mismatch	<p>The safety signature for the Safety Slave monitored by the Safety Master does not match the safety signature of the Safety Slave itself.</p> <ul style="list-style-type: none"> Reset the Safety Slave to default settings then download the device parameters again. If the above remedy does not work, delete then re-register the connections registered to the Safety Master.
01:080E	TUNID Mismatch	<p>The TUNID for the Safety Slave monitored by the Safety Master does not match the TUNID of the Safety Slave itself.</p> <ul style="list-style-type: none"> Reset the Safety Slave to default settings then download the correct device parameters. If the above remedy does not work, delete then re-register the connections registered to the Safety Master. <p>Refer to 3-4-2 Network Numbers for information on TUNIDs.</p>
01:080F	Safety Configuration not possible	<p>The Safety Slave is configuration locked and <i>Configure the target device</i> is selected for the Open Type setting for the Safety Master connection.</p> <ul style="list-style-type: none"> Release the configuration lock on the Safety Slave to configure the Safety Slave from the Safety Master. To configure the Safety Slave from a configuration tool, set the Safety Master connection to <i>Check the safety signature</i> under Open Type. Then reset the Safety Slave to default settings and download the device parameters to the Safety Slave again.

8-1-3 Connection Status for the NE1A-series Controller (Safety Slave Function)

Status		Countermeasure
00:0001	Normal communications	The Safety I/O connection status is normal.
01:0001	Safety I/O Connection Timeout	The Safety I/O connection has timed out. Check the following items. <ul style="list-style-type: none"> • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise? • Is the network bandwidth allocation suitable?
01:0106	Output Connection Owner Error	The Safety Slave established an output safety I/O connection with a Safety Master with a different node address last time. Reset the Safety Slave to the default settings and download the device parameters again. Refer to 5-1-2 <i>Setting Safety Connection Parameters</i> for information on output connection owners.
01:0109	Data Size Error	The Safety Slave I/O size set to the NE1A-series Controller Safety Slave and the size set under the Safety Master safety connection setting does not match. The Safety Slave I/O setting may have been changed, so delete then re-register the connections registered to the Safety Master.
01:0110	Unconfigured Device	The Safety Slave has not been configured. Download the device parameters to the Safety Slave.
01:0111	EPI Error	The EPI set under the Safety Master safety connection setting is smaller than the Safety Slave cycle time. The EPI must be longer than both the Safety Master and the Safety Slave cycle times. Check the Safety Master safety connection setting.
01:0113	No. of Connections Error	The setting exceeds the maximum number of safety I/O connections supported by the Safety Slave. Check the relevant Safety Master safety connection settings.
01:0114	Vendor ID or Product Code Error	The device data (vendor ID or product code) for the device on the Configurator and the device used in the actual system does not match. <ul style="list-style-type: none"> • Use Safety Slave Verification (Device – Parameter – Verify) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0115	Device Type Error	The device data (device type) for the device on the Configurator and the device used in the actual system does not match. <ul style="list-style-type: none"> • Use Safety Slave Verification (Device – Parameter – Verify) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0116	Firmware Revision Error	The device data (firmware revision) for the device on the Configurator and the device used in the actual system does not match. <ul style="list-style-type: none"> • Use Safety Slave Verification (Device – Parameter – Verify) to check that the device in the system and the device registered to the Safety Master match. • If they do match, delete then re-register the connections registered to the Safety Master.
01:0117	Connection Path Error	Two or more single-cast safety I/O connections or a multi-cast safety I/O connection with a different EPI has been set for a safety slave I/O. <ul style="list-style-type: none"> • To share one safety slave I/O on a Safety Slave with more than one Safety Master, make the EPI all the same and set the connection type to Multi-cast. • NE1A-series Controller Safety Slaves cannot have more than one single-cast safety I/O connection for each Safety Slave I/O. Set multiple connection paths for the NE1A-series Safety Slave Safety Slave I/O. • If the connection is not restored with the above remedy, delete then re-register the connections registered to the Safety Master.
01:031E	No. of Connections Error	The setting for the number of safety I/O connections exceeds the upper limit supported by the Safety Slave. Adjust the Safety Connection setting for the relevant Safety Master. In particular, check that no more than 15 Safety Masters are set for each Multi-cast connection, with a maximum total of 60.

Status		Countermeasure
01:031F	Connection ID Resource Error	The maximum number of connection IDs for one Safety Master (12) has been exceeded. Change the ID allocation under Edit Safety Connection – Expansion Connection Setting to “Check Produced IDs in the Safety Slave” in the corresponding Safety I/O Connection (Safety Input Assembly) setting, then download the device parameters to the Safety Master again.
01:07FF	Non-existent Safety Slave	The Safety Slave may not have been added to the network correctly. Check that the corresponding Safety Slave is online (i.e., the NS indicator is flashing green or lit green.) If the Safety Slave is not online, check the following items. <ul style="list-style-type: none"> • Is the node address for the Safety Slave correct? • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise?
01:080C	Safety Signature Mismatch	The safety signature for the Safety Slave monitored by the Safety Master does not match the safety signature of the Safety Slave itself. <ul style="list-style-type: none"> • Reset the Safety Slave to default settings then download the device parameters again. • If the above remedy does not work, delete then re-register the connections registered to the Safety Master.
01:080E	TUNID Mismatch	The TUNID for the Safety Slave monitored by the Safety Master does not match the TUNID of the Safety Slave itself. <ul style="list-style-type: none"> • Reset the Safety Slave to default settings then download the correct device parameters. • If the above remedy does not work, delete then re-register the connections registered to the Safety Master. Refer to 3-4-2 Network Numbers for information on TUNIDs.
D0:0001	IDLE Mode	The NE1A-series Safety Master is in IDLE mode, so safety I/O connections have not been established. Change the NE1A-series Safety Master operating mode to RUN mode.

8-2 Errors When Downloading

8-2-1 Outline

The NE1A-series Controller or DST1-series or other Safety Devices may return an error when configuration data is downloaded to them. The cause of the error can be determined from the error information displayed on the Network Configurator.

8-2-2 Error Messages and Countermeasures

Message displayed on the Network Configurator	Countermeasure
Object state conflict.	A fatal error (Abort)(MS indicator flashes red) has occurred. Set the switches correctly or execute reset (Out-of-Reset) to clear the configuration data.
The device is locked.	The configuration data is locked. (LOCK indicator is lit.) Release the lock.
The TUNID not matched.	<p>The device is waiting for a TUNID setting after being reset (NS indicator is flashing green/red) or the TUNID of the Network Configurator is different from the device when downloading. Use the following steps to check the setting.</p> <ol style="list-style-type: none"> (1) Reset the device to default settings then download the parameters again. The network number may, however, be different from other devices. If the NE1A-series Controller 7-segment display shows "d6" (A <i>Safety I/O Connection Establishment Failure</i> message appears on the Error History Tab Page in the Network Configurator Monitor Device Window) after the operating mode has been changed, use steps (2) or (3) to correct the error. (2) Select Network – Upload in the Network Configurator. Unify the network numbers and reset all devices to the default settings. Once reset, download the parameters to all devices again. (3) Select Network – Property to display the Network Property Dialog Box in Network Configurator then click the Get from Network Button in the Network Number Field. If there are multiple network numbers, select one of these numbers to unify all to that network number.
Privilege violation.	<p>The password used does not provide authority to change configurations. Check that the correct password is being used.</p> <p>Attempted to change the setting to stand alone mode via DeviceNet. Connect the Network Configurator to a USB connection and download the data again.</p>
Device state conflict.	Downloading from more than one Network Configurator at the same time. Wait until other downloads have been completed.
The error occurred in the validation of a device parameter.	<p>There is a non-alignment between configuration parameters. Check the following items and change the parameters.</p> <ul style="list-style-type: none"> • The time parameters (e.g., Discrepancy Time) set for function blocks in the NE1A-series Controller settings are shorter than the NE1A-series Controller cycle time. • The safety connection EPI is shorter than the cycle time. • The safety inputs are set to <i>Test pulse from test out</i> but the test source has not been set. • One of the safety inputs in a dual channel setting is set as a standard input and the other has a different setting. • One of the safety inputs in a dual channel setting is set to <i>Not used</i> and the other has a different setting. • One of the safety outputs in a dual channel setting is set to <i>Not used</i> and the other has a different setting. • The maximum number of connection IDs for one Safety Master (12) has been exceeded in the safety I/O configuration. Change the ID allocation under Edit Safety Connection – Expansion Connection Setting to "Check Produced IDs in the Safety Slave" in the corresponding Safety I/O Connection (Safety Input Assembly) setting, then download the device parameters to the Safety Master again.

Message displayed on the Network Configurator	Countermeasure
The error occurred in the validation of a device parameter.	<p>The program may have been created with an earlier Network Configurator than version 1.5□. The checks for safety functions have been improved in version 1.5□ so programs created in an earlier version of the NE1A-series Controller cannot be downloaded as is. Use the following procedure to convert the program and then download the program again.</p> <ol style="list-style-type: none"> (1) Click the Edit Button on the Logic Tab page in the Edit Device Parameters Window of the NE1A-series Controller to open the Logic Editor. (2) Select Edit – Find Function Blocks with Open Connections to check all function block I/O are connected. For information on open function block connections, refer to <i>Precautions When Moving from Version 1.3□ to 1.5□</i> on page 24. (3) Select File – Apply to save the logic program then close the Logic Editor. (4) Return to the NE1A-series Controller's Edit Device Parameters Window and click the OK Button. <p>The hardware may be malfunctioning. Cycle the NE1A-series Controller power and execute self-diagnosis. If the MS indicator is lit red, replace the hardware.</p>
Logic Editor: Consistency Error.	The network configuration has changed, which has resulted in a non-alignment between the logic program data and other data. Start Logic Editor and check changed I/O locations and make the settings again.
Device can not be accessed.	<p>Device is waiting for a TUNID setting (NS indicator is flashing green/red) after reset was executed from another node during download. Set the TUNID and download again.</p> <p>Refer to 3-4-2 <i>Network Numbers</i> for information on TUNIDs.</p>
Connection can not be opened.	<p>1: Could not establish connection with device when downloading to the device via DeviceNet. Check that the power is ON to the device and download again.</p> <p>2: The connection resources available for the device are being used to establish safety I/O connections with the Safety Master, so a connection cannot be established with the Network Configurator. Change the operating mode of the Safety Master to which the safety connections are registered to IDLE mode.</p> <p>3: If the above causes do not apply, noise or other factors may be making communications unstable. Check the following items.</p> <ul style="list-style-type: none"> • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise?
Sending message failed.	Downloaded via USB to the device but could not connect to the device. Check that the power is turned ON to the device and download again.
Connection failed.	<p>Tried to configure a device on the DeviceNet network via the NE1A-series Controller USB port, but connection failed. Check that power is turned ON to the device and download again.</p> <p>If the above cause does not apply, noise or other factors may be making communications unstable. Check the following items.</p> <ul style="list-style-type: none"> • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise?
In order to configure the device, the device needs to be reset. Because, the device is configured by another device.	<p>The Safety Slave was configured from a Safety Master last time (see note). Reset the Safety Slave to default settings and download the device parameters again.</p> <p>Note: Refer to 5-1-2 <i>Setting Safety Connection Parameters</i> for information on configuration from Safety Masters.</p>

Section 8-2 *Errors When Downloading*

Message displayed on the Network Configurator	Countermeasure
Logic is incomplete. Please confirm logic.	<p>There are open inputs or outputs in a function block used in the logic program. Click the Edit Button on the Logic Tab Page to open the logic and perform the following measures.</p> <ul style="list-style-type: none">• Connect the open inputs or outputs.• Change the number of I/O setting for the function block to delete the open input or output. <p>Function blocks with open inputs or outputs can be searched by using Edit – Find Function Blocks with Open Connections. For details, refer to <i>Finding Function Block with Open Connections</i> in 6-3-3 <i>Programming Using Function Blocks</i> and <i>Precautions When Moving from version 1.3□ to 1.5□</i> on page 24.</p>

8-3 Errors When Resetting

8-3-1 Outline

When the NE1A-series Controller or a DST1-series or other Safety Device is reset, the device may return an error response. The cause of the error can be determined from the error information shown in the Network Configurator.

8-3-2 Error Messages and Countermeasures

Message displayed on the Network Configurator	Countermeasures
Object state conflict.	The specified reset cannot be executed in the current device status. Refer to 7-2-2 <i>Reset Type and NE1A-series Controller Status</i> in the Safety Network Controller Operation Manual (Z906) and change the operating mode or configuration lock status of the NE1A-series Controller. Then execute the reset again.
Invalid TUNID of Device (%s). Device will be reset by Device's TUNID. OK?	The TUNID saved to the device and the TUNID specified by Network Configurator do not match. Check that the device MAC ID matches and execute the reset if it is OK to use the device TUNID.
Privilege violation.	The password used does not provide authority to change configurations. Check that the correct password is being used.
Specified device can not be accessed, or wrong device type or password.	The device has just been reset or the power cycled and the device is not ready for communications (i.e., not online with the NS indicator flashing or lit green.) Check that the device is communications ready then reset.
	The device specified for reset may not support that service. Check that the device node address is correct.
	The configuration data is locked. (The LOCK indicator is lit.) Remove the lock then execute the specified reset.
	The device is performing safety I/O communications and cannot, therefore, execute the specified reset. Change the operating mode of the relevant Safety Master to IDLE mode. Then execute the specified reset.
Connection failed.	<p>Tried to reset a device on the DeviceNet network via the NE1A-series Controller USB port, but connection failed. Check that power is turned ON to the device and reset again.</p> <p>If the above cause does not apply, noise or other factors may be making communications unstable. Check the following items.</p> <ul style="list-style-type: none"> • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise?

8-4 Errors When Changing Modes

8-4-1 Outline

When the operating mode of the NE1A-series Controller or DST1-series or other Safety Device is changed, the device may return an error response. The cause of the error can be determined from the error information shown in the Network Configurator.

8-4-2 Error Messages and Countermeasures

Message Displayed on the Network Configurator	Countermeasures
Object state conflict.	A fatal error (Abort)(MS indicator flashes red) has occurred. Set the switches correctly or execute reset (Out-of-Reset) to clear the configuration data.
Object state conflict.	<ol style="list-style-type: none"> 1. The device has not been configured (Configuration Mode). Download the device parameters. 2. A fatal error (Abort) has occurred. Set the switches correctly or execute reset (Out-of-Reset) to clear the configuration data. Once the configuration data is cleared, download the device parameters again.
Already set to the specified mode.	The device is already in the specified operating mode.
The TUNID is not matched.	The TUNID saved to the device and the TUNID specified by the Network Configurator do not match. Check that the device MAC ID matches. If it does, it means that the device network number and the network number in the Network Configurator do not match. Select Network – Upload in the Network Configurator to match the network numbers.
Privilege violation.	The password used does not provide authority to change the operating mode. Check that the correct password is being used.
Specified device can not be accessed, or wrong device type or password.	The device has just been reset or the power cycled and the device is not ready for communications (i.e., not online with the NS indicator flashing or lit green.) Check that the device is communications ready then reset.
	The device for which the operating mode change request was made may not support that service. Check that the device MAC ID is correct.
Connection failed.	<p>Tried to change the operating mode of a device on the DeviceNet network via the NE1A-series Controller USB port, but connection failed. Check that power is turned ON to the device and reset again.</p> <p>If the above cause does not apply, noise or other factors may be making communications unstable. Check the following items.</p> <ul style="list-style-type: none"> • Do all nodes have the same baud rate? • Is the cable length correct (trunk lines and branch lines)? • Is the cable disconnected or slack? • Is the terminating resistance only on both ends of the main line? • Is there a lot of noise?

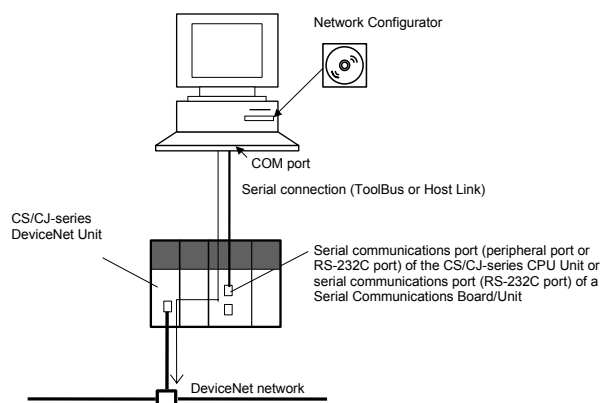
Appendices

A-1 Connecting to the Network via a CS/CJ-series PLC

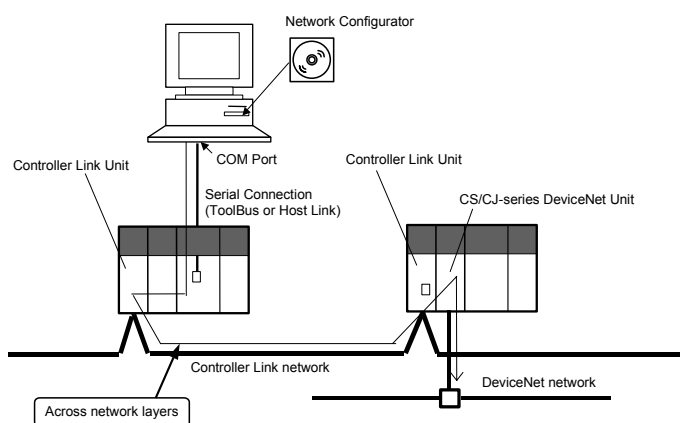
A-1-1 Connecting to the DeviceNet Network

The Network Configurator can be connected online to the DeviceNet network via a serial communications port on a CS/CJ-series CPU Unit or via a CS/CJ-series Ethernet Unit, as shown in the following figure. This section describes the procedure. Refer to 3-3 *Connecting to the Network* to connect to the network via the USB port on the NE1A-series Controller and a DeviceNet Interface Card installed in the computer.

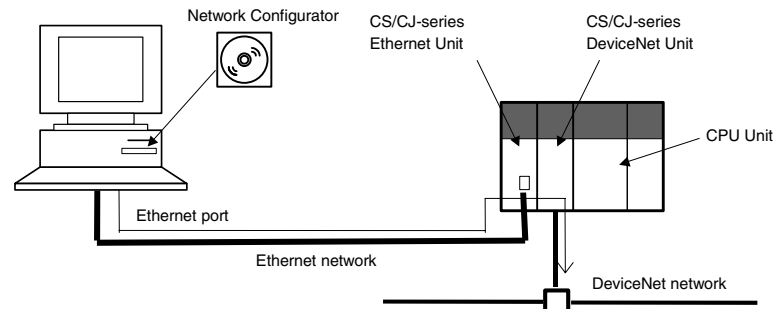
- 1) Connect the COM port on the computer to a serial communications port on the CS/CJ-series CPU Unit (i.e., the peripheral port or the RS-232C port) or a Serial Communications Board/Unit (i.e., a RS-232C port or a RS-422A/485 port) using a peripheral bus (ToolBus) or Host Link connection. To connect to the DeviceNet network, the PLC must have a CS/CJ-series DeviceNet Unit (i.e., the CS1W-DRM21(-V1) or CJ1W-DRM21).



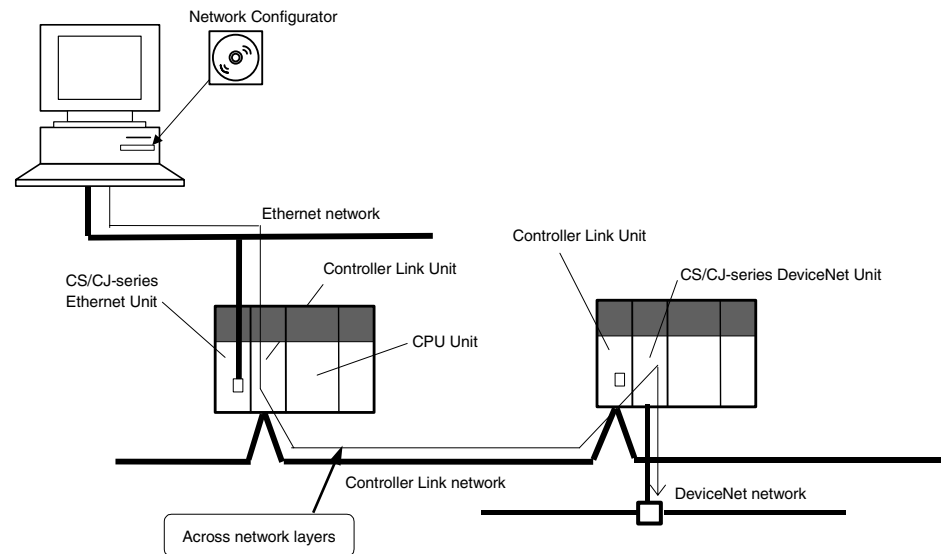
The DeviceNet can be connected to crossing multiple network layers (3 layers max.) using serial communications, as shown in the following figure.



- 2) Connect the Ethernet port of the computer to a CS/CJ-series Ethernet Unit.
To connect to the DeviceNet network, the PLC must have a CS/CJ-series DeviceNet Unit (i.e., the CS1W-DRM21(-V1) or CJ1W-DRM21).



The DeviceNet network can be connected to crossing multiple network layers (3 layers max.) using Ethernet, as shown in the following figure.



A-1-2 Specifying the Connection Interface

Use the following procedure to specify the connection interface to use.

Note: Specify the connection interface whenever specifying an online connection.

- 1 Select **Option - Select Interface** from the menu bar.
(The interface currently used will be selected.)
- 2 Select an interface to use from those displayed on the submenu.
 - Serial Port: Select **SYSMAC CS/CJ I/F Port**.
 - Ethernet Unit: Select **SYSMAC CS/CJ Ethernet Unit I/F**.
- 3 Select **Network - Connect** from the menu bar.
The window corresponding to the specified connection interface will be displayed.
Refer to *Specifying the SYSMAC CS/CJ Interface Port as the Connection Interface*
or *Selecting the SYSMAC CS/CJ Ethernet Unit Interface as the Connection Interface* in the following pages for the operating procedure.

Note: The interface cannot be changed while the Network Configurator is online.
Select **Network – Unconnect** and then change the interface offline.

Specifying the SYSMAC CS/CJ Interface Port as the Connection Interface

(Continued from step 3 on the previous page.)

- 1 When **SYSMAC CS/CJ I/F Port** is selected as the connection interface, the Setup Interface Window will be displayed. An example is shown below.

The screenshot shows a 'Setup Interface' dialog box with the following settings:

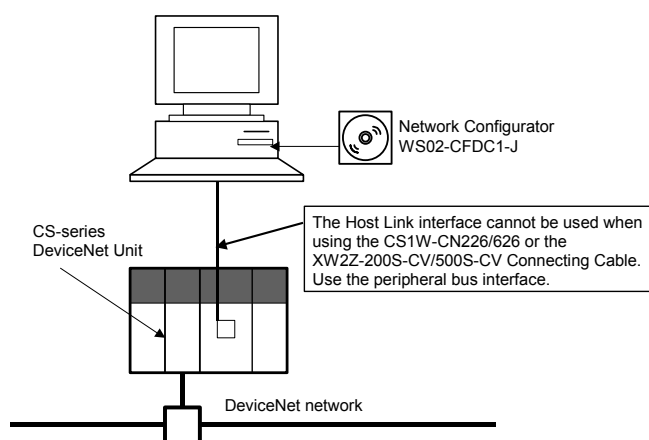
- Interface: Toolbus
- Network Address: 0
- Node Address: 0
- Unit No.: 0
- COM Port: COM1
- Baud Rate: 115200 Bit/s
- Data Length: 8Bits
- Parity: No
- Stop Bit: 1Bit

Set each item as described below.

Interface	<p>Select either one of the following interfaces as the serial communications mode for the serial communications port on the CS/CJ-series PLC.</p> <ul style="list-style-type: none"> • Peripheral bus (ToolBus) • Host Link
Network Address	<p>Enter the FINS network address of the destination DeviceNet Unit. Enter this address when crossing the network farther than the serial communications port of the CS/CJ-series CPU Unit. Enter 0 when not crossing network layers.</p>
Node Address	<p>Enter this address when crossing the network farther than the serial communications port of the CS/CJ-series CPU Unit. Enter 0 when not crossing network layers.</p>
CPU Bus Unit Number	<p>Enter the unit number of the DeviceNet Unit (i.e., the CS1W-DRM21(-V1)) as a CPU Bus Unit (i.e., the value set on the rotary switches on the front of the DeviceNet Unit).</p> <ul style="list-style-type: none"> • The unit number is between 0 and 15.
Communications Port	<p>Select the COM port on the computer running the Network Configurator (version 2.□).</p> <ul style="list-style-type: none"> • Select from the list of available COM ports.

Baud Rate	<p>Set the baud rate for the serial communications port on the CS/CJ-series PLC.</p> <ul style="list-style-type: none"> • 9,600, 19,200, 38,400, or 115,200 bit/s. <p>Note: The baud rates that can be selected for the peripheral bus (ToolBus) and Host Link are different. For details, refer to the <i>CS/CJ Series Operation Manual</i>.</p>
Data Length	<p>Set the data length for the serial communications port on the CS/CJ-series PLC. This setting is required only when using the Host Link interface.</p> <ul style="list-style-type: none"> • 7 or 8 bits
Parity	<p>Set the parity for the serial communications port on the CS/CJ-series PLC. This setting is required only when using the Host Link interface.</p> <ul style="list-style-type: none"> • None, even, or odd
Stop Bits	<p>Set the number of stop bits for the serial communications port on the CS/CJ-series PLC. This setting is required only when using the Host Link interface.</p> <ul style="list-style-type: none"> • 1 or 2 bits

IMPORTANT: Always select the peripheral bus (ToolBus) interface when making a serial connection through the CS1W-CN226/626 or the XW2Z-200S-CV/500S-CV Connecting Cable to a CS-series PLC with the CS1W-DRM21(-V1) mounted to the CPU Rack. A connection will not be possible if the Host Link interface is selected.



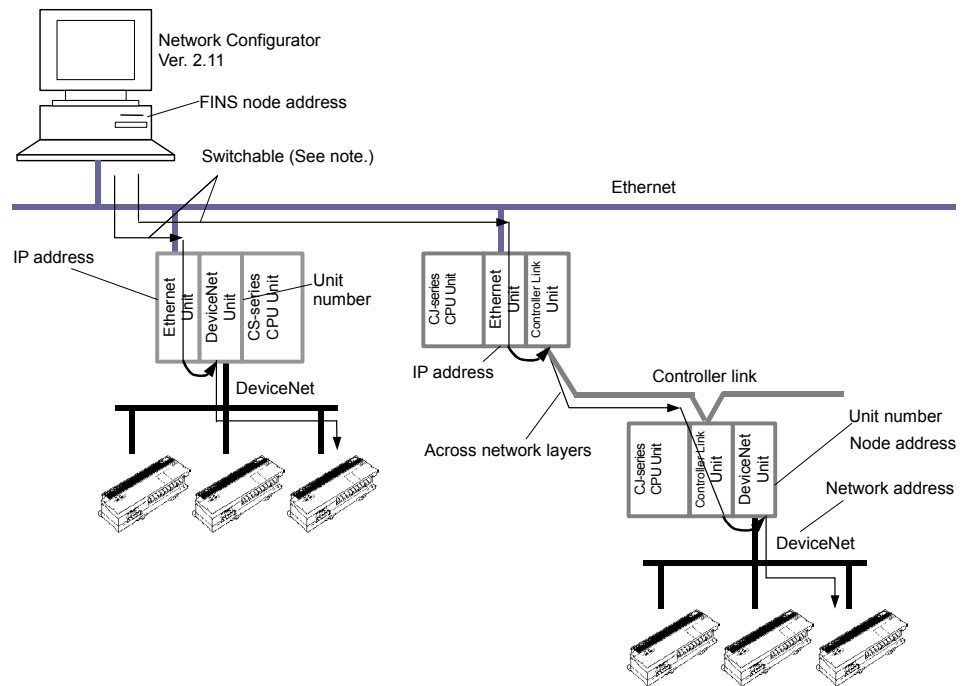
- Note:**
- For information on the FINS node address, refer to the *CS/CJ-series DeviceNet Unit Operation Manual (W380)*.
 - When **Host link** is selected, it may take several minutes to download from the network. It is recommended to select the *Peripheral Bus (ToolBus)* for the serial connection.

Selecting the SYSMAC CS/CJ Ethernet Unit Interface as the Connection Interface

The user can connect the computer (i.e., the Network Configurator) directly to an Ethernet network and connect online to the DeviceNet network using a CS/CJ-series Ethernet Unit and CS/CJ-series DeviceNet Unit.

Note: Connection via Ethernet is supported only when using both the CS/CJ-series Ethernet Unit and the CS/CJ-series DeviceNet Unit. (This connection is not possible if Units from any other PLC Series are used.)

When multiple PLCs with both Ethernet Units and DeviceNet Units are connected to the Ethernet network, the specified DeviceNet network can be connected to online by switching the connection destination. The destination DeviceNet network is registered by specifying the IP address of the Ethernet Unit and the unit number of the DeviceNet Unit.



Note: The registered name of the destination DeviceNet network can be specified to switch the destination DeviceNet network. The name of the destination DeviceNet network can be registered by specifying the following items.

- IP address and UDP port number of the Ethernet Unit
- Network address, node address, and CPU Bus Unit unit number of the DeviceNet Unit
- FINS node address of the computer (i.e., the Network Configurator)

Registering Destination DeviceNet Networks

It is necessary to register the destination DeviceNet network in advance for a connection via Ethernet. A maximum of 20 DeviceNet networks can be registered. Use the following procedure to register the destination DeviceNet network.

- 1 Select **Network - Connect**.
- 2 The following window will be displayed.

Interface Setting Window

Host (PC) Information	Settings of the computer running the Network Configurator are displayed.	
	Host Name	The name of the computer is displayed automatically.
	IP Address	The IP address of the computer is displayed automatically.
	Network Address	The FINS network address set in the computer is displayed. (The value set in the Destination Registration Window after clicking the Set Button in step 3 below will be displayed.)
	Node Address	The FINS node address set in the computer is displayed. (The value set in the Destination Registration Window after clicking the Set Button in step 3 below will be displayed.)

- Click the **Set** Button. The Destination Registration Window will be displayed. An example is shown below.

Destination Registration Window

Destination Registration Window

Registration Name	Set the registered name of the destination DeviceNet network. Up to 20 names can be registered. A registration name can use up to 25 characters.		
Host (PC) Information	Computer (i.e., Network Configurator) settings		
	Network Address	Enter the FINS network address of the computer. Set the same value as the network address of the Ethernet Unit. Enter 0 to not set a network address.	
	Node Address	Enter the FINS node address of the computer.	
Remote Information	Setting items for the DeviceNet and the Ethernet Unit that relay the connection to the DeviceNet Network.		
	DeviceNet Unit	Network Address	Enter the FINS network address of the destination DeviceNet Unit. Enter an address here to cross the network farther than the Ethernet network directly connected to the computer. Enter 0 when not crossing network layers.
		Node Address	Enter the node address of the destination DeviceNet Unit. Enter an address here to cross the network farther than the Ethernet network directly connected to the computer. Enter 0 when not crossing network layers.
		CPU Bus Unit Number	Enter the unit number of the destination DeviceNet Unit as a CPU Bus Unit.
	Ethernet Unit	Port Number	Enter the UDP port number for the FINS of the Ethernet Unit.
		IP Address	Enter the IP address of the Ethernet Unit.

Setting the Network Address in the Host (PC) Information Area

Set the FINS node address of the computer.

The computer (i.e., the Network Configurator) uses the OMRON FINS communications service to connect to the DeviceNet network via the Ethernet. It is necessary to set the FINS node address as well as the IP address.

For the network address, set the same value as the Ethernet Unit. The network address of the Ethernet Unit is set in the routing table of the CPU Unit. Enter 0 when not using the routing table.

Setting the Node Address in the Host (PC) Information Area

Set the FINS node address of the computer.

For this setting, it is necessary to set the correspondence between the remote IP address and the FINS node address using the OMRON Ethernet Unit. For details, refer to the *SYSMAC CS/CJ Series Ethernet Unit Operation Manual (W420, W421 and W343)*.

Setting the Network Address in the *DeviceNet Unit* Field of the Remote Information Area

Set the FINS network address of the DeviceNet Unit to which the destination DeviceNet network is connected.

Enter the value when crossing the network farther than the Ethernet network directly connected to the computer. Enter 0 when not crossing network layers.

Setting the Node Address in the *DeviceNet Unit* Field of the Remote Information Area

Set the Node Address of the DeviceNet Unit to which the destination DeviceNet network is connected.

Enter the value when crossing the network farther than the Ethernet directly connected to the computer. Enter 0 when not crossing network layers.

Setting the CPU Bus Unit Number in the *DeviceNet Unit* Field of the Remote Information Area

Set the unit number (0 to F) of the DeviceNet Unit as a CPU Bus Unit to which the destination DeviceNet network is connected.

Setting the Port Number in the *Ethernet Unit* Field of the Remote Information Area

Set the UDP port number with which the Ethernet Unit performs the FINS Communications Service. Set the same value as in the setting in the CPU Bus Unit System Setting Area in the CPU Unit to which the Ethernet Unit is mounted. Normally 9600 is used.

Setting the IP Address in the *Ethernet Unit* Field of the Remote Information Area

Set the IP address of the Ethernet Unit.

To set the IP address of the Ethernet Unit, refer to *SYSMAC CS/CJ Series Ethernet Unit Operation Manual (W420, W421 and W343)*.

- 4 Click the **Register** Button. The set values will be registered and displayed in the Registration List.
 - Name: Registration name of the destination DeviceNet network
 - Node: FINS network address and FINS node address (the third number is always 0) of the computer
 - Unit: FINS network address, FINS node address, and unit number of the DeviceNet Unit
 - Port: FINS UDP port number of the Ethernet Unit
 - IP Address: IP address of the Ethernet Unit
- 5 Click the **Close** Button to exit and return to the Setup Interface Window.

Selecting the Registration Name (Destination DeviceNet Network)

Select the DeviceNet network that you want to connect from the registration names of the registered connection destinations in the Setup Interface Window.

- 1 Select the destination registration name from the *Registration Name* Drop-down List in the *Remote Information Area*.

In the *Remote Information Area*, the following set values of the selected registration name will be displayed.

- Network Address: FINS network address of the DeviceNet Unit
- Node Address: Node address of the DeviceNet Unit
- CPU Bus Unit Number: Unit number of the DeviceNet Unit
- Port Number: FINS UDP port number of the Ethernet Unit
- IP Address: IP address of the Ethernet Unit

- 2 Click the **OK** Button.

Click the **OK** Button in the confirmation dialog box.

The connection to the DeviceNet network will be made.

When the connection is successful, the status indicator on the status bar will turn blue and "On-line" will be displayed.

Note: For information on FINS network addresses and FINS node addresses, refer to the *CS/CJ Series DeviceNet Unit Operation Manual (W380)* and the *SYSMAC CS/CJ Series Ethernet Unit Operation Manual (W420, W421 and W343)*.

A-2 Editing CS/CJ-series DeviceNet Unit Parameters

This section describes how to edit the parameters of a CS/CJ-series DeviceNet Unit.

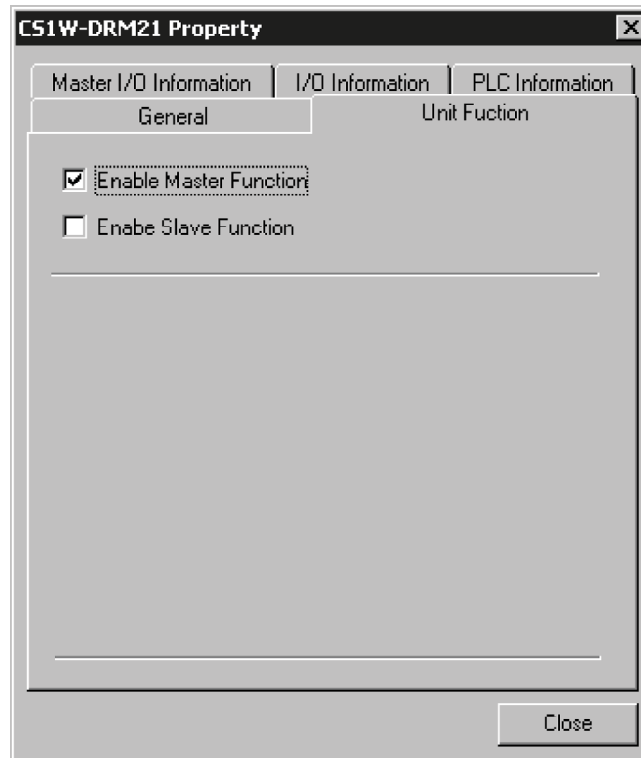
A-2-1 Setting the Unit Functions

The master function and slave function can be set.

Follow the procedure below to perform the settings.

- 1 Select the icon of the master in the Network Configuration Pane (right pane).
- 2 Select **Device - Property**.

The following window will be displayed. Click the **Unit Function** Tab.



- 3 Select the *Enable Master Function* or *Enable Slave Function* Option (or both).

A-2-2 Master Parameter Overview

Use the following procedure to open the Parameter Edit Window.

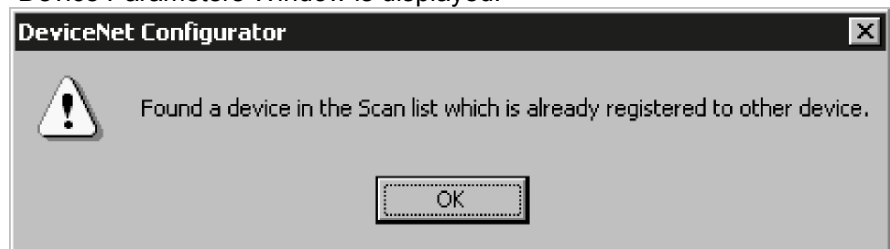
- 1 Select the device for which you want to edit the parameters.
- 2 Select **Device - Parameter - Edit**.
- 3 The Edit Device Parameters Window for the master will be displayed.

Note: • If the I/O size of the device displayed in the Network Configuration Pane and the I/O data size of the device registered in the Scan List do not match, the following warning dialog box will be displayed and the I/O size set in the Scan List will be given priority.



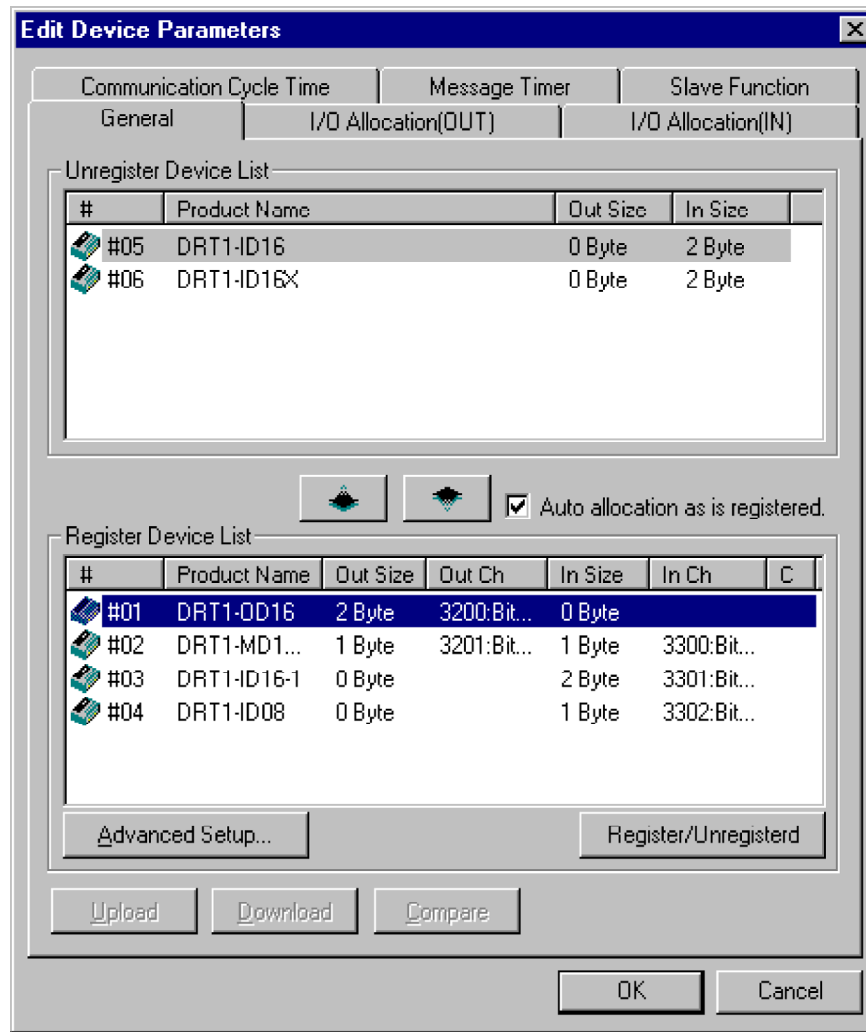
If there is a slave with no EDS installed, obtain an EDS and install it.

- If a slave device registered to another master device is registered in the Scan List, the following warning message will be displayed when the Edit Device Parameters Window is displayed.



Modify the registered slave in the Scan List.

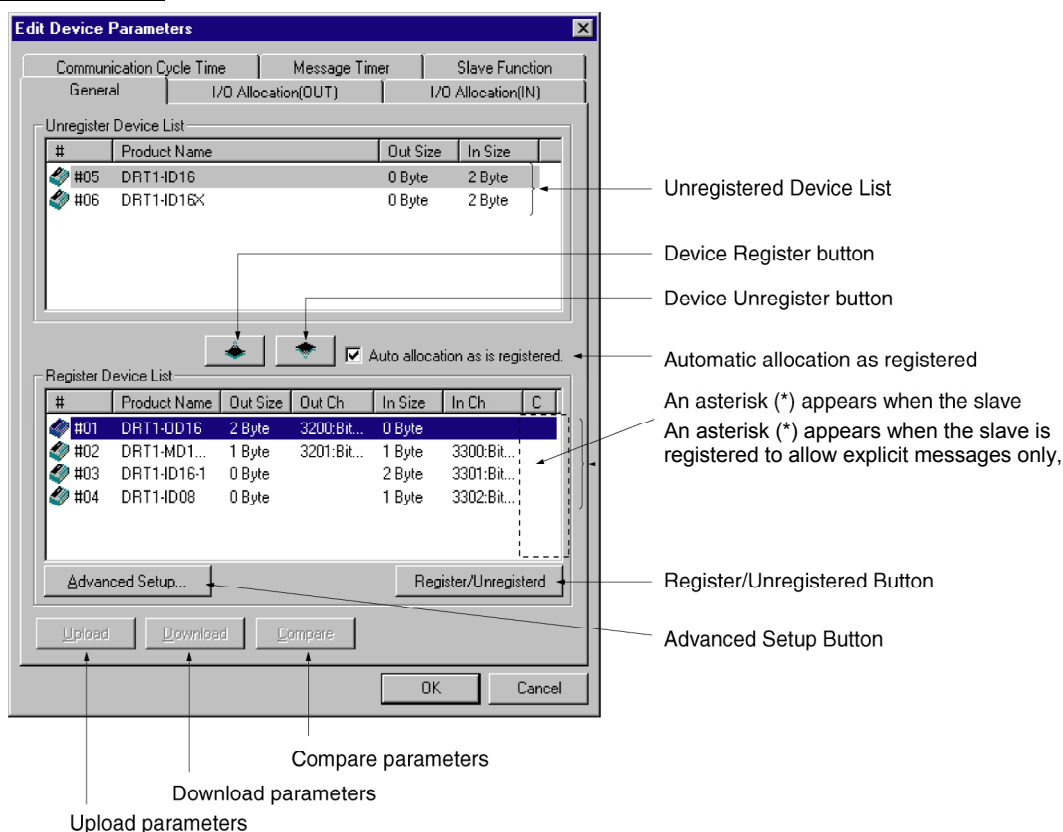
- To operate the master function, select a device, select **Device - Properties**, and then select the Enable Master Function Option in the Property Dialog Box of the CS1W-DRM21(-V1)/CJ1W-DRM21.





The Edit Device Parameters Window consists of the following 5 tab pages.

Tab page name	Description
General	Registers devices in the Scan List and performs I/O allocations using automatic setting.
I/O Allocation (OUT)	Sets the OUT data allocation and OUT memory block of the CPU Unit using the Advanced Setup.
I/O Allocation (IN)	Sets the IN data allocation and IN memory block of the CPU Unit using the Advanced Setup.
Communication Cycle Time	Sets the communications cycle time.
Slave Function	Sets parameters for using the slave function.
Message Timer	Set the monitoring timer for message communications (the same time is used for both explicit and FINS message communications).

General Tab Page



Item	Description
Unregistered Device List	Displays the slave devices displayed in the Network Configuration Pane but not yet registered to a master.
Registered Device List	Displays slave devices currently registered to the master.
Device Register and Unregister Buttons	 Use the Device Register Button to move a device from the Unregistered Device List above to the Registered Device List below.  Use the Device Unregister Button to move a device from the Registered Device List below to the Unregistered Device List above.
Auto allocation as is registered	Select this option to allocate unused words in the registration order when registering slaves to a master in the Edit Device Parameters Window.
Register/Unregister Button	Click this button to cancel and re-allocate the I/O allocations (allocation of unused words with no unallocated words) to the selected slave.
Advanced Setup Button	Click this button to set the connection settings and to display or check device information.
Upload Button	Click this button to upload online device parameters from devices in an actual network.
Download Button	Click this button to download online device parameters to devices in an actual network.
Verify Button	Click this button to verify online parameters of devices in an actual network and the parameters held by the Network Configurator.

Slave Registration and Automatic I/O Area Allocation

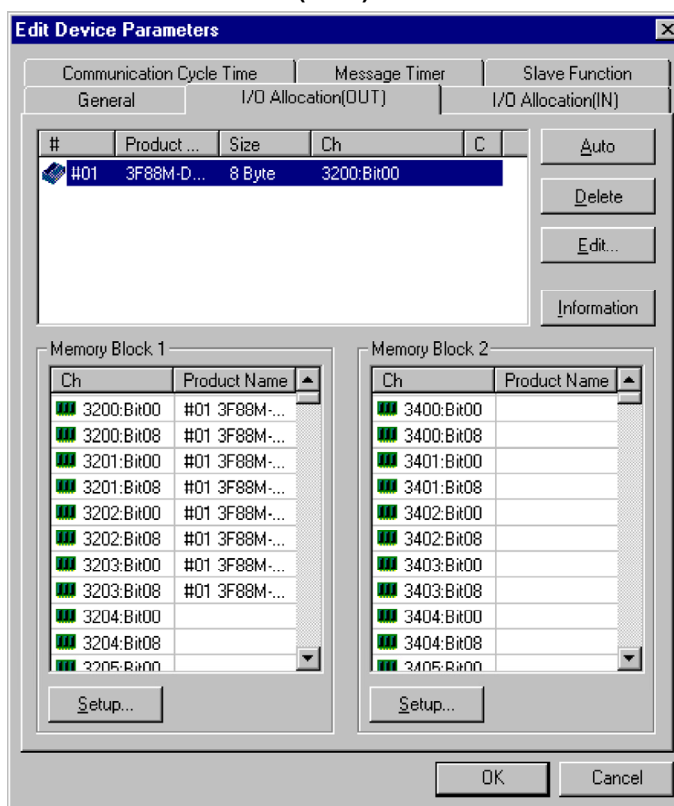
If a slave is registered when the master function is enabled, words are automatically allocated to it in the memory block set for I/O allocation.

Allocation is performed forward from the beginning of Memory Block 1 in the order of registration for both the input and output areas. When Memory Block 1 is completely allocated, allocation is performed in Memory Block 2. Set the areas and ranges of the memory blocks for allocation in advance before registering slaves.

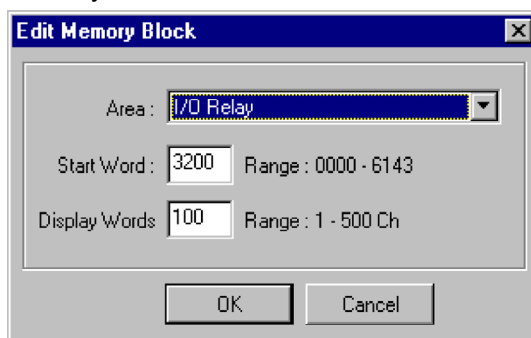
Note: Auto-allocation areas can be changed later.

Setting Memory Blocks for Allocation

- 1 Select a master and then select **Device – Parameter – Edit**. The Edit Device Parameter Dialog Box will be displayed.
- 2 Click the **I/O Allocation (OUT)** Tab.



- 3 Click the **Setup...** Button in the Memory Block 1 Area.
- 4 Set the **Area**, **Start Word**, and **Display Words** (i.e., the number of words in) for Memory Block 1.



- 5 Set Memory Block 2 in the same way.

- 6 Click the **I/O Allocation (IN)** Tab and set the Memory Blocks in the same way as the OUT block.

- Note:**
- Set the Area setting for unused blocks to *Not Use*.
 - The number of displayed words is the number of words of a block displayed in the Network Configurator. This value is not downloaded to the Unit. If the allocated area in a block is 100 words or less when uploaded, the number of displayed words will be set to 100 and displayed.

Specifying Auto-allocation at Registration

- If the option for auto-allocation (*Auto-allocation as is registered*) is selected, words will be allocated for I/O automatically in the order of registration when slaves are registered to a master in the Edit Device Parameters Window. This option is effective only in the Edit Device Parameters Window.
Auto-allocation allocates words starting from unused words in Block 1 of the corresponding I/O memory block in the order of registration (i.e., in the order slaves are dropped).
- Deleting or changing I/O allocations for the selected slaves (allocating unused word) can be performed anytime by clicking the Auto Register/Unregister Button.

A-2-3 I/O Allocation Using the Parameter Wizard (Simple I/O Allocation)

- I/O in PLC memory can be allocated to slaves simply and interactively.
- I/O allocation is as follows: In order of node addresses, simple I/O allocation from Block 1, and I/O allocation of 100-word blocks.

Allocation is performed in the order of slave node addresses from Block 1 (allocating from Block 2 when Block 1 is completely allocated) with a block size of 100 words.

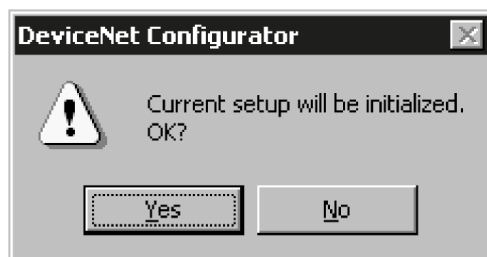
Note: After allocating I/O using this wizard, node addresses can be changed and other allocation changes can be made in the *Editing Parameters*, as described later.

The Parameter Wizard specifies the beginning address of each block (the block size is always 100 words), the allocation method (allocation by word or minimum allocation of unused words), and slave registration or deletion.

- Note:**
- Allocate areas larger than 100 words for each block in *Editing Parameters*.
 - Use the following procedure to allocate I/O to the slave devices of a master device with the Parameter Wizard.

- 1 Select the master device to register.
- 2 Select **Device - Parameter - Wizard**.
- 3 Click the **Yes** Button.

The present settings will all be initialized if the Parameter Wizard is used for the setup. A confirmation dialog box will be displayed. An example is shown below.

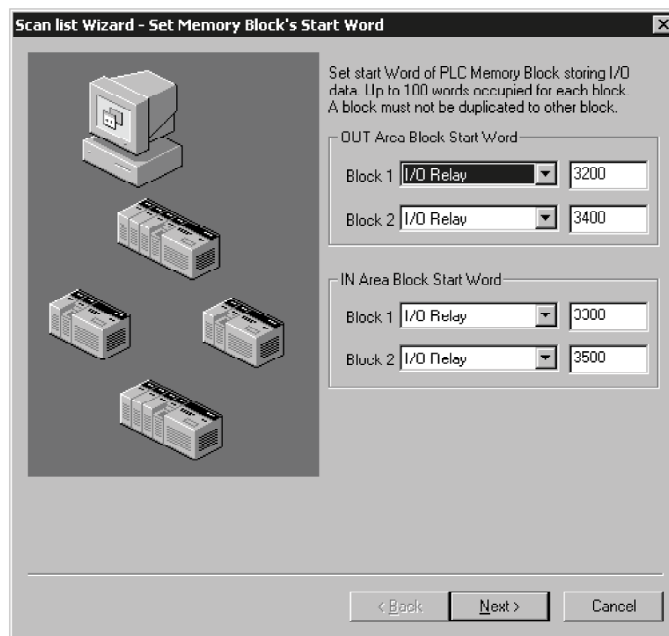


4 Setting the Start Word for Each Block

The Scan List Wizard-Setting Memory Block's Start Word Window will be displayed. An example is shown below.

Set the memory areas to use and the start words, and then click the **Next** Button. Allocation starts automatically from Block 1. If Block 1 is completely allocated, allocation will be performed in Block 2. Each block will be allocated from the start word to a maximum of 100 words (fixed).

Note: If an area overlaps blocks or the start word results in exceeding the memory area range, you cannot move to the next step.

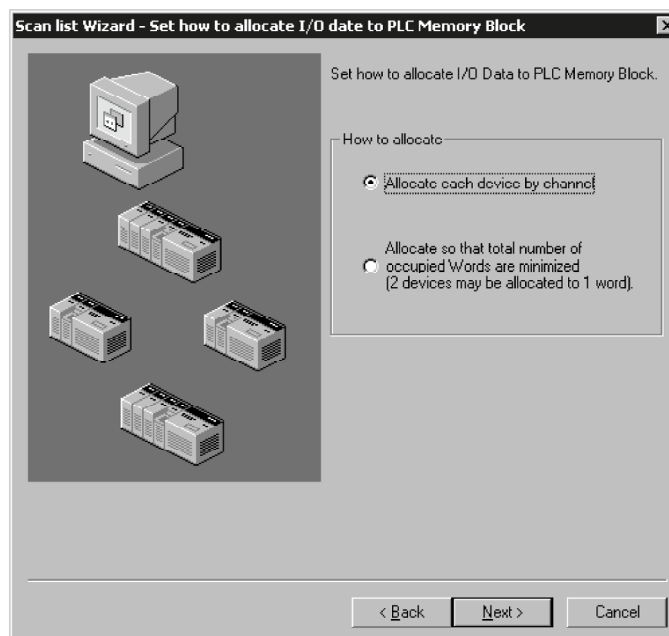


The window is titled "Scan list Wizard - Set Memory Block's Start Word". It contains a graphic of a PLC rack on the left. On the right, there is instructional text: "Set start Word of PLC Memory Block storing I/O data. Up to 100 words occupied for each block. A block must not be duplicated to other block." Below this, there are two sections: "OUT Area Block Start Word" and "IN Area Block Start Word". Each section has two rows: "Block 1" and "Block 2". Each row has a dropdown menu set to "I/O Relay" and a text box containing a start word value. For OUT Area, the values are 3200 for Block 1 and 3400 for Block 2. For IN Area, the values are 3300 for Block 1 and 3500 for Block 2. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

5 Setting Remote I/O Allocations

The Scan List Wizard-Set how to allocate I/O data to PLC Memory Block Window, which specifies the I/O data allocation method for devices, will be displayed. An example is shown below.

Specify the allocation method and click the **Next** Button.



The window is titled "Scan list Wizard - Set how to allocate I/O data to PLC Memory Block". It contains a graphic of a PLC rack on the left. On the right, there is instructional text: "Set how to allocate I/O Data to PLC Memory Block." Below this, there is a section titled "How to allocate" with two radio button options. The first option, "Allocate each device by channel", is selected. The second option is "Allocate so that total number of occupied Words are minimized (2 devices may be allocated to 1 word)". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

There are two methods for allocation.

<p>Allocate each device by channel</p>	<p>Each slave is always allocated the low byte (lower 7 bits) of the word. Therefore, each slave is allocated one word even if 1-byte I/O slaves come sequentially.</p> <p>Example:</p> <div><div><div>High</div><div>Low</div><div>15 ... 8 7 ... 0</div><div><div>#0</div><div><div></div><div>#1</div><div>#3</div><div>#4</div><div>#6</div></div></div></div><div><div>Node address order</div><div>↓</div><div><div></div>Unused</div></div></div>
<p>Allocate so that the total number of allocated words is minimized (two devices may be allocated to one word)</p>	<p>If there are 1-byte I/O slaves, allocation is in the order of low byte (lower 7 bits) to high byte (upper 7 bits) to create as few unused areas as possible.</p> <p>Example:</p> <div><div><div>High</div><div>Low</div><div>15 ... 8 7 ... 0</div><div><div>#0</div><div><div>#3</div><div>#1</div><div>#4</div><div>#6</div></div></div></div><div><div>Node address order</div><div>↙ ↘</div><div><div></div>Unused</div></div></div>

Examples of allocation are as follows:

Allocation when outputs or inputs are as shown below

#00	1 byte
#01	2 bytes
#02	1 byte
#03	4 bytes
#04	1 byte
#05	1 byte

Allocation by Word

	15	High	8	7	Low	0
+0 word	#00					
+1 word	#01					
+2 word	#02					
+3 word	#03					
+4 word	#03					
+5 word	#04					
+6 word	#05					

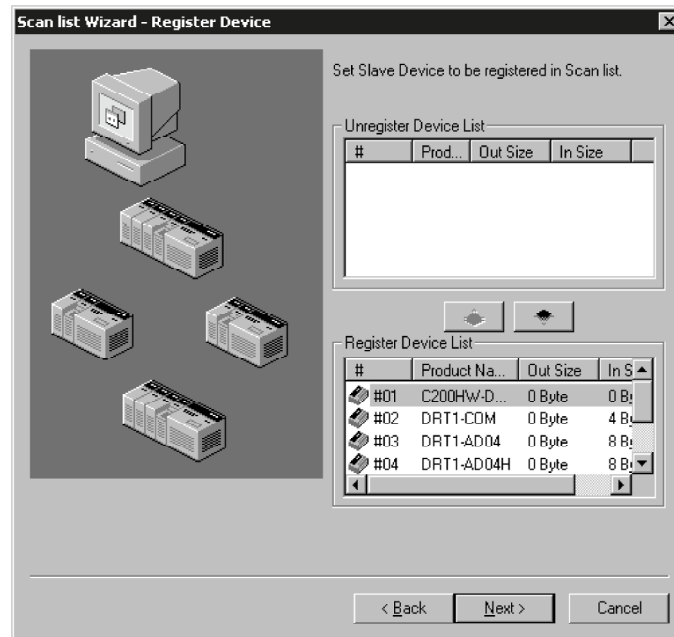
Allocation Minimizing the Number of Allocated Words

	15	High	8	7	Low	0
+0 word	#02					
+1 word	#01					
+2 word	#03					
+3 word	#03					
+4 word	#05					
	#04					


6 Slave Registration and Deletion

The Scan List Wizard-Register Device Window will be displayed.

An example is shown below. Specify the slave devices to register to the master device and click the **Next** Button.



Devices in the network will be displayed in the Registered Device List as already

registered. If there is a device that you do not want registered, click the  Button to unregister it. You cannot go on to the next step if there are no registered

devices.

7 Displaying Remote I/O Allocation Results

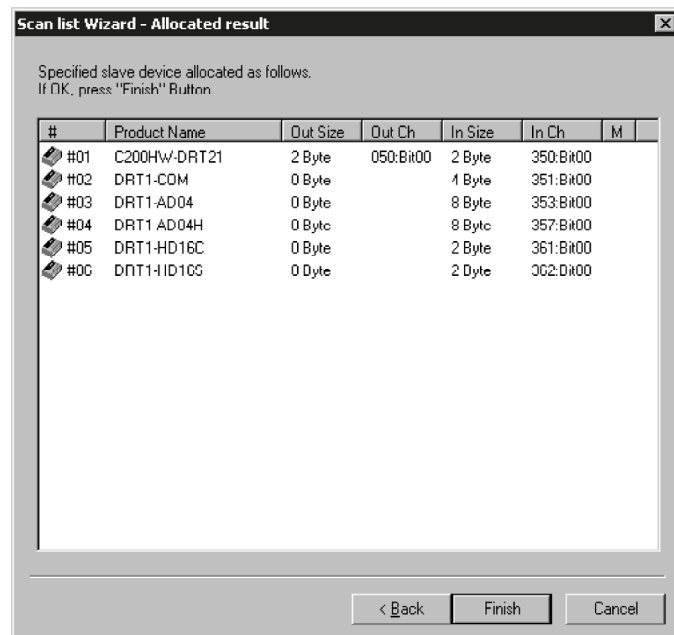
After allocating I/O with the specified method, the Scan List Wizard - Allocation

Result Window will be displayed. An example is shown below. If the displayed

details are correct, click the **Finish** Button. This exits the Parameter Wizard. Click

the **Back** Button to go back to the previous setting pages.

The set contents will be set as device parameters.



8 Downloading Parameters to a Master Device

The following dialog box will be displayed when the Network Configurator is online.



If you click the **Yes** Button to download to a master device, the remote I/O communications will start with the new settings.

Note: Device parameters set in the Parameter Wizard can be changed using the parameter edit function.

A-2-4 Manual I/O Allocation

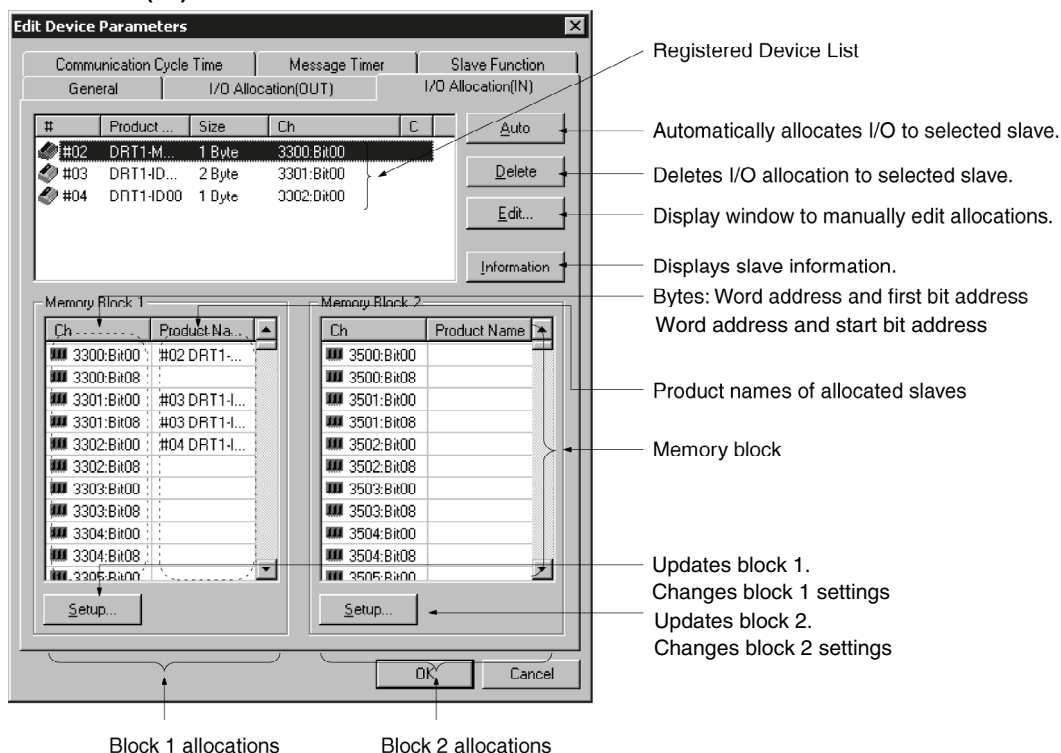
Memory can be manually allocated for slave I/O.

I/O Allocation Tab Page

The following items are set on the I/O Allocation Tab Page.

- 1) Allocation of I/O memory in the CPU Unit for I/O Memory Blocks 1 and 2
- 2) Allocation to slaves for each block

The following window will be displayed when you click the **I/O Allocation (OUT)** or **I/O Allocation (IN)** Tab.



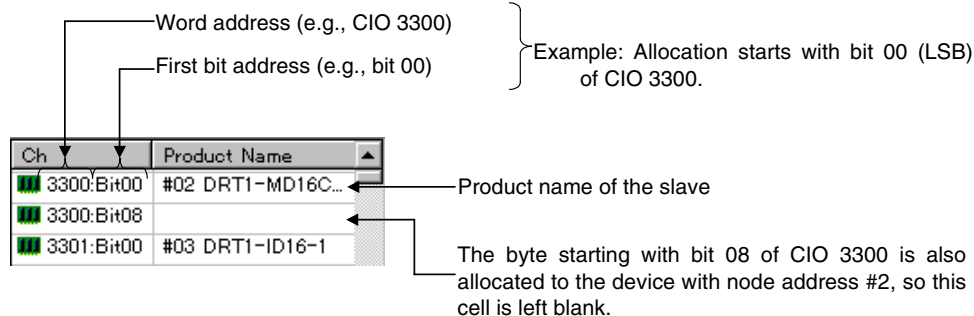
Item	Description
Registered Device List	Displays only devices with valid output or input data of the registered devices on the General Tab Page.
Auto Button	Allocates unused words to the slaves selected in the Registered Device List starting from the first unused words.
Delete Button	Releases the words allocated to the selected slaves in the Registered Device List.
Edit Button	Enables manually editing allocations using the Edit Window.
Information Button	Displays the slave information (allocated words and I/O comments).
Memory Blocks 1 and 2	Displays the allocation state of each slave (product name) in Blocks 1 and 2.
Ch	Beginning of allocation. The start bit address is displayed after the word address.
Product Name	The name of the device to which memory is allocated.
Setup Button	Sets the start words and size (number of words) of Blocks 1 and 2.

Additional Information: Allocation State of Blocks 1 and 2

The product name of the device to which memory is allocated in each area and the first CPU Unit word allocated are displayed in the Allocation State List for the blocks. The first bit that is allocated is given in the *Ch* column. The word address is given first followed by the first bit.

Example: "3300: Bit 00" indicates that the first allocated bit is bit 00 of CIO 3300 (i.e., the allocation starts from the low byte).

Example: "3300: Bit 08" indicates that the first allocated bit is bit 08 of CIO 3300 (i.e., the allocation starts from the high byte).



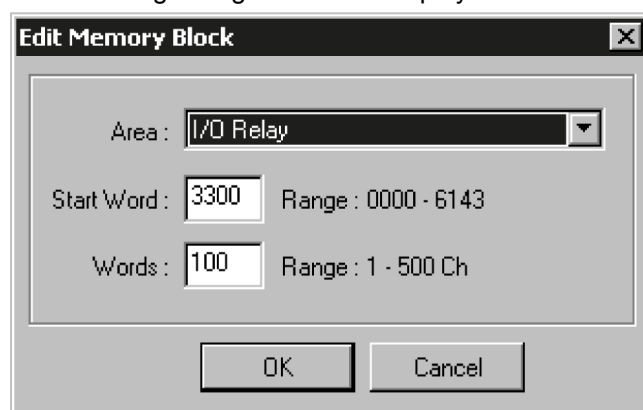
CPU Unit words are not displayed in unused memory block.

Changing the I/O Block Start Word

Setup Button on the I/O Allocation Tab Pages (*Device – Parameter - Edit*)

Use the following procedure to change the allocation areas for the I/O blocks in CPU Unit I/O memory.

- 1 Click the **Setup** Button of the block to change.
- 2 The following dialog box will be displayed.



- 3 Set the *Area*, *Start Word*, and *Words*.
For the *Words*, set the number of words displayed by the Network Configurator. The maximum number of words that can be allocated for one block is 500. The setting ranges are as follows:

PLC model	Memory area	Range
CS Series CJ Series	CIO Area	0000 to 6143
	DM Area	D0000 to D8191
	Work Area	W000 to W511
	Holding Area	H000 to H511
	EM Area	E00000 to E32767

Banks 0 to12 can be used for the EM Area.

- Note:**
- The number of words of a block displayed on the Network Configurator is set for *Words*. This value is not downloaded to the master.
 - If the number of allocated words in 1 block is 100 or less, the number of words will be displayed as 100 words when uploading.

- 4 Click the **OK** Button to change the memory block.
If memory has already been allocated to devices, it will be re-allocated in the new memory block. If the area is exceeded, however, the corresponding device allocation will be deleted. Allocate memory again.

I/O Allocation Method

I/O Allocation Tab Pages (*Device - Parameter - Edit*)

There are three ways to allocate I/O.

- 1) Manual Allocation Using the Edit Window
Select a slave device from the Registered Device List and click the Edit Button.
Use the Edit Window to manually allocate memory to each slave.
- 2) Allocation Using a Drag-and-drop Operation
Drag a device from the Registered Device List and drop it at the corresponding word location in the memory block that you want to allocate.
- 3) Auto-allocation
Select a device from the Registered Device List and click the Auto Button. This enables auto-allocation for unused words. (A device for which the user setting was performed using the Advanced Setup Button on the General Tab Page, however, cannot be automatically allocated.)

- Note:** An image like the following will be displayed in the *Size* Field of the Registered Device List for the I/O data size of a device for which multiple connections are set on the General Tab Page.

Name	Size	Ch
ProductCode (...	4, 4 Byte	

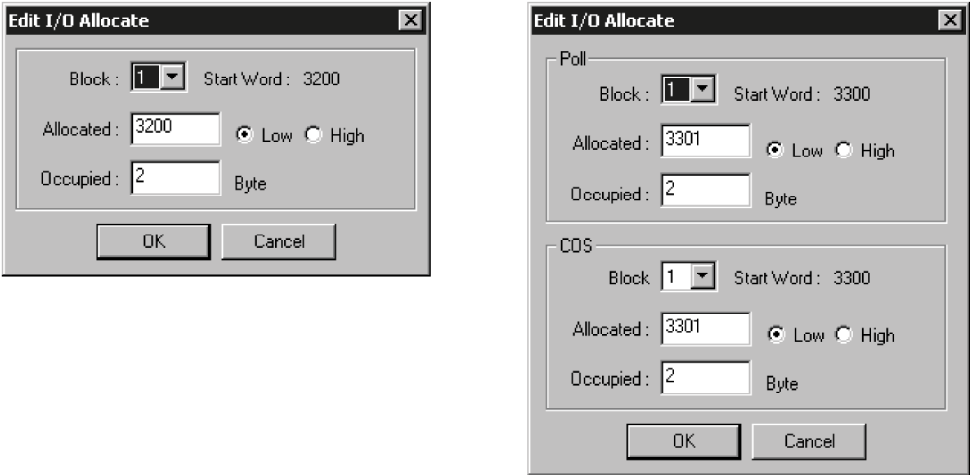
To allocate the I/O on the left using a drag-and-drop operation, drag it with the left button on the mouse. To allocate the I/O on the right using a drag-and-drop operation, drag with the right button on the mouse. When there is only one connection, use the left button on the mouse.

Manual Allocation Using the Edit Window

Edit Button on an I/O Allocation Tab Page

Use the following procedure to allocate manually using the Edit Window.

- 1 Select the device for which you want to edit the I/O allocation.
- 2 Click the **Edit** Button.
- 3 The Edit I/O Allocation Dialog Box will be displayed. Examples are shown below. Specify Block 1 or 2, the allocated word, start byte (low byte: *Low*, high byte: *High*), and the number of allocated bytes (*occupied*).



Connections are specified in the General tab with the advanced setup function.

Specify the start word to allocate and the number of allocated bytes.

Byte location (i.e., high/low) can also be specified with the allocated word setting.

When the number of allocated bytes is 2 bytes or more, you must specify *Low*.

Allocating One Low Byte to a Device

	High		Low	
	15	8	7	0
+0CH			#00	
+1CH				
+2CH				

Allocating One High Byte to a Device

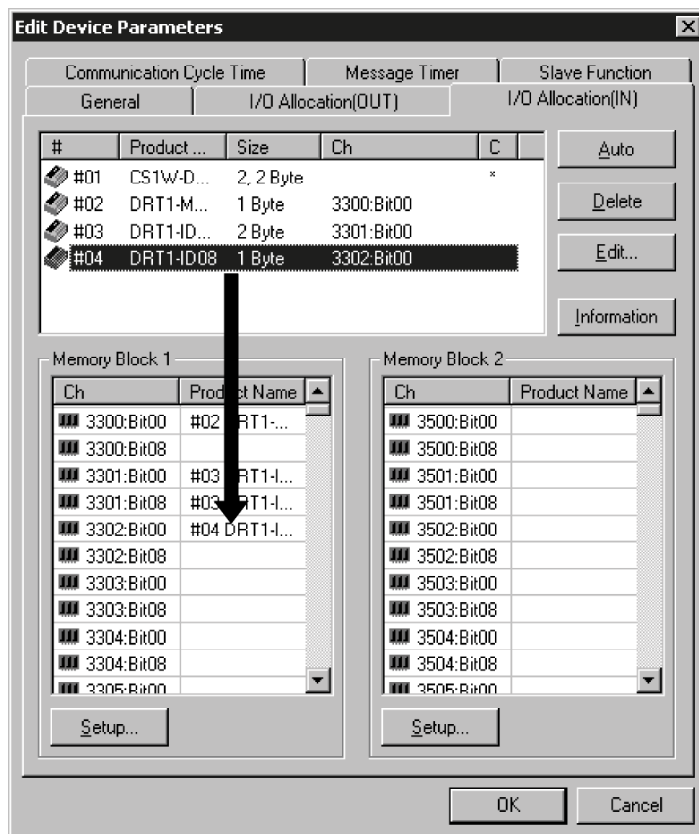
	High		Low	
	15	8	7	0
+0CH	#00			
+1CH				
+2CH				

- 4 Click the **OK** Button to perform the I/O allocation.

Allocation Using a Drag-and-drop Operation

Drag-and-drop operation on an I/O Allocation Tab Page

- 1 Display the Memory Block List where you want to allocate memory to the slave.
- 2 Select the slave from the Registered Device List in the upper pane.
- 3 Drag it to the start byte you want to allocate to the slave.



• Memory Block List Contents

In the Memory Block Lists at the bottom of the window, the allocated memory (i.e., word address and start bit address) is displayed in the *Ch* column and the product name (i.e., model) of the slave to which the memory is allocated is displayed in the *Product Name* column.

• Registered Device List Contents

In the Registered Device List at the top of the window, the node address is displayed in the *#* column, the slave product name (i.e., model) in the *Product Name* column, the number of allocated bytes in the *Size* column, and, when memory is already allocated, the start byte (i.e., word address and start bit address) in the *Ch* column.

When deleting or changing allocations for slaves, select the slave from the Registered Device List and click the **Delete** Button.

Note: To automatically allocate the next unused word to a slave, select the slave from the Registered Device List and then click the **Auto** Button.

Auto-allocation

Auto/Delete Button on the I/O Allocation Tab Page

- Click the **Auto** Button to allocate the next unused word for the I/O of the selected slave.
 - Click the **Delete** Button to release the I/O allocation of the selected slave.
- If auto-allocation is specified, however, the Advanced Setup function described later cannot be used.

Displaying Slave Information

Information Button on the I/O Allocation Tab Page

Information, such as I/O comments of registered slave devices, can be accessed on the I/O Allocation Tab Page. (To set I/O comments for the I/O data of the slave devices, select *Edit I/O Comment* from the Device Menu.)

Use the following procedure to display the slave information.

- 1 Select the device for which you want to display the information.
- 2 Click the **Slave Information** Button.
- 3 The following window will be displayed.

#03 C200HW-DRT21 Information

Description : C200HW-DRT21
 MAC ID : #03
 Vendor : OMRON Corporation
 DeviceType : Communications Adapter
 Product Code : 51
 Product Name : C200HW-DRT21
 Status : Registered to #02.

Poll

OUT Size : 2 Byte

Area	Bit	Comment
% 3201	Bit00	OUT Comment1
% 3201	Bit06	OUT Comment2
% 3201	Bit12	OUT Comment3

IN Size : 2 Byte

Area	Bit	Comment
% 3301	Bit02	IN Comment1
% 3301	Bit05	IN Comment2
% 3301	Bit15	IN Comment3

Close

If a registered device is selected while the Information Window is displayed, the slave information will be updated to the information of the selected device.

A-2-5 Advanced Settings: Connection, Communications Cycle Time, Slave Function Settings, etc.

This section describes connection settings, device information and check selection displays, the communications cycle time setting, message timer settings, and slave function settings.

Advanced Setup

Advanced Setup Button after Selecting a Slave on the General Tab Page

(Device - Parameter - Edit)

Advanced settings, including device information and check selection displays, and connection settings, can be made for remote I/O communications.

Device Information Display and Check Selections

• Device Information Tab Page

It is possible to display device information and to perform checks for the slave devices. Use the following procedure.

- 1 Select a slave device from the Registered Device List.
- 2 Click the **Advanced Setup** Button.
- 3 The following window will be displayed.
Device Information Tab Page

The device information on the selected slave will be displayed.

If these options are selected, the device information will be compared with the corresponding data in the scan list during remote I/O communications. If the information does not coincide with the data, a verify error will occur.

The device information (vendor, device type, product code) of the currently selected slave device will be displayed.

Select these options to check device information (and indicate an error for inconsistencies) in remote I/O communications (i.e., when a connection is opened).

Connection Settings

- Connection Tab Page

The user can specify a maximum of two connections per slave to use in remote I/O communications. Use the following procedure.

- 1 Select the slave device in the Registered Device List.
- 2 Click the **Advanced Setup** Button.
- 3 The following window will be displayed.
Click the **Connection** Tab.

The screenshot shows the 'Advanced setting' dialog box with the 'Connection' tab selected. The 'Auto Connection' radio button is chosen. Below it, 'OUT Size' and 'IN Size' are both set to 2 Byte. The 'User Setup' section is expanded, showing three checked options: 'Use Poll Connection', 'Use COS Connection', and 'Use Cyclic Connection'. Each checked option has its own 'OUT Size', 'IN Size', and 'Con. Path' fields. 'Use Poll Connection' and 'Use COS Connection' have 'OUT Size' and 'IN Size' set to 2 Byte. 'Use Cyclic Connection' has 'OUT Size' and 'IN Size' set to 0 Byte. The 'COS/Cyclic Heart Beat Timer' at the bottom is set to 1000 ms. 'OK' and 'Cancel' buttons are at the bottom right.

The default setting is *Auto Connection*.

Use the following procedure to specify a connection.

- 1 Select the *User Setup* Option.
Settings will be enabled for connections.
- 2 Select the connections to use.
Up to two connections can be set.
Note: *COS* and *Cyclic* cannot be set at the same time.
- 3 Set a connection path if necessary.
- 4 Set the *COS/Cyclic Heartbeat Timer* value if necessary.
- 5 Click the **OK** Button.
An asterisk will be displayed in the C column at the right in the Registered Device List.

If a connection for a device for which I/O allocation has already been performed is changed, the present I/O allocation will be deleted. Allocate memory again.

IMPORTANT:

- *COS* and *Cyclic* cannot be set at the same time.
- If both a poll and *COS* connection or a both poll and cyclic connection are used, the output settings for both connections must be the same.

Note: The auto-allocation function cannot be used for a device for which a connection has been set in the Advanced Setup. To enable using the auto-allocation function, unregister the device and then register it again.

Communications Cycle Time Setting

Communications Cycle Time Tab Page (Device - Parameter - Edit)

The communications cycle time setting and the communications cycle times calculated based on the currently registered device information can be accessed on the Communications Cycle Time Tab Page.

Click the **Communications Cycle Time** Tab to display the following window.

Edit Device Parameters

General | I/O Allocation(OUT) | I/O Allocation(IN)

Communication Cycle Time | Message Timer | Slave Function

Communication Cycle Time : 0 ms

Setup Range : 0 : Auto (Default) , 1 - 500 ms

Default Setup

Communication Cycle Time (Auto Setting)

Baud rate 125K Bit/s :	2.942 ms
Baud rate 250K Bit/s :	2.000 ms
Baud rate 500K Bit/s :	2.000 ms

OK Cancel

The communications cycle time is set between 1 and 500 ms. Click the Default Setup Button or specify 0 ms to enable automatic setting.

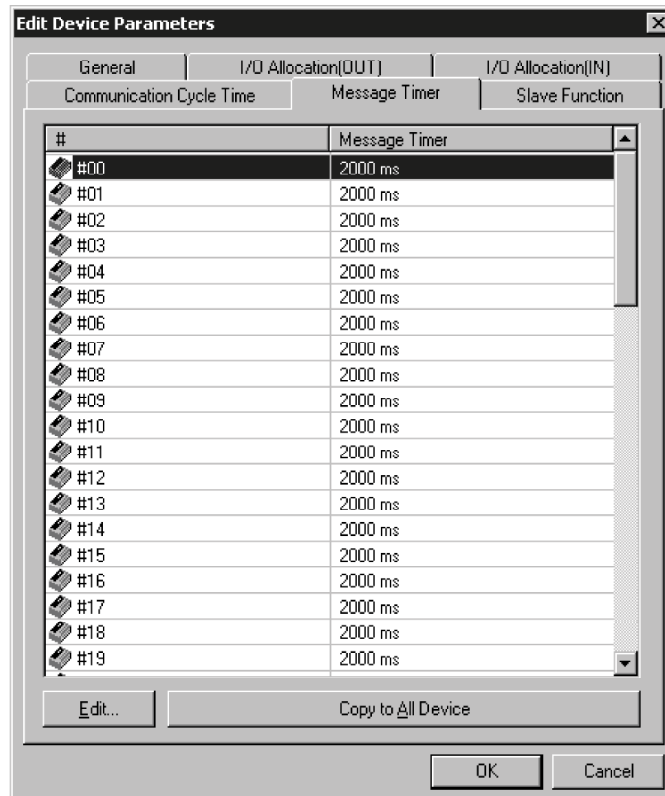
The communications cycle time for the automatic setting is calculated and displayed for each baud rate based on the currently registered device information.

Note: The communications cycle time is the interval at which remote I/O communications are performed for the same slave. Setting this time can prevent fluctuations in the communications cycle time based on conditions. Setting a longer communications cycle time can prevent a slave with a slower processing speed from being detected as having an error.

If actual remote I/O communications take shorter than the communications cycle time setting, remote I/O communications will wait for the communications cycle time to expire. If the actual remote I/O communications take longer, the remote I/O communications are performed in the actual time interval regardless of the communications cycle time setting.

Message Timer Settings

Message Timer Tab Page (Device - Parameter - Edit)



The default value for the message timer is 2 seconds (2,000 ms). Set a value between 500 and 30,000 in increments of milliseconds.

Use the following procedure to change the value.

- 1 Double-click a node address (#) (or select a node address and click the **Edit** Button) to change the setting. The following dialog box will be displayed.



- 2 Enter a value and click the **OK** Button.

Note: To set the same value for all the devices, select the node address value you want to set and click the *Copy to All Device* Button.

- Note:**
- The message timer monitors timeouts in message communications (the same timer is used for both explicit message communications and FINS messages), and it can be set for each device for which communications are performed (message destinations).
 - If the target communications device (i.e., the message destination) is slow to respond, the message time setting will need to be increased. (The response may take a long time especially when crossing network layers for FINS message communications. Set a longer timer value when crossing network layers.) When a long timer value is set, however, the next message cannot be sent to the same communications device while waiting for a response.
 - The DeviceNet Unit monitors message timeouts by using this timer. In contrast, monitoring using the response monitoring time for CMND, SEND, and RECV instructions is performed by the CPU Unit. Therefore, there is no effect if the message timer or response monitoring time for CMND, SEND, and RECV instructions is set longer than the other.
 - Set the response monitoring timer for CMND, SEND, and RECV instructions to the same or longer than the message timer (Response monitoring time for CMND/SEND/RECV instructions \geq Message timer).
If many timeouts occur, set both values longer while maintaining the relation given above.

Setting as Slave Function

Slave Function Tab Page (*Device - Parameter – Edit*)

The slave function can be enabled by the setting on the Slave Function Tab Page.

IMPORTANT: To enable the slave function, select the device and select **Device – Property**. Select the *Enable Slave Function* Option in the CS/CJ-series DeviceNet Unit Properties Dialog Box.

Use the following procedure to set the slave function.

- 1 Click the **Slave Function** Tab.
- 2 The following window will be displayed.

The screenshot shows the 'Edit Device Parameters' dialog box with the 'Slave Function' tab selected. The 'Auto Connection' radio button is selected. Under 'Auto Connection', there are two sections: 'OUT' and 'IN'. Each section has a dropdown menu for 'Area' (set to 'I/O Relay'), a text box for 'Allocated' (set to '3370' for OUT and '3270' for IN), and a text box for 'Occupied' (set to '2' for both). Below these is the 'User Setup' section, which is currently unselected. It has sub-tabs for 'Poll', 'Bit-Strobe', 'COS', and 'Cyclic'. The 'Poll' sub-tab is active, showing 'OUT' and 'IN' sections with 'Area' set to 'I/O Relay' and 'Allocated' and 'Occupied' both set to '0'. At the bottom are 'OK' and 'Cancel' buttons.

- 3 Specify a connection.
The default setting is *Auto Connection*. Click the *User Setup* Option to set a connection.
- 4 Set the I/O areas to use for remote I/O communications.
Set the areas, start words, allocated sizes for input (Slave to Master) and output (Master to Slave).
If the *User Setup* Option is selected, set all the connections to be used.
Up to 2 connections can be set.

IMPORTANT:

- COS and *Cyclic* cannot be set at the same time.
- If both a poll and COS connection or both a poll and cyclic connection are used, the output settings for both connections must be the same.

A-3 EDS File Management

This section describes the managing the EDS file used in the Network Configurator.

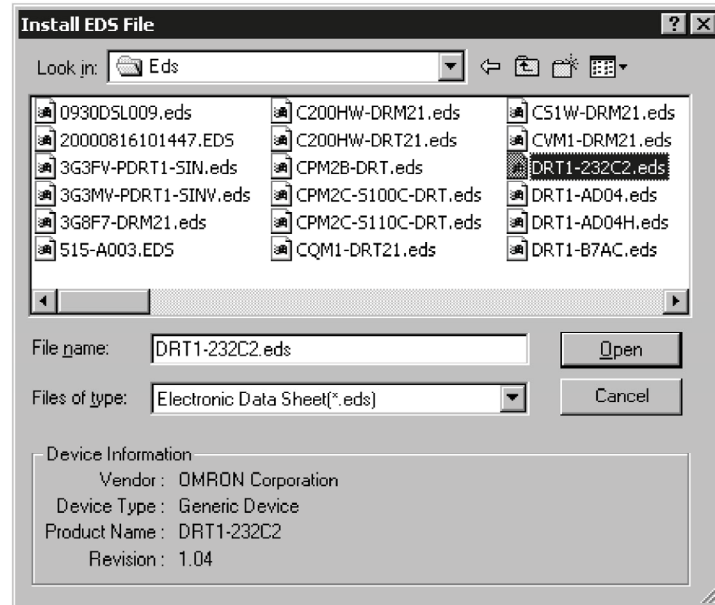
A-3-1 Installing EDS Files

EDS File - Install

Installing an EDS file enables the Network Configurator to support a new device type. Use the following procedure to install an EDS file.

- 1 Select **EDS File - Install**.

The following window will be displayed.



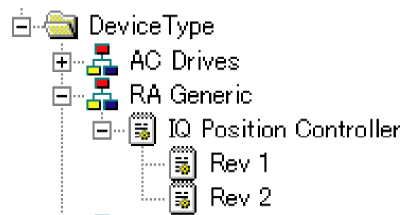
- 2 Select the EDS file to install. The device information will be displayed in the lower part of the window.

- 3 Click the **Open** Button.

The file will be added to the Hardware List Window as new hardware.

If the same hardware already exists, it will be updated to the latest version.

If the hardware version is different, it will be added to the Hardware List in the following way.



A-3-2 Creating EDS Files

EDS File - Create

An EDS file is absolutely essential to create a network configuration using the Network Configurator. Use the following procedure to create an EDS file.

- 1 Select **EDS File - Create**.

The following window will be displayed.

- 2 Set the device information and I/O information.
The device information can be obtained from a device in the network when it is online.
- 3 Click the **Obtain from Device** Button. The following window will be displayed.

- 4 Set the node address for a target device and click the **OK** Button.
Refer to the relevant device manual and set an I/O connection and an I/O size that the device supports.
- 5 Click the **OK** Button.
The file will be added to the Hardware List Window as a new device in the same way as in the EDS file installation.

Note: The device parameter settings cannot be created using the EDS file creation function of the Network Configurator. To set device parameters, obtain the EDS file from the device manufacturer.

A-3-3 Deleting EDS Files

EDS File - Delete

Use the following procedure to delete an EDS file.

- 1 Select the hardware (i.e., device) in the Hardware List Window.
- 2 Select **EDS File - Delete**.

A confirmation window will be displayed. An example is shown below.



- 3 Click the **Yes** Button.

The EDS file and the target device will be deleted from the Hardware List Window.

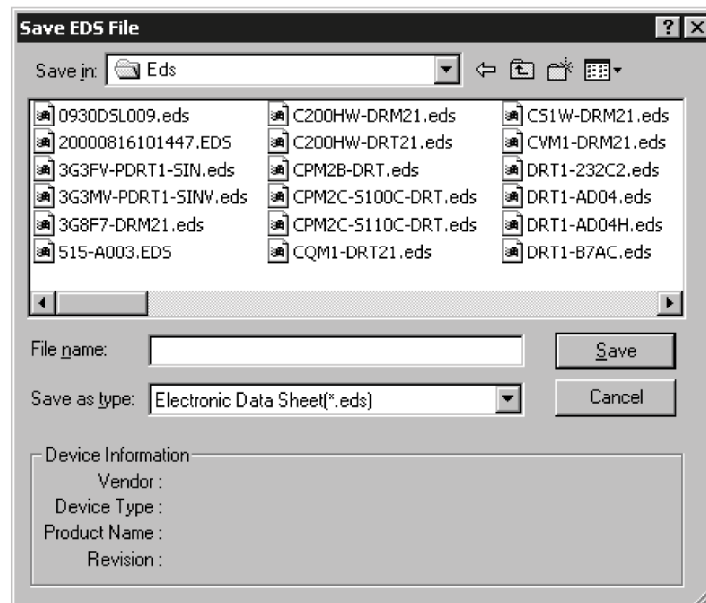
A-3-4 Saving EDS Files

EDS File - Save

Use the following procedure to save an EDS file.

- 1 Select the hardware (i.e., device) in the Hardware List Window.
- 2 Select **EDS File - Save**.

A window for specifying the folder and file name for saving the EDS file will be displayed. An example is shown below.



- 3 Specify a folder and file name and click the **Save** Button.
- The EDS will be saved.

A-3-5 Searching EDS Files

EDS File - Find

Use the following procedure to search for a device (i.e., EDS file) displayed in the Hardware List Window.

- 1 Select **EDS File - Find**.
The following window will be displayed.



- 2 Set the character string to search for and click the **Find Next** Button.
- 3 The cursor will move to the device if there is a matching device.
- 4 Click the **Cancel** Button to exit the search.

Note:

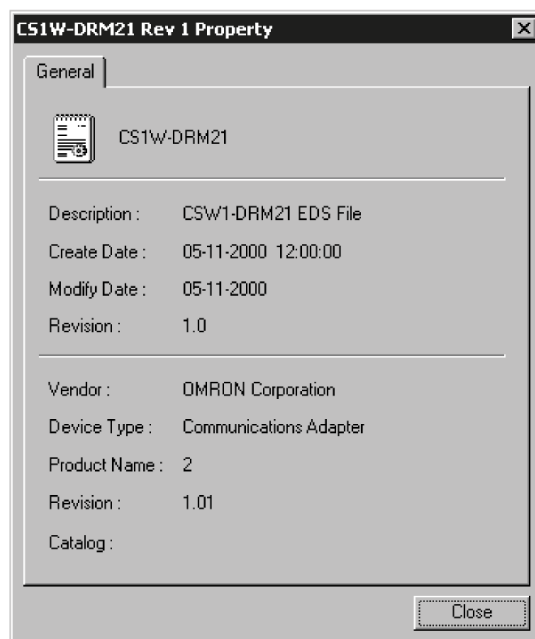
- The search will be made for devices below the present cursor position in the Hardware List Window.
- To search all the devices, select **Hardware** in the Hardware List Window and then perform the search.

A-3-6 EDS File Properties

EDS File - Property

Use the following procedure to display the properties of an EDS file.

- 1 Select the hardware (i.e., device) in the Hardware List Window.
- 2 Select **EDS File - Property**.
The following window will be displayed.



The date and time the EDS file was created and device information will be displayed.

A-4 Using General-purpose Tools to Set Devices

This section describes how to set parameters that are not written in an EDS file and how to set node addresses and baud rates through the network.

A-4-1 Setting Device Parameters by Specifying Class and Instance

Tool - General Parameter

The following items can be set to enable setting device parameters that are not written in an EDS file.

- Service Code
- Class (object class), instance (class instance), attribute (instance attribute)

To set parameters other than these codes, the configuration information for the data setting for the attributes must be obtained from the device manufacturer. If there is any unknown information, the parameters cannot be set.

Use the following procedure to set device parameters.

- 1 Connect the Network Configurator online.
- 2 Select **Tool - General Parameter**.

The following window will be displayed.

Setup Parameters

Target Node Address: Setup Range 0 - 63

Service: ☒ Generic ☐ Custom Service code set in HEX format string.

Parameter: Class: Instance: Data: All parameters set in HEX format string. Attribute data set in Data field.

Result:

- 3 Set the node address of the device for which parameters are being set in the *Target Node Address* Field.

4 Specify a service.

A service code can be specified by using a common service code defined in the DeviceNet or by directly specifying a service code. To specify a common service code defined in the DeviceNet, select a service from the drop-down list.

To specify a service code directly, select the *Custom Service* Option in the *Service* Field and directly enter a service code in hexadecimal.

Specifying a Common Service Code Defined in the DeviceNet	Directly Specifying the Service Code

5 Specify the class and instance of the parameters for which the settings are to be read or written.

6 Enter the data based on the specified service type.

7 Enter all the items and click the **Send** Button. The response from the device will be displayed in the *Result* Field.

8 Click the **Close** Button to exit the Device Parameter Setting Window. The Device Parameter Setting Window will close.

Example 1: Reading Parameters

- 1 Select the *Standard* Option in the *Service* Field and select *Get Attribute Single* from the drop-down list.
- 2 Specify the class and instance of the parameter to read.
- 3 Enter the attribute of the parameter to read in the *Data* Field.
- 4 Click the **Send** Button. The read value will be displayed in the *Result* Field.

Example 2: Setting Parameters

- 1 Select the *Standard* Option in the *Service* Field and select *Set Attribute Single* from the drop-down list.
- 2 Specify the class and instance of the parameter to set.
- 3 Enter the attribute of the parameter to set in the *Data* Field.
- 4 Set the value in the *Parameter* Area after the attribute in the *Data* Field.
- 5 Click the **Send** Button.

A-4-2 Setting the Node Addresses and Baud Rates via the Network

Tool - Node Address/Baud Rate Setting

Use the following procedure to set a device node address and baud rate via the network.

- 1 Leave only the target device and the Network Configurator operating in the DeviceNet network. Refer to the manual of the device used for the device node address and baud rate in the default settings. Also connect the Network Configurator using the same baud rate.
- 2 Connect the Network Configurator online.
- 3 Select **Tool - Node Address/Baud Rate Setting**.
The following window will be displayed.

The screenshot shows a Windows-style dialog box titled "Setup Node Address/Baud rate". It contains three main sections. The first section, "Target Node Address", has a spinner control showing the value "0" and the text "Setup Range 0 - 63". The second section, "Change Node Address", has a label "New Node Address :", a spinner control showing "0", the text "Setup Range 0 - 63", and a "Change" button. The third section, "Change Baud rate", has a label "Current Setup : ---", a label "New Setup :", a dropdown menu showing "125K Bit/s", and a "Change" button. A "Close" button is located at the bottom right of the dialog.

- 4 Specify the present node address of the target device in the *Target Node Address* Field.
- 5 To change the node address, specify a new node address in the *New Node Address* Field and click the **Change** Button.
The node address of the target device will be changed.
- 6 To change the baud rate, select the rate in the *New Baud Rate* Field and click the **Change** Button.
The baud rate of the target device will be changed.

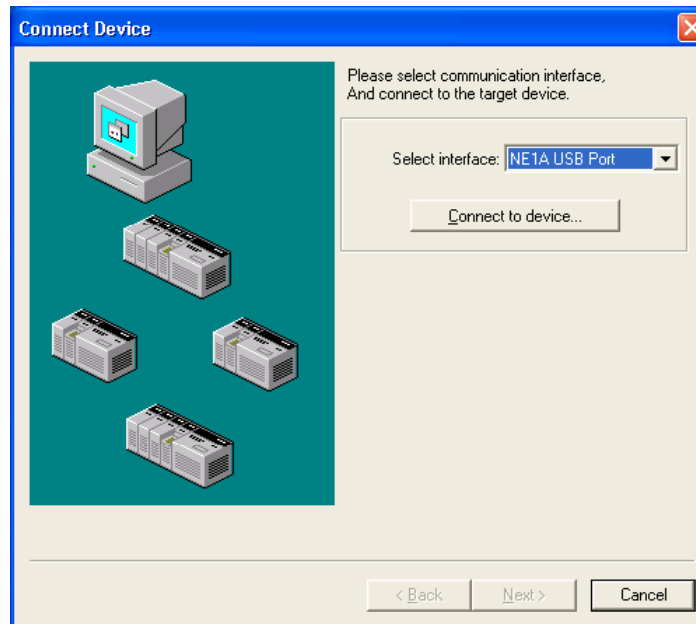
Note: The node address and baud rate can be set via the network only for devices that support this function.

A-5 Using the Password Recovery Tool

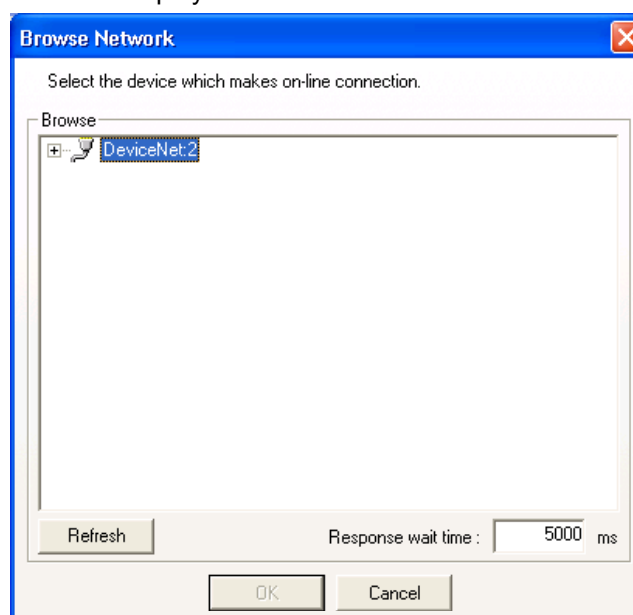
If the password set for a device is lost, use the Password Recovery Tool to reset the password and to return to the state without any password setting (default settings).

Use the following procedure to reset a device password.

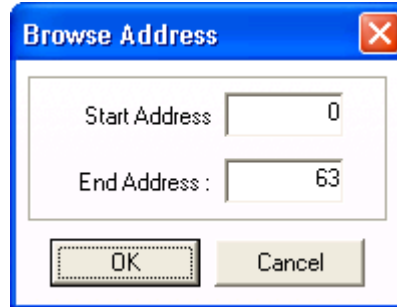
- 1 Prepare the computer for connecting to the DeviceNet via a USB port or DeviceNet Interface Card.
- 2 Select **Program - OMRON Network Configurator for DeviceNet Safety - Password Recovery Tool** (when using the default program folder names) from the Start Menu. The Password Recovery Tool will start, and the following Main Window will be displayed.



- 3 Select an interface for connecting to the network and click the **Connect to Device** Button. Click the **Refresh** Button when the window to search for the destination device is displayed.

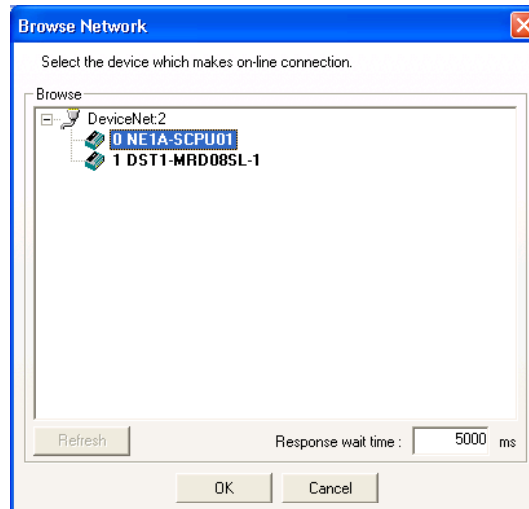


- 4 Set the node address range to search for and click the **OK** Button.



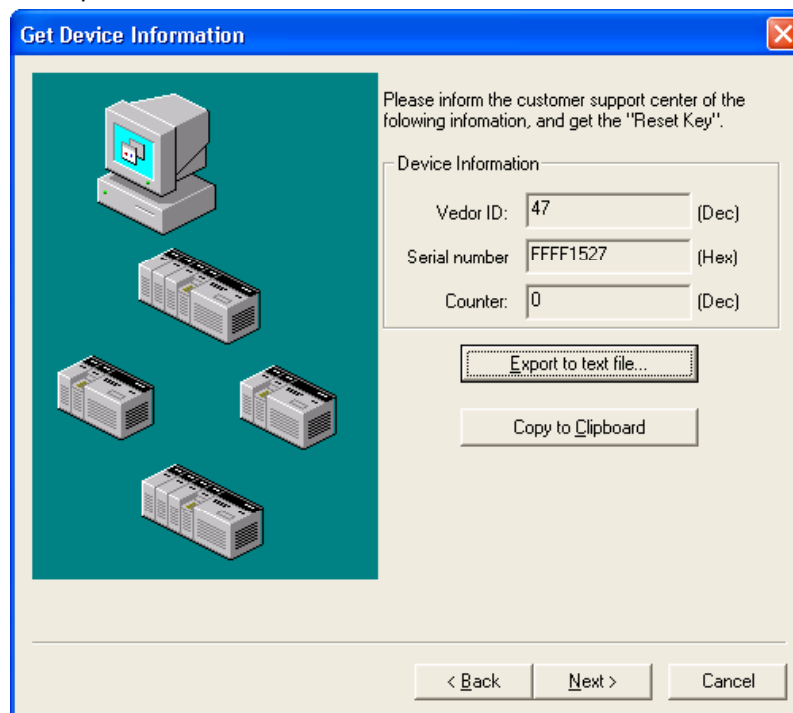
The 'Browse Address' dialog box has a blue title bar with a close button. It contains two input fields: 'Start Address' with the value '0' and 'End Address' with the value '63'. Below these fields are two buttons: 'OK' and 'Cancel'.

- 5 The devices in the network will be displayed. Select a device for which to reset the password and click the **OK** Button.



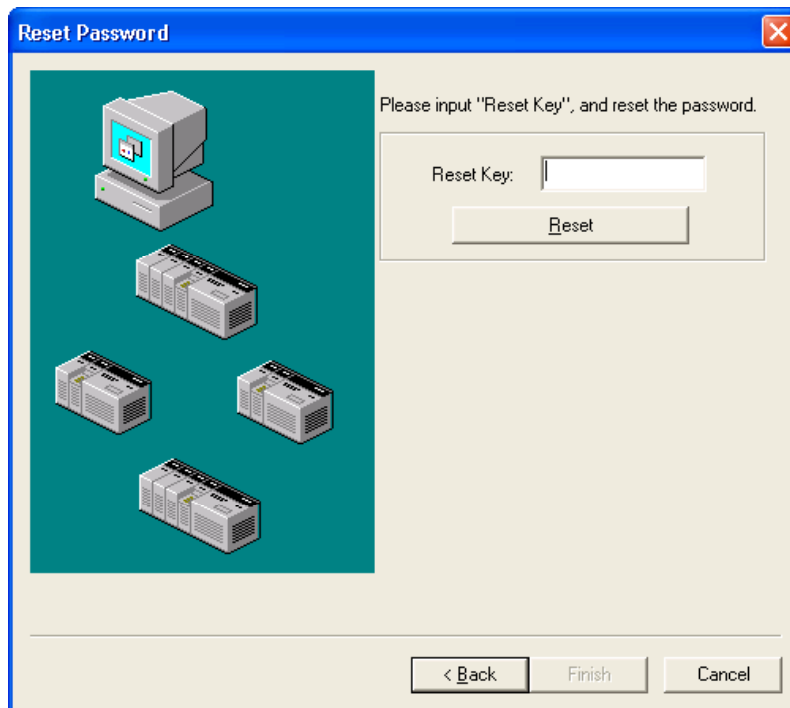
The 'Browse Network' dialog box has a blue title bar with a close button. It contains a text area with the instruction 'Select the device which makes on-line connection.' Below this is a 'Browse' section showing a tree view with 'DeviceNet:2' expanded, listing '0 NE1A-SCPU01' and '1 DST1-MRD08SL-1'. At the bottom, there is a 'Refresh' button, a 'Response wait time' field set to '5000 ms', and 'OK' and 'Cancel' buttons.

- 6 The necessary information for resetting the password will be displayed. The information is required when inquiring from the Support Center. Print the information by outputting to a text file and or copying to another application using the clipboard.

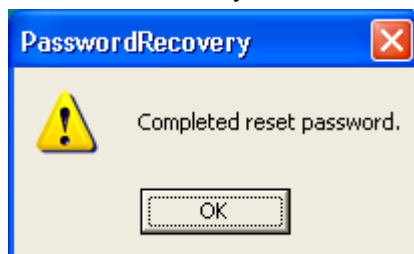


The 'Get Device Information' dialog box has a blue title bar with a close button. It features a large image of a computer monitor and several network devices on the left. On the right, there is a text area with the instruction 'Please inform the customer support center of the following information, and get the "Reset Key".' Below this is a 'Device Information' section with three input fields: 'Vendor ID' with the value '47' (Dec), 'Serial number' with the value 'FFFF1527' (Hex), and 'Counter' with the value '0' (Dec). Below these fields are two buttons: 'Export to text file...' and 'Copy to Clipboard'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- 7 Click the **Next** Button to display the Reset Key Enter Window. Enter the Reset Key obtained from the Support Center and click the **Reset** Button.



- 8 If the password is successfully reset, the following dialog box will be displayed. The device will be returned to the state without any password setting (default setting). Click the **OK** Button to close the dialog box. Click the **Finish** Button In the Password Recovery Tool Window to exit.



Glossary

Term	Definition
assembly	Internal data in a device gathered as one group to be accessed externally.
Busoff	Status that occurs when the error rate is extremely high over a communications cable. An error is detected when the internal error counter exceeds a certain threshold value. (The internal error counter is cleared when the Master is started or restarted.)
configuration	The settings for a device and a network.
connection	A logical communications path used to communicate between devices.
DeviceNet Safety	A safety network that adds a safety protocol to DeviceNet to comply with up to SIL3 according to IEC61508, up to Safety Category 4 according to EN954-1.
discrepancy time	The time period from a change in one of two inputs until the other input changes.
dual channel	Using two inputs or outputs as the input or output for redundancy.
Dual Channel Complementary	Setting to evaluate that two logic states are complementary.
Dual Channel Equivalent	Setting to evaluate that two logic states are equivalent.
EPI	The interval of safety data communications between the Safety Master and the Safety Slave.
error latch time	The time period to hold an error state (control data, status data, and LED indications).
multi-cast connection	Safety I/O communications in a 1:n configuration (n = 1 to 15).
open type	The open method for Safety Connection. One of three types is selected in the settings of a connection to the Safety Master.
safety chain	The logical chain to actualize a safety function, that consists of the input device (sensor), the control device (including a remote I/O device), and the output device (actuator).
safety controller (safety PLC)	A controller with high reliability used for the safety control.
safety data	Data with high reliability.
safety protocol	The communications hierarchy added to actualize highly reliable communications.
safety signature	A certificate of the configuration data issued to a device from the Network Configurator. The device verifies that the configuration data is correct by using the safety signature.
single channel	Using only one input or output as the input or output.
single-cast connection	Safety I/O communications in 1:1 configuration.
Standard	A device or device function to which safety measures are not applied.
test pulse	A signal used to detect external wiring coming into contact with the power supply (positive) or short circuits between signal lines.
TUNID	An identifier to specify one device in all the network domains. Values combining the network address and the node address are used.
output connection owner	The Safety Slave stores the TUNID of the Safety Master that established connections as the output connection owner to prevent unintended safety outputs from a Safety Master. The stored TUNID is held until the Safety Slave is reset to default settings.
configuration owner	The Safety Slave stores configuration owner data to prevent unintended configuration from a remote device. If the Safety Slave was configured by Support Software such as the Network Configurator, it stores the configuration owner was Support Software. If the Safety Slave was configured by a Safety Master, it stores the Safety Master TUNID. the stored data is held until the Safety Slave is reset to default settings.

Index

A

- acceptable bandwidth, 46, 53
- adding a page, 162
- adding devices, 82
- allocating network bandwidth usage rates and calculating best EPI, 55
- allocation by word, 254
- allocation minimizing the number of allocated words, 254
- AND, 155
- Automatic Execution Mode, 145

B

- batch exporting, 177

C

- calculating the maximum reaction time, 62
- changing device status, 102
- Channel Mode, 137, 143
- checking, 176
- checking the version, 70
- clearing the error history, 197
- configuration information, 101
- configuration lock, 99
- confirming the cycle time, 144
- Connected Component Maintenance Flag, 205, 208
- connecting to the DeviceNet Network, 236
- connecting to the network, 77, 236
- connection cables, 236
- connection status, 193
- connection type, 121
- connections, 159
- contact operations alarm threshold, 220
- creating a new virtual network, 79
- cycle time, 55, 138, 144

D

- deleting a page, 162
- deleting devices, 84
- deleting EDS files, 271
- device parameters, 67, 90
- device password, 88
- device password protection, 88
- device properties, 90
- device status, 193
- DeviceNet Interface Card, 40, 145
- DeviceNet safety communications, 34
- DeviceNet Safety Master, 33
- DeviceNet Safety Slaves, 33
- DeviceNet standard communications, 34
- DeviceNet Standard Master, 33
- DeviceNet Standard Slave, 33
- discrepancy time, 136
- downloading, 91
- downloading device parameters, 91
- dual channel safety input status, 195
- dual channel setting, 143

E

- Edit All Connection Window, 125
- editing CS/CJ-series DeviceNet Unit parameters, 246
- editing function block parameters, 164
- editing parameters, 106
- EDM, 156
- EDS file management, 269
- Emergency Stop Switch Monitoring, 155
- enabling master function, 246
- enabling slave function, 246
- EPI, 121
- error device list, 92
- error latch time, 137, 140, 142
- E-STOP, 155
- example of EPI calculations, 58
- Exclusive NOR, 155
- Exclusive OR, 155
- EXNOR, 155
- EXOR, 155
- exporting, 176
- External Device Monitoring, 156

F

- finding function blocks with open connections, 168
- forgotten passwords, 276
- function block I/O information, 164
- function blocks, 155, 157, 168

G

- general, 108
- general parameter group, 108
- Get from Network Button, 81
- Group Copy Button, 106

H

- hardware list, 71

I

- I/O assemblies, 126
- I/O comments, 73, 110, 166
- I/O connections, 119
- I/O refresh cycle, 145
- I/O refresh time, 63
- I/O tags, 127, 135, 143
- I/O type, 127, 134
- importing, 173
- input I/O tag placement, 158

J

- jump addresses, 163

L

- last maintenance date, 203
- Light Curtain Monitoring, 155
- local I/O settings, 136
- local safety I/O, 34
- Logic Editor, 150
- logic functions, 155, 156

M

Maintenance Counter Mode, 205, 210
maintenance functions, 198
maintenance functions of DST1-series Safety I/O Terminals, 198
master parameter overview, 247
menu list, 72, 152
Message Pane, 71
Monitor Mode, 194, 198
monitoring, 184
monitoring devices, 190
monitoring functions, 190
monitoring parameters, 194
monitoring safety connections, 192
monitoring status, 190
monitoring the contact operation counters, 205
monitoring the error history, 196
monitoring the operation time, 212
monitoring the program, 184
monitoring the run hours, 200
monitoring the total ON times, 208

N

network bandwidth, 53
network configuration files, 86
Network Configuration Pane, 71
Network Configurator, 69
network numbers, 79
node address/baud rate settings, 275
node addresses, 84
NOT, 155

O

OFF delay, 138
Off-Delay Timer, 155
ON delay, 138
On-Delay Timer, 155
online monitoring, 184
open type, 120
operation time, 113, 212
Operation Time Exceed Hold alarm, 215
operation time parameter groups, 113
OR, 155
output tag placement, 159

P

parameter verification, 96
password protection for user-defined function blocks, 181
password protection of network configuration files, 85
password recovery tool, 276
printing programs, 186
programming, 154
programming restrictions, 154
Protect Mode, 87

R

reaction time, 61, 62
reading network configuration files, 85
recording the maintenance date, 203
registering Safety Slaves, 116
Reset, 156
reset types, 101

resetting, 68, 101
resetting devices, 102
Restart, 156
reusing user-defined function block files, 176
routing, 155

S

safety configuration, 32
safety connection settings, 116
Safety Gate Monitoring, 155
safety I/O points, 34
Safety Input Channel Mode, 137
safety input parameter groups, 109
safety input terminal status, 195
safety inputs, 109
Safety Logic Controller, 33
Safety Output Channel Mode, 143
safety output parameter groups, 112
safety output terminal status, 195
safety outputs, 112
Safety Slave settings, 126
saving EDS files, 271
saving the error history, 197
saving the program, 182
searching EDS files, 272
sending explicit messages, 167
serial communications port, 236
setting assembly data, 134
setting general parameters, 273
setting output points, 166
setting remote I/O allocations, 253
setting safety connection parameters, 119, 125
setting Safety Inputs, 136
setting safety outputs, 142
setting Slave input data in Idle State, 134
setting test outputs, 140
setting the contact operation counter threshold, 206
setting the node addresses and baud rates via the network, 275
setting the operating mode, 144
setting the threshold run hours, 200
setting the threshold value for total ON time, 210
setting unit functions, 246
Slave I/O, 133
specifying the connection interface, 238
Standalone Controller Mode, 34
standard configuration, 32
Standard Slave settings, 115, 133
status, 130, 135
status changes, 101
SYSMAC CS/CJ Ethernet Unit interface, 238
SYSMAC CS/CJ interface port, 238

T

Test Output Channel Mode, 141
test output parameter groups, 111
test output terminal status, 195
test outputs, 111
test source, 138
threshold maintenance counter, 206, 210

threshold network power voltage, 198
threshold response time, 214
threshold run hours, 200
total ON time alarm threshold, 218
trigger address, 167
TUNID, 79
Two Hand Controller, 155

U

unlocking the device configuration, 100
uploading, 67, 90
uploading device parameters, 90

uploading the network configuration, 83
USB port, 77
User Mode Switch, 156
User Mode Switch Monitoring, 156
user-defined function block files, 178
user-defined function blocks, 170

V

voltage monitoring, 198

W

Workspace, 154

Revision History

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

Cat. No.	Z905-E1-03
-----------------	-------------------

↑ Revision code

The following table outlines the changes made to the manual during each revision. Page numbers refer to the previous version.

Revision code	Date	Revised content
01	May 2005	Original production
02	April 2006	Revisions for changing from Network Configurator version 1.32 to 1.5□.
03	September 2006	Revised to include the Network Configurator upgrade from version 1.5□ to 1.6□.

OMRON Corporation
Technology Development Center H.Q.
Shiokoji Horikawa, Shimogyo-ku,
Kyoto, 600-8530 Japan
Tel: (81)75-344-7123/Fax: (81)75-344-7172

Regional Headquarters

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

OMRON ELECTRONICS LLC
1 East Commerce Drive, Schaumburg, IL 60173
U.S.A.
Tel: (1)847-843-7900/Fax: (1)847-843-8568

OMRON ASIA PACIFIC PTE. LTD.
83 Clemenceau Avenue,
#11-01, UE Square,
Singapore 239920
Tel: (65)6835-3011/Fax: (65)6835-2711

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120 China
Tel: (86)21-5037-2222/Fax: (86)21-5037-2200



Authorized Distributor: