NE1A-SCPU01
DST1-ID, DST1-MD, DST1-MR

DeviceNet Safety

SYSTEM CONFIGURATION MANUAL

OMRON

DeviceNet Safety
System Configuration Manual

Produced May 2005

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.

Table of contents

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.

NE1A-SCPU01 Safety Network Controller Operation Manual (Z906)

This manual describes the specifications, functions, and usage of the NE1A-SCPU01.

DST1-series 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.

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.	❶
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.	❶
Safety functions may be impaired and serious injury may occasionally occur. For the DST1-MRD08SL-1, apply only one AC line phase to the relay output.	❶
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.	❶
Safety functions may be impaired, and serious injury may occasionally occur. Before connecting a device to the network, clear the previous configuration data.	❶
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.	❶
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.	❶
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.	❶
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.	❶

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

Confirim 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 mm2 (AWG 24 to AWG 12)
Stranded (flexible) wire	0.34 to 1.5 mm2 (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.

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.
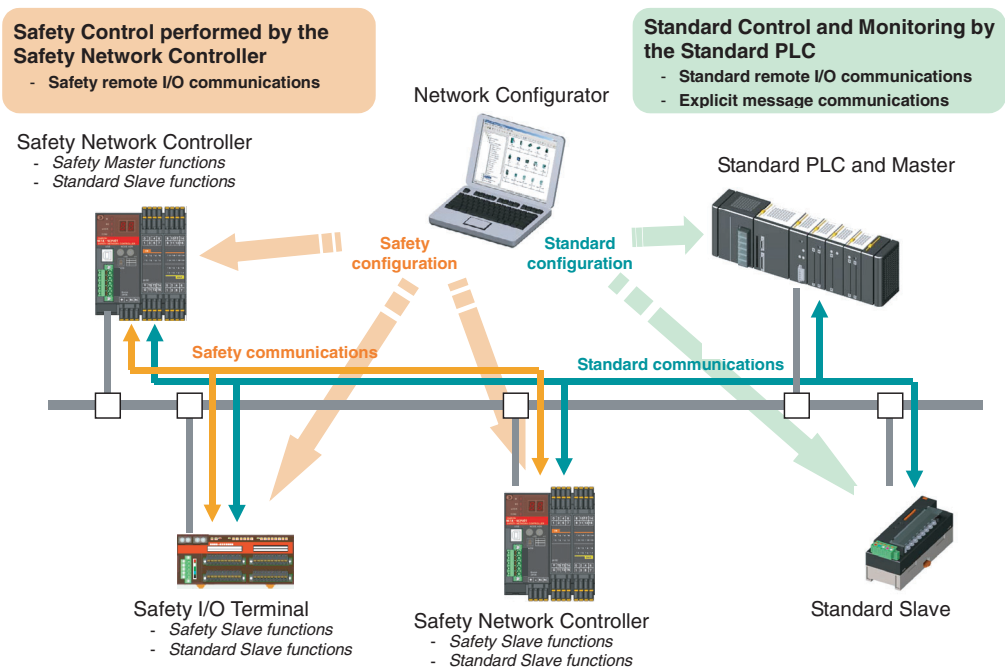
1-2 Safety Network Controller Overview

1-2-1 About the NE1A Safety Network Controller

The NE1A Safety Network Controller (NE1A-SCPU01) provides various functions, such as safety logic operations, safety I/O control, and a DeviceNet Safety protocol. The NE1A-SCPU01 allows 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-SCPU01 and the monitoring system implemented with the standard PLC are realized on the same network.

- As a Safety Logic Controller, the NE1A-SCPU01 executes safety logic operations and controls local I/O.
- As a Safety Master, the NE1A-SCPU01 controls the remote I/O of Safety Slaves.
- As a Standard Slave, the NE1A-SCPU01 communicates with the Standard Master.
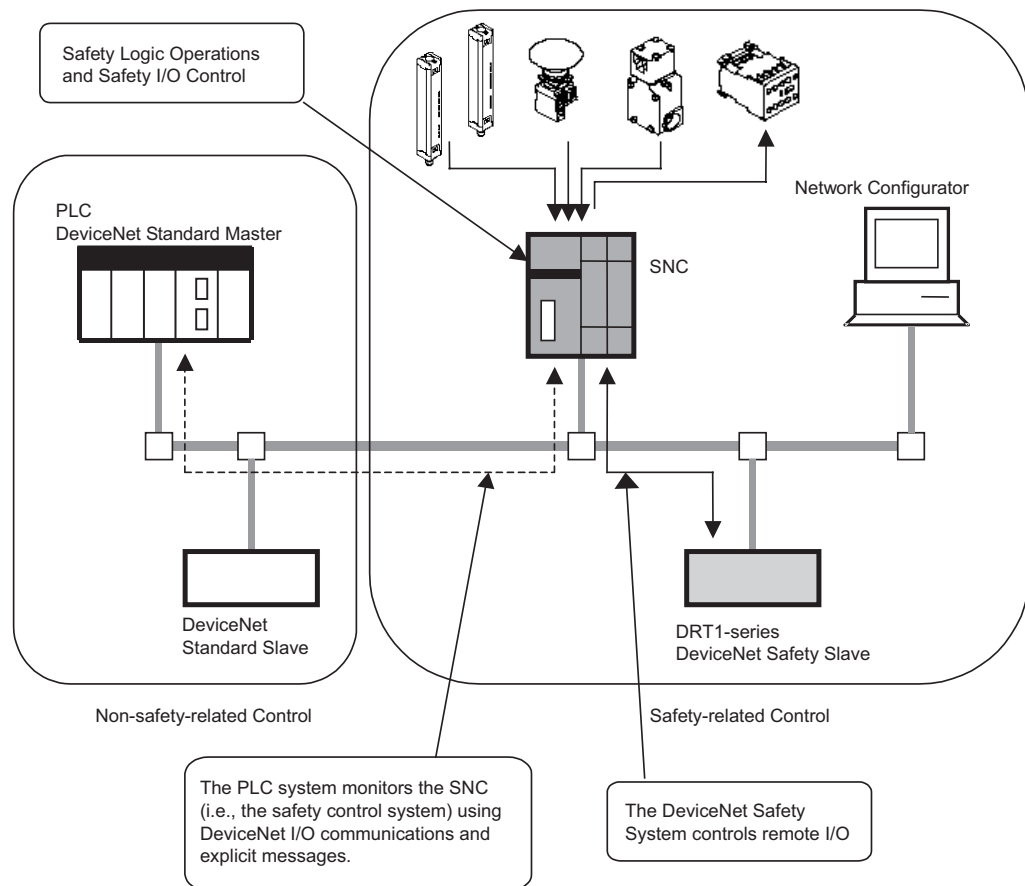
1-2-2 Safety Network Controller Features

Safety Logic Operations

In addition to basic logic functions, such as AND and OR, the NE1A-SCPU01 also supports application function blocks, such as Emergency Stop Pushbutton Monitoring and Safety Gate Monitoring, that enable various safety applications.

Local Safety I/O

- A total of 24 local safety I/O points are supported: 16 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-SCPU01 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-SCPU01 can evaluate the output data patterns.

DeviceNet Safety Communications

- As a Safety Master, the NE1A-SCPU01 can perform safety I/O communications with up to 16 connections using up to 16 bytes per connection.

- As a Safety Slave, the NE1A-SCPU01 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-SCPU01 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-SCPU01 can be used as a Standalone Controller by disabling the NE1A-SCPU01'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 log function or the indicators on the front of the NE1A-SCPU01.
- The NE1A-SCPU01'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-SCPU01 configuration data is protected by a password.
- Network configuration files (project files) created with the Network Configurator are also password protected.

1-2-3   Standard Models

| Model number	Name	Number of I/O points		
		Safety inputs	Test outputs	Safety outputs
NE1A-SCPU01	Safety Network Controller (NE1A-SCPU01)	16 inputs	4 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 (NE1A-SCPU01).

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.
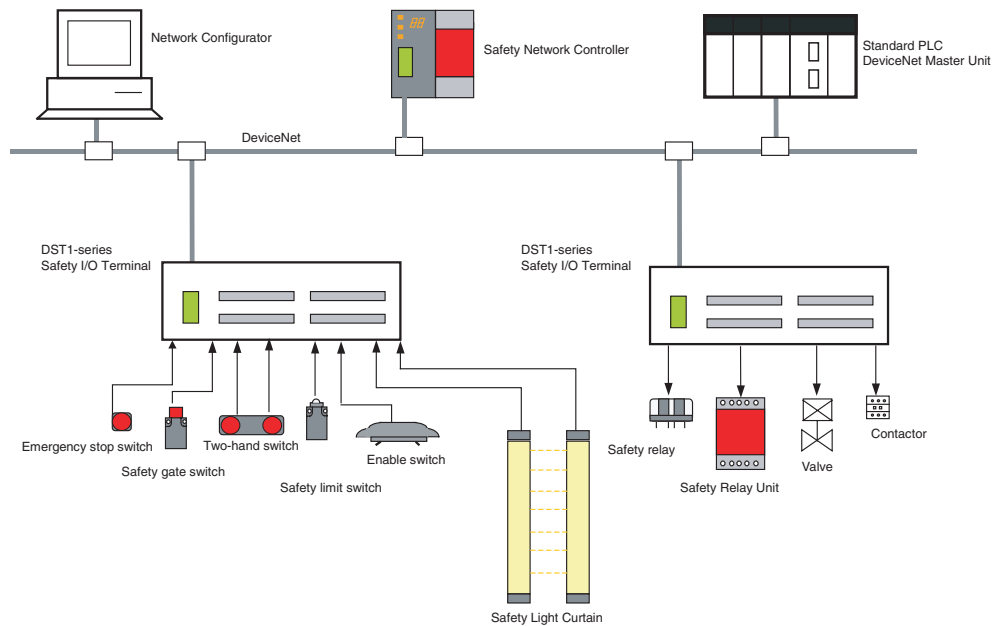
1-3-2 Safety I/O Terminal Features

Safety Inputs

- Semiconductor output devices such 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 log function 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, cumulative 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 is Support Software 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.
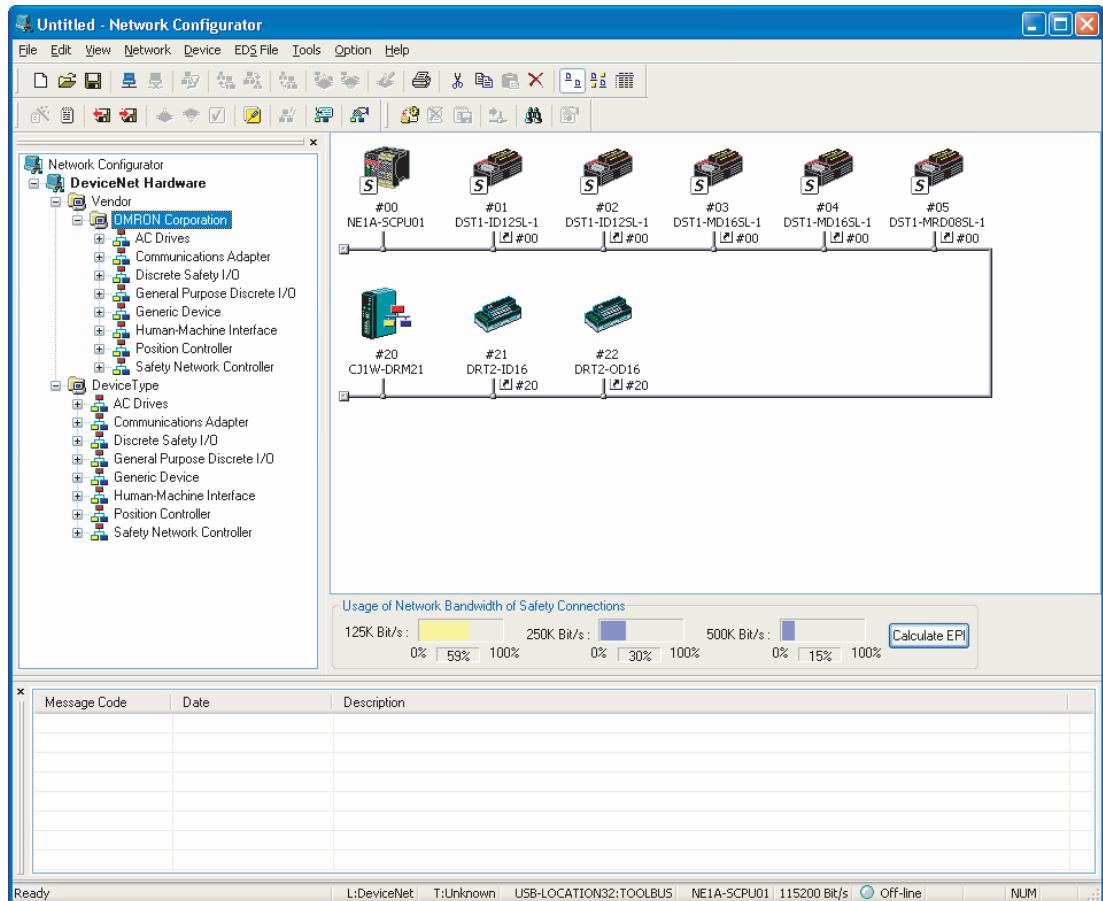
1-4-2 Network Configurator Features

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. Consequently, the Network Configurator supports various system configurations, including standard systems, safety systems, and mixed systems containing both standard and safety devices.

NE1A-SCPU01 Programming

The Network Configurator is equipped with a Programming Tool that is compatible with the NE1A-SCPU01's safety logic programming. DeviceNet Safety applications can be created independently with the Network Configurator.

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.

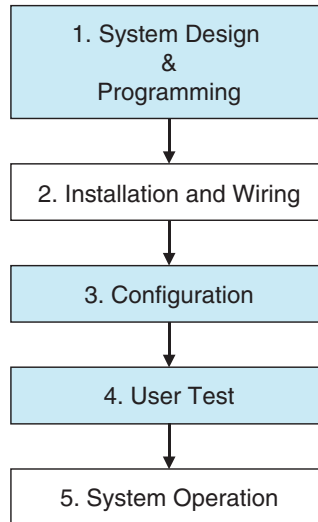| Item	Specification
Computer	IBM PC/AT or compatible computer with 300 MHz or faster processor
	128 MB RAM min.
	40 MB free hard disk space
	Super VGA (800 x 600) or higher Display
	CD-ROM drive or DVD drive
OS	Windows$^®$ 2000 or Windows$^®$ XP
COM Port	One of the following COM Ports is required:
	• USB Port: For an online connection via the NE1A-SCPU01'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. System Design  │
        │          &          │
        │    Programming      │
        └─────────────────────┘
                   │
                   ▼
        ┌─────────────────────┐
        │ 2. Installation and Wiring │
        └─────────────────────┘
                   │
                   ▼
        ┌─────────────────────┐
        │   3. Configuration  │
        └─────────────────────┘
                   │
                   ▼
        ┌─────────────────────┐
        │    4. User Test     │
        └─────────────────────┘
                   │
                   ▼
        ┌─────────────────────┐
        │ 5. System Operation │
        └─────────────────────┘
```

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-SCPU01.
- 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-SCPU01 and Safety I/O Terminal parameter settings, and NE1A-SCPU01 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 *2-4 Creating a Virtual Network* (page 34).
- Editing Device Parameters
  - Refer to *2-7 Device Parameters and Properties* (page 41).
  - Refer to *Section 4: Editing Safety I/O Terminal Parameters* (page 69).
  - Refer to *Section 5: Editing Safety Network Controller Parameters* (page 79).
- Checking the Usage Rate of Network Bandwidth
  - Refer to *3-2 Verifying the Network Bandwidth* (page 59).
- Calculating the Reaction Time
  - Refer to *3-3 Calculating and Verifying the Maximum Reaction Time* (page 63).

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-SCPU01 installation	NE1A-SCPU01 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 *2-7 Device Parameters and Properties* (page 41).
- Verification
    - Refer to *2-8 Parameter Verification* (page 45).

> **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 *2-9 Configuration Lock* (page 48) 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: **Basic Operation of the Network Configurator**

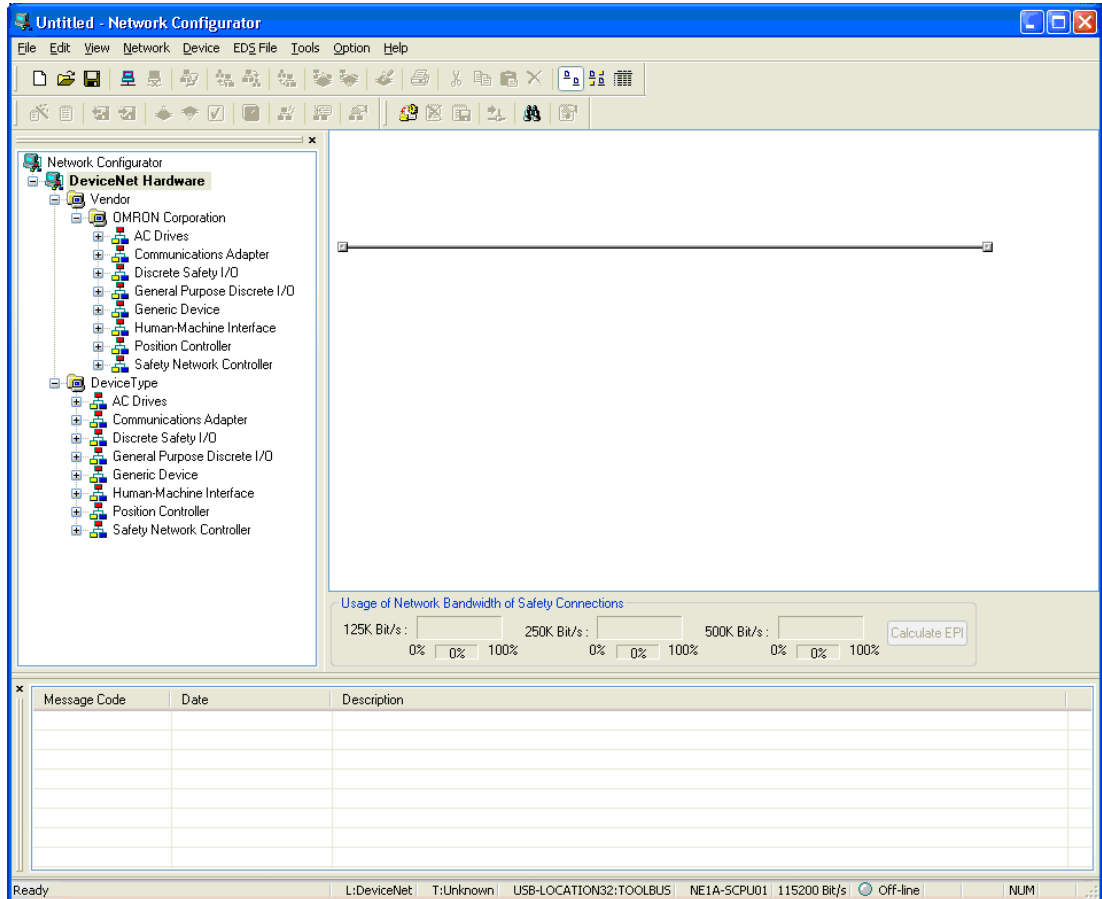## 2-1 Network Configurator Startup and Main Window

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

2-1-1 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.
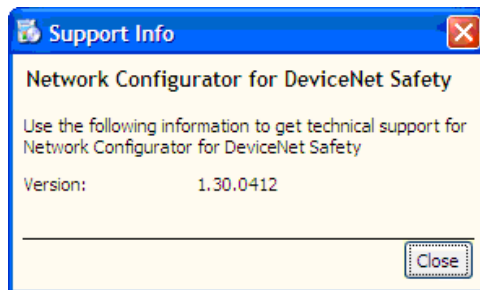
The Network Configurator will close.

2-1-2 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.
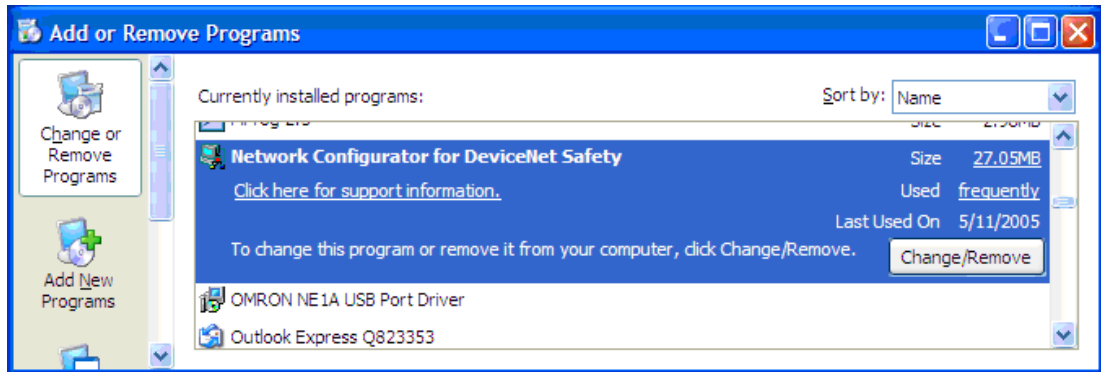
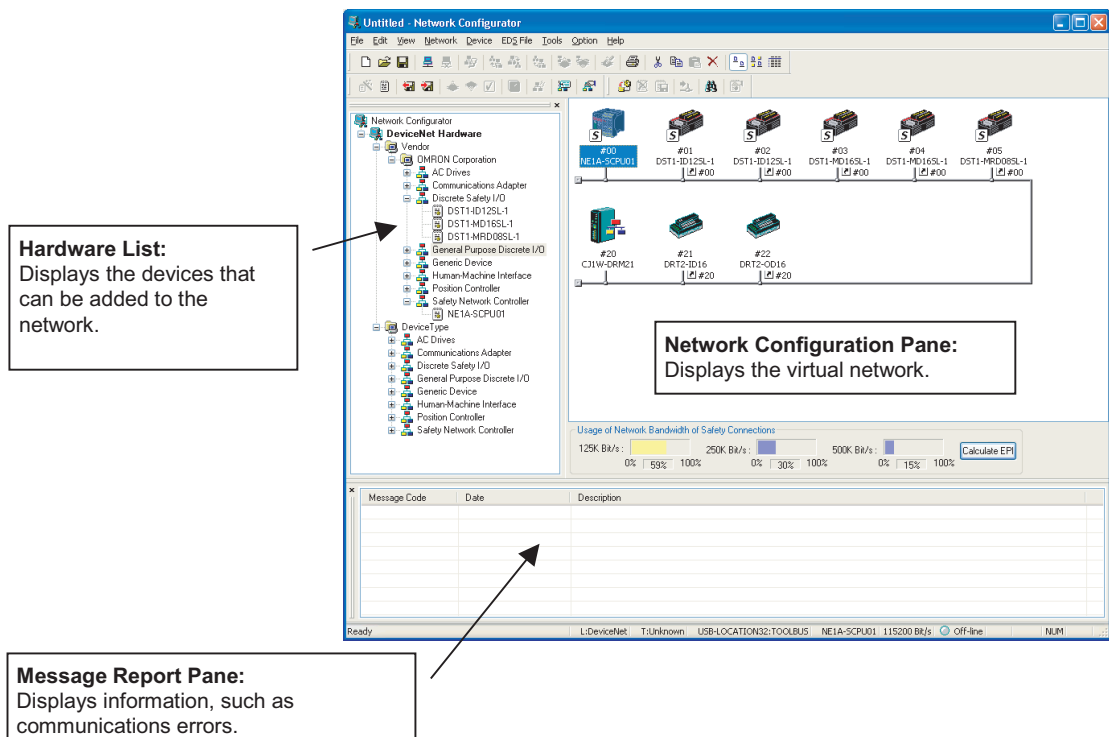4. The version will be displayed as support information.

2-1-3 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.

Network Configuration Pane:
Displays the virtual network.

Message Report Pane:
Displays information, such as communications errors.

2-2 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.

2-2-1 File Menu

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
			O: Supported	x: Not supported

2-2-2 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
		O: Supported	x: Not supported

2-2-3 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
Details	Switches to the detailed display.	O	O
Hardware List	Displays or hides the Hardware List.	O	O
		O: Supported	x: Not supported

2-2-4 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
		O: Supported	x: Not supported

Submenu		Description	Offline	Online
Wireless Network	Move to Upper Network	Displays the network one layer above the current network in the wireless networks.	×	O
	Move to Lower Network	Displays the network one layer below the current network in the wireless networks.	×	O
Upload		Uploads all the device parameters in the network to the Network Configurator.	×	O
Download		Downloads all the device parameters in the Network Configurator to the devices in the network.	×	O
Verify Structure		Verifies the current network configuration in the Network Configurator with the actual network configuration of the destination online connection.	×	O
Update Maintenance Information		Updates the maintenance information of each device to the latest information.	×	O
Check Connection		Checks the consistency of all the connections.	O	O
Property		Displays the network properties. The network name and safety network number can be set.	O	O
		O: Supported ×: Not supported		

2-2-5   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.	×	O
	Download	Downloads the device parameters to a device in the network.	×	O
	Verify	Verifies the device and the device parameters in the network.	×	O
	Lock	Locks the configuration of a device in the network.	×	O
	Unlock	Unlocks the locked configuration of a device in the network.	×	O
Monitor		Monitors the parameters and status of a device in the network. Not all devices support this function.	×	O
Reset		Resets a device in the network.	×	O
Change Mode		Changes the status of a device in the network. Not all devices support this function.	×	O
Change Password		Changes the password of a device in the network.	×	O
Maintenance Information		Displays the maintenance information of a device in the network.	×	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
Edit I/O Comment		Edits the I/O comment.	O	O
Property		Displays the properties of a device.	O	O
		O: Supported ×: Not supported		

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

2-2-6 EDS File Menu

Submenu	Description	Offline	Online
Install	Installs an EDS file and adds a device to the Hardware List.	O	O
Create	Creates a new EDS file and adds a device to the Hardware List.	O	O
Delete	Deletes a device from the Hardware List. The installed EDS file is also deleted.	O	O
Save As	Names and saves the EDS file of a device on the Hardware List.	O	O
Find	Searches for a specified EDS file from the Hardware List.	O	O
Add to Network	Adds a device on the Hardware List to the virtual network.	O	O
Property	Displays the properties of an EDS file.	O	O
		O: Supported ×: Not supported	

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

2-2-7 Tools Menu

Submenu	Description	Offline	Online
Setup Parameters	Sets parameters by using explicit message communications.	×	O
Setup Node Address/Baud Rate	Sets the node address and baud rate of a device in the network.	×	O
		O: Supported ×: Not supported	

2-2-8 Option Menu

Submenu	Description	Offline	Online
Select Interface	Selects an interface for the Network Configurator to use for the network connection.	O	O
Edit Configuration File	Edits various configuration files.	O	O
Setup Monitor Refresh Timer	Sets the monitor refresh timer values (monitoring cycles in device monitoring).	O	O
Install Extend Module	Installs an Expansion Module.	O	O
Install Interface Module	Installs an Interface Module.	O	O
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.	O	O
		O: Supported ×: Not supported	

2-2-9 Help Menu

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

2-3　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-SCPU01 and a DeviceNet Interface Card installed in a computer. Refer to the Appendix for other network connection procedures.

2-3-1　Network Connection via USB Port

1. Turn ON the power supply to the NE1A-SCPU01 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.
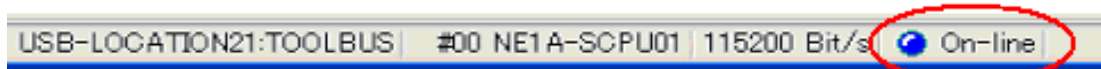
## 2-3-2 Network Connection via DeviceNet Interface Card

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

   The Select Interface Dialog Box will be displayed.
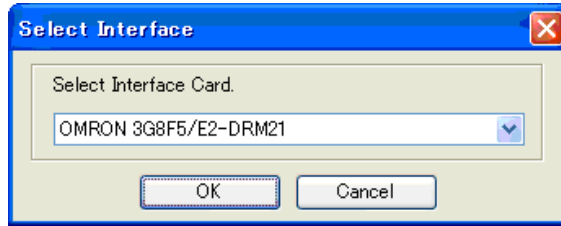
3. Select the interface card, and click the OK Button.

    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.
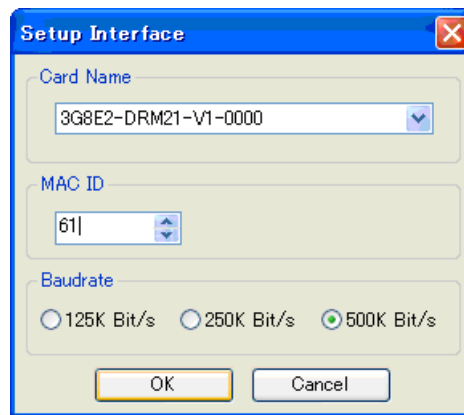
4. Set the MAC ID (node address) and baud rate, and click the **OK** Button.

    The Select Connect Network Port Dialog Box will be displayed.
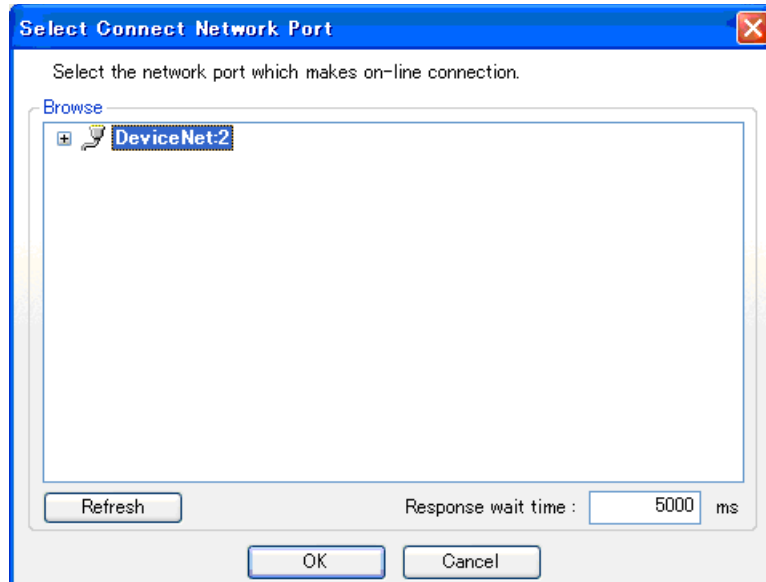
In the first network connection, a network search is performed automatically with this dialog box displayed. Wait until the search has been performed for all addresses. After the search, the networks that can be connected will be displayed.

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.

2-4 Creating a Virtual Network

To set device parameters and to program the NE1A-SCPU01, 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.

2-4-1 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.

2-4-2 Network Numbers

The network number (i.e., the network address) is the number set for each network domain. All devices on the same network must have the same network number.

The network number is set as a unique node identifier (UNID) in combination with the node address from the Network Configurator and saved in the device. UNID is used to identify one device from all the network domains.

The Network Configurator automatically creates the network number based on the time and date when a new network configuration file is created. Under normal conditions, the user does not have to consider this operation.

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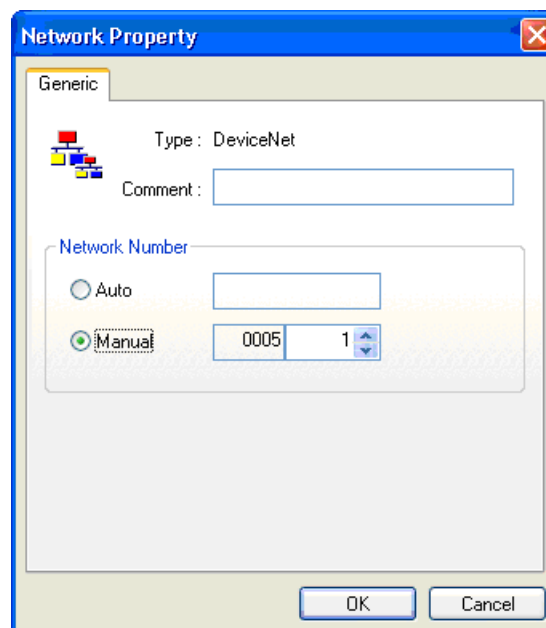
IMPORTANT: Always allocate a unique network number when a network or subnetwork is established.

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.

2-4-3 Adding Devices

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

(1) Adding from the Hardware List.

(2) Uploading the network configuration from the actual network.

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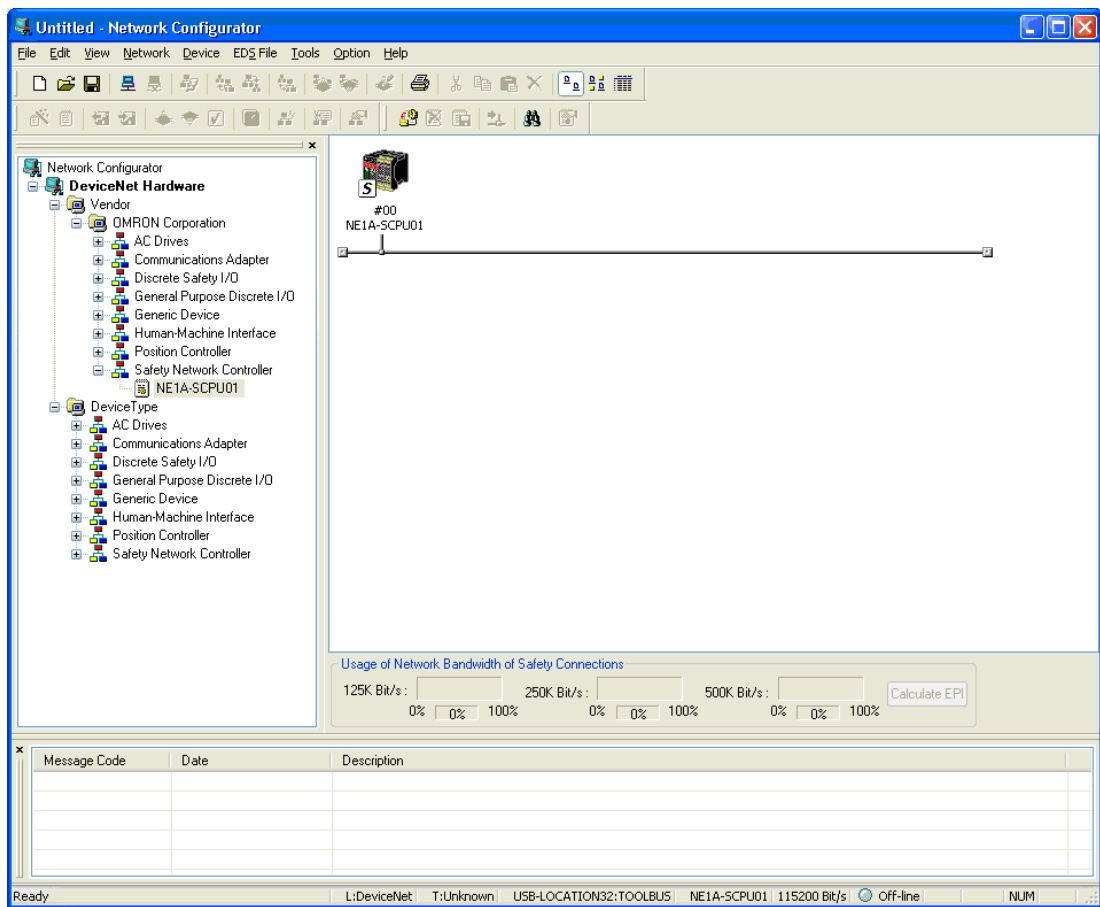
Uploading the Network Configuration from the Actual Network (Network Upload)

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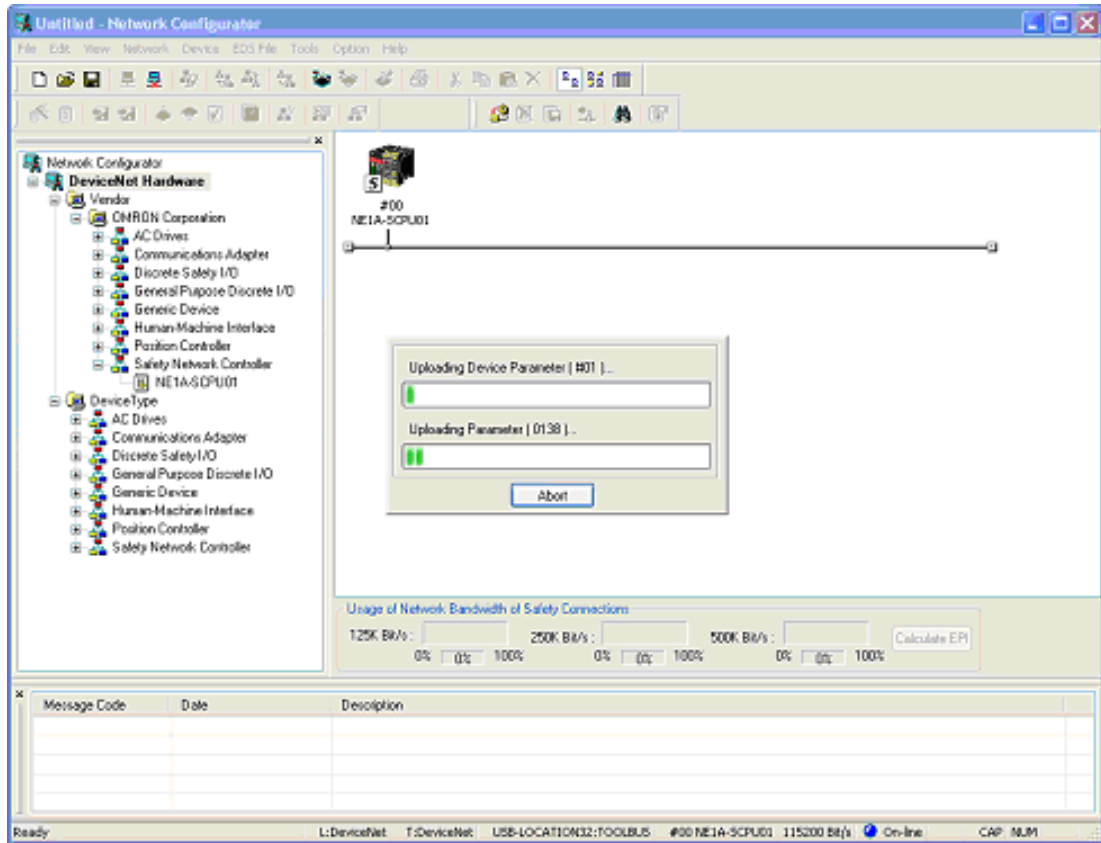
If there is another device that must be added after the upload has completed, add the device following the same procedure as in Adding Devices from the Hardware List, above.

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 a network is uploaded, the virtual network information that was displayed until then will be deleted. If the previous virtual network information is required, save the data before the network upload.
– When a network in which devices already have a set network number is uploaded, the value that is already set in the devices is used for the network number.

2-4-4   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.

2-4-5　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.
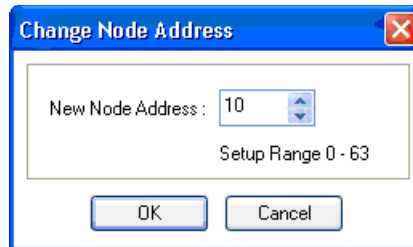
2-4-6　Changing Device Comments

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.

2-5　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.

2-5-1　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.

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 cannot open a network configuration file if the password is forgotten.

2-5-2　Saving the Network Configuration File

The network configuration can be saved using either of the following methods.
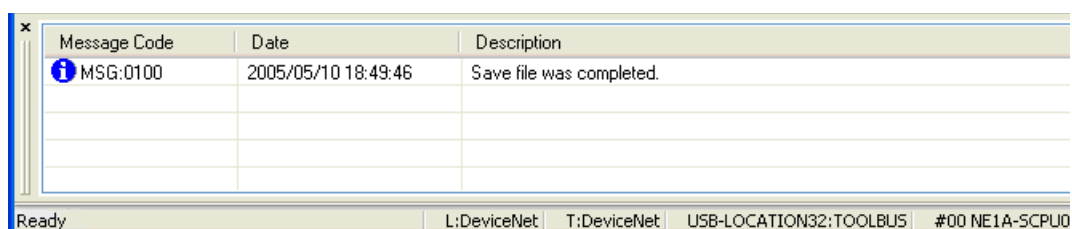
(1) Select **File - Save** or **File - Save As** from the menu bar.

(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:

2-5-3   Reading a Network Configuration File
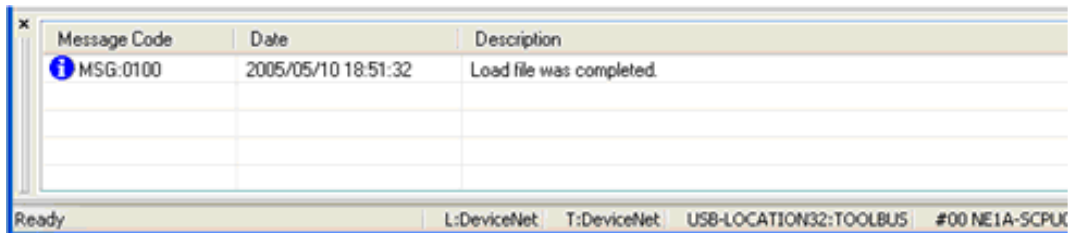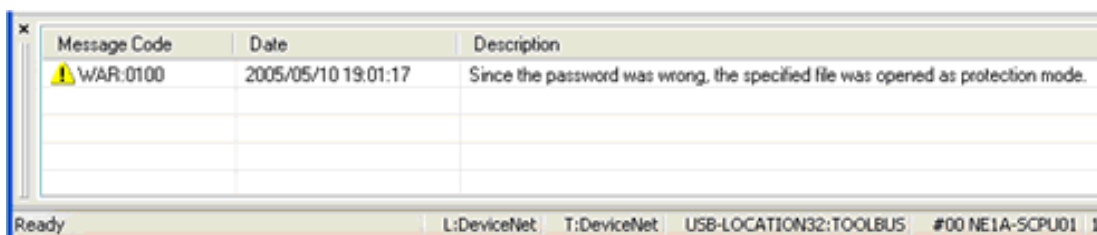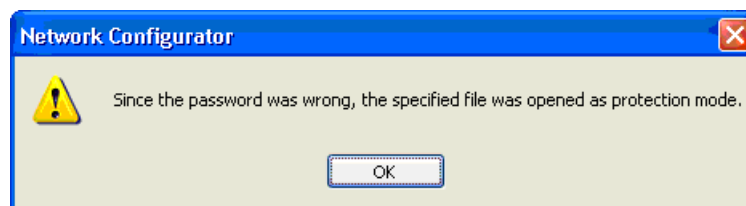
The saved network configuration file can be read for use by the Network Configurator using either of the following methods.

(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:

Message Code	Date	Description
ⓘ MSG:0100	2005/05/10 18:51:32	Load file was completed.

Ready   L:DeviceNet   T:DeviceNet   USB-LOCATION32:TOOLBUS   #00 NE1A-SCPU0

> **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 *2-5-4 Protect Mode* (page 39) for details.

2-5-4   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.

Network Configurator

⚠ Since the password was wrong, the specified file was opened as protection mode.

OK

Message Code	Date	Description
⚠ WAR:0100	2005/05/10 19:01:17	Since the password was wrong, the specified file was opened as protection mode.

Ready   L:DeviceNet   T:DeviceNet   USB-LOCATION32:TOOLBUS   #00 NE1A-SCPU01 1

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

2-6　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.

2-6-1　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.

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.

2-6-2　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

2-7 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.

2-7-1 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* (page 69) for editing device parameters of DST1-series Safety I/O Terminals.

Refer to *Section 5* (page 79) for editing device parameters of the NE1A-SCPU01.

2-7-2 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 *2-4-3 Adding Devices* (page 35).

2-7-3 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.
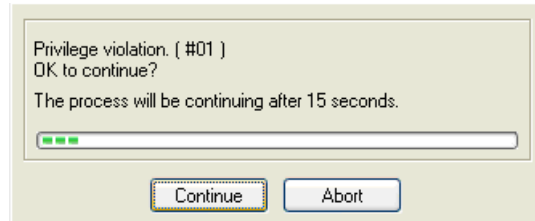
Downloading will continue to the next device if 15 seconds passes and neither button is clicked. If you want to perform the next download immediately, however, click the **Continue** Button.

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 listed at the end of processing and displayed in the Message Pane.
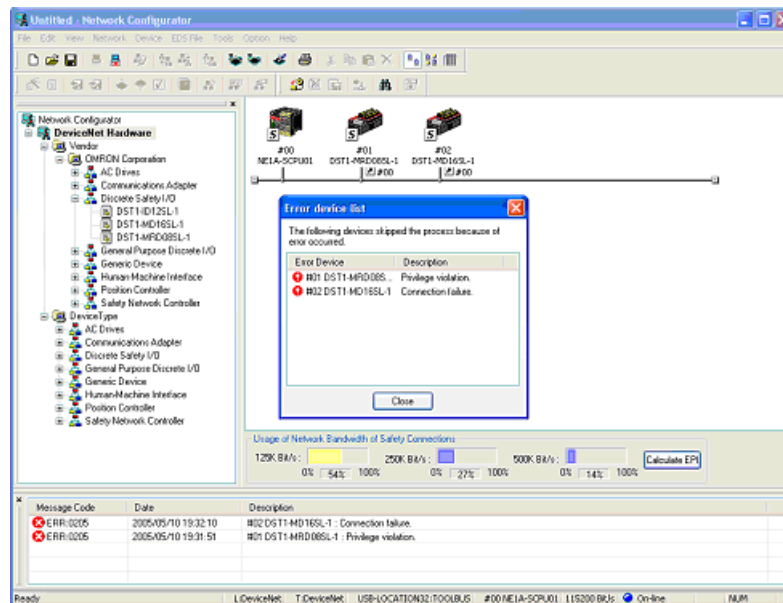
2-7-4   Device Properties

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 the 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.
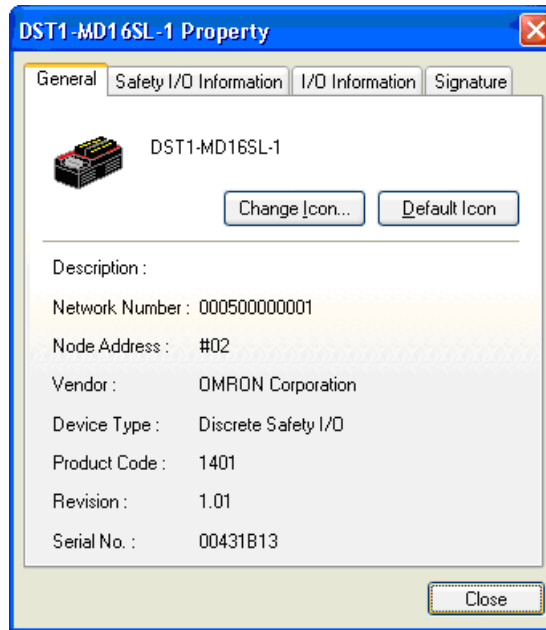
Safety I/O Information Tab Page

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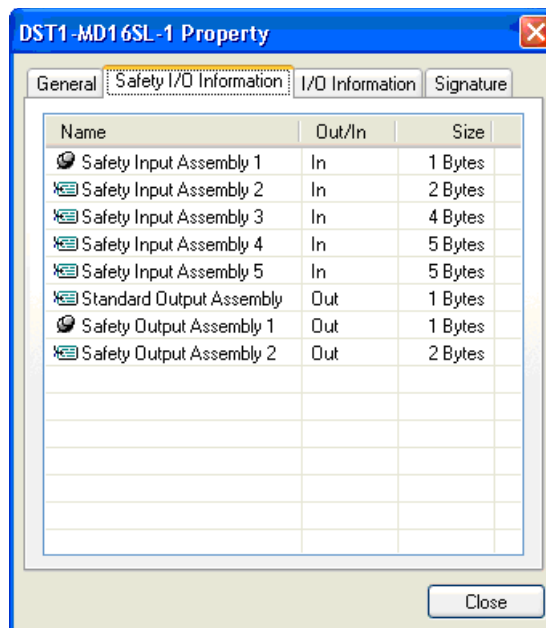
I/O Information Tab Page

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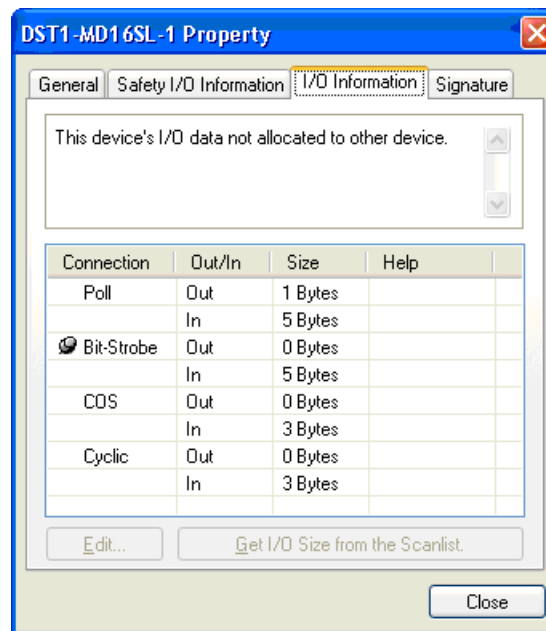
Signature Tab Page

In this tab page, you can check the safety signature that the Network Configurator generated and the one that the actual device has.
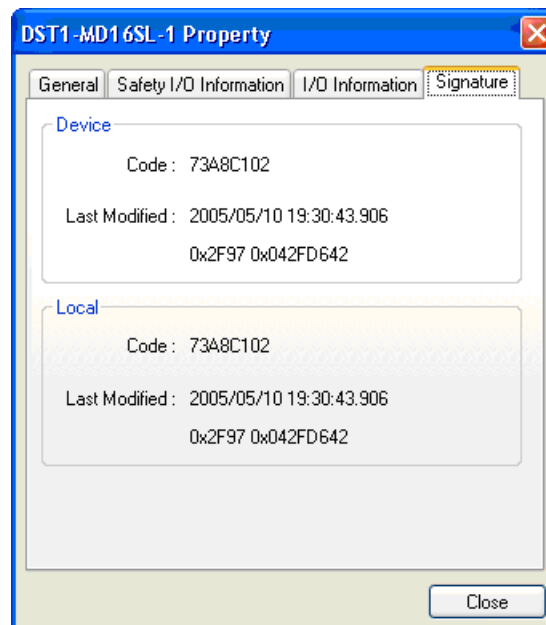
2-8 Parameter Verification

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.

2-8-1 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.
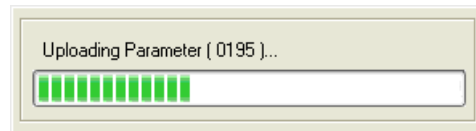
First, the Network Configurator itself checks if the uploaded parameters are different from the parameters in the virtual network. If there are no differences, the following dialog box will be displayed.
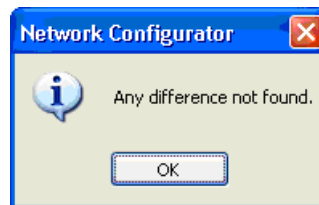
If you click the **OK** Button, the uploaded parameters will be displayed.

The user must check whether all the displayed parameters match the input values. If the device is the NE1A-SCPU01, the Logic Program will also be displayed as in the following window. Check whether the Logic Program matches.
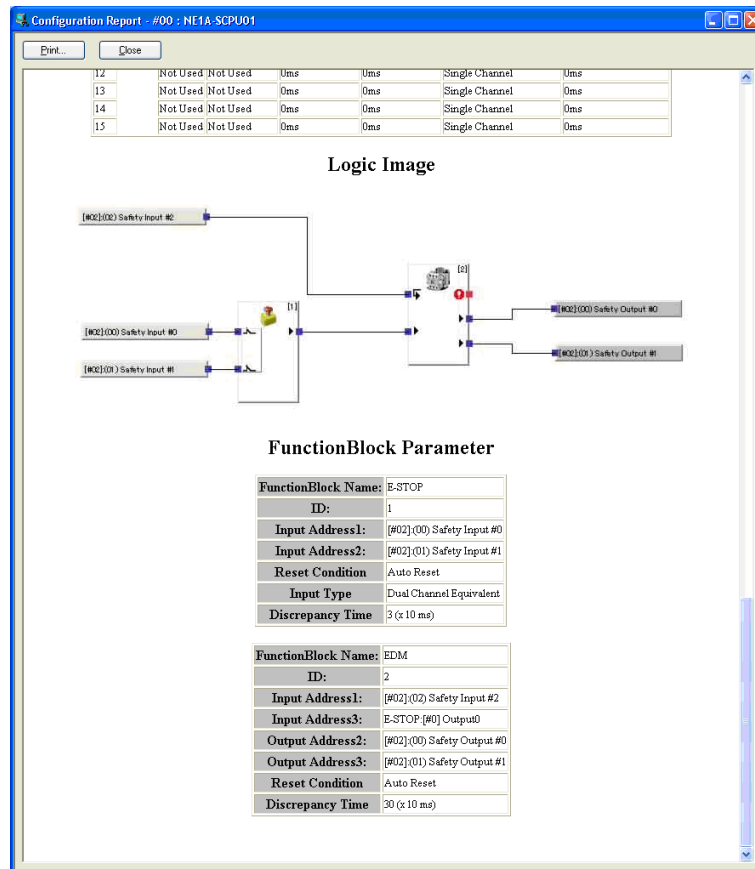
Note: The displayed parameters and logic can also be printed. To print, click the Print Button at the upper left of the window.

After completing the verification, click the **Close** Button in the upper left to close the window.
The following window will be displayed.
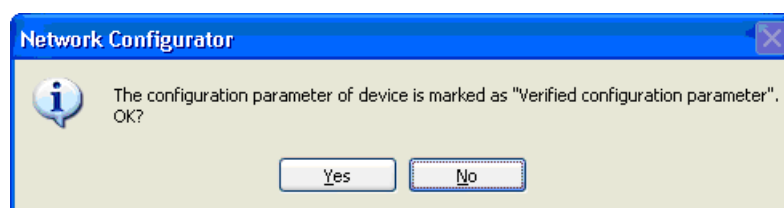
If the parameters match, click the **Yes** Button.
After the verification has been completed, the safety symbol attached to the device icon in the virtual network will turn green, which indicates that verification is done.

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: – 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.

Section 2: Basic Operation of the Network Configurator

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.
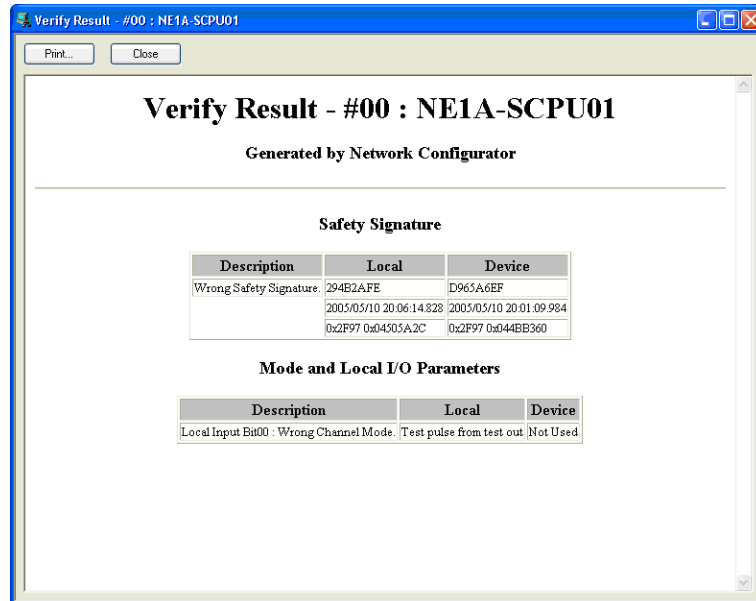
2-9 Configuration Lock

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.

2-9-1 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.
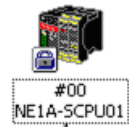
IMPORTANT: Operation of the device must be tested before lock the configuration.

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.

2-9-2 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* (page 48), 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.

2-10 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.

2-10-1 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-SCPU01 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 communi- cations	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. ❗

2-10-2 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:
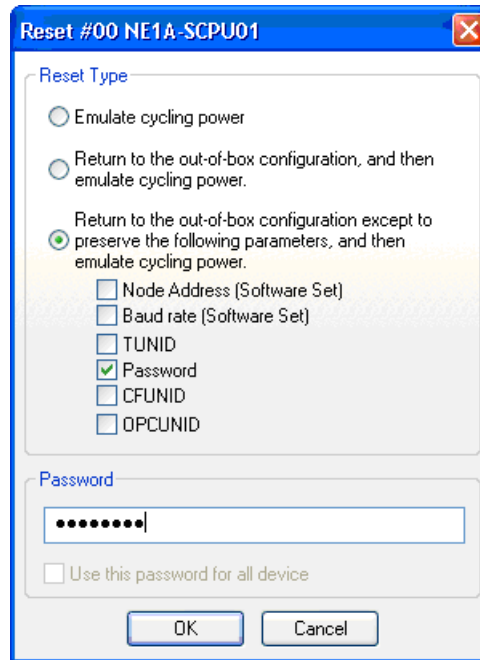
2-10-3 Reset Types and Device Status

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.

2-10-4   Changing Device Status

Changing the device status is not supported by all devices.

The NE1A-SCPU01 can switch between IDLE mode and RUN mode. For details on NE1A-SCPU01 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 3: **Constructing a Safety Network**

3-1 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

3-1-1 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 *2-1-1 Starting and Exiting the Network Configurator* (page 27).

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 *2-4 Creating a Virtual Network* (page 34).

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* (page 69) and to the *DST1 Series I/O Terminal Operation Manual (Z904)*.

    Set the parameters of the NE1A-SCPU01 configured in the virtual network.

    Refer to *Section 5: Editing Safety Network Controller Parameters* (page 79) and to the *Safety Network Controller Operation Manual (Z906)*.

    Program the NE1A-SCPU01 configured in the virtual network.

    Refer to *Section 6: Programming the Safety Network Controller* (page 97) 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 *3-2 Verifying the Network Bandwidth* (page 59).

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 *3-3 Calculating and Verifying the Maximum Reaction Time* (page 63).

6. Saving the Network Configuration File

    Save the network configuration file with the completed design.

    Refer to *2-5-2 Saving the Network Configuration File* (page 38).

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-SCPU01 or a DeviceNet Interface Card.

    Refer to *2-3 Connecting to the Network* (page 32).

9. Reading the Network Configuration File

    Read the saved network configuration file with the completed design.

    Refer to *2-5-3 Reading a Network Configuration File* (page 39).

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 *3-1-2 Changing an Established Safety Network* (page 56).

11. Downloading Device Parameters

Download the parameters to all the devices.

Refer to *2-7-3 Downloading Device Parameters* (page 41).

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 *2-8 Parameter Verification* (page 45).

13. Saving the Network Configuration File

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

Refer to *2-5-2 Saving the Network Configuration File* (page 38).

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-SCPU01 or a DeviceNet Interface Card.

Refer to *2-3 Connecting to the Network* (page 32).

17. Reading the Network Configuration File

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

Refer to *2-5-3 Reading a Network Configuration File* (page 39).

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 *2-9-1 Locking the Device Configuration* (page 48).

19. Saving the Network Configuration File

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

Refer to *2-5-2 Saving the Network Configuration File* (page 38).

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.

3-1-2 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-SCPU01.

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-SCPU01 or a DeviceNet Interface Card.

   Refer to *2-1-1 Starting and Exiting the Network Configurator* (page 27) and *2-3 Connecting to the Network* (page 32).

3. Uploading the Network Configuration

   Upload the network to obtain the current network configuration.

   Refer to *2-4 Creating a Virtual Network* (page 34).

4. Unlocking the Configurations

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

   Refer to *2-9-2 Unlocking the Device Configuration* (page 48).

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.

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.

⚠ **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 *2-5-3 Reading a Network Configuration File* (page 39).

10. Changing the Virtual Network

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

    Refer to *2-4 Creating a Virtual Network* (page 34).

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* (page 69) and to the *DST1 Series I/O Terminal Operation Manual (Z904)*.

    Set and change the parameters of the NE1A-SCPU01 configured in the virtual network according to specified changes.

    Refer to *Section 5: Editing Safety Network Controller Parameters* (page 79) and to the *Safety Network Controller Operation Manual (Z906)*.

Create and change the program of the NE1A-SCPU01 configured in the virtual network according to specified changes.

Refer to *Section 6: Programming the Safety Network Controller* (page 97) 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 *3-2 Verifying the Network Bandwidth* (page 59).

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 *3-3 Calculating and Verifying the Maximum Reaction Time* (page 63).

14. Saving the Network Configuration File

Save the network configuration file with the completed changes.

Refer to *2-5-2 Saving the Network Configuration File* (page 38).

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-SCPU01 or a DeviceNet Interface Card.

Refer to *2-3 Connecting to the Network* (page 32).

17. Reading the Network Configuration File

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

Refer to *2-5-3 Reading a Network Configuration File* (page 39).

18. Downloading Device Parameters

Download the parameters to all the devices.

Refer to *2-7-3 Downloading Device Parameters* (page 41).

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 *2-8 Parameter Verification* (page 45).

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 *2-5-2 Saving the Network Configuration File* (page 38).

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-SCPU01 or a DeviceNet Interface Card.

    Refer to *2-3 Connecting to the Network* (page 32).

24. Reading the Network Configuration File

    Read the saved network configuration file with verified parameters.

    Refer to *2-5-3 Reading a Network Configuration File* (page 39).

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 *2-9-1 Locking the Device Configuration* (page 48).

26. Saving the Network Configuration File

    Save the file of a virtual network with a locked configuration.

    Refer to *2-5-2 Saving the Network Configuration File* (page 38).

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.

3-2 Verifying the Network Bandwidth

Approximately 100% of the network bandwidth in the DeviceNet can be used. If the setting exceeds the acceptable bandwidth, however, timeouts will occur.

This section describes how to check the network bandwidth used for safety I/O communications in the designed network and how to calculate EPI from the usage rate of the set bandwidth.

3-2-1 Checking the Network Bandwidth Used for Safety I/O Communications

In the lower portion of the network window, the Network Configurator displays the percentage of the network bandwidth used for safety I/O communications from the connections set in the virtual network.
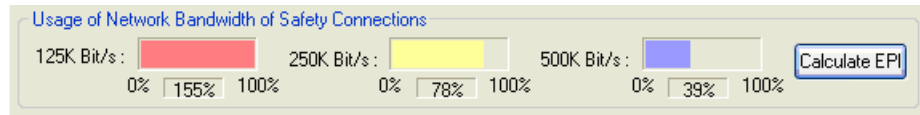
The percentage of network bandwidth used is displayed for each baud rate.

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 bandwidth exceeds 90%, obtain the average EPI by referring to the next section and use it as the reference for setting connections.

IMPORTANT: Keep 10% or more space in the network bandwidth for establishing a connection and for communications of the Network Configurator. If the user application uses explicit message communications, additional network bandwidth is necessary. In this case, decide the network bandwidth for the explicit messaging in consideration of the amount of the data and the frequency of the communications.

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

When both safety I/O communications and standard I/O communications are mixed on one network, it is necessary to determine the network bandwidth to use for each communication. In this case, check that the network bandwidth used for safety I/O communications does not exceed the determined value.

The Network Configurator can calculate the average EPI by the user entering the network bandwidths to use for communications. Set the EPI for each safety connection and the communications cycle of the Standard Master referring to this value.

3-2-2　Allocating Network Bandwidth

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

Calculate the EPIs using the following procedures:

1. Set the virtual network on the Network Configurator as needed.
2. Click the **EPI Calculation** Button in the lower portion of the Network Configuration Pane.
3. Input the network bandwidth used in safety I/O communications and the bandwidth used in standard I/O communications, and then click the **Calculate** Button.
4. The average EPI of all the connections in the safety I/O communications and the communications cycle time in the standard I/O communications will be displayed for each baud rate. Review the EPIs for safety I/O communications and the communications cycle time of the Standard Master referring to the baud rate that is to be used.

IMPORTANT:
- Keep 10% or more space in the network bandwidth for establishing a connection and for communications of the Network Configurator. If the user application uses explicit message communications, additional network bandwidth is necessary. In this case, decide the network bandwidth for the explicit messaging in consideration of the amount of the data and the frequency of the communications.
- The calculation result is the average value of all the safety connections. Use this value as a guideline. Adjust the EPI for the whole network by shortening the EPI for connections that require a high-speed reaction time and lengthening the EPI for connections that do not require high speed.
- Check that the displayed usage rate in the lower portion of the Network Configuration Pane is the allocated value or less when adjusting the EPI of the whole network based on the calculation results. Communications timeout might occur if the calculated bandwidth is not properly allocated to the standard connections because the priority of safety I/O communications is higher than that of standard I/O communications.
- The total network bandwidth used in the safety connections and the standard connections must be around 90% at the maximum, i.e., 10% or more available bandwidth must be left for explicit message communications.
- Perform user testing to make sure that there is no problem in the set values.

Note:
- If you do not want to mix with standard I/O communications, set the network bandwidth used for standard connections to 0.
- The EPI is set in 1 ms increments. The network bandwidth to be used may thus be smaller than the allocated value when the calculated value is used.

3-2-3 Example of EPI Calculation

The following network configuration is used for an example of calculating the EPI. The baud rate is 500 Kbit/s.
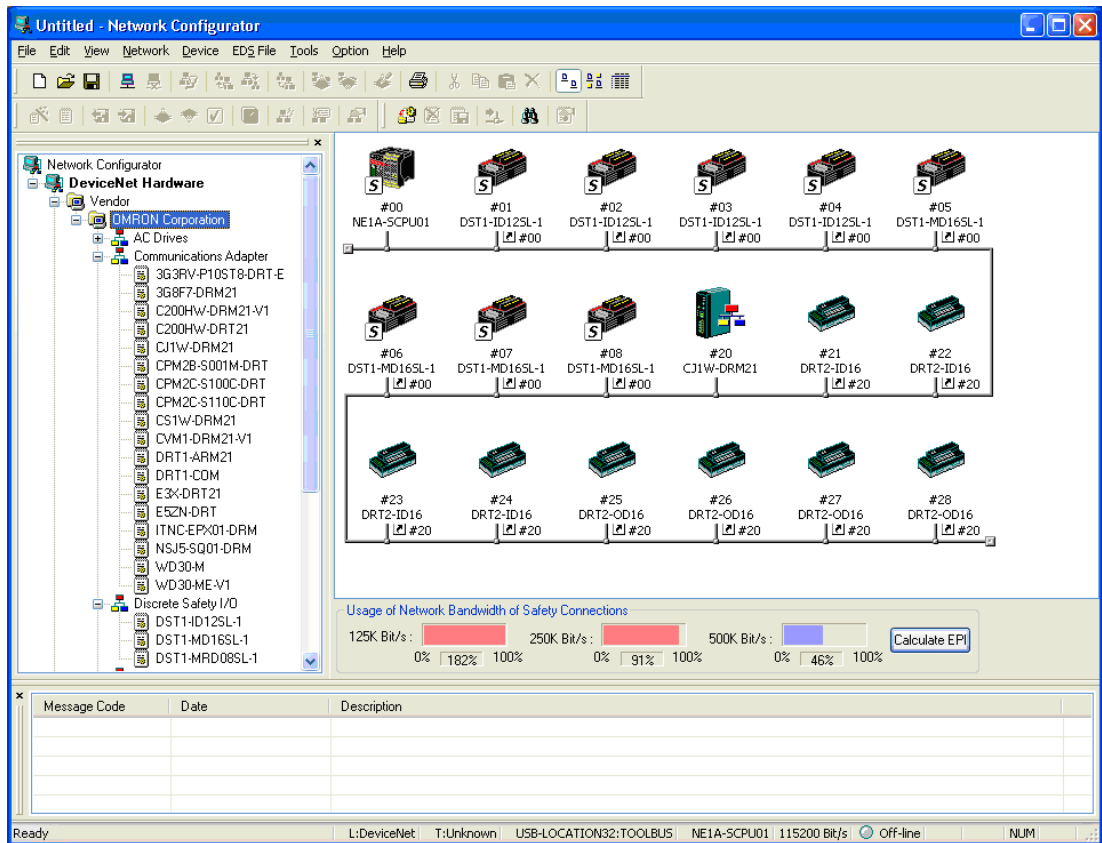
The NE1A-SCPU01 sets safety connections between four DST1-ID12SL-1 Input Terminals and four DST1-MD16SL-1 I/O Terminals. The default set values are used for all the safety connections, and the EPI is 10 ms.

Also, the CJ1W-DRM21 sets the standard connections between four DRT2-ID16 Input Terminals and four 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.
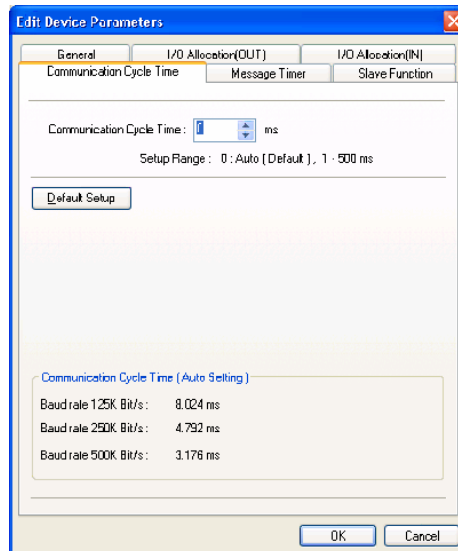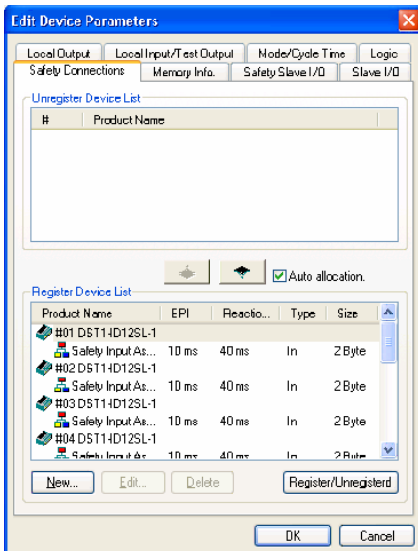
Here, we allocate 70% of the network bandwidth to safety connections and 20% to standard connections.

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.
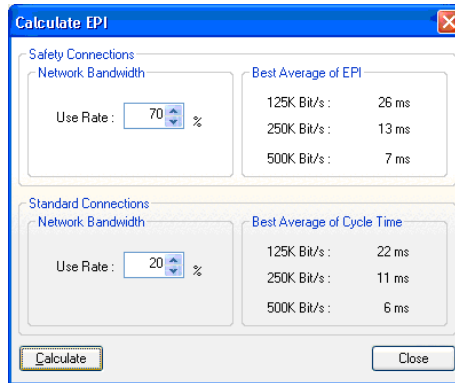
Following the calculation results, set the EPI of all safety connections set in the NE1A-SCPU01 to 7 ms.
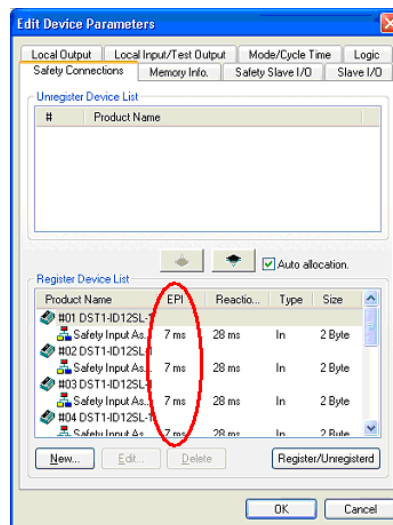
Also, set the communications cycle of the CJ1W-DRM21 to 6 ms.
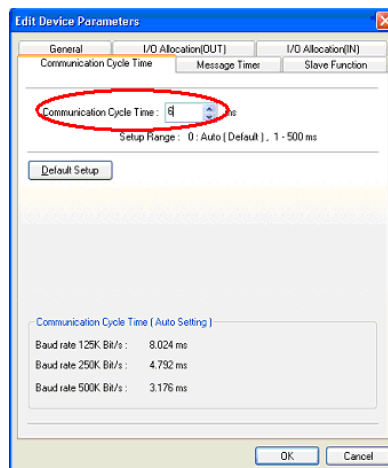
3-3 Calculating and Verifying the Maximum Reaction Time

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

3-3-1 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-SCPU01 Standalone System

Safety sensor/switch	NE1A-SCPU01	Actuator

(2) Remote Input - NE1A-SCPU01 Output

Safety sensor/switch	DST1-series I/O Terminal	Network	NE1A-SCPU01	Actuator

(3) NE1A-SCPU01 Input - Remote Output

Safety sensor/switch	NE1A-SCPU01	Network	DST1-series I/O Terminal	Actuator

(4) Remote Input - Remote Output

Safety sensor/switch	DST1-series I/O Terminal	Network	NE1A-SCPU01	Network	DST1-series I/O Terminal	Actuator

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

3-3-2   Calculating the Maximum Reaction Time

Reaction Time Components

Reaction time components are displayed for each safety chain.

(1) NE1A-SCPU01 Standalone System
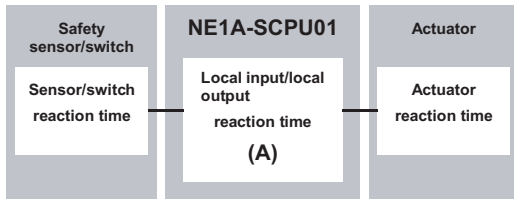
(2) Remote Input - NE1A-SCPU01 Output
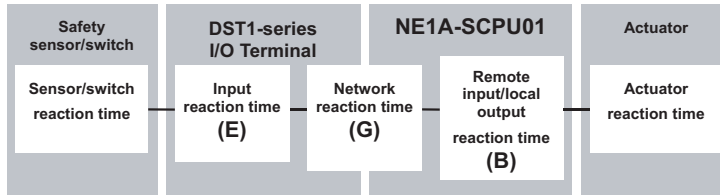
(3) NE1A-SCPU01 Input - Remote Output
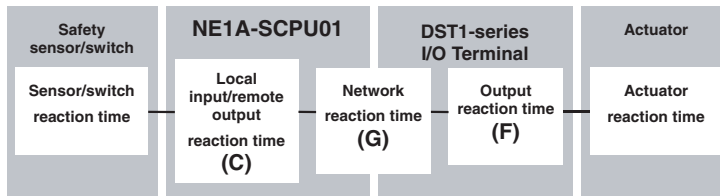
(4) Remote Input - Remote Output
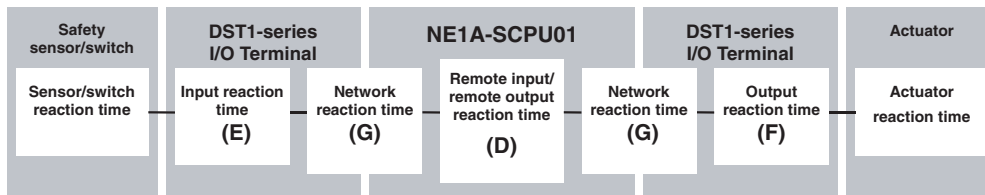
Maximum Reaction Time Formula

	Item	Formula
A	Local input/local output reaction time of the NE1A-SCPU01 (ms)	ON/OFF delay + I/O refresh cycle + NE1A-SCPU01 cycle time x 2 + 2.5
B	Remote input/local output reaction time of the NE1A-SCPU01 (ms)	NE1A-SCPU01 cycle time + 2.5
C	Local input/remote output reaction time of the NE1A-SCPU01 (ms)	ON/OFF delay + I/O refresh cycle + NE1A-SCPU01 cycle time x 2
D	Remote input/remote output reaction time of the NE1A-SCPU01 (ms)	NE1A-SCPU01 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-SCPU01 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-SCPU01 cycle time, I/O refresh cycle time, and network reaction time in the Network Configurator.

Check the NE1A-SCPU01 cycle time and I/O refresh time in Mode/Cycle Time Tab of the Edit NE1A-SCPU01 Parameters Window.
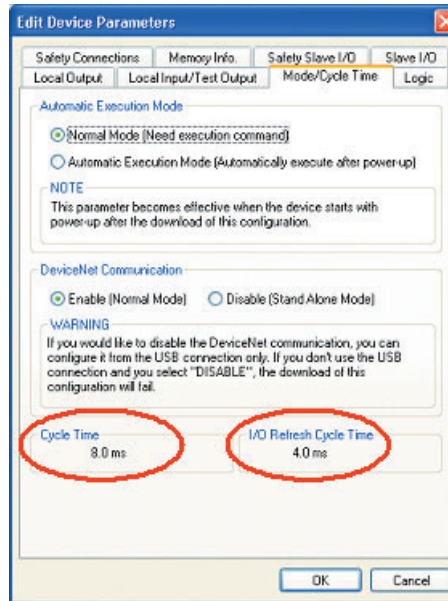
Check the network reaction time in the Safety Connection Tab of the Edit NE1A-SCPU01 Parameters Window.
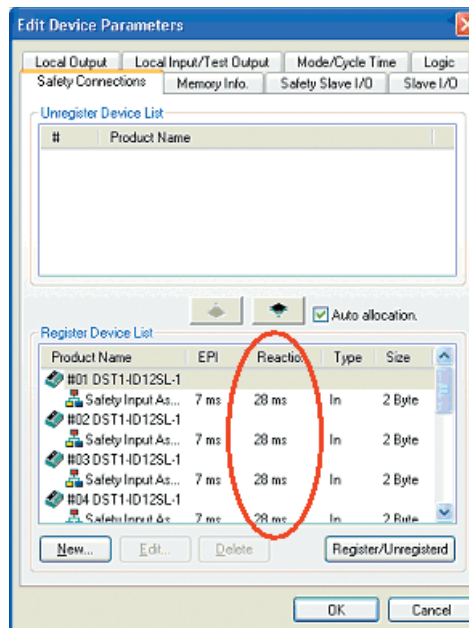
Example of Maximum Reaction Time Calculation
Example 1: Remote Input - NE1A-SCPU01 Output
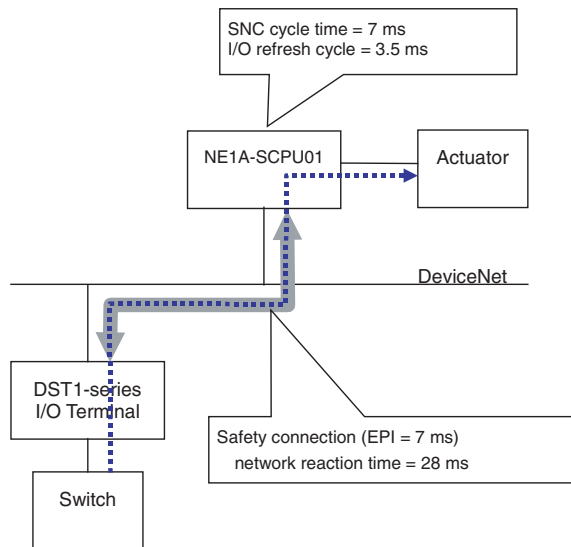
Maximum reaction time (ms)

= Switch reaction time

+ DST1-series I/O Terminal input reaction time

+ Network reaction time

+ NE1A-SCPU01 remote input/local output reaction time

+ Actuator reaction time

= Switch reaction time

+ ON/OFF delay (DST1-series I/O Terminal) + 16.2

+ 28

+ 7 + 2.5

+ Actuator reaction time

= 53.7 + ON/OFF delay + Switch reaction time + Actuator reaction time

Example 2: Local Input - Remote Output

Switch → NE1A-SCPU01 A (SNC cycle time = 7 ms, I/O refresh cycle = 3.5 ms) → NE1A-SCPU01 B (SNC cycle time = 6 ms, I/O refresh cycle = 6 ms) → Actuator

DeviceNet

Safety connection (EPI = 7 ms) network reaction time = 28 ms
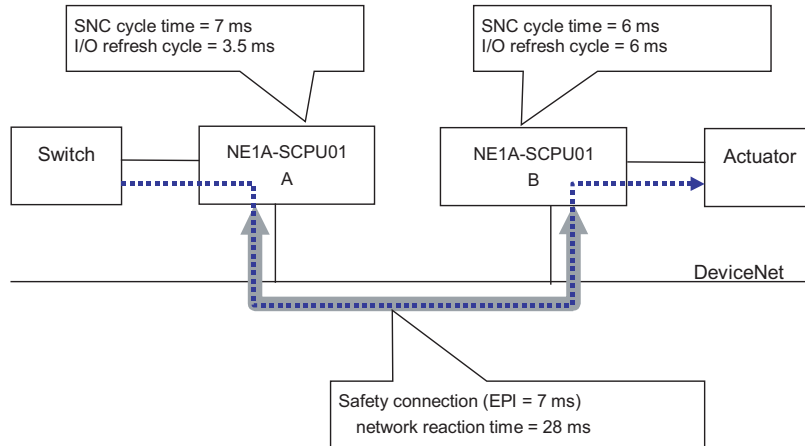
Maximum reaction time (ms)

= Switch reaction time

    + NE1A-SCPU01-A local input/remote output reaction time

    + Network reaction time

    + NE1A-SCPU01-B remote input/local output reaction time

    + Actuator reaction time

= Switch reaction time

    + ON/OFF delay (NE1A-SCPU01) + 3.5 + 7 × 2

    + 28

    + 6 + 2.5

    + Actuator reaction time

= 54.0 + ON/OFF delay + Switch reaction time + Actuator reaction time

3-3-3 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-SCPU01 cycle time is automatically calculated based on the program size, the number of connections, etc. It is also possible to use different NE1A-SCPU01 Controllers for safety chains that require a high-speed reaction time and other safety chains.

Section 4: Editing Safety I/O Terminal Parameters

4-1   Editing Parameters

4-1-1   Parameter Groups

Parameters for DST1-series Safety I/O Terminals are grouped into general parameters; parameters for each safety input, each test output, and each safety output; and operation time parameters. Parameter groups can be switched using the Parameter Group Box. There are many DST1-series parameters, so switching the parameter groups to display them separately makes it easier to set the parameters.
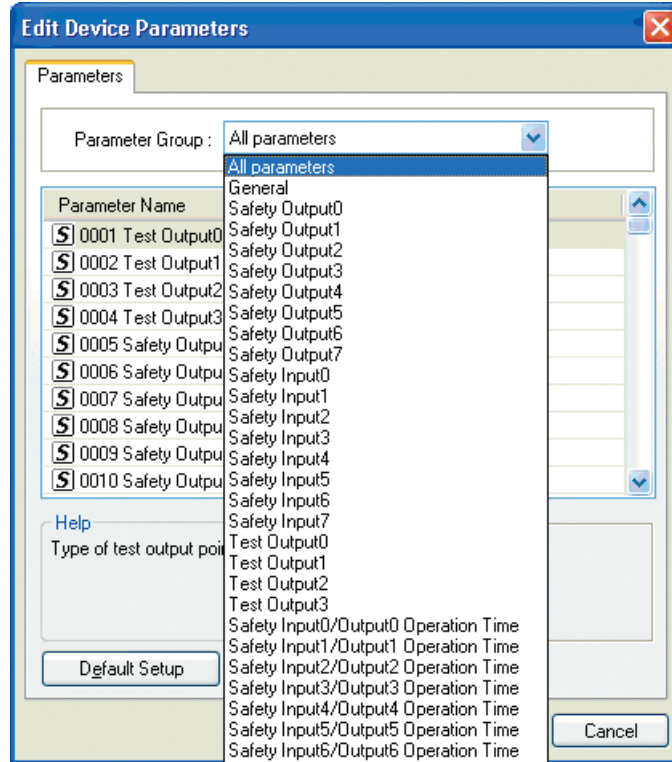
The parameters with an $\boxed{S}$ icon on the left are relevant to safety applications.

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	This parameter is common to all test outputs for which the Test Output Channel Mode is set to Standard Output.	Clear off
		Keep output data	It sets the output state of the test output when idle data is received.	
	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

Item	Settings	Description	Default
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 Pulse Test Output. 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 Test Pulse from Test Out, the test output is selected for use in combination with the safety input. Set the channel mode of the test output selected here to Pulse Test Output.	Not used.
		Test Output 0		
		Test Output 1		
		Test Output 2		
		Test Output 3		

	Item	Settings	Description	Default
S	Dual Channel Safety Input Mode	Single Channel	Specifies using Single Channel Mode. If Single Channel 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
	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	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

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.
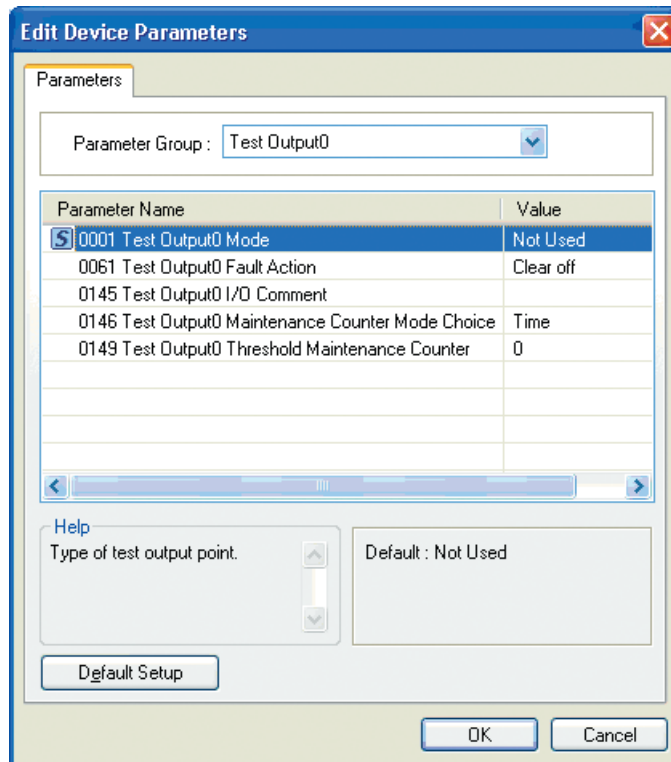
	Item	Settings	Description	Default
S	Test Output Mode	Not used.	The corresponding test output is not used.	Not used.
		Standard Output	Specifies connecting to the input for a muting lamp or PLC. Used as a monitor output.	
		Pulse Test Output	Specifies connecting a device with a contact output in combination 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 Standard Output or Muting Lamp Output.	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.
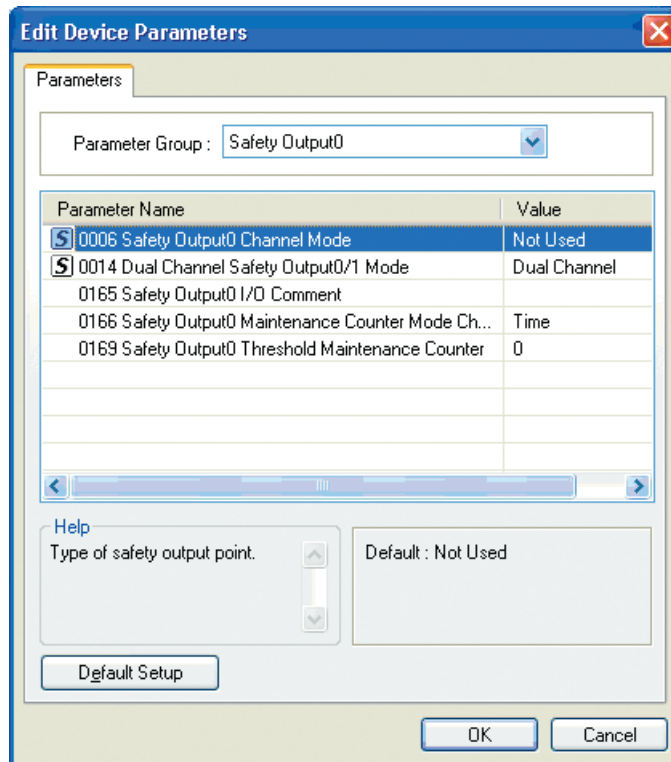
	Item	Settings	Description	Default
S	Safety Output Channel Mode	Not used.	The safety output is not used. (External output device not connected.)	Not used.
		Safety	Specifies not outputting the test pulse when the output is ON. Contact between the output signal line and the power supply (positive) when 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 Single Channel 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

Open the Edit Parameter Window of the NE1A-SCPU01 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-SCPU01 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.
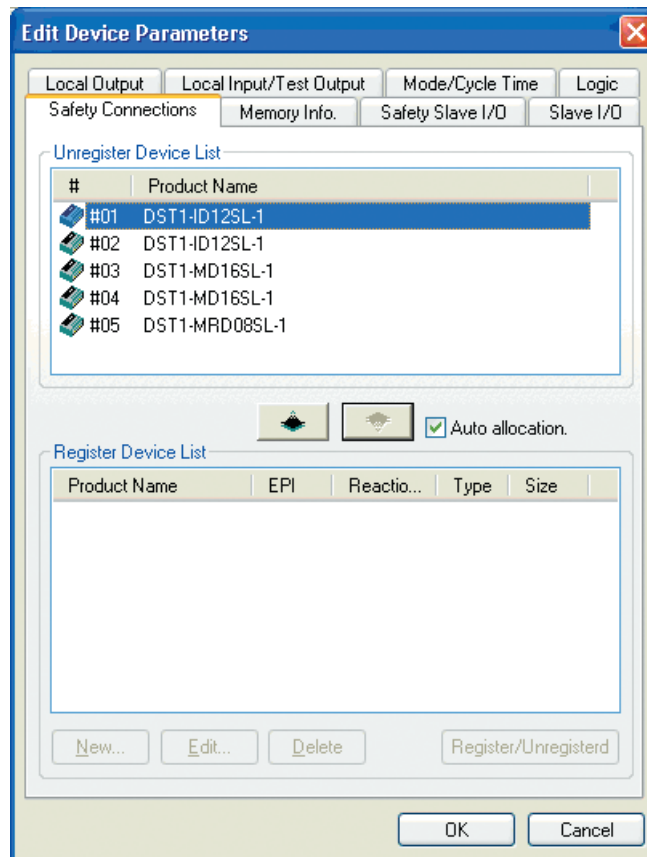
2. Select a Safety Slave to register in the Unregister Device List and click the ⬥ Button.
3. The Safety Slave selected in step 2 will be registered.

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.
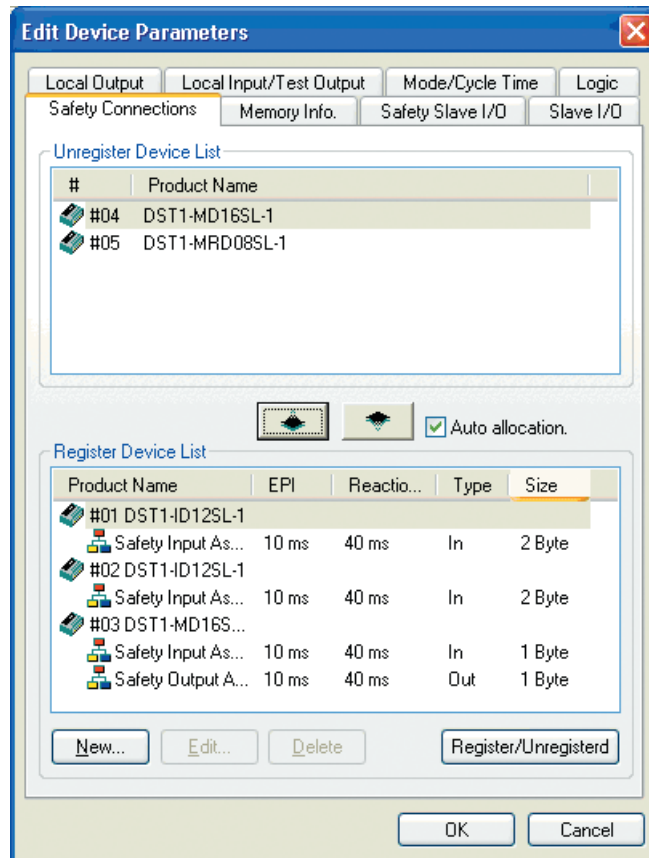
The following information is displayed in the Register Device List.

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 *5-1-2 Setting Safety Connection Parameters* (page 82).
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* (page 82) 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* (page 82) 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-SCPU01.

(2) Selecting a slave device and specifying the destination as the NE1A-SCPU01 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.
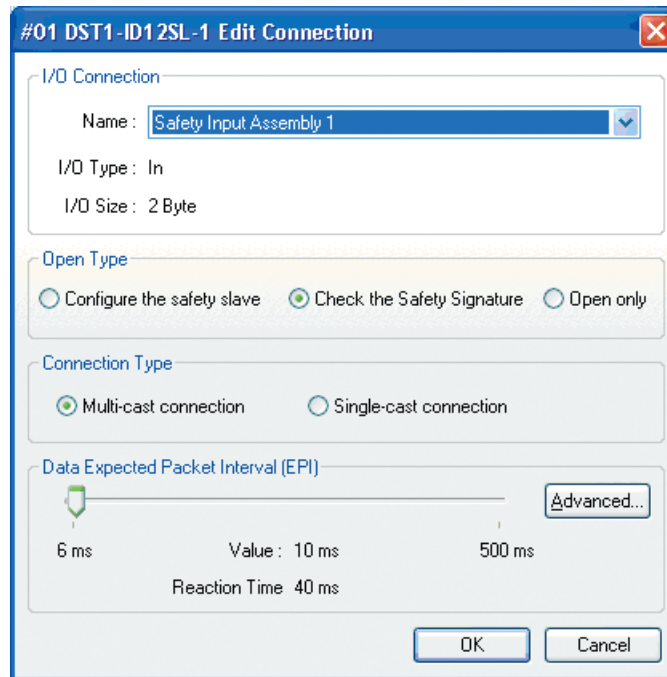
I/O Connection

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-SCPU01 is used, the I/O assembly must be set in the Safety Slave I/O Window. Refer to *5-2 Safety Slave Settings* (page 84).

Open Type

Select the type of open processing to be performed when the NE1A-SCPU01 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-SCPU01 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-SCPU01 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-SCPU01, 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. Only this open type can be selected when the slave is the NE1A-SCPU01.

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-SCPU01 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.

Connection Type

Select the connection type to use between the NE1A-SCPU01 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-SCPU01 Controllers via a multi-cast connection.
	These NE1A-SCPU01 Controllers are classified as the same multi-cast group when multiple NE1A-SCPU01 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-SCPU01.
Single-cast connection	This connection type can be selected for an input connection or output connection. The NE1A-SCPU01 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 Slave communicates the safety data with the NE1A-SCPU01. The minimum set value is the greater of the destination Safety Slave cycle time and NE1A-SCPU01 cycle time.

The cycle time of the DST1-series Safety I/O Terminals is always 6 ms. Check the cycle time of the NE1A-SCPU01 in the Mode/Cycle Time Window when all the parameter settings and programming have been performed.

The time set here affects the network bandwidth and the network reaction time. For information on the network bandwidth, refer to *3-2 Verifying the Network Bandwidth* (page 59) and for information on the network reaction time, refer to *3-3 Calculating and Verifying the Maximum Reaction Time* (page 63).

Advanced

The **Advanced** Button enables changing more detailed communications parameters. These parameters affect system operation; do not change them under normal conditions.

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-SCPU01 as a Safety Slave. The I/O assembly set here is displayed and can be selected in the Connection Setting Window of the NE1A-SCPU01 that is functioning as a Safety Master.

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

Note: When the NE1A-SCPU01 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-SCPU01 functions as a Safety Slave.
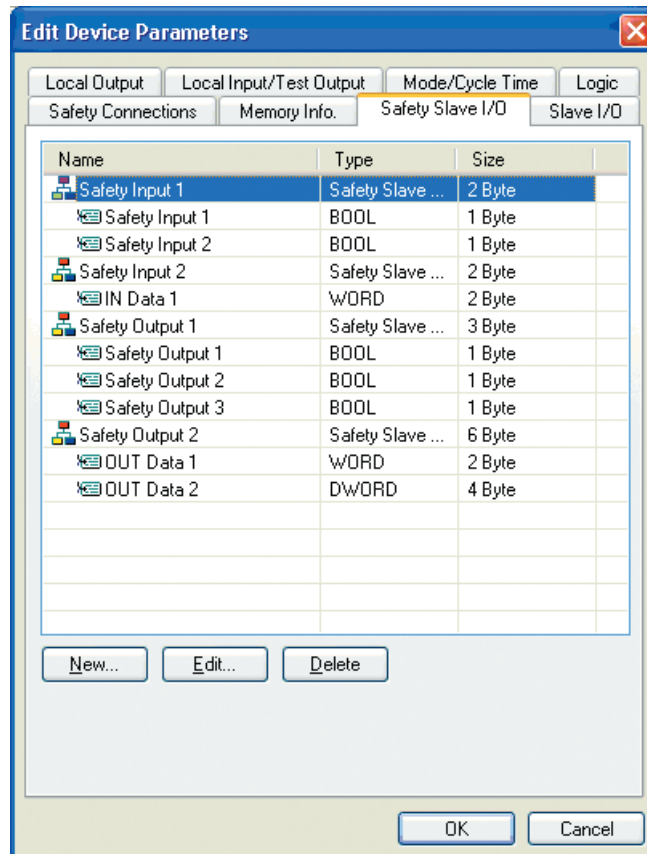
The following information is displayed in this window.

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* (page 85).
- 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* (page 85).
- 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.
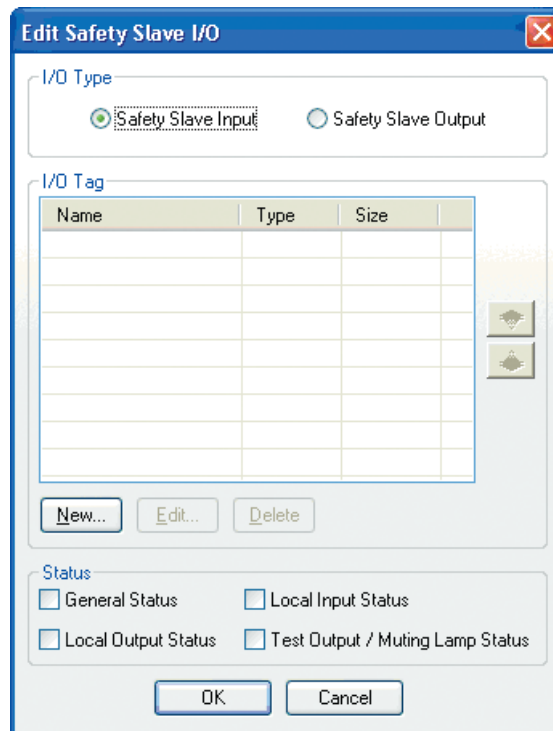
I/O Type

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

Safety Slave Input: NE1A-SCPU01 (Safety Slave) →Safety Master

Safety Slave Output: Safety Master →NE1A-SCPU01 (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.
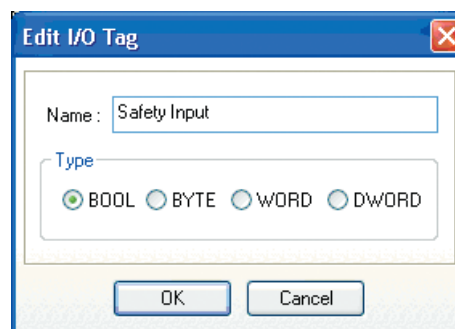
- To change an I/O tag that has already been defined, select the I/O tag you want to change and click the **Edit I/O Tag** Button.
- To delete an I/O tag that has already been defined, select the I/O tag you want to delete and click the **Delete** Button.

Status

When the I/O type is *Target Input*, the NE1A-SCPU01 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

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

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-SCPU01 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-SCPU01 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-SCPU01 functions as a Standard Slave.
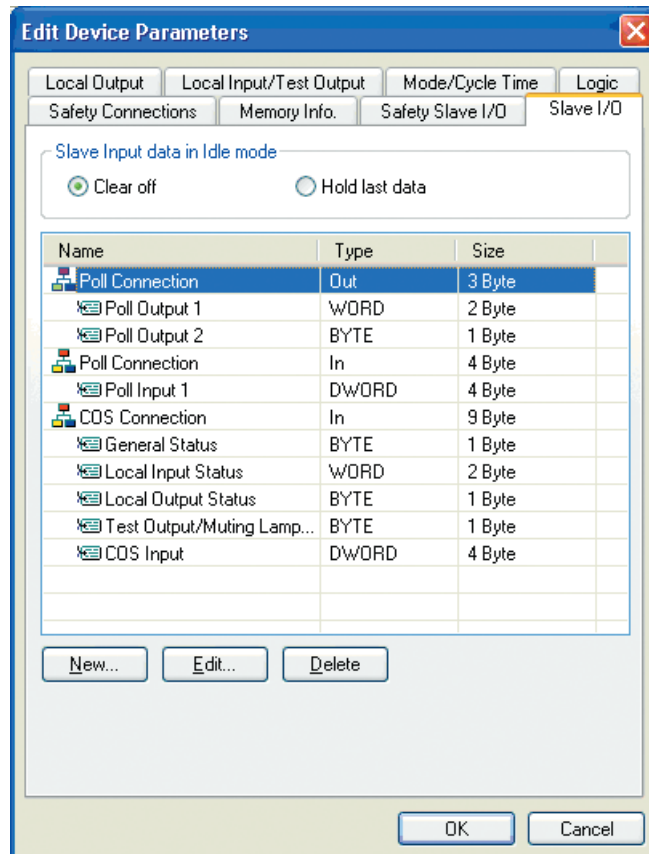
The following information is displayed in this window.

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* (page 88) 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* (page 88) 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-SCPU01 transmits to the Standard Master in either of the following conditions:

- When changing the NE1A-SCPU01 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.
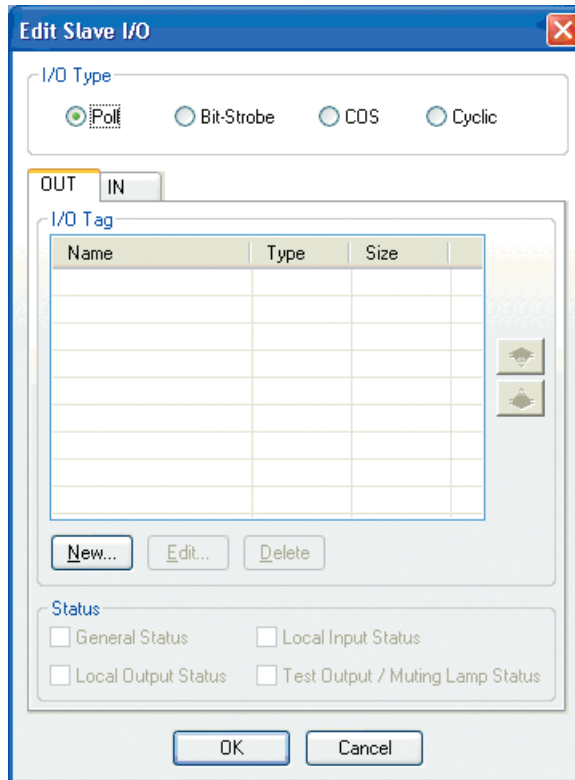
I/O Type

Select the connection type to use for the I/O assembly. Input assemblies and output assemblies can be registered for each connection. Output assembles 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.
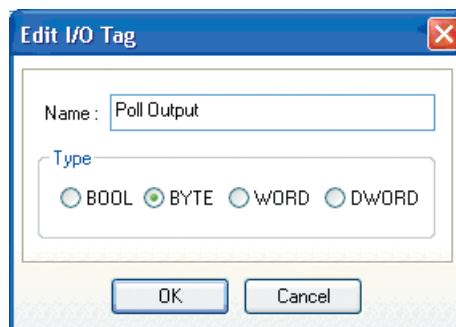
- To change an I/O tag that has already been defined, select the I/O tag you want to change and click the **Edit I/O Tag** Button.
- To delete an I/O tag that has already been defined, select the I/O tag you want to delete and click the **Delete** Button.

Status

When the I/O type is *Input*, the NE1A-SCPU01 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

5-4　Local I/O Settings

Click the **Local OUT** Tab or **Local IN/Test Output** Tab to display the NE1A-SCPU01'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-SCPU01, 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.
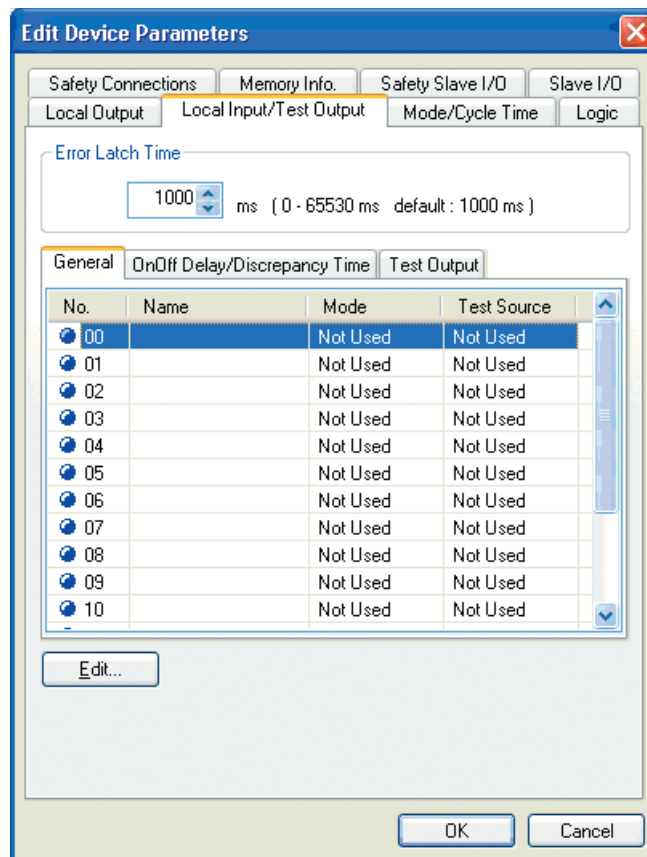
Note: There are many settings for safety inputs. The display window is thus separated into the **General** Tab Page and **On-Off Delay/Discrepancy Time** Tab Page. Safety input scan are set from both tab pages.

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 *Test Source* and then set the test output mode to *Pulse Test Output*.
	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-SCPU01 cycle time. Check the displayed NE1A-SCPU01 cycle time and determine the set value.

IMPORTANT: • The optimum value for the NE1A-SCPU01 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 Parameter Window is closed.

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 *Single Channel* 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.
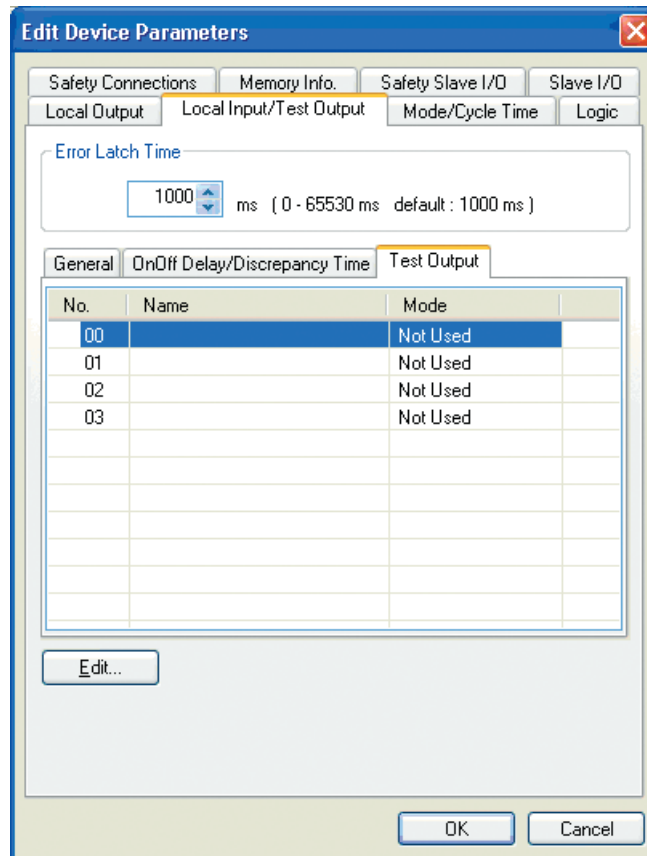
Error Latch Time

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* (page 90).

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.
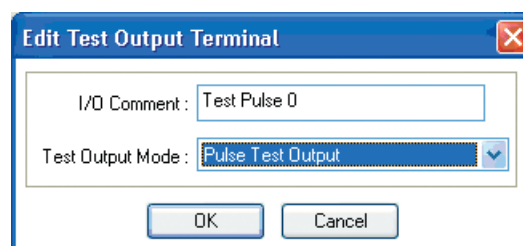
Terminal Name

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.
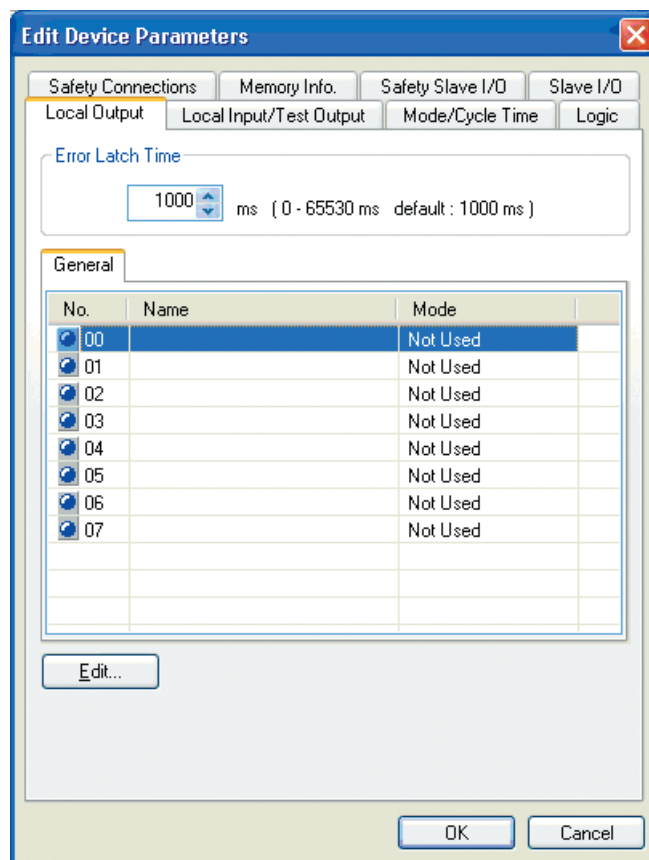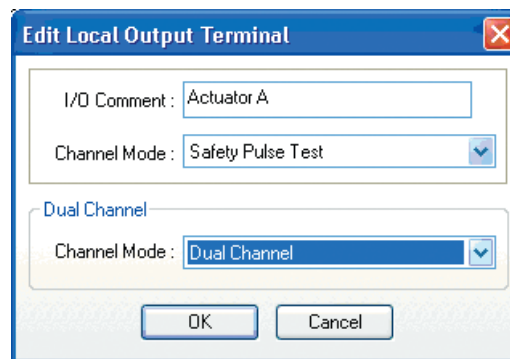
Error Latch Time

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 Single Channel 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 Operation Modes and Confirming the Cycle Time

Click the **Mode/Cycle Time** Tab to display the NE1A-SCPU01 operation mode settings and the cycle time.
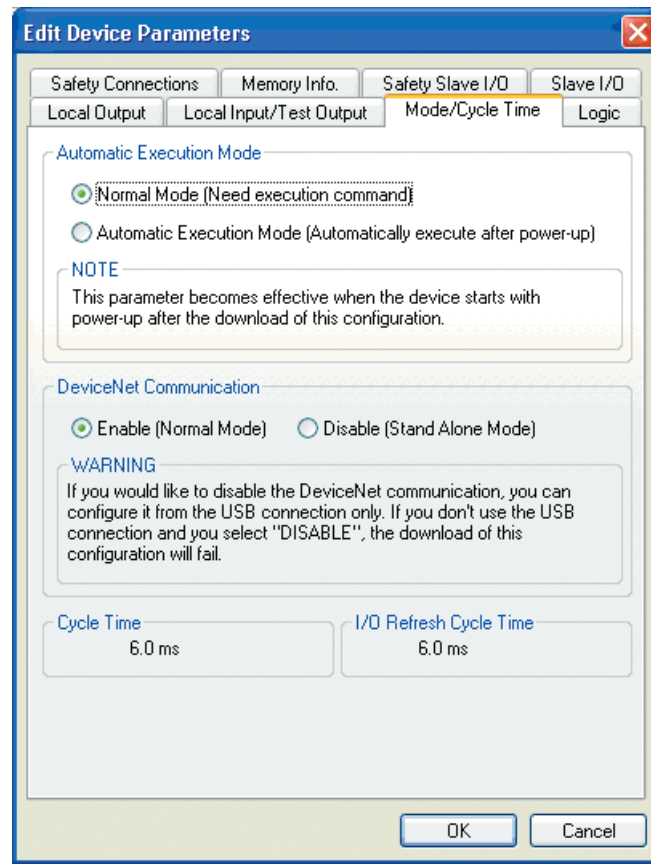
5-5-1 Setting the NE1A-SCPU01 Operation Modes

Automatic Execution Mode

Set the NE1A-SCPU01 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:
	• 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-SCPU01 is used in Standalone Mode, DeviceNet communications can be disabled. If DeviceNet communications are disabled, the cycle time of the NE1A-SCPU01 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-SCPU01USB 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-SCPU01 will stopped.

5-5-2 Confirming the Cycle Time

Cycle Time

The NE1A-SCPU01 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.

Section 6: Programming the Safety Network Controller

6-1 Starting and Exiting the Logic Editor

6-1-1 Starting the Logic Editor

Use the Logic Editor to program the NE1A-SCPU01.

Use the following procedure to start the Logic Editor.

1. Click the **Logic** Tab in the Edit Device Parameters Window of the NE1A-SCPU01.
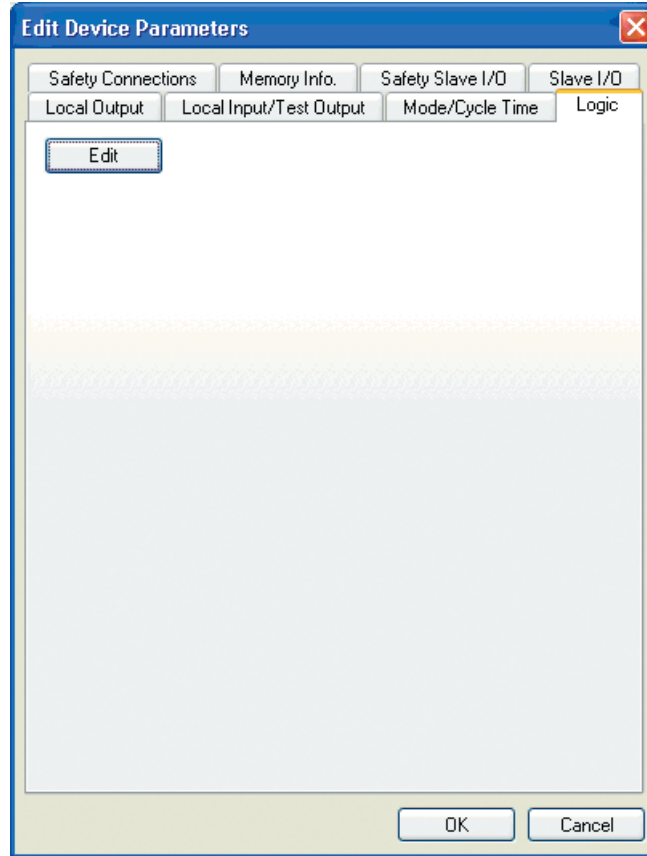
2. Click the **Edit** Button.

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.

Object List

Workspace
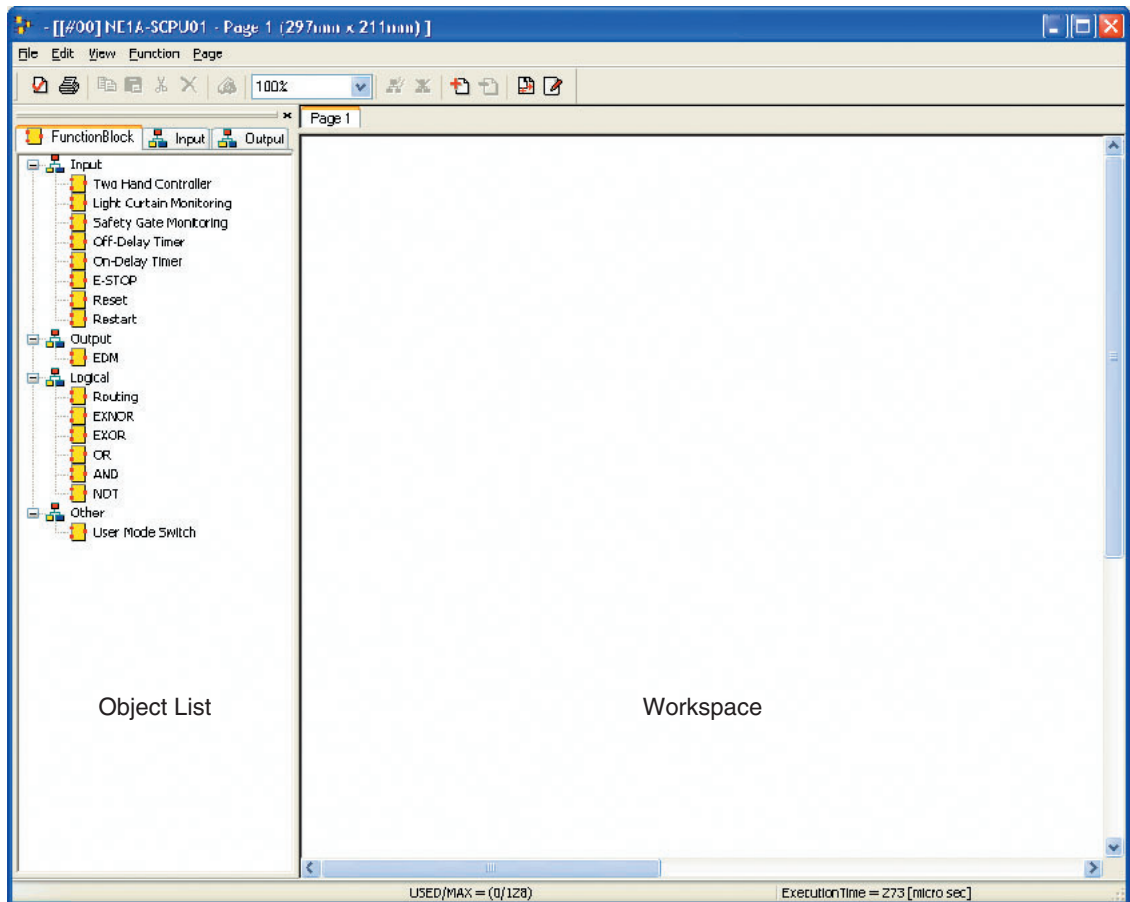
6-1-2   Exiting the Logic Editor

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-SCPU01. The connection between I/O tags, however, is 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	Copies the function block on the clipboard to the Workspace.	OK	OK
Delete	Deletes the selected item.	OK	OK
Properties	Displays the property window of the selected function block.	OK	OK

6-2-3 View Menu

Command	Description	Online	Offline
Object List	Display or hides the Object List.	OK	OK
Status Bar	Display or hides the status bar.	OK	OK
Tool Bar	Displays or hides the toolbar.	OK	OK

6-2-4 Function Menu

Command		Description	Online	Offline
User EM		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	New	Creates a new jump address (jump source).	OK	OK
	Select	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
Delete Last Page	Deletes the last page.	OK	OK
Change Page Title	Changes the title of the selected page.	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.
- Only function blocks can be copied. The I/O tags, I/O tag connections, and connections between function blocks cannot be copied.
- 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.
- A maximum of 128 number jump addresses can be used.
- A maximum of 32 of pages can be used.

6-3-2 Programming Using Function Blocks

Input Tag Placement

1. Click the **Input** Tab in the Object List.
2. Select the input tag to use, drag it to the Workspace, and drop it where you want to position it. The user can select multiple I/O tags and position them at the same time.
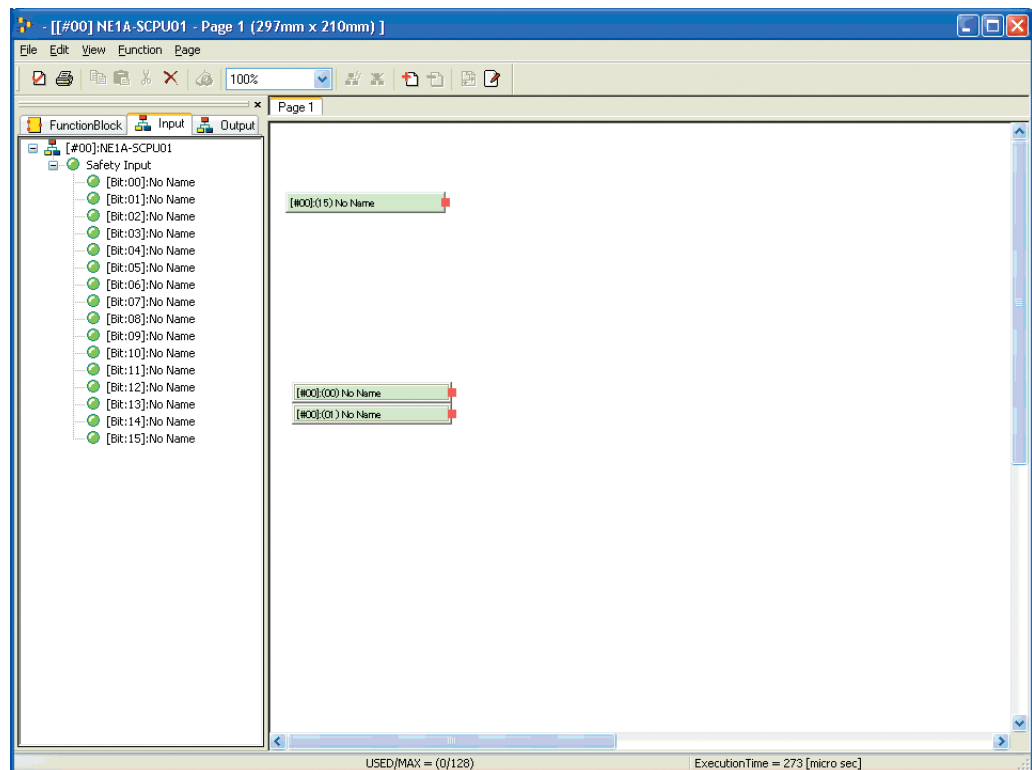
Function Block Placement

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.
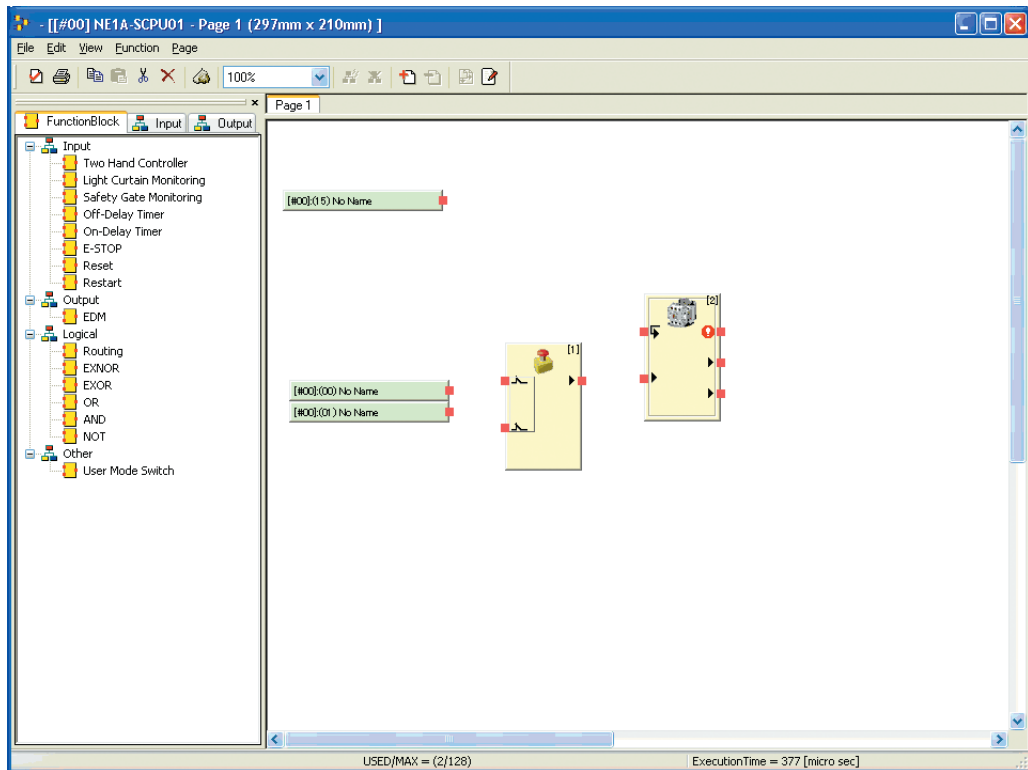
Output Tag Placement

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.
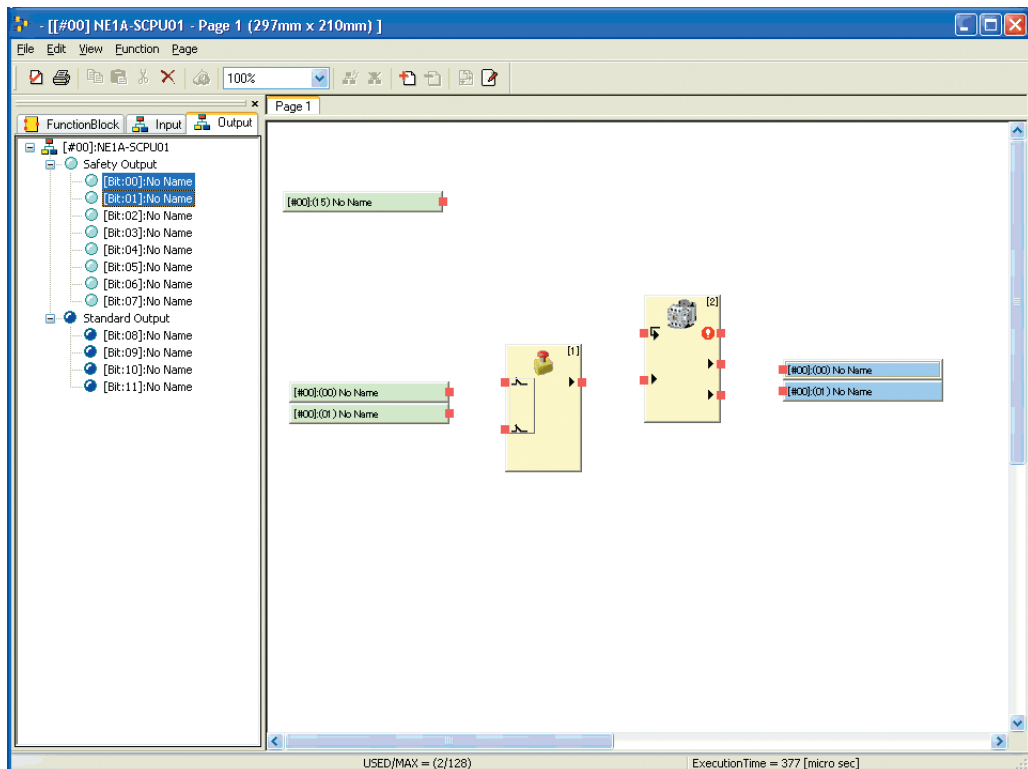
Connections

Connect the I/O tags and the function block.

1. Click the source connector (■) and drag it to the destination connector.
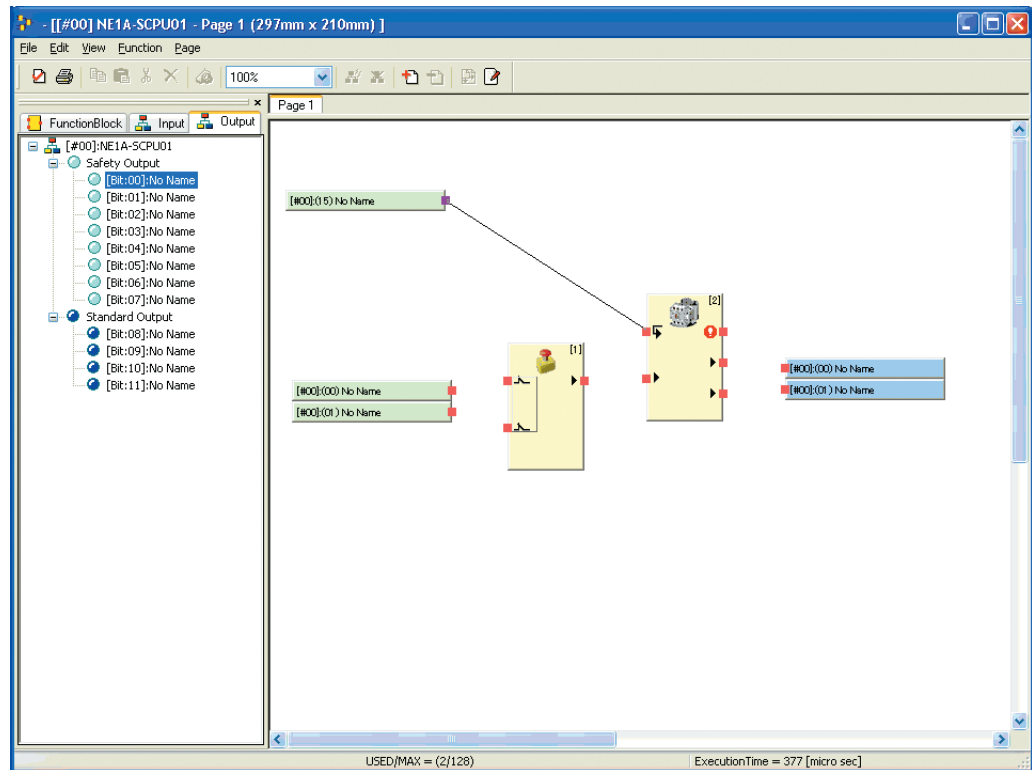
2. Repeat this operation to create the program.

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

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 last page will be deleted.

(1) Select **Page - Delete Last Page** from the menu bar.

(2) Click the **Delete Last Page** Button on the toolbar.

Page Title

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

(1) Select **Page - Change Page Title** from the menu bar.

(2) Right-click the page tab in the Workspace 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 the Workspace and select **Jump Address**.
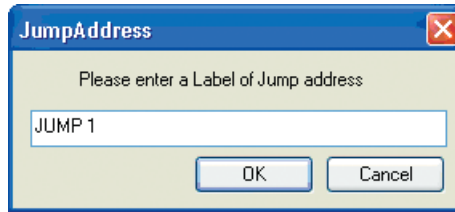
2. Enter a name for the jump address and click the **OK** Button.

   The jump address will be displayed as follows:
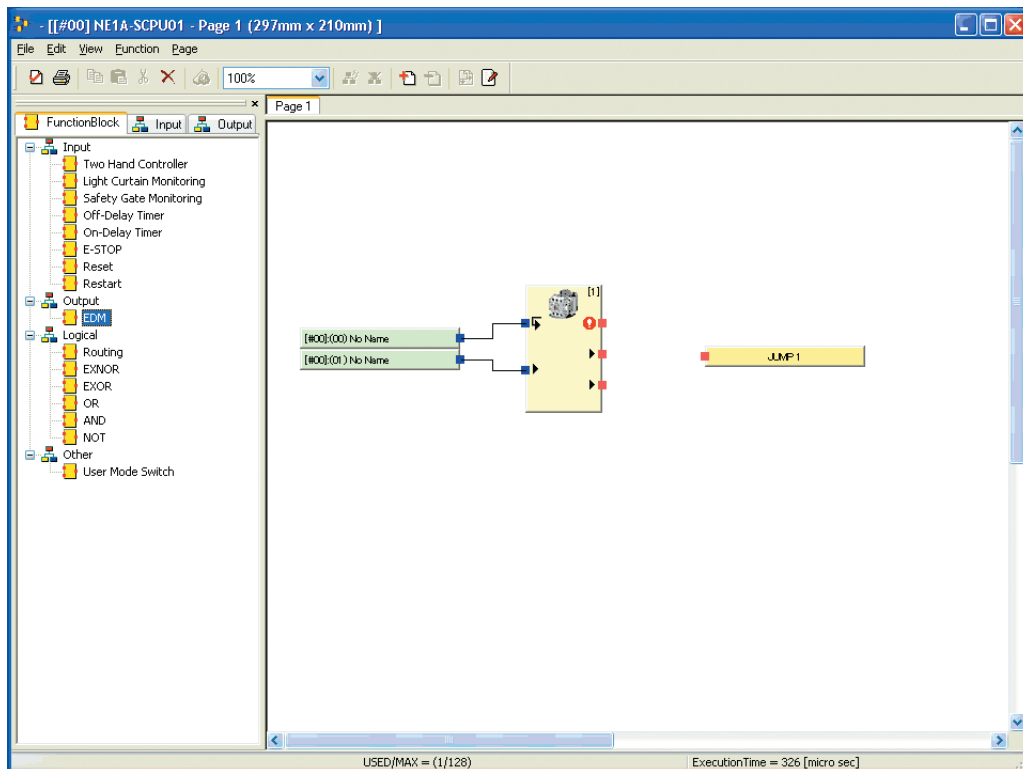
3. Enter the jump destination using either of the following methods:
   (1) Select **Menu - Jump Address - Select** from the menu bar.
   (2) Right-click in the Workspace and select **Select Jump Address**.
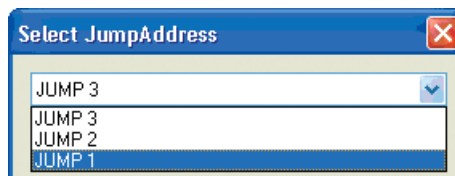
4. Select the name of the jump source and click the **OK** Button.

The jump address will be displayed as follows:
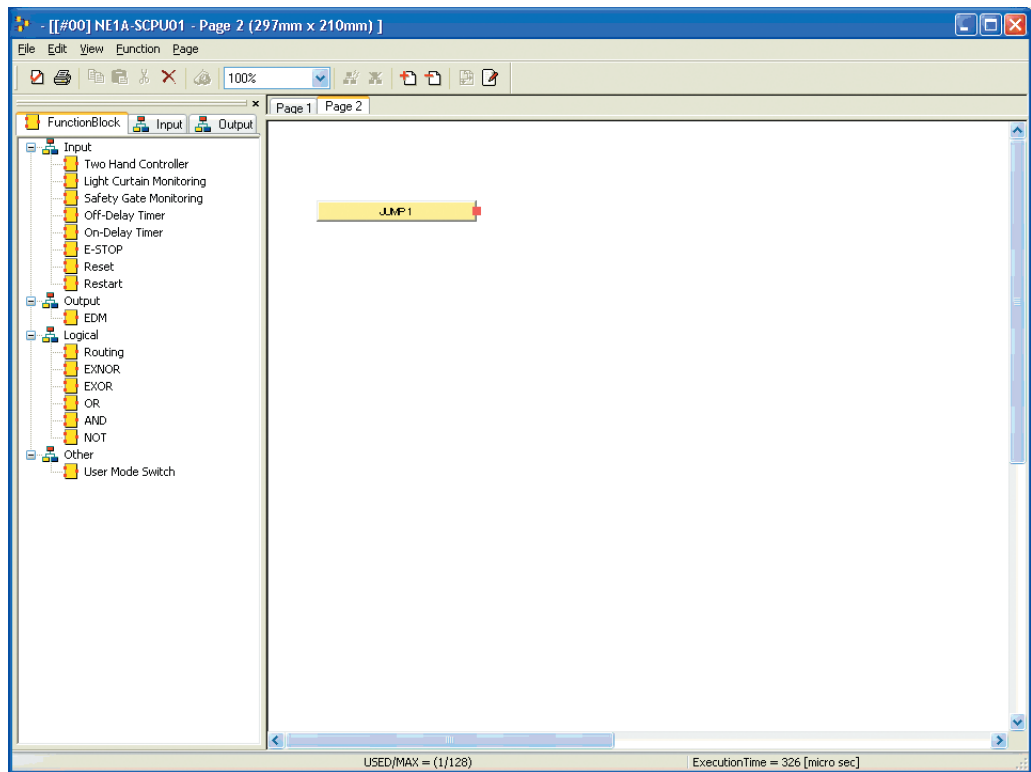
Function Block I/O Information

The I/O information of a function block can be confirmed using the following method:

- Right-click the function block and select **Detail**.
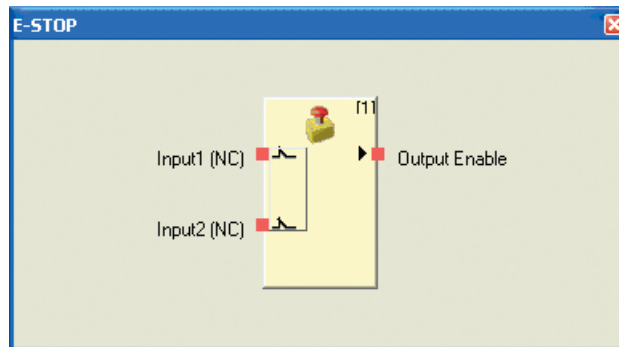
Editing Function Block Parameters
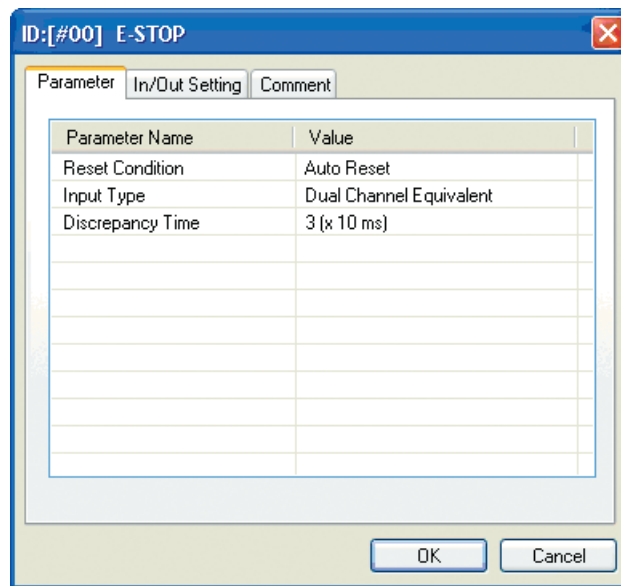
To edit the parameters of a function block, use any of the following methods to display the Parameter Edit Window.

(1) Select the function block and then select **Edit - Properties** from the menu bar

(2) Right-click the function block and the select **Edit** from the pop-up menu.

(3) 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* (Cat. No. Z906-E1).

Parameters

Click the **Parameter** Tab to set the parameters of the function block.
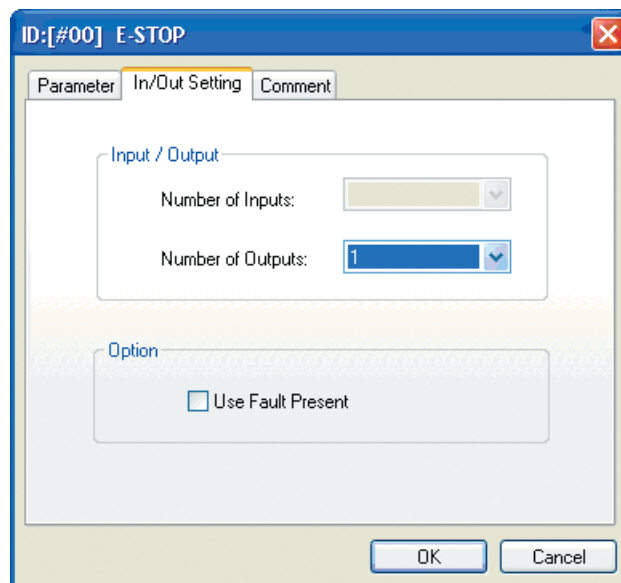
Input/Output Settings

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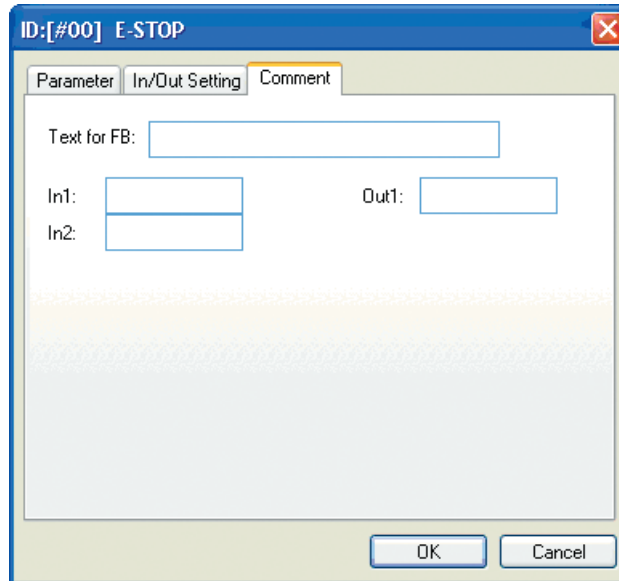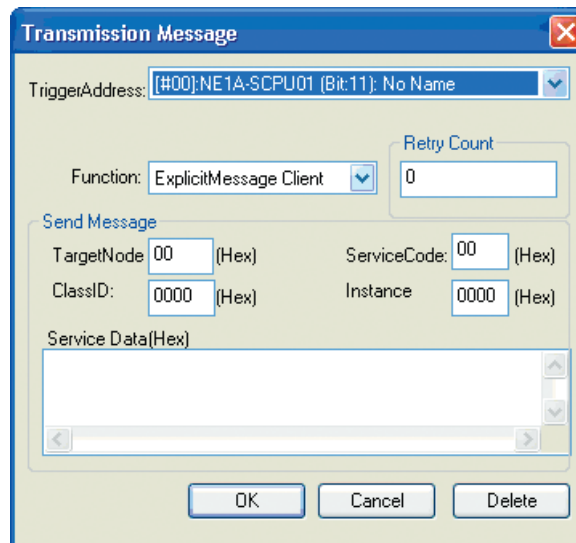
Comment

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. All the names entered in this window, however, are printed when the program is printed.

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.

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.

6-3-3 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.
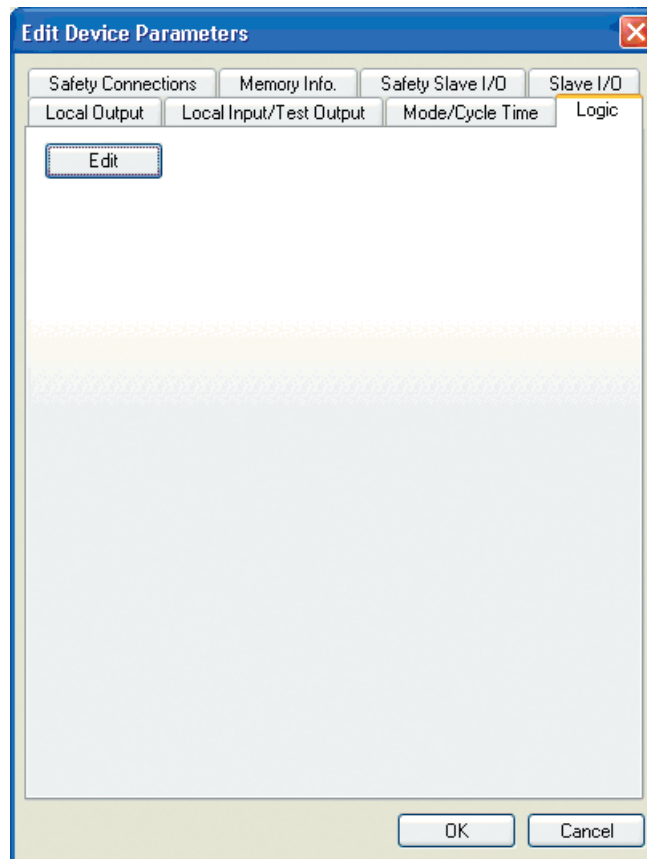
3. To save the file, select *File* and *Save* or *Save As* in the Main Window of the Network Configurator.

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 selecting *File - Apply* will also be deleted.

6-3-4 Updating the Program

If the I/O tags of the Safety Slaves that configure the NE1A-SCPU01 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-SCPU01 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.

6-3-5 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-SCPU01 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 color.

I/O tags and connections that are ON can be monitored.
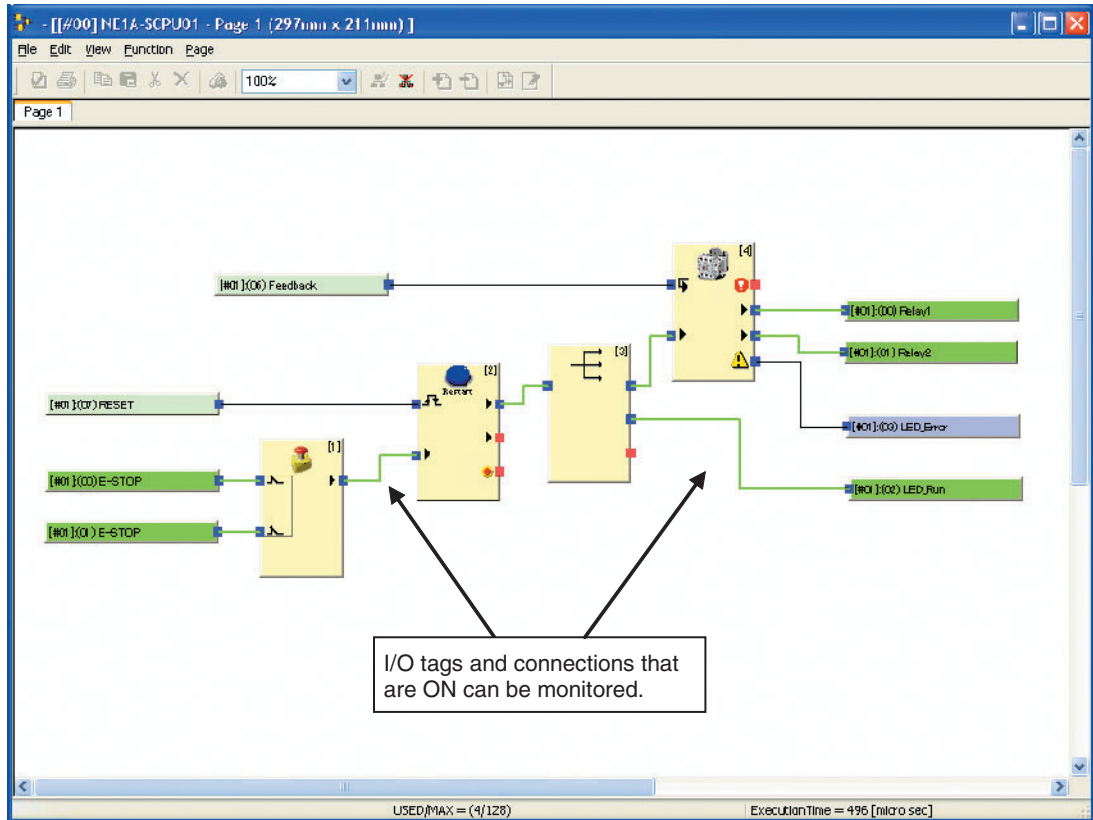
Stopping Online Monitoring

Use either of the following methods to stop online monitoring:

(1) Select Function - Monitoring from the menu bar once again.

(2) Click the Stop Monitoring Button on the toolbar.

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 a NE1A-SCPU01 DST1-series Safety I/O Terminal 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.
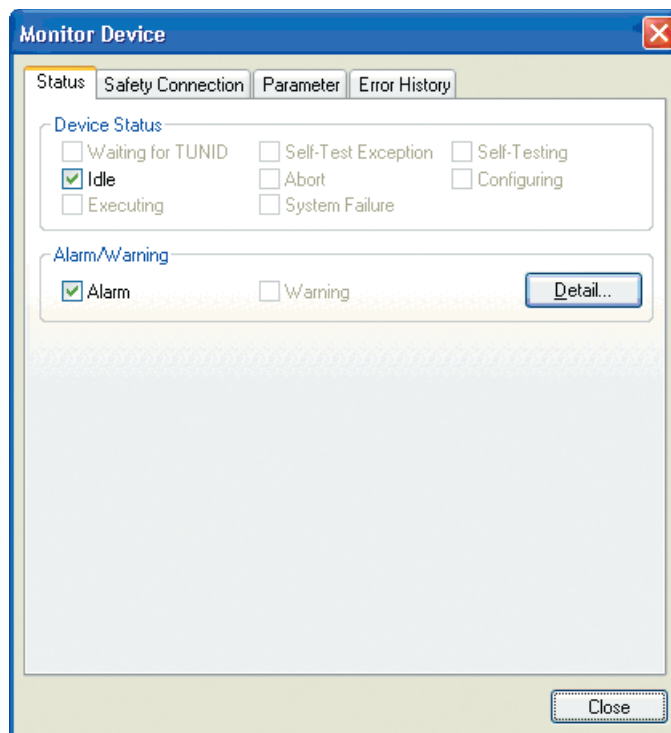
Device Status

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.
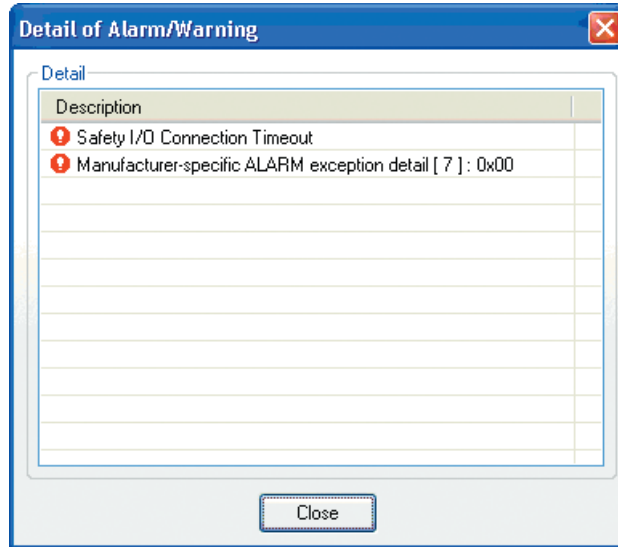
7-1-2   Monitoring Safety Connections

Description

The safety connection status of the NE1A-SCPU01 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-SCPU01 and select *Device - Monitor* from the menu bar. Click the **Safety Connection** Tab in the displayed window.

(2) Select the NE1A-SCPU01 and click the **Monitor Device** Button on the toolbar. Click the **Safety Connection** Tab in the displayed window.

(3) Right-click the NE1A-SCPU01 and select *Monitor* from the pop-up menu. Click the **Safety Connection** Tab in the displayed window.
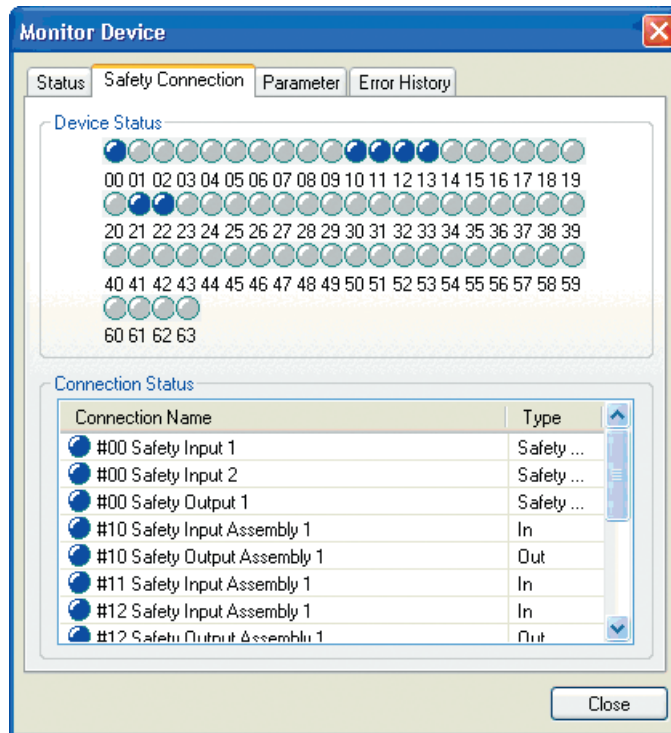
The connection status of the Safety Slave is displayed for the local node address. For the other node addresses, the statuses of the safety connections configured for the device parameters are displayed.

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-SCPU01 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.
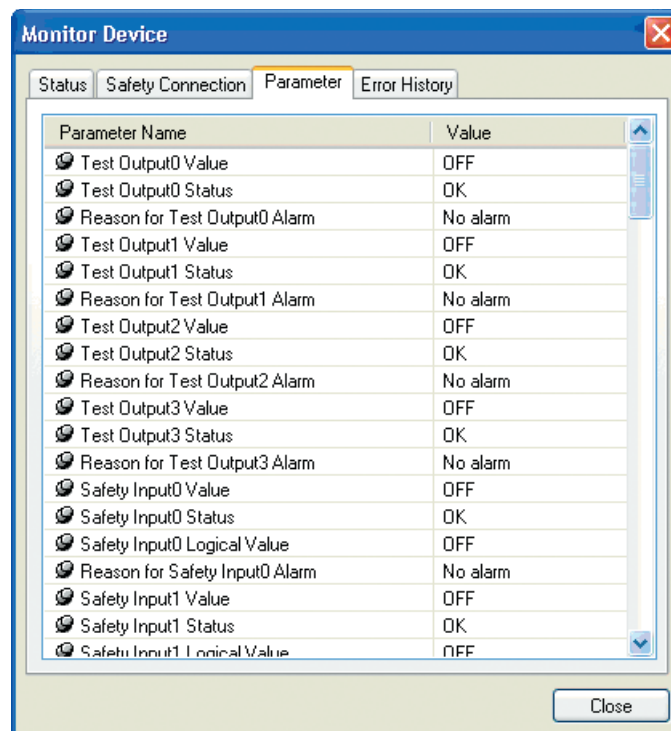
Test Output Terminal Status

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-SCPU01 or DST1-series Safety I/O Terminal can be monitored using the Network Configurator.

Twenty error history records can be saved internally in a NE1A-SCPU01 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.
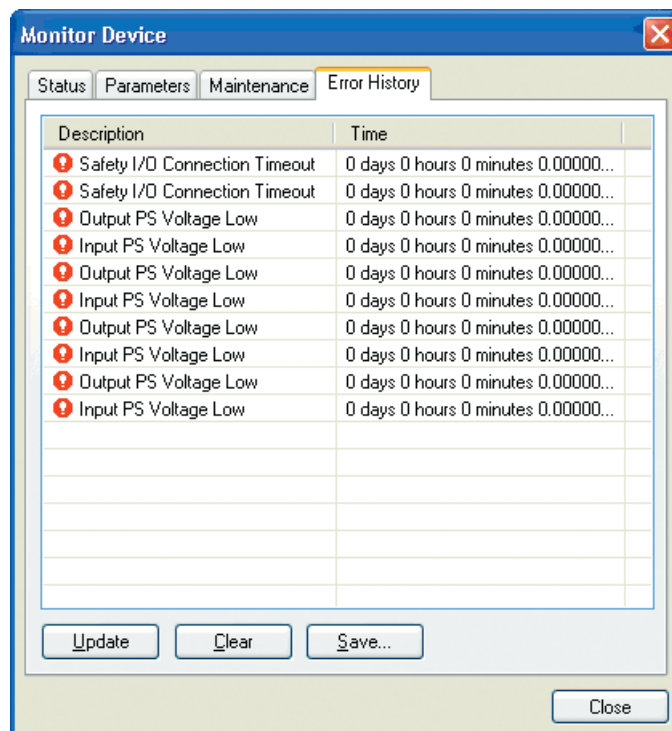
Error History Display Items

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-SCPU01 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
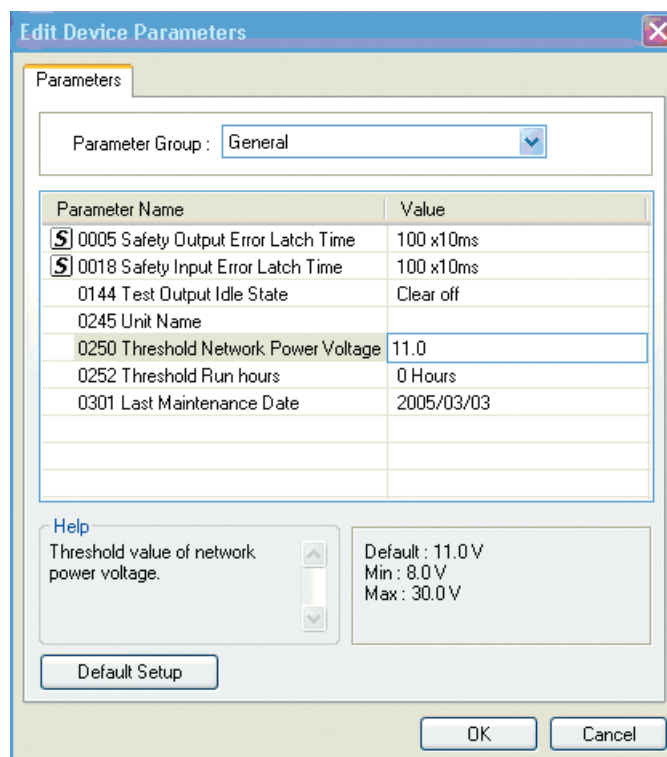
Description

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
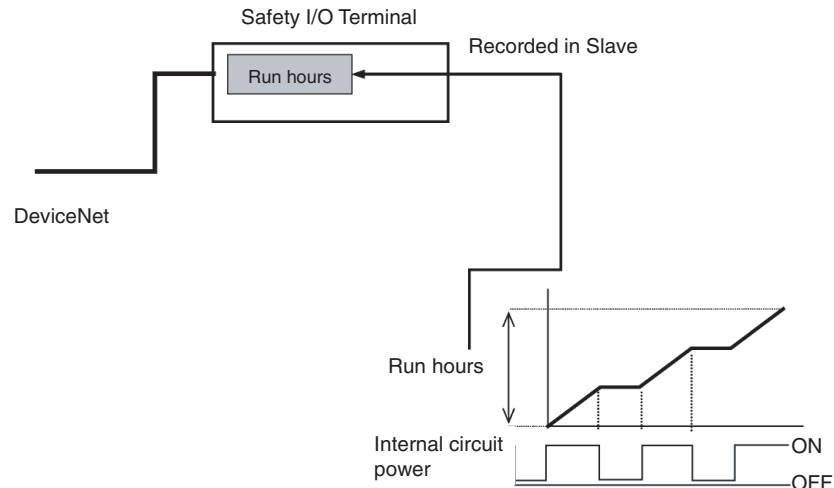
The user can monitor this information using the Network Configurator and explicit messages.

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.
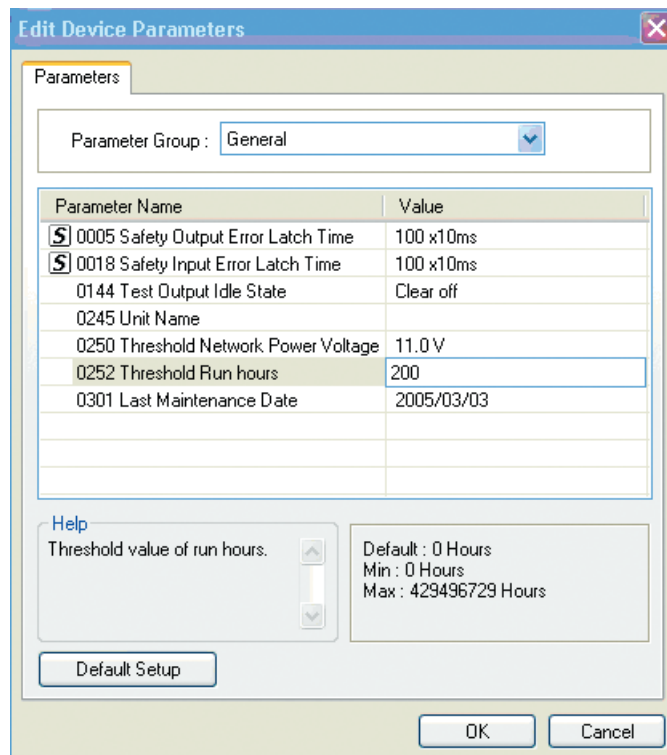
If the threshold value is set to 0, the threshold value will not be checked.

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.

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.
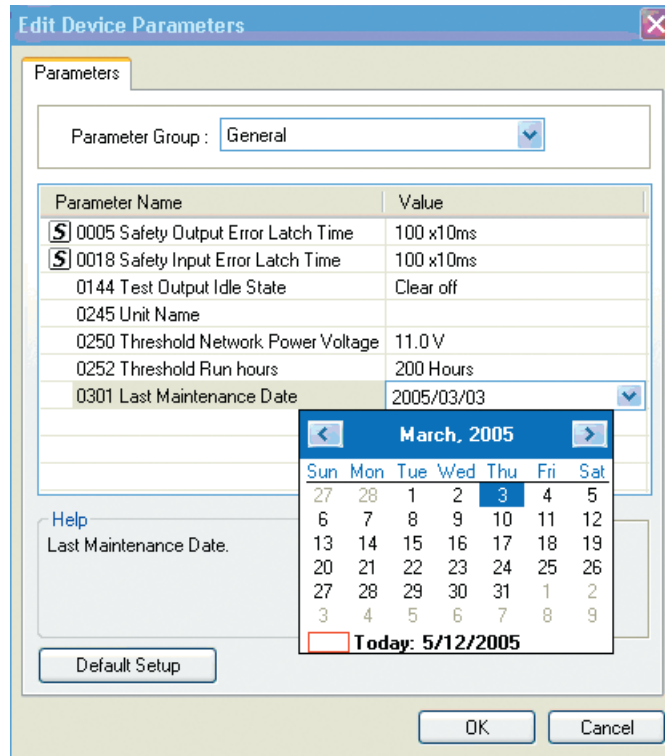
Monitoring Using the Network Configurator

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.
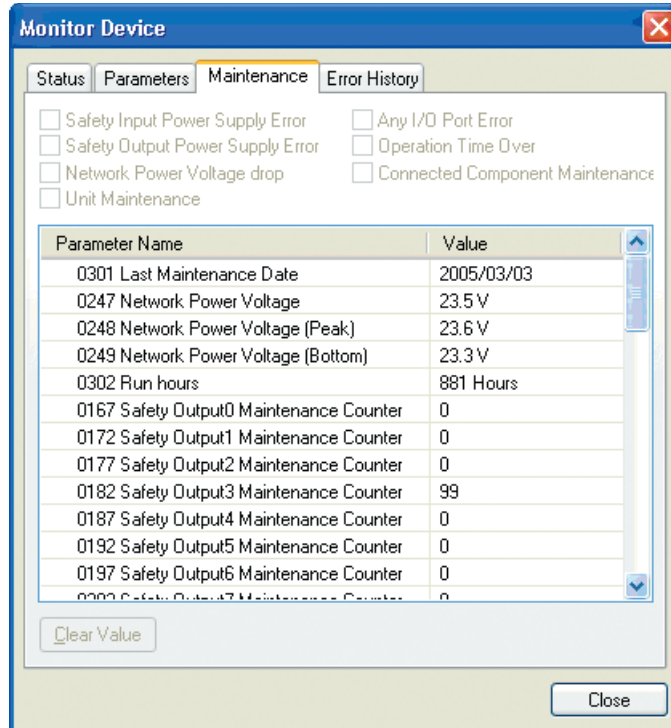
7-2-4　Monitoring the Contact Operation Counters

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
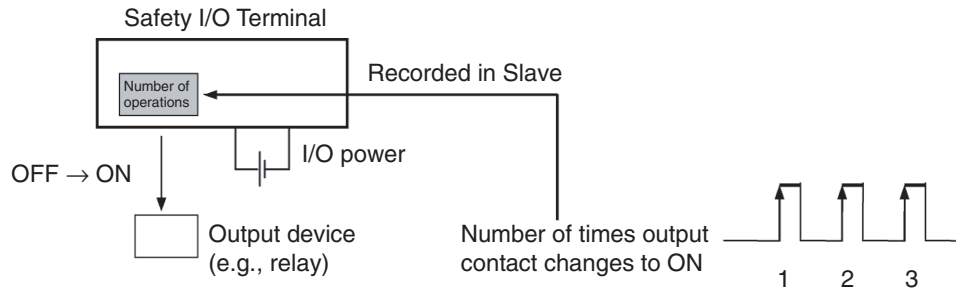
The user can monitor this information using the Network Configurator and explicit messages.

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.
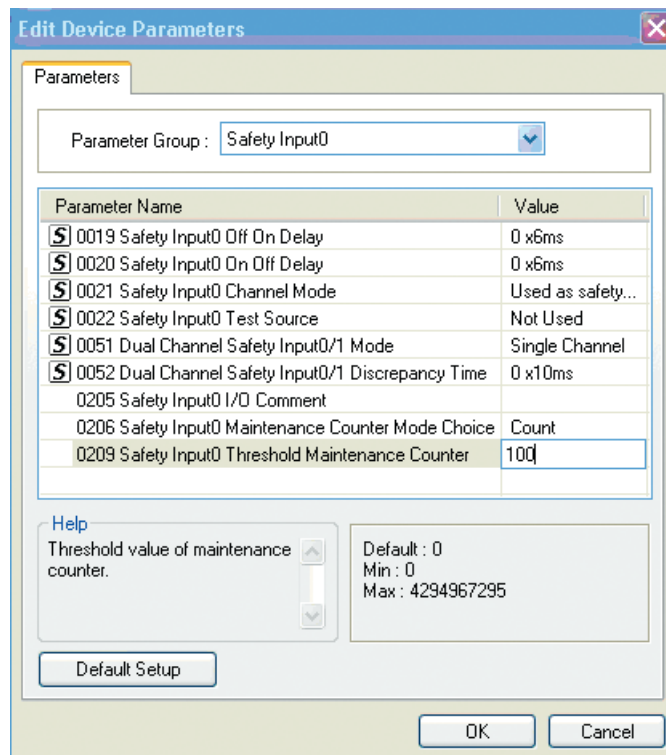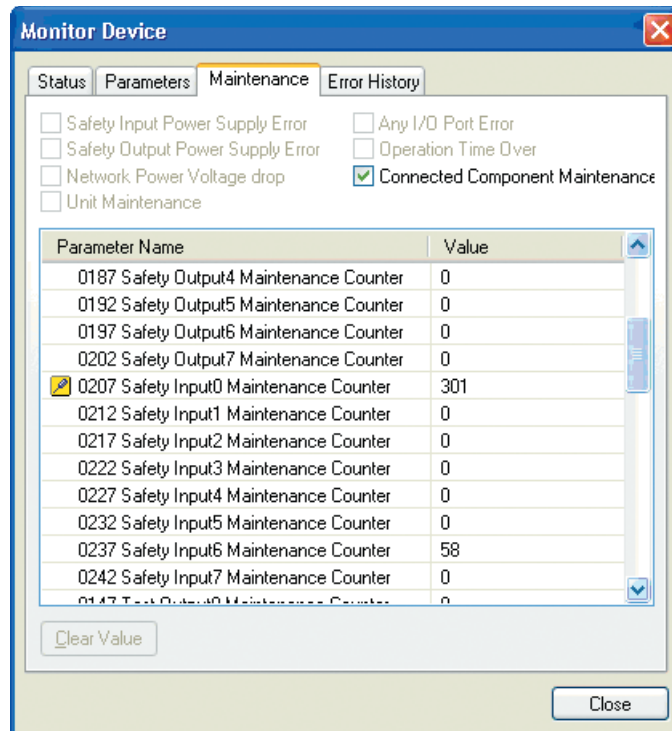

When the Threshold Maintenance Counter is set to 0, the threshold value will not be checked.

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.
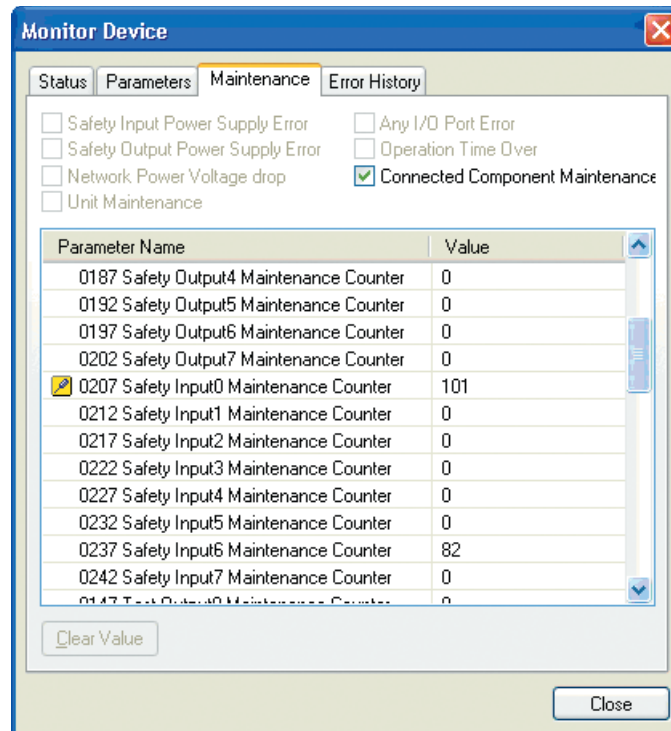
Each counter can be cleared. Select the counter to clear and click the **Clear Value** Button.

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
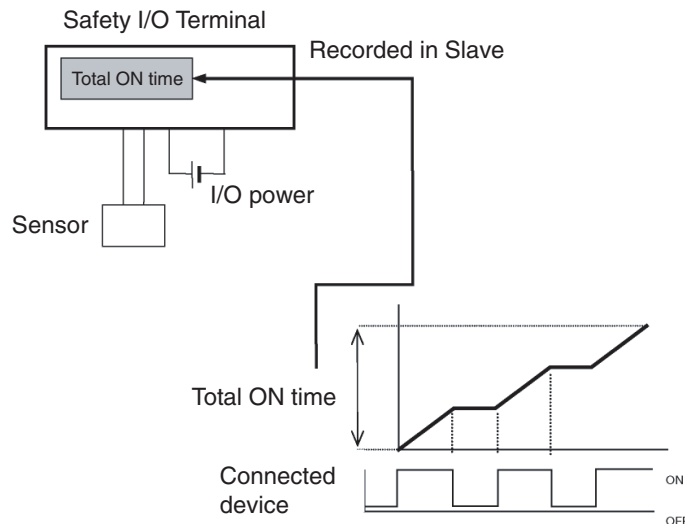
The user can monitor this information using the Network Configurator and explicit messages.

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.
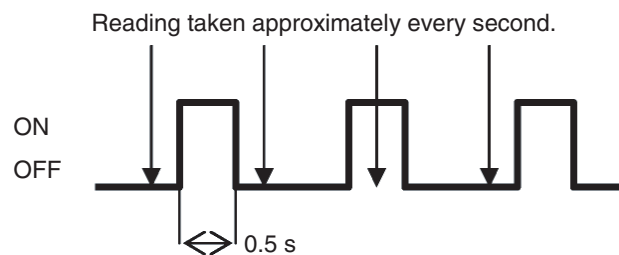
Figure A

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.
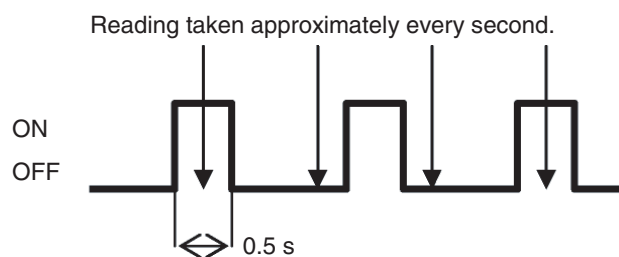
Figure B

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.
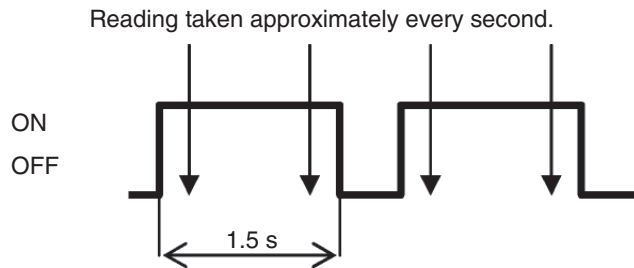
Figure C

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.
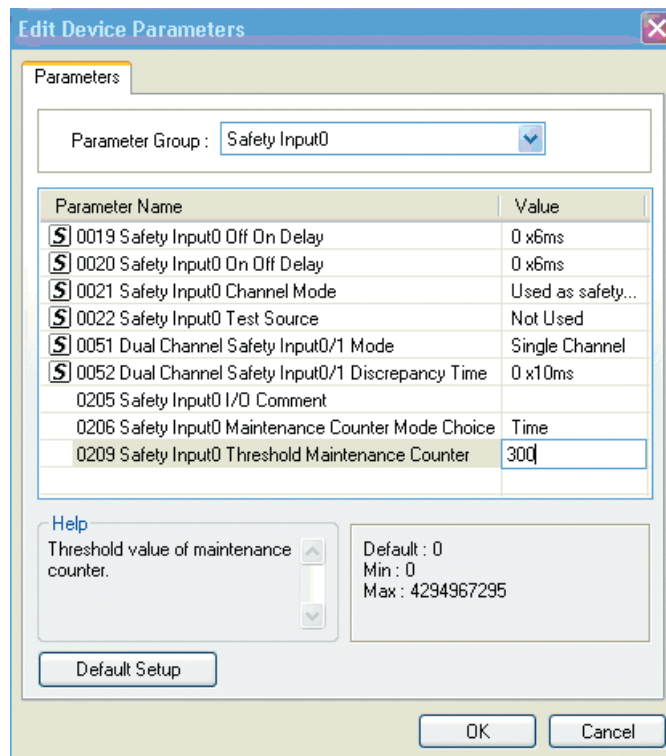
If the Threshold Maintenance Counter is set to 0, the threshold value will not be checked.

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.

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
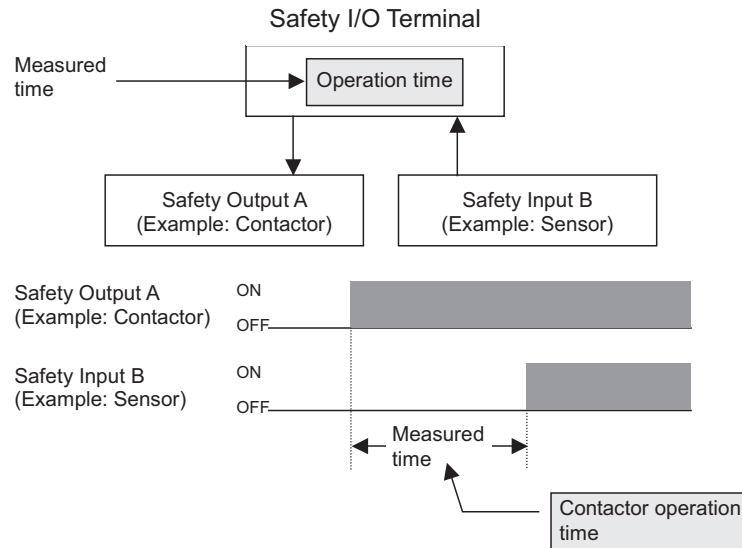
The input reaction time and the output reaction time of the DST1-series Safety I/O Terminal are added to monitor the operation time.

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.
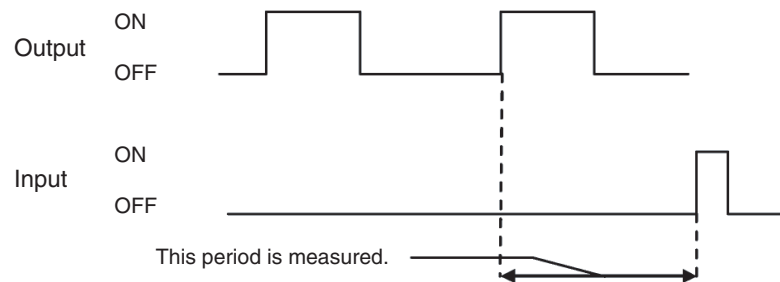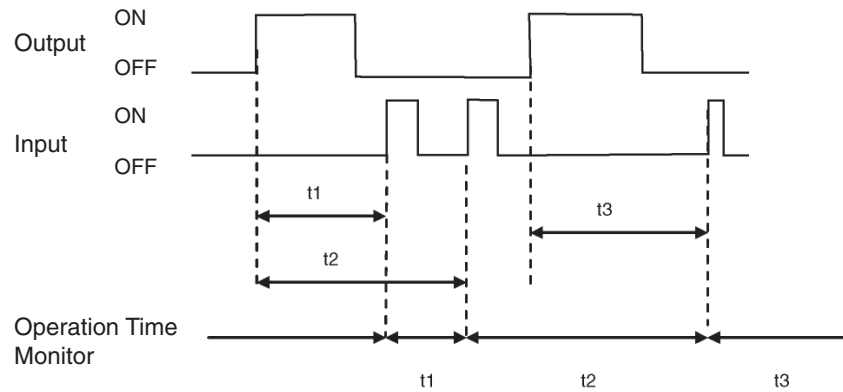
Setting the Threshold Response Time Using the Network Configurator

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.
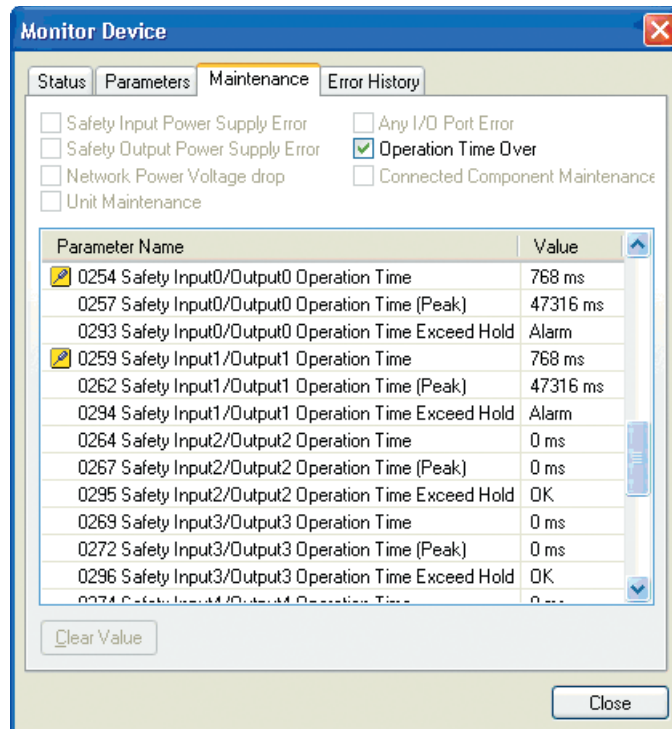
- The present value of the operation time is displayed for the *Operation Time*.
- The slowest value of the operation time is displayed for the *Operation Time (Peak)*.
- If Threshold Response Time is set and the value exceeds the threshold value even once, "Alarm" will be displayed for the *Operation 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.

Appendices

A   Connecting to the Network via a CS/CJ-series PLC

A-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 *2-3 Connecting to the Network* (page 32) to the network via the USB port on the NE1A-SCPU01 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).
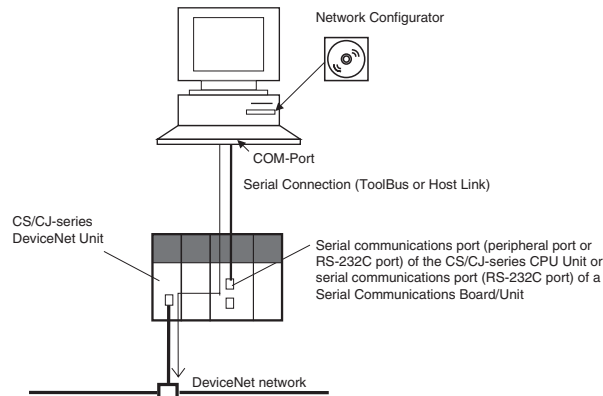
The DeviceNet can be connected to crossing multiple network layers (3 layers max.) using serial communications, as shown in the following figure.
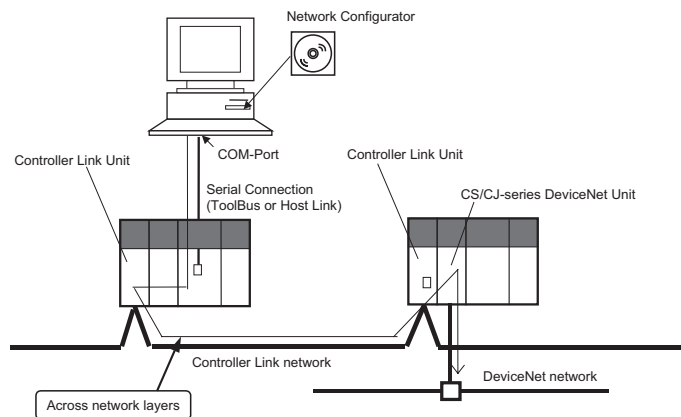
2. Connect the Ethernet port of the computer to a CS/CJ-series Ethernet Unit.

    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).
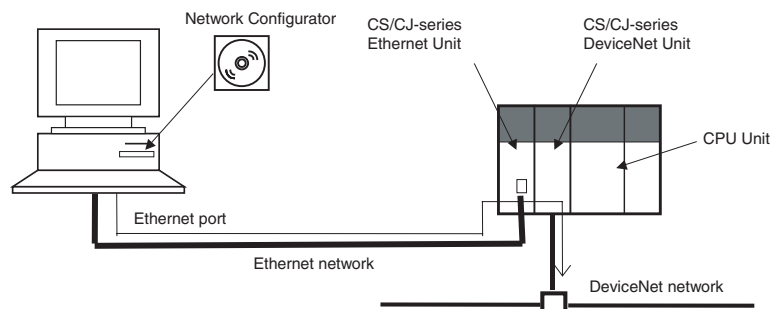
The DeviceNet network can be connected to crossing multiple network layers (3 layers max.) using Ethernet, as shown in the following figure.
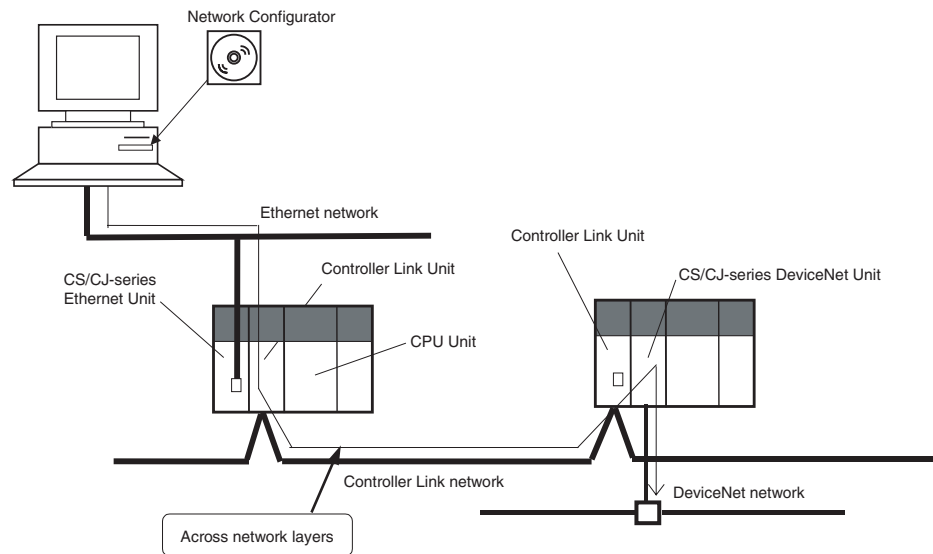
A-2   Specifying the Connection Interface

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* (page 137)
   or *Selecting the SYSMAC CS/CJ Ethernet Unit Interface as the Connection Interface* (page 138) 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.
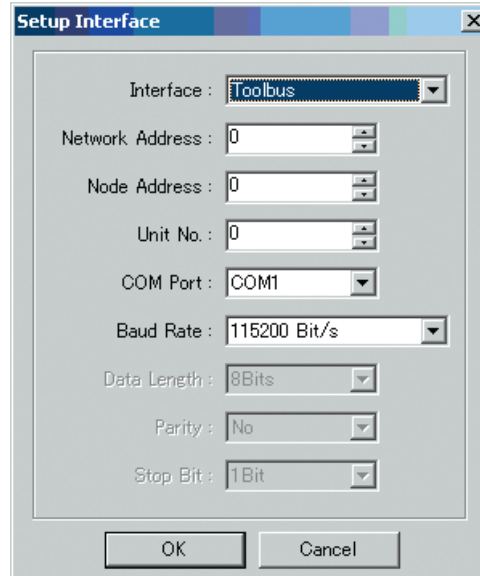
Set each item as described below.

Interface	Select either one of the following interfaces as the serial communications mode for the serial communications port on the CS/CJ-series PLC.
	• Peripheral bus (ToolBus)
	• Host Link
Network Address	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.
Node Address	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.
CPU Bus Unit Number	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).
	• The unit number is between 0 and 15.
Communications Port	Select the COM port on the computer running the Network Configurator (Ver.2).
	• Select from the list of available COM ports.
Baud Rate	Set the baud rate for the serial communications port on the CS/CJ-series PLC.
	• 9,600, 19,200, 38,400, or 115,200 bit/s.
	The baud rates that can be selected for the peripheral bus (ToolBus) and Host Link are different. For details, refer to the CS/CJ Series Operation Manual.
Data Length	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.
	o 7 or 8 bits
Parity	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.
	o None, even, or odd
Stop Bits	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.
	o 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.

The Host Link interface cannot be used when using the CS1W-CN226/626 or the XW2Z-200-CV/500S-CV Connecting Cable. Use the peripheral bus interface.
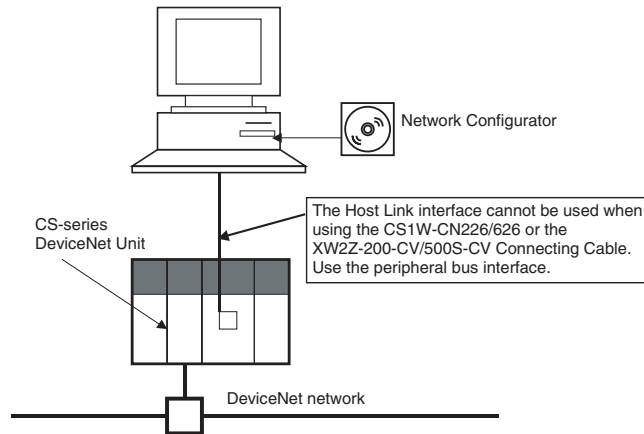
Note: – For information on the FINS node address, refer to the *CS/CJ-series DeviceNet Unit Operation Manual (W380)*.

– 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.
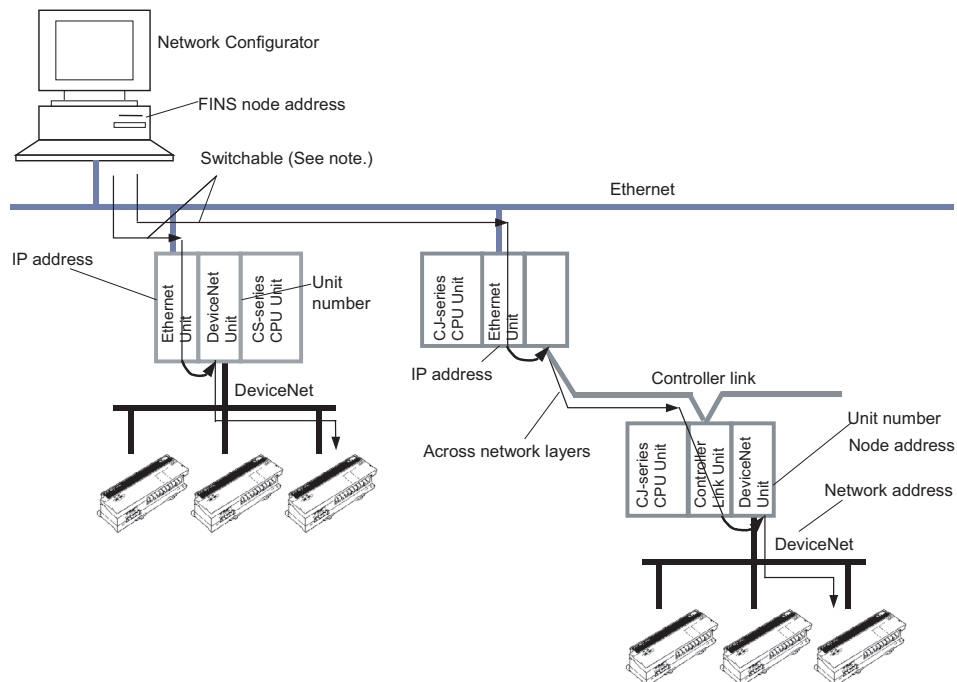
Note: The registered name of the destination DeviceNet network can be specified to switch the destination DeviceNet network. The name of the destination DeviceNet network can be registered by specifying the following items.

– 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.)

3. Click the **Set** Button. The Destination Registration Window will be displayed. An example is shown below.

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)*.

B Editing CS/CJ-series DeviceNet Unit Parameters

This section describes how to edit the parameters of a CS/CJ-series DeviceNet Unit.
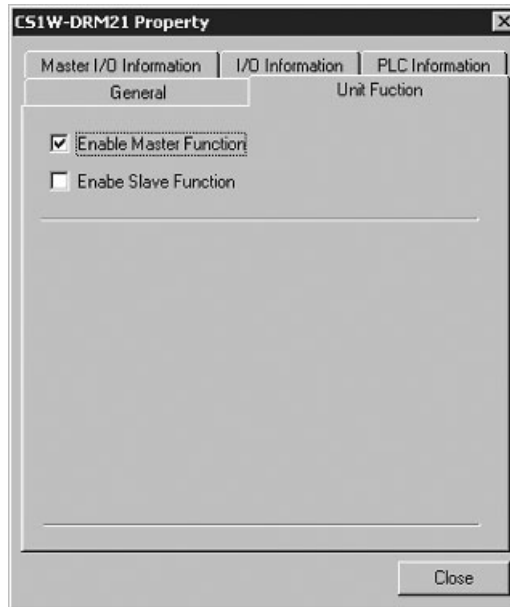
B-1 Setting the Unit Functions

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**.

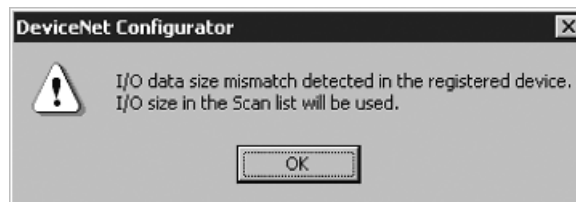The following window will be displayed. Click the **Unit Function** Tab.

3. Select the *Enable Master Function* or *Enable Slave Function* Option (or both).

B-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.
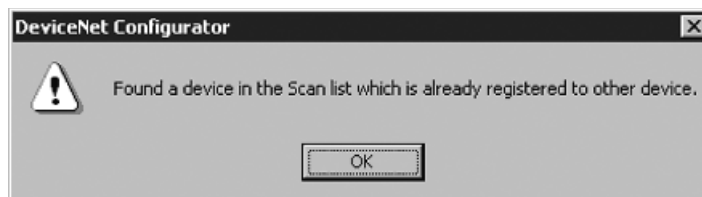
Modify the registered slave in the Scan List.

– 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.
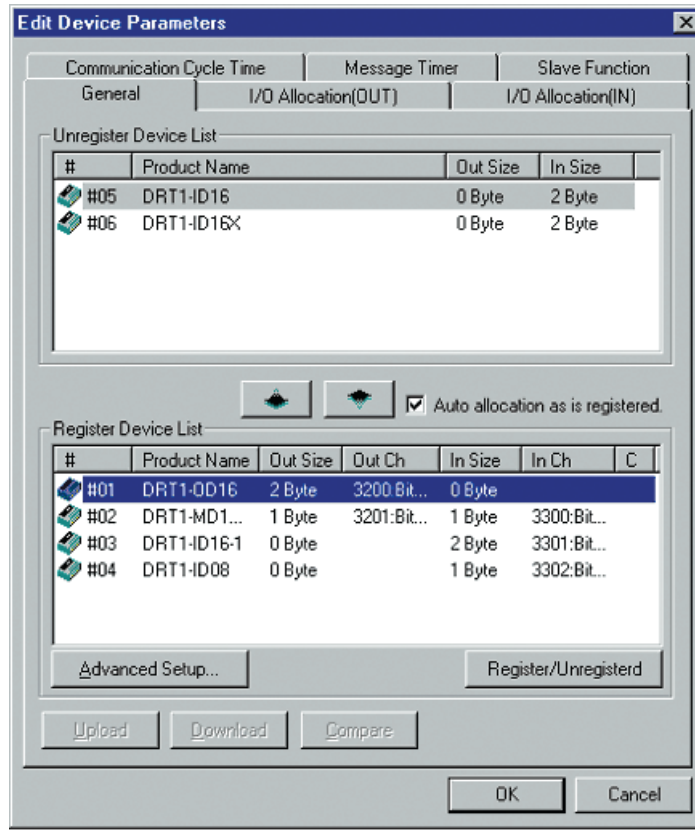
The Edit Device Parameters Window consists of the following 5 tab pages.

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.
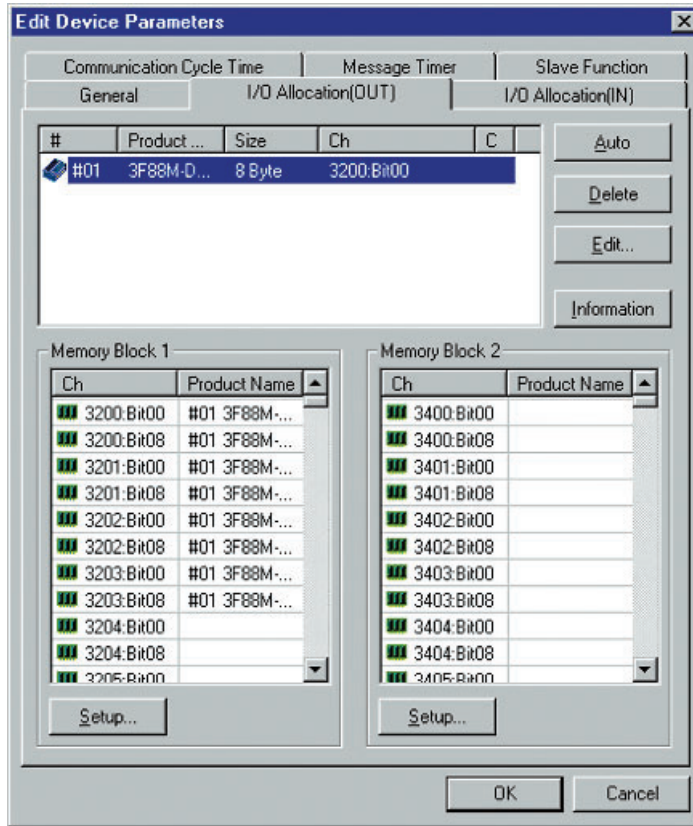
3. Click the **Setup…** Button in the Memory Block 1 Area.
4. Set the *Area*, *Start Word*, and *Display Words* (i.e., the number of words in) for Memory Block 1.
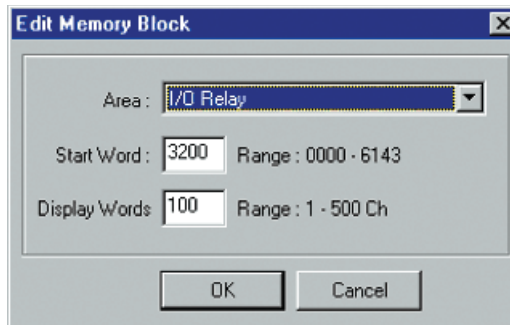
5. Set Memory Block 2 in the same way.
6. Click the **I/O Allocation (IN)** Tab and set the Memory Blocks in the same way as the OUT block.

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.

B-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.
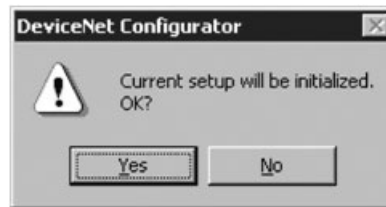
4. Setting the Start Word for Each Block

    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.
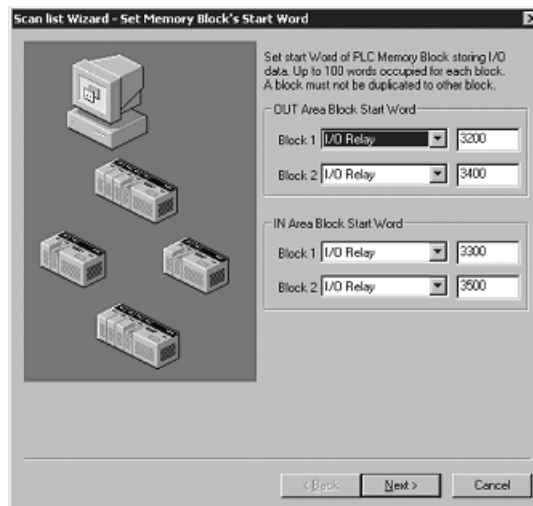
5. Setting Remote I/O Allocations

    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.
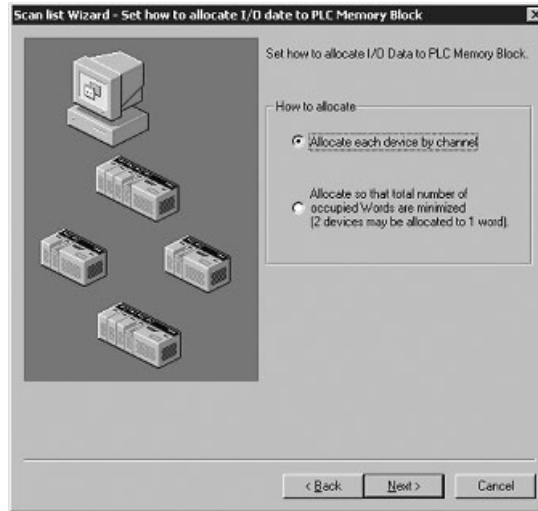
There are two methods for allocation.

Allocate each device by channel	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. Example:
Allocate so that the total number of allocated words is minimized (two devices may be allocated to one word)	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. Example:

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

	High		Low	
	15	8	7	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

	High		Low	
	15	8	7	0
+0 word	#02		#00	
+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.
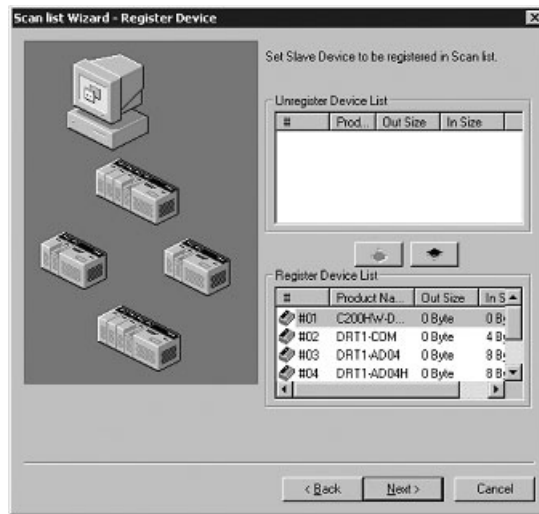
   Devices in the network will be displayed in the Registered Device List as already registered. If there is a device that you do not want registered, click the [button] Button to unregister it. You cannot go on to the next step if there are no registered devices.

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.
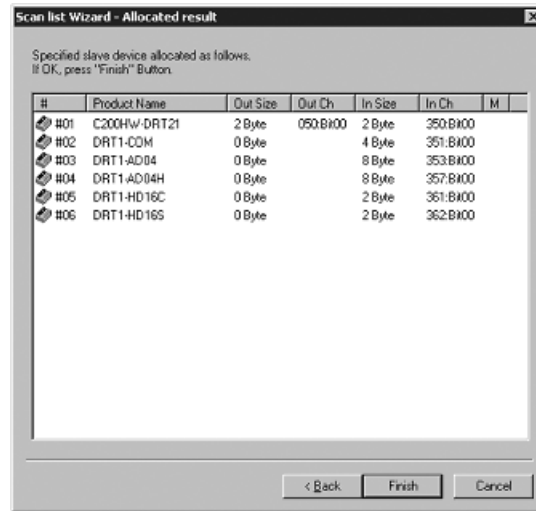
8. Downloading Parameters to a Master Device

    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.

B-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.
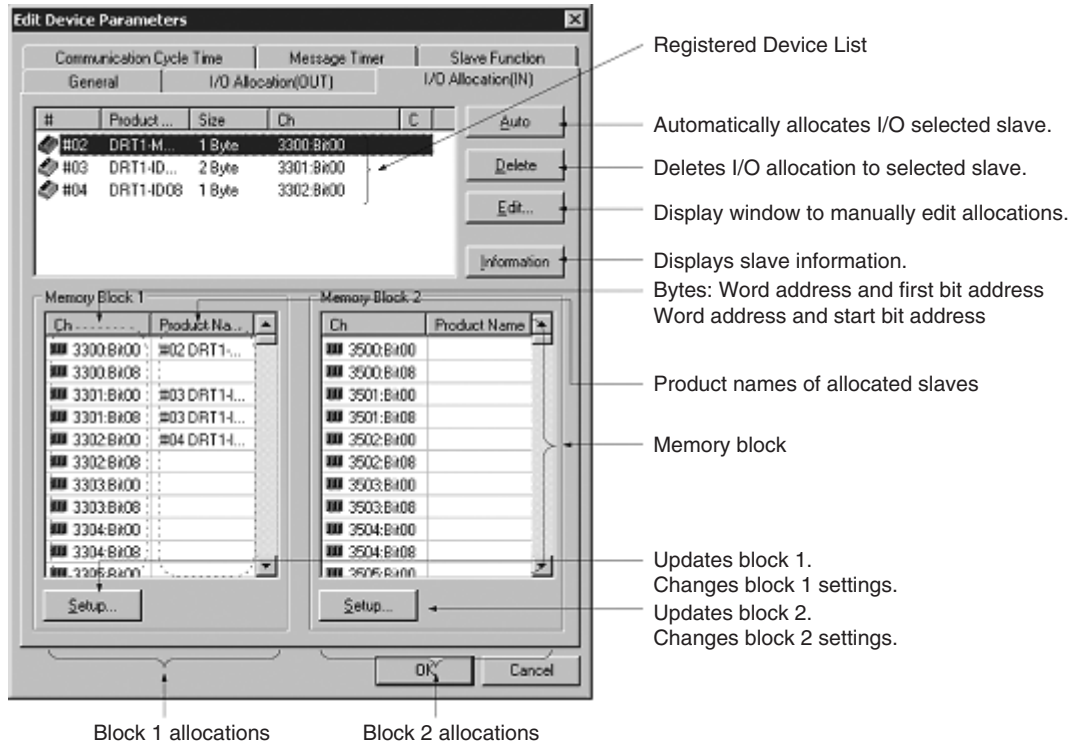
Item	Description
Registered Device List	Displays only devices with valid output or input data of the registered devices on the General Tab Page.
Auto Button	Allocates unused words to the slaves selected in the Registered Device List starting from the first unused words.
Delete Button	Releases the words 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).
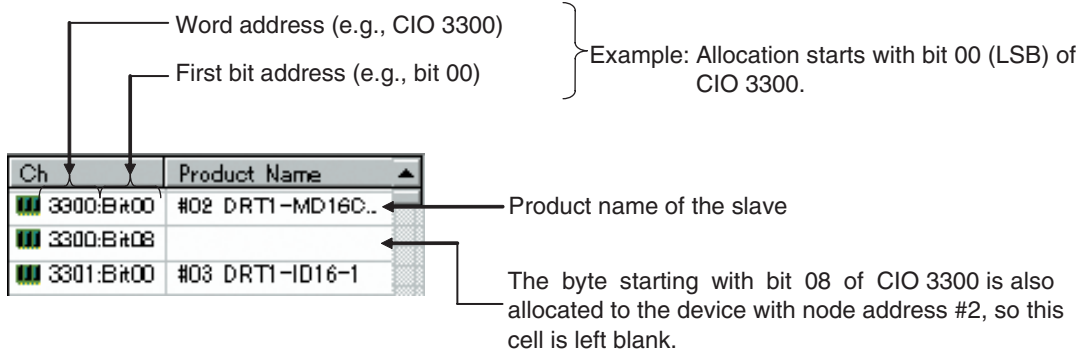
CPU Unit words are not displayed in unused memory block.

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.
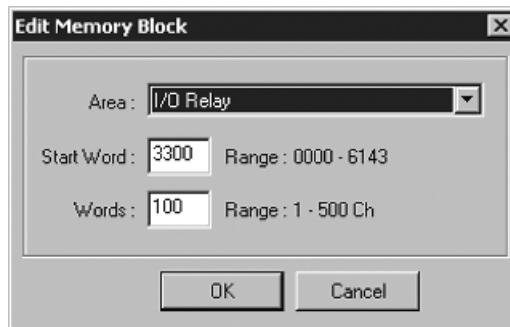
3. Set the *Area*, *Start Word*, and *Words*.

   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	CIO Area	0000 to 6143
CJ Series	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, is 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.

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*).
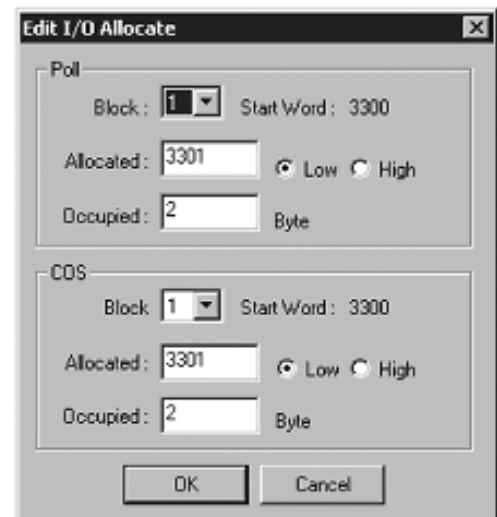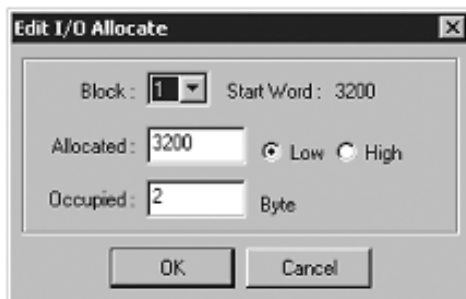
Connections are specified in the General tab with the advanced setup function

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

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.
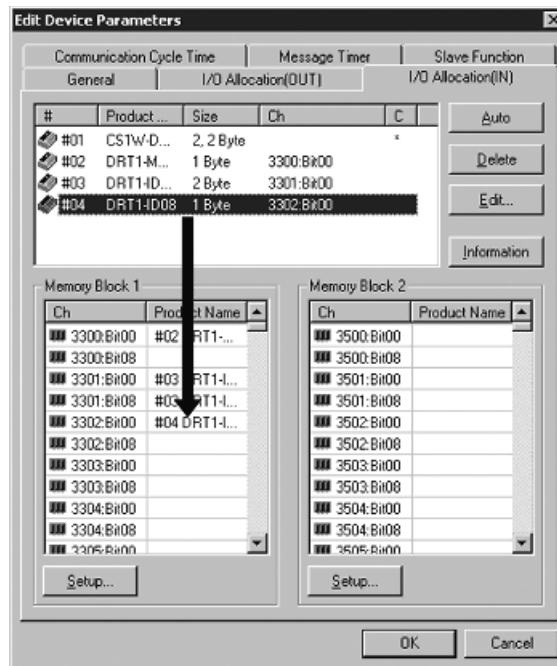
- Memory Block List Contents

  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.
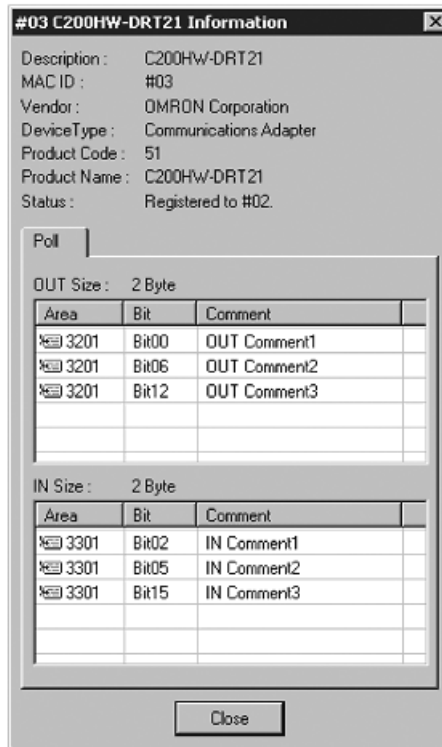
If a registered device is selected while the Information Window is displayed, the slave information will be updated to the information of the selected device.

B-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.
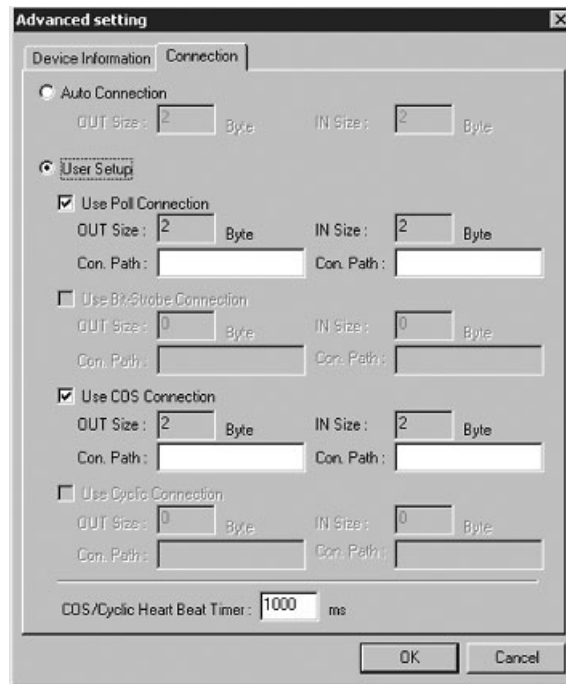
The default setting is *Auto Connection*.

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.
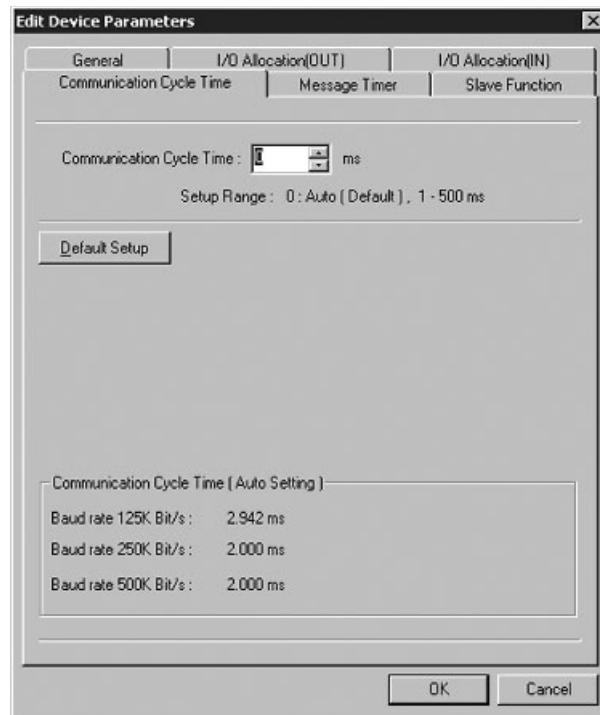
The communications cycle time is set between 1 and 500 ms. Click the Default Setup Button or specify 0 ms to enable automatic setting.

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*)
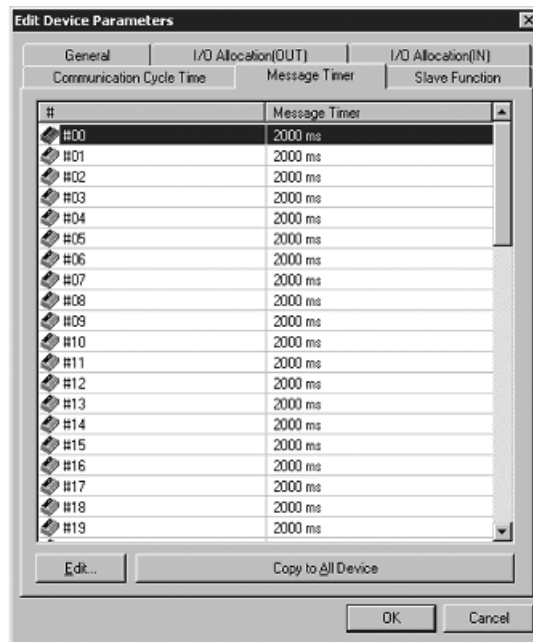
The default value for the message timer is 2 seconds (2,000 ms). Set a value between 500 and 30,000 in increments of milliseconds.

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   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.
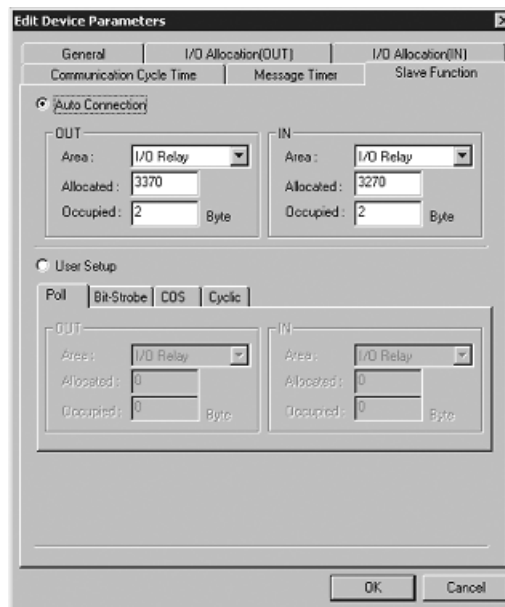
3. Specify a connection.

   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.

C EDS File Management

This section describes the managing the EDS file used in the Network Configurator.

C-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.
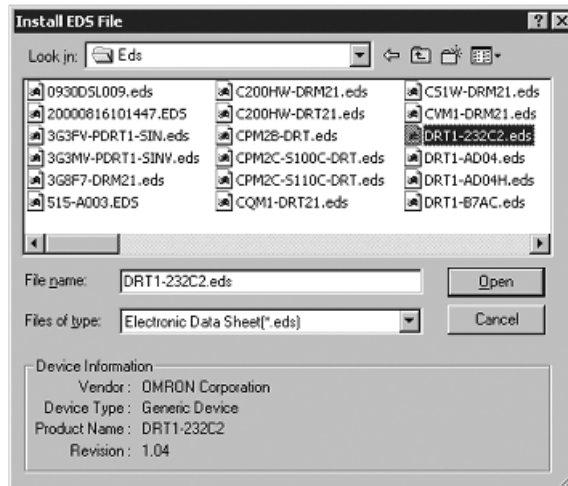
2. Select the EDS file to install. The device information will be displayed in the lower part of the window.
3. Click the **Open** Button.

   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.
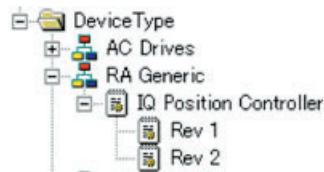
C-2 Creating EDS Files

EDS File - Create
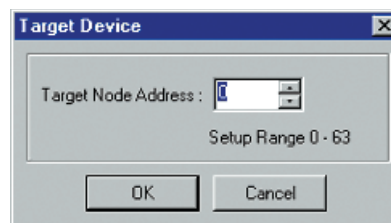
An EDS file is absolutely essential to create a network configuration using the Network Configurator. Use the following procedure to create an EDS file.

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.

C-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.
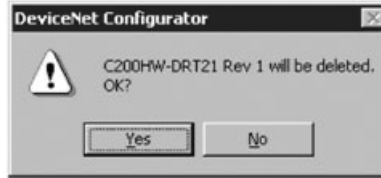
3. Click the **Yes** Button.

    The EDS file and the target device will be deleted from the Hardware List Window.

C-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.
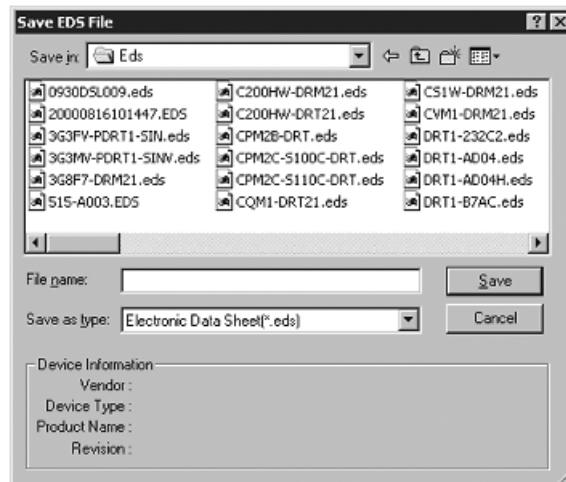
3. Specify a folder and file name and click the **Save** Button.

    The EDS will be saved.

C-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.

C-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.

D   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.

D-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.

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
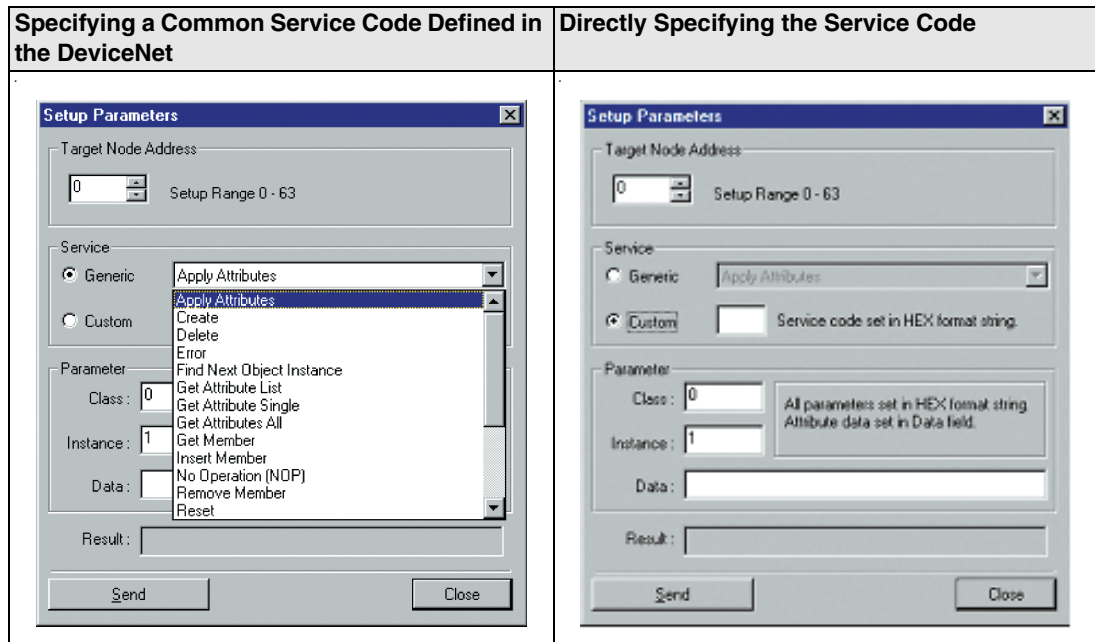
5. Specify the class and instance of the parameters for which the settings are to be read or written.
6. Enter the data based on the specified service type.
7. Enter all the items and click the **Send** Button. The response from the device will be displayed in the *Result* Field.
8. Click the **Close** 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.

D-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.
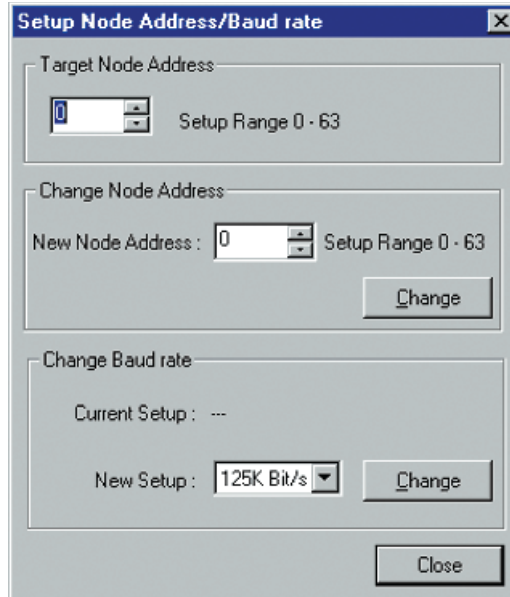
4. Specify the present node address of the target device in the *Target Node Address* Field.
5. To change the node address, specify a new node address in the *New Node Address* Field and click the **Change** Button.
    The node address of the target device will be changed.
6. To change the baud rate, 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.

D   Using General-purpose Tools to Set Devices

E   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.
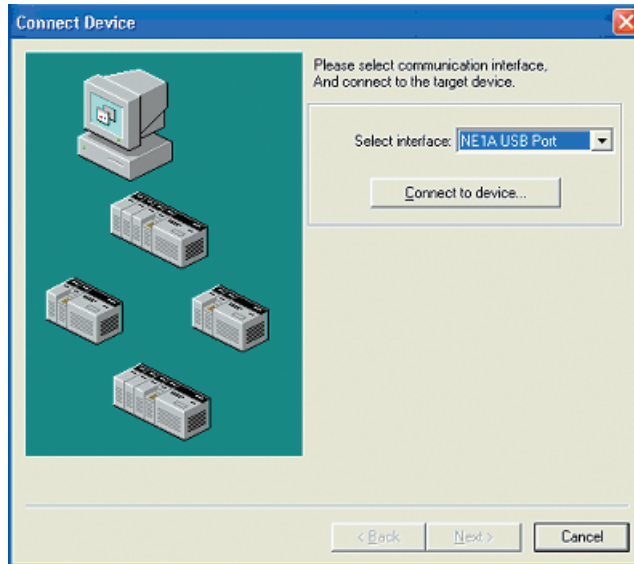
3.   Select an interface for connecting to the network and click the **Connect to Device** Button. Click the **Refresh** Button when the window to search for the destination device is displayed.
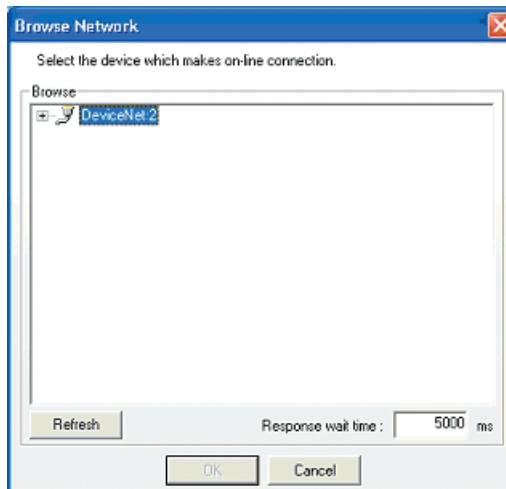
4.   Set the node address range to search for and click the **OK** Button.
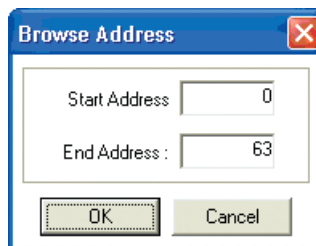
5. The devices in the network will be displayed. Select a device for which to reset the password and click the **OK** Button.
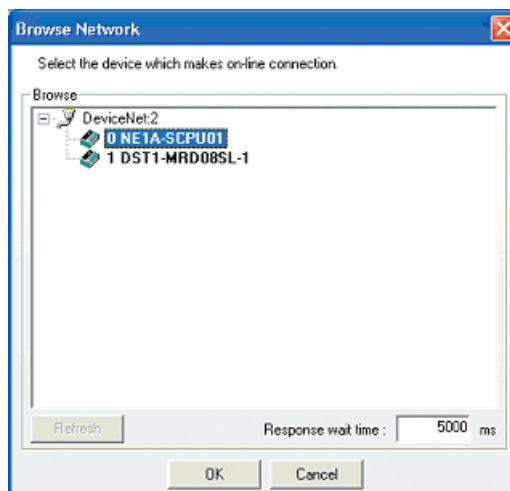
6. The necessary information for resetting the password will be displayed. The information is required when inquiring from the Support Center. Print the information by outputting to a text file and or copying to another application using the clipboard.
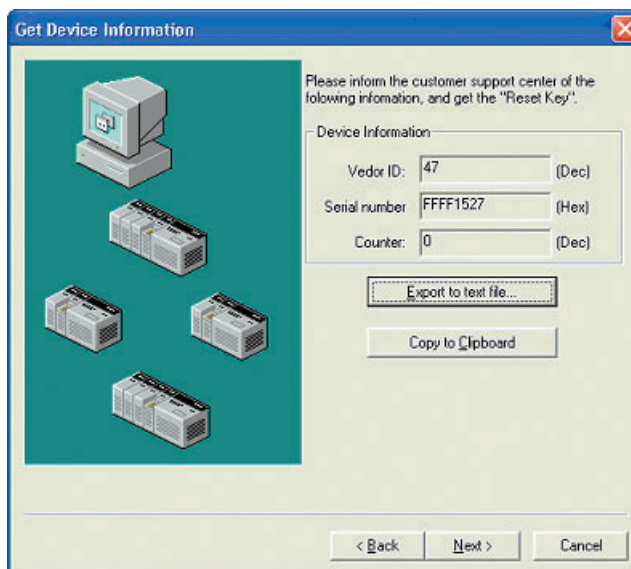
7. Click the **Next** Button to display the Reset Key Enter Window. Enter the Reset Key obtained from the Support Center and click the **Reset** Button.
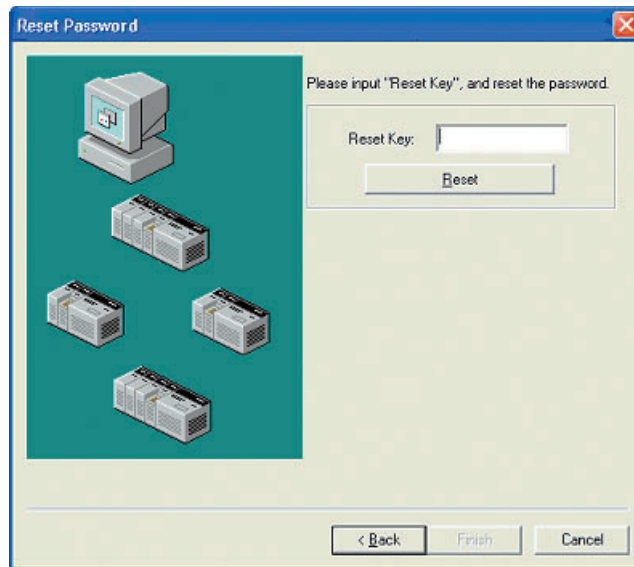
8. If the password is successfully reset, the following dialog box will be displayed. The device will be returned to the state without any password setting (default setting). Click the **OK** Button to close the dialog box. Click the **Finish** Button In the Password Recovery Tool Window to exit.
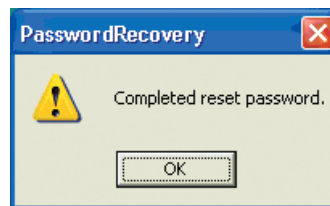
Term	Definition
assembly	Internal data in a device gathered as one group to be accessed externally.
Busoff	Status that occurs when the error rate is extremely high over a communications cable. An error is detected when the internal error counter exceeds a certain threshold value. (The internal error 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 top 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	The UNID of the local node. Usually the TUNID is set from the Network Configurator.
UNID	An identifier to specify one device in all the network domains. Values combining the network address and the node address are used.

Index

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-E2-01

‾Ⱶ——— 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
1	May 2005	Original production