

SmartGuard 600 Controllers

Catalog Numbers 1752-L24BBB, 1752-L24BBBE



Important User Information

Read this document and the documents listed in the additional resources section about installation, configuration, and operation of this equipment before you install, configure, operate, or maintain this product. Users are required to familiarize themselves with installation and wiring instructions in addition to requirements of all applicable codes, laws, and standards.

Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with applicable code of practice.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.



WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.



ATTENTION: Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.

IMPORTANT

Identifies information that is critical for successful application and understanding of the product.

Labels may also be on or inside the equipment to provide specific precautions.



SHOCK HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.



BURN HAZARD: Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.



ARC FLASH HAZARD: Labels may be on or inside the equipment, for example, a motor control center, to alert people to potential Arc Flash. Arc Flash will cause severe injury or death. Wear proper Personal Protective Equipment (PPE). Follow ALL Regulatory requirements for safe work practices and for Personal Protective Equipment (PPE).

Summary of Changes

The information below summarizes the changes to this manual since the last printing.

To help you find new and updated information in this release of the manual, we have included change bars as shown to the right of this paragraph.

Topic	Page
Updated the procedure for handling forgotten passwords	48
Updated DeviceNet driver information	50

Notes:

	Important User Information	2
Summary of Changes		
Table of Contents		
Preface	Who Should Use This Manual	13
	Purpose of This Manual	13
	Additional Resources	13
	Common Techniques Used in This Manual	14
	Chapter 1	
Overview	Introduction	15
	About the SmartGuard 600 Controller	15
	Hardware	17
	Communication	20
	Configuration and Programming	20
	Status and Error Monitoring	20
	Safety Concept of the Controller	21
	Additional Resource	21
	Chapter 2	
Installing and Wiring the SmartGuard 600 Controller	Introduction	23
	General Safety Information	23
	Understanding Node Addressing	25
	Set the Node Address	26
	Setting the Communication Rate	26
	DeviceNet Communication	26
	Ethernet Communication	28
	Mount the SmartGuard Controller	29
	Grounding the SmartGuard Controller	30
	Connecting a Power Supply	30
	Making Communication Connections	31
	Connect to the DeviceNet port	31
	Connecting to USB Port	33
	Connecting to the Ethernet port	33
	Wiring the SmartGuard 600 Controller	34
	Wire Output Devices	36
	Wiring Examples	37
	Chapter 3	
Set Up Your DeviceNet Network	Introduction	41
	Connecting a Computer to the DeviceNet Network	41
	Configure a Driver for the Network	41
	Make Sure the Driver Works	42
	Commission All Nodes	42
	Browse the Network	44

	Configuration Signature	44
	Safety Reset (optional)	45
	Setting Passwords (optional)	47
	Set or Change a Password	47
	Forgotten Passwords	48
	 Chapter 4	
Set Up Your EtherNet/IP Network	Introduction	49
	Connecting a Computer to the EtherNet/IP Network	49
	Configure a Driver for the Network	50
	Make Sure the Driver Works	50
	Connecting the SmartGuard 600 Controller to the EtherNet/IP Network	50
	Setting the IP Address	51
	Using BOOTP to Set the IP Address	51
	Use the Rockwell BOOTP Utility	52
	Use RSLinx Software to Set the IP Address	54
	Bridging across Networks	56
	EtherNet/IP Network to a DeviceNet Network	57
	USB Port to the EtherNet/IP Network	59
	 Chapter 5	
Manage the Safety Network Number	Introduction	61
	Safety Network Number (SNN) Formats	61
	Time-based Safety Network Number (recommended)	62
	Manual Safety Network Number (SNN)	62
	Assignment of the Safety Network Number (SNN)	62
	Automatic (time-based)	63
	Manual	63
	Set the Safety Network Number (SNN) in All Safety Nodes	63
	Safety Network Number (SNN) Mismatch	65
	Safety Network Number (SNN) and Node Address Changes	65
	 Chapter 6	
Configure Local I/O	Introduction	67
	Configure Local Safety Inputs	67
	Example: Input Channel as Test Pulse from Test Output	70
	Automatic Adjustment of On- and Off-delay Times	71
	Configure Local Test Outputs	71
	Configure Local Safety Outputs	73
	 Chapter 7	
Configure Your Controller for DeviceNet Communication	Introduction	77
	Setting Up the Controller as a Safety Master	77
	Configure CIP Safety I/O Targets on the DeviceNet Network ...	78

	Configure Safety I/O Connections	80
	Change an I/O Connection	82
	Setting Up the Controller as a Safety Slave	87
	Create Safety Slave I/O Data	87
	Use the Safety Generic Profile in RSLogix 5000 Software	90
	SmartGuard Controller to SmartGuard Controller Safety Interlocking	92
	Setting Up the Controller as a DeviceNet Standard Slave	95
	Create Standard Slave I/O Data	95
	Adding the SmartGuard Standard Slave to the Standard Master's Scanlist	99
	Reading and Writing to and from the SmartGuard Controller to a PanelView Plus Interface	100
	Read BOOLS from the SmartGuard Controller and Display Them on the PanelView Plus Interface	101
	Configure the Scanlist of the PanelView Scanner	103
	Configure the RN10C DeviceNet Scanner	104
	Read and Write from and to the SmartGuard Controller from the PanelView Plus Interface Concurrently	110
	Configure the Scanlist of the PanelView Scanner	113
	Configure the RN10C DeviceNet Scanner	115
	Configure the Data that is Written from the PanelView Plus Interface to the SmartGuard Controller	116
	COS versus Polled	120
	Maximum Connection Sizes	122
	 Chapter 8	
Configure Your Controller for EtherNet/IP Communication	Introduction	125
	Multicast Connections	125
	Configure Target I/O in RSNetWorx for DeviceNet Software	126
	Set Up Your Controller as a Slave by Using RSLogix 5000 Software Generic Profile	130
	Configure Communication between a Standard PanelView Terminal and a SmartGuard 600 Controller over an EtherNet/IP Network	132
	 Chapter 9	
Set Controller Modes	Introduction	135
	Set Automatic Execution Mode (optional)	135
	Set Standalone Communication Mode (optional)	136
	Change Controller Mode	137
	 Chapter 10	
Create Your Application Program	Introduction	139
	The Logic Editor	139
	Programming Basics	140
	Logic Functions and Function Blocks	141

Input Tags	141
Output Tags	143
I/O Comment Function	144
Programming Restrictions.....	144
Creating a Function Block Program.....	144
Add an Input or Output Tag	144
Add a Function Block.....	145
Connect the Tags to the Function Block.....	145
Edit Function Block Parameters	146
In/Out Settings	146
Optional Output Point Selections.....	147
Comments.....	148
Find Function Blocks with Open Connections	148
Program on Multiple Pages.....	149
Save the Program	150
Update the Program.....	150
Monitor the Program Online.....	151
Program Execution Sequence.....	152
User-defined Function Blocks	152
Create User-defined Function Blocks.....	153
Password Protect User-defined Function Blocks.....	154
Reuse User-defined Function Block Files	155
Precautions for Reusing User-defined Function Blocks.....	157
Additional Resources	157

Chapter 11

Download and Verify

Introduction	159
Download the DeviceNet Network Configuration	159
Verifying Your DeviceNet Safety Configuration	161
Start the Safety Device Verification Wizard.....	161
Determine if Devices Can Be Verified.....	161
Select Devices to Verify	163
Review the Safety Device Verification Reports	164
Lock Safety Devices.....	166
View the Safety Device Verification Wizard Summary.....	167

Chapter 12

Monitor Status and Handle Faults

Introduction	169
Status Indicators	169
Alphanumeric Display	170
Monitoring I/O Power Supply Input.....	171
Monitoring I/O Maintenance Information.....	172
Contact Operation Counter Monitoring	172
Total On-time Monitoring.....	172
Configure a Maintenance Monitoring Mode.....	173
Clear the Maintenance Values	174

	Viewing I/O Status Data	175
	General Status Data	176
	Local Input Status	176
	Local Output Status	177
	Test Output or Muting Lamp Status	177
	Controller Connection Status (safety slave function)	177
	Error Categories	179
	Error History Table	179
	Error History Memory Area	179
	Display the Error History Table for the 1752-L24BBB Controller	179
	Display the EtherNet/IP Error History Table for the 1752-L24BBBE Controller	180
	Ethernet Error History Table	181
	Error History Messages and Corrective Actions	183
	Download Errors and Corrective Actions	185
	Reset Errors and Corrective Actions	187
	Mode Change Errors and Corrective Actions	188
	 Appendix A	
Controller Specifications	Introduction	189
	General Specifications	189
	Environmental Specifications	191
	Certifications	193
	 Appendix B	
Status Indicators	Introduction	195
	Module Status Indicators	195
	Identifying Errors Using Module Status Indicators and Alphanumeric Display	199
	Identifying EtherNet/IP Errors Using Status Indicators and Alphanumeric Display	202
	 Appendix C	
Logic Functions Command Reference	Introduction	203
	NOT Instruction	203
	NOT Instruction Diagram	203
	NOT Instruction Truth Table	203
	AND Instruction	204
	AND Instruction Diagram	204
	AND Instruction Truth Tables	204
	OR Instruction	206
	OR Instruction Diagram	206
	OR Instruction Truth Tables	206
	Exclusive OR Instruction	209
	Exclusive OR Diagram	209

Exclusive OR Truth Table.....	209
Exclusive NOR Instruction	210
Exclusive NOR Instruction Diagram	210
Exclusive NOR Instruction Truth Tables.....	210
Routing Instruction	211
Routing Instruction Diagram	211
Routing Instruction Truth Table	211
Reset Set Flip-flop (RS-FF) Instruction.....	211
Reset Set Flip-flop Instruction Diagram	211
Reset Set Flip-flop Error Handling.....	212
RS Flip-flop Instruction Timing Chart	212
Multi-connector Instruction	212
Multi-connector Instruction Diagram.....	212
Multi-connector Instruction Truth Table	213
Comparator Instruction	213
Comparator Instruction Diagram.....	214
Comparator Instruction Parameters.....	214
Comparator Instruction Truth Table	215
Comparator Instruction Timing Chart.....	216

Appendix D

Function Blocks Command Reference

Introduction	217
Reset Function Block.....	217
Reset Function Block Parameters	218
Reset Function Block Timing Charts.....	219
Restart Function Block	219
Restart Function Block Parameters.....	220
Restart Function Block Timing Charts	221
Emergency Stop (ESTOP)	221
ESTOP Function Block Parameters	222
ESTOP Function Block Truth Tables.....	222
ESTOP Function Block Error Handling.....	223
ESTOP Function Block Timing Chart	223
Light Curtain (LC) Function Block.....	223
Light Curtain Function Block Parameters	224
Light Curtain Function Block Truth Tables	224
Light Curtain Function Block Error Handling	224
Light Curtain Function Block Timing Chart	225
Safety Gate Monitoring Function Block.....	225
Safety Gate Monitoring Function Block Optional Outputs	226
Safety Gate Monitoring Function Block Fault Present Output Setting.....	226
Safety Gate Monitoring Function Block Function Tests	226
Safety Gate Monitoring Function Block Parameters	227
Safety Gate Monitoring Function Block Truth Tables	227
Safety Gate Monitoring Function Block Error Handling.....	228
Safety Gate Monitoring Function Block Timing Charts.....	229

Two-hand Control Function Block	230
Two-hand Control Function Block Optional Outputs	230
Two-hand Control Function Block Fault Present Output Setting	230
Two-hand Control Function Block Parameters	230
Two-hand Control Function Block Truth Table	231
Two-hand Control Function Block Error Handling	231
Two-hand Control Function Block Timing Chart	232
OFF-delay Timer Function Block	232
OFF-delay Timer Function Block Timing Chart	233
ON-delay Timer Function Block	233
ON-Delay Timer Function Block Timing Chart	234
User Mode Switch Function Block	234
User Mode Switch Function Block Optional Outputs	234
User Mode Switch Function Block Fault Present Output Setting	235
User Mode Switch Function Block Truth Table	235
User Mode Switch Function Block Error Handling	235
User Mode Switch Function Block Timing Chart	236
External Device Monitoring (EDM)	236
EDM Function Block Optional Outputs	236
EDM Function Block Fault Present Output Setting	237
EDM Function Block Parameter	237
EDM Function Block Error Handling	237
EDM Function Block Timing Chart	238
Muting	238
Muting Function Block Parameters	239
Muting Function Block Optional Outputs	239
Muting Function Block Fault Present Output Setting	240
Muting Function Block Error Handling	240
Muting Function Details	240
Example: Parallel Muting with Two Sensors	241
Example: Position Detection	249
Example: Override Function	251
Enable Switch	254
Enable Switch Function Block Parameters	255
Optional Outputs	255
Fault Present Output Setting	255
Enable Switch Function Block Error Handling	256
Enable Switch Function Block Timing Charts	256
Pulse Generator	257
Pulse Generator Function Block Parameters	257
Pulse Generator Function Block Timing Chart	257
Counter	258
Counter Function Block Parameters	258
Reset Condition	258
Count Type	259
Counter Function Block Timing Charts	259

Explicit Messages	Appendix E	
	Introduction	261
	Receiving Explicit Messages	261
	Command Format	261
	Response Format	262
	Error Response Format	263
	Example Read Message from a GuardLogix Controller	263
	Send Explicit Messages	264
	Restrictions on Sending Explicit Messages	265
	Accessing Controller Parameters By Using DeviceNet Explicit Messages	265
Application and Configuration Examples	Appendix F	
	Introduction	271
	Emergency Stop Application	271
	Safety Gate Application with Automatic Reset	273
	Dual Zone Safety Gate Application Using Emergency Stop Switch with Manual Reset	274
	Safety Mat Application	276
	Light Curtain Application	279
Glossary		
Index		

Read this preface to familiarize yourself with the rest of the manual. It provides information concerning:

- who should use this manual.
- the purpose of this manual.
- additional resources.
- conventions used in this manual.

Who Should Use This Manual

Use this manual if you are responsible for designing, installing, programming, or troubleshooting control systems that use SmartGuard™ 600 controllers.

You must have a basic understanding of electrical circuitry and familiarity with relay logic. You must also be trained and experienced in the creation, operation, and maintenance of safety systems.

Purpose of This Manual

This manual is a guide for using SmartGuard 600 controllers. It describes the specific procedures you use to configure, operate, and troubleshoot your SmartGuard 600 controller.

Additional Resources

The table provides a listing of publications that contain important information about SmartGuard 600 controller systems.

Resource	Description
SmartGuard 600 Controller Installation Instructions, publication 1752-IN001	Information on installing the SmartGuard 600 controller
SmartGuard Controllers Systems Safety Reference Manual, publication 1752-RM001	Detailed requirements for achieving and maintaining SIL 3 with the SmartGuard controller system
DeviceNet Safety I/O Installation Instructions, publication 1791DS-IN001	Information on installing Guard I/O™ DeviceNet Safety modules
Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001	Information on using Guard I/O DeviceNet Safety modules
DeviceNet Media Design Installation Guide, publication DNET-UM072	Information on planning your EtherNet/IP™ network

You can view or download publications at <http://www.rockwellautomation.com/literature>. To order paper copies of technical documents, contact your local Allen-Bradley® distributor or Rockwell Automation sales representative.

Common Techniques Used in This Manual

These conventions are used throughout this manual:

- Bulleted lists, such as this one, provide information, not procedural steps.
- Numbered lists provide sequential steps or hierarchical information.

Overview

Introduction

Topic	Page
About the SmartGuard 600 Controller	15
Safety Concept of the Controller	21
Additional Resource	21

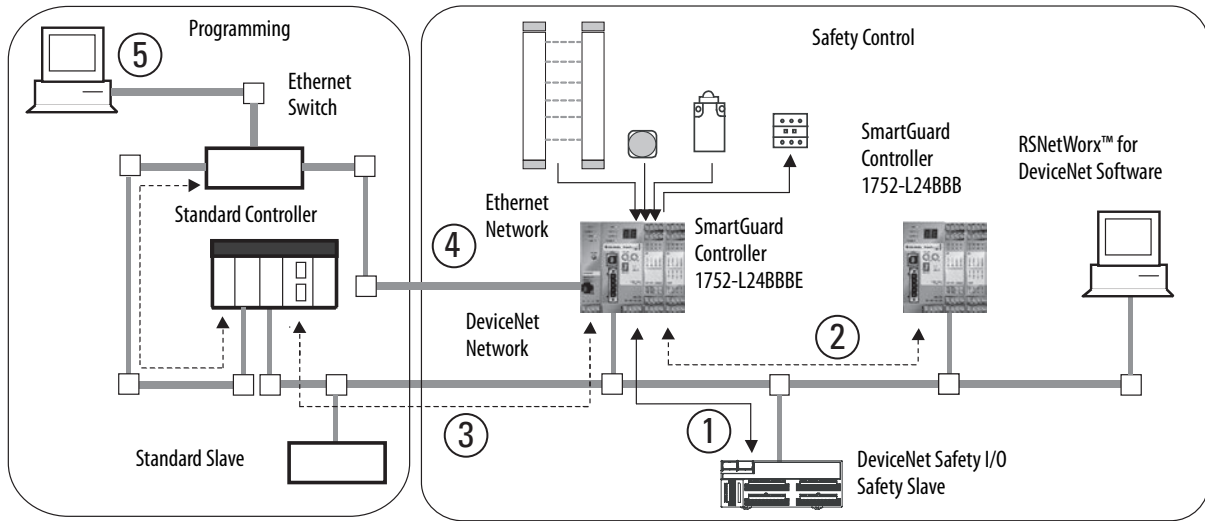
About the SmartGuard 600 Controller

The SmartGuard 600 controller (catalog numbers 1752-L24BBB and 1752-L24BBBE) are programmable electronic systems featuring 16 digital inputs, 8 digital outputs, 4 test pulse sources, and connections for USB and DeviceNet™ communication. In addition, the 1752-L24BBBE controller offers EtherNet/IP connectivity.

The SmartGuard 600 controller supports both standard and CIP Safety communication over DeviceNet networks, and supports standard CIP communication over EtherNet/IP networks.

The SmartGuard 600 controller is certified for use in safety applications up to and including Safety Integrity Level (SIL) 3, according to IEC 61508, Performance Level PL(e) according to ISO 13849-1, and Category (CAT) 4, according to EN 954-1.

Figure 1 - SmartGuard 600 Controller Safety Control System Example

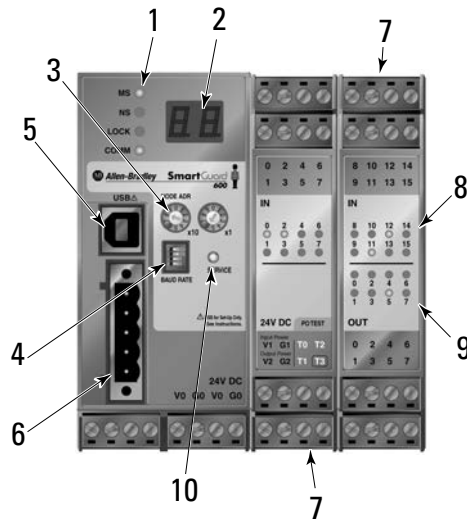


Number	Description
1	As a DeviceNet safety master, the SmartGuard 600 controller can control up to 32 Guard I/O modules. These 1791DS and 1732DS modules are the same distributed safety I/O modules used with GuardLogix® controllers.
2	As a DeviceNet safety slave, the SmartGuard 600 controller looks like distributed safety I/O to a safety master. A GuardLogix or another SmartGuard safety master can read and write safety data to the SmartGuard slave controller. This lets you perform distributed safety control through the interlocking of multiple controllers via CIP Safety on DeviceNet networks.
3	As a DeviceNet standard slave, the SmartGuard 600 controller can look like a standard distributed I/O module and respond to explicit messages so that standard DeviceNet masters like ControlLogix®, SLC™ 500, or PLC-5® controllers or an HMI can read and write information to and from the SmartGuard 600 controller. This facilitates coordination with your standard PLC application, including displaying safety system information on an HMI.
4	As an EtherNet/IP standard target, the SmartGuard 600 controller communicates with an EtherNet/IP standard originator, such as a CompactLogix™ or MicroLogix™ controller or an HMI device. The SmartGuard controller does not support CIP Safety on EtherNet/IP communication. As a result, the SmartGuard controller cannot control 1791ES safety modules. All safety control must be done over the DeviceNet network as shown in numbers 1 and 2 above.
5	As a limited EtherNet/IP bridge device, the SmartGuard 600 controller lets programming tools bridge to DeviceNet to view and program the SmartGuard 600 controller and configure other DeviceNet devices.

Hardware

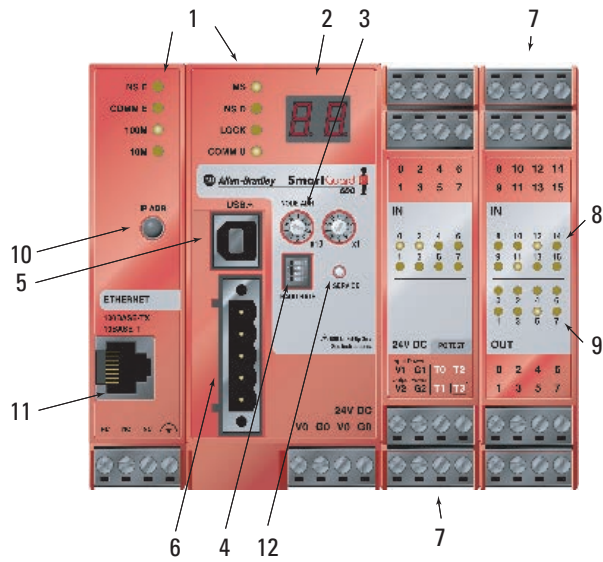
The SmartGuard 600 controller (catalog numbers 1752-L24BBB and 1752-L24BBBE) features 16 digital inputs, 8 digital outputs, 4 pulse test sources, and connections for USB and DeviceNet Safety protocol. In addition, the 1752-L24BBBE controller offers EtherNet/IP connectivity.

Figure 2 - SmartGuard 600 Controller (catalog number 1752-L24BBB) Features



Number	Feature
1	Module status Indicators
2	Alphanumeric display
3	Node address switches
4	Baud rate switches
5	USB port
6	DeviceNet communication connector
7	Terminal connectors
8	Input status indicators
9	Output status indicators
10	Service switch

SmartGuard 600 Controller (catalog number 1752-L24BBBE) Features



Number	Feature
1	Module status indicators
2	Alphanumeric display
3	Node address switches
4	Baud rate switches
5	USB port
6	DeviceNet communication connector
7	Terminal connectors
8	Input status indicators
9	Output status indicators
10	IP address display switch
11	Ethernet connector
12	Service switch

Safety Inputs

The controller has 16 local safety inputs, which support the features described below.

- Input circuit diagnosis — Test pulse sources can be used to monitor internal circuits, external devices, and external wiring.
- Input on- and off-delays — You can set input time filters of 0...126 ms in multiples of the controller cycle time. Setting input on- and off-delays helps reduce the influence of chattering and external noise.
- Dual Channel mode — You can set Dual Channel mode for pairs of related local inputs. When Dual Channel mode is set, time discrepancies in changes in data or input signals between two paired, local inputs can be evaluated.

Safety Outputs

The controller has eight local safety outputs, which support the features described below.

- Output circuit diagnosis — Test pulses can be used to diagnose the controller's internal circuits, external devices, and external wiring.
- Overcurrent detection and protection — To protect the circuit, an output is blocked when an overcurrent is detected.
- Dual Channel mode — Both of two paired outputs can be set into a safety state without depending on the user program when an error occurs in either of the two paired local outputs.

Test Pulse Sources

Four independent test outputs are normally used in combination with safety inputs. They can also be set for use as standard signal output terminals. The test pulse outputs support the following features.

- Overcurrent detection and protection — To protect the circuit, an output is blocked when an overcurrent is detected.
- Current monitoring for muting lamp — Disconnection can be detected for the T3 terminal only.

Communication

The controller can act as a DeviceNet safety master or slave, as a DeviceNet standard slave, or as a standalone controller when DeviceNet communication is disabled. A single controller can function simultaneously as a safety master, safety slave, and standard slave.

Explicit messages can be used to read controller status information. The user program can be configured to send explicit messages from the user program. The messages can be routed between DeviceNet and EtherNet/IP networks.

The USB port can be used to program the SmartGuard controller and to configure devices on the DeviceNet network. The SmartGuard provides some limited pass-through capability from USB to DeviceNet, for programming and configuration purposes. When used in Standalone mode, the controller communicates with the configuration software via USB communication.

Configuration and Programming

Use RSNetWorx for DeviceNet software, version 8.0 (minimum) or later (version 9.1 is recommended), to configure, program, and monitor the status of the 1752-L24BBB controller. Use RSNetWorx for DeviceNet software, version 9.1 or later, to configure, program, and monitor the status of the 1752-L24BBBE controller. With RSNetWorx for DeviceNet software, you can configure the controller by using the SmartGuard controller's USB port or via the DeviceNet network or EtherNet/IP network.

You also need RSLinx® software, version 2.55 or later, which lets you configure a 1752-L24BBBE controller on EtherNet/IP.

The logic editor is launched from within RSNetWorx for DeviceNet software. Basic logic operations, such as AND and OR, and function blocks, such as ESTOP and light curtain, are supported. A maximum of 254 logic functions and function blocks can be used in a maximum of 32 programming pages. You can password-protect both configuration data and project files.

Status and Error Monitoring

The controller's internal status information and I/O data can be monitored online by using RSNetWorx for DeviceNet software with either a USB, DeviceNet network connection or EtherNet/IP network connection.

The status indicators and alphanumeric display on the controller provide status and error information. When the service switch on the front of the controller is pressed, the alphanumeric display shows the controller's safety configuration signature two digits at a time for a total of ten pairs of numbers.

When the IP Address display switch is pressed for 1 second or longer, the display shows the EtherNet/IP address that is set.

Errors detected by the controller are recorded in an error history log and an EtherNet/IP history log, along with the time the error occurred. (The time is shown as total operating time since the controller was powered up.)

Safety Concept of the Controller

The SmartGuard 600 controller is certified for use in safety applications up to and including Safety Integrity Level (SIL) 3, according to IEC 61508, Performance Level PL(e) according to ISO 13849-1, and Category (CAT) 4, according to EN 954-1, in which the de-energized state is the safety state. Safety application requirements include evaluating the probability of failure rates (PFD and PFH), system reaction-time calculations, and functional verification tests that fulfill SIL 3 criteria. You must read, understand, and fulfill these requirements prior to operating a SmartGuard 600 controller-based SIL 3 or CAT 4 safety system.

The controller uses the following mechanisms to support the integrity of safety data.

- Safety network number (SNN) — A unique number that identifies the safety network. CIP safety nodes must have a unique SNN and DeviceNet network address.
- Configuration signature — The combination of an ID number, date, and time that uniquely identifies a specific configuration for a safety device.
- Configuration lock (or safety-lock) — After the configuration data has been downloaded and verified, you can lock the controller's configuration to prevent it from being modified.
- Password protection — The controller's configuration can be protected by the use of an optional password. If you set a password, download, locking, unlocking, resetting, and changing the status of the controller requires a password to perform.

You must create and document a clear, logical, and visible distinction between the safety and any standard portions of the application.

Additional Resource

Refer to the SmartGuard Controllers Safety Reference Manual, publication [1752-RM001](#), for information on SIL 3 and CAT 4 safety system requirements, including functional verification test intervals, system reaction time, and PFD/PFH values.

Notes:

Installing and Wiring the SmartGuard 600 Controller

Introduction

Topic	Page
General Safety Information	23
Understanding Node Addressing	25
Set the Node Address	26
Setting the Communication Rate	26
Mount the SmartGuard Controller	29
Grounding the SmartGuard Controller	30
Connecting a Power Supply	30
Wiring the SmartGuard 600 Controller	34

General Safety Information



ATTENTION: Environment and Enclosure

This equipment is intended for use in Pollution Degree 2 Industrial environment, in Overvoltage Category II applications (as defined in IEC publication 60664-1), at altitudes up to 2000 m (6562 ft) without derating.



This equipment is considered Group 1, Class A industrial equipment according to IEC/CISPR Publication 11. Without appropriate precautions, there may be potential difficulties ensuring electromagnetic compatibility in other environments due to conducted as well as radiated disturbance.

This equipment is supplied as open type equipment. It must be mounted within an enclosure that is suitably designed for those specific environmental conditions that will be present and appropriately designed to prevent personal injury resulting from accessibility to live parts. The enclosure must have suitable flame-retardant properties to prevent or minimize the spread of flame, complying with flame spread rating or 5VA, V2, V1, V0 (or equivalent) if non-metallic. The interior of the enclosure must be accessible only by the use of a tool. Subsequent sections of this publication may contain additional information regarding specific enclosure type ratings that are required to comply with certain product safety certifications.

In addition to this publication, see:

- Industrial Automation Wiring and Grounding Guidelines, Allen-Bradley publication [1770-4.1](#).
- NEMA Standards publication 250 and IEC publication 60529, as applicable, for explanations of the degrees of protection provided by different types of enclosure.

Table 1 - North American Hazardous Location Approval

The following information applies when operating this equipment in hazardous locations		Informations sur l'utilisation de cet équipement en environnements dangereux	
<p>Products marked CL I, DIV 2, GP A, B, C, D are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest T number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.</p>		<p>Les produits marqués CL I, DIV 2, GP A, B, C, D ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.</p>	
	<p>EXPLOSION HAZARD</p> <ul style="list-style-type: none"> •Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. •Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. •Substitution of components may impair suitability for Class I, Division 2. •If this product contains batteries, they must only be changed in an area known to be nonhazardous. 		<p>RISQUE D'EXPLOSION</p> <ul style="list-style-type: none"> •Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. •Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. •La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. •S'assurer que l'environnement est classé non dangereux avant de changer les piles.



ATTENTION: Safety Programmable Electronic Systems (PES)

Personnel responsible for the application of safety-related programmable electronic systems (PES) shall be aware of the safety requirements in the application of the system and shall be trained in using the system.



ATTENTION: Prevent Electrostatic Discharge

This equipment is sensitive to electrostatic discharge, which can cause internal damage and affect normal operation. Follow these guidelines when you handle this equipment.

- Touch a grounded object to discharge potential static.
- Wear an approved wrist grounding strap.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- Use a static-safe workstation, if available.
- Store the equipment in appropriate static-safe packaging when not in use.



ATTENTION: Protective Debris Strip

Do not remove the protective debris strip until after the controller and all the other equipment near the controller is mounted and wiring is complete.

Once wiring is complete, remove the protective debris strip. Failure to remove the strip before operating can cause overheating.



ATTENTION: Serious injury may occur due to the loss of required safety function.

- Do not use test outputs as safety outputs.
- Do not use DeviceNet standard I/O data or explicit message data as safety data.
- Do not use status indicators for safety operations.
- Do not connect loads beyond the rated value to safety outputs or test outputs.
- Wire the controller properly so that the 24V dc line does not accidentally touch the outputs.
- Ground the 0V line of the power supply for external output devices so that the devices do not turn on when the safety output line or test output line is grounded.
- Do not dismantle, repair, or modify the controller. Doing so may impair the safety functions.

Understanding Node Addressing

To communicate on the DeviceNet network, each device requires its own address. Follow the recommendations below when assigning addresses to the devices on your network.

Table 2 - Node Address Recommendations

Give this device	This address	Notes
Scanner	0	If you have multiple scanners, give them the lowest addresses in sequence.
Any device on your network, except the scanner	1...61	Gaps between addresses are allowed and have no effect on system performance. Leaving gaps gives you more flexibility as you develop your system.
RSNetWorx for DeviceNet workstation	62	If you connect a computer directly to the DeviceNet network, use address 62 for the computer or bridging/linking device.
No device	63	Leave address 63 open. This is where a non-commissioned node typically enters the network.

The standard DeviceNet network assigns communication priority based on the device's node number. The lower the node number, the higher the device's communication priority. This priority becomes important when multiple nodes are trying to communicate on the network at the same time.

DeviceNet safety nodes have additional priority on the network, regardless of node number. DeviceNet safety communication from devices with lower node numbers have priority over DeviceNet safety communication from devices with higher node numbers.

Set the Node Address

Set the node address before you mount the controller.

IMPORTANT Turn off power to the controller before setting the node address or communication rate via the switches.

Do not change the switch settings while the power supply is on. The controller will detect this as a change in the configuration and will switch to the ABORT mode.

Use a small flathead screwdriver to set the node address by using the two rotary switches on the front panel of the controller. Use care not to scratch the switches. Values from 00...63 are valid. The default setting is 63.

Follow these steps to set the node address.

1. Set the tens digit of the node address (decimal) by turning the left rotary switch.
2. Set the ones digit by turning the right rotary switch.
3. To allow the node address to be set by using RSNetWorx for DeviceNet software, set the rotary switches to a value from 64...99.

IMPORTANT A node address duplication error will occur if the same node address is set for more than one node.

Setting the Communication Rate

Set the communication rate before you mount the controller.

IMPORTANT Turn off power to the controller before setting the node address or communication rate via the switches.

Do not change the switch settings while the power supply is on. The controller will detect this as a change in the configuration and will switch to the ABORT mode.

DeviceNet Communication

The default communication rate for a DeviceNet network is 125 Kbps.

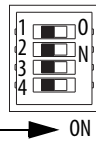
If you choose to use a different communication rate, the length of the trunkline and types of cable determine which communication rates your application can support.

Table 3 - DeviceNet Communication Rates and Cable Lengths

Communication Rate	Distance, max			Cumulative Drop Line Length
	Flat Cable	Thick Cable	Thin Cable	
125 Kpbs	420 m (1378 ft)	500 m (1640 ft)	100 m (328 ft)	156 m (512 ft)
250 Kpbs	200 m (656 ft)	250 m (820 ft)	100 m (328 ft)	78 m (256 ft)
500 Kpbs	75 m (246 ft)	100 m (328 ft)	100 m (328 ft)	39 m (128 ft)

Set the communication rate by using the DIP switch on the front of the controller.

Figure 3 - Communication Rate Dip Switch



DIP Switch Pin				Communication Rate
1	2	3	4	
OFF	OFF	OFF	OFF	125 Kbps
ON	OFF	OFF	OFF	250 Kbps
OFF	ON	OFF	OFF	500 Kbps
ON	ON	OFF	OFF	Set by software
ON or OFF	ON or OFF	ON	OFF	Set by software
ON or OFF	ON or OFF	ON or OFF	ON	Automatic baud rate detection

IMPORTANT If you change the communication rate of your network, make sure that all devices change to the new communication rate. Mixed communication rates produce communication errors.

If you set other devices to autobaud, at least one device on the network must have a communication rate established. If you set all devices on the network to autobaud, they will not be able to establish a communication rate and will not communicate with each other.

Ethernet Communication

We recommend connecting the module to the network via a 100 Mbps Ethernet switch, which will help reduce collisions and lost packets and increase bandwidth.

The 1752-L24BBBE controller is shipped with BOOTP enabled for setting the IP address. You can use any commercially available BOOTP server. If you do not have BOOTP Server capabilities on your network, download the free Rockwell Automation BOOTP server from <http://www.rockwellautomation.com/rockwellsoftware/download/>.

To set the IP address by using the Rockwell Automation BOOTP utility, refer to [page 51](#).

The following table provides additional EtherNet/IP information.

For detailed information on EtherNet/IP communication, refer to the EtherNet/IP Performance and Application Solution, publication [ENET-AP001](#).

Attribute	Value
Number of CIP packets	2
Allowable Unit communication bandwidth	3000 pps ⁽¹⁾
Explicit message communication	502 B ⁽²⁾

(1) PPS is packets Per second. It indicates the number of send or receive packets that can be processed per second.

(2) The maximum message length for class 3 connection and UCMM connection.

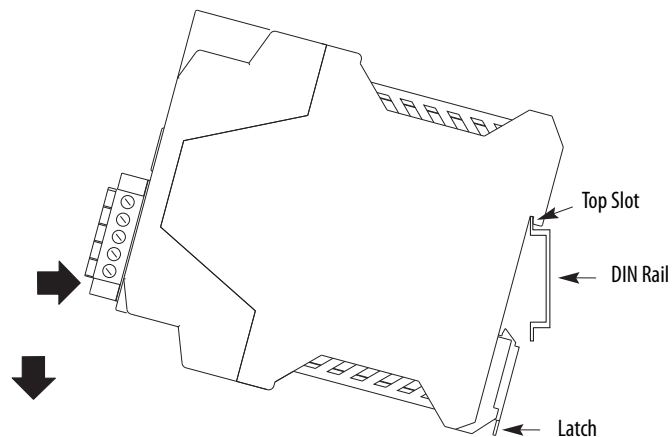
Mount the SmartGuard Controller

IMPORTANT For effective cooling:

- mount the controller on a horizontal DIN rail. Do not mount the controller vertically.
- provide a gap of at least 50 mm (2.0 in.) above and below the controller and 5 mm (0.20 in.) on each side.
- select a location where air flows freely or use an additional fan.
- do not mount the controller over a heating device.

The controller cannot be panel-mounted. Follow these steps to mount the controller to an EN50022-35x7.5 or EN50022-35x15 DIN rail.

1. Hook the top slot over the DIN rail.
2. Snap the bottom of the controller into position while pressing the controller down against the top of the rail.



3. Attach end plates to each end of the DIN rail.

To remove the controller from the DIN rail, use a flathead screwdriver to pull down the latch and lift the controller off of the rail. The 1752-L24BBB controller has one latch and the 1752-L24BBBE controller has two latches on the bottom of the controller.

Grounding the SmartGuard Controller



ATTENTION: This product is grounded through the DIN rail to chassis ground. Use zinc plated yellow-chromate steel DIN rail to assure proper grounding. The use of other DIN rail materials (for example, aluminum or plastic) that can corrode, oxidize, or are poor conductors, can result in improper or intermittent grounding. Secure DIN rail to mounting surface approximately every 200 mm (7.8 in.) and use end anchors appropriately.

You must provide an acceptable grounding path for each device in your application. Functionally ground the controller through its V0/G0 power connection.

In addition, if you are using the 1752-L24BBBE controller, you should connect the Ethernet ground terminal to an acceptable ground.

Figure 4 - Ethernet Ground



Refer to the Industrial Automation Wiring and Grounding Guidelines, publication [1770-4.1](#), for additional information.

Connecting a Power Supply

Power for the controller is provided via an external 24V dc power source. The output hold time must be 20 ms or longer.

To comply with the CE Low Voltage Directive (LVD), DeviceNet connections and I/O must be powered by a dc source compliant with Safety Extra Low Voltage (SELV) or Protected Extra Low Voltage (PELV).

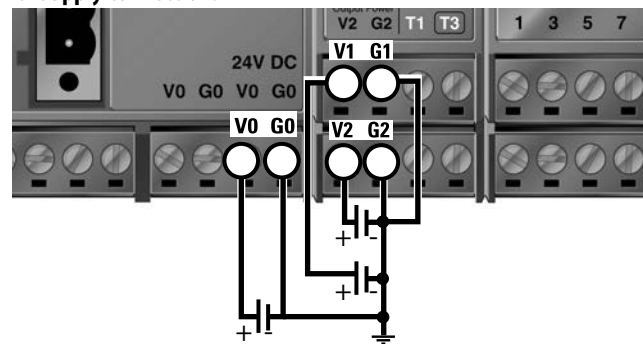
To comply with UL restrictions, DeviceNet connections and I/O must be powered by dc sources whose secondary circuits are isolated from the primary circuit by double insulation or reinforced insulation. The dc power supply must satisfy the requirements for Class 2 circuits or limited voltage/current circuits defined in UL 508.

TIP The following Allen-Bradley 1606 power supplies are SELV- and PELV-compliant, and they meet the isolation and output hold-off time requirements of the SmartGuard 600 controller:

- 1606-XLP30E
- 1606-XLP72E
- 1606-XLSDNET4
- 1606-XLP50E
- 1606-XLP95E
- 1606-XLP50EZ
- 1606-XLDNET4

The SmartGuard controller has three V/G terminal pairs that require a power connection. There are two V0/G0 pairs, but because they are internally connected, you only need to connect one V0/G0 pair. You can use the other pair to distribute power to other devices.

Figure 5 - Power Supply Connections



Making Communication Connections



ATTENTION: Do not connect or disconnect the communication cable with power applied to this controller or any device on the network, because an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

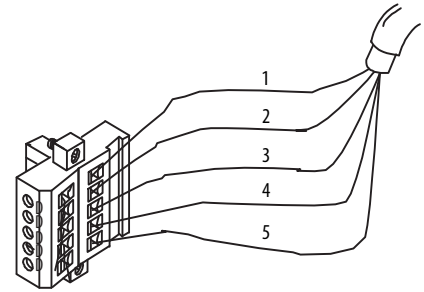
You can configure the network and controller on the DeviceNet network by using a 1784-PCD card inside your personal computer and RSNetWorx for DeviceNet software. You may also configure the network and controller by using the controller's USB port and RSNetWorx for DeviceNet software. In addition, you can configure the controller using RSNetWorx for DeviceNet software by connecting to the EtherNet/IP port and routing down to DeviceNet network.

Connect to the DeviceNet port

Follow these steps to connect to the DeviceNet port.

1. Wire the connector according to the colors on the connector.

Wire No.	Wire Color	Connects to
V+	Red	V+
CAN H	White	CAN H
Drain	—	Drain
CAN L	Blue	CAN L
V-	Black	V-



2. Attach the connector to the DeviceNet port.
3. Tighten the screws to 0.25...0.3 N•m (2.21...2.65 lb•in).

For detailed DeviceNet connection information, refer to the DeviceNet Media Design Installation Guide, publication [DNET-UM072](#). Also refer to the Industrial Automation Wiring and Grounding Guidelines, publication [1770-4.1](#).

Connecting to USB Port

Connect the USB communication connector to your personal computer when you want to configure the network and controller by using RSNetWorx for DeviceNet software. Use a commercially available USB-A to USB-B male/male cable to make the connection.



ATTENTION: To reduce the potential for electromagnetic interference, the USB cable length must be less than 3 m (10 ft).

The USB port is intended for temporary programming purposes only and is not intended for permanent connection.



ATTENTION: If you connect or disconnect the USB cable with power applied to this module or any device on the USB network, an electrical arc could occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

Connecting to the Ethernet port

Depending on where you plan to route your cable you must select the correct cable for the environment. Shielded cable performs better than non shielded cable in industrial environments. In particular, if your application is in a high noise environment or your cable must be run in close proximity to noise radiating sources then you should plan to use shielded cables.

You should consider shielded cables if your application includes one or more of the following:

- spot welding control
- Motor Control Centers
- drives greater than 10 Hp
- induction welding processes
- proximity to high-power RF radiation
- electrostatic processes
- high current devices (greater than 100 A)

IMPORTANT Shields play an important role in providing noise immunity for your system. However, an improperly installed shielded cable can cause problems due to voltage offsets in your grounding system. To help minimize the effects of ground offsets you will need to isolate the shield at one end of the cable. In this case the shield should be isolated at the device, not at the switch.

Use an RJ45 connector to connect the controller to the EtherNet/IP network. When connecting to the SmartGuard controller to a switch or a hub, use a

standard Ethernet cable. When connecting the SmartGuard controller directly to your personal computer or a NIC card, use a cross-over (null modem) cable.



ATTENTION: The cable length must be less than 100 m (328 ft) between hub and nodes.



WARNING: If you connect or disconnect the Ethernet cable with power applied to this controller or any other device on this network, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

Pin No.	Pin Name	Pin placement
8	Not used	
7	Not used	
6	RD-	
5	Not used	
4	Not used	
3	RD+	
2	TD-	
1	TD+	

Wiring the SmartGuard 600 Controller

Use cables of 30 m (98 ft) or less.

Attribute	Value
Wire type	Copper
Wiring category ⁽¹⁾	2 - on power, signal, and communication ports
Wire size	For power supply and I/O, use 0.2...2.5 mm ² (12...24 AWG) solid wire, or 0.34...1.5 mm ² (16...22 AWG) stranded flexible wire. Before connecting, prepare stranded wires by attaching ferrules with plastic insulation collars (DIN 46228-4 standard compatible).
I/O Terminal Screw Torque	0.56...0.79 N·m (5...7 lb·in)

(1) Use this Conductor Category information for planning conductor routing. Refer to Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1.

Terminal Designation	Description
V0	Power terminal for internal circuit (logic).
G0	Power terminal for internal circuit (logic).
V1	Power terminal for input circuits and test outputs.
G1	Power terminal for input circuits and test outputs.
V2	Power terminal for safety outputs.
G2	Power terminal for safety outputs.

IN0...IN15	Terminals for safety inputs.
TO...T3	These are test output terminals that can provide pulse test sources for safety inputs IN0...IN15. T3 can also support wire off detection and burned out bulb detection for a load such as a muting lamp.
OUT0...OUT7	Terminals for safety outputs.



ATTENTION: If you connect or disconnect wiring while the field-side power is applied, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

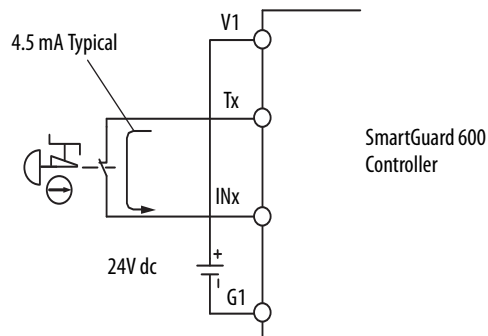


ATTENTION: If you connect or disconnect the removable terminal block (RTB) while the field-side power is applied, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

IMPORTANT Prepare stranded wires by attaching ferrules with plastic insulation covers (compliant with the DIN 46228-4 standard). Ferrules similar in appearance but not compliant may not match the terminal block on the controller.

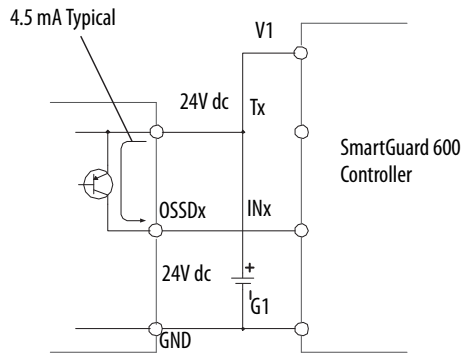
When safety devices are connected via test outputs to an input circuit on the SmartGuard controller, we recommend the length of the wire to be 30 m (98.4 ft) or less.

Figure 6 - Input Devices with Mechanical Contact Outputs



Devices, such as light curtains, with current-sourcing PNP semiconductor outputs send a signal to the SmartGuard 600 controller safety input terminal and do not use a test output.

Figure 7 - Input Devices with PNP Semiconductor Outputs



Wire Output Devices



ATTENTION: Serious injury may occur due to a loss of required safety functions.

Do not connect loads beyond the rated value of safety or test outputs.

Do not use test outputs as safety outputs.

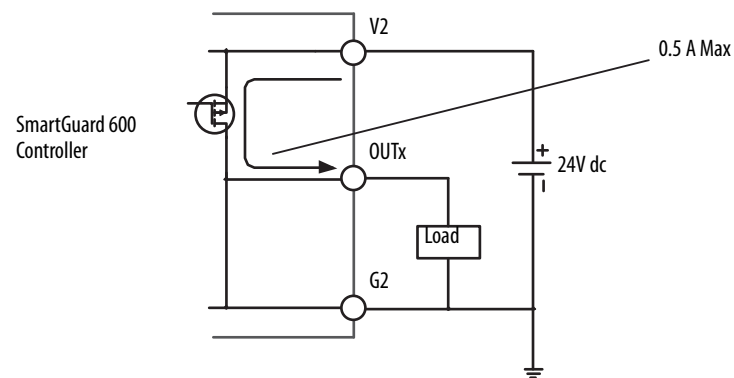
Wire the controller properly so that the 24V dc lines do not touch the safety or test outputs.

Do not apply the power supply to the test output terminals.

Ground the 0V line of the power supply for external output devices so that the devices do not turn on when the safety output line or the test output line is grounded.

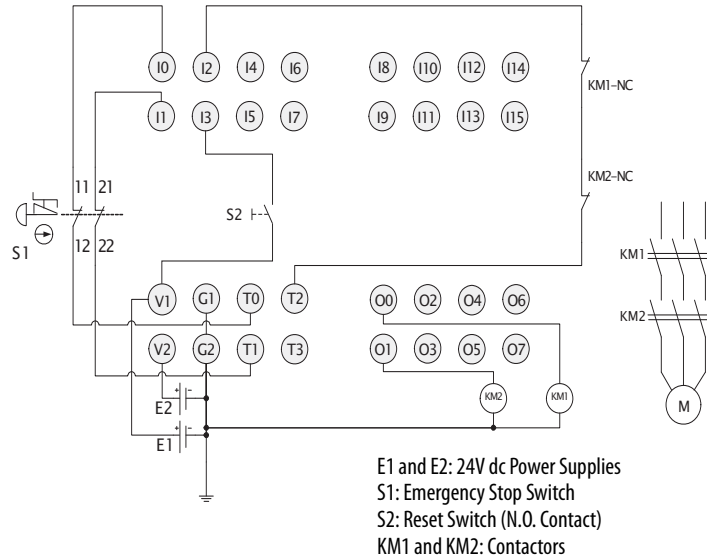
Separate I/O cables from high voltage or high current lines.

Figure 8 - Output Device Wiring



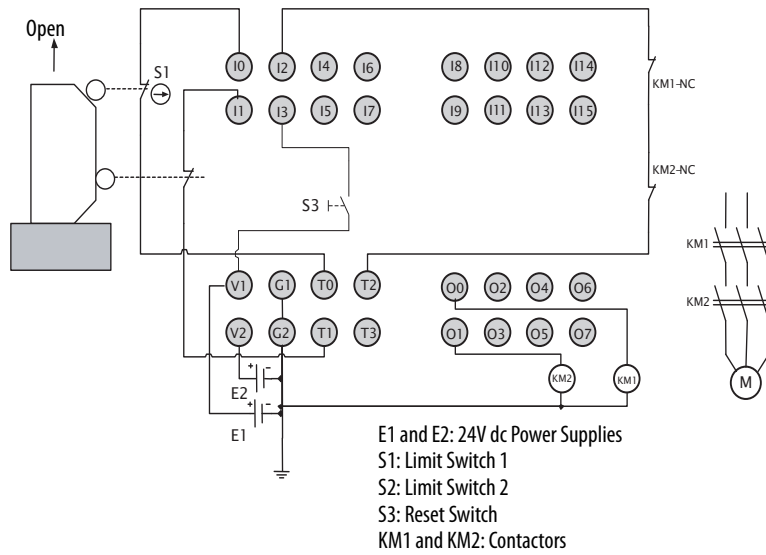
Wiring Examples

Figure 9 - ESTOP



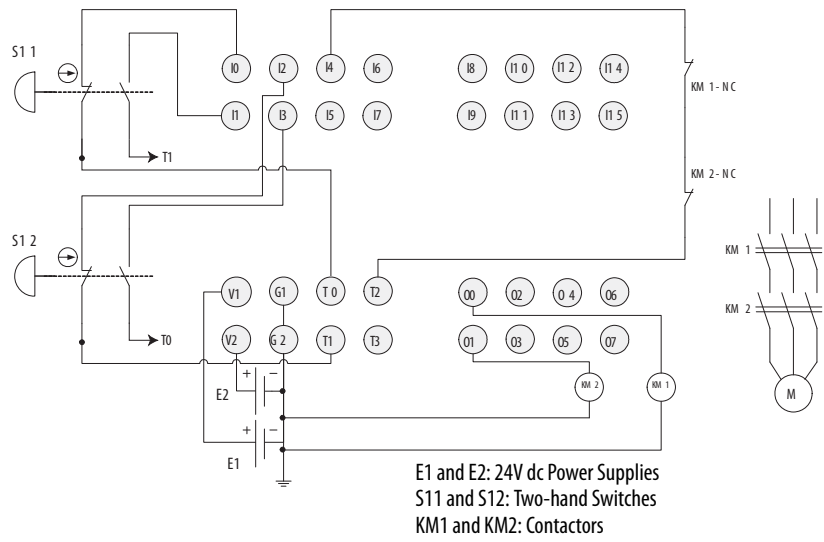
Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 10 - Safety Gate



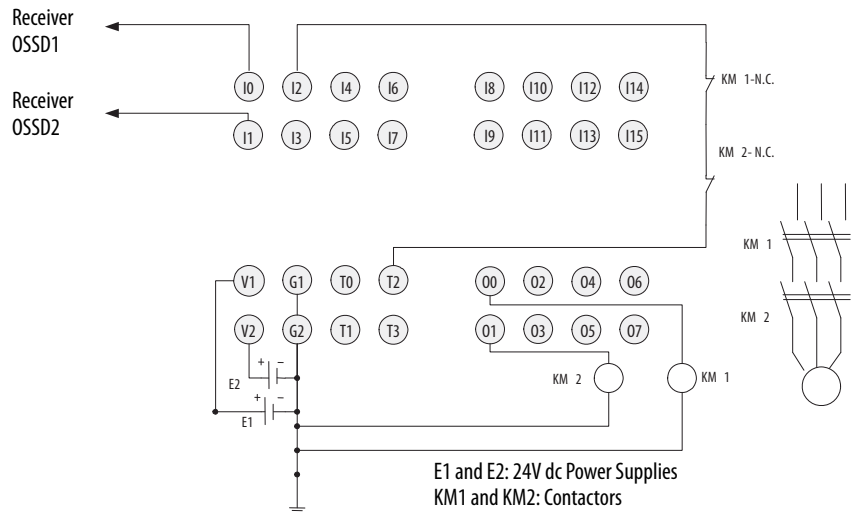
Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 11 - Two-hand Switch



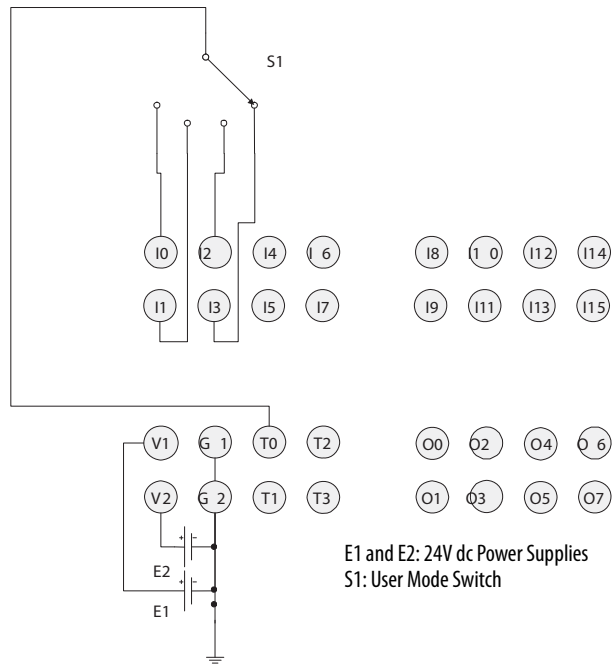
Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 12 - Light Curtain



Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 13 - User Mode Switch



E1 and E2: 24V dc Power Supplies
S1: User Mode Switch

Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Notes:

Set Up Your DeviceNet Network

Introduction

Topic	Page
Connecting a Computer to the DeviceNet Network	41
Commission All Nodes	42
Browse the Network	44
Configuration Signature	44
Safety Reset (optional)	45
Setting Passwords (optional)	47

Connecting a Computer to the DeviceNet Network

To access a network, either:

- connect directly to the network.
- connect to a different network and browse to the desired network via a linking device.

TIP You can browse the DeviceNet and EtherNet/IP networks through the USB port of the SmartGuard controller.

The SmartGuard USB to DeviceNet bridging capability is limited. For example, you cannot configure a 1734-ADN nor any POINT I/O™ modules. You also cannot configure a 1753-DNSI module through the SmartGuard controller. Use a 1784-PCD card instead for these operations.

Once you choose a network:

- install the communication card, if required.
- determine any network parameters for the computer, such as a network address.
- connect the computer to the network by using the correct cable.

IMPORTANT The first time you connect a SmartGuard controller to your personal computer by using the USB port, Windows goes through its device recognition sequence and prompts you for USB drivers. The driver is on the RSLinx Classic CD in the SmartGuardUSB-KernelDrivers folder.

Configure a Driver for the Network

1. Start RSLinx software.
2. Click Configure Driver.

- From the pull-down the list of Available Driver Types, add the driver for your network.

Network	Driver
RS-232	RS-232 DF1 devices
EtherNet/IP	Ethernet devices
DeviceNet	DeviceNet drivers
USB	SmartGuard USB Driver

- Configure the driver.

The settings you make are dependent upon the network you choose and whether you are using a communication card or interface module.

Make Sure the Driver Works

- Check the Configure Drivers dialog box to make sure that the driver is running.
- Close the dialog box.
- Open the RSWho dialog box.
- Double-click the driver to see the network.

Commission All Nodes

If you have not specifically set the node address and communication rate of your devices by using hardware switches, you will need to commission each device by using RSNetWorx for DeviceNet software.

Before you can use RSNetWorx for DeviceNet's Node Commissioning tool, your computer and your DeviceNet devices must be connected to the DeviceNet network.

Use the Node Commissioning tool in RSNetWorx for DeviceNet software to set the node address and/or communication rate of the SmartGuard controller and other DeviceNet devices.

Follow the guidelines on [page 26](#) when selecting node addresses for your DeviceNet network.

IMPORTANT To allow the node address to be set by using the Node Commissioning tool in RSNetWorx for DeviceNet software, set the node address rotary switch on the controller to a value from 64...99.

See [page 26](#) for information on setting the node address by using the rotary switch.

Follow these steps to use the Node Commissioning tool.

1. Within RSNetWorx for DeviceNet software, choose Tools>Node Commissioning.
2. Click Browse on the Node Commissioning dialog box to select a device by browsing the network.

You can browse through the SmartGuard USB port or the Ethernet/IP port to reach the DeviceNet port.

3. Select the DeviceNet network in the left panel.
4. Select the device you want to commission in the right panel and click OK.
5. Select the desired value if you want to change the communication rate of the device.

IMPORTANT The communication rate of the device will not update until the device is power-cycled or reset.

6. On the Node Commissioning dialog box, type the new address for the device and click Apply.

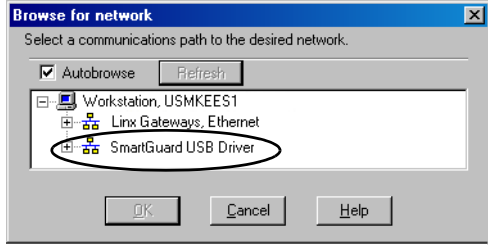
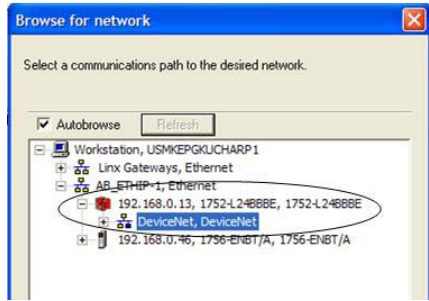
A confirmation message tells you if the operation was successful.


IMPORTANT To change the node address of a Safety device, you must first reset the safety network number (SNN) to an uninitialized state by performing a safety reset as described on [page 45](#).

Browse the Network

Follow these steps to browse the network.

1. Determine your connection type.

If you are using this connection type	Then
DeviceNet network	Go to step 2.
USB Port	<p>Follow these steps to configure a path to the DeviceNet network.</p> <p>A. From the Network menu, choose Properties.</p> <p>B. On the DeviceNet dialog box, click Set Online Path.</p> <p>C. On the Browse for Network dialog box, select the desired path and click OK.</p> 
EtherNet/IP Network	<p>Follow these steps to configure a path to the DeviceNet network.</p> <p>A. From the Network menu, choose Properties.</p> <p>B. On the DeviceNet dialog box, click Set Online Path.</p> <p>C. On the Browse for Network dialog box, select the desired path and click OK.</p> 

2. Click the online icon .
3. Wait for the Browse Network operation to complete.

As the network is browsed, all of the devices on the network will appear in RSNetWorx for DeviceNet software.

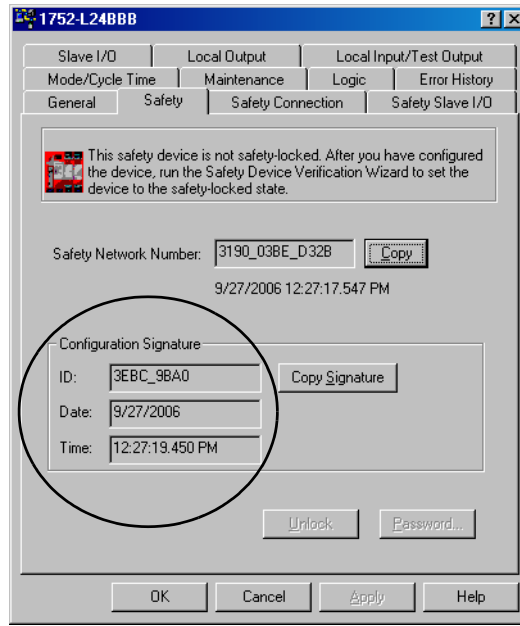
4. Verify that all of your nodes are visible.
5. Save your project in RSNetWorx for DeviceNet software.

Configuration Signature

Each safety device has a unique configuration signature, which identifies its configuration to verify the integrity of configuration data during downloads, connection establishment, and module replacement.

The configuration signature is composed of an ID number, a date, and a time and is set automatically by RSNetWorx for DeviceNet software when a configuration update is applied to the device. The configuration signature is found on the Safety tab of the Device Properties dialog box. It is also displayed on the alphanumeric display, on character at a time, when the service switch is pressed.

Figure 14 - SmartGuard 600 Controller Configuration Signature

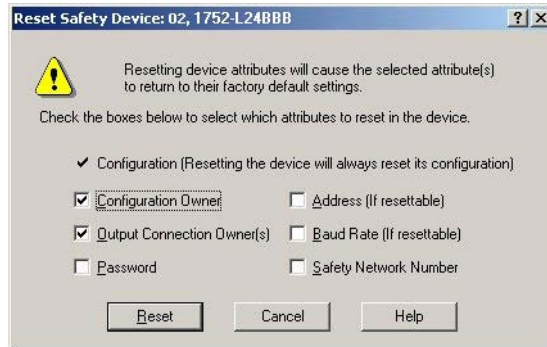


The configuration signature is read during each browse and whenever the Device Properties dialog box is launched while the software is in the Online mode. RSNetWorx for DeviceNet software compares the configuration signature in the software (offline) device configuration file to the configuration signature in the online device. If the configuration signatures do not match, you are prompted to upload the online device configuration or download the software device configuration to resolve the mismatch.

Safety Reset (optional)

If you need to reset the safety device's attributes to the out-of-box default state, you can do so via the Reset Safety Device dialog box.

You can reset the attributes shown on the Reset Safety Device dialog box by checking their associated checkbox. Leaving an attribute checkbox blank preserves that attribute's setting during the safety reset operation.



1. Open the Reset Safety Device dialog box by clicking on the device in the RSNetWorx for DeviceNet software graphic view and selecting Reset Safety Device from the Device menu.
2. Check the attributes you want to reset.

Attribute	Reset Behavior
Configuration	The configuration of the device is erased as a result of any safety reset action.
Configuration Owner	Check this checkbox to reset the device's configuration owner. The configuration software is always the configuration owner for SmartGuard controllers.
Output Connection Owner(s)	Check this checkbox to reset any existing output connection owners. The next device that accesses an output connection point following the safety reset becomes the output connection owner.
Password	Check this checkbox to reset the device password. You must know the current device password to reset a password from the Reset Safety Device dialog box.
Address	Check this checkbox to reset the device's software-configured node address to 63. If the device's node address has been set by using switches, the reset operation has no effect on the node address.
Baud Rate	Check this checkbox to reset the device's communication rate to 125 Kbps. If the device's communication rate has been set by using switches, the reset operation has no effect on the communication rate.
Safety Network Number	Check this checkbox to reset the device's safety network number (SNN).

3. Click Reset.

If the device is safety-locked, you are prompted to first unlock the device.



ATTENTION: Once unlocked, the device cannot be relied upon to perform safety operations.

You must test and verify the device's operation and run the Safety Device Verification Wizard to safety-lock the device before operating the device in a safety application.

4. Type the password when prompted, if you have set a password for the device.

Setting Passwords (optional)

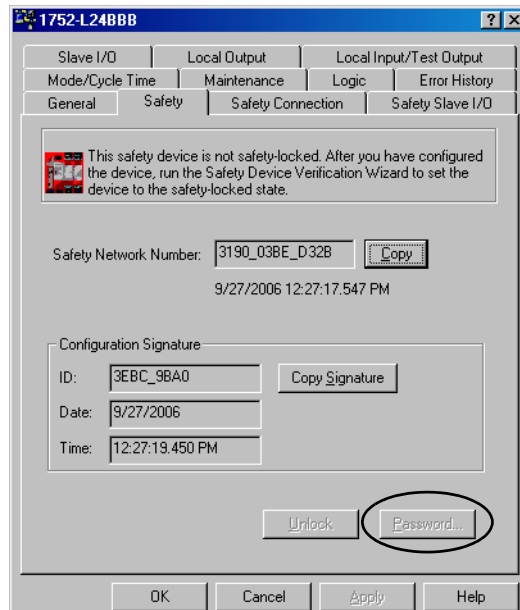
You can protect safety devices with a password to prevent changes to the configuration of the device by unauthorized personnel. When a password is set, the following operations require the password to be typed.

- Download
- Safety-configuration reset
- Safety-lock
- Safety-unlock

Set or Change a Password

Follow the steps below to set a password for a module.

1. Double-click the module to open the Device Properties dialog box.
2. Select the Safety tab.
3. Click Password.



TIP

You can also access the Set Device Password dialog box by either:

- clicking the module and choosing Set Password from the Device menu.
- right-clicking the module and choosing Set Password.

4. Type the old password, if one exists.
5. Type and confirm the new password.

Passwords may be from 1...40 characters in length and are not case-sensitive. Letters, numerals, and the following symbols may be used: ' ~ ! @ # \$ % ^ & * () _ + , - = { } | [] \ : ; ? / .

6. Click OK.

Forgotten Passwords

It is in the best interests of Rockwell Automation customers and partners that, where possible, user-defined configurations, programs, and intellectual property stored within a product remain protected from unauthorized disclosure and tampering. Definitive authorship or ownership of such user-defined content cannot be completely verified by Rockwell Automation.



ATTENTION: Rockwell Automation does not provide any form of password or security override services. That is why it is important that you implement a policy for managing passwords for your SmartGuard controller. If you apply a password to your SmartGuard controller and then forget it, there is no way for you to access the controller to reset it. You must then replace the controller by using one of the following procedures:

- New Product Satisfaction Return
 - Warranty Transaction
-

New Product Satisfaction Return

Use the New Product Satisfaction Return procedure if you forget the password within 24 hours of startup.

1. Contact Rockwell Automation Technical Support at <http://www.rockwellautomation.com/support>, explain that you have forgotten the password, and request a service ticket for a New Product Satisfaction Return.
2. Contact your Allen-Bradley distributor, provide the service ticket number, and request a New Product Satisfaction Return.

Warranty Transaction

Use the Warranty Transaction procedure if you forget the password after 24 hours of operation, and the product is still within its warranty period.

1. Contact your Allen-Bradley distributor and explain that you have forgotten the password.
2. Request a Warranty Transaction and specify that the transaction be handled as a Priority Exchange.

Set Up Your EtherNet/IP Network

Introduction

Topic	Page
Connecting a Computer to the EtherNet/IP Network	49
Connecting the SmartGuard 600 Controller to the EtherNet/IP Network	50
Bridging across Networks	56

Connecting a Computer to the EtherNet/IP Network

To access the EtherNet/IP network, either:

- connect directly to the network.
- connect to a different network and browse to the desired network via a linking device.

TIP You can browse the Ethernet network through the USB port of the SmartGuard controller.

The SmartGuard USB to Ethernet bridging capability is limited.

Once you choose a network:

- install the communication card, if required.
- determine any network parameters for the computer, such as a network address.
- connect the computer to the network by using the correct cable.

IMPORTANT The first time you connect a SmartGuard controller to your personal computer by using the USB port, the Windows operating system goes through its device recognition sequence and prompts you for USB drivers. The driver is on the RSLinx Classic CD in the SmartGuardUSB-KernelDrivers folder.

Configure a Driver for the Network

1. Start RSLinx software.

For the RSLinx software to locate new devices on the EtherNet/IP network, the driver can be set up (browse the remote subnet option) to look for a specific IP address and mask.

2. Click Configure Driver.
3. From the Available Driver Types pull-down menu, choose the driver for your network.

Network	Driver
RS-232	RS-232 DF1 devices
EtherNet/IP	Ethernet devices
DeviceNet	DeviceNet driver
USB	SmartGuard USB Driver

4. Configure the driver.

The settings you make are dependent upon the network you choose and whether you are using a communication card or interface module.

Make Sure the Driver Works

1. Check the Configure Drivers dialog box to make sure that the driver is running.

TIP You can configure the driver by using the Remote Subnet selection and by setting the IP address and mask to the value of the SmartGuard controller. This lets RSLinx software quickly find the device.

2. Close the dialog box.
3. Open the RSWho dialog box.
4. Double-click the driver to see the network.

Connecting the SmartGuard 600 Controller to the EtherNet/IP Network

IMPORTANT The SmartGuard controllers must not be directly connected to any network that is not protected from outside intrusion. For example, do not connect the SmartGuard 600 controller to an Ethernet network that is not protected with a firewall or other security measures.

Setting the IP Address

To configure the controller, define the IP address, subnet mask, and gateway.

Table 4 - EtherNet/IP Parameters

EtherNet/IP Parameter	Description
IP Address	The IP address uniquely identifies the controller. The IP address is in the form <i>xxx.xxx.xxx.xxx</i> , where each <i>xxx</i> is a number between 0 and 255. The following reserved values cannot be used: <ul style="list-style-type: none"> •127.0.0.1 •0.0.0.0 •255.255.255.255
Subnet Mask	Subnet addressing is an extension of the IP address scheme that allows a site to use a single network ID for multiple physical networks. Routing outside of the site continues by dividing the IP address into a net ID and a host ID via the class. Inside a site, the subnet mask is used to redivide the IP address into a custom network ID portion and host ID portion. This field is set to 0.0.0.0 by default. If you change the subnet mask of an already-configured controller, you must cycle power for the change to take effect.
Gateway	A gateway connects individual physical networks into a system of networks. When a node needs to communicate with a node on another network, a gateway transfers the data between the two networks. This field is set to 0.0.0.0 by default.

You can configure your controller via two options; configuring through RSLinx Classic software or through a BOOTP utility. Refer to [page 51](#) for using BOOTP or to [page 54](#) for using RSLinx software.

Using BOOTP to Set the IP Address

BOOTP (bootstrap protocol) is a low-level protocol that TCP/IP nodes use to obtain start-up information. An IP address is not set until a BOOTP reply has been received. BOOTP lets you dynamically assign IP addresses to processors on the Ethernet link.

To use BOOTP, a BOOTP server must exist on the local Ethernet subnet. The server is a computer that has BOOTP server software installed and reads a text file containing network information for individual nodes on the network.

The host system's BOOTP configuration file must be updated to service requests from the SmartGuard controller. In the default state (out of the box), the SmartGuard controller requires the use of a BOOTP server to set its IP address.

Refer to [Setting the IP Address](#) for the parameters that need to be configured.

TIP You can use any commercially-available BOOTP server. If you do not have BOOTP server capabilities on your network, and you want to dynamically configure the SmartGuard controller, you can download the free Rockwell Automation BOOTP server from <http://www.rockwellautomation.com/rockwellsoftware/download/>.

When BOOTP is enabled, the following events occur at power up:

- The processor broadcasts a BOOTP-request message containing its hardware address over the local network or subnet.
- The BOOTP server compares the hardware address with the addresses in its look-up table.
- The BOOTP server sends a message back to the processor with the IP address and other network information that corresponds to the hardware address it received.

With all hardware and IP addresses in one location, you can change IP addresses in the BOOTP configuration file if your network needs changed.

The BOOTP request can be disabled by clearing the BOOTP Enable parameter in the Port Configuration tab. When BOOTP Enable is cleared (disabled), the SmartGuard controller uses the existing channel configuration data.

IMPORTANT When BOOTP protocol is used to set the IP address in a SmartGuard controller, the SmartGuard controller must receive an initial IP address from the server before the BOOTP protocol can be turned off. It can be disabled by using the Module Configuration function in RSLinx software.

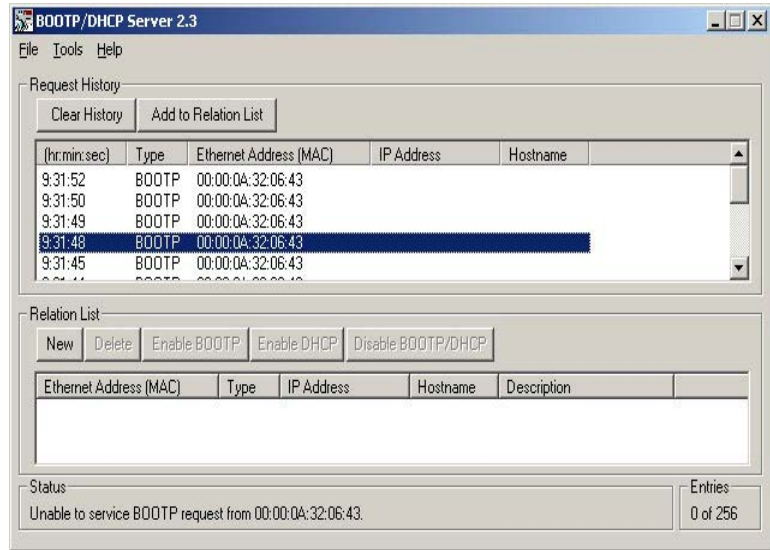
Use the Rockwell BOOTP Utility

The Rockwell BOOTP utility is a standalone program that incorporates the functionality of standard BOOTP software with a user-friendly graphical interface. You can download it from <http://www.rockwellautomation.com/rockwellsoftware/download/>. The device must have BOOTP enabled (factory default) to use the utility.

To configure your device by using the BOOTP utility, perform the following steps.

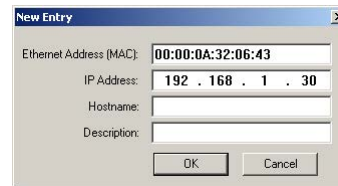
1. Run the BOOTP software.

In the BOOTP Request History panel you will see the hardware addresses of devices issuing BOOTP requests.



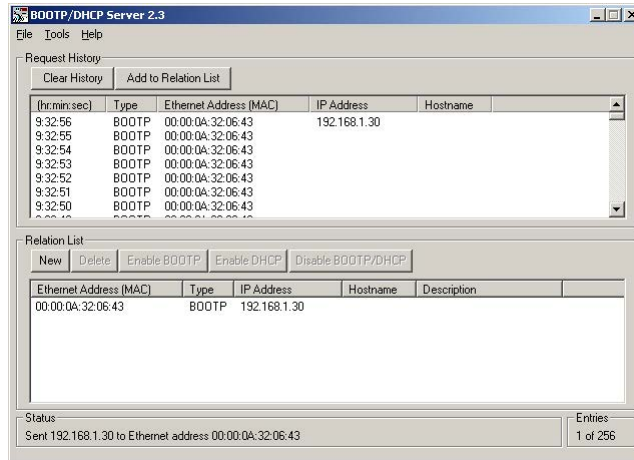
2. Double-click the hardware address of the device you want to configure.

You will see the New Entry pop-up window with the device's Ethernet Address (MAC).



3. Enter the IP Address (Hostname and Description are optional) that you want to assign to the device, and click OK.

The device will be added to the Relation List, displaying the Ethernet Address (MAC) and corresponding IP Address, Subnet Mask, and Gateway (if applicable).

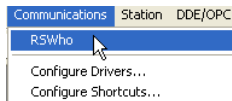


Use RSLinx Software to Set the IP Address

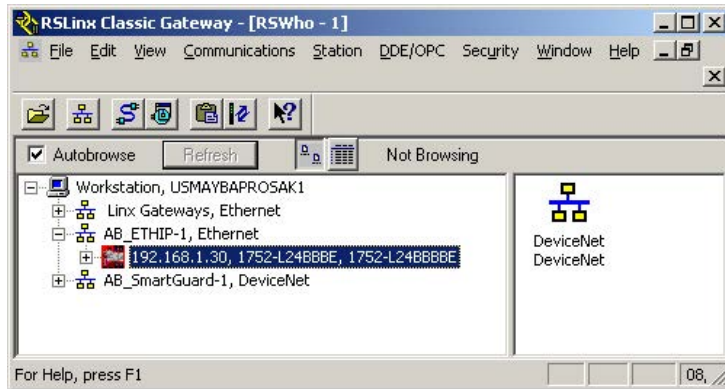
After you have used the BOOTP utility to initially set the IP address of a brand new SmartGuard 600 controller, you can then use RSLinx software to change the IP address. If this is the functionality you want, be sure to disable the BOOTP utility in the SmartGuard controller, or otherwise every time you apply power to the SmartGuard controller, it will power up in the BOOTP mode.

To use RSLinx software to configure the IP address parameters in the 1752-L24BBBE controller, perform this procedure.

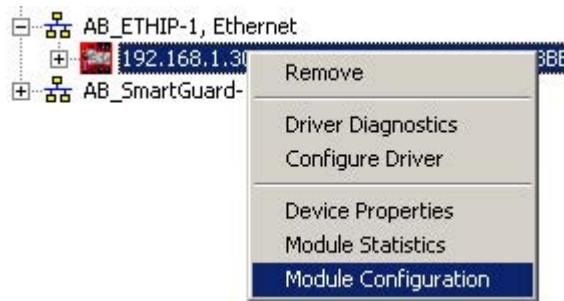
1. Make sure the 1752-L24BBBE controller is installed and powered up.
2. Start RSLinx software.
3. From the Communications pull-down menu, choose RSWho.



The RSWho dialog box appears.

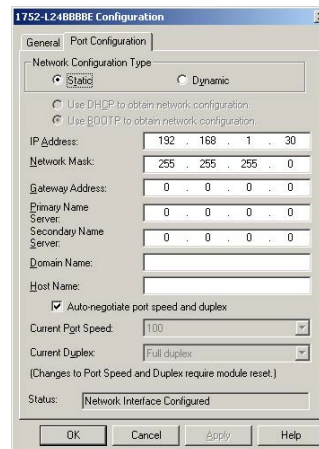


4. Navigate in RSWho to the Ethernet network.
5. Right-click the SmartGuard controller and choose Module Configuration.



TIP The module configuration option is also shown when viewing the SmartGuard controller from DeviceNet software, but the IP configuration is applied only when it is executed directly from the EtherNet/IP network.

The Module Configuration dialog box appears.



6. Click the Port Configuration tab.
7. For Network Configuration Type, click Static to permanently assign this configuration to the port.

IMPORTANT If you select Dynamic, on a power cycle, the controller clears the current IP configuration and resumes sending BOOTP requests. Refer to [page 52](#) for more information.

- a. In the IP Address field, type the IP address.
 - b. In the Network Mask field, type the network mask address.
 - c. In the Gateway Address field, type the gateway address or leave as all zeros.
 - d. In the Primary Name Server field, type the address of the primary name server or leave as zeros.
 - e. In the Secondary Name Server field, type the address of the secondary name server or leave as zeros.
 - f. In the Domain Name field, type the domain name or leave blank.
 - g. In the Host Name field, type the host name or 'SmartGuard ENIP'.
8. Configure the port settings.

To	Then
Use the default port speed and duplex settings	Leave checked the Auto-negotiate port speed and duplex checkbox. Important: The default port speed is 100, and the default duplex setting is Full.
Manually configure your port's speed and duplex settings.	<ol style="list-style-type: none"> a. Uncheck the Auto-negotiate port speed and duplex checkbox. b. From the Current Port Speed pull-down menu, choose a port speed. c. From the Current Duplex pull-down menu, choose Half Duplex.

9. Click OK.

Bridging across Networks

The 1752-L24BBBE controller supports the ability to bridge or route communication to various devices, depending on the capabilities of the platform and communication devices.

You have a bridge when you have a connection between communication devices on two networks. For example, a bridge device has both EtherNet/IP and DeviceNet connections, enabling Device 1 on the EtherNet/IP network to communicate with Device 2 on a DeviceNet network through the bridge.

EtherNet/IP Network to a DeviceNet Network

Here is a connection between the EtherNet/IP network and the DeviceNet network. The SmartGuard controller lets you use your personal computer that is connected to the EtherNet/IP network to configure the 1791DS module on the DeviceNet network by bridging through the SmartGuard controller.

IMPORTANT The bridging capability of the SmartGuard controller is limited. It is designed for configuring safety DIO modules on another network, but it should not be used to program other PLCs and must not be used as a bridging device during machine operation.

Figure 15 - EtherNet/IP Network to a DeviceNet Network

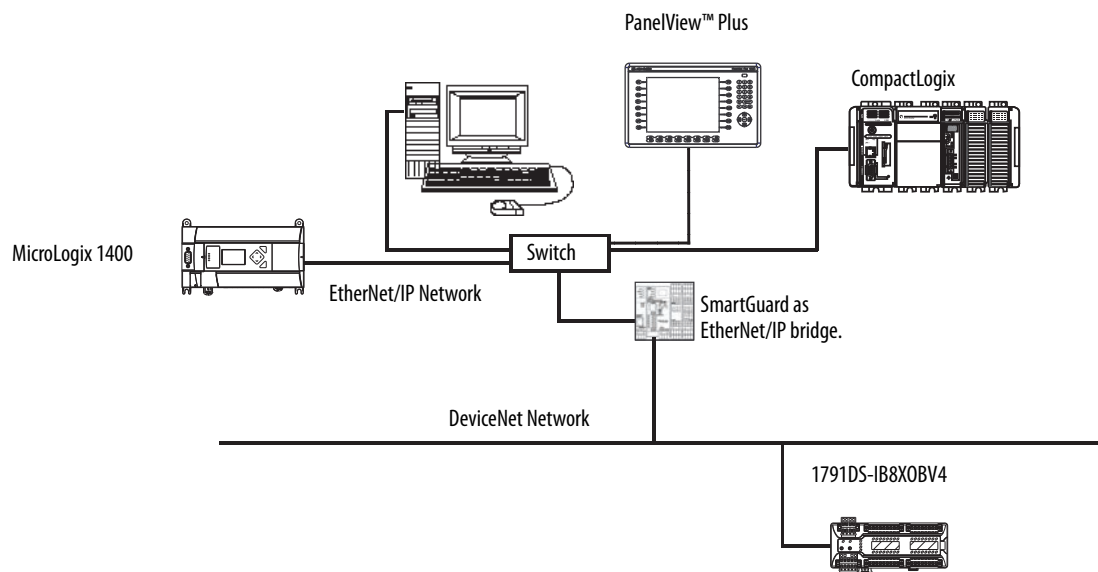
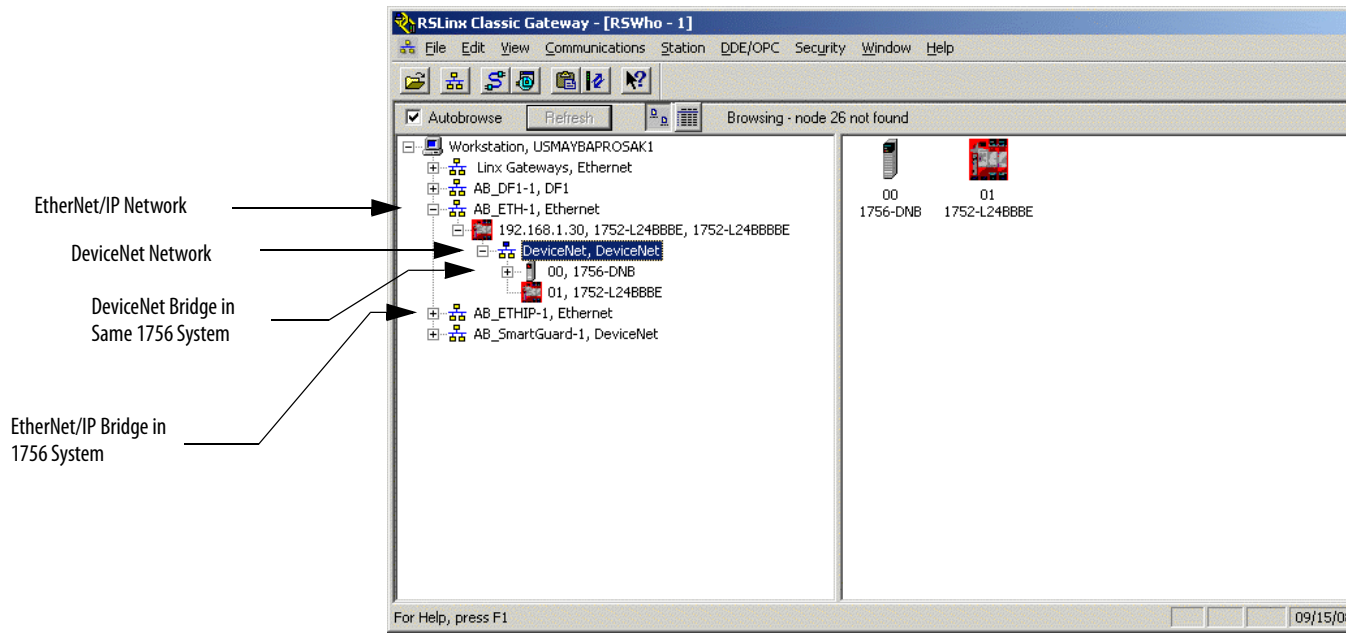


Figure 16 - EtherNet/IP Bridge Linking to a DeviceNet Network

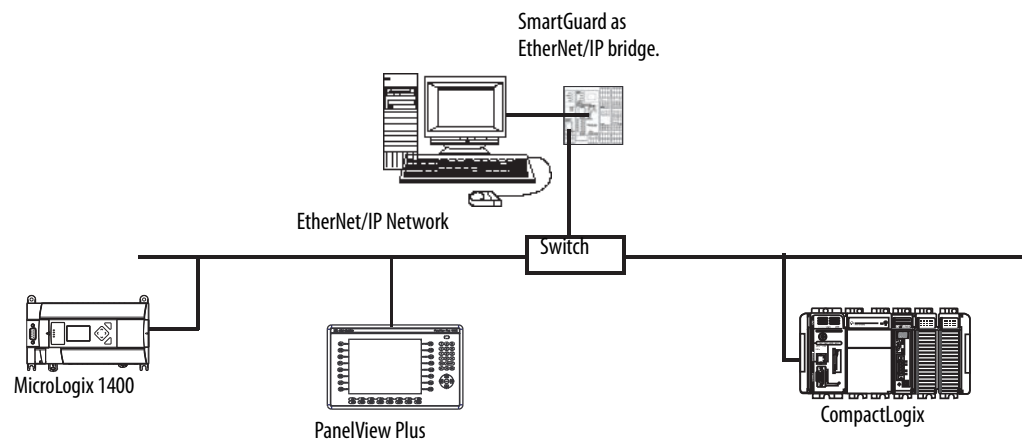


USB Port to the EtherNet/IP Network

The SmartGuard controller supports bridging from the USB port to the EtherNet/IP network. However, we recommend not using this feature but rather connecting directly to the EtherNet/IP network to configure devices other than the SmartGuard controller.

The SmartGuard controller can browse only on the Ethernet subnet that it is connected to. You could browse to a MicroLogix 1400 controller or to a CompactLogix controller, but you could not browse to a ControlLogix controller because you cannot route past the 1756-ENBT module in the ControlLogix chassis.

Figure 17 - USB Port to EtherNet/IP Network



Notes:

Manage the Safety Network Number

Introduction

Topic	Page
Safety Network Number (SNN) Formats	61
Assignment of the Safety Network Number (SNN)	62
Set the Safety Network Number (SNN) in All Safety Nodes	63
Safety Network Number (SNN) Mismatch	65
Safety Network Number (SNN) and Node Address Changes	65

Each DeviceNet Safety device must be configured with a safety network number (SNN). The combination of SNN and DeviceNet node address provides a unique identifier for every safety node in a complex industrial network. This unique identifier prevents data intended for a specific target node address on one DeviceNet subnet from being mis-routed and accepted by a node with the same node address on a different DeviceNet subnet.

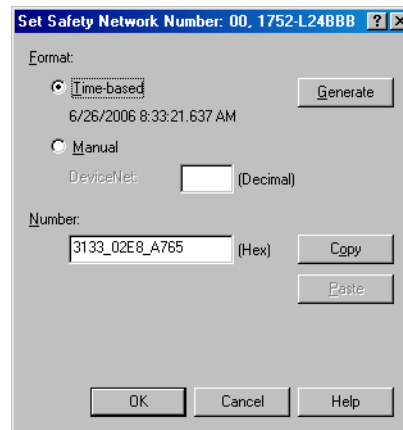
Safety network numbers assigned to each safety network or network sub-net must be unique. You must be sure that a unique safety network number (SNN) is assigned to each DeviceNet network that contains safety nodes.

Safety Network Number (SNN) Formats

The safety network number (SNN) can be either software-assigned (time-based) or user-assigned (manual). These two formats of the SNN are described in the following sections.

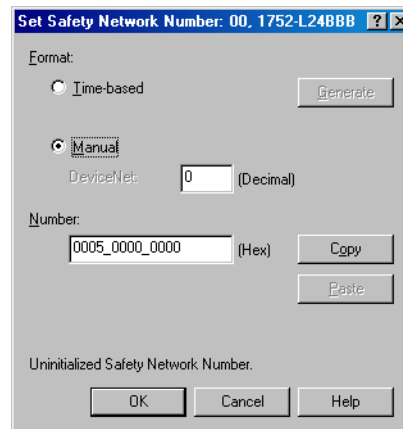
Time-based Safety Network Number (recommended)

In the time-based format, the safety network number (SNN) represents the date and time at which the number was generated, according to the personal computer running RSNetWorx for DeviceNet software.



Manual Safety Network Number (SNN)

In the manual format, the SNN represents typed values from 1...9999 decimal.



TIP Click Copy on the Set Safety Network Number dialog box to copy the SNN to the Windows clipboard.

Assignment of the Safety Network Number (SNN)

An SNN can be generated automatically via RSNetWorx for DeviceNet software or you can manually assign one. An automatically generated SNN is sufficient and recommended for most applications.

Automatic (time-based)

When a new safety device is added to the network configuration, a default SNN is automatically assigned via the configuration software, as follows.

- If at least one safety device already exists in the DeviceNet network configuration, subsequent safety additions to that network configuration are assigned the same SNN as the lowest-addressed safety device.
- If no other safety devices exist in the DeviceNet network configuration, a time-based SNN is automatically generated by RSNetWorx for DeviceNet software.

Manual

The manual option is intended for systems where the number of DeviceNet subnets and interconnecting networks is small, and where you might like to manage and assign each SNN in a logical manner pertaining to your specific application.

IMPORTANT If you assign an SNN manually, take care to be sure that system expansion does not result in duplication of SNN and node address combinations.

To set the SNN in a safety device via RSNetWorx for DeviceNet software, select the device in the hardware graphic view and choose Set Safety Network Number from the Device menu.

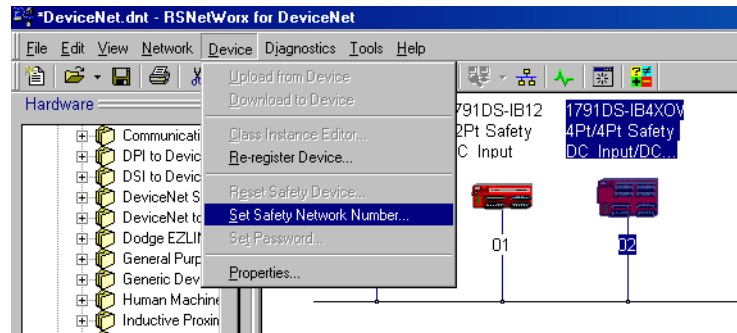
IMPORTANT When you set the SNN, the device is returned to its factory default configuration.

Set the Safety Network Number (SNN) in All Safety Nodes

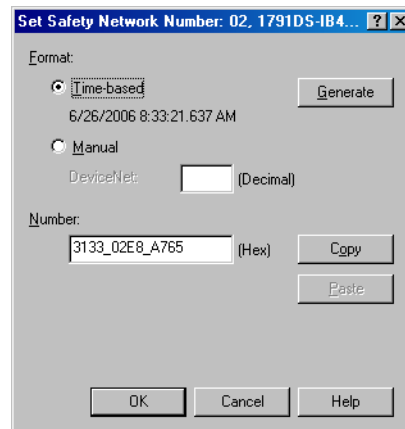
A time-based SNN is automatically generated when the first new safety device is added to the network. Subsequent additions to the network are assigned the same SNN as the lowest-addressed safety device. This automatic, time-based SNN is sufficient and recommended for most applications.

Follow these steps if you need to set the SNN for a particular device.

1. Click the target device in the hardware graphic view and choose Set Safety Network Number from the Device menu.



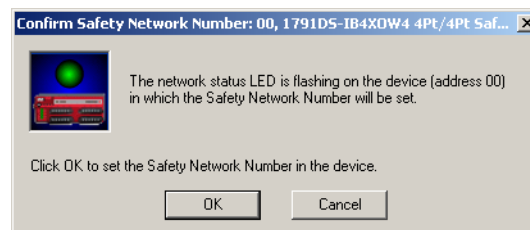
2. Choose Time-based and click Generate, or choose Manual and fill in a decimal number from 1...9999.



3. Click OK.

TIP You can use the copy and paste buttons on the Set Safety Network Number dialog box to copy and paste an SNN between devices and to make a record of the SNN.

4. Verify that the Network status indicator is rapidly alternating between red and green on the correct device and click OK.



Safety Network Number (SNN) Mismatch

RSNetWorx for DeviceNet software compares the offline SNN to the online SNN during each browse operation, one-shot or continuous, and during upload and download operations. If the SNNs do not match, RSNetWorx for DeviceNet software indicates an error with the SNN. The hardware graphic view displays the ! symbol over the safety device icon.

When online, RSNetWorx for DeviceNet software also checks for an SNN mismatch whenever a safety device's Device Properties dialog box is selected, either from the Device>Properties menu or by double-clicking the device. If an SNN mismatch condition exists, the Safety Network Number Mismatch dialog box is displayed.

The Safety Network Number Mismatch dialog box displays the online (device) SNN and the offline (software) SNN. You can choose to upload the device's SNN or download the offline SNN to resolve the mismatch.



If the device's SNN has not been initialized, the Device Safety Network Number field displays the default SNN: FFFF_FFFF_FFFF. When the device's SNN is FFFF_FFFF_FFFF, the Upload button is dimmed and unavailable.

Safety Network Number (SNN) and Node Address Changes

If you want to change the address of a safety device, the SNN must be uninitialized, or you must first reset the SNN.

Follow these steps to reset the SNN.

1. Select the device in the hardware graphic view.
2. From the Device menu, choose Reset Safety Device.
3. Check the Safety Network Number checkbox on the Reset Safety Device dialog box and click Reset.

Only the attributes selected on the dialog box are reset to their factory default settings. The Safety Reset only affects the safety device; the configuration in the RSNetWorx project is not lost.

See [Safety Reset \(optional\)](#) on page 45 for more information on the Safety Reset function.

TIP After the safety reset, the node address can be changed in RSNetWorx for DeviceNet software by double-clicking the safety device's node address in the graphic view. After changing the node address, right-click the device and click Download to Device to restore the safety device's SNN and configuration.

Configure Local I/O

Introduction

Topic	Page
Configure Local Safety Inputs	67
Configure Local Test Outputs	71
Configure Local Safety Outputs	73

Configure Local Safety Inputs

The controller has 16 local safety inputs that support the following features.

- Input circuit diagnosis — Test pulse sources can be used to monitor internal circuits, external devices, and external wiring.
- Input on- and off-delays — You can set input time filters of 0...126 ms in multiples of the controller cycle time. Setting input on- and off-delays helps reduce the influence of chattering and external noise.

IMPORTANT Input on- and off-delays must be added to the I/O response time. This will affect the system reaction time calculations.

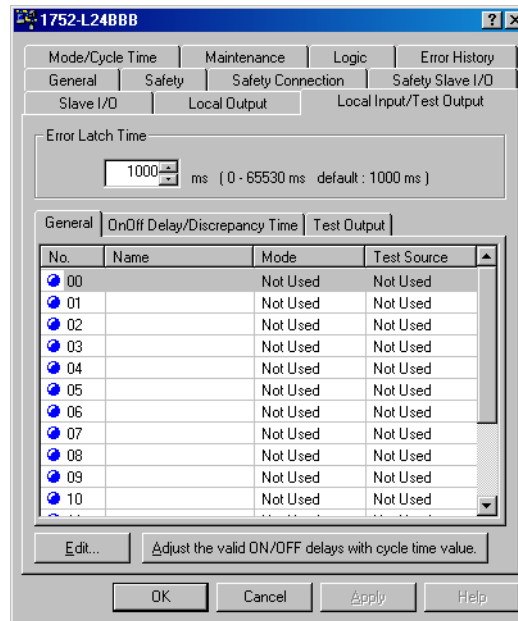
Refer to *SmartGuard Controllers Safety Reference Manual*, publication [1752-RM001](#), for information on calculating reaction times.

- Dual Channel mode — You can set Dual Channel mode for pairs of related local inputs. When Dual Channel mode is set, time discrepancies in data changes or input signals between two paired local inputs can be evaluated.

Follow these steps to configure local safety inputs.

1. Right-click the SmartGuard controller and choose Properties.

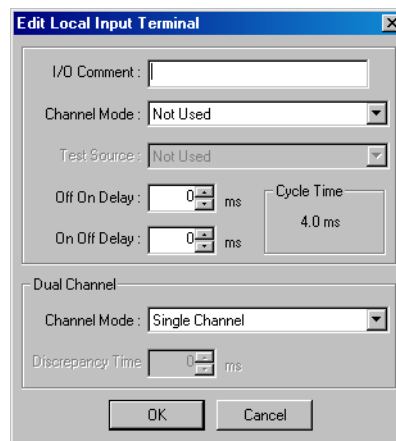
2. Select the Local Input/Test Output tab.



3. Set the Error Latch Time.

The error latch time 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 the error is removed, the error state is always latched for the configured error latch time. The error latch time is set from 0...65530 ms in 10 ms increments. The default is 1000 ms.

4. Select a safety input terminal and click Edit.



5. Type an I/O Comment.

The I/O comment typed here is used as an I/O tag name in the Logic Editor.

6. Set the Channel Mode for the safety input.

Channel Mode	Description
Not used	The input channel is not connected to an external device. This is the default.
Test pulse from test output	Use this mode when you are achieving a Category 4 input circuit. This mode assumes that you have connected your input device to a Pulse Test Source, and then wired to this input terminal. This enables detection of short circuits with the power supply line (positive side), earth faults, and short circuits with other input signal lines (channel-to-channel shorts). The controller must know that the input signal is being pulse-tested, or nuisance trips may occur. See the Example: Input Channel as Test Pulse from Test Output on page 70.
Used as a safety input	Use this mode to connect to a safety device with a semiconductor output, such as a light curtain.
Used as a standard input	Use this mode to connect to a standard (non-safety) device.

7. If you set the Channel Mode to Test pulse from test output, choose the test output to use in combination with the safety input by selecting it from the Test Source pull-down list.

TIP The Channel mode of the test output selected is automatically set to Pulse Test Output.

8. Set the Dual Channel mode and Discrepancy Time.

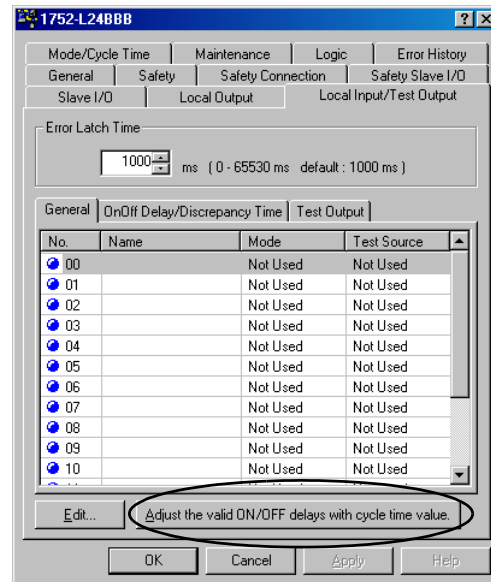
Setting Dual Channel mode enables the status of two inputs to be evaluated and reflected in I/O tags. The discrepancy time between changes in the status of two inputs can also be evaluated. The combinations that can be set are pre-defined. The Discrepancy Time can be set between 0...65530 ms in 10 ms increments. Both inputs must change state within the discrepancy time or an error occurs.

Channel Mode	Description
Single Channel	The safety input terminal is used independently.
Dual Channel Equivalent	The safety input terminal is used as a Dual Channel Equivalent with a pair safety input terminal.
Dual Channel Complementary	The safety input terminal is used as a Dual Channel Complement with a paired safety input terminal.

TIP The controller supports function blocks with functionality equivalent to Dual Channel mode. In many cases, annunciation and troubleshooting of system faults is easier when the function blocks are used to detect faults rather than the SmartGuard hardware. If you wish to use the function blocks to detect system faults, the safety inputs must be configured for single channel.

Automatic Adjustment of On- and Off-delay Times

If parameters that affect the cycle time are changed after the on- and off-delays have been set, you may not be able to close the Controller Properties dialog box because of an error in the parameter settings. If this occurs, you can re-adjust the on-and off-delay times based on the cycle time by using the Adjust valid ON/OFF delays with cycle time value button on the Local Input/Test Output tab.



Configure Local Test Outputs

These four independent test outputs can be used in combination with safety inputs. They can also be set for use as standard output terminals. The test pulse output features are listed below.

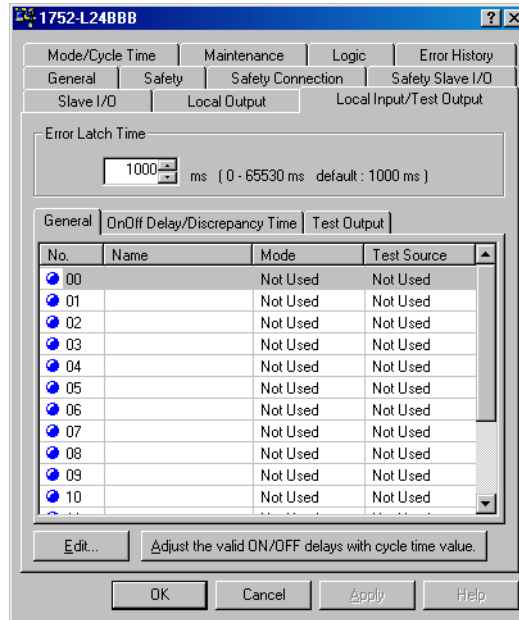
- Current monitoring for muting lamp — A wire off or burned out light bulb can be detected for the T3 terminal only.
- Overcurrent detection and protection — To protect the circuit, an output is blocked when an overcurrent is detected.



ATTENTION: Pulsed outputs must not be used as safety-related outputs (for example, for the control of safety-related actuators) because they are not safety rated.

Follow these steps to configure a test output.

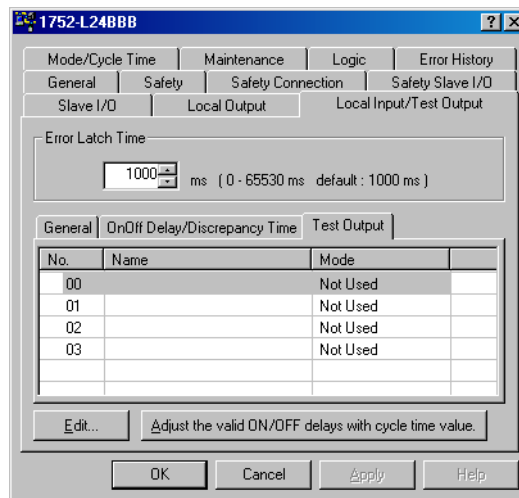
1. Right-click the SmartGuard controller and choose Properties.
2. Select the Local Input/Test Output tab.



3. Set the Error Latch Time.

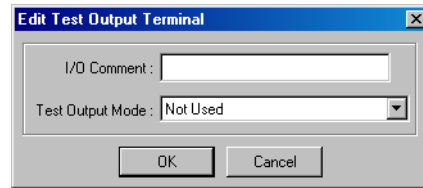
The error latch time applies to all safety inputs and test outputs. It sets the time to latch the error state when an error occurs in an input or output. Even if the error is removed, the error state is always latched for the configured error latch time. The error latch time is set from 0...65530 ms in 10 ms increments. The default is 1000 ms.

4. Select the Test Output tab.
5. Select a test output terminal and click Edit.



6. Type an I/O Comment.

The I/O comment typed here is used as an I/O tag name in the Logic Editor.



7. Choose a Test Output Mode from the pull-down list.

Test Output Mode	Description
Not used	The corresponding Test Output is not used.
Standard Output	Choose this mode when connecting to the output from a muting lamp or programmable logic controller. This output is used as a monitor output.
Pulse Test Output	Choose this mode when connecting a device with a contact output in combination with a safety input.
Muting Lamp Output	Choose this mode to specify a muting lamp output. This setting is supported only on the T3 terminal. When the output is on, disconnection of the muting lamp can be detected.

Configure Local Safety Outputs

The controller has eight local safety outputs that support the functions listed below.

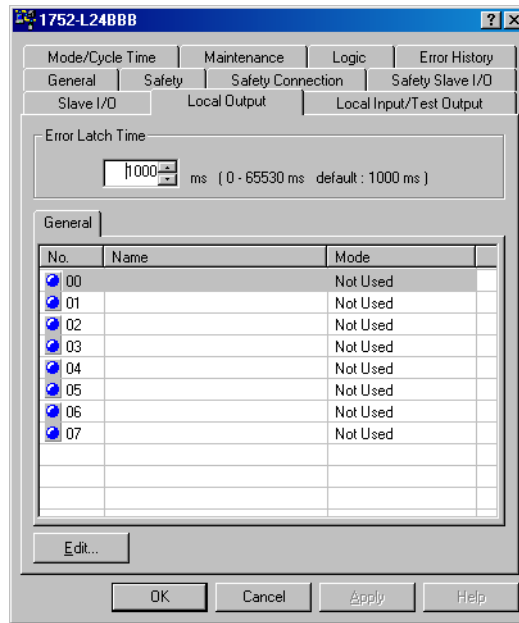
- Output circuit diagnosis — Test pulses can be used to diagnose the controller's internal circuits, external devices, and external wiring.
- Overcurrent detection and protection — To protect the circuit, an output is blocked when an overcurrent is detected.
- Dual Channel mode — Both of two paired outputs can be set into a safety state when an error occurs in either of the two paired local outputs without depending on the user program.

Follow these steps to configure a local safety output.

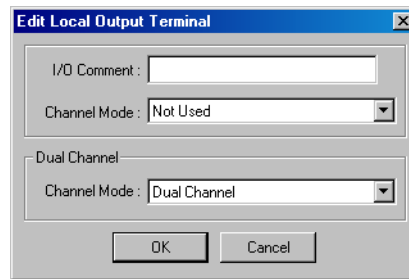
1. Right-click the SmartGuard controller and choose Properties.
2. Select the Local Output tab.
3. Set the Error Latch Time.

The error latch time applies to all safety outputs. It sets the time to latch the error state when an error occurs in an input or output. Even if the error is removed, the error state is always latched for the configured error latch

time. The error latch time is set from 0...65530 ms in 10 ms increments. The default is 1000 ms.



4. Select a safety output terminal and click Edit.



5. Type an I/O Comment.

The I/O comment typed here is used as an I/O tag name in the Logic Editor.

6. Set the Channel Mode for the safety output.

Channel Mode	Description
Not used	The output terminal is not connected to an output device.
Safety	A test pulse is not sent when the output is on. When the output is off, short circuits with the power supply line can be detected. Ground faults can also be detected.
Safety Pulse Test	A test pulse is sent when the output is on. This enables detection of short circuits with the power supply line (positive side) whether the output is on or off. Ground faults and short circuits between output signals can also be detected.

IMPORTANT If a safety pulse test is set, an off pulse signal (pulse width 580 μ s) is output to diagnose the output circuit when the safety output turns on. Check the input response time of the control device to make sure this output pulse will not cause malfunctions.

7. Set the Dual Channel mode for the safety output.

Setting Dual Channel mode enables an error to be detected if the two outputs from a user program are not equivalent. If an error is detected in one of two outputs circuits, both outputs to the device will become inactive.

Table 5 - Output Dual Channel Mode Settings

Channel Mode	Description
Single Channel	The safety output terminal is used independently.
Dual Channel	The safety output terminal is paired with another output terminal. The output can be turned on when both the output and the paired safety output are consistent.

Notes:

Configure Your Controller for DeviceNet Communication

Introduction

The SmartGuard controller can function simultaneously as a safety master, safety slave, or standard slave.

Topic	Page
Setting Up the Controller as a Safety Master	77
Setting Up the Controller as a Safety Slave	87
Setting Up the Controller as a DeviceNet Standard Slave	95
Reading and Writing to and from the SmartGuard Controller to a PanelView Plus Interface	100

Setting Up the Controller as a Safety Master

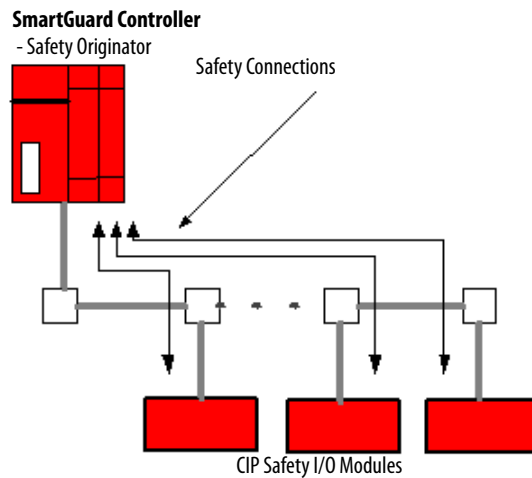
As a safety master, the controller can perform safety I/O communication with up to 32 connections, by using up to 16 bytes per connection. Connections may be either single-cast or multi-cast.

Different types of safety distributed I/O modules consume differing amounts of the 32 available connections. For example, an input-only module may consume 1 of the 32 connections (input connection), while a module with both inputs and outputs may consume 2 of the 32 safety connections (1 input connection and 1 output connection).

The configuration of the module also dictates how many safety connections it consumes. For example, the 1791DS-IB12 module has 12 safety inputs, no safety outputs, and 4 standard or pulse test outputs. If this module is configured for safety inputs only, it consumes 1 safety connection. However, if this module is configured to use safety inputs and standard outputs, it will consume 2 safety connections. Ultimately, the number and type of safety distributed I/O modules you have connected to the SmartGuard controller will determine the maximum number of modules the controller can control.

A master-slave relationship is established for each connection on the DeviceNet safety network, separate from the master-slave communication on the DeviceNet standard network. This enables the controller that is the safety master to control the safety connections.

Figure 18 - SmartGuard Controller as the Safety Master

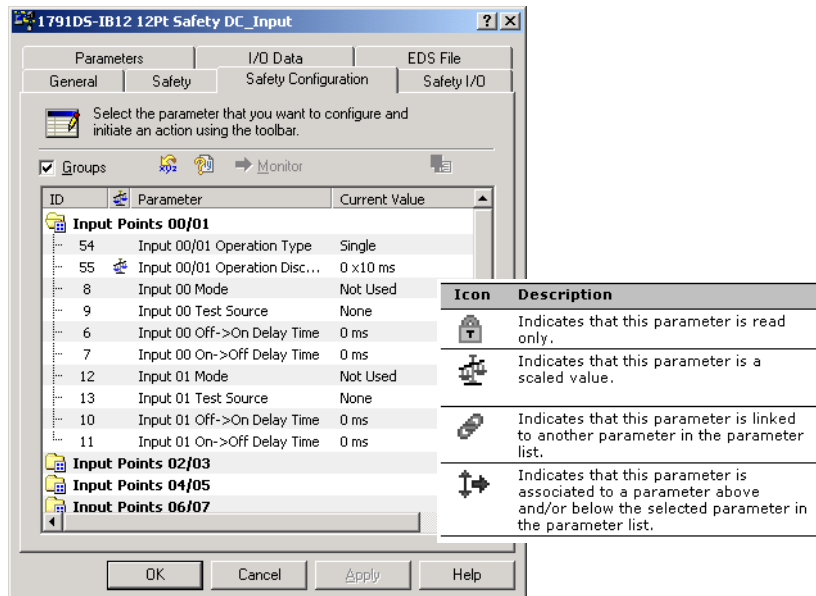


Configure CIP Safety I/O Targets on the DeviceNet Network

To configure your module, double-click the module in the graphic view or right-click the module and choose Properties.

Safety Input, Output, and Test Parameters

Safety parameters are configured by using the Safety Configuration tab on the Module Properties dialog box.



Single Channel versus Dual-channel Equivalent or Dual-channel Complementary

You can configure distributed I/O modules inputs for either Single- or Dual-channel mode. This tells the Guard I/O module whether to view the inputs individually (single-channel) or as input pairs (dual-channel). Dual-channel inputs may be configured as equivalent, where both inputs should always be the same or as complementary, where both inputs should always be opposite.

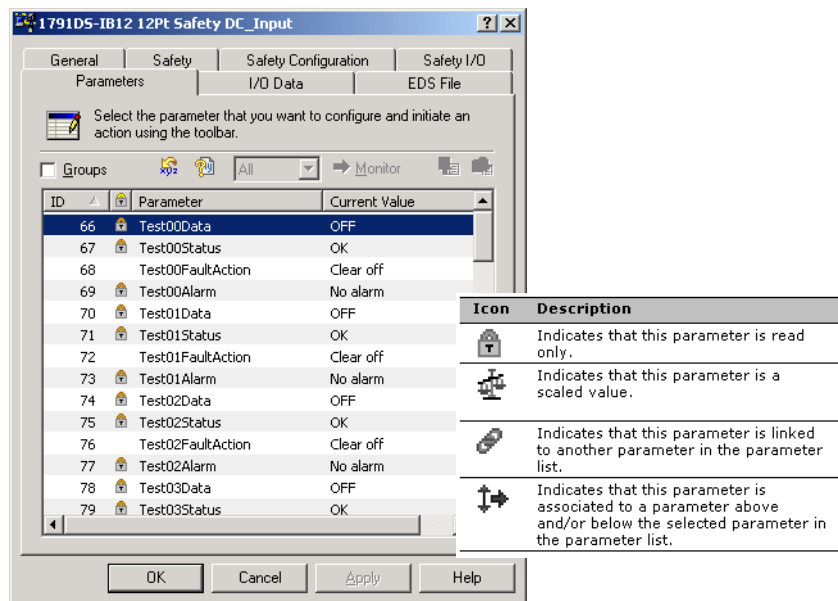
If configured as dual-channel, the Guard I/O module will always send the channel data to the SmartGuard controller as both channels LO or both channels HI. This means that the Inputs Inconsistent fault on the SmartGuard instruction will never occur.

If you want the SmartGuard instruction to perform the diagnostics of the safety input on the Guard I/O modules, configure the Guard I/O modules as a single channel. This will allow you to use the fault indicators provided by the SmartGuard instructions in your program, which is what we recommend.

If you want to perform the diagnostics of the safety input on the Guard I/O module with the module status indicators and status bits and not by using the SmartGuard instruction diagnostics, configure the Guard I/O module as dual-channel complementary or equivalent.

Standard Input and Output Parameters

1791DS modules shown here support standard data as well as safety data. Configure standard input and output parameters by using the Parameters tab on the Module Properties dialog box.



TIP Other devices may have different configuration options. Consult the user manual for your device for more information.

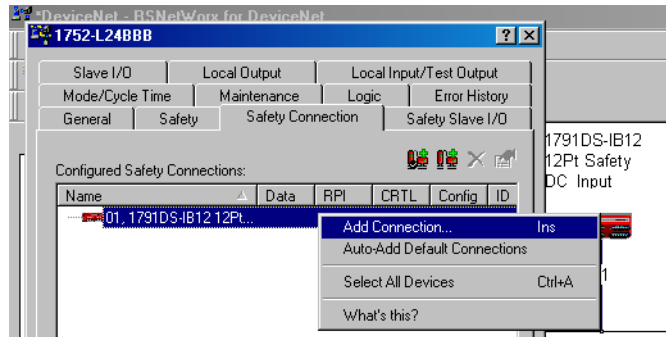
Download the Device Configurations

Once you have configured the safety and standard I/O module parameters, download the configuration to the modules. To do this in RSNetWorx for DeviceNet software, from the Device menu, choose Download to Device.

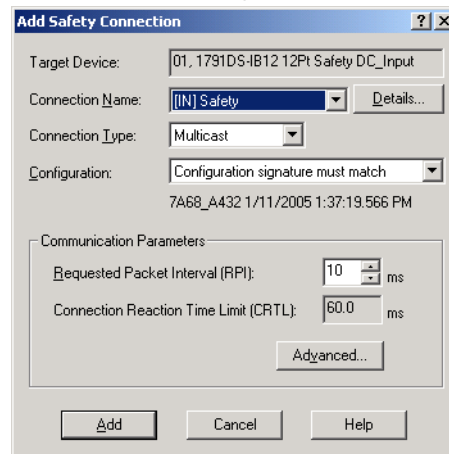
Configure Safety I/O Connections

Safety I/O connections are used to exchange data automatically with the safety slaves without user programming. To perform safety I/O communication with other slaves, you must configure the connection to the SmartGuard controller.

1. On the Safety Connections tab, right-click the I/O module and choose Add Connections to display all of the available connections.



The Add Safety Connection dialog box lets you configure a connection.



2. Select the desired connection by choosing the Connection Name.
3. Select a type of connection, either Multicast (input connections only) or Point-to-point (input or output connections).
4. Click Configuration signature must match.

This selection will cause the SmartGuard controller to include the configuration signature when connecting to the I/O module and the I/O

module will only accept the connection if the signature matches what is in the device.

IMPORTANT If you do not choose Configuration signature must match, you are responsible for verifying the safety integrity of your system by some other means.

5. Review the Connection Reaction Time Limit.

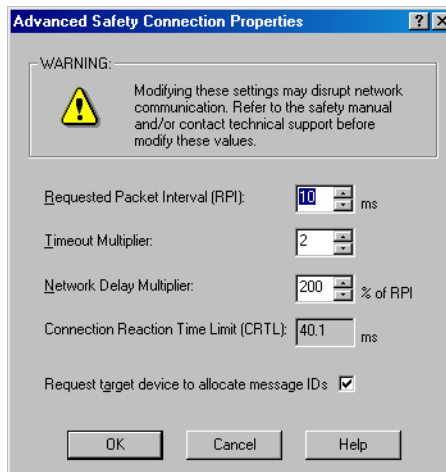
The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. If the age of the data used by the consuming device exceeds the Connection Reaction Time Limit, a connection fault occurs. Adjust the Connection Reaction Time Limit by changing the RPI or the Advanced Communication Properties as described in steps 6 and 7.

6. Set the requested packet interval (RPI).

The RPI specifies the period at which data updates over a connection. The RPI is entered in 1 ms increments, and the controller supports a valid range of 5...500 ms with a default of 10 ms. Other target devices may have more limited RPI constraints. Consult the documentation for each type of target device to determine its supported range and incremental values.

Modifying the RPI affects the Connection Reaction Time Limit. For simple timing constraints, setting the RPI is usually sufficient. However, for more complex requirements, click Advanced to further adjust the timing values affecting the Connection Reaction Time Limit.

7. Set the Advanced Safety Connection Properties (if required).



- Timeout Multiplier – The Timeout Multiplier determines the number of RPIs to wait for a packet before declaring a connection timeout. This translates into the number of messages that may be lost before a connection error is declared. For example, a Timeout Multiplier of 1 indicates that messages must be received during every RPI interval. A Timeout Multiplier of 2 indicates that 1 message may be lost as long as at least 1 message is received in 2 times the RPI (2 x RPI).
- Network Delay Multiplier – The Network Delay Multiplier defines the message transport time that is enforced by the communication protocol. The Network Delay Multiplier specifies the round trip delay from the producer to the consumer and back to the producer. You can use the Network Delay Multiplier to reduce or increase the Connection Reaction Time Limit in cases where the enforced message transport time is significantly less or more than the RPI.

8. From the File menu, choose Save to save your configuration.

Change an I/O Connection

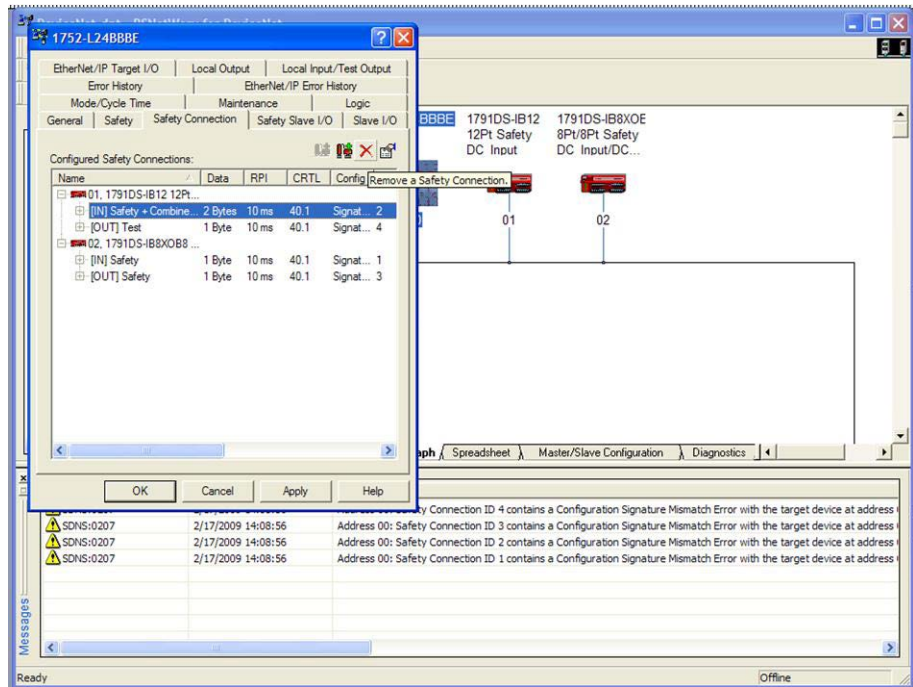


ATTENTION: When logic is programmed using distributed I/O modules (DIO) with the SmartGuard controller, and you delete (or delete and re-add) a safety connection to a DIO module, the remote I/O connections in the logic editor will be flagged as invalid and could be moved to the wrong function block. You will not be able to download until these errors are corrected.

If you delete a connection to a DIO module after the logic has been written, you must go back to your logic and verify or adjust the tags in your program to the correct function blocks. Take note of the safety connections and mappings before deleting or restoring the connections. Verify these connections before you run the logic in your application.

Follow this procedure to change your safety connections.

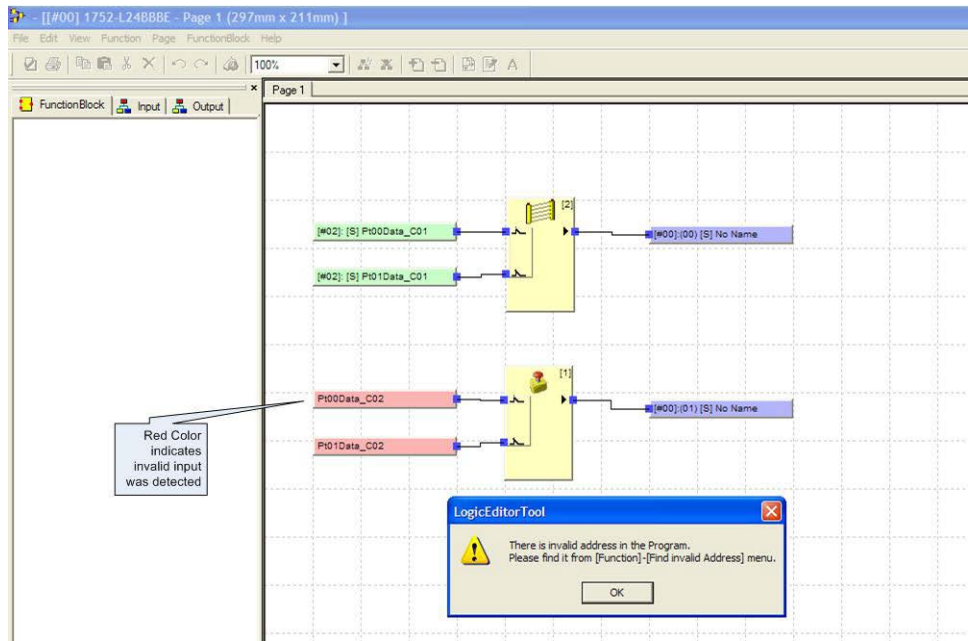
1. Highlight the I/O connection that you want to change or remove.



2. Click the 'x' button.

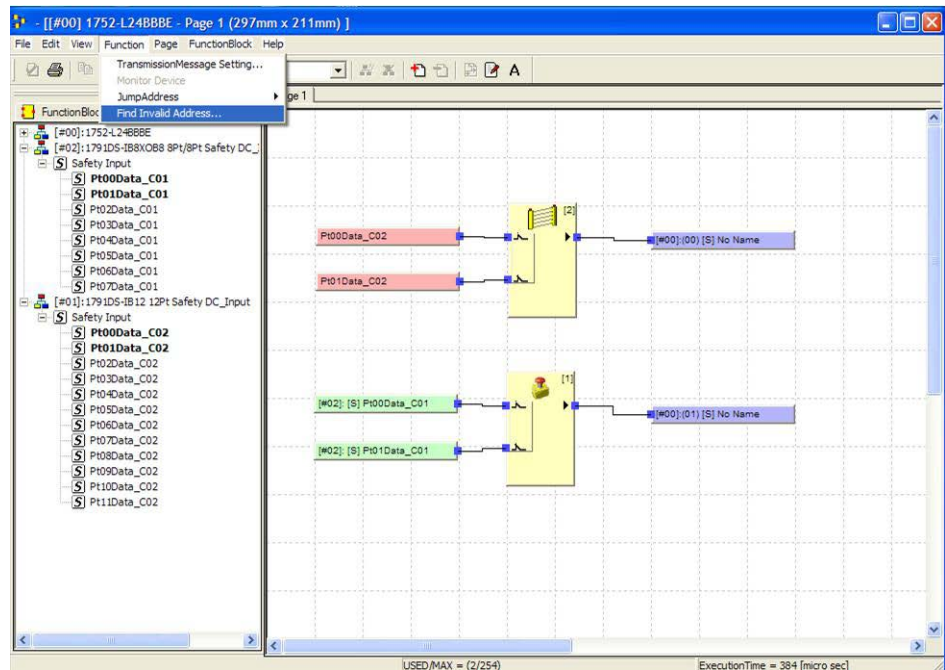
This will let you remove an I/O connection.

In this example, the next time you view your logic, an error message dialog box appears.

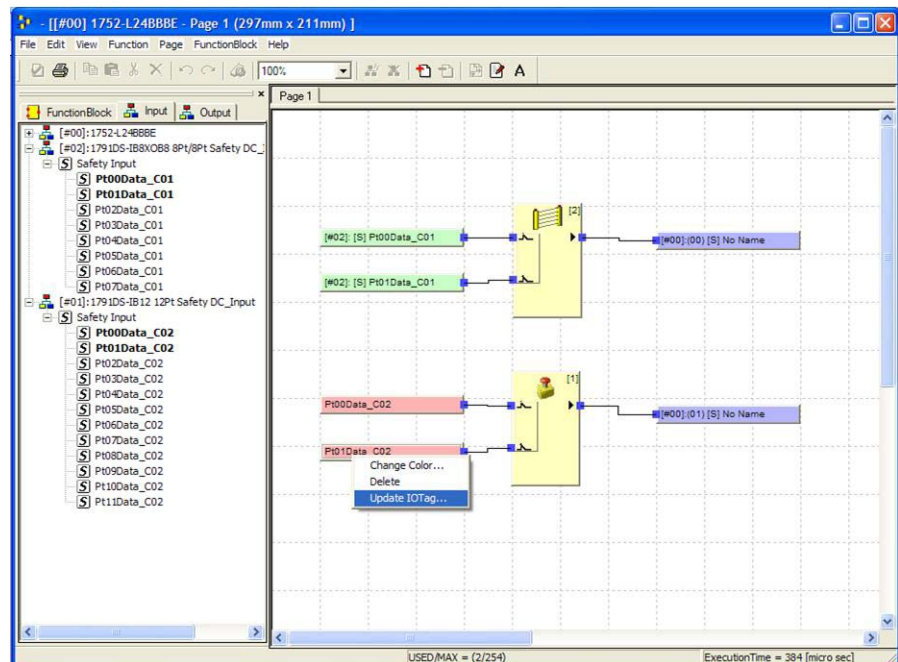


3. Click OK.

- To locate invalid addresses, choose Function>Find Invalid Address or locate all red-flagged I/O tags and right-click on the red-flagged tag.



The pull-down menu appears on the invalid tag.

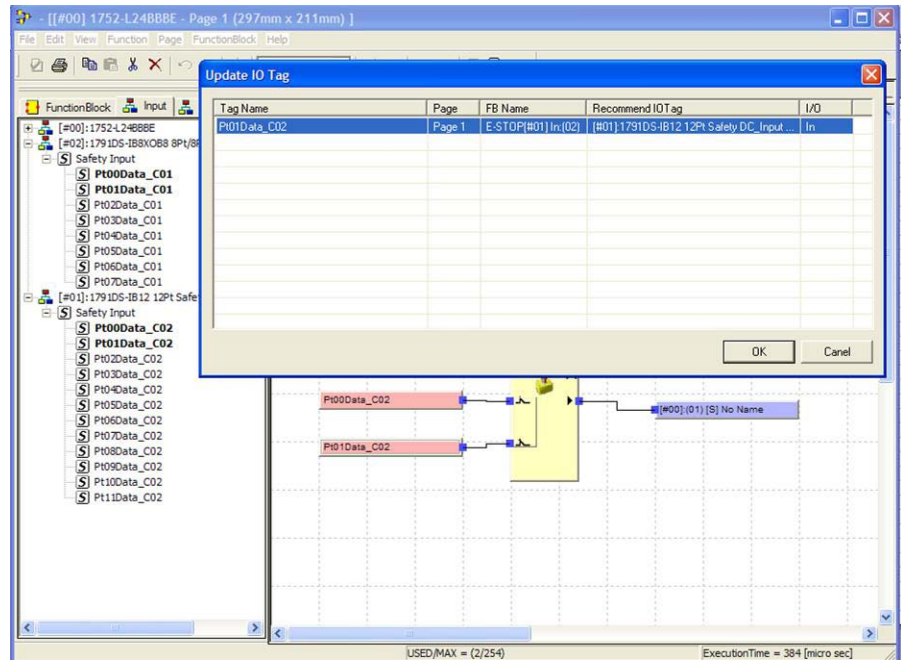


- Right-click the invalid tag.

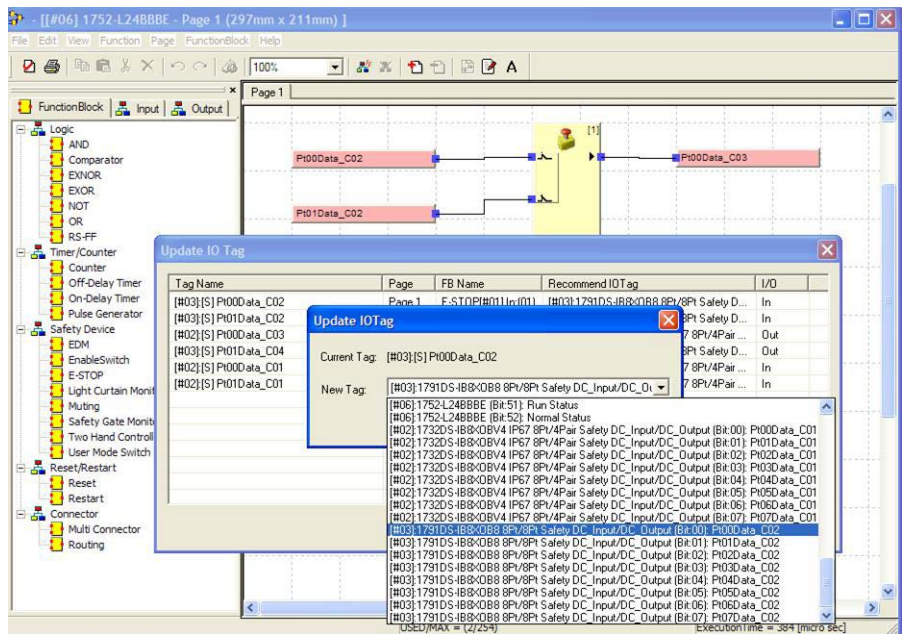
The Update IO Tag pull-down menu appears.

The dialog box shows the tag error with the recommended tag. The recommended tag is a suggestion from the software as to what I/O point

the tag was connected to originally. But you must verify and confirm that by double-clicking the suggested option.



6. If the recommended tag is correct, highlight the tag and click OK. If the recommended tag is not correct, double-click the line and a new dialog box appears that lets you select a replacement tag. You can also scroll for more options.



7. Click OK.



ATTENTION: If multiple tags appear in the Update I/O Tag dialog box, all the tags must be accepted or alternatives picked before selecting OK. Otherwise the recommended I/O tag will be used.

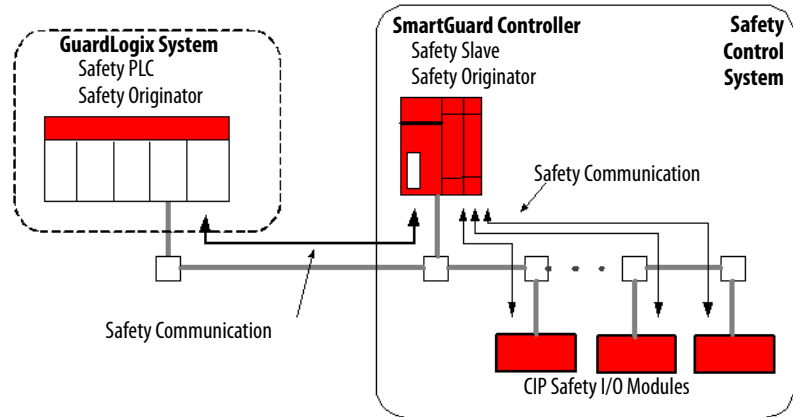
Refer to SmartGuard 600 Controllers Safety Reference Manual, publication [1752-RM001](#), for recommendations on setting up your safety system.

Setting Up the Controller as a Safety Slave

As a safety slave, the controller can perform safety I/O communication with a maximum of 4 connections, by using up to 16 bytes per connection. These connections can be either single-cast or multi-cast. However, for 1 multicast connection, the total number of masters that can be communicated with is 15.

For the SmartGuard controller to perform safety I/O communication as a safety slave, safety slave I/O data must be created and safety I/O connections must be configured in the safety master.

Figure 19 - SmartGuard Controller as Safety Slave and Safety Originator



When the controller operates as a safety slave, you can configure the safety slave assemblies to transfer local I/O data (monitor data), controller and I/O status data, and distributed I/O data to a safety master. The safety master can also write safety data to the slave SmartGuard controller, which it can use in its application program.

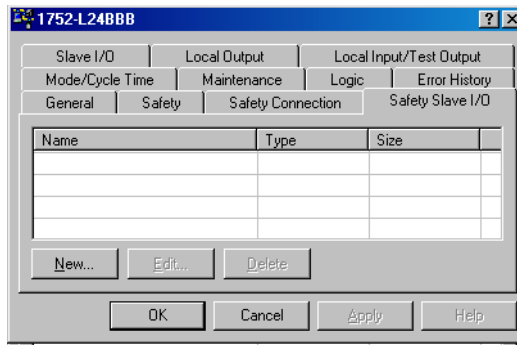
When status data is set, the status is allocated at the beginning of the remote I/O area, with status data preceding local I/O data. User-registered I/O tags follow. Status areas that are not set are not reserved. All valid data is allocated with no unassigned areas.

Create Safety Slave I/O Data

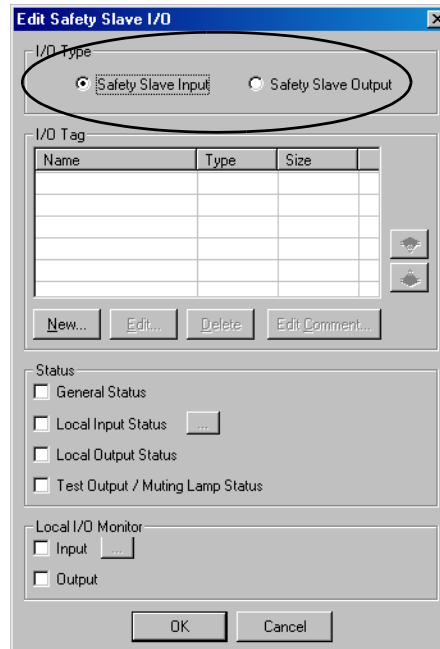
Follow these steps to create a safety slave assembly.

1. In RSNetWorx for DeviceNet software, right-click the SmartGuard controller that will act as the safety slave and choose Properties.

- Click the Safety Slave I/O tab.



- Click New.
- In the Edit Safety Slave I/O dialog box, click the I/O Type, either Safety Slave Input or Safety Slave Output.



I/O Type	Safety Data Direction
Safety Slave Input	SmartGuard controller safety slave → safety master
Safety Slave Output	Safety master → SmartGuard controller safety slave

- To add status information for Safety Input types, check the appropriate Status checkbox.

Tag Name	Data Size	Attribute Type
General Status	Byte	Non-safety
Local Input Status	Word	Safety
Local Output Status	Byte	Safety
Test Output/Muting Lamp Status	Byte	Non-safety

Safety Output types cannot include status data. You can only read status data; you cannot write to it.

6. To add local I/O monitor data for Safety Input types, check the appropriate Local I/O Monitor checkbox.

Tag Name	Data Size	Attribute Type
Local Input Monitor 1 (Inputs 0...7)	Byte	Safety
Local Input Monitor 2 (Inputs 8...15)	Byte	Safety
Local Output Monitor (Outputs 0...7)	Byte	Safety

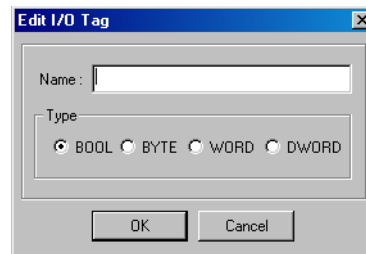
Safety Output types cannot include local I/O monitor data. You can read only input and output values; you cannot directly write to them.

7. Click New to create an I/O tag for the safety assembly.

Multiple I/O tags can be defined in an I/O assembly. I/O tags for up to 16 bytes can be defined in each I/O assembly. The I/O tags defined here can be used in the Logic Editor.

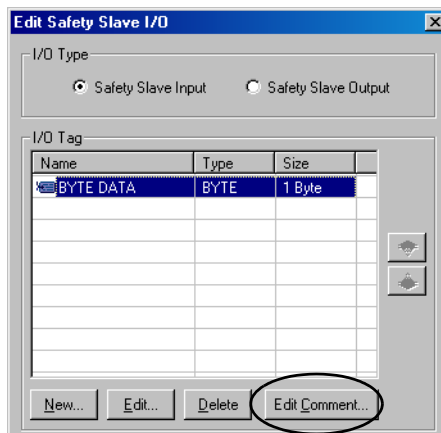
Enter specific input or output points if you do not want to share all of them. You can also share distributed I/O inputs or outputs by entering their tag names here.

8. Type a name for the tag and choose the type: BOOL, BYTE, WORD, or DWORD.

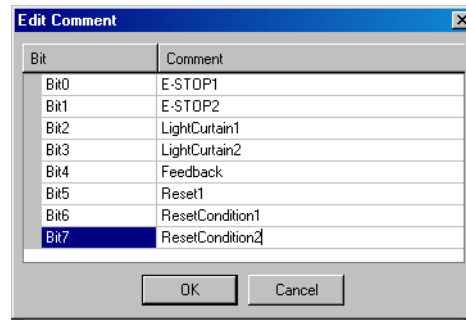


9. Click OK.

10. To create a tag name for each bit in an I/O assembly, follow these steps.
 - a. Select the applicable assembly and click Edit Comment.



b. Type a comment for each bit in the tag.



The tag name comments typed here are displayed in the Logic Editor.

c. Click OK.

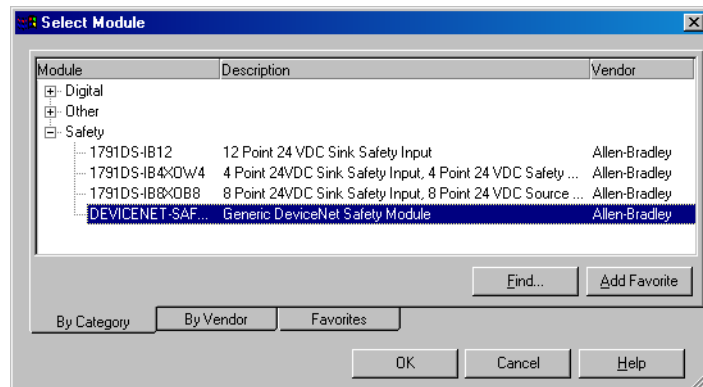
11. Click OK again to return to the Safety Slave I/O tab.
12. Create additional safety slave input or output assemblies as required for your application by repeating steps 3...11.
13. To save your configuration, from the File menu, choose Save.

Use the Safety Generic Profile in RSLogix 5000 Software

You can connect to the SmartGuard slave controller by using the safety generic profile in RSLogix™ 5000 software.

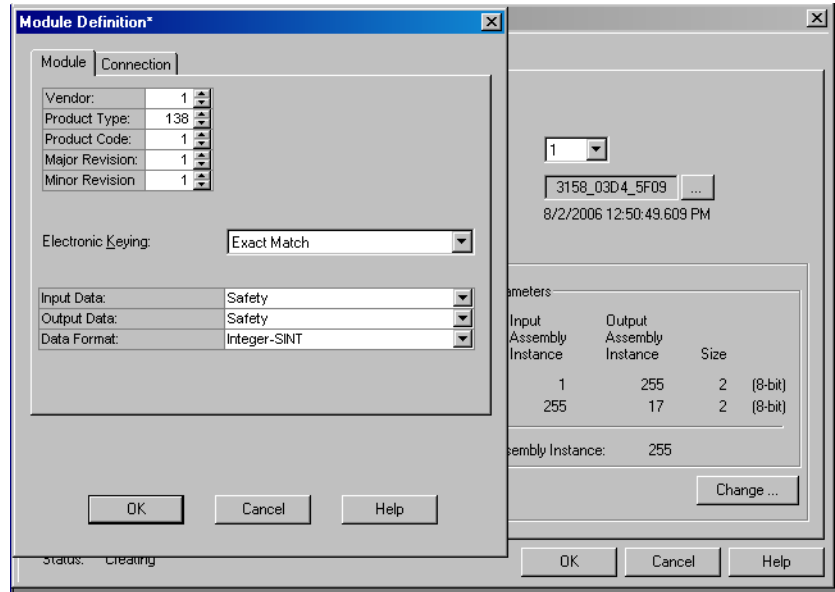
Follow these steps to connect to the controller.

1. In RSLogix 5000 software, right-click the DeviceNet network and choose New Module.
2. Select Generic DeviceNet Safety Module and click OK.

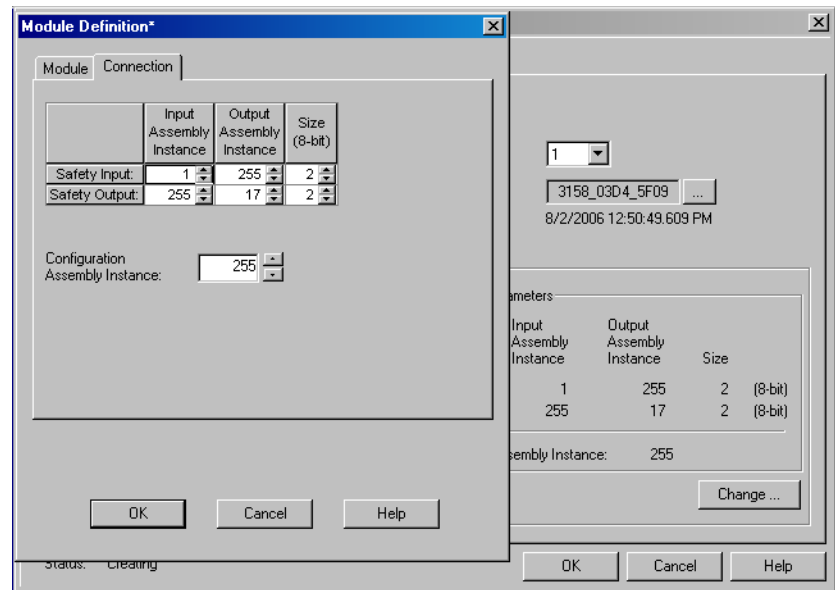


3. On the New Module dialog box, click Change.

- On the Module Definition dialog box, set the parameters as shown.



- On the Module Definition tab, click the Connection tab.



- Set the safety input and output parameters by using the following tables.

Table 6 - Input Assemblies

When the safety slave input name is	Set the generic profile input instance number to	Set the generic profile output instance number to
Safety Input 1	1	255
Safety Input 2	2	255
Safety Input 3	3	255
Safety Input 4	4	255

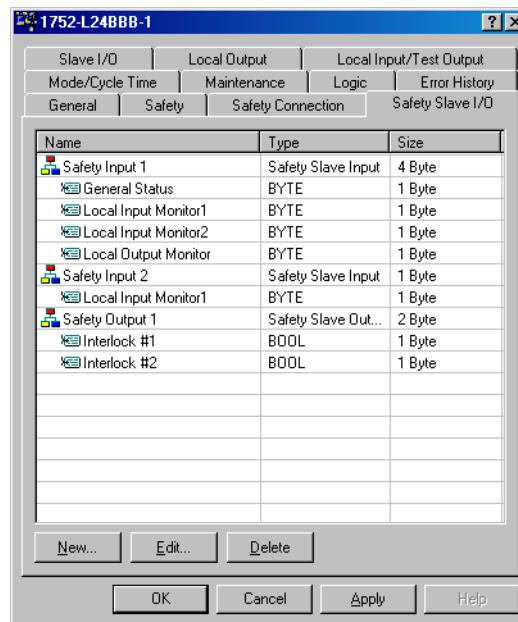
Table 7 - Output Assemblies

When the safety slave output name is	Set the generic profile input instance number to	Set the generic profile output instance number to
Safety Output 1	255	17 (for 0x11)
Safety Output 2	255	18 (for 0x12)
Safety Output 3	255	19 (for 0x13)
Safety Output 4	255	20 (for 0x14)

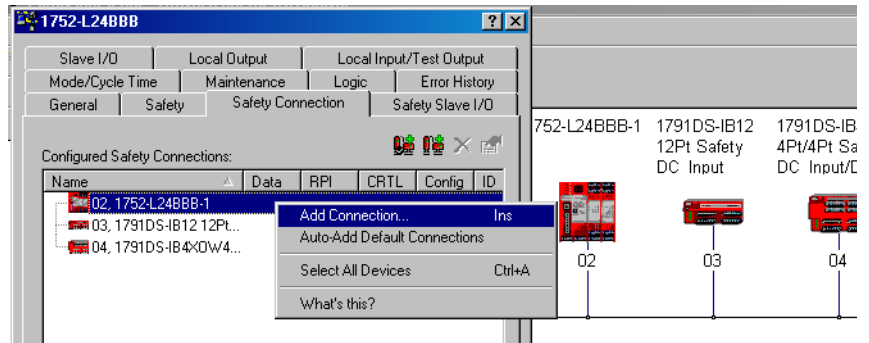
SmartGuard Controller to SmartGuard Controller Safety Interlocking

Safety interlocking allows two SmartGuard controllers to share safety data and make decisions based on one another's inputs or outputs. Safety interlocking lets you distribute your safety control to multiple SmartGuard controllers that work together.

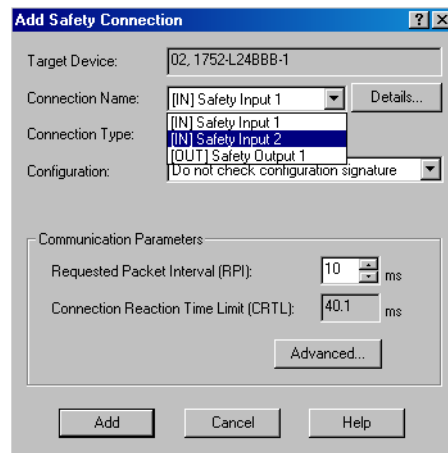
1. Configure one of the SmartGuard safety slave I/O as described in [Create Safety Slave I/O Data](#) on page 87.



- On the Safety Connections tab of the other SmartGuard controller, the one that will be the safety master, right-click the SmartGuard controller and choose Add Connection.

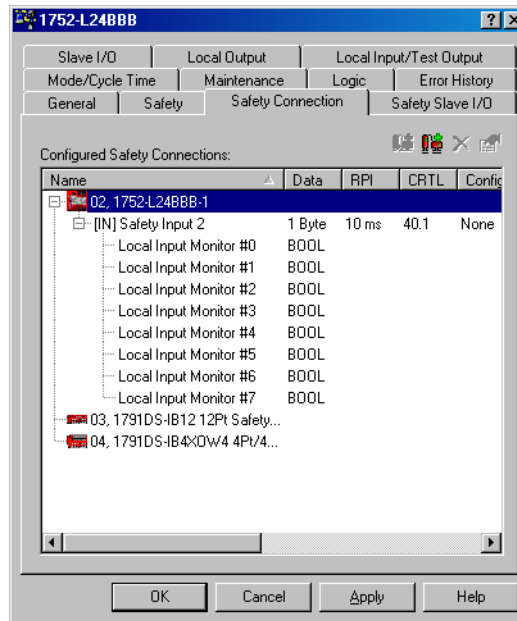


- From the Connection Name pull-down menu, choose the safety I/O assembly you want to use.



- Click Add.

Now the SmartGuard controller acting as the safety master will be able to read the other SmartGuard controller's inputs, 0...7.



Setting Up the Controller as a DeviceNet Standard Slave

As a DeviceNet standard slave, the controller can perform standard I/O communication with 1 standard master for up to 2 connections, by using up to 16 bytes per connection (128 bytes for input data for EtherNet/IP communication). The SmartGuard controller can also respond to explicit standard messages.

The controller's internal-status information and a specified area of I/O can be allocated in the standard master.

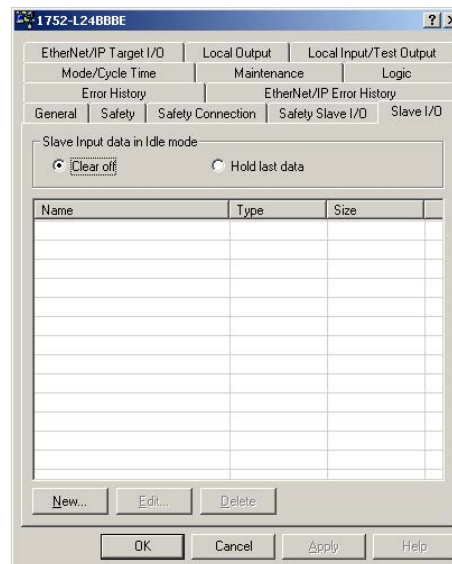
IMPORTANT Data written to the SmartGuard controller via its standard slave connection must be considered as non-safety and must not be used to control safety functions in the SmartGuard application program.

For the SmartGuard controller to perform standard I/O communication as a standard slave, standard slave I/O data must be created and I/O connections must be configured in the standard master.

Create Standard Slave I/O Data

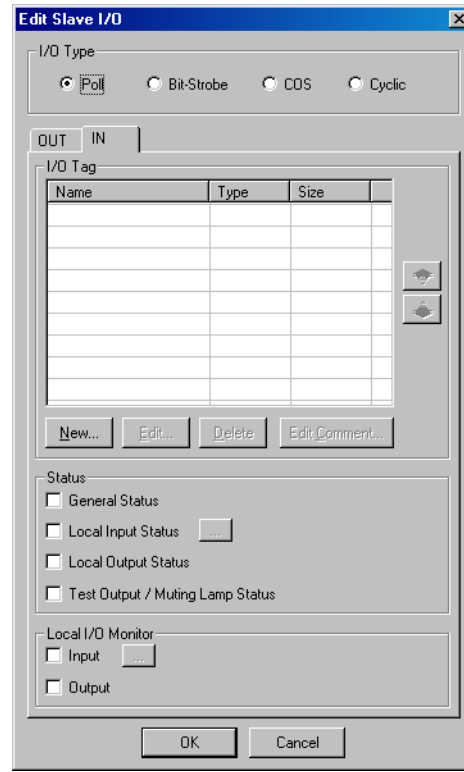
Follow these steps to create standard slave I/O assemblies.

1. In RSNetWorx for DeviceNet software, right-click the SmartGuard controller that will act as the standard slave and choose Properties.
2. Click the Slave I/O tab.



3. Configure the slave controller to either clear or hold the last data for an input assembly that the slave controller transmits to the standard master when:
 - the slave controller changes from Run to Idle mode.
 - the controller detects an error, such as a communication error in a safety chain that sets the data to an I/O tag in an input assembly.

4. Click New.
5. Click the I/O type: Poll, Bit-Strobe, COS, or Cyclic.



Output data cannot use a bit-strobe connection type because bitstrobe data cannot be output from the standard master. Also, the maximum size for bitstrobe data input to the standard master is 8 bytes. COS and cyclic connections cannot be used at the same time.

6. To add status information for Input types, check the Status checkboxes (optional).

When the I/O type is Input, you can include the following status information in the I/O assembly.

Tag Name	Data Size	Attribute Type
General Status	Byte	Non-safety
Local Input Status	Word	Non-safety
Local Output Status	Byte	Non-safety
Test Output/Muting Lamp Status	Byte	Non-safety

7. To add local I/O monitor data for Input types, check the appropriate Local I/O Monitor checkbox.

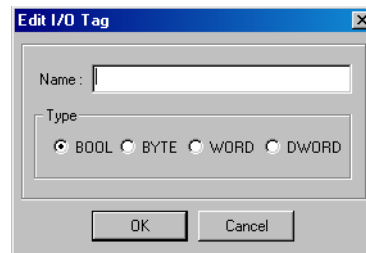
Tag Name	Data Size	Attribute Type
Local Input Monitor 1 (Inputs 0...7)	Byte	Non-safety
Local Input Monitor 2 (Inputs 8...15)	Byte	Non-safety
Local Output Monitor (Outputs 0...7)	Byte	Non-safety

Output types cannot include local I/O monitor data. You can read only input and output values; you cannot directly write to them.

8. Click New to create an I/O tag.

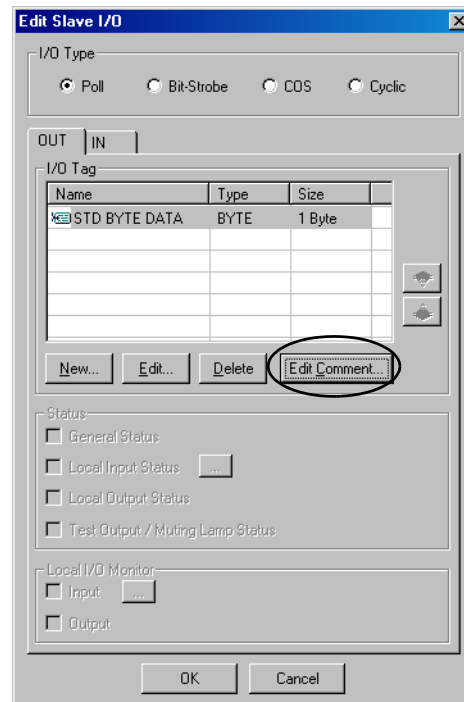
Multiple I/O tags can be defined in an I/O assembly. I/O tags for up to 16 bytes can be defined in each I/O assembly. The I/O tags defined here can be used in the Logic Editor.

9. Type a name for the tag and click the type: BOOL, BYTE, WORD, or DWORD.



10. Click OK.

11. To create a tag name for each bit in an I/O assembly, follow these steps.
 - a. Select the applicable assembly and click Edit Comment.



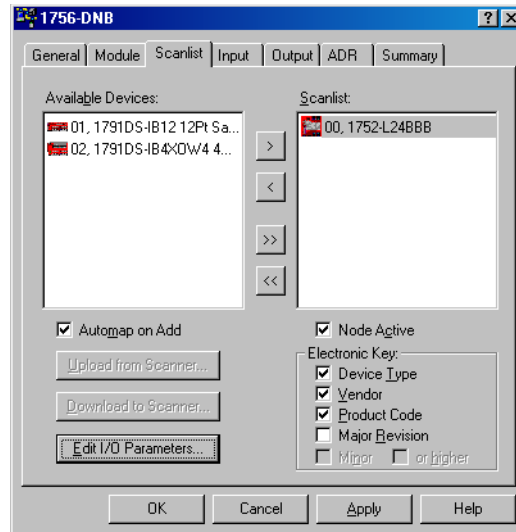
- b. Type a comment for each bit in the tag.

The tag name comments typed here are displayed in the Logic Editor.

- c. Click OK.
12. Click OK again to return to the Slave I/O tab.
13. Create additional slave input or output assemblies as required for your application by repeating steps 4...12.
14. From the File menu, choose Save to save your configuration.

Adding the SmartGuard Standard Slave to the Standard Master's Scanlist

To make the standard slave I/O assemblies available to the standard master, add the SmartGuard standard-slave controller to the master's scanlist.



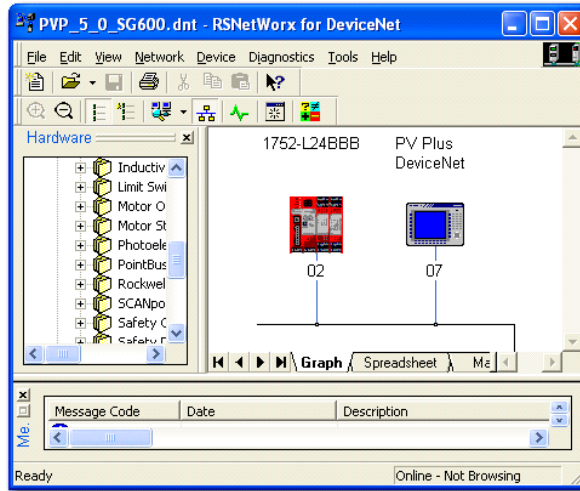
Refer to the user documentation for your standard master for information on configuring your specific device.

Save your configuration in RSNetWorx for DeviceNet software by choosing File>Save.

Reading and Writing to and from the SmartGuard Controller to a PanelView Plus Interface

This section describes how to read and write from the SmartGuard controller and the PanelView™ Plus interface. The SmartGuard controller is a standard slave within this architecture. Refer to [page 95](#) for more information.

Figure 20 - SmartGuard Controller and PanelView Plus Interface on the Network

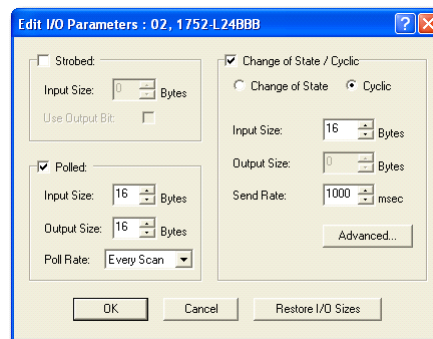


Up to two connections can be selected from the four connection types, but only one connection of each type can be made. For example, one polled connection and 1 COS connection can be made, but not two polled connections. Both polled and COS/Cyclic allow both inputs and outputs (read and write) in a single connection.

A polled connection that uses both inputs and outputs can have 16 bytes of input data and 16 bytes of output data. If you add another connection, you can have 16 additional bytes of data.

If you use the polled connection and then add a COS/Cyclic connection, the output is unavailable. The maximum data configuration is shown below.

Figure 21 - Edit I/O Parameters Dialog Box



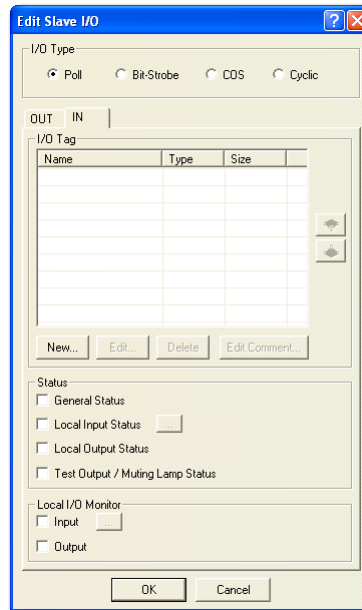
This configuration allows 32 bytes of input data (16 via polled and 16 via COS or Cyclic) and 16 bytes of output data via the polled connection. This configuration is described in greater detail in this chapter.

Read BOOLs from the SmartGuard Controller and Display Them on the PanelView Plus Interface

Follow this procedure to read BOOLs from the SmartGuard controller and display them on the PanelView Plus interface.

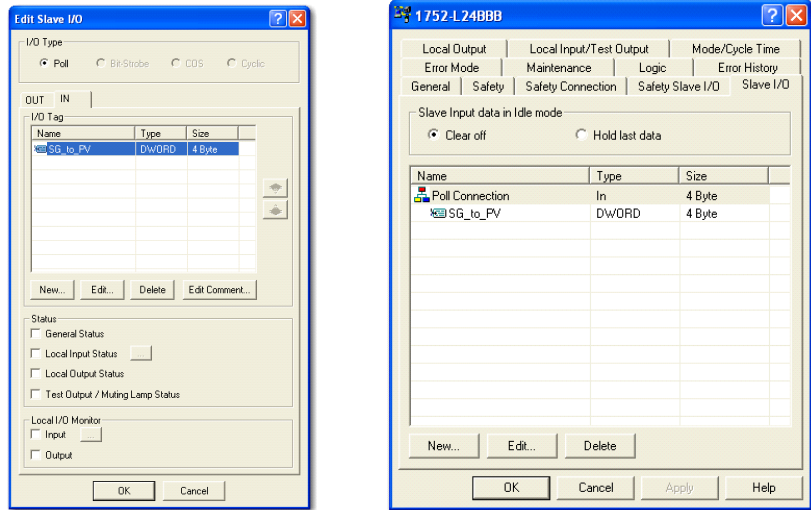
1. Open your RSNetWorx software.
2. Open the SmartGuard properties.
3. Click the Slave I/O tab.

The following dialog box appears.



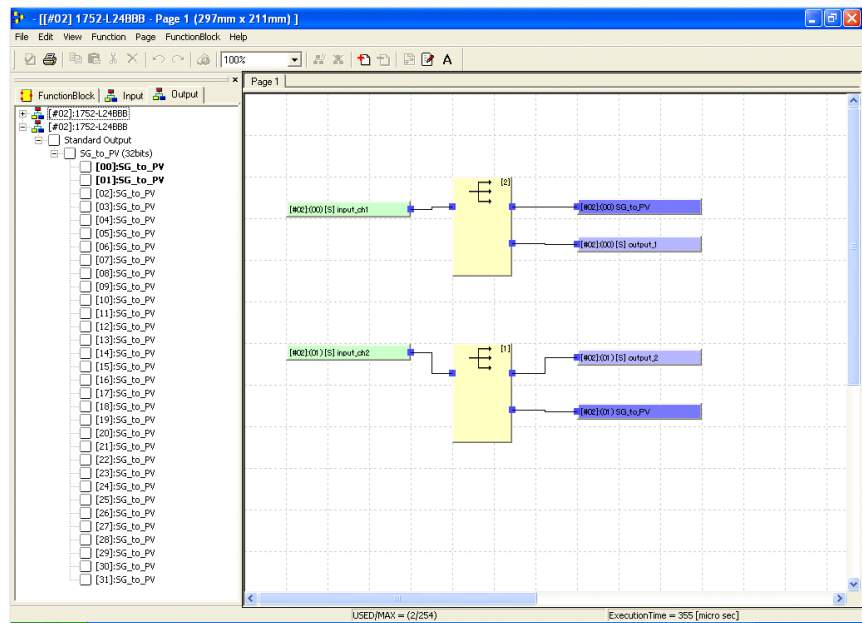
4. Click the IN tab.
5. Enter the tag names that will be read by the PanelView Plus interface.

In this case, a single 4-byte tag has been created and will use a polled connection. These 4 bytes are read by the PanelView Plus interface.



Even though you created a DWORD tag, you have access to all 32 bits of the DWORD within the SmartGuard editor. The sample SmartGuard code is controlling two of the 32 bits.

The bolded tags in the taglist are used in code.

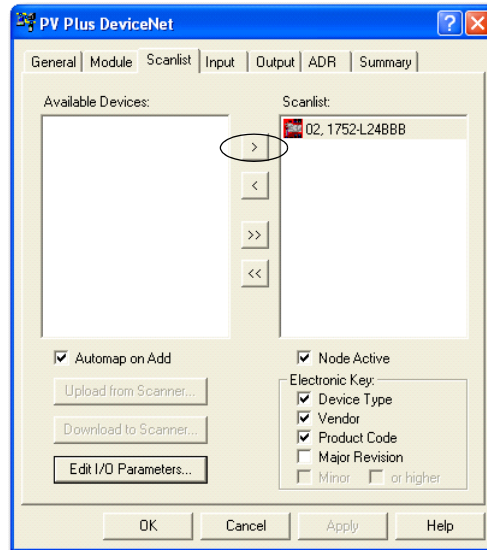


6. Download the configuration to the SmartGuard 600 controller.

Configure the Scanlist of the PanelView Scanner

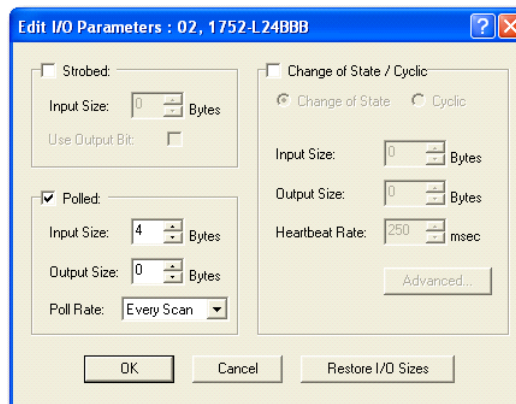
Follow this procedure to configure the scanlist of the PanelView Plus DeviceNet scanner.

1. Click the Scanlist tab.
2. Click the right arrow to move the SmartGuard controller to the scanlist.



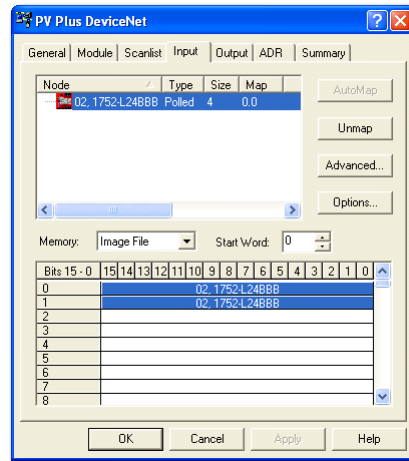
3. Click Edit I/O Parameters and verify it is configured as shown below.

The example has a 4-byte polled connection that will be an input to the PanelView Plus interface.



Because the Automap on Add was checked, the following mapping occurred automatically.

- Verify that the 4 bytes of input data are mapped as shown.



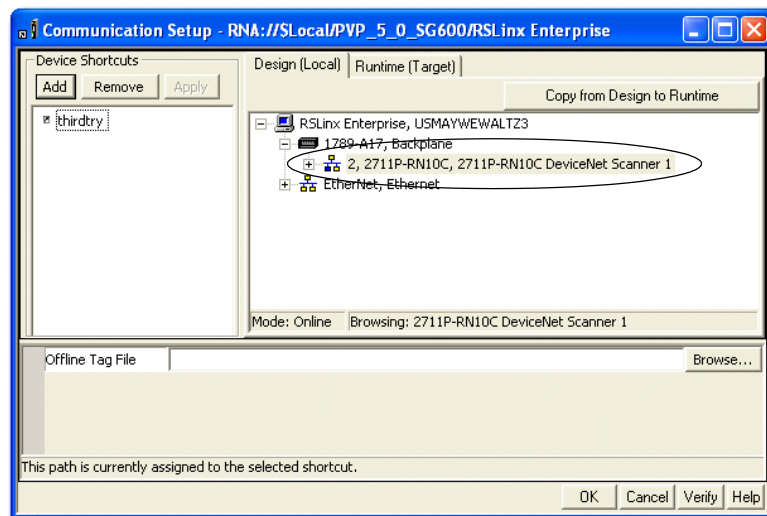
- Right-click the PanelView Plus Interface in RSNetWorx software and choose Download to Device.

Configure the RN10C DeviceNet Scanner

Follow this procedure to configure the RN10C DeviceNet scanner.

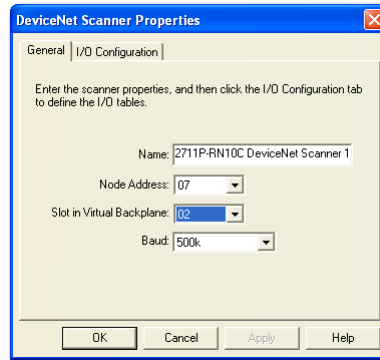
The shortcut in RSLinx Enterprise software should appear similar as shown.

Note that the slot number of the RN10C scanner is 2.



- Right-click the RN10C scanner and choose Properties.
- Enter the name of the scanner.

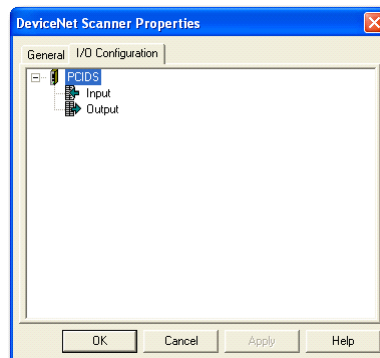
- From the appropriate pull-down menu, choose the Node Address, Slot in the Virtual Backplane, and Baud rate.



The PanelView Plus interface is configured for DeviceNet node 7. The SmartGuard controller has the DIP switches set for auto-sensing (left/left/left/right from top to bottom). Choose the the baud rate that is appropriate for your application.

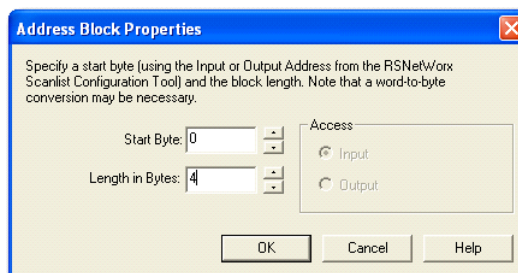
- Click the I/O Configuration tab.

The following dialog box appears.



- Right-click Input and choose Add Address Block.

The following dialog box appears.

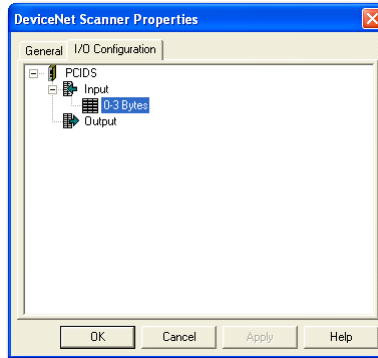


- Enter 4 as the Length in Bytes.

This will match what the scanner is reading from the SmartGuard controller.

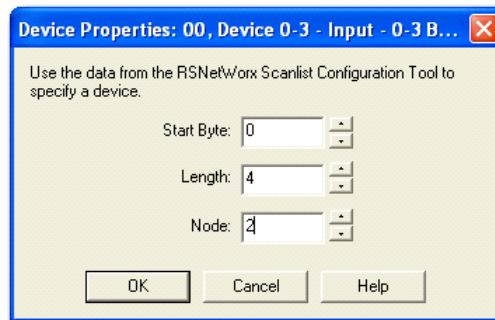
7. Click OK.

The I/O configuration appears.



8. Right-click 0-3 Bytes and choose Add Devices.

The following dialog box appears.

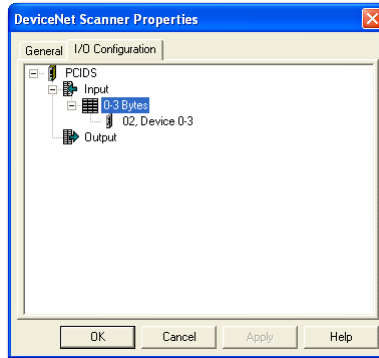


9. Set the Node number to match your SmartGuard controller.

The node number is 2 in this example.

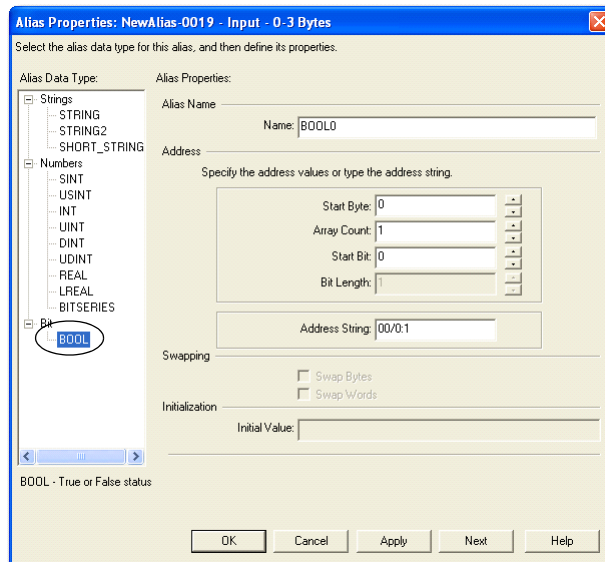
10. Click OK.

The following dialog box appears.



11. Right-click 0-3 Bytes and choose Add Alias.

The following dialog box appears.

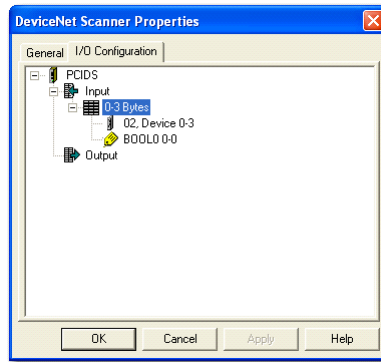


12. Select the bolded data type (BOOL) and from the appropriate pull-down, choose the Start Byte, Array Count, and Start Bit.

The values shown above represent bit 0 of the first byte.

13. Enter the Name.
14. Click OK.

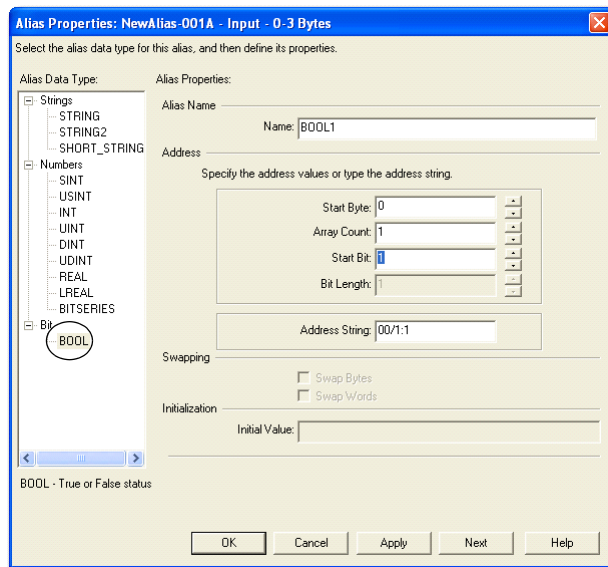
The following dialog box appears.



To add a second BOOL that represents bit 1 of the first byte, follow this procedure.

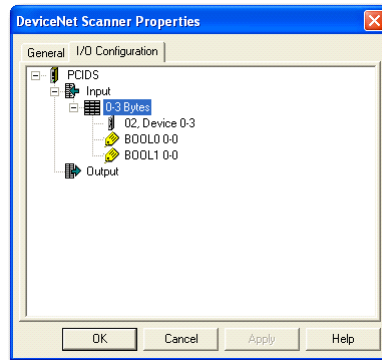
1. Right-click 0-3 Bytes and choose Add Alias.

The following dialog box appears when BOOL data type is selected.



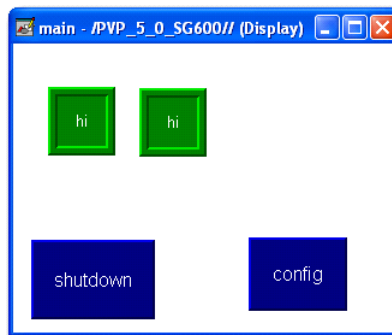
2. From the appropriate pull-down menu, choose the Start Byte, Array Count, and Start Bit.
3. Enter the Name.
4. Click OK.

The following dialog box appears.

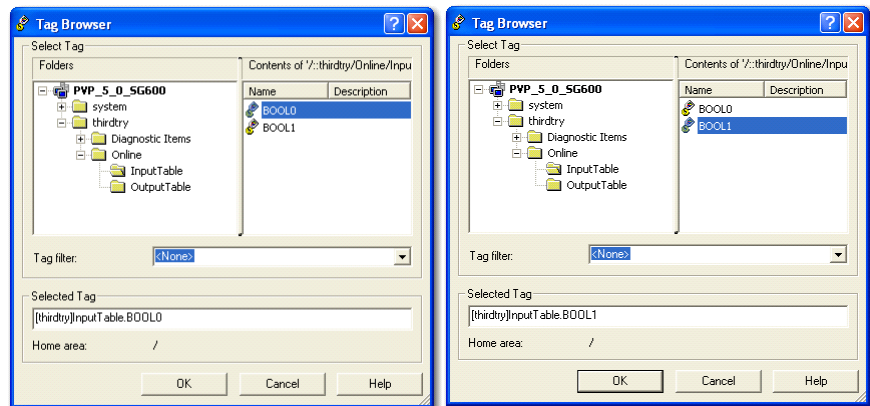


5. Click OK.

The final step is to create the PanelView Plus graphic that reads the alias tags. This example will use two multistate indicators that read the two aliases.



The tags for each of the multistate indicators can be browsed by using RSLinx Enterprise software. Select the tags as shown.



Finally, you need to save your project, generate a Runtime file, and download it to the PanelView Plus interface.

Read and Write from and to the SmartGuard Controller from the PanelView Plus Interface Concurrently

This example shows how to use two maintained push buttons on a PanelView Plus screen to control two tags within the SmartGuard 600 controller. To accomplish this, a single byte of data is sent from the the PanelView Plus interface to the SmartGuard controller. BOOL does not exist in either the PanelView Plus scanner properties or the SmartGuard controller. Even if you create a BOOL tag in the SmartGuard controller to accept data from the PanelView Plus interface, it uses a byte of data.

There are also no integer values within the SmartGuard controller that you can access programmatically. Because only Boolean data values are sent to the SmartGuard controller, and since the smallest data type within the SmartGuard controller is a byte, there is no reason to ever send less than a byte from the PanelView Plus interface to the SmartGuard controller, even if you only are using a couple of bits. This example configures a byte of output data that is to be sent to the SmartGuard controller, but use only two buttons. If you need to send more than eight BOOLS to the SmartGuard controller from the PanelView Plus interface, edit the following example and change 1 byte to x bytes in the output parameters.

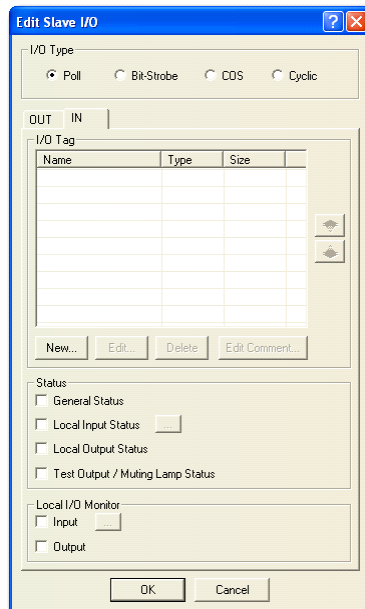
Tags that are being read by the PanelView Plus interface should be entered under the IN tab.

Tags that are being written to by the PanelView Plus interface should be entered under the OUT tab.

Follow this procedure to read and write from and to the SmartGuard controller from the PanelView Plus interface concurrently.

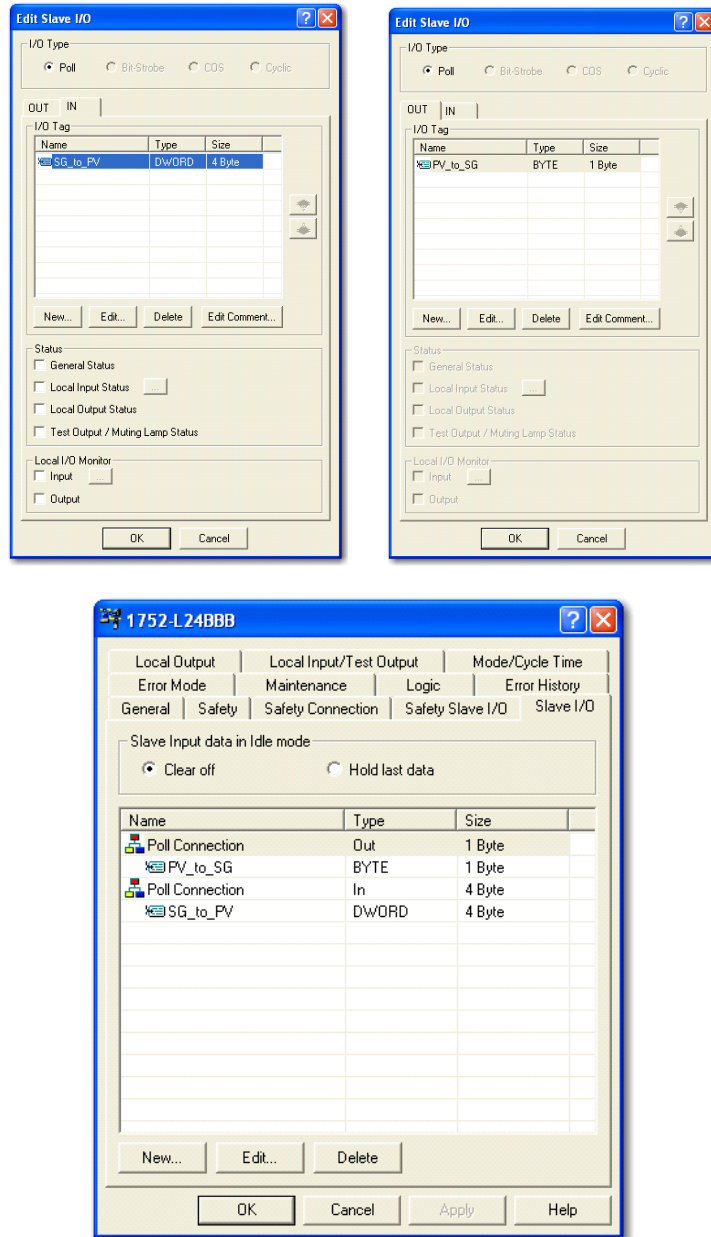
1. Open your RSNetWorx software.
2. Open the SmartGuard properties.
3. Click the Slave I/O tab.

The following dialog box appears.



4. Click the IN tab.
5. Enter the tag names that will be read by the PanelView Plus interface.
6. Click the OUT tab.
7. Enter the tag names that will be written to by the PanelView Plus interface.

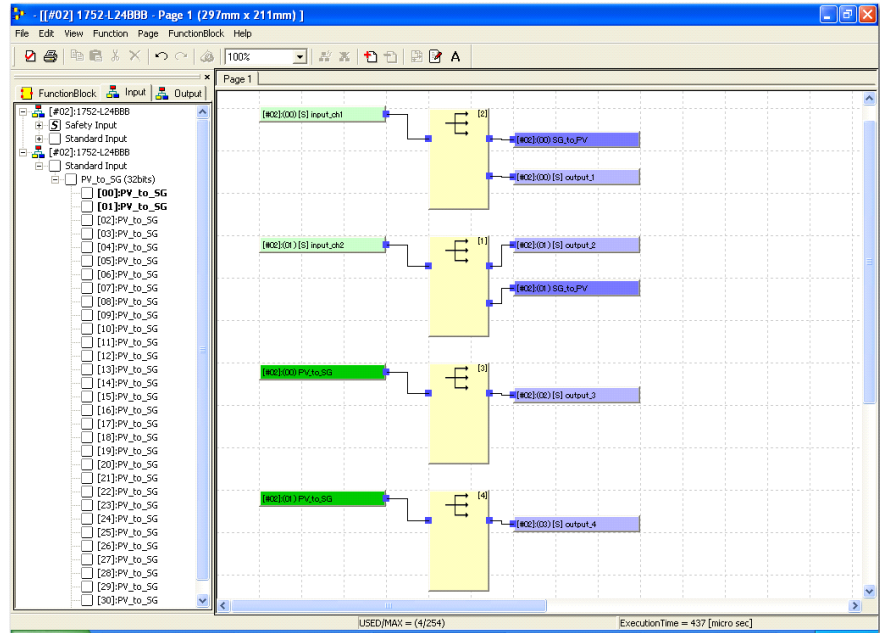
In this case, a polled connection with 4 bytes that can be read and 1 byte that can be written to will be used.



You also have access to all the bits of the DWORD and BYTE within the SmartGuard editor. The sample SmartGuard code is using two bits in both buffers.

The four bolded tags in the taglist are used in code.

The Input tab is shown below and so the PV_to_SG tags are displayed. To view the SG_to_PV tags, click the Output tab.



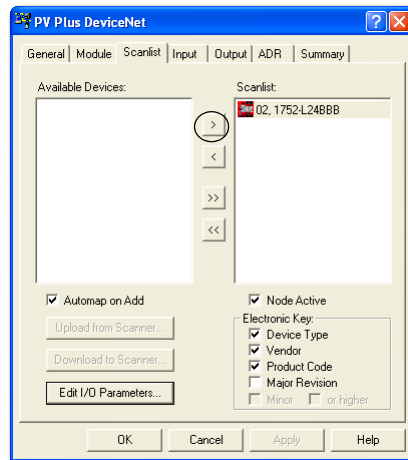
8. Download the configuration to the SmartGuard 600 controller.

Configure the Scanlist of the PanelView Scanner

For the PanelView Plus DeviceNet scanner, you must configure the scan list.

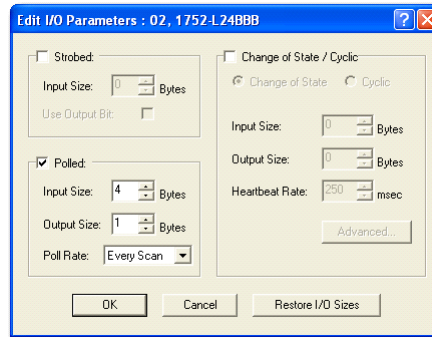
Follow this procedure to add the SmartGuard 600 controller to the Scan list.

1. Click the Scanlist tab.
2. Click the right arrow to move the SmartGuard controller to the scanlist.



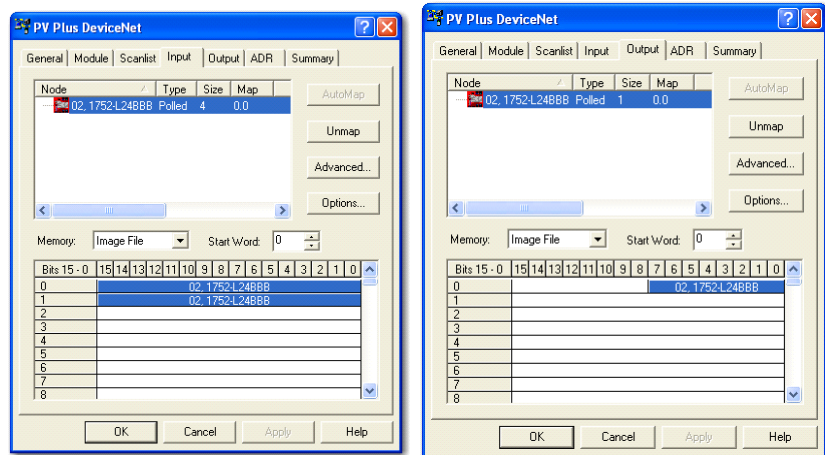
3. Click Edit I/O Parameters and verify it is configured as shown below.

The example has a polled connection that will read 4 bytes and write 1 byte between the SmartGuard controller and the PanelView Plus interface.



Because the Automap on Add was checked, the following mapping occurred automatically.

- Verify that the 4 bytes of input data and the single byte of output data are mapped as shown.

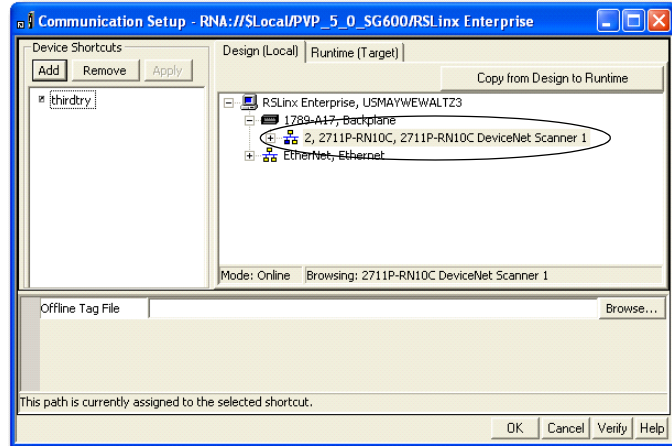


- In RSNetWorx software, right-click the PanelView Plus interface and choose Download to Device to download this configuration to the PanelView Plus interface.

Configure the RN10C DeviceNet Scanner

Follow this procedure to configure the RN10C DeviceNet scanner.

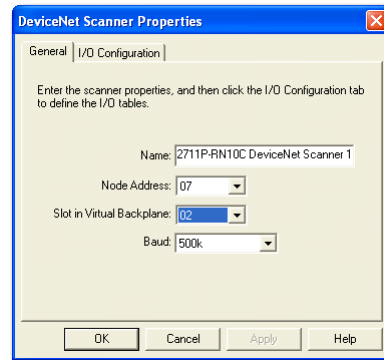
The shortcut in RSLinx Enterprise software should appear similar as shown.



Note that the slot number of the RN10C is 2.

1. Right-click the RN10C scanner and choose Properties.

The following dialog box appears.

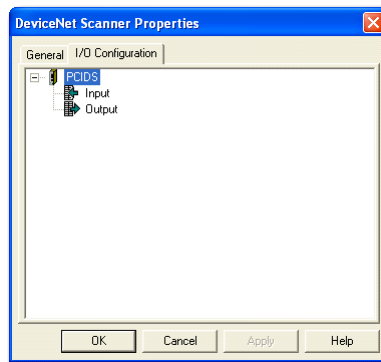


2. Enter the name of the scanner.
3. From the appropriate pull-down menu, choose the Node Address, Slot in the Virtual Backplane, and Baud rate.

The PanelView Plus interface is configured for DeviceNet node 7. The SmartGuard controller has the DIP switches set for auto-sensing (left/left/right from top to bottom). Choose the the baud rate that is appropriate for your application.

4. Click the I/O Configuration tab.

The following dialog box appears.



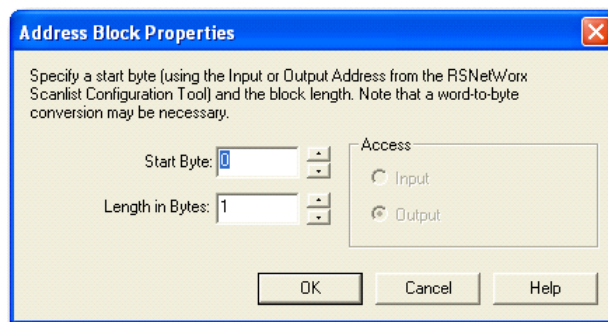
The configuration of the input block is covered in the ‘How to Read BOOLS’ section of this document. Refer to that section to configure the data that will be read from the SmartGuard controller and displayed on the PanelView Plus interface.

Configure the Data that is Written from the PanelView Plus Interface to the SmartGuard Controller

Follow this procedure to configure the data that is written from the PanelView Plus interface to the SmartGuard controller.

1. Right-click Output and choose Add Address Book.

The following dialog box appears.

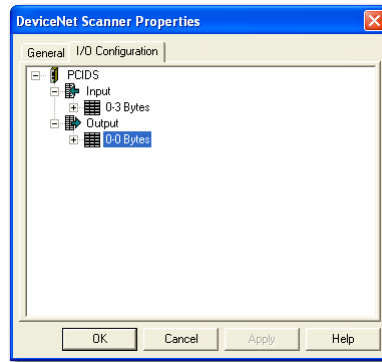


2. Select one as the Length in Bytes.

This will match what the scanner is writing to the SmartGuard controller.

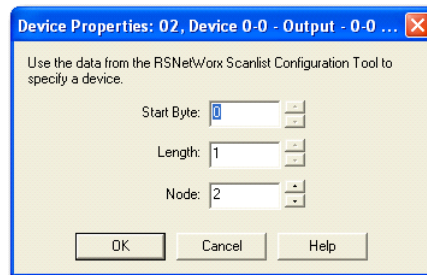
3. Click OK.

The following dialog box appears.



4. Right-click 0-0 Bytes and choose Add Devices.

The following dialog box appears.

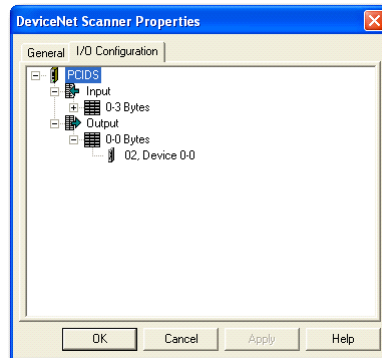


5. Set the Node number to match your SmartGuard controller.

The node number is 2 in this example.

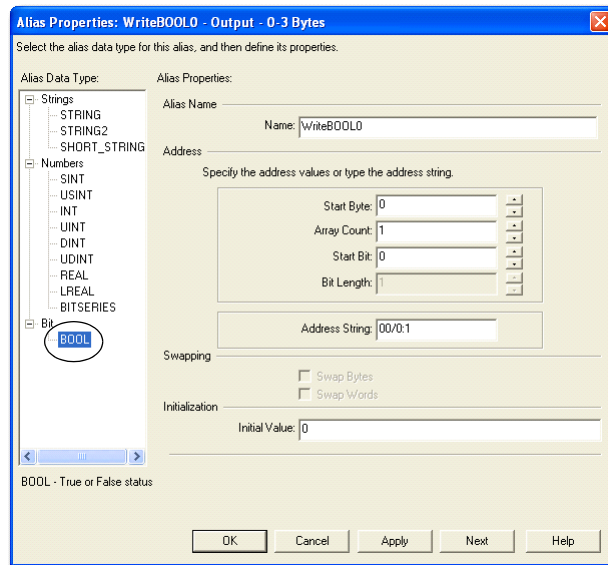
6. Click OK.

The following Dialog box appears.



7. Right-click 0-0 Bytes and choose Add Alias.

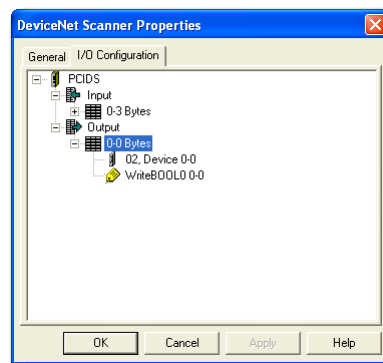
The following dialog box appears when the BOOL data type is selected.



The values shown above represent bit 0 of the first byte.

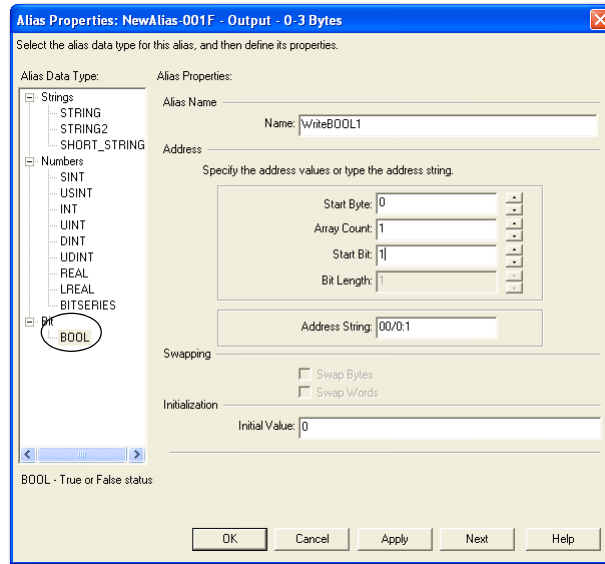
8. From the appropriate pull-down menu, choose the Start Byte, Array Count, and Start Bit.
9. Enter the Name.
10. Enter the initial value of 0.
11. Click OK.

The following dialog box appears.



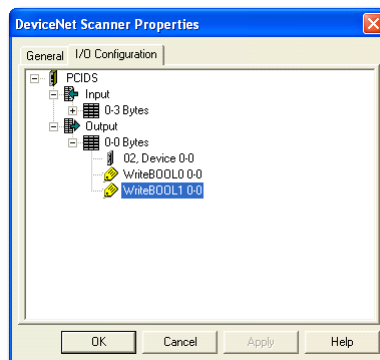
To add a second BOOL that represents bit 1 of the first byte, follow this procedure.

1. Right-click 0-0 Bytes and choose Add Alias.



2. Select the BOOL data type and from the appropriate pull-down, choose the Start Byte, Array Count, and Start Bit.
3. Enter the Name.
4. Enter the initial value of 0.
5. Click OK.

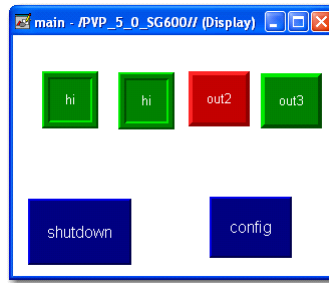
The following dialog box appears.



6. Click OK.

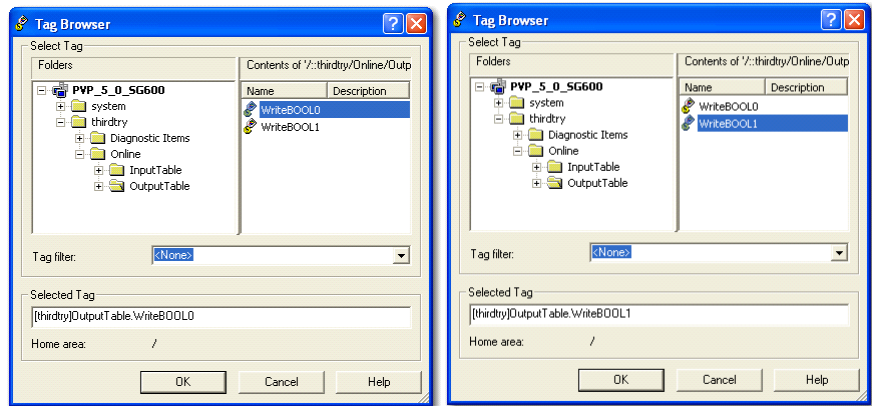
The final step is to create the PanelView Plus graphic that reads the alias tags. This example will use 2 maintained buttons that read the 2 aliases.

Figure 22 - PanelView Plus Graphic



The tags for each of the maintained buttons can be browsed by using RSLinx Enterprise software. Select the tags as shown.

Figure 23 - Browse the Tags for Maintained Buttons



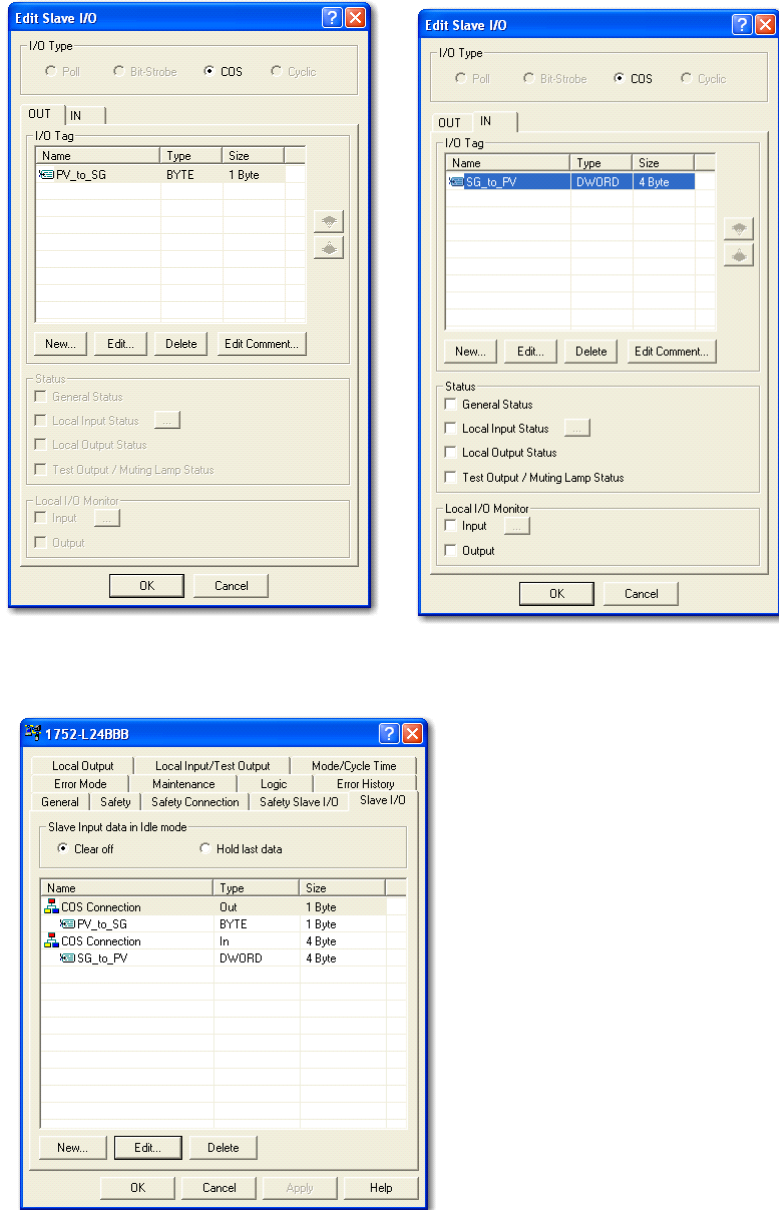
Finally, you need to save your project, generate a Runtime file, and download it to the PanelView Plus interface.

COS versus Polled

To use Change of State (COS) rather than polled, make the appropriate changes from [page 110](#) up to this section as shown by the following dialog boxes.

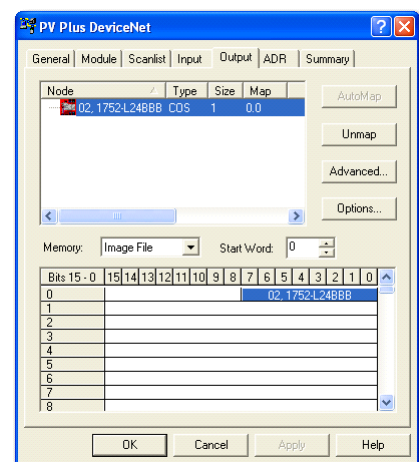
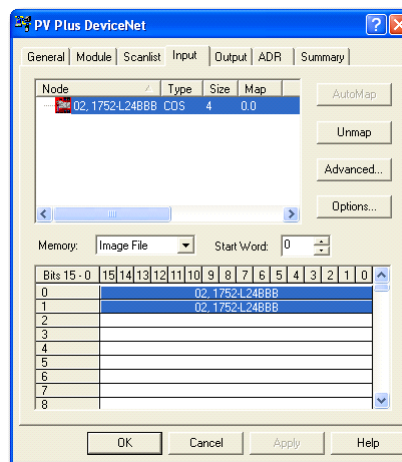
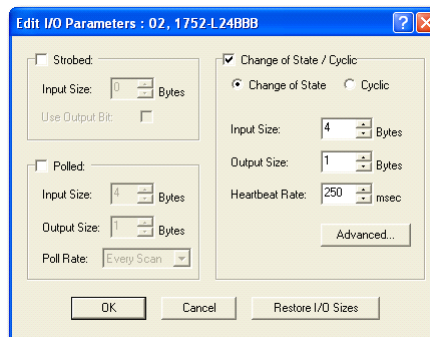
The following edits occur in the SmartGuard slave I/O configuration.

Figure 24 - SmartGuard Slave I/O Configuration Changes



The following edits occur in the RN10C DeviceNet scanner configuration in RSNetWorx software.

Figure 25 - RN10C DeviceNet Scanner Configuration Changes

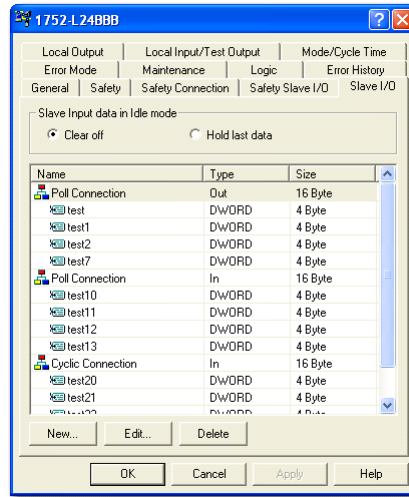


Maximum Connection Sizes

This example has a polled connection with 16 bytes input and 16 bytes output. A second connection (cyclic) of 16 bytes input was added. The following show the changes required to support the configuration.

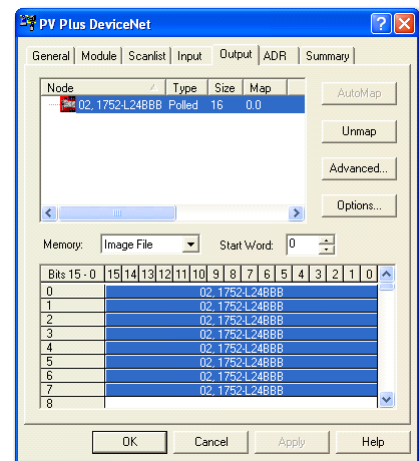
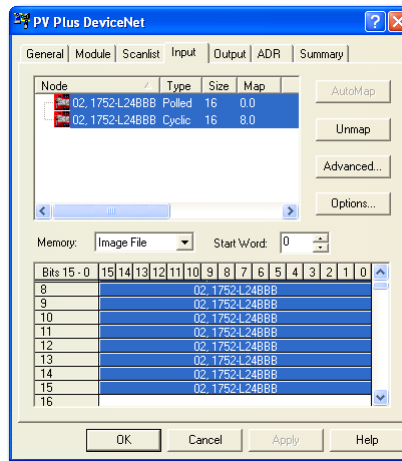
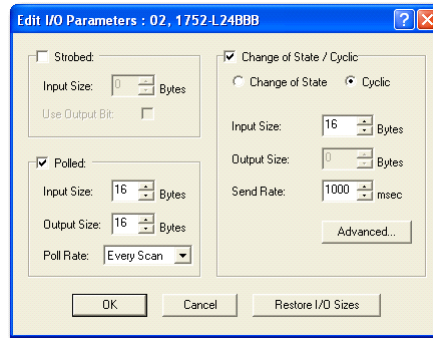
The SmartGuard slave I/O configuration appears as shown.

Figure 26 - SmartGuard Slave I/O Configuration



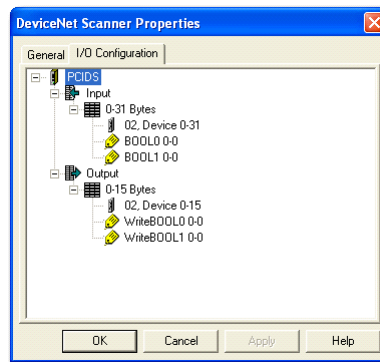
The DeviceNet scanner connection properties appear as shown.

Figure 27 - DeviceNet Scanner Configuration



The FactoryTalk® to RSView® Enterprise software I/O configuration appears as shown.

Figure 28 - FactoryTalk to RSView Enterprise Software I/O Configuration



Configure Your Controller for EtherNet/IP Communication

Introduction

The SmartGuard controller (catalog number 1752-L24BBBE) offers EtherNet/IP connectivity.

Topic	Page
Configure Target I/O in RSNetWorx for DeviceNet Software	126
Set Up Your Controller as a Slave by Using RSLogix 5000 Software Generic Profile	130
Configure Communication between a Standard PanelView Terminal and a SmartGuard 600 Controller over an EtherNet/IP Network	132

Multicast Connections

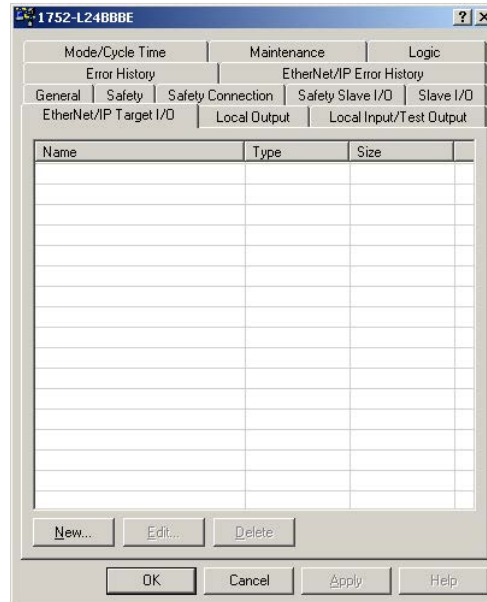
You can make only two connections to the SmartGuard controller at any one time. It can be one input and one output, or two inputs or two outputs. Even though the connections are multicast, once the two connections are made, no other connections are accepted.

For example, you can have two controllers connected to one input connection on the SmartGuard controller multicast input assembly, and this would consume the two EtherNet/IP connections.

Configure Target I/O in RSNetWorx for DeviceNet Software

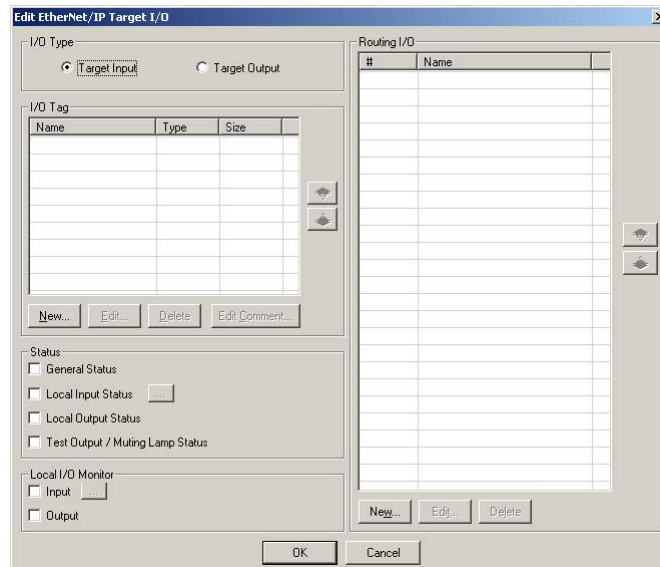
Follow these steps to create standard EtherNet/IP target I/O assemblies.

1. In RSNetWorx for DeviceNet software, right-click the SmartGuard controller and choose properties.
2. Click the EtherNet/IP Target I/O tab.



3. Click New.

The following dialog box appears.



4. Under I/O type, click either Target Input or Target Output.

Target Input means that this data is produced by the SmartGuard controller and read by the originating device. Target Output means that this data is produced by the originating device and is sent to the SmartGuard controller.

If you have checked Target Input, you can include the following status information in the I/O assembly.

Tag Name	Data Size	Attribute Type
General Status	Byte	Non-safety
Local Input Status	Word	
Local Output Status	Byte	
Test Output/Muting Lamp Status		

5. Add status information for input types by checking the Status checkboxes.
6. Add local I/O monitor data for input types by checking the appropriate Local I/O Monitor checkbox.

Tag Name	Data Size	Attribute Type
Local Input Monitor 1 (inputs 0...7)	Byte	Non-safety
Local Input Monitor 2 (inputs 8...15)		
Local Output Monitor (outputs 0...7)		

Output types cannot include local I/O monitor data. You can only read input and output values; you cannot directly write to them.

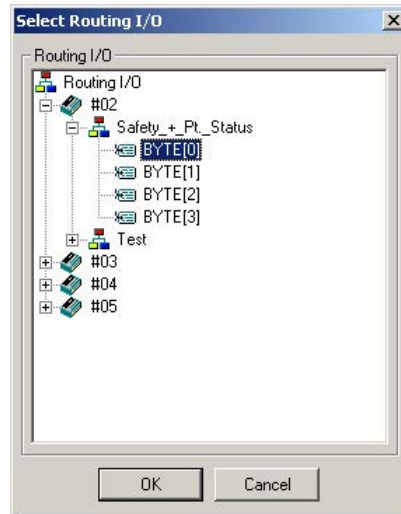
7. Add Routing I/O data for the modules.

If the SmartGuard controller is controlling safety DIO modules on the DeviceNet network, using the Routing I/O feature allows the values of the I/O points on the DIO modules to be passed to a standard controller or an HMI interface on the EtherNet/IP network.

TIP Modules appear only in the routing I/O table after they have been added to the Safety Scan list and you have clicked Apply.

- a. Under Routing I/O, click New.
- b. Expand the node that you would like to add routing data for.
- c. Expand one of the listed assemblies.

- d. Select the byte you would like to add.



- e. Click OK.
 - f. Repeat steps a...e to add additional Routing I/O.
8. Under I/O Tag, click New to create an I/O tag.

Multiple I/O tags can be defined in an I/O assembly. I/O tags up to 16 bytes can be defined in each I/O assembly. The I/O tags here can be used in the Logic Editor. For example, you can create tags that represent faults from instructions in your function block code, and then display these on an HMI device.

The following dialog box appears.

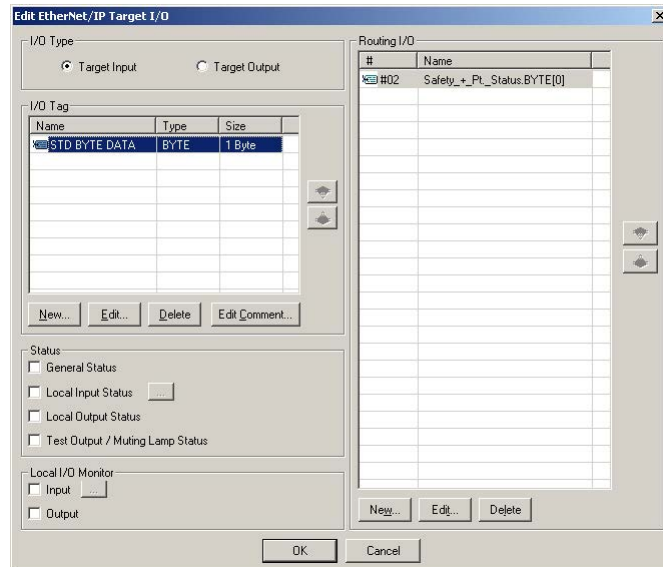


9. Enter a name for the tag and check the type.

The choices are BOOL, BYTE, WORD, or DWORD.

10. Click OK.

The following dialog box appears.



11. Create a tag name for each bit in an I/O assembly.
 - a. Under I/O Tag, select the applicable assembly and click Edit Comment.
 - b. Enter a comment for each bit in the tag.

The tag name comments entered here are displayed in the Logic Editor.

- c. Click OK.
12. Click OK to return to the EtherNet/IP Target I/O tab.

You can create additional input or output assemblies needed for your application by repeating steps 2...11.

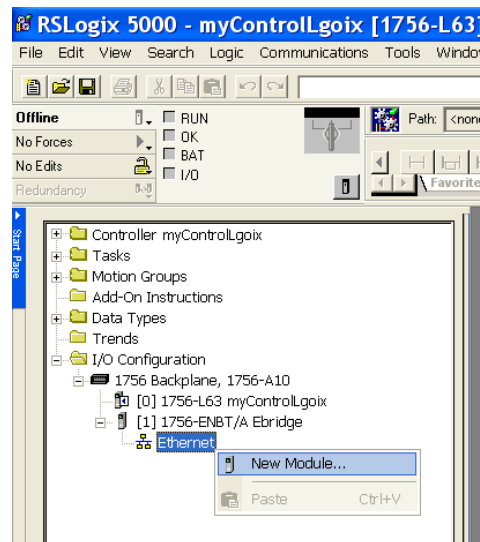
13. To save your configuration, from the file menu, choose save.

Set Up Your Controller as a Slave by Using RSLogix 5000 Software Generic Profile

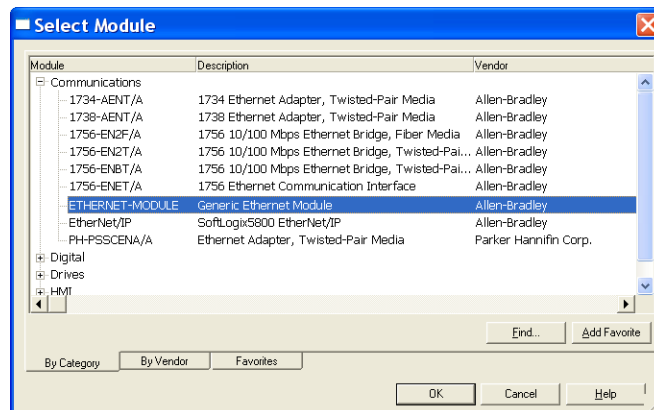
Once you have configured the data to be shared in the SmartGuard controller, you can now use the RSLogix 5000 software and the standard generic profile to exchange that data with a Logix controller.

Follow these steps to connect to the controller.

1. Right-click the Ethernet network in the controller organizer and choose New Module.

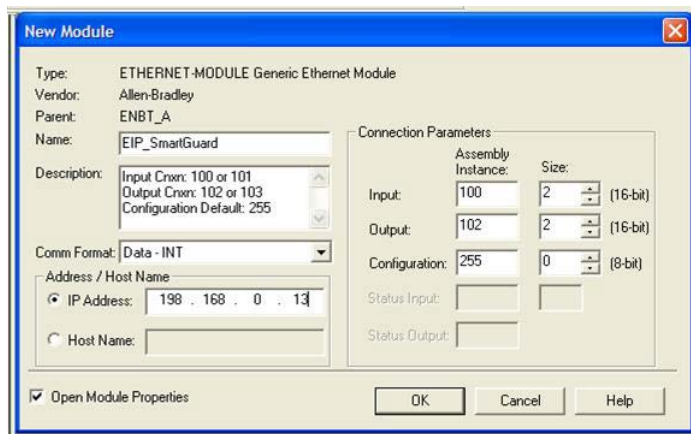


2. Expand the Communications group and select ETHERNET-MODULE.



3. Click OK.
4. On the New Module dialog box, set the parameters as needed.

This dialog box shows the instance values for an input/output connection.



The table provides the instance values for an input/output connection and input only connection.

Connection Type		Instance Number
Input/Output	Input (SmartGuard controller to controller)	100, 101
	Output (controller to SmartGuard controller)	102, 103
Input only	Input	100, 101
	Output	199

5. Click OK.

Configure Communication between a Standard PanelView Terminal and a SmartGuard 600 Controller over an EtherNet/IP Network

Follow these steps to configure a standard PanelView terminal to be able to communicate with a SmartGuard 600 controller over an EtherNet/IP network.

1. Open your PanelView application within PanelBuilder™ 32 software.

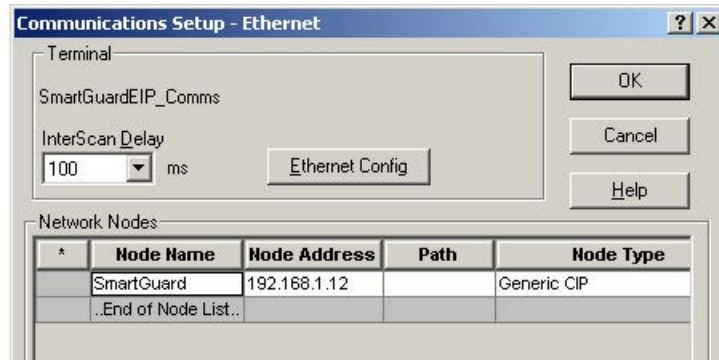
You need to define the communication path between the PanelView terminal and the SmartGuard 600 controller.

2. Click Communications Setup.



The Communications Setup - Ethernet dialog box appears.

3. Click Insert.
4. Enter the node name and node address of the SmartGuard controller.
5. Enter the node type as Generic CIP.



6. Click OK.

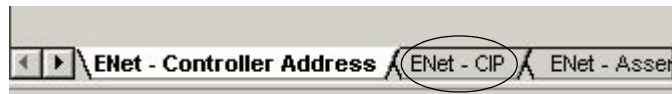
Follow this procedure to define tags within the PanelView tag database that will access the target I/O assemblies in the SmartGuard 600 controller.

1. Click Tag Editor in the application explorer.



The application's tag editor opens.

2. On the bottom of the tag editor, click the ENet-CIP tab.



3. Click Insert to add a new tag.



4. In the new tag cells, type the Tag Name, a Data Type, and Node Name (which matches the node name you defined for the SmartGuard controller in the Communications Setup).

In this example, we chose DINT as the data type.

	Tag Name	Data Type	Descrip	Node Name
1	SG_InputAssembly	DINT		SmartGuard

There can be up to four target I/O assemblies configured in the SmartGuard controller (two input and two output).

For input assemblies, the CIP message codes include the following:

- Service: 0xE - Get Single Attribute
- Class: 4
- Instance: 100 or 101 (input 1 or input 2 respectively)
- Attribute: 3

For output assemblies, the CIP message codes include the following:

- Service: 0x10 - Set Single Attribute
- Class: 4
- Instance: 102 or 103 (output 1 or output 2 respectively)
- Attribute: 3

This example shows a CIP message code that accesses Input Assembly 1 of the SmartGuard controller.

The member field is always defined as 1.

1. From the Service Code pull-down menu, choose the CIP service code.
2. Type the class, instance, and attributes codes for the tag in order to access the correct target I/O assemblies in the SmartGuard controller.

	Tag Name	Data Type	Descrip	Node Name	Initial Value	Array Size	Service Code	Class	Instance	Attribute	Member	Byte Offset
1	SG_InputAssembly	DINT		SmartGuard	0	0	Get Attribute Single (0xE)	4	100	3	1	0

The maximum size of a single member tag defined in the PanelView terminal is a DINT (4 bytes). A target I/O assembly in the SmartGuard controller can be as large as 16 bytes. In order to access all of the bytes in the target assembly, you may need to create up to 4 DINT tags, where an Offset is defined for each tag to correspond with the target bytes of that tag.

Set Controller Modes

Introduction

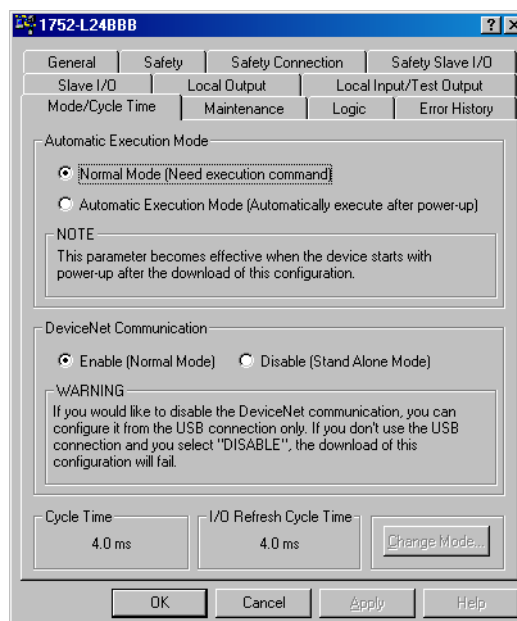
Topic	Page
Set Automatic Execution Mode (optional)	135
Set Standalone Communication Mode (optional)	136
Change Controller Mode	137

Set Automatic Execution Mode (optional)

The controller can be configured for Normal mode or Automatic Execution mode. Set the Automatic Execution mode only after the system has been configured. The setting becomes effective after you have cycled power following a configuration download.

Follow these steps to set the mode.

1. Right-click the controller and choose Properties.
2. Select the Mode/Cycle Time tab.



3. Choose either Normal Mode or Automatic Execution Mode.

Mode	Description
Normal	The controller starts in Idle mode when the power supply is turned on. You must use RSNetWorx for DeviceNet software to change to Execute mode by clicking Change Mode on the Mode/Cycle Time tab of the Controller Properties dialog box.
Automatic Execution	The controller starts in the Execute mode when the power supply is turned on, if the configuration has been locked and the controller was in Execute mode before the power supply was turned off.

4. Click OK.

Set Standalone Communication Mode (optional)

The SmartGuard controller can operate with or without DeviceNet communication enabled. The default setting is enabled.

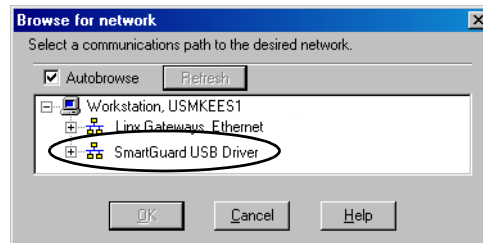
In Standalone mode, the cycle time of the controller is shorter, but none of the DeviceNet communication functions can be used.

If you want to use the SmartGuard controller in Standalone mode, you can disable DeviceNet communication and use the USB connection to configure the module.

IMPORTANT If you disable DeviceNet communication and you do not use the USB connection, the configuration download will fail.

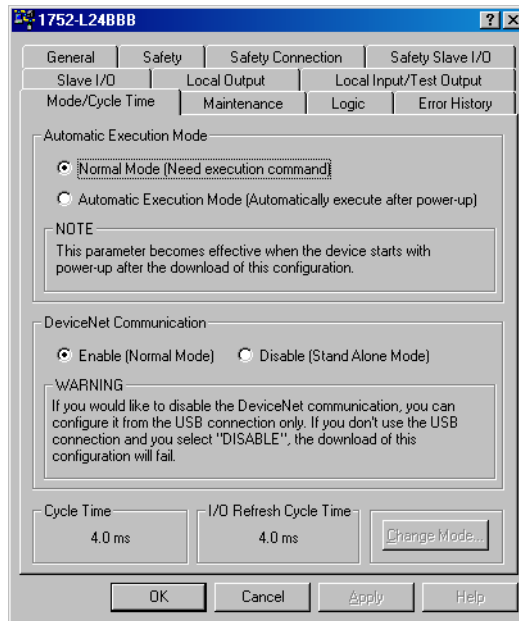
Follow these steps to disable DeviceNet communication.

1. Make sure you are connected to the programming device by using the USB connection.
2. If you haven't already, set up a path to use the USB connection in RSNetWorx for DeviceNet software.
 - a. From the Network menu, choose Properties.
 - b. On the DeviceNet dialog box, click Set Online Path.
 - c. On the Browse for Network dialog box, select the desired path and click OK.



3. In RSNetWorx for DeviceNet software, right-click the controller and choose Properties.

4. Select the Mode/Cycle Time tab.



5. Choose Disable (Stand Alone Mode) and click OK.

Change Controller Mode

Follow these steps to change the controller mode.

1. Go online with the SmartGuard controller.
2. Right-click the controller and choose Properties.
3. Select the Mode/Cycle Time tab on the Controller Properties dialog box.
4. Click Change Mode.
5. Select the Idle or Execute radio button.
6. Click OK.

Notes:

Create Your Application Program

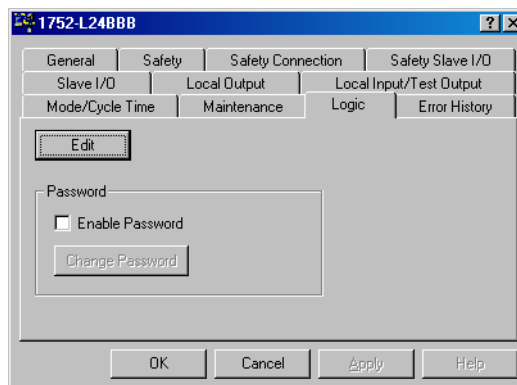
Introduction

Topic	Page
The Logic Editor	139
Programming Basics	140
Creating a Function Block Program	144
Edit Function Block Parameters	146
Find Function Blocks with Open Connections	148
Program on Multiple Pages	149
Save the Program	150
Update the Program	150
Monitor the Program Online	151
Program Execution Sequence	152
User-defined Function Blocks	152
Additional Resources	157

The Logic Editor

You program the SmartGuard 600 controller by using the Logic Editor in RSNetWorx for DeviceNet software. The Logic Editor consists of a object list, where function blocks, I/O tags, and other programming elements are registered, and a workspace, where programming is performed.

Open the Logic Editor by choosing the Logic tab on the Edit Device Parameters dialog box and clicking Edit.



You can password-protect your application program to prevent unauthorized editing, verification, or printing of programs. To create a password, follow these steps.

1. On the Logic tab of the Controller Properties dialog box, check the Enable Password checkbox.
2. On the Change Password dialog box, type in the password in the New Password field.

Passwords may contain up to six characters.

3. Re-type the password in the Confirm Password field.
4. Click OK.

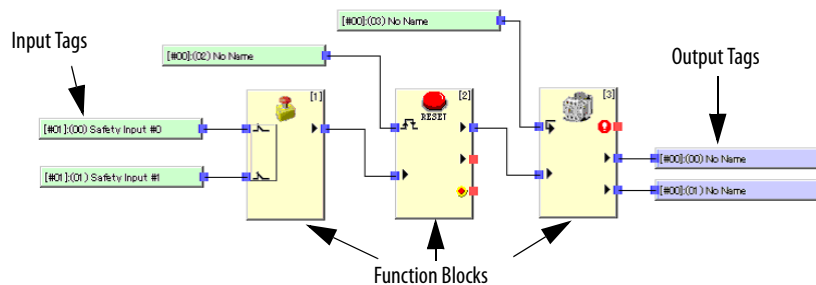
The password will be requested whenever the Edit button is clicked to open the Logic Editor. You can upload or download the program without the password, but program edit, verification, print and report functions are not available.

IMPORTANT If you forget the password, it cannot be recovered.

Programming Basics

Programs are created from logic functions and function blocks that indicate commands, from input tags that indicate data input sources, and from output tags that indicate data output destinations. The I/O are connected with connection lines.

Figure 29 - I/O Connections



Logic Functions and Function Blocks

A maximum of 254 logic functions and function blocks can be used.

Table 8 - Supported Logic Instructions and Function Blocks

Logic Instructions	Function Blocks
•NOT	•Reset
•AND	•Restart
•OR	•Emergency stop push-button monitoring
•Exclusive OR	•Light curtain monitoring
•Exclusive NOR	•Safety gate monitoring
•Routing	•Two-hand controller
•RS Flip-Flop	•Off-delay timer
•Multi Connector	•On-delay timer
•Comparator	•User Mode Switch
	•External device monitoring
	•Muting
	•Enable switch
	•Pulse generator
	•Counter

Input Tags

Input tags reflect the status of inputs from these I/O areas:

- The controller's local terminals
- Input area of safety slaves registered as communication partners
- Input area reflected from safety master data
- Input area reflected from standard master data

Data are reflected in these I/O areas:

- local input status
- local output status
- general unit status
- test output status
- muting lamp status

In the object list, I/O tags are displayed with symbols to indicate how they are configured.

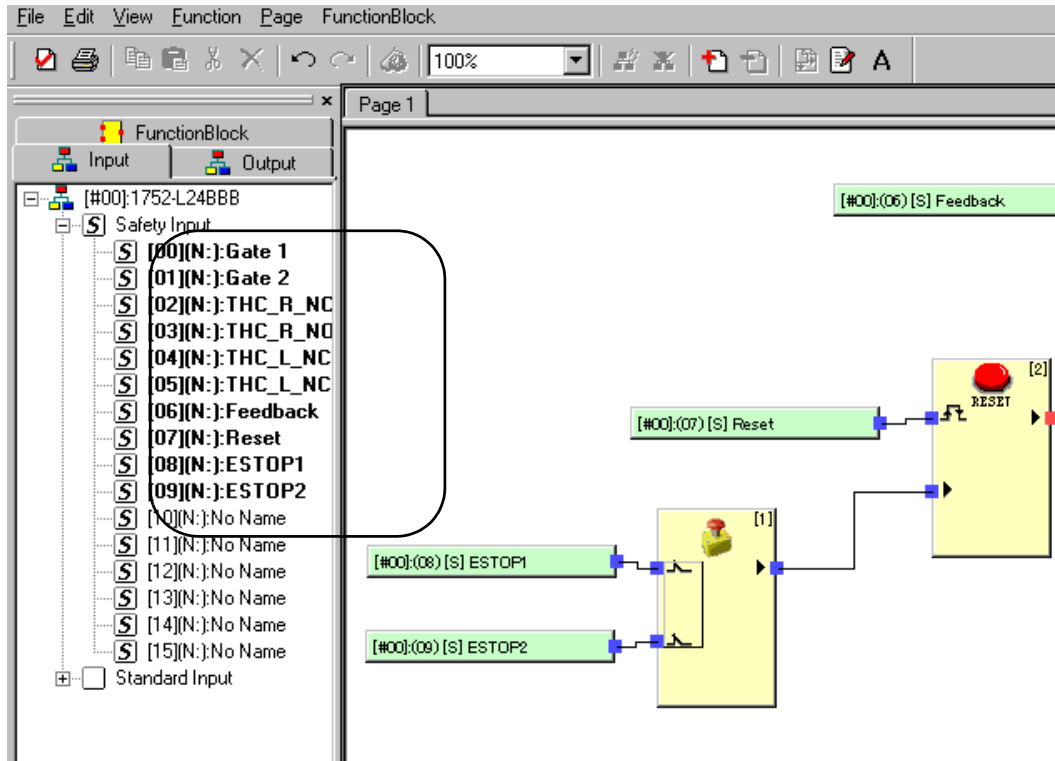
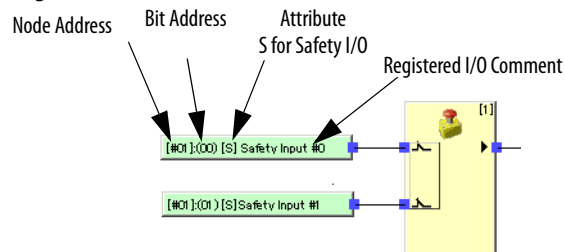


Table 9 - Input Tag Symbols

Input Mode	Symbol	Channel Mode	Symbol
Not Used	N	Single	None
Test Pulse From Test Out	P	Dual Channel Equivalent	e
Used As Safety Input	S	Dual Channel Complementary	c
Used As Standard Input	ST		—

When used in the workspace, input tags include the node address, bit address, attribute (S for safety, none for standard), and registered I/O comment.

Figure 30 - Input Tags



Output Tags

Output tags reflect the status of outputs from these I/O areas:

- The controller's local terminals
- Output area of safety slaves registered as communication partners
- Output area reflected from safety master data
- Output area reflected from standard master data

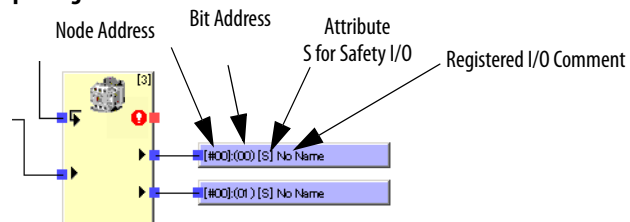
In the object list, I/O tags are displayed with symbols to indicate how they are configured.

Table 10 - Output Tag Symbols

Output Mode	Symbol	Channel Mode	Symbol
Not Used	N	Single	None
Safety	S	Dual	d
Safety Pulse Test	P	—	—

When used in the workspace, output tags include the node address, bit address, attribute (S for safety, none for standard), and registered I/O comment.

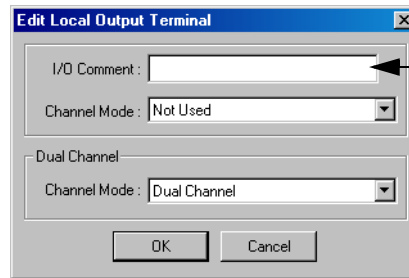
Figure 31 - Output Tags



I/O Comment Function

The I/O comment is an optional name, consisting of up to 32 ASCII characters that can be registered in the controller for each I/O terminal by using RSNetWorx for DeviceNet software. These I/O comments can be used in the object list of the Logic Editor as I/O tags, simplifying programming.

Figure 32 - I/O Comment



Programming Restrictions

Items, such as I/O tags and function blocks, can be used on each page with the following restrictions:

- The same input tag can be placed on more than one page.
- The same input tag can only be used once on each page.
- Each output tag can only be used once in the application program.
- Only function blocks can be copied. 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 254 function blocks can be used.
- A maximum of 128 number jump addresses can be used.
- A maximum of 32 pages can be used.
- A maximum of 128 text boxes can be used for program comments.
- The page setup cannot be changed if there are any items on the workspace. Set up the size of the workspace first by choosing File>Page Setup.

Creating a Function Block Program

To create a program using function blocks, you create connections from the function block to input and output tags.

Add an Input or Output Tag

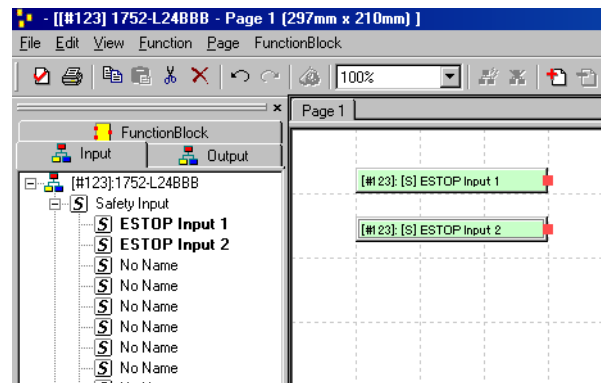
Follow these steps to add a tag.

1. Click the Input or Output tab in the object list.

2. Select the tag you want to use, and drag and drop it into position on the workspace.

You can select multiple I/O tags and position them at the same time.

Figure 33 - Place Input Tags



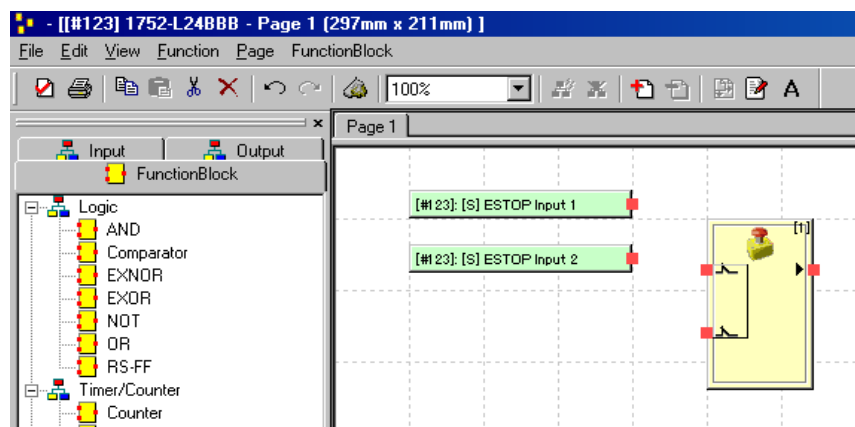
TIP Input and output tags that are used in the application program appear bolded in the object list.

Add a Function Block

Follow these steps to add a function block to the workspace.

1. Click the Function Block tab in the object list.
2. Select the function block you want to use, and drag and drop it into position on the workspace.

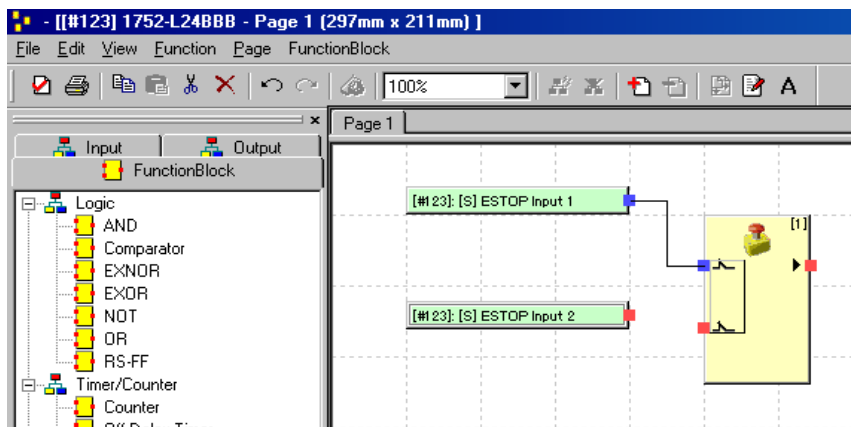
Figure 34 - Place a Function Block



Connect the Tags to the Function Block

To connect the I/O tags to the function block, click the source connector (?) and drag it to the destination connector (?).

Figure 35 - Connect Tags to Function Blocks

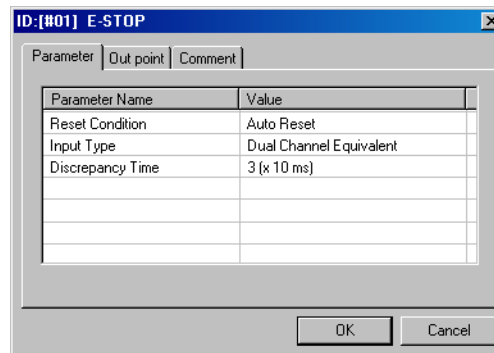


Edit Function Block Parameters

You can edit function blocks by changing parameter settings, changing the number of inputs or outputs, adding optional I/O, and adding comments pertaining to your application. The parameters that can be edited depend upon the type of function block.

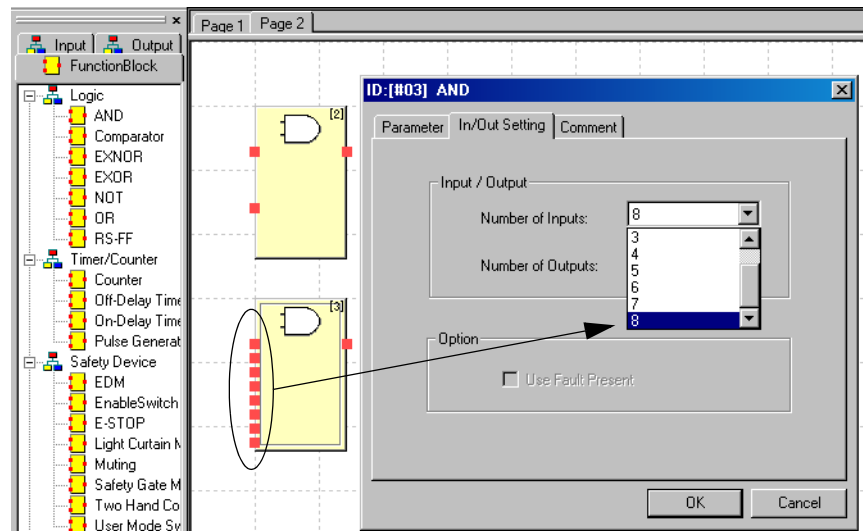
To open the Function Block Properties dialog box, right-click the function block and choose Edit.

Figure 36 - Parameter Tab



In/Out Settings

You can edit the Number of Inputs, Number of Outputs, and, in some cases, the Fault Present settings for many instructions.

Figure 37 - In/Out Setting Tab

Number of Inputs

The number of inputs for logic functions can be increased or the optional input to function blocks can be enabled.

Number of Outputs

The number of outputs for logic functions can be increased or the optional outputs, such as error outputs, from function blocks can be enabled.

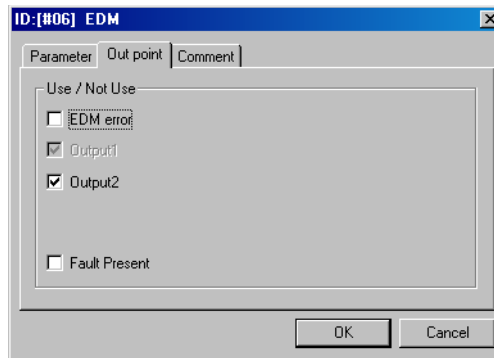
Fault Present Bit

You can enable the Fault Present diagnostic-status bit in some function blocks by selecting the checkbox located on the In/Out Setting tab of the Function Block Properties dialog box. If the Use Fault Present checkbox is checked, an additional Fault Present output is displayed on the function block.

Optional Output Point Selections

You can enable optional outputs, including the Fault Present bit for some functions blocks, by checking the appropriate checkboxes on the Out point tab of the Function Block Properties dialog box. When the optional outputs are checked, they are displayed on the function block.

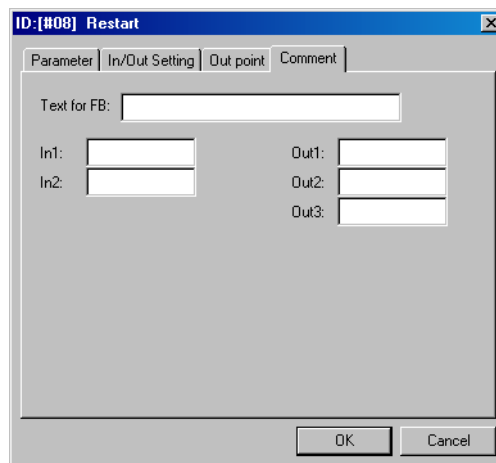
Figure 38 - Out point Tab



Comments

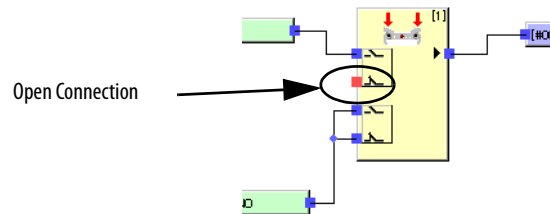
Choose the Comments tab to type a name for the function block or I/O signals. The names of I/O signals are not displayed in the workspace, but the name of the function block is displayed under the function block in the workspace. All names typed in this dialog box are printed when the application program is printed.

Figure 39 - Comment Tab



Find Function Blocks with Open Connections

Newly created programs containing function blocks with open inputs or outputs cannot be downloaded. All I/O must be used.

Figure 40 - Function Block With Open Connections

To find all open connections in the Logic Editor, choose Edit>Search OpenConnection.


The Open Connection dialog box shows all the function blocks with open connections. Double-click an item on the list to display the function block. Open connections are shown in red in the workspace.

TIP If a jump address is used for the I/O point and the corresponding jump address is not used, the I/O point will not be displayed in red and will appear to be connected.

See [Program on Multiple Pages](#) on page 149 for information on jump addresses.

Program on Multiple Pages

The SmartGuard 600 controller supports up to 32 pages of programming logic.

To create a new page, click the Add Page icon .

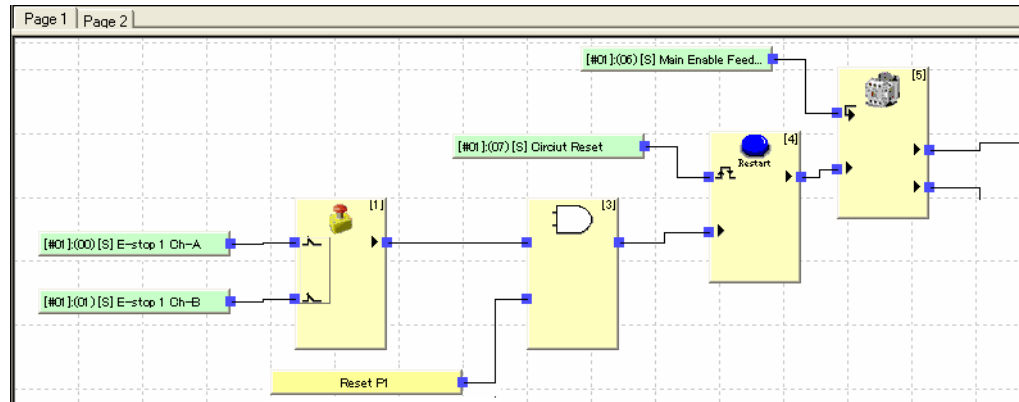
Use jump addresses to connect logic between pages. A SmartGuard 600 controller program can contain up to 128 jump addresses.

Follow these steps to create a jump address.

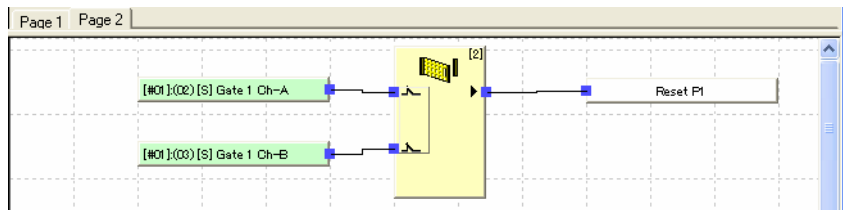
1. Right-click anywhere on the programming page and choose Make JumpAddress.
2. Type a name for the jump address.



3. Connect the jump address to the function block.



4. Select the page to which you want to connect the logic.
5. Right-click anywhere on the page and choose Select JumpAddress.
6. Select the jump address from the pull-down menu.
7. Connect the jump address to the function block.



Save the Program

Follow these steps to save your application program.

1. Choose File>Apply.

The program is saved temporarily in RSNetWorx for DeviceNet software.

2. Exit the Logic Editor by choosing File>Exit.
3. Click OK or Apply on the Edit Device Parameters dialog box.

If you do not click OK or Apply or you click Cancel, none of your program changes are saved. Any programming saved temporarily by using File>Apply is deleted.

4. Choose Save or Save As from the RSNetWorx for DeviceNet software main dialog box.

Update the Program

If the I/O tags of safety slaves that configure the SmartGuard controller's local I/O are changed, you must start the Logic Editor and check the program.

If you load the parameters to the controller without starting the Logic Editor, a download error occurs in the Logic Editor because of data inconsistency. If this

error occurs, start the Logic Editor and check the program, making any necessary modifications.

Monitor the Program Online

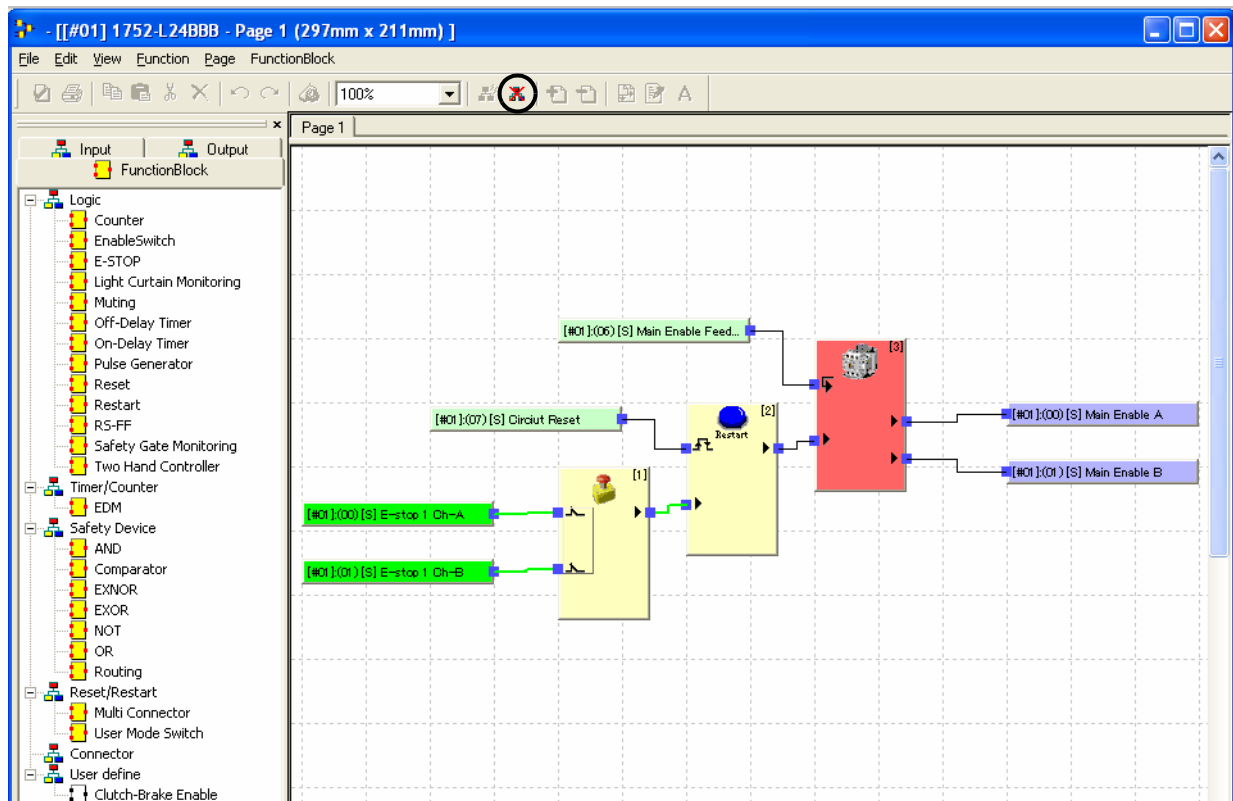
The I/O tag values and signal states of connections with function blocks can be monitored online in the Logic Editor. Make sure that RSNetWorx for DeviceNet software is connected to the network and that the controller being monitored is in Run mode before starting online program monitoring.

IMPORTANT You may need to change the controller's mode to Execute Mode to monitor online.

To start online monitoring, click Monitoring  on the toolbar.

During monitoring, the I/O tags or connections that are on are displayed in a darker color.

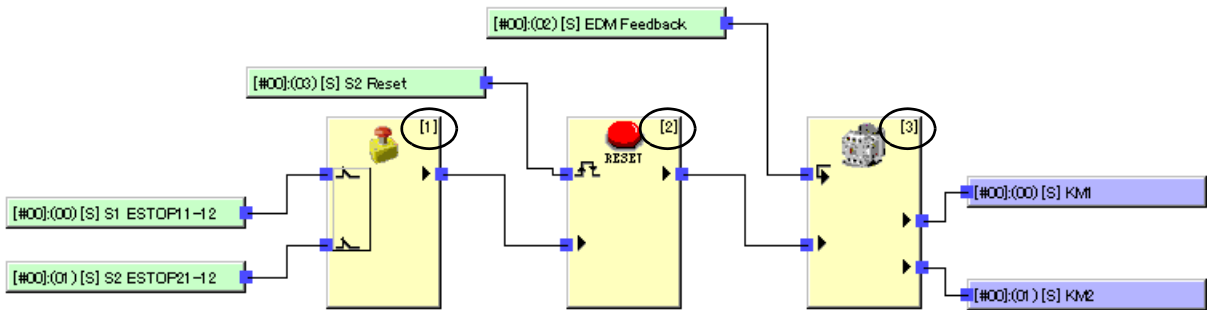
To stop online monitoring, click Stop Monitoring on the toolbar.



Program Execution Sequence

The order of execution of function blocks is automatically set by the Logic Editor and displayed in the right-hand corner of each function block.

Figure 41 - Example Program

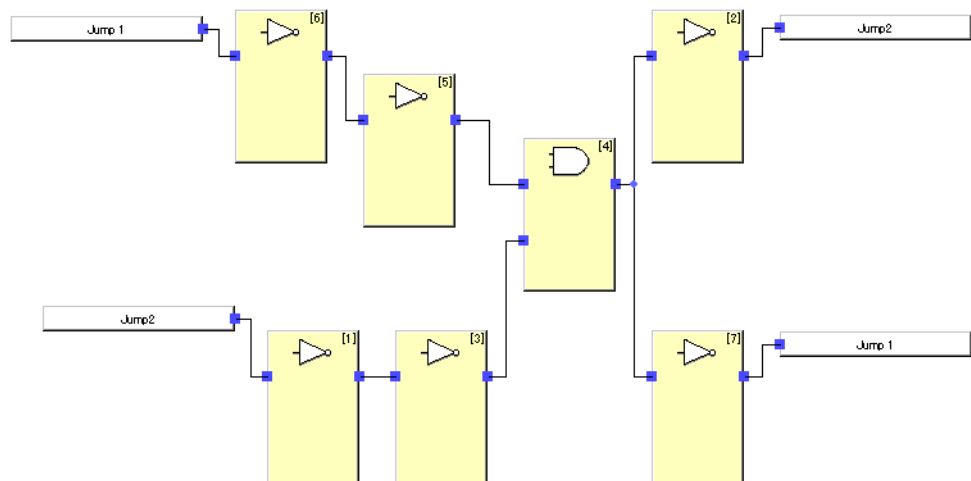


In this example, the execution order is:

1. E-stop
2. Reset
3. External Device Monitoring (EDM)

Jump addresses can be used in programs to create loopbacks. If a program contains more than one loopback, for example a jump 1 to jump 1 and a jump 2 to jump 2, the sequence of execution is in the order that the function blocks are positioned. Carefully test all programs containing more than one loopback to make sure they execute properly.

Figure 42 - Loopback Example



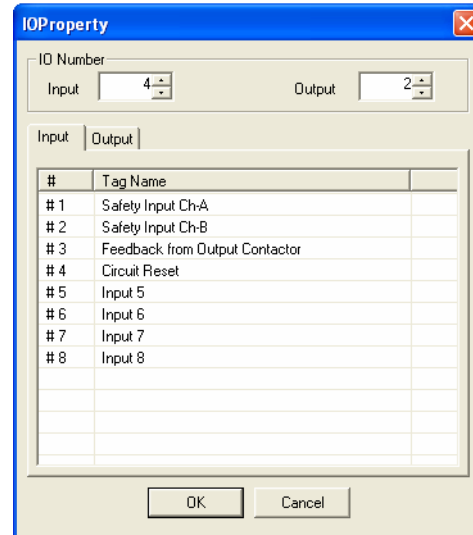
User-defined Function Blocks

The Logic Editor lets you create user-defined function blocks that consist of existing function block logic. Once created, these function blocks are stored in a user-defined library and can be used in any SmartGuard controller application.

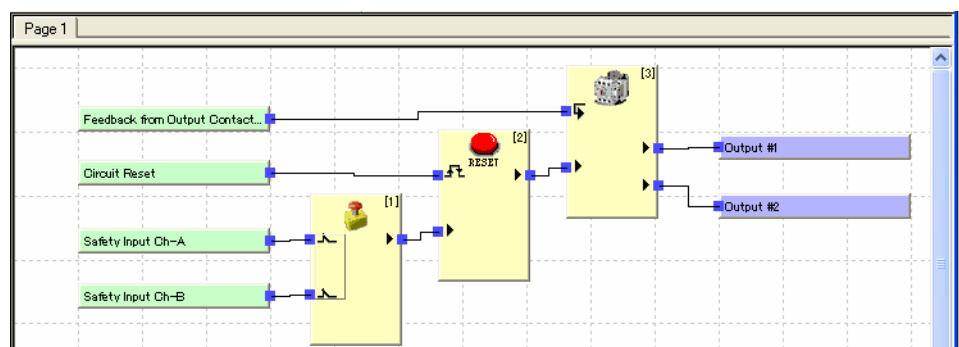
Create User-defined Function Blocks

Follow these steps to create a user-defined function block.

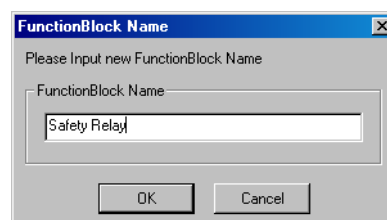
1. Open the Logic Editor by right-clicking the controller, choosing Properties, and clicking Edit on the Logic tab.
2. Choose FunctionBlock>Create.
3. On the IOProperty dialog box, define the number of inputs and outputs for the function block.



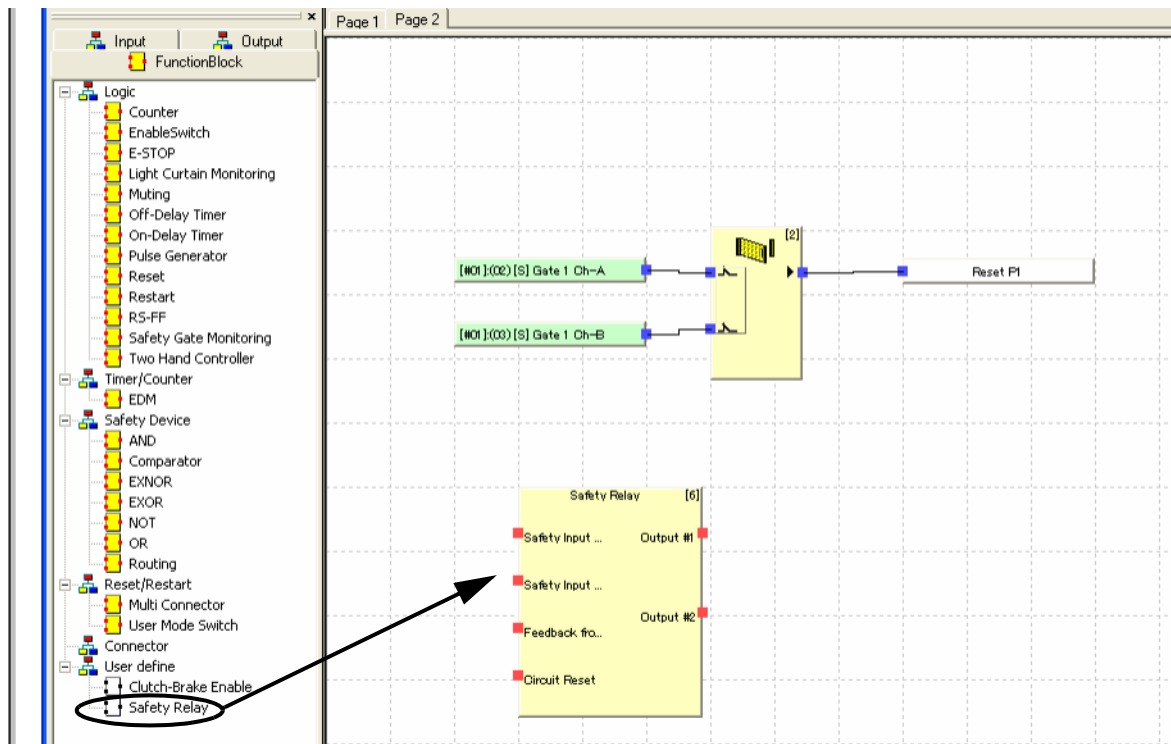
4. Assign names to each input and output.
5. Click OK to open the Function Block Logic Editor.
6. Write the logic for the function block.



7. Choose File>Save and type a name for the function block, when prompted.



8. Add the new function block to your application logic.



TIP If you wish to edit your user-defined function block, it cannot be used in the current application. If it is, the edit option is unavailable.

IMPORTANT Always download programs with user-defined function blocks to the controller, check their configuration, and verify their operation before using them in an application.

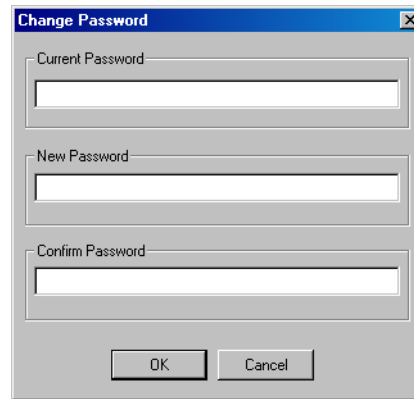
Password Protect User-defined Function Blocks

You can set a password to protect user-defined function block files from unauthorized edits. Verify, report, and print operations are not password-protected.

To set a password, follow these steps.

1. To open the Function Block Editor, right-click a user-defined function block and choose Edit.

2. In the Function Block Editor, choose File>Change Password.



3. Type a password of up to six alphanumeric characters in the New Password field.
4. Re-type the password in the Confirm Password field.
5. Click OK.

The user-defined function block cannot be edited or deleted without entering the password.

We recommend using a password to protect user-defined function blocks that have been tested to prevent unauthorized or unintentional changes once the function block has been allocated in a user program.

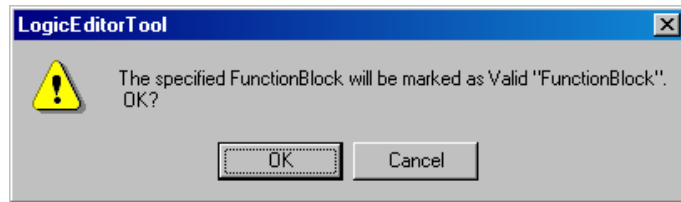
Reuse User-defined Function Block Files

Project files (*.dnt) and user-defined function block files (*.fbd) exist as separate files. You can reuse user-defined function block files when creating programs. You must have Windows Administrator rights to import, save, delete, check, or edit user-defined function blocks.

To reuse user-defined function blocks, follow these steps.

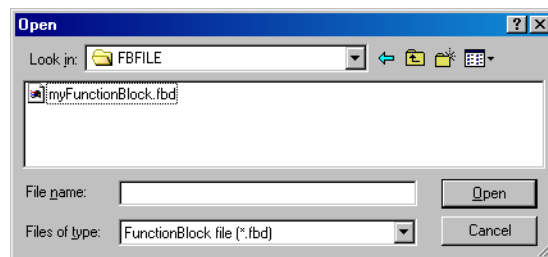
1. Create the user-defined function block as described on page [152](#).
2. Check the operation of the user-defined function block.
 - a. In the object list of the Logic Editor, right-click the new function block and choose Edit.
 - b. Review the function block program and correct any problems.
 - c. Save the function block program, if you made any changes.
 - d. Close the Function Block Logic Editor.

3. Validate the user-defined function block.
 - a. In the object list of the Logic Editor, right-click the new function block and choose Validate.
 - b. Click OK on the confirmation dialog box.



The icon for the new function block changes from white to yellow to indicate that the function block has been validated.

4. Export the user-defined function block to a file.
 - a. In the object list of the Logic Editor, click the saved user-defined function block.
 - b. From the main menu, choose FunctionBlock>Export.
 - c. In the Save As dialog box, type a name for the file and click Save.
5. Move or copy the file to other personal computers, if necessary.
6. Import the user-defined function block.
 - a. In RSNetWorx for DeviceNet software, create a new project and add a SmartGuard controller.
 - b. Right-click the controller, choose Properties and select the Logic tab.
 - c. Click Edit to start the Logic Editor.
 - d. Choose FunctionBlock>Import.



- e. Select the appropriate file and click Open.


The imported, user-defined function block is displayed in the object list of the logic editor.

IMPORTANT Always import user-defined function block files before editing or verifying application programs that will use them.

Precautions for Reusing User-defined Function Blocks

This table indicates which actions require user-defined function block files and describes what happens if the action is attempted without the function block file.



Table 11 - Outcomes Without Function Block Files

Action	File	Outcome
Download	Not required	Operates normally
Upload	Not required	Operates normally
Save project file	Not required	Operates normally
Load project file	Not required	Operates normally
Verification	Required	Program verification can be completed even without the function block file once the file is downloaded to the controller, but the function block configuration cannot be checked.
Edit the program	Required	A warning message will appear if the Logic Editor is opened without the function block file. The user-defined function block without a file will appear with a  icon and any connections to or from it are deleted. Editing features such as copy and paste are not available. If the program is edited in any way, it cannot be saved or downloaded.
Apply program	Required	This command cannot be executed without the user-defined function block file.

TIP If you import the user-defined function block file with the program open, it will not automatically update. Close the program and open it again to display the function block correctly.

IMPORTANT Always check the original program after editing user-defined function blocks. If you created a user-defined function block, used it in the original program, and edited the function block after the original program was saved, the function block occurrence in the program is not updated.

Additional Resources

Resource	Description
 Logic Functions Command Reference	Provides detailed information on the logic functions.
 Function Blocks Command Reference	Provides detailed information on the function blocks.

Notes:

Download and Verify

Introduction

Topic	Page
Download the DeviceNet Network Configuration	159
Verifying Your DeviceNet Safety Configuration	161
Start the Safety Device Verification Wizard	161
Determine if Devices Can Be Verified	161
Select Devices to Verify	163
Review the Safety Device Verification Reports	164
Lock Safety Devices	166
View the Safety Device Verification Wizard Summary	167

Download the DeviceNet Network Configuration


Before you download, you must go online to the DeviceNet network by using RSNetWorx for DeviceNet software. Your computer and the devices you wish to communicate with must be connected to the DeviceNet network. Or, if you are running your controller in standalone mode, your computer must be connected to the SmartGuard controller's USB port.

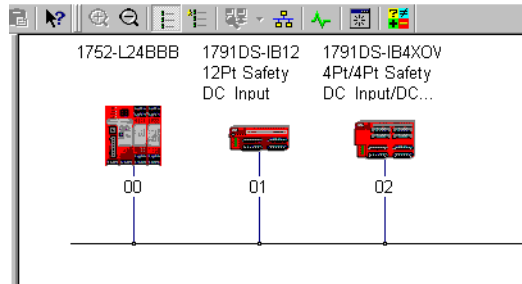
If you are connected to the SmartGuard controller using EtherNet/IP protocol, you need to follow the steps in this section. When connected to the SmartGuard via the EtherNet/IP protocol, you are essentially bridging through the SmartGuard controller to the DeviceNet network, and then going online, downloading and monitoring. Though this chapter deals with using DeviceNet protocol, you need to follow the same steps for EtherNet/IP protocol.

When you go online to a DeviceNet network, RSNetWorx for DeviceNet software browses the network one time and shows you the devices on the network. It does not read (upload) or change (download) the parameters of any of the devices.

The graphics representation of the network created by the browse operation remains static. It does not automatically update to show changes since the last browse, unless the Continuous Browse option is selected.

Follow these steps to download the DeviceNet network configuration.

1. Go online by clicking the online  icon.
2. Browse to the DeviceNet network and click OK at the prompt.



During each browse operation, RSNetWorx for DeviceNet software reads the following attributes of each device.

Safety Attribute	Description
Safety Network Number (SNN) and Node Address Combination	The node address and SNN stored in the RSNetWorx for DeviceNet configuration file must match the node address and SNN of the online device. If the SNNs do not match, the device enters the SNN error state. See page 65 for information on resolving an SNN mismatch error.
Configuration Signature	RSNetWorx for DeviceNet software compares the configuration signature in its configuration file with the configuration signature in the online device.
Safety-Lock	If the device is safety-locked, its configuration cannot be modified without first unlocking the device.

3. Download your configuration to the network by right-clicking the device and choosing Download to Device.
4. Confirm your intent to download by clicking Yes.

If a device is password-protected, RSNetWorx for DeviceNet software prompts you to type the password for each protected device.

If a device is safety-locked, you must first unlock the device and then download.

IMPORTANT If you safety-unlock a device, you must run the Safety Device Verification Wizard to re-verify and safety-lock the device before operating the device in your safety system.

TIP If none of your devices are password-protected or safety-locked, you can choose Download to Network from the Network menu to download your configuration to the network. However, this process skips devices that are password-protected or safety-locked.

Verifying Your DeviceNet Safety Configuration

IMPORTANT Before running the Safety Device Verification Wizard, you should browse and upload your network and test the safety devices and all of their safety functions on your network to verify that they are operating properly. You must fully test your application prior to safety-locking your devices.

Refer to the SmartGuard Controller Safety Reference Manual, publication [1752-RM001](#), for information on verification testing for safety applications.

The Safety Device Verification Wizard, accessed from RSNetWorx for DeviceNet software, guides you through the process of verifying the configuration of your safety devices and provides the means for safety-locking those devices. The verification process includes upload and comparison of the configuration stored in the device and the configuration stored in the RSNetWorx for DeviceNet software configuration file. The configuration is displayed in a report to facilitate visual verification and record keeping.

IMPORTANT Some devices on your network may not support verification by the Safety Device Verification Wizard. Consult the user documentation to determine the method required for verifying these devices.

Start the Safety Device Verification Wizard

Follow these steps to run the Safety Device Verification Wizard.

1. Choose Network>Safety Device Verification Wizard.

The Welcome dialog box, which describes the verification process, appears.

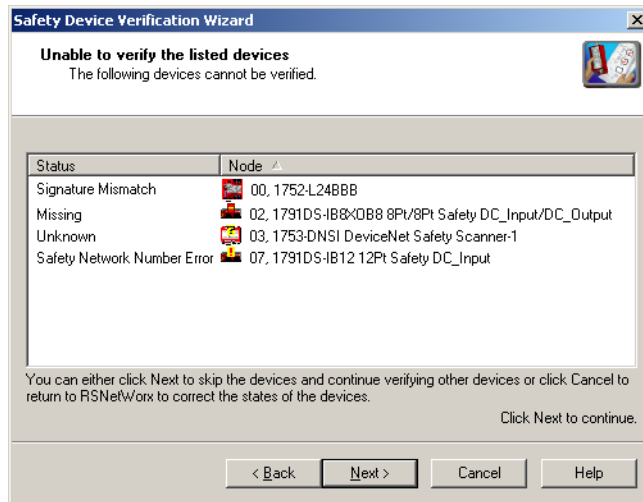
2. Click Next.






Determine if Devices Can Be Verified

When the Safety Device Verification Wizard browses the network, it checks the safety status of the devices on the network to determine if the devices can be verified.

If any devices are in a state that prevents the wizard from continuing the verification process, the Unable to verify the listed devices dialog box appears

listing those devices and their current status, including a device icon overlaid with a status icon.



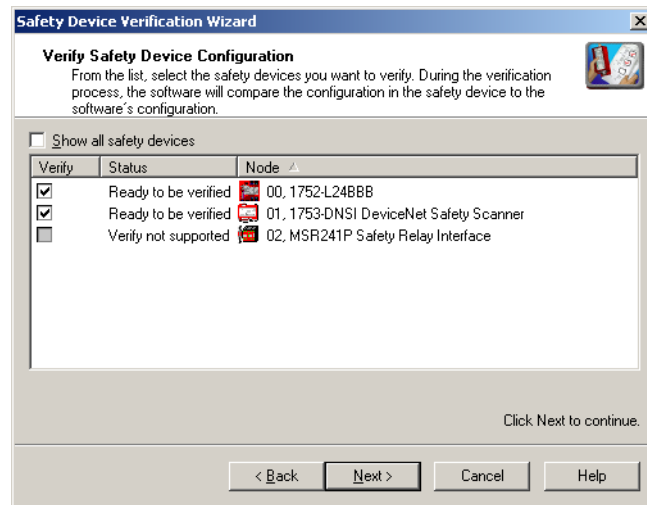
Status	Icon Overlay	Description
Missing		The device is part of the network configuration, but was not found during the browse operation.
Mismatch		The device identity in the network configuration does not match the identity of the online device.
Unknown		The device is in the configuration, but has not been detected on the network yet.
Safety Network Number Error		The safety network number (SNN) in the device is either invalid or does not match the SNN for the device in the RSNetWorx for DeviceNet configuration file.
Signature Mismatch	None	The configuration signature in the device does not match the configuration signature in the RSNetWorx for DeviceNet configuration file.
Safety Locked		The device is already locked.

To return to RSNetWorx for DeviceNet software so that you can correct the status of the indicated devices, close the Safety Device Verification Wizard by clicking Cancel.

To skip the devices listed and continue the verification process for other safety devices on the network, click Next.

Select Devices to Verify

Choose which devices to verify by using the checkboxes in the Verify column of the Verify Safety Device Configuration dialog box. You can select only the devices whose status is Ready to be verified.



If the Show all safety devices checkbox is checked, the dialog box lists all of the safety devices on the network and shows their current status. If it is unchecked, which is the default, only devices with the following status are shown:

- Verify FAILED

The upload and compare operation indicated that the configuration in the device does not match the configuration in the RSNetWorx for DeviceNet configuration file.

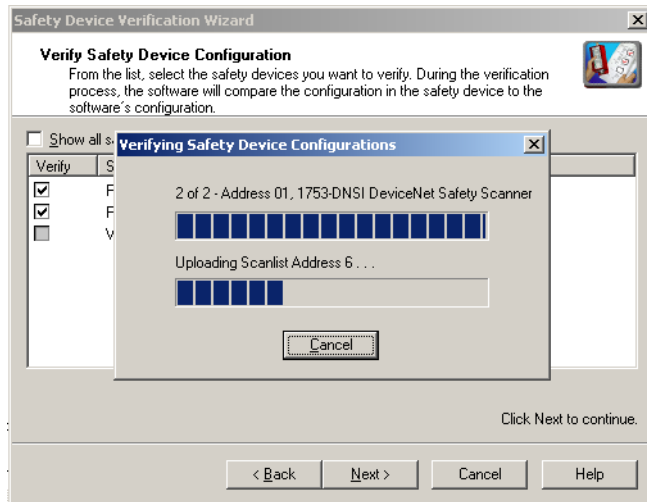
- Ready to be verified

The device is not safety-locked and can be selected for verification.

- Verify not supported

The device is not safety-locked, but the device does not support verification via the Safety Device Verification Wizard. Consult your user documentation for information on how to verify this device. Once the device has been verified, it can be safety-locked by the wizard.

Click Next to begin the upload and compare process.

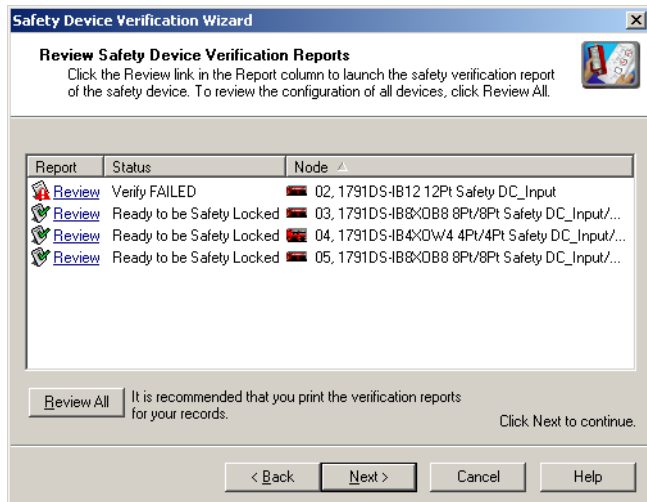


TIP If you click Next without selecting a device to verify, the wizard checks whether any devices were verified or are ready to be locked in this execution of the wizard.

If	Then the wizard displays
Devices were verified	the Review dialog box listing those devices.
Devices are ready to be safety-locked	the Lock dialog box listing those devices.
No devices were verified	the Finish dialog box.
No devices are ready to be safety-locked	the Finish dialog box.

Review the Safety Device Verification Reports

The Review page displays safety devices with status of either Verify FAILED or Ready to be Safety Locked.



1. Click Review in the Report column to launch the device's HTML report in your default browser.
2. Click Review All to generate an HTML verification report for all of the devices listed.

TIP If a device's status is Verify FAILED, more information is provided in the verification failure report.

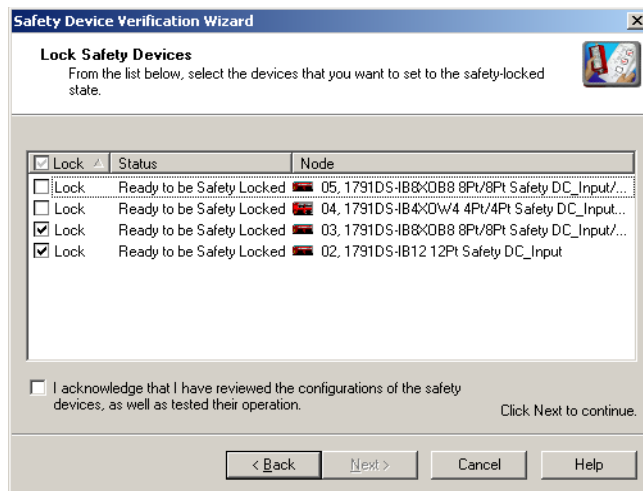
3. Review and print the verification reports for your records.

IMPORTANT You must review the device configurations and record the configuration signatures prior to operating a safety application.

Lock Safety Devices

IMPORTANT Before you lock your safety device configurations, you must perform all of the verification steps required for your application.

1. Choose which devices to safety-lock by checking the checkbox in the Lock column for each device that is ready to be safety-locked.



2. You must check the acknowledgement checkbox before the locking process can continue.
3. Click Next.

The wizard performs a final comparison of the configuration signature in each safety device to its configuration signature in RSNetWorx for DeviceNet software before locking the device.

4. If any of the selected devices are password-protected, you will be prompted to type the password for that device.



If you want to skip the device and allow the locking process to continue for other devices, click Skip.

View the Safety Device Verification Wizard Summary

Before closing, the wizard displays a summary of all the safety devices that were safety-locked, the number of safety devices that still need to be safety-locked, and lets you display the verified and safety-locked state of all of the safety devices on the network.

Click Finish to close the wizard.

Notes:

Monitor Status and Handle Faults

Introduction

Topic	Page
Status Indicators	169
Alphanumeric Display	170
Monitoring I/O Power Supply Input	171
Monitoring I/O Maintenance Information	172
Viewing I/O Status Data	175
Controller Connection Status (safety slave function)	177
Error Categories	179
Error History Table	179
Error History Messages and Corrective Actions	183
Download Errors and Corrective Actions	185
Reset Errors and Corrective Actions	187
Mode Change Errors and Corrective Actions	188

Status Indicators

The SmartGuard 600 controller features status indicators for module, DeviceNet and EtherNet/IP network status, lock, USB and EtherNet/IP communication, individual input and output status, as well as an alphanumeric display for DeviceNet error codes, DeviceNet node address, and EtherNet/IP address information.

For a description of the color and status combinations of the status indicators and recommended actions, see [Appendix B](#).

Alphanumeric Display

The controller's alphanumeric display provides DeviceNet error codes, DeviceNet node address, and EtherNet/IP address information. Under normal operating conditions, the display shows the node address of the module, 00...63 in decimal format. If the controller is operating in a standalone configuration (not networked), the display shows 'nd'. The display flashes when the controller is self-testing, configuring, or in Idle mode. If a fault exists, the display alternates between the error code and the node address where the error occurred. If a fatal error has occurred, the display shows the error code only.

When the service switch is pressed, the display shows the controller's safety-configuration signature two digits at a time. The configuration signature can also be viewed on the Safety tab of the Controller Properties dialog box in RSNetWorx for DeviceNet software. You can use the configuration signature to verify that the program and configuration of the controller has not been changed.

When the IP address display switch is pressed for 1 second or longer, the display shows the EtherNet/IP address that is set. The error code 'n4' is displayed if an error occurs in the EtherNet/IP configuration.

Table 12 - Explanation of Display Operation

Status		Display	
Normal conditions with DeviceNet enabled	Operating mode: Run Safety I/O communication: operating	The controller node address.	Lit
	Operating mode: Run Safety I/O communication: not operating		Flashing
	Operating mode: Self-testing, Configuring, or Idle		Flashing
Normal conditions with DeviceNet disabled	Operating mode: Run	nd	Lit
	Operating mode: Self-testing, Configuring, or Idle		Flashing
Error conditions	Critical error	Error code only	Lit
	Abort	Error code only	Lit
	Nonfatal error	Alternates between the error code and the node address where the error occurred.	

For a description of the combinations of the status indicators and alphanumeric display codes, including corrective actions, see [Appendix B](#).

Monitoring I/O Power Supply Input

You can monitor the I/O power supply input by using the alphanumeric display on the front of the controller, as well as the general status data in DeviceNet I/O communication.

If an I/O terminal on the controller is set to anything other than Not Used, and the normal power supply voltage is not supplied, the alphanumeric display shows:

- P4: The power supply for inputs (V1,G1) is out of range.
- P5: The power supply for outputs (V2, G2) is out of range.

Monitoring I/O Maintenance Information

You can configure a maintenance mode and alarm threshold for each local input, test output, and local output terminal by using the Maintenance tab of the Controller Properties dialog box in RSNetWorx for DeviceNet software. You can configure a terminal for either contact operation counter or total on-time monitoring.

Contact Operation Counter Monitoring

This maintenance function counts the number of off-to-on operations at a local input, test output, or local output terminal and stores the count internally in nonvolatile memory.

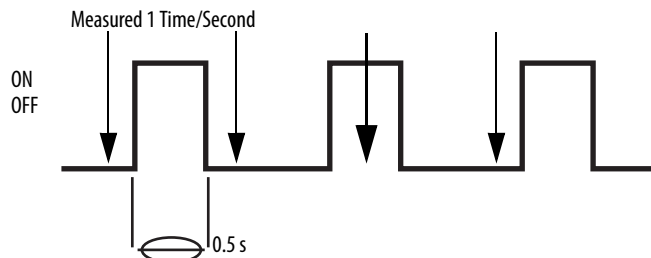
Total On-time Monitoring

This maintenance function times how long a local input, test output, or local output is on and stores that total on-time internally in nonvolatile memory. The monitor function checks whether the connected device is on at intervals of one second. If the device is on for less than one second, the total on-time may not be precise.

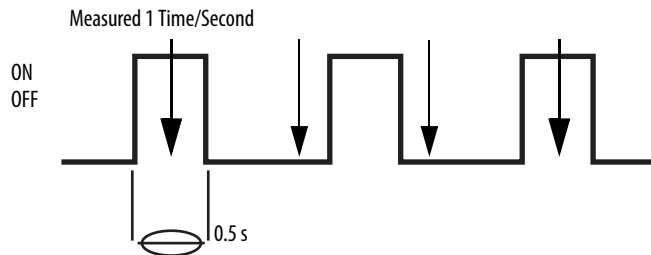
EXAMPLE

Calculating Total On-time with 0.5 Second On Pulses

ATTENTION: In this first example, the bit is actually on for $0.5 \text{ s} \times 3 = 1.5 \text{ s}$. However, the bit is on only once when the status is checked, so the total on-time is measured as 1 s.

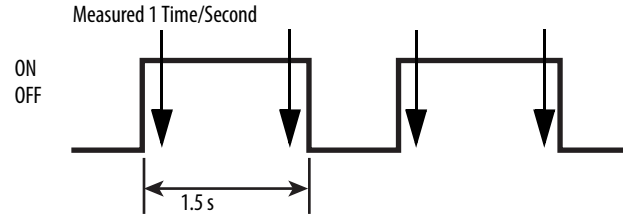


ATTENTION: In this second example, the bit is actually on for $0.5 \text{ s} \times 3 = 1.5 \text{ s}$, but the bit is on twice when the status is checked, so the total on-time is measured as 2 s.



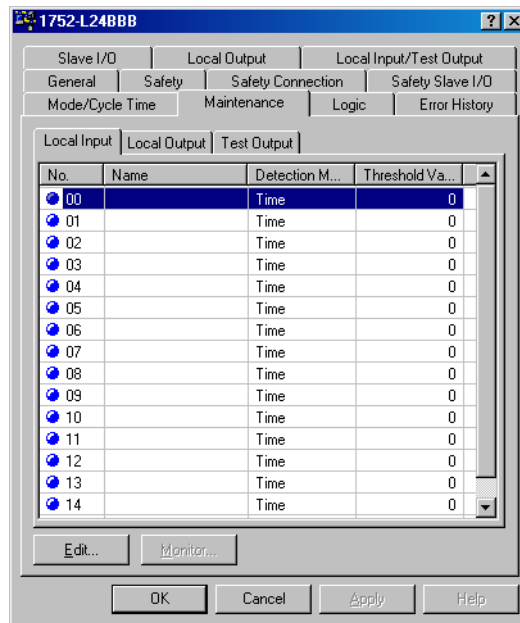
EXAMPLE**ATTENTION: Calculating Total On-time With 1.5 Second On Pulses**

ATTENTION: In this example, the bit is actually on for $1.5\text{ s} \times 2 = 3\text{ s}$, but the bit is on 4 times when status is checked, so the total on-time is measured as 4 s.

**Configure a Maintenance Monitoring Mode**

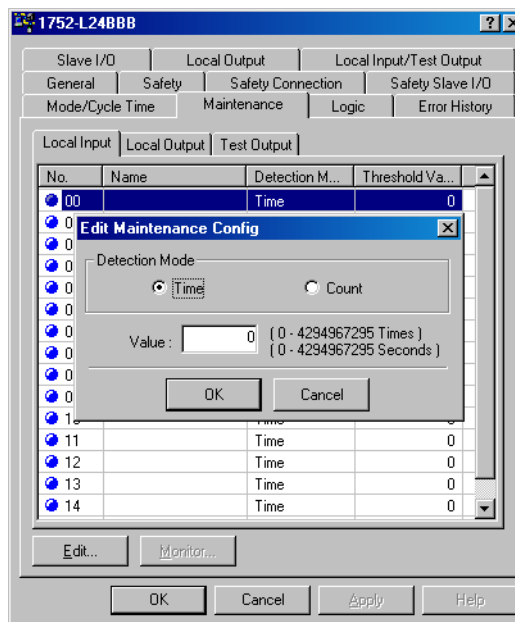
Follow these steps to configure contact operation counter mode for a terminal.

1. In RSNetWorx for DeviceNet software, right-click the controller and choose Properties.
2. Select the Maintenance tab.



3. Select the Local Input, Local Output, or Test Output tab.

4. Select the desired terminal and click Edit.



5. On the Edit Maintenance Config dialog box, choose the Detection mode, either Count or Time.
6. Type an alarm threshold value for the specified Detection mode.

Detection Mode	Valid Range for Values
Time	0...4,294,967,295 seconds
Count	0...4,294,967,295 times

7. Click OK.
8. Click OK.

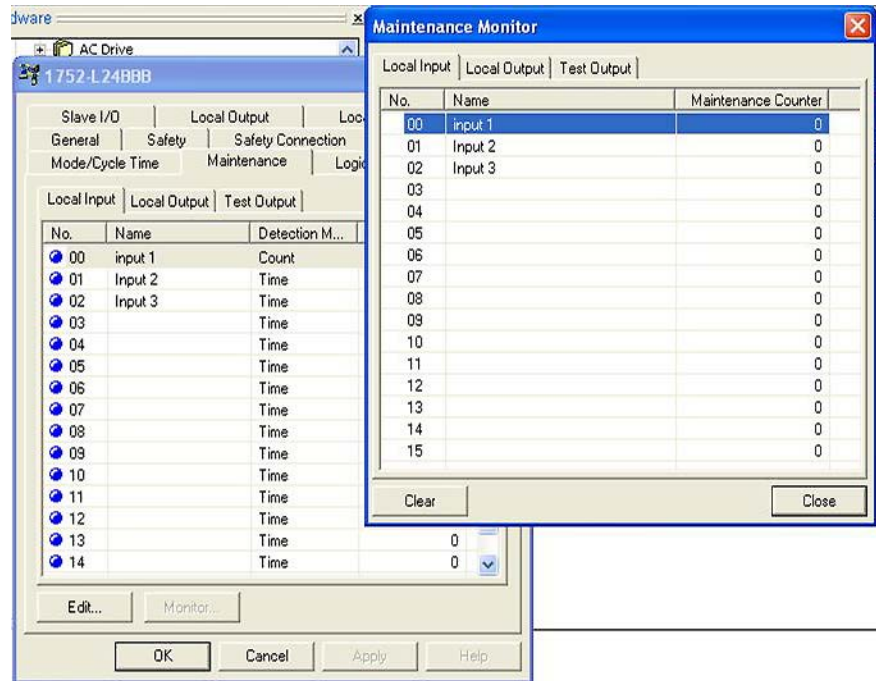
When you are online with the controller, you can monitor the configured terminals by clicking Monitor on the Maintenance tab.

Clear the Maintenance Values

Follow these steps to clear the count or on-time accumulated values while online with the controller.

1. On the Maintenance tab, click Monitor.

2. Click Clear on the Maintenance Monitor dialog box.



Viewing I/O Status Data

When the controller operates as a safety slave or a standard slave target, status information can be added to the first line of the transmit data. The information can be stored in a controller and used to establish a monitoring system.

Table 13 - Controller Status Data

Tag Name	Data Size	Attribute Type
General Status	1 Byte	Non-safety
Local Input Status	Word	Safety
Local Output Status	Byte	Safety
Test Output/Muting Lamp Status	Byte	Non-safety



ATTENTION: Do not use data with a non-safety attribute to configure the safety control system. The necessary measures for safety data are not taken during the generation of non-safety data.

General Status Data

The general status flags are non-safety attributes that indicate system status.

Table 14 - General Status Data Details

Bit	Name	Description
0	Input Power Supply Voltage Status Flag	Indicates the status of the power supply voltage for inputs. OFF: Normal power supply is on. ON: Power-supply voltage error or power supply is off.
1	Output Power Supply Voltage Status Flag	Indicates the status of the power supply voltage for outputs. OFF: Normal power supply is on. ON: Power-supply voltage error or power supply is off.
2	Standard I/O Communication Error Flag	Indicates whether there is any error in standard I/O communication. OFF: No error. ON: An error has been detected in one or more standard connections.
3	Standard I/O Communication Status Flag	Indicates whether standard I/O communication is in progress. Flag is ON if normal communication is in progress for all standard connections.
4	Safety I/O Communication Error Flag	Indicates whether there is any error in safety I/O communication. OFF: No error. ON: An error has been detected in one or more safety connections.
5	Safety I/O Communication Status Flag	Indicates whether safety I/O communication is in progress. Flag is ON if normal communication is in progress for all safety connections.
6	Operating Mode Flag	Indicates the operating mode of the controller. OFF: The controller is not in Run mode. ON: The controller is in Run mode.
7	Controller Status Flag	Indicates the status of the controller. OFF: An error exists. ON: The controller is operating normally.

Local Input Status

When the bit is on, the status of the input is normal. When the bit is off, an error has been detected

Table 15 - Local Safety-Input Terminal Status

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Terminal 7	Terminal 6	Terminal 5	Terminal 4	Terminal 3	Terminal 2	Terminal 1	Terminal 0
1	Terminal 15	Terminal 14	Terminal 13	Terminal 12	Terminal 11	Terminal 10	Terminal 9	Terminal 8

Local Output Status

When the bit is on, the status of the output is normal. When the bit is off, an error has been detected

Table 16 - Local Safety-Output Terminal Status

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Terminal 7	Terminal 6	Terminal 5	Terminal 4	Terminal 3	Terminal 2	Terminal 1	Terminal 0

Test Output or Muting Lamp Status

When the bit is on, the status of the test output is normal. When the bit is off, an error has been detected.

Table 17 - Test Output/Muting Lamp Status

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Terminal 3 disconnection detected status	Reserved			Terminal 3	Terminal 2	Terminal 1	Terminal 0

Controller Connection Status (safety slave function)

Code	Status	Corrective Action
00:0001	Normal communication	The safety I/O connection status is normal.
01:0001	Safety I/O Connection Timeout	The safety I/O connection has timed out. Check the following: <ul style="list-style-type: none"> -Do all nodes have the same baud rate? -Is the cable length correct? -Is the cable disconnected or slack? -Is the terminating resistance only on both ends of the main line? -Is there excessive noise?
01:0106	Output Connection Owner Error	The safety slave established an output safety I/O connection with a safety master that had a different node address last time.
01:0109	Data Size Error	The safety slave I/O size set to the SmartGuard controller safety slave and the size set under the safety master safety connection setting does not match. The safety slave I/O setting may have been changed so delete and then re-configure the connections registered to the safety master.
01:0110	Unconfigured Device	The safety slave has not been configured. Download the device parameters to the safety slave.
01:0111	RPI Error	The RPI set under the safety master safety connection is smaller than the safety slave cycle time.
01:0113	Number of Connections Error	The setting exceeds the maximum number of safety I/O connections supported by the safety slave. Check the relevant safety master safety connection settings.
01:0114	Vendor ID or Product Code Error	The device data for the device in the RSNetWorx for DeviceNet configuration file and the physical device in the system does not match. Use the Safety Device Verification Wizard to check that the device in the system and the device in the configuration file match. If they do match, re-configure the connections to the safety master.

Code	Status	Corrective Action
01:0115	Device type Error	The device data for the device in the RSNetWorx for DeviceNet configuration file and the physical device in the system does not match. Use the Safety Device Verification Wizard to check that the device in the system and the device in the configuration file match. If they do match, re-configure the connections to the safety master.
01:0116	Firmware Revision Error	The device data for the device in the RSNetWorx for DeviceNet configuration file and the physical device in the system does not match. Use the Safety Device Verification Wizard to check that the device in the system and the device in the configuration file match. If they do match, re-configure the connections registered to the safety master.
01:0117	Connection Path Error	Two or more single-cast safety I/O connections or a multi-cast safety I/O connection with a different RPI has been set for a safety slave I/O. To share one safety slave I/O on a safety slave with more than one safety master, make the RPI all the same and set the connection type to multi-cast. SmartGuard controller safety slaves cannot have more than one single-cast safety I/O connection for each safety slave I/O. Set multiple connection paths for the controller's safety slave I/O. If previous solutions do not resolve the problem, delete and then re-configure the connections to the safety master.
01:031E	Number of Connections Error	The setting for the number of safety I/O connections exceeds the upper limit supported by the safety slave. Adjust the safety connection setting for the relevant safety master. In particular, check that no more than 15 safety masters are set for each multi-cast connection, with a maximum total of 60.
01:031F	Connection ID Resource Error	The maximum number of connection IDs for one safety master (12) has been exceeded. Click Advanced on the Safety Connection Properties dialog box. Check the Request target device to allocate message IDs checkbox. Download the device parameters to the safety master.
01:07FF	Non-existent Safety Slave	The safety slave may not have been added to the network correctly. Check that the corresponding safety slave is online. If the safety slave is not online, check the following items: <ul style="list-style-type: none"> -Is the node address for the safety slave correct? -Do all nodes have the same communication rate? -Is the cable length correct? -Is the cable disconnected or slack? -Is the terminating resistance only on both ends of the main line? -Is there excessive noise?
01:080C	Safety Signature Match	The safety signature for the safety slave monitored by the safety master does not match the safety signature of the safety slave itself. Reset the safety slave to default setting then download the device parameters again. If the above remedy does not work, delete then re-configure the connections configured in the safety master.
01:080E	Safety Network Number (SNN) mismatch	The SNN for the safety slave monitored by the safety master does not match the SNN of the safety slave itself. Reset the safety slave to default settings, then download the correct device parameters. If the above remedy does not work, delete then re-configure the connections configured in the safety master.
D0:0001	Idle Mode	The SmartGuard controller safety master is in the Idle mode, so safety I/O connections have not been established. Change the SmartGuard controller's operating mode to Execute mode.

Error Categories

Controller errors can be categorized into nonfatal errors, abort errors, and critical errors.

Table 18 - Controller Error Categories

Error Category	Description
Non-fatal Errors	An error that stops each local I/O or safety I/O connection terminal and places it in the safety state. The controller continues to operate in Run mode.
Abort Errors	The controller drops out of Run mode, goes to the Idle mode, and places all safety I/O into their safety state. Explicit message communication or partial RSNetWorx for DeviceNet software functions are supported to enable you to check the error state.
Critical Error	The controller completely stops functioning when this type of error occurs. See page 185 for download errors. See Reset Errors and Corrective Actions for reset errors. See Mode Change Errors and Corrective Actions for errors that can occur when changing modes.

Error History Table

When an error is detected, a record is made in the error history table in the controller's RAM. If the number of error records exceeds the maximum of 100, the oldest records are deleted sequentially and the most recent error data is stored as a new record.

The error history table stores the controller's status when the error occurred, the time at which the error occurred (total operating time of the controller⁽¹⁾), and the node address where the error occurred.

Error History Memory Area

The description of an error is recorded as an error history entry in the controller's RAM. If the error is critical, it is also saved in nonvolatile memory. The error history recorded in nonvolatile memory is retained even when the controller does not have power or the controller is restarted. The error history in nonvolatile memory is copied to the controller's RAM at the start of a controller power cycle. The error history in RAM is read when reading the error history from RSNetWorx for DeviceNet software. When clearing the error history, however, the error histories in both RAM and nonvolatile memory are cleared.

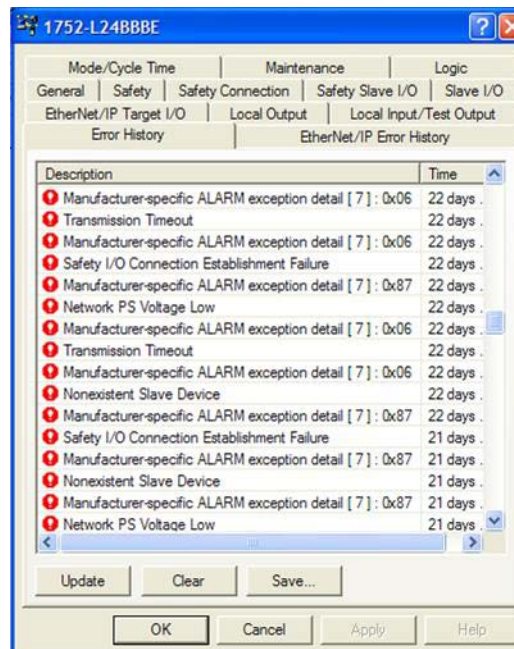
Display the Error History Table for the 1752-L24BBB Controller

Follow these steps to display the error history in real time by using RSNetWorx for DeviceNet software while online with the controller.

1. Right-click the SmartGuard controller and choose Properties.

(1) The total operating time of the controller is recorded as the accumulated time in 6 minute increments while the power supply for V0, G0 is on. The total operating time is cleared by the controller Reset Command.

2. Click the Error History tab.



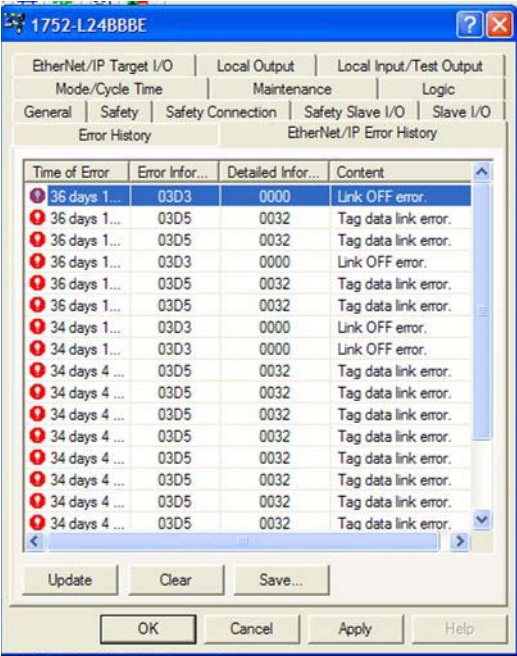
- a. Click Save to save the error history data, which can also be saved in a separate CSV file.
- b. Click Clear to erase the error history saved in the controller.
- c. Click Update to refresh the error history information.

Display the EtherNet/IP Error History Table for the 1752-L24BBBE Controller

Follow these steps to display the error history in real time by using RSNetWorx for DeviceNet software while online with the controller.

1. Right-click the SmartGuard controller and choose Properties.

2. Click the EtherNet/IP Error History tab.



- a. Click Save to save the error history data, which can also be saved in a separate CSV file.
- b. Click Clear to erase the error history saved in the controller.
- c. Click Update to refresh the error history information.

Ethernet Error History Table

Error Code	Error	Detail Code		7-segment Display
		1st Byte ⁽¹⁾	2nd Byte ⁽¹⁾	
0602	CPU Bus Unit Memory	01: Read error	Variable	E9<->n4
		02: Write error		
020F	Communications Controller	00	01	F4<->n4
0211	Duplicate IP Address	02	Lower byte of IP address	F0<->n4
021A	Logic Error in Setting table	00	Variable	UF
03C4	Server Connection	04;BOOTP	01; Specific host does not exist	E3<0>n4
			07: Transmission error	
			08: Reception error	
			0A: Obtaining IP address error	

Error Code	Error	Detail Code		7-segment Display
		1st Byte ⁽¹⁾	2nd Byte ⁽¹⁾	
03D0	Ethernet Basic Setting	01: Ethernet Setting error	01: Checksum error	F2<->n4
			11: Inconsistent setting	
			12: Specified baud rate is not supported	
		02: TCP/IP Basic Setting error	01: Checksum error	
			11: Invalid IP address	
			12: Invalid subnet mask	
			13: Invalid default gateway address	
			14: Invalid primary name server	
			15: Invalid secondary name server	
			16: Invalid domain server	
17: Invalid host name				
03D5	Tag Data Link	00	Lower byte of IP address	L9<->n4
03D3	Link OFF	00	00	E1<->n4

(1) The first byte combined with the second byte appear as a single, 4-hex character in the Detailed Information column under the EtherNet/IP Error History tab. Refer to the dialog box in the [Display the EtherNet/IP Error History Table for the 1752-L24BBBE Controller](#) section for examples.

Error History Messages and Corrective Actions

Use the error history messages to identify and correct errors.

Table 19 - Controller System Failure Error Messages

Message	Description	Corrective Action
System Failure	A system failure occurred.	Replace the controller if a system failure occurs again after cycling power.
Invalid Configuration	The configuration is invalid.	The current configuration differs from the original configuration. Reconfigure after checking.

Table 20 - Programming-related Error Messages

Message	Description	Corrective Action
Function Block Status Error	An incompatible signal input was set as an input condition in the function block's Set Parameters.	Check the inputs entered in the function block or program logic.

Table 21 - DeviceNet Communication Error Messages

Message	Description	Corrective Action
Switch Setting Mismatch	Switch settings do not match.	Check that the node address is the same as the address in the last configuration. If not, change back to the original node address or reconfigure. If the error occurs again, replace the controller.
Duplicate MAC ID	One or more node addresses have been duplicated.	Check the node addresses of the other nodes. Correct the configuration so that each node address is used only once and then cycle the power supply.
Network PS Voltage Low	The network power-supply voltage is low.	Make sure the power supply voltage is set within the specification range. Make sure a cable or wire is not disconnected.
Bus Off	Communication has been cut off by frequent data errors.	Make sure the communication rate of all nodes is the same. Make sure the cable lengths of main or branch lines are not too long. Make sure a cable or wire is not disconnected or loose. Make sure terminating resistance is at both ends of the main line and only at both ends. Make sure that there is not excessive noise in the system.
Transmission Timeout	Transmission has timed out.	
Standard I/O Connection Timeout	The standard I/O connection has timed out.	
Relevant Safety I/O Communication Stopped Because of a Safety I/O Communication Error	The corresponding safety I/O connection was stopped due to a safety I/O connection timeout.	
All Safety I/O Communication Stopped Because of a Safety I/O Communication Error	All safety I/O connections were stopped due to a safety I/O connection timeout.	
Safety I/O Connection Timeout	The safety I/O connection has timed out.	
Nonexistent Slave Device	No slave device in the system.	
Safety I/O Connection Establishment Failure	An error occurred in establishing a safety connection.	Make sure the device is configured and operating normally.
Invalid Slave Device	An unauthorized slave device is on the network (verification error).	Verify the slave device and connect a suitable slave device.
EM Transmission Error (Duplicate MAC ID)	Unable to transmit due to node address duplication.	Check the node addresses of the other nodes. Correct the configuration so that each node address is used only once and then cycle the power supply.
EM Transmission Error (Invalid Header)	Unable to transmit due to invalid header.	Check the node address, the class ID, and the instance ID of the transmission message.
EM Transmission Error (Device Offline)	Unable to transmit because the local device is not on the network.	Make sure the communication rate of all nodes is the same. Make sure the cable lengths of main or branch lines are not too long.
EM Transmission Error (Message ID Error)	Unable to transmit due to a message ID error.	Make sure terminating resistance is at both ends of the main line and only at both ends. Take precautions against excessive noise.
EM Transmission Error (Response Timeout)	Unable to transmit due to response timeout.	Make sure the power supply voltage for the network power source is set within the specification range.

Table 21 - DeviceNet Communication Error Messages

Message	Description	Corrective Action
EM Transmission Error (Destination Device Absence)	Unable to transmit because the destination device is not on the network.	Check the node address of the destination node and the node address of the transmission message. Make sure the power supply voltage for the destination node is set within the specification range. Make sure the communication rate of all nodes is the same. Make sure the cable lengths of the main and branch lines are not too long. Make sure a cable or wire is not disconnected or loose. Make sure terminating resistance is at both ends of the main line and only at both ends. Take precautions against excessive noise.
EM Transmission Error (Destination Buffer Full)	Unable to transmit because the destination buffer was busy.	Check the message receive size at the destination node.
EM Transmission Error (Command Length Error)	Unable to transmit because the command is longer than the maximum length.	Check the response message size from the destination. Also check if the response size expected in the request message is correct.
EM Transmission Error (New Request Received)	Message was deleted due to receiving new request.	None.
Received Error Response (UEM)	Receiving an error response when the user explicit-message function is used.	Check that the specified service or data size in the user explicit message matches the destination object specifications.

Table 22 - EtherNet/IP Controller System Failure Error Messages

Message	Description	Corrective Action
System Failure	A system failure occurred.	Cycle the power supply. If a failure occurs again, replace the controller.
	An EtherNet/IP memory error occurred.	
	An EtherNet/IP communication controller error occurred.	
	The same IP address is set for another device on the network.	Check the IP addresses of the other devices, and set an address that does not duplicate any other.
	A setting table logic error occurred.	Check the configuration. If a failure occurs again, replace the controller.
	A BOOTP server connection error occurred.	Make sure the cable is connected correctly. Make sure the BOOTP server is operating normally.
	An EtherNet/IP basic setting logic error occurred.	Check the configuration. If a failure occurs again, replace the controller.
	An EtherNet/IP standard target communication error occurred.	Make sure the same communication settings are used for each node. Make sure the cables are not disconnected or bent. Make sure the power is supplied to the originator.
A Link Off error occurred.	Make sure the same communication settings are used for each node. Make sure the cables are not disconnected or bent. Make sure the power is supplied to the hub.	

Table 23 - Error Messages Related to the I/O Power Supply

Message	Description	Corrective Action
Input PS Voltage Low	I/O power supply (V1, G1) is not connected.	Make sure the power supply voltage is set within the specification range. Make sure that a cable or wire is not disconnected.
Output PS Voltage Low	I/O power supply (V2, G2) is not connected.	

Table 24 - Safety Input Error Messages

Message	Description	Corrective Action
External Test Signal Failure at Safety Input	A failure has occurred in the external wiring at the safety input.	Make sure the input signal wire is not contacting the power source (positive side).
Discrepancy Error at Safety Input	A discrepancy exists between two inputs configured as Dual Channel.	Make sure the input signal wire does not have an earth fault. Make sure the input signal wire is not disconnected. Make sure there is not a short circuit between the input signal wires. Make sure a failure has not occurred in the connected device. Make sure the configured value of the discrepancy time is valid. To recover from this error state, the latch input error time must have passed and the cause of the error must have been corrected. The target safety inputs must turn off. To change the discrepancy time, you must reconfigure the safety input.
Internal Input Failure at Safety Input	An internal circuit failure occurred at the safety input.	Replace the unit if the system failure occurs again after cycling the power supply.

Table 25 - Test Output Error Messages

Message	Description	Corrective Action
Overload Detected at Test Output	Too much current is being drawn at the test output.	Check whether the output signal wire has an earth fault or is overloaded.
Stuck-at-high Detected at Test Output	A test output is stuck on.	Check whether the power source is contacting the output signal wire. After the latch input-error time has passed, turn off the input when the cause of the error has been removed, and the error will be reset. If there is no fault with the wires, replace the unit.
Under-current Detected Using Muting Lamp	The lower limit error of current was detected at the test output T3.	Check whether the output signal wire is disconnected or if the muting lamp is burned out. If there is no fault with the wires, check the status indicators.

Table 26 - Safety Output Error Messages

Message	Description	Corrective Action
Over Current Detected at Safety Output	Overcurrent was detected at the safety output.	Make sure there is no overcurrent for the output.
Short Circuit Detected at Safety Output	A short-circuit was detected at the safety output.	Make sure the output signal wire does not have an earth fault.
Stuck-at-high Detected at Safety Output	A safety output is stuck-at-high.	Make sure the output signal wire is not contacting the power source (positive side). Make sure there is not a short circuit between the output signal wires.
Cross Connection Detected at Safety Output	A short-circuit was detected between output signal wires at a safety output.	
Dual Channel Violation at Safety Output	Output data error has occurred at a safety output.	Check whether the data of the two outputs in the Dual Channel mode are configured as equivalent channels.

Download Errors and Corrective Actions

The controller may return an error response when downloading configuration data to the controller. Use the messages displayed in RSNetWorx for DeviceNet software to identify the error.

Table 27 - RSNetWorx for DeviceNet Software Download Error Messages and Corrective Actions

Message	Description	Corrective Action
Cannot be executed in the current mode.	A fatal error (abort) has occurred, and the MS indicator flashes red.	Check the switches to see if they are set correctly. Otherwise, execute a reset to clear the configuration data.
The device is locked.	The configuration is locked and the LOCK status indicator is lit.	Unlock the device.
The TUNID is different.	The safety network number (SNN) has not been set since the device reset (the NS status indicator flashes green and red), or the SNN in the device disagrees with the SNN downloaded from RSNetWorx for DeviceNet software.	<ol style="list-style-type: none"> 1. Reset the device to its default settings and download the parameters again. The SNN may be different than other devices. If the controller's alphanumeric display shows d6 and a Safety I/O Connection Establishment Failure message appears in the error history table after the operating mode has been changed, go to the next step. 2. Choose Network>Upload from Network in RSNetWorx for DeviceNet software. Unify the SNN across the network and reset all devices to the default settings. Once they are reset, download the parameters to the devices again.
Privilege violation.	<ol style="list-style-type: none"> 1. The password being used does not have the right to change the configuration. 2. An attempt was made to set Standalone mode through a DeviceNet connection. 	<ol style="list-style-type: none"> 1. Check that the password is correct. 2. Connect to the SmartGuard controller via the USB connector and download the configuration again. With the 1752-L24BBBE controller, you can also download via the EtherNet/IP network.
Cannot be executed in the current device mode.	Data is being downloaded from more than one instance of RSNetWorx for DeviceNet software.	Wait until download from the other instance is complete.
An error was found during parameter check.	An inconsistency exists between configuration parameters.	<p>Correct the parameters settings. Check for the following:</p> <ul style="list-style-type: none"> • A configured time parameter for a function block is shorter than the controller's cycle time. • The requested packet interval (RPI) for a safety connection is shorter than the cycle time. • A safety input is configured as 'Used with test pulse', but the test source is not set. • When safety inputs were configured for Dual Channel mode, one input was configured as a standard input but the other has a different setting. • When safety inputs were configured for Dual Channel mode, one input was set to not used, but the other has a different setting. • When safety outputs were configured for Dual Channel mode, one output was set to not used, but the other has a different setting. • For a safety I/O configuration, a setting was made that caused the maximum number of connection IDs (12) held by the master to be exceeded. Click Advanced on the Safety Connection Properties dialog box. Check the Request target device to allocate message IDs checkbox.
The data used by the logic program is not aligned with other data.	A change in the network configuration caused the data used by program logic to disagree with other data.	Use the Logic Editor to check the I/O locations that changed and reset the data.
Could not access the device.	The controller was reset from another node while a download was being executed and the safety network number (SNN) has not yet been set. The NS status indicator flashes red/green.	Set the SNN and download the data again.

Table 27 - RSNetWorx for DeviceNet Software Download Error Messages and Corrective Actions

Message	Description	Corrective Action
Could not open connection.	A connection to the controller could not be created when downloading to the controller via the DeviceNet or EtherNet/IP network.	<ol style="list-style-type: none"> 1. Make sure that power to the device has been turned on and try downloading the data again. 2. Change the operating mode of the safety master to Idle. 3. It is also possible that noise or another factor has made communication unstable. <ul style="list-style-type: none"> • Make sure the communication rate of all nodes is the same. • Make sure the cable lengths of main and branch lines are not too long. • Make sure a cable or wire is not disconnected or loose. • Make sure terminating resistors are at both ends of the main line. • Take precautions against excessive noise.
Message could not be sent.	A connection to the controller could not be created when downloading to the controller via USB port or EtherNet/IP network.	Make sure that power to the device has been turned on and try downloading the data again.
Connection failed.	An attempt was made to configure a device on the DeviceNet or EtherNet/IP network via the USB port, but the connection could not be made.	<p>Make sure that power to the device has been turned on and try downloading the data again. It is also possible that noise or another factor has made communication unstable.</p> <ul style="list-style-type: none"> • Make sure the communication rate of all nodes is the same. • Make sure the cable lengths of main and branch lines are not too long. • Make sure a cable or wire is not disconnected or loose. • Make sure terminating resistors are at both ends of the main line. • Take precautions against excessive noise.
Program incomplete. Start Logic Editor and check program.	There are open inputs or outputs in a function block used in the logic program.	In the Logic Editor in RSNetWorx for DeviceNet software, connect the open inputs or outputs or change the number of I/O set for the function block to delete the unconnected inputs or outputs.

Reset Errors and Corrective Actions

The controller may return an error response when it is reset. Use the messages displayed in RSNetWorx for DeviceNet software to identify the error.

Table 28 - RSNetWorx for DeviceNet Software Reset Error Messages and Corrective Actions

Message	Description	Corrective Action
Cannot execute in current mode.	The specified reset cannot be executed while the controller is in its current state.	Change the operating mode or configuration lock status, and then execute the reset.
The device has a different TUNID. the device TUNID will be used to reset. Is that OK?	The safety network number (SNN) saved in the device does not agree with the SNN specified from RSNetWorx for DeviceNet software.	Check whether the MAC ID of the device agrees. If the MAC ID agrees and you want to reset with the SNN saved in the device, proceed with the reset.
Access error.	The password used does not provide authority to change configurations.	Make sure the correct password is being used.
The device cannot be accessed or the device type or password is different.	<ol style="list-style-type: none"> 1. The device has just been reset or the power has been cycled and the device is not ready for communication. 2. The device specified for reset may not support that service. 3. The configuration data is locked. The LOCK status indicator is lit. 4. The device is performing safety I/O communication and cannot execute the specified request. 	<ol style="list-style-type: none"> 1. Check that the device is ready for communication and try the reset again. 2. Check to make sure the MAC ID of the device is correct. 3. Remove the lock and execute the specified reset. 4. Change the operating mode of the relevant safety master to Idle and execute the specified reset.
Connection failed.	An attempt was made to reset a device on the DeviceNet or EtherNet/IP network via the USB port, but the connection could not be made.	<p>Make sure that power to the device has been turned on and try resetting again. It is also possible that noise or another factor has made communication unstable.</p> <ul style="list-style-type: none"> • Make sure the communication rate of all nodes is the same. • Make sure the cable lengths of main and branch lines are not too long. • Make sure a cable or wire is not disconnected or loose. • Make sure terminating resistors are at both ends of the main line. • Take precautions against excessive noise.

Mode Change Errors and Corrective Actions

The controller may return an error response when you change modes. Use the messages displayed in RSNetWorx for DeviceNet software to identify the error.

Table 29 - RSNetWorx for DeviceNet Software Mode-Change Error Messages and Corrective Actions

Message	Description	Corrective Action
Cannot be executed in the current mode.	<ol style="list-style-type: none"> 1. The device has not been configured. 2. A fatal error (abort) has occurred. 	<ol style="list-style-type: none"> 1. Download the device parameters. 2. Set the device switches correctly or execute a reset to clear the configuration data and download the device parameters again.
Already set to the specified mode.	The device is already in the specified mode.	
The device has a different TUNID.	The safety network number (SNN) saved in the device does not match the SNN specified from the RSNetWorx for DeviceNet software.	Check to see if the MAC ID of the device matches. If it matches, the network address of the device is not the same as the network address in the RSNetWorx for DeviceNet configuration file. Upload the network to RSNetWorx for DeviceNet software so that the network address will be the same.
Access error.	The password used does not provide authority to change the operating mode.	Make sure the correct password is being used.
The device cannot be accessed, or the device type or password is different.	<ol style="list-style-type: none"> 1. The device has just been reset or the power has been cycled, and the device is not ready for communication. 2. The device for which the change mode request was made may not support that service. 	<ol style="list-style-type: none"> 1. Check that the device is ready for communication and try to change the mode again. 2. Check to make sure the MAC ID of the device is correct.
Connection failed.	An attempt was made to change the operating mode of a device on the DeviceNet or EtherNet/IP network via the USB port, but the connection could not be made.	<p>Make sure that power to the device has been turned on and try changing the mode again.</p> <p>It is also possible that noise or another factor has made communication unstable.</p> <ul style="list-style-type: none"> •Make sure the communication rate of all nodes is the same. •Make sure the cable lengths of main and branch lines are not too long. •Make sure a cable or wire is not disconnected or loose. •Make sure terminating resistors are at both ends of the main line. •Take precautions against excessive noise.

Controller Specifications

Introduction

Topic	Page
General Specifications	189
Environmental Specifications	191
Certifications	193

General Specifications

Attribute	1752-L24BBB	1752-L24BBBE
Dimensions (HxWxD), approx.	99.0 ⁽⁴⁾ x 99.4 x 131.4 mm ⁽⁵⁾ (3.90 ⁽⁴⁾ x 3.91 x 5.18 ⁽⁵⁾ in.)	99.0 ⁽⁴⁾ x 113.0 x 131.4 ⁽⁵⁾ mm (3.90 ⁽⁴⁾ x 4.48 x 5.18 ⁽⁵⁾ in.)
Weight, approx.	460 g (1.23 lb)	575 g (1.54 lb)
DeviceNet current load, max	15 mA @ 24V DC	
Supply voltage ⁽¹⁾	20.4...26.4V DC (24V DC, -15...10%)	
Inrush current - unit power supply	4.8 A peak for 600 μs @ V0/G0	
Inrush current - safety input power supply	2.6 A peak for 3 ms @ V1/G1	
DeviceNet voltage range	11...25V DC	
Current consumption (V0 - internal logic circuit)	230 mA @ 24V DC	280 mA @ 24V DC
Overload protection	Shut down of the affected output with cyclic reconnecting	
Isolation voltage	50V, Functional insulation type Tested at 600V AC for 60 s, between all groups	
Wire type	Copper	
Wiring category ⁽²⁾	2 - on power, signal, and communication ports	2 - on power, 1 - on signal, 1 - communication port
Wire size	For power supply and I/O, use 0.2...2.5 mm ² (12...24 AWG) solid wire, or 0.34...1.5 mm ² (16...22 AWG) standard flexible wire. Before connecting, prepare standard wires by attaching ferrules with plastic insulation collars (DIN 46228-4 standard compatible) For Ethernet connections: RJ45 connector according to IEC 60603-7, 2 or 4 pair Category 5e Minimum cable according to TIA 569-B.1 or Category 5 cable according to ISO/IEC 24701	
I/O terminal screw torque	0.56...0.79 N•m (5...7 lb•in)	
North American temperature code	T4A	
Input type	Current sinking	
Voltage, on-state input, min	11V DC	

Attribute	1752-L24BBB	1752-L24BBBE
Voltage, off-state input, max	5V DC	
Current, off-state input, max	1 mA	
Input current	4.5 mA	
Input impedance	2.6 kΩ	
Test output type	Current sourcing	
Pulse test output current ⁽³⁾	0.7 A	
Test output surge current	0.7 A	
Pulse test off-state voltage, max	1.2V	
Pulse test output leakage current, max	0.1 mA	
Muting lamp output current (T3) <ul style="list-style-type: none"> • More than 25 mA • Less than 5 mA 	<ul style="list-style-type: none"> • Normal operation (to avoid fault when used as a muting lamp output) • Fault (a fault indication is generated when used as a muting lamp output) 	
Output type	Current sourcing	
Output current	0.5 A	
Output surge current	0.5 A	
Voltage, off-state output max	1.2V	
Leakage current, off-state output, max	0.1 mA	
Heat dissipation	9.3 W under max load	

Attribute	1752-L24BBB	1752-L24BBBE
Ethernet communication		
CIP connections	Not applicable	2
Auto negotiation	Not applicable	Supported
Data rate	Not applicable	10/100 Mbps
Duplex	Not applicable	Full/half
Allowable unit communication bandwidth	Not applicable	3000 pps ⁽⁶⁾
Explicit message communication	Not applicable	502 bytes ⁽⁷⁾

(1) V0/G0 for internal logic circuit; V1/G1 for external input devices and test outputs; V2/G2 for external output devices.

(2) Use this Conductor Category information for planning conductor routing. Refer to Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1.

(3) T0...T3 total current at the same time: 1.4 A.

(4) Height includes terminal connectors.

(5) Depth includes DeviceNet connector.

(6) PPS is packets per second. It indicates the number of send or receive packets that can be processed per second.

(7) The maximum message length for class 3 connection and UCMM connection.

Environmental Specifications

Attribute	1752-L24BBB	1752-L24BBBE
Temperature, storage	IEC 60068-2-1 (Test Ab, Unpackaged Nonoperating Cold), IEC 60068-2-2 (Test Bb, Unpackaged Nonoperating Dry Heat), IEC 60068-2-14 (Test Na, Unpackaged Nonoperating Thermal Shock): -40...70 °C (-40...158 °F)	
Temperature, operating	IEC 60068-2-1 (Test Ad, Operating Cold), IEC 60068-2-2 (Test Bd, Operating Dry Heat), IEC 60068-2-14 (Test Nb, Operating Thermal Shock): -10...55 °C (14...131 °F)	
Relative humidity	IEC 60068-2-30 (Test Db, Unpackaged Nonoperating Damp Heat): 10...95% noncondensing	
Vibration	IEC 60068-2-6 (Test Fc, Operating): 0.35 mm @ 10...57 Hz 5 g @ 57...150 Hz	IEC 60068-2-6 (Test Fc, Operating): 5 g @ 10...500 Hz
Shock, operating	IEC 60068-2-27 (Test Ea, Unpackaged Shock): 15 g	
Shock, nonoperating	IEC 60068-2-27 (Test Ea, Unpackaged Shock): 30 g	
Enclosure type rating	Meets IP20	
Emissions	CISPR 11: Group 1, Class A	
ESD immunity	IEC 61000-4-2: • 4 kV contact discharges • 8 kV air discharges	IEC 61000-4-2: • 6 kV contact discharges • 8 kV air discharges

Attribute	1752-L24BBB	1752-L24BBBE
Radiated RF immunity	IEC 61000-4-3: <ul style="list-style-type: none"> • 10 V/m with 1 kHz sine-wave 80% AM from 80...1000 MHz • 10 V/m with 1 kHz sine-wave 80% AM from 1.4...2.0 GHz • 10 V/m with 200 Hz 50% Pulse 100% AM at 900 MHz • 10 V/m with 200 Hz 50% Pulse 100% AM at 1200 MHz • 3 V/m with 1 kHz sine-wave 80% AM from 2000...2700 MHz 	IEC 61000-4-3: <ul style="list-style-type: none"> • 10 V/m with 1 kHz sine-wave 80% AM from 80...1000 MHz • 10 V/m with 1 kHz sine-wave 80% AM from 1.4...2.0 GHz • 20 V/m with 200 Hz 50% Pulse 100% AM at 800, 900, 1200 MHz • 3 V/m with 1 kHz sine-wave 80% AM from 2000...2700 MHz
EFT/B immunity	IEC 61000-4-4: <ul style="list-style-type: none"> • ± 2 kV @ 5 kHz on power ports • ± 2 kV @ 5 kHz on signal ports • ± 2 kV @ 5 kHz on communication ports 	IEC 61000-4-4: <ul style="list-style-type: none"> • ± 2 kV @ 5 kHz on power ports • ± 1 kV @ 5 kHz on signal ports • ± 1 kV @ 5 kHz on communication ports
Surge transient immunity	IEC 61000-4-5: <ul style="list-style-type: none"> • ± 1 kV line-line (DM) and ± 2 kV line-earth (CM) on power ports • ± 1 kV line-line (DM) and ± 2 kV line-earth (CM) on signal ports • ± 1 kV line-earth (CM) on communication ports 	IEC 61000-4-5: <ul style="list-style-type: none"> • ± 500V line-line (DM) and ± 1 kV line-earth (CM) on power ports • ± 1 kV line-earth (CM) on signal ports • ± 1 kV line-earth (CM) on communication ports
Conducted RF immunity	IEC 61000-4-6: <ul style="list-style-type: none"> • 10V rms with 1 kHz sine-wave 80% AM from 150 kHz...80 MHz 	

Certifications

Certification ⁽¹⁾ (when product is marked)	Value
c-UL-us	UL Listed for Class I, Division 2 Group A,B,C,D Hazardous Locations, certified for US and Canada. See UL File E194810
CE	European Union 2004/108/EEC EMC Directive, compliant with: <ul style="list-style-type: none"> • EN 61000-6-4; Industrial Emissions • EN 61131-2; Programmable Controllers (Clause 8, Zone A & B) • EN 61326-1; Meas./Control/Lab., Industrial Requirements • EN 61000-6-2; Industrial Immunity
C-Tick	Australian Radiocommunications Act, compliant with: AS/NZS CISPR 11; Industrial Emissions
TÜV	TÜV Certified for Functional Safety Functional Safety: SIL 1 to 3, according to IEC 61508; Performance Level PL(e) according to ISO 13849-1, Category 1 to 4, according to EN954-1; NFPA79
UL	UL Certified for Functional Safety. See UL File E256621
ODVA	ODVA conformance tested to DeviceNet and Ethernet/IP specifications

(1) See the Product Certification link at <http://ab.com> for Declarations of Conformity, Certificates, and other certifications details.

Notes:

Status Indicators

Introduction

Topic	Page
Module Status Indicators	195
Identifying Errors Using Module Status Indicators and Alphanumeric Display	199
Identifying EtherNet/IP Errors Using Status Indicators and Alphanumeric Display	202

Module Status Indicators

Use these tables to interpret the color of the status indicators and take recommended actions where applicable.



ATTENTION: Status indicators are not reliable indicators for safety functions. They should be used only for general diagnostics during commissioning and troubleshooting. Do not use status indicators as operational indicators.

If the Module Status (MS) indicator is	It means	Take this action
Off	No power.	Refer to the corrective action following this table.
Green, on	The controller is operating in Run mode and under normal conditions.	No action required.
Green, flashing	The controller is idle.	
Red, flashing	A recoverable fault exists.	Refer to the corrective action following this table.
Red, on	An unrecoverable fault exists.	
Red/green flashing	Self-test in progress. Or, the controller's configuration is being downloaded or is incomplete or incorrect. For example, the network ID (UNID) is not set.	

If your Module Status indicator is off, follow these steps.

1. Cycle the power supply.
2. Take corrective actions for noise.
3. Contact Rockwell Automation.

If you Module Status indicator is flashing red, follow these steps.

1. Configure the switches properly.
2. Reset the configuration data.

If your Module Status indicator is solid red (on), follow these steps.

1. Cycle the power supply.
2. Check external wiring.
3. Take corrective actions for noise.
4. Contact Rockwell Automation.

If your Module Status indicator is flashing red and green, follow these steps.

1. Configure the switches properly.
2. Set the safety network number.
3. Reconfigure the device.

If the DeviceNet Network Status (NS D) indicator is	It means	Take this action
Off	The controller is not online or may not have power from the DeviceNet network.	Refer to the corrective action following this table.
Green, on	The controller is online; connections are established.	No action required.
Green, flashing	The controller is online; no connections are established.	
Red, on	Communication failure due to duplicate MAC ID (error code F0) or Bus OFF (error code F1).	Refer to the corrective action following this table.
Red, flashing	Communication timeout.	
Red/green flashing	The Safety Network Number (SNN) is being set.	No action required.

If your Network Status indicator is off, follow these steps.

1. Cycle the power supply.
2. Check external wiring.
3. Take corrective actions for noise.
4. Contact Rockwell Automation.

If your Network Status indicator is on or flashing red, follow these steps.

1. View the Alphanumeric display for the node address of the error and error code.
2. Check that node addresses have not been duplicated.
3. Make sure the communication rate is the same for all nodes.
4. Check that cables are not loose, disconnected or too long.
5. Verify that terminating resistors have been installed only at both ends of the main line.
6. Take corrective action for noise.
7. Make sure target devices are configured, verified, and in normal operating state.

If the Lock Configuration (Lock) indicator is	It means	Take this action
Yellow, on	A locked valid configuration exists.	No action required.
Yellow, flashing	An unlocked valid configuration exists.	Lock the configuration before operating the safety system.
Off	The configuration is invalid.	Reconfigure the controller.

If the USB Communication (Comm U) indicator is	It means	Take this action
Yellow, flashing	The controller is communicating.	No action required.
Off	The controller is not communicating.	

If the I/O status indicator is	It means	Take this action
Red, on	A failure has been detected in the input or output circuit or a discrepancy error has occurred in the I/O set for Dual-channel mode.	Refer to the corrective action following this table.
Red, flashing	A failure has been detected in the associated I/O circuit's dual channel configuration.	
Off	The input or output signal is off.	
Yellow, on	The input or output signal is on.	No action required.

If your I/O Status indicator is on or flashing red, follow these steps.

1. Check that the signal wire:
 - is not making contact with the power source (positive side).
 - does not have an earth fault.
 - is not disconnected.
2. Make sure there is not a short-circuit between signal wires.
3. Check that there is no overcurrent for the output.
4. Make sure there is no failure in the connected devices.
5. Verify that the Discrepancy Time settings are valid.

If your I/O Status indicator is off, follow these steps.

1. Check that the power supply voltage is set within the specified range.
2. Make sure a cable or wire is not disconnected.

If the EtherNet/IP Status (NS E) indicator is	It means	Take this action
Off	The controller does not have an IP address or is not turned on.	Refer to the corrective action following this table.
Green, flashing	The controller has no established connections but has obtained an IP address.	

If the EtherNet/IP Status (NS E) indicator is	It means	Take this action
Green, on	The controller has at least one established connection (even to the message router).	No action required.
Red, flashing	One or more of the connections in which this device is the target has timed out. This shall be left only if all timed out connections are reestablished or if the device is reset.	Refer to the corrective action following this table.
Red, on	The controller has detected that its IP address is already in use.	Reset the IP address.

If your EtherNet/IP Status indicator is off, follow these steps.

1. Apply power to the controller.
2. Set the IP address.

If your EtherNet/IP Status indicator is flashing green, follow these steps.

1. Checking the wiring to the controller.
2. Configure the originator to connect to the target.

If your EtherNet/IP Status indicator is flashing red, follow these steps.

1. Check external wiring.
2. Check the endpoints.
3. Check the switches.

If the Communication (COMM E) indicator is	It means	Take this action
Green, on	The controller is communicating on the Ethernet network.	No action required.
Off	The controller is not communicating on the Ethernet network.	

If the Network Speed (100) indicator is	It means	Take this action
Yellow, on	The communication rate is 100 Mbps.	No action required.
Off ⁽¹⁾	The communication rate is 10 Mbps.	Check that the Network Speed (10) indicator is on.

(1) If this indicator is Off along with the Network Speed (10) indicator, check your Ethernet connection.

If the Network Speed (10) indicator is	It means	Take this action
Yellow, on	The communication rate is 10 Mbps.	No action required.
Off ⁽¹⁾	The communication rate is 100 Mbps.	Check that the Network Speed (100) indicator is on.

(1) If this indicator is Off along with the Network Speed (10) indicator, check your Ethernet connection.

Identifying Errors Using Module Status Indicators and Alphanumeric Display

Use these tables to interpret the color and status combinations of the status and alphanumeric display indicators and take corrective action where applicable.

Table 30 - Critical Errors

MS	Indicators		Error Log	Cause	Corrective Action
	NS	Alphanumeric Display Code			
Off	Off	Off	None	Critical hardware fault. Noise level higher than expected.	1. Cycle the power supply. 2. Check external wiring. 3. Take corrective actions for noise. 4. Contact Rockwell Automation.
Red, on	Off	Left: H Right: ---	System Failure	Critical hardware fault. Noise level higher than expected. Output terminal shorted to 24V dc before operation.	
Red, on	Off	P6	System Failure	Output terminal shorted to 24V dc before operation.	1. Cycle the power supply. 2. Check external wiring.

Table 31 - Abort Error

MS	Indicators		Error Log	Cause	Corrective Action
	NS	Alphanumeric Display ⁽¹⁾ Code			
Red, flashing	Green, on or flashing	E8	Switch setting mismatch	The node address and baud rate were changed after the normal completion of configuration download.	1. Set switches properly. 2. Reconfigure the device.

(1) Display alternates between error code and node address of the error.

Table 32 - Nonfatal Errors

MS	Indicators		Error Log	Cause	Corrective Action
	Alphanumeric Display ⁽¹⁾ Code	I/O			
Red, on	F0	---	Duplicate MAC ID	The same node address is set for more than one node.	Check that node addresses have not been duplicated and reconfigure the device if necessary.
Red, on	F1	---	Bus Off	Communication is cut off because of frequent data errors.	1. Make sure the communication rate is the same for all nodes. 2. Check that cables are not loose, disconnected, or too long. 3. Verify that terminating resistors have been installed only at both ends of the main line. 4. Take corrective action for noise. 5. Cycle the power supply.
Red, flashing	L9	---	Standard I/O Connection Timeout	Standard I/O connection timeout.	
Red, flashing	dA	---	Safety I/O Connection Timeout	Safety I/O connection timeout.	
Red, flashing	d5	---	Nonexistent Slave Device	No slave detected.	
Red, flashing	d6	---	Safety I/O Connection Establishment Failure	Safety I/O connection could not be established.	Make sure the slave device is configured and in a normal operational state.
Red, flashing	d6	---	Invalid Slave Device	Invalid slave device due to verification error.	1. Verify the slave device's configuration. 2. Connect a compatible slave device.
Off	E0	---	Network PS Voltage Low	Network power supply voltage is low.	1. Make sure the power supply voltage is set within the specified range. 2. Check that cables or wires are not loose or disconnected.

Table 32 - Nonfatal Errors

MS	Indicators		Error Log	Cause	Corrective Action
	Alphanumeric Display ⁽¹⁾ Code	I/O			
---	E2	---	Transmission Timeout	DeviceNet Transmission timeout or nothing connected to the DeviceNet network.	<ol style="list-style-type: none"> 1. Make sure the communication rate is the same for all nodes. 2. Check that cables are not loose, disconnected, or too long. 3. Verify that terminating resistors have been installed only at both ends of the main line. 4. Take corrective action for noise.
Red, flashing	A0	---	Relevant Safety I/O communication stopped because of a Safety I/O communication error	A safety I/O connection timed out, interrupting the relevant safety I/O connection.	
Red, flashing	A1	---	All Safety I/O communication stopped because of a Safety I/O communication error	A safety I/O connection timed out, interrupting all I/O connections.	
---	P4	All off	Input PS Voltage Low	I/O power for inputs (V1, G1) is not connected, although a safety input terminal or test output terminal is used.	<ol style="list-style-type: none"> 1. Make sure the power supply voltage is set within the specified range. 2. Check that cables or wires are not loose or disconnected.
---	P5	All off	Output PS Voltage Low	I/O power for outputs (V2, G2) is not connected although a safety output terminal is used.	
---	P1	Target terminal red, on Paired terminal red, flashing	External Test Signal Failure at Safety Input	An external wiring error has occurred at a safety input.	<ol style="list-style-type: none"> 1. Check that the signal wire: <ul style="list-style-type: none"> • is not contacting the power source (positive side). • does not have an earth fault. • is not disconnected. 2. Make sure there is not a short-circuit between signal wires. 3. Make sure there is no failure in the connected devices. 4. Verify that the discrepancy time settings are valid. <p>To recover from this error state, the latch input error time must have passed and the cause of the error must have been corrected. The target safety inputs must turn off.</p> <p>To change the discrepancy time, you must reconfigure the safety input.</p>
---	P1	Target terminal red, on	Discrepancy Error at Safety Input	A discrepancy error occurred between two inputs configured for dual channel.	
---	P1	Target terminal red, on Paired terminal red, flashing	Internal Input Failure at Safety Input	An internal circuit failure occurred at the safety input.	
---	P2	N/A	Overload Detected at Test Output	Overloading was detected at the test output, when a test output was configured as a standard signal output.	Check whether the output signal wire has an earth fault or is overloaded.
---	P2	N/A	Stuck-at-high Detected at Test Output	A test output, configured as a standard signal output, was stuck on.	<ol style="list-style-type: none"> 1. Make sure the power supply source (positive side) is not contacting the output signal wire. After the latch input error time has passed and the cause of the error has been corrected, turn off the input. The error will reset. 2. If there is no fault with the wires, replace the unit.
---	P2	N/A	Undercurrent Detected Using Muting Lamp	Disconnection of indicator light was detected at the test output, when the T3 terminal is configured as the muting-lamp signal output.	<ol style="list-style-type: none"> 1. Make sure the output signal wire is not disconnected. 2. Check the indicator light to make sure it is not burned out.

Table 32 - Nonfatal Errors

MS	Indicators		Error Log	Cause	Corrective Action
	Alphanumeric Display ⁽¹⁾ Code	I/O			
---	P3	Target terminal red, on Paired terminal red, flashing	Overcurrent Detected at Safety Output	An overcurrent was detected at the safety output.	<ol style="list-style-type: none"> 1. Make sure there is no overcurrent for the output. 2. Check that the signal wire: <ul style="list-style-type: none"> • is not contacting the power source (positive side). • does not have an earth fault. 3. Make sure there is not a short-circuit between signal wires. <p>To recover from this error state, the latch input error time must have passed and the cause of the error must have been corrected. The output signal from the user application for the target safety output must turn off.</p>
---	P3	Target terminal red, on Paired terminal red, flashing	Short-circuit Detected at Safety Output	A short-circuit was detected at the safety output.	
---	P3	Target terminal red, on Paired terminal red, flashing	Stuck-at-high Detected at Safety Output	A safety output was stuck on.	
---	P3	Target terminal red, on Paired terminal red, flashing	Cross Connection Detected at Safety Output	A cross connection was detected at the safety output.	
---	P3	Target terminal red, on	Dual Channel Violation at Safety Output	An output data error has occurred at the safety output. For example, an output is configured for Dual Channel, but only one of the output bits is being turned on by the program.	

(1) Display alternates between error code and node address of the error.

Identifying EtherNet/IP Errors Using Status Indicators and Alphanumeric Display

Use these tables to interpret the color and status combinations of the status and alphanumeric display indicators and take corrective action where applicable.

For the 1752-L24BBBE controller, when the IP address display switch for 1 second or longer, the display shows the EtherNet/IP address that is set. The error code 'n4' is displayed if an error occurs in EtherNet/IP configuration.

Table 33 - EtherNet/IP Controller Errors

MS	Indicators		Error Log	Cause	Corrective Action
	NS	Alphanumeric Display ⁽¹⁾ Code			
Off	Red, on	UF	System Failure	An EtherNet/IP adaptor hardware fault occurred.	Cycle the power supply. If a failure occurs again, replace the controller.
Red, on	---	F0		An IP address duplication fault occurred.	Check the IP address of the other devices, and set an address that does not duplicate any other.
Off	---	E3		A BOOTP server connection fault occurred.	<ol style="list-style-type: none"> 1. Make sure the cable is connected correctly. 2. Make sure the BOOTP server is operating normally.
Off	---	F2		A Basic setting logic processing fault occurred.	Check the configuration. If a failure occurs again, replace the controller.
Off	Red, flashing	E9		An EtherNet/IP memory fault occurred.	Cycle the power supply. If a failure occurs again, replace the controller.
Off	Red, flashing	F4		An EtherNet/IP communication controller fault occurred.	
Red, flashing	---	L9		An EtherNet/IP standard target communication error occurred.	<ol style="list-style-type: none"> 1. Make sure the same communication settings are used for each node 2. Make sure the cables are not disconnected or bent. 3. Make sure power is supplied to the originator.
Off	---	E1		A Link OFF error occurred.	<ol style="list-style-type: none"> 1. Make sure the same communication settings are used for each node 2. Make sure the cables are not disconnected or bent. 3. Make sure power is supplied to the hub.

(1) Display alternates between error code and n4.

Logic Functions Command Reference

Introduction

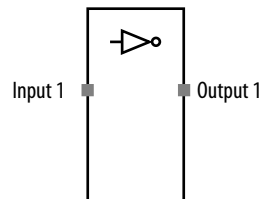
This appendix describes the logic functions used for programming.

Topic	Page
NOT Instruction	203
AND Instruction	204
OR Instruction	206
Exclusive OR Instruction	209
Exclusive NOR Instruction	210
Routing Instruction	211
Reset Set Flip-flop (RS-FF) Instruction	211
Multi-connector Instruction	212
Comparator Instruction	213

NOT Instruction

The outcome is the inverse of the input.

NOT Instruction Diagram



NOT Instruction Truth Table

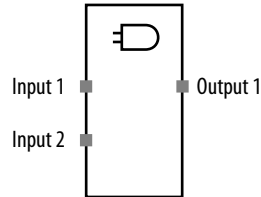
In the truth table, 0 is off and 1 is on.

Input 1	Output 1
0	1
1	0

AND Instruction

The output is the logical AND of up to eight input conditions. The number of inputs can be set by using the In/Out Setting tab in the Function Block Properties dialog box. The default setting is two inputs.

AND Instruction Diagram



AND Instruction Truth Tables

In the truth table, 0 is off and 1 is on. Lowercase x is don't care.

Table 34 - Truth Table for One-input AND Evaluation

Input 1	Output 1
0	0
1	1

Table 35 - Truth Table for Two-input AND Evaluation

Input 1	Input 2	Output 1
0	x	0
x	0	0
1	1	1

Table 36 - Truth Table for Three-input AND Evaluation

Input 1	Input 2	Input 3	Output 1
0	x	x	0
x	0	x	0
x	x	0	0
1	1	1	1

Table 37 - Truth Table for Four-input AND Evaluation

Input 1	Input 2	Input 3	Input 4	Output 1
0	x	x	x	0
x	0	x	x	0
x	x	0	x	0
x	x	x	0	0
1	1	1	1	1

Table 38 - Truth Table for Five-input AND Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Output 1
0	x	x	x	x	0
x	0	x	x	x	0
x	x	0	x	x	0
x	x	x	0	x	0
x	x	x	x	0	0
1	1	1	1	1	1

Table 39 - Truth Table for Six-input AND Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Output 1
0	x	x	x	x	x	0
x	0	x	x	x	x	0
x	x	0	x	x	x	0
x	x	x	0	x	x	0
x	x	x	x	0	x	0
x	x	x	x	x	0	0
1	1	1	1	1	1	1

Table 40 - Truth Table for Seven-input AND Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Output 1
0	x	x	x	x	x	x	0
x	0	x	x	x	x	x	0
x	x	0	x	x	x	x	0
x	x	x	0	x	x	x	0
x	x	x	x	0	x	x	0
x	x	x	x	x	0	x	0
x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1

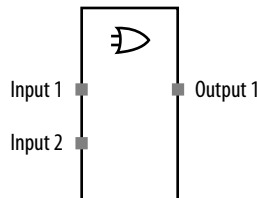
Table 41 - Truth Table for Eight-input AND Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Input 8	Output 1
0	x	x	x	x	x	x	x	0
x	0	x	x	x	x	x	x	0
x	x	0	x	x	x	x	x	0
x	x	x	0	x	x	x	x	0
x	x	x	x	0	x	x	x	0
x	x	x	x	x	0	x	x	0
x	x	x	x	x	x	0	x	0
x	x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1	1

OR Instruction

The Output is the logical OR of up to eight input conditions. The number of inputs can be set by using the In/Out Setting tab in the Function Block Properties dialog box. The default setting is two inputs.

OR Instruction Diagram



OR Instruction Truth Tables

In the truth table, 0 is off and 1 is on. Lowercase x is don't care.

Table 42 - Truth Table for One-input OR Evaluation

Input 1	Output 1
0	0
1	1

Table 43 - Truth Table for Two-input OR Evaluation

Input 1	Input 2	Output 1
0	0	0
1	x	1
x	1	1

Table 44 - Truth Table for Three-input OR Evaluation

Input 1	Input 2	Input 3	Output 1
0	0	0	0
1	x	x	1
x	1	x	1
x	x	1	1

Table 45 - Truth Table for Four-input OR Evaluation

Input 1	Input 2	Input 3	Input 4	Output 1
0	0	0	0	0
1	x	x	x	1
x	1	x	x	1
x	x	1	x	1
x	x	x	1	1

Table 46 - Truth Table for Five-input OR Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Output 1
0	0	0	0	0	0
1	x	x	x	x	1
x	1	x	x	x	1
x	x	1	x	x	1
x	x	x	1	x	1
x	x	x	x	1	1

Table 47 - Truth Table for Six-input OR Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Output 1
0	0	0	0	0	0	0
1	x	x	x	x	x	1
x	1	x	x	x	x	1
x	x	1	x	x	x	1
x	x	x	1	x	x	1
x	x	x	x	1	x	1
x	x	x	x	x	1	1

Table 48 - Truth Table for Seven-input OR Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Output 1
0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	1
x	1	x	x	x	x	x	1
x	x	1	x	x	x	x	1
x	x	x	1	x	x	x	1
x	x	x	x	1	x	x	1
x	x	x	x	x	1	x	1
x	x	x	x	x	x	1	1

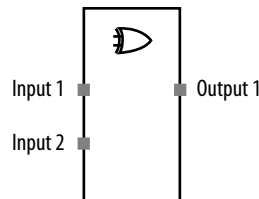
Table 49 - Truth Table for Eight-input OR Evaluation

Input 1	Input 2	Input 3	Input 4	Input 5	Input 6	Input 7	Input 8	Output 1
0	0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	x	1
x	1	x	x	x	x	x	x	1
x	x	1	x	x	x	x	x	1
x	x	x	1	x	x	x	x	1
x	x	x	x	1	x	x	x	1
x	x	x	x	x	1	x	x	x
x	x	x	x	x	x	1	x	1
x	x	x	x	x	x	x	1	1

Exclusive OR Instruction

The output is the exclusive OR of the input conditions.

Exclusive OR Diagram



Exclusive OR Truth Table

In the truth table, 0 is off and 1 is on.

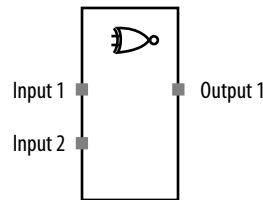
Table C.1 Truth Table for Exclusive OR Evaluation

Input 1	Input 2	Output 1
0	0	0
0	1	1
1	0	1
1	1	0

Exclusive NOR Instruction

The output is an exclusive NOR of the input conditions.

Exclusive NOR Instruction Diagram



Exclusive NOR Instruction Truth Tables

In the truth table, 0 is off and 1 is on.

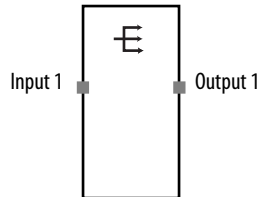
Table C.2 Truth Table for Exclusive NOR Evaluation

Input 1	Input 2	Output 1
0	0	1
0	1	0
1	0	0
1	1	1

Routing Instruction

The Routing instruction routes one input signal to a maximum of eight output signals. It is used to output a signal to more than one physical address, such as an output tag. The number of outputs can be set by using the I/O Setting tab in the Function Block Properties dialog box. The default setting is one.

Routing Instruction Diagram



Routing Instruction Truth Table

In the truth table, 0 is off and 1 is on.

Table C.3 Truth Table for Routing Evaluation

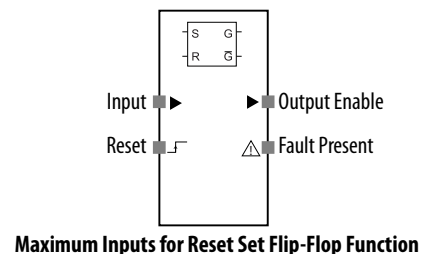
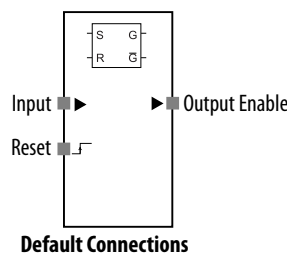
Input 1	Output 1	Output 2	Output 3	Output 4	Output 5	Output 6	Output 7	Output 8
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1

Reset Set Flip-flop (RS-FF) Instruction

When the input signal is on, the Output Enable signal is turned on. The Output Enable signal stays on even if the input signal turns off. When the Reset signal is on, the Output Enable signal turns off.

A Fault Present output can also be used in programming. To enable this optional output, check the Use Fault Present checkbox on the I/O Settings tab of the Function Block Properties dialog box in RSNetWorx for DeviceNet software.

Reset Set Flip-flop Instruction Diagram



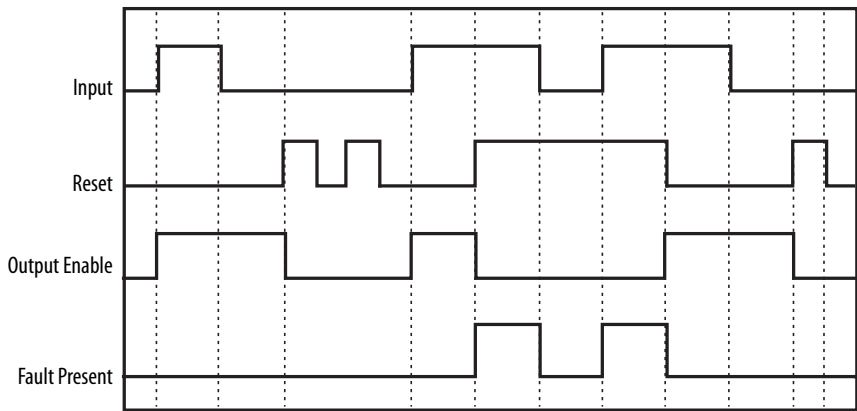
Reset Set Flip-flop Error Handling

Use this table to diagnose and reset a discrepancy error condition in the RS Flip-flop instruction.

Table 4 - Error Detection and Reset for RS Flip-flop Instruction

Error Condition	Status When an Error Occurs		To Reset the Error Condition
	Output Enable	Fault Present	
Input and Reset are active simultaneously	OFF (Safety State)	ON	Make one of the signals inactive.

RS Flip-flop Instruction Timing Chart

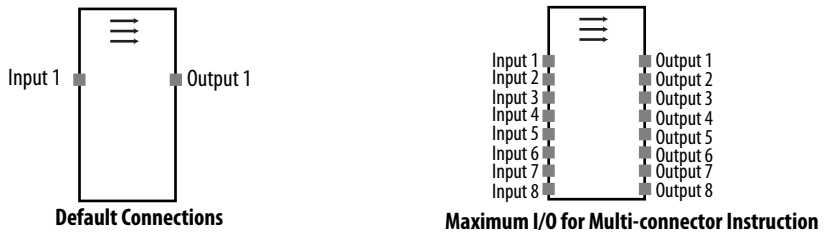


Multi-connector Instruction

The Multi-connector instruction converts input signals for up to eight inputs into output signals for up to eight outputs. The input signals and output signals are associated one-to-one for signals one to eight. The status of other input signals has no effect.

The number of inputs and outputs can be increased to eight on the I/O Settings tab of the Function Block Properties dialog box in RSNetWorx for DeviceNet software. The default setting is one.

Multi-connector Instruction Diagram



Multi-connector Instruction Truth Table

In the truth table, 0 is off and 1 is on.

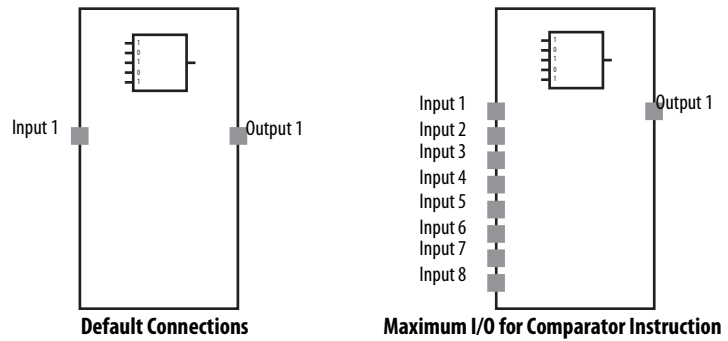
Table 5 - Truth Table for Multi-connector Instruction

Inputs								Outputs							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
0	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x
1	x	x	x	x	x	x	x	1	x	x	x	x	x	x	x
x	0	x	x	x	x	x	x	x	0	x	x	x	x	x	x
x	1	x	x	x	x	x	x	x	1	x	x	x	x	x	x
x	x	0	x	x	x	x	x	x	x	0	x	x	x	x	x
x	x	1	x	x	x	x	x	x	x	1	x	x	x	x	x
x	x	x	0	x	x	x	x	x	x	x	0	x	x	x	x
x	x	x	1	x	x	x	x	x	x	x	1	x	x	x	x
x	x	x	x	0	x	x	x	x	x	x	x	0	x	x	x
x	x	x	x	1	x	x	x	x	x	x	x	1	x	x	x
x	x	x	x	x	0	x	x	x	x	x	x	x	0	x	x
x	x	x	x	x	1	x	x	x	x	x	x	x	1	x	x
x	x	x	x	x	x	0	x	x	x	x	x	x	x	0	x
x	x	x	x	x	x	1	x	x	x	x	x	x	x	1	x
x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	0
x	x	x	x	x	x	x	1	x	x	x	x	x	x	x	1

Comparator Instruction

The comparator instruction compares the specified input signals of up to eight inputs with the configured comparison pattern and turns on the Output 1 signal when all of the input signals match the comparison pattern. The Output 1 signal turns off when the input signals no longer match the comparison value.

Comparator Instruction Diagram



Comparator Instruction Parameters

Set these parameters for the Comparator instruction.

Table 6 - Comparator Function Block Parameters

Parameter	Valid Range	Default Setting
Comparison value	00000000...11111111 (bit 7...0)	00000001

You can set the comparison pattern and increase the number of inputs from one to eight on the In/Out Setting tab of the Function Block Properties dialog box in RSNetWorx for DeviceNet software. The default is one input. You set the comparison pattern by using a combination of 0 (input off), 1 (input on), and X (input on or off).

Comparator Instruction Truth Table

In the truth table, 0 is off and 1 is on. CV is the comparison value. An X indicates that the status of the input (match or don't match) is not applicable.

Table 7 - Truth Table for Comparator Instruction

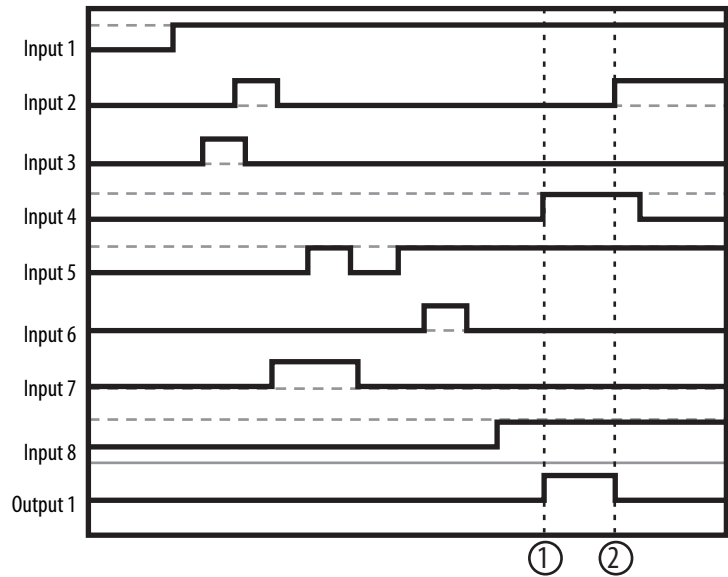
Input 8	Input 7	Input 6	Input 5	Input 4	Input 3	Input 2	Input 1	Output 1
≠CV for bit 7	X	X	X	X	X	X	X	0
X	≠CV for bit 6	X	X	X	X	X	X	0
X	X	≠CV for bit 5	X	X	X	X	X	0
X	X	X	≠CV for bit 4	X	X	X	X	0
X	X	X	X	≠CV for bit 3	X	X	X	0
X	X	X	X	X	≠CV for bit 2	X	X	0
X	X	X	X	X	X	≠CV for bit 1	X	0
X	X	X	X	X	X	X	≠CV for bit 0	0
= CV for bit 7	= CV for bit 6	= CV for bit 5	= CV for bit 4	= CV for bit 3	= CV for bit 2	= CV for bit 1	= CV for bit 0	1

Comparator Instruction Timing Chart

The horizontal dashed lines in the chart represent the comparison values (CV) for each input.

1. Output 1 turns on when all of the input signals match the comparison value.
2. Output 1 turns off when any of the input signals does not match the comparison value.

Figure 43 - Comparator Timing Chart



Function Blocks Command Reference

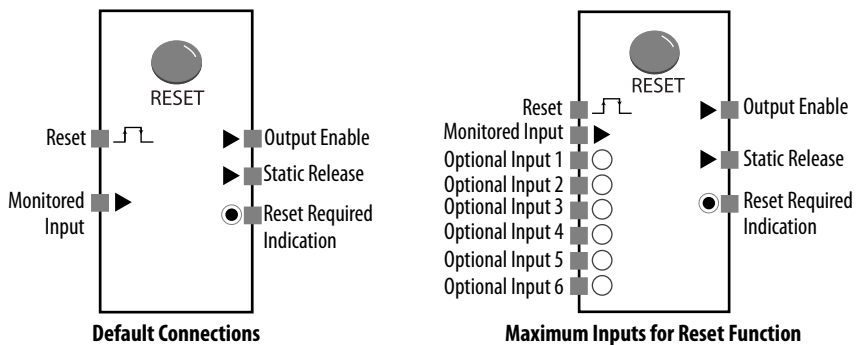
Introduction

This appendix describes the function blocks used for programming.

Topic	Page
Reset Function Block	217
Restart Function Block	219
Emergency Stop (ESTOP)	221
Light Curtain (LC) Function Block	223
Safety Gate Monitoring Function Block	225
Two-hand Control Function Block	230
OFF-delay Timer Function Block	232
ON-delay Timer Function Block	233
User Mode Switch Function Block	234
External Device Monitoring (EDM)	236
Muting	238
Enable Switch	254
Pulse Generator	257
Counter	258

Reset Function Block

Figure 44 - Reset Function Block Diagram



The number of inputs can be increased from two to eight on the I/O Settings tab of the Function Block Properties dialog box in RSNetWorx for DeviceNet software. The default number of inputs is two.

The Output Enable signal turns on if the Reset signal is correctly received while the Monitored Input condition to the Reset function block is on. This function block can be used to prevent the machine from automatically resetting when power to the controller is turned on, when the operating mode is changed from Idle mode to Run mode, or when a signal from a safety input device turns on.

The Static Release and Reset Required Indication are optional outputs. To enable either of these outputs, check the checkbox on the Out point tab of the Function Block Properties dialog box.

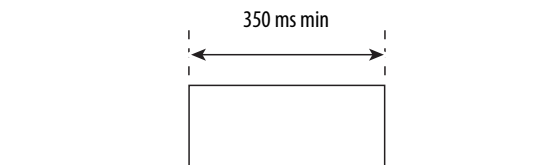
Table 8 - Conditions for Outputs Turning On

Output	Condition for Turn-on
Output Enable	The Monitored Input and all enabled optional inputs must be ON, and the Reset signal must be received correctly.
Static Release	The Monitored Input and all enabled optional inputs must be ON.
Reset Required Indication	The Reset Required Indication becomes a 1 Hz pulse output if the Monitored Input and all enabled optional inputs are ON, and the Output Enable signal is OFF. The Reset Required Indication turns ON only when the Reset signal is ON.

Reset Function Block Parameters

You can set the Reset signal for either Low-High-Low or Rising Edge by using the Parameter tab of the Function Block Properties dialog box. The default setting is Low-High-Low.

When configured for Low-High-Low, the Reset signal must meet the following conditions.



Reset Function Block Timing Charts

Figure 45 - Low-High-Low Reset Signal

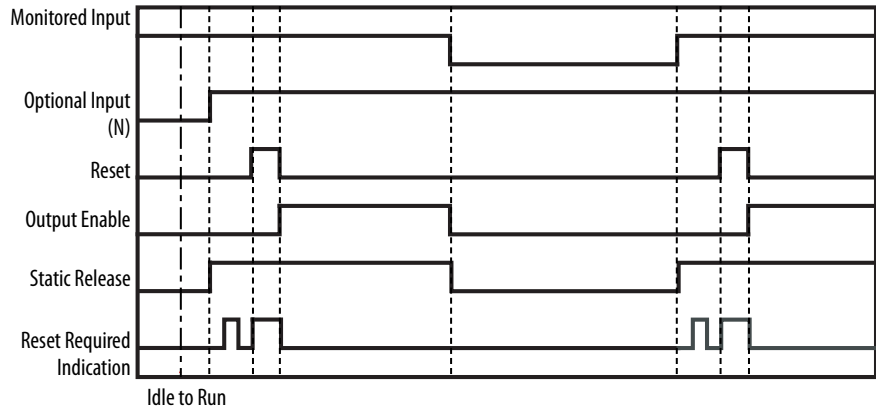
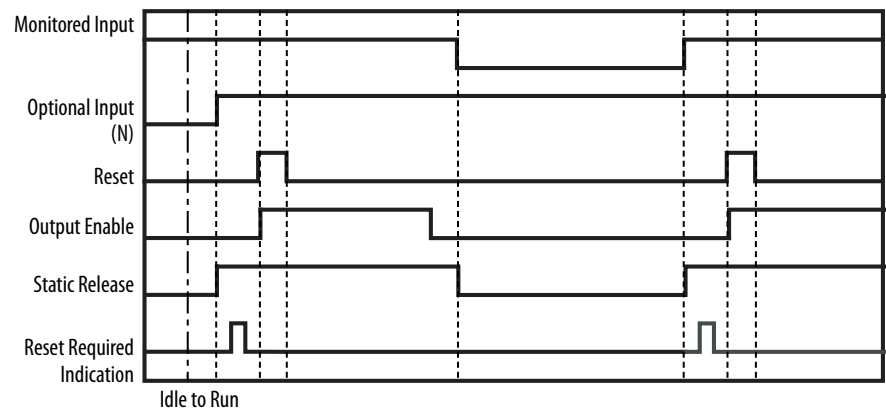
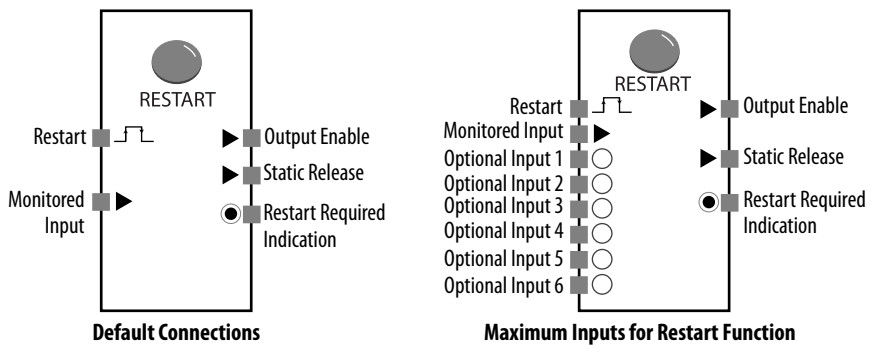


Figure 46 - Rising Edge Reset Signal



Restart Function Block

Figure 47 - Restart Function Block Diagram



The number of inputs can be increased from two to eight on the I/O Settings tab of the Function Block Properties dialog box in RSNetWorx for DeviceNet software. The default number of inputs is two.

The Output Enable signal turns on if the Restart signal is correctly received while the Monitored Input condition to the Restart function block is on. This function block can be used to prevent the machine from automatically restarting when the power to the controller is turned on, when the operating mode is changed, or when a signal from a safety input device turns on. Reset and Restart are functionally identical.

The Static Release and Restart Required Indication are optional outputs. To enable either of these outputs, check the checkbox on the Out point tab of the Function Block Properties dialog box.

Table 9 - Conditions for Outputs Turning On

Output	Condition for Turn-on
Output Enable	The Monitored Input and all enabled optional inputs must be on, and the Restart signal must be received correctly.
Static Release	The Monitored Input and all enabled optional inputs must be on.
Restart Required Indication	The Restart Required Indication becomes a 1 Hz pulse output if the Monitored Input and all enabled optional inputs are on, and the Output Enable signal is off. The Restart Required Indication turns on only when the Restart signal is on.

Restart Function Block Parameters

You can set the Restart signal for either Low-High-Low or Rising Edge on the Parameter tab of the Function Block Properties dialog box. The default setting is Low-High-Low.

When configured for Low-High-Low, the Restart signal must meet the following conditions.



Restart Function Block Timing Charts

Figure 48 - Low-High-Low Restart Signal

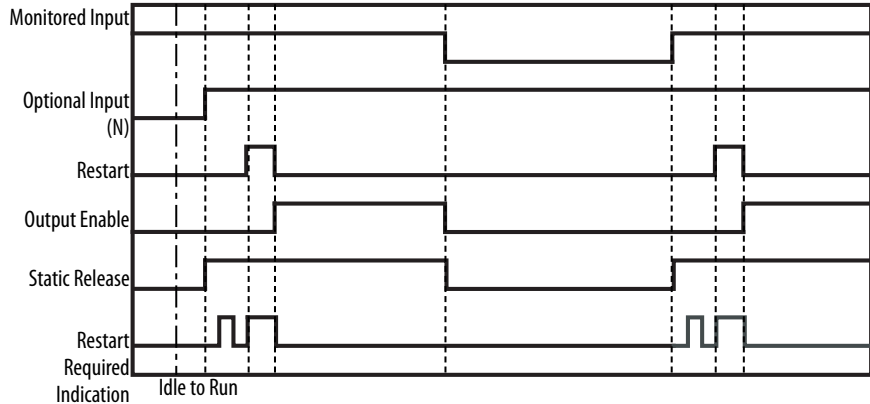
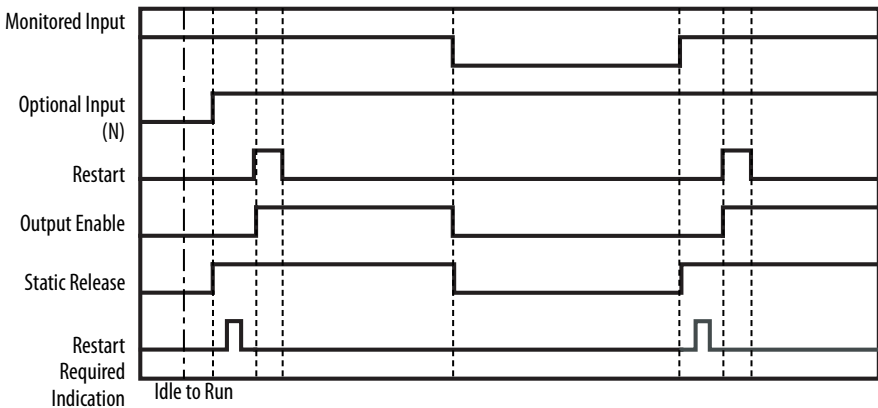
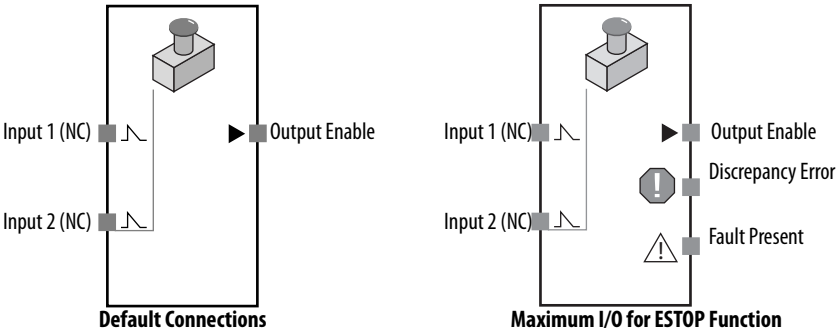


Figure 49 - Rising Edge Restart Signal



Emergency Stop (ESTOP)

Figure 50 - ESTOP Function Block Diagram



The Emergency Stop push button monitoring function lets you monitor an emergency stop push button switch. The Output Enable signal turns on if the inputs from the emergency push button being monitored are active. The Output

Enable turns off if the inputs become inactive or if an error is detected for the function block.

IMPORTANT A manual reset function is required for emergency stop applications. When using the Emergency Stop push button function block, you must also use the Reset function block.

The Discrepancy Error output can be used when programming the ESTOP function block. To display this optional output, check the Discrepancy Error checkbox on the Out point tab of the Function Block Properties dialog box in the Logic Editor of RSNetWorx for DeviceNet software.

A Fault Present output can also be used in programming. To enable this optional output, check the Fault Present checkbox on the Out point tab of the Function Block Properties dialog box.

ESTOP Function Block Parameters

Set these parameters for the ESTOP function block.

Table 10 - ESTOP Function Block Parameters

Parameter	Valid Range	Default Setting
Input Type	Single Channel, Dual Channel Equivalent Dual Channel Complementary	Dual Channel Equivalent
Discrepancy Time	0 . . 30 s in 10 ms increments. ⁽¹⁾ The discrepancy time must be equal to or greater than the cycle time of the controller.	30 ms

(1) A discrepancy time check is not performed when the discrepancy time is set to 0.

ESTOP Function Block Truth Tables

In the truth table, 0 is off and 1 is on.

Table 11 - Truth Table for ESTOP Function Block

Single Channel		Dual Channel Equivalent			Dual Channel Complementary		
Input 1 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Output Enable	Input 1 (NC)	Input 2 (NO)	Output Enable
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

ESTOP Function Block Error Handling

A discrepancy error is generated when one of the inputs is not in its correct state for longer than the Discrepancy Time. For example, in Dual Channel Equivalent mode, both inputs must be active (on) within the Discrepancy Time or an error occurs.

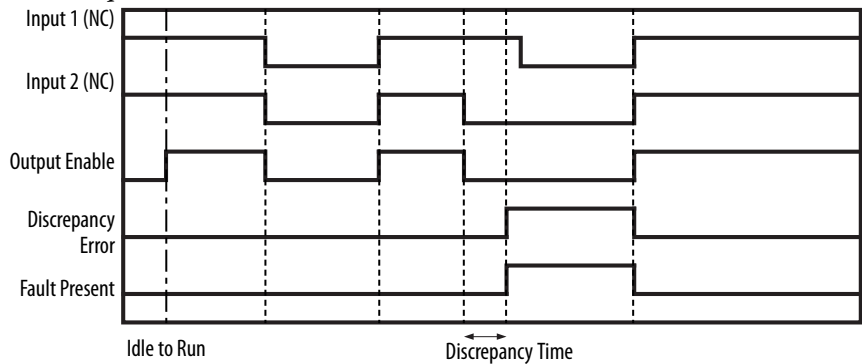
Use this table to diagnose and reset a discrepancy error condition in the ESTOP function block.

Table 12 - Error Detection and Reset for ESTOP Function Block

Error Condition	Status When an Error Occurs			To Reset the Error Condition
	Output Enable	Fault Present	Error Output	
Discrepancy Error	OFF (Safety State)	ON	Discrepancy Error Output: ON	Remove the cause of the error and then either: 1. Make the inputs active and inactive again. 2. Change the controller's operating mode to Idle and back to Run.

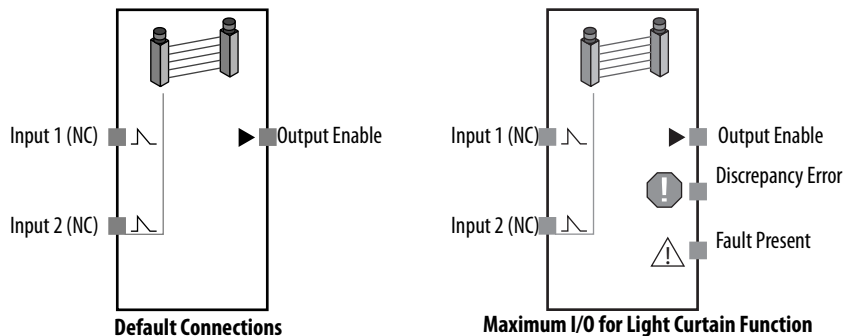
ESTOP Function Block Timing Chart

The chart shows the I/O timing when the function block is set up as Dual Channel Equivalent.



Light Curtain (LC) Function Block

Figure 51 - Light Curtain Function Block Diagram



The Light Curtain monitoring function block monitors a type-4 safety light curtain. The Output Enable signal turns on when the inputs from the safety light curtain being monitored are active. The Output Enable signal turns off if the inputs become inactive or if an error is detected for the function block.

You can use a Discrepancy Error output when programming the LC function block. To display this optional diagnostic output, check the Discrepancy Error checkbox on the Out point tab of the Function Block Properties dialog box in the Logic Editor of RSNetWorx for DeviceNet software.

A Fault Present output can also be used in programming. To enable this optional output, check the Fault Present checkbox on the Out point tab of the Function Block Properties dialog box of the Function Block Properties dialog box.

Light Curtain Function Block Parameters

Set these parameters for the LC function block.

Table 13 - LC Function Block Parameters

Parameter	Valid Range	Default Setting
Input Type	Dual Channel Equivalent Dual Channel Complementary	Dual Channel Equivalent
Discrepancy Time	0...30 s in 10 ms increments. ⁽¹⁾ The discrepancy time must be equal to or greater than the cycle time of the controller.	30 ms

(1) A discrepancy time check is not performed when the discrepancy time is set to 0.

Light Curtain Function Block Truth Tables

In the truth table, 0 is off and 1 is on.

Table 14 - Truth Table for LC Function Block

Dual Channel Equivalent			Dual Channel Complementary		
Input 1 (NC)	Input 2 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Output Enable
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	1
1	1	1	1	1	0

Light Curtain Function Block Error Handling

A discrepancy error is generated when one of the inputs is not in its correct state for longer than the Discrepancy Time. For example, in Dual Channel Equivalent mode, both inputs must be active (on) within the Discrepancy Time or an error occurs.

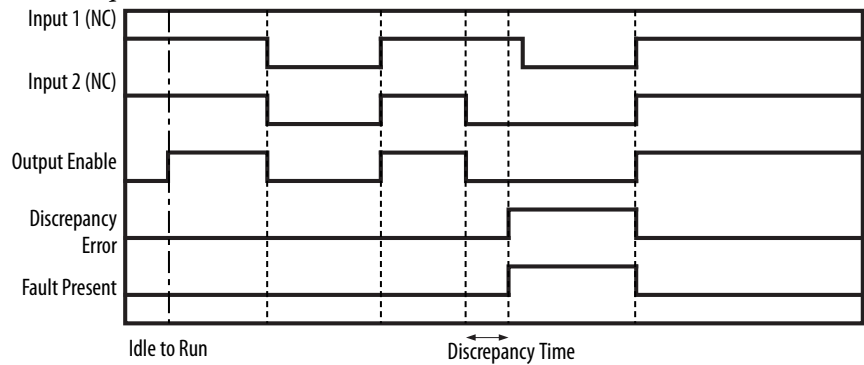
Use this table to diagnose and reset a discrepancy error condition in the LC function block.

Table 15 - Error Detection and Reset for LC Function Block

Error Condition	Status When an Error Occurs			To Reset the Error Condition
	Output Enable	Fault Present	Error Output	
Discrepancy Error	OFF (Safety State)	ON	Discrepancy Error Output: ON	Remove the cause of the error and then either: 1. Make the inputs inactive and active again. 2. Change the controller's operating mode to Idle and back to Run.

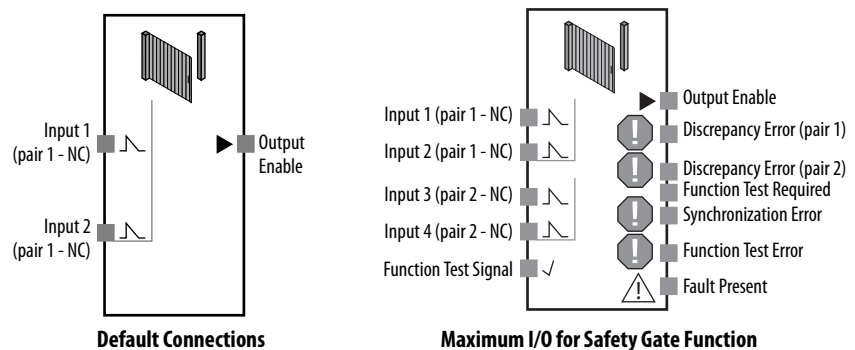
Light Curtain Function Block Timing Chart

The chart shows the I/O timing when the function block is set up as Dual Channel Equivalent.



Safety Gate Monitoring Function Block

Figure 52 - Safety Gate Monitoring Function Block Diagram



The Safety Gate Monitoring function monitors the status of a safety gate, by using input signals from a safety door switch or safety limit switch connected to the door. The Output Enable signal turns on if the inputs from the switch being monitored are active. The Output Enable signal turns off if the inputs become inactive or if an error is detected for that function block.

Safety Gate Monitoring Function Block Optional Outputs

Optional outputs may also be used in programming. To display these optional outputs, check the appropriate checkbox on the Out point tab of the Function Block Properties dialog box in the Logic Editor of RSNetWorx for DeviceNet software.

- Discrepancy Error Pair 1
- Discrepancy Error Pair 2
- Function Test Required Signal
- Synchronization Error
- Function Test Error

Safety Gate Monitoring Function Block Fault Present Output Setting

The Fault Present output can also be used in programming. To enable this output, check the Fault Present checkbox on the Out point tab of the Function Block Properties dialog box.

Safety Gate Monitoring Function Block Function Tests

For some safety gate applications, such as Category 2, safeguarding devices require physical verification that the gate continues to operate properly.

If the function test is enabled for the Safety Gate Monitoring function block, a safety gate test, in which the safety gate must be physically opened and closed again, can be added as a condition for turning on the Output Enable signal.

If enabled, the safety gate test must be executed under the following conditions:

- Startup – The safety gate test must be executed when the controller is started, that is, when the operating mode changes from Idle to Run. If the test ends normally, the Output Enable signal turns on.
- Function Test Request From the Machine – The safety gate test must be executed after the controller detects the Function Test Signal from the machine, turns on, and before the Function Test Signal turns on again. If the Function Test Signal turns on a second time before the safety gate test is completed normally, a function test error occurs, the Output Enable signal turns off, and the Function Test Error Signal turns on.
- Error Detected in Safety Gate Monitoring Function Block – If a function test error, a discrepancy error, or other function block error occurs, the safety gate test must be executed after the cause of the error is removed.

The Function Test Required Signal from the Safety Gate Monitoring function block turns on when a safety gate test is required. It remains on until the safety gate test has been completed normally.

Safety Gate Monitoring Function Block Parameters

Set these parameters for the Safety Gate Monitoring function block.

Table 16 - Safety Gate Monitoring Function Block Parameters

Parameters	Range	Default
Input Type	Single Channel Dual Channel Equivalent (1 pair) Dual Channel Complementary (1 pair) Two Dual Channel Equivalent (2 pairs) Two Dual Channel Complementary (2 pairs)	Dual Channel Equivalent
Function Test	No Function Test/Function Test Required	No Function Test
Discrepancy Time Pair 1	0...30 s in 10 ms increments A discrepancy time check is not performed if 0 is set.	30 ms
Discrepancy Time Pair 2		
Synchronization Time	0...30 s in 10 ms increments A synchronization time check is not performed if 0 is set.	300 ms

Safety Gate Monitoring Function Block Truth Tables

In the truth tables, 0 is off and 1 is on.

Table 17 - Truth Table for Single Channel and Dual Channel (1 Pair) Safety Gate Monitoring Function Block

Single Channel		Dual Channel Equivalent			Dual Channel Complementary		
Input 1 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Output Enable
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

Table 18 - Truth Table for Dual Channel (2 Pairs) Safety Gate Monitoring Function Block

Dual Channel Equivalent (2 Pairs)					Dual Channel Complementary (2 Pairs)				
Input 1 (NC)	Input 2 (NC)	Input 3 (NC)	Input 4 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Input 3 (NC)	Input 4 (NC)	Output Enable
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	1	0
0	0	1	0	0	0	0	1	0	0
0	0	1	1	0	0	0	1	1	0
0	1	0	0	0	0	1	0	0	0
0	1	0	1	0	0	1	0	1	0
0	1	1	0	0	0	1	1	0	0
0	1	1	1	0	0	1	1	1	0
1	0	0	0	0	1	0	0	0	0

Table 18 - Truth Table for Dual Channel (2 Pairs) Safety Gate Monitoring Function Block

Dual Channel Equivalent (2 Pairs)					Dual Channel Complementary (2 Pairs)				
Input 1 (NC)	Input 2 (NC)	Input 3 (NC)	Input 4 (NC)	Output Enable	Input 1 (NC)	Input 2 (NC)	Input 3 (NC)	Input 4 (NC)	Output Enable
1	0	0	1	0	1	0	0	1	0
1	0	1	0	0	1	0	1	0	1
1	0	1	1	0	1	0	1	1	0
1	1	0	0	0	1	1	0	0	0
1	1	0	1	0	1	1	0	1	0
1	1	1	0	0	1	1	1	0	0
1	1	1	1	1	1	1	1	1	0

Safety Gate Monitoring Function Block Error Handling

A discrepancy error is generated when one of the inputs is not in its correct state for longer than the discrepancy time. For example, in Dual Channel Equivalent mode, both inputs must be active (on) within the discrepancy time or an error occurs.

If two pairs of inputs are selected and a synchronization time is entered, both pairs of inputs must be in the same state within the synchronization time or a synchronization error occurs. The discrepancy time applies to both inputs of the same input pair being in the same state within a given time, whereas the synchronization time applies to both sets of input pairs being in the same state within a given time.

Use this table to diagnose and reset a discrepancy error condition in the Safety Gate Monitoring function block.

Table 19 - Error Detection and Reset for Safety Gate Monitoring Function Block

Error Condition	Status When an Error Occurs			To Reset the Error Condition	
	Output Enable	Fault Present	Error Output	When Function Test is Disabled	When Function Test is Enabled
Discrepancy Error at Pair 1	OFF (Safety State)	ON	Discrepancy Error Pair 1: ON	Remove the cause of the error and then either 1. Make the inputs active and inactive again. ⁽²⁾ 2. Change the controller's operating mode to IDLE and back to RUN.	Remove the cause of the error and then make the inputs active and inactive again (that is, perform the safety gate test).
Discrepancy at Pair 2			Discrepancy Error Pair 2: ON		
Function Test Error ⁽¹⁾			Function Test Error: ON		
Synchronization Error			Synchronization Test Error: ON		

(1) Safety gate test was not performed normally between Function Test signals.

(2) If a Discrepancy Error occurs in one of the pairs when set to Dual Channel Equivalent (2 Pairs) or Dual Channel Complementary (2 Pairs), make input pairs 1 and 2 both inactive and then active.

Safety Gate Monitoring Function Block Timing Charts

Figure 53 - Single Channel With Function Test Enabled

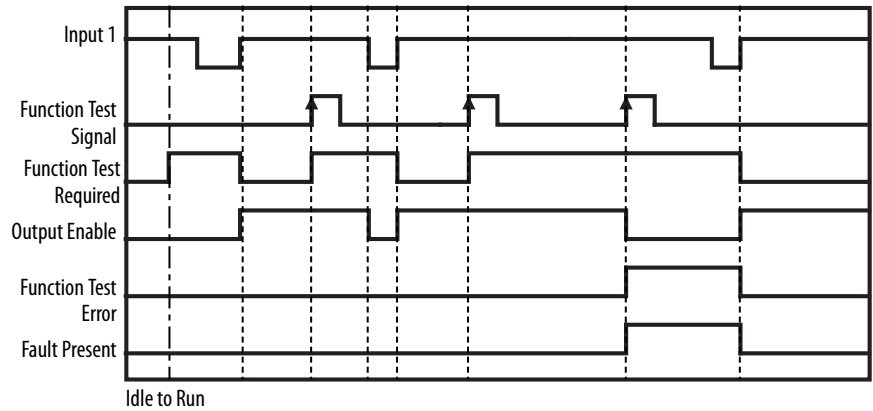


Figure 54 - Dual Channel Equivalent With Function Test Disabled

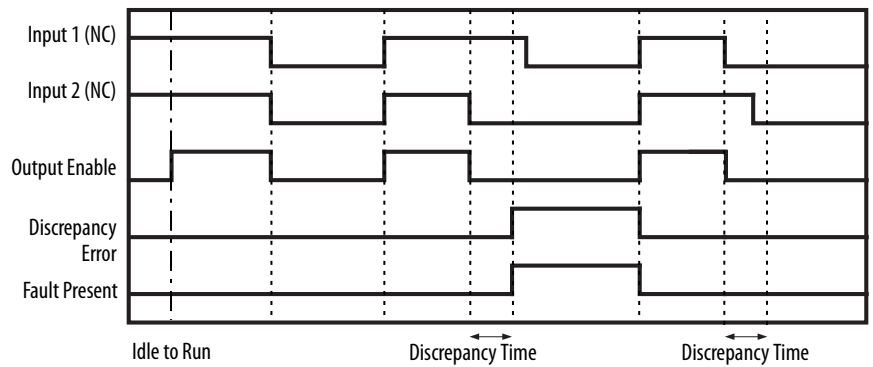
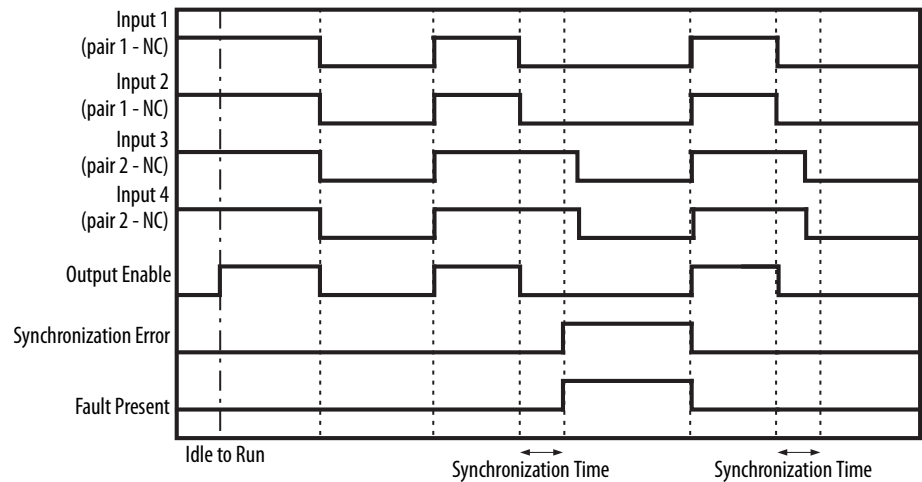
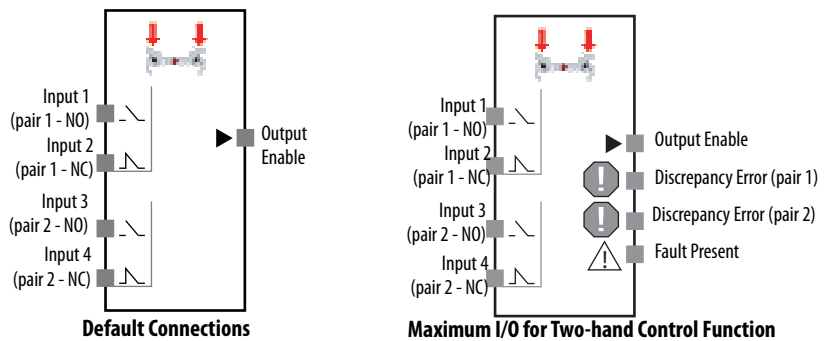


Figure 55 - Dual Channel Equivalent (2 Pairs) With Function Test Disabled



Two-hand Control Function Block

Figure 56 - Two-hand Control Function Block Diagrams



The Two-hand Control function block enables monitoring the status of a two-hand switch. The two-hand control function block can be used with a suitable two-hand switch to meet the requirements of type III C in EN 574, Two-hand Control Devices, Functional Aspect - Principle for Design.

The output signal turns on only if both inputs from the two-hand switch are active and satisfy the requirements of EN 574. The Output Enable signal turns off if the inputs from the two-hand switch do not satisfy the requirements of EN 574, an input is inactive, or if an error in the function block is detected.

Two-hand Control Function Block Optional Outputs

Optional outputs can also be used in programming. To display these optional outputs, check the appropriate checkbox on the Out point tab of the Function Block Properties dialog box in the Logic Editor of RSNetWorx for DeviceNet software.

- Discrepancy Error Pair 1
- Discrepancy Error Pair 2

Two-hand Control Function Block Fault Present Output Setting

The Fault Present output can also be used in programming. To enable this output, check the Fault Present checkbox on the Out point tab of the Function Block Properties dialog box.

Two-hand Control Function Block Parameters

Set these parameters for the two-hand control function block.

Table 20 - Two-hand Control Function Block Parameters

Parameter	Range	Default
Discrepancy Time Input Pair 1	0...500 ms in 10 ms increments ⁽¹⁾	30 ms
Discrepancy Time Input Pair 2	The discrepancy times must be equal to or greater than the cycle time of the controller.	

(1) A discrepancy time check is not performed if 0 is set.

Two-hand Control Function Block Truth Table

In the truth table, 0 is off and 1 is on.

Table 21 - Truth Table for Two-hand Control Function Block

Input 1 (Pair 1 - NO)	Input 2 (Pair 1 - NC)	Input 3 (Pair 2 - NO)	Input 4 (Pair 2 - NC)	Output Enable
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Two-hand Control Function Block Error Handling

A discrepancy error is generated when one of the inputs is not in its correct state for longer than the discrepancy time. For example, in Dual Channel Equivalent mode, both inputs must be active (on) within the discrepancy time or an error occurs.

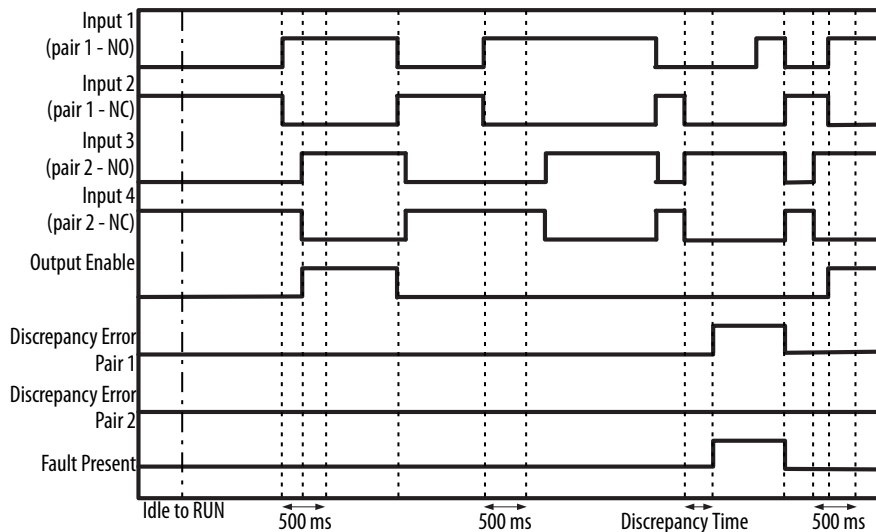
Use this table to diagnose and reset a Discrepancy Error condition in the Two-hand Control function block.

Table 22 - Error Detection and Reset for Two-hand Control Function Block

Error Condition	Status When an Error Occurs			To Reset the Error Condition
	Output Enable ⁽¹⁾	Fault Present	Error Output	
Discrepancy Error at Pair 1	OFF (Safety State)	ON	Discrepancy Error Pair 1: ON	Remove the cause of the error and then either: 1. Make both input pairs 1 and 2 inactive and active again. 2. Change the controller's operating mode to Idle and back to Run.
Discrepancy Error at Pair 2			Discrepancy Error Pair 2: ON	

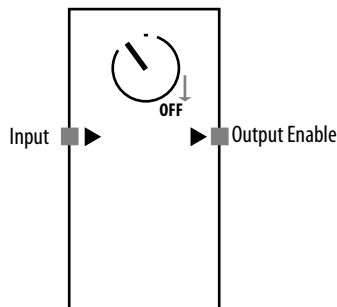
- (1) The Output Enable signal will not turn ON if the synchronization time requirement is not met (that is, operation inputs for both hands must be completed within 500 ms), but this is not considered an error.

Two-hand Control Function Block Timing Chart



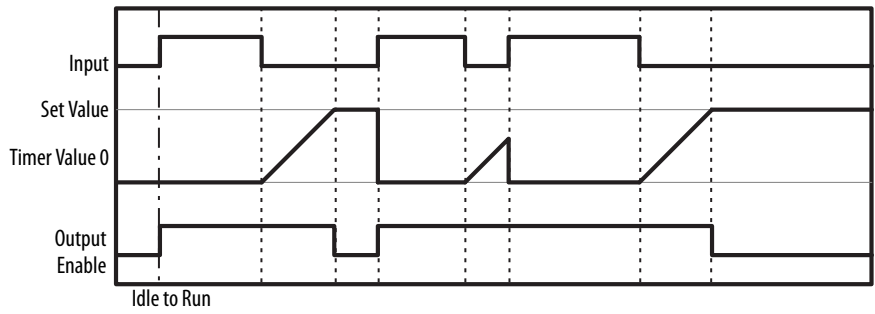
OFF-delay Timer Function Block

Figure 57 - OFF-delay Timer Function Block Diagram



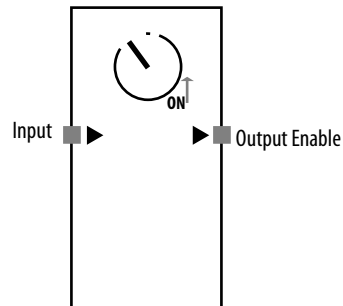
The OFF-delay timer function block performs a timer operation for an OFF-delay set in 10 ms increments. The range for this delay is from 0 ms...300 seconds. The default setting is 0 ms.

OFF-delay Timer Function Block Timing Chart



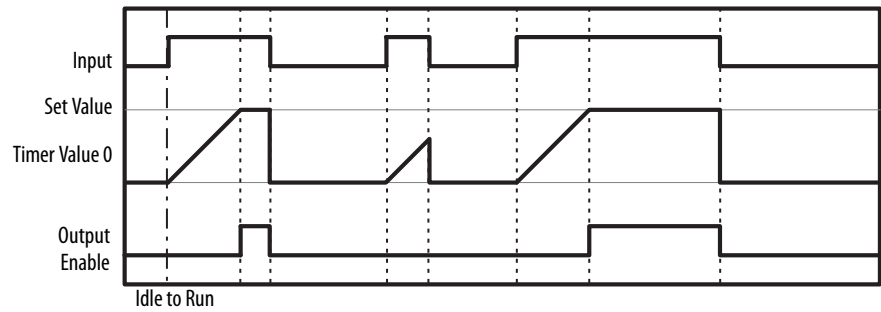
ON-delay Timer Function Block

Figure 58 - ON-delay Timer Function Block Diagram



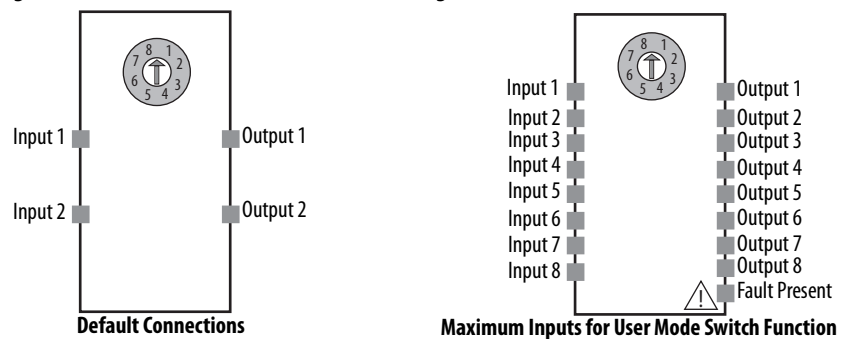
The ON-delay timer function block performs a timer operation for an ON-delay set in 10 ms increments. The range for this delay is 0 ms...300 seconds. The default setting is 0 ms.

ON-Delay Timer Function Block Timing Chart



User Mode Switch Function Block

Figure 59 - User Mode Switch Function Block Diagram



The User Mode Switch function block is used to monitor an operating mode switch in the user system or device. The operating mode switch that can be connected with this function block must be a 1-of-N type switch, that is, one of the N contacts is ON. The function block supports a maximum of eight inputs and eight corresponding outputs.

User Mode Switch Function Block Optional Outputs

The number of I/O can be increased on the In/Out Settings tab of the Function Block Properties dialog box.

Set these parameters for the optional outputs.

Table 23 - User Mode Switch Optional Output Parameters

Parameter	Range	Default
Number of Inputs	2...8	2
Number of Outputs	2...8	2

User Mode Switch Function Block Fault Present Output Setting

The Fault Present output can also be used in programming. To enable this output, check the Use Fault Present checkbox on the In/Out Settings tab of the Function Block Properties dialog box.

User Mode Switch Function Block Truth Table

In the truth table, 0 is off and 1 is on.

Table 24 - Truth Table for User Mode Switch Function Block

Inputs								Outputs							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

User Mode Switch Function Block Error Handling

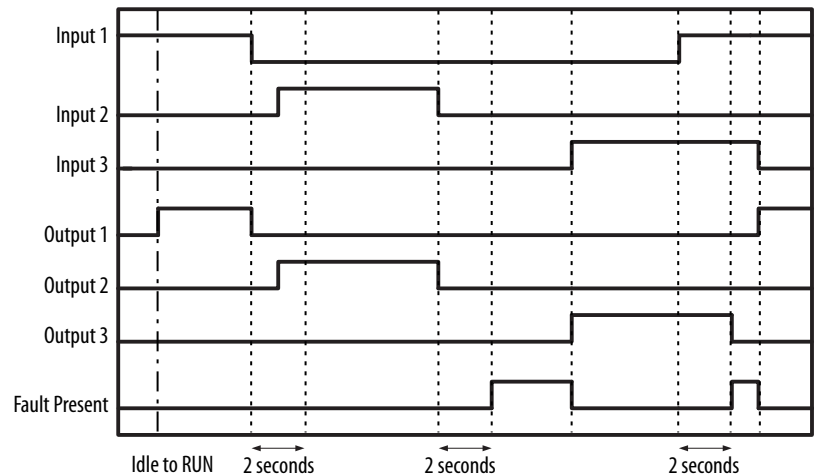
Use this table to diagnose and reset a discrepancy error condition in the User Mode Switch function block.

Table 25 - Error Detection and Reset for User Mode Switch Function Block

Error Condition	Status When an Error Occurs		To Reset the Error Condition
	Output	Fault Present	
More than 1 input was on for more than 2 seconds. ⁽¹⁾	Off (Safety State)	On	Correct the system so that only one contact is on.
All inputs were off for more than 2 seconds.			

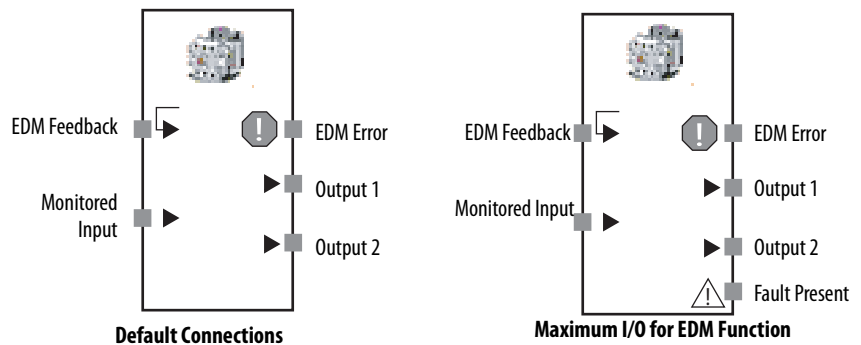
(1) If more than 1 input is on at the same time, the corresponding output of the first input to turn on will turn on for 2 seconds.

User Mode Switch Function Block Timing Chart



External Device Monitoring (EDM)

Figure 60 - External Device Monitoring Function Block Diagram



The External Device Monitoring (EDM) function block evaluates the Monitored Input signal and the status of an external device feedback signal (EDM Feedback) and then turns on safety outputs to an external device.

If the Monitored Input signal turns on, the Output 1 and Output 2 signals turn on. When this occurs, the status of the feedback signal must change within the specified time. If the Monitored Input signal turns off, the Output 1 and Output 2 signals turn off. When this occurs, the status of the feedback signal must change within the specified time.

If the status of the feedback signal does not change within the specified time, an EDM error occurs, the Output 1 and Output 2 signals turn off, and the EDM error signal turns on.

EDM Function Block Optional Outputs

Optional outputs can also be used in programming. To use these optional outputs, check the appropriate checkbox on the Out point tab of the Function

Block Properties dialog box in the Logic Editor of RSNetWorx for DeviceNet software.

- EDM error
- Output 2

EDM Function Block Fault Present Output Setting

The Fault Present output can also be used in programming. To enable this output, check the Use Fault Present checkbox on the Out point tab of the Function Block Properties dialog box.

EDM Function Block Parameter

Set this parameter for the EDM function block.

Table 26 - EDM Function Block Parameter

Parameter	Range	Default
EDM Feedback Maximum Time Delay (T_{EDM})	100 ... 1000 ms in 10 ms increments	300 ms

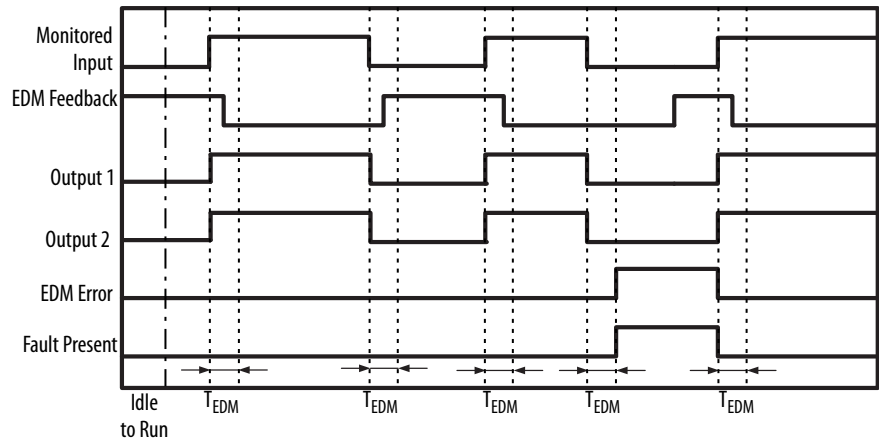
EDM Function Block Error Handling

Use this table to diagnose and reset a discrepancy error condition in the EDM function block.

Table 27 - Error Detection and Reset for EDM Function Block

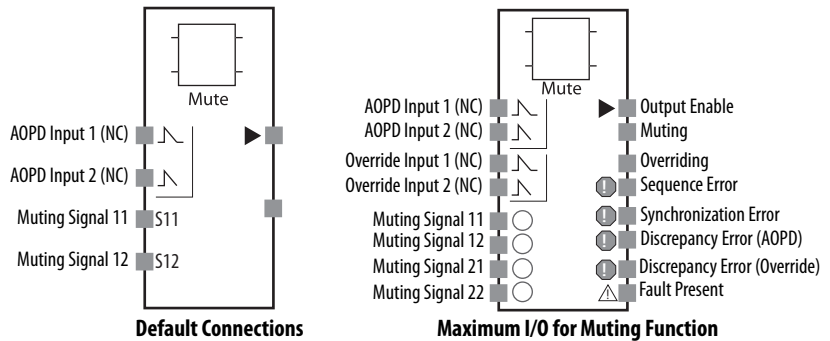
Error Condition	Status When an Error Occurs			To Reset the Error Condition
	Output Enable	Fault Present	Error Output	
EDM Feedback Error	OFF (Safety State)	ON	EDM Error Output: ON	Remove the cause of the error and turn ON the safety input.

EDM Function Block Timing Chart



Muting

Figure 61 - Muting Function Block Diagrams



The Muting function block temporarily disables the light-interruption signal (AOPD input) in a light curtain while the muting sensor is being triggered. While the muting function is operating, machine operation is not stopped, so an object can be removed from the light curtain's detection zone. In addition, the Muting function block has an override function that can disable the light-interruption signal of the light curtain and cause the machine to operate while the light of the light curtain is obstructed. For example, when an object has stopped in the light curtain's detection zone, the machine can be operated in order to remove the object.

Muting Function Block Parameters

Set these parameters for the two-hand control function block.

Table 28 - Muting Function Block Parameters

Parameter	Settings/Range	Default
Muting Mode	<ul style="list-style-type: none"> •Parallel muting with 2 sensors This pattern is suitable for applications at a conveyor entrance. Use this pattern when two retro-reflective photoelectric sensors are set up as muting sensors with intersecting detection zones. •Sequential muting (forward direction) This pattern is suitable for applications at a conveyor entrance. Use this pattern when four through-beam photoelectric sensors are set up as muting sensors. •Sequential muting (both directions) This pattern is suitable for applications at a conveyor entrance or exit. Use this pattern when four through-beam photoelectric sensors are set up as muting sensors. •Position detection This pattern is suitable for applications in which muting is controlled by a switch input. Use this pattern to temporarily disable the light-interruption signal of the light curtain when an operator is placing an object in the machine opening, and the machine is in a state where it will not harm the operator (hazards are in a different zone of the machine). <p>In all of these setting explanations, the muting sensors are on when detection is performed and off when detection is not performed.</p>	Parallel muting with 2 sensors
Synchronization Time ⁽¹⁾	30 ms . . . 3 seconds in 10 ms increments. The timer SV must be longer than the controller's cycle time.	3 seconds
Input Type of AOPD	<ul style="list-style-type: none"> •Dual Channel Equivalent (NC/NC) •Dual Channel Complementary (NC/NO) 	Dual Channel Equivalent
Discrepancy Time (AOPD)	10 . . . 500 ms in 10 ms increments ⁽²⁾ The timer SV must be longer than the controller's cycle time.	30 ms
Input Type of Override Signal	<ul style="list-style-type: none"> •Single Channel •Dual Channel Equivalent (NO/NO) •Dual Channel Complementary (NC/NO) •Not Used 	Not used
Discrepancy Time (Override)	10 . . . 500 ms in 10 ms increments ⁽²⁾ The timer SV must be longer than the controller's cycle time.	30 ms
Max Muting Time	500 ms . . . 127.5 seconds in 500 ms increments 0 . . . 500 ms in 10 ms increments	60 seconds
Max Override Time	500 ms . . . 127.5 seconds in 500 ms increments	60 seconds

(1) Between Muting Signal 11 and Muting Signal 12 or between Muting Signal 21 and Muting Signal 22.

(2) A discrepancy time check will not be performed if 0 is set.

Muting Function Block Optional Outputs

Optional outputs can also be used in programming. To use these optional outputs, check the appropriate checkbox on the In/Out Setting tab of the Function Block Properties dialog box in the Logic Editor of RSNetWorx for DeviceNet software.

- Overriding
- Synchronization error
- Sequence error
- Discrepancy error (AOPD)
- Discrepancy error (Override)

Muting Function Block Fault Present Output Setting

The Fault Present output can also be used in programming. To enable this output, check the Use Fault Present checkbox on the In/Out Setting tab of the Function Block Properties dialog box.

Muting Function Block Error Handling

Use this table to diagnose and reset error conditions in the Muting function block.

Table 29 - Error Detection and Reset for Muting Function Block

Error Condition	Status When an Error Occurs			To Reset the Error Condition
	Output Enable	Fault Present	Error Output ⁽³⁾	
Synchronization Error (between Muting Signal 11 and Muting Signal 12 or between Muting Signal 21 and Muting Signal 22) ⁽¹⁾	ON ⁽²⁾	OFF ⁽²⁾	Synchronization Error: ON	Apply muting again or change the controller's operating mode to Idle and then back to Run mode.
Sequence Error			Sequence Error: ON	
Discrepancy Error (AOPD)	OFF (safety state)	ON	Discrepancy Error (AOPD): ON	Reset when both light curtain input signals change from inactive to active status or you change the controller's operating mode to Idle and then back to Run mode.
Discrepancy Error (Override)			Discrepancy Error (Override): ON	

(1) This error is detected only when the muting mode is configured as Sequential muting (both directions).

(2) If the light curtain goes from this error status to inactive (no light), the Output Enable signal will turn off and the Fault Present signal will turn on. If the light curtain becomes active (light incident) or the override function is executed, the Output Enable signal will turn on and the Fault Present signal will turn off.

(3) If more than one error occurs, errors will be indicated at all affected error outputs.

Muting Function Details

The Muting Function Block reset, start, and stop conditions are described in the following sections.

Reset Conditions

The safety output (Output Enable) is on when all of the following conditions are met:

- The light curtain signal is active (light incident).
- A discrepancy error has not occurred.

Start Conditions

If the muting sensors meet the following conditions while the Output Enable signal is on, muting is applied, and the muting signal turns on:

- the muting sensors are all off.

- while the muting sensors are off, two muting sensors detect an object in the correct sequence.
- while the muting sensors are off, the synchronization times of the two muting sensors are within the normal range (not including the position detection setting).

If an error occurs, an alarm output is generated. The sequence error signal goes on if there is an invalid sequence. The synchronization error signal goes on if an object cannot be detected within the synchronization time. The safety output (Output Enable) goes off if the light curtain signal is inactive (no light) before the controller transitions into the muting state.

Stop Conditions

If the following conditions are met while muting is in effect, the muting is stopped, and the muting signal turns off:

- two or more sensors are not on.
- the maximum muting time has elapsed.
- a discrepancy error has occurred.

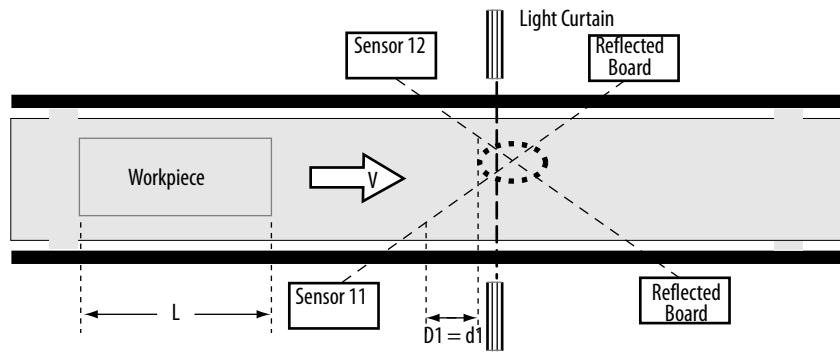
The safety output (Output Enable) goes off if muting is stopped and the light curtain is obstructed.

IMPORTANT When the operating mode of the SmartGuard controller is changed from Idle to Run mode, the input data from the slaves will be off until communication is established. If slave input data is used for the AOPD Input, the Fault Present and Sequence Error Outputs will turn on just after the operating mode is changed to Run mode. When the AOPD Input turns on, the Fault Present output will turn off. When the muting start condition is met, the Sequence Error Output will turn off.

Example: Parallel Muting with Two Sensors

In this example, two retro-reflective photoelectric sensors are set up as the muting sensors with intersecting detection zones. The intersection of the two sensors must be behind the light curtain. Use this configuration when the length of the workpiece (L) is not fixed or long enough to activate sequential muting sensors.

Figure 62 - Application Setup



Sensor 12 is connected to Muting Signal 12. Sensor 11 is connected to Muting Signal 11.

Muting Sequence

In this example, the muting sequence is described below.

1. The light is not interrupted between sensors 11 and 12 and the light curtain, so the Output Enable signal is on.
2. As the workpiece moves to the right and sensors 11 and 12 go on in order, muting is enabled.
3. As the workpiece continues to advance, the Output Enable signal is kept on even if the light curtain is obstructed.
4. As the workpiece continues to advance, the light from sensor 11 is no longer interrupted by the workpiece, the muting status is cleared, and the muting signal turns off.

Distance Settings

When setting up this type of muting application, the distance settings must prevent a passing person from enabling the muting function, and the light curtain and muting sensors must be set up so that a workpiece passes by all of the muting sensors before the next workpiece arrives at the muting sensors.

To calculate the appropriate setup distances for this example use these formulas, where:

D1 = minimum distance required for muting sensor performance

d1 = maximum distance required for muting sensor performance

L = length of the workpiece

V = transit speed of the workpiece

T1min = controller cycle time

T1max = synchronization time setting (the default setting is 3 seconds)

Formula 1: $D1 < L$

Formula 2: $V \times T1min < d1 < V \times T1max$

For the muting function to operate effectively, both formulas must be satisfied.

Sequential Muting (forward direction) Timing Charts

Figure 63 - Normal Operation

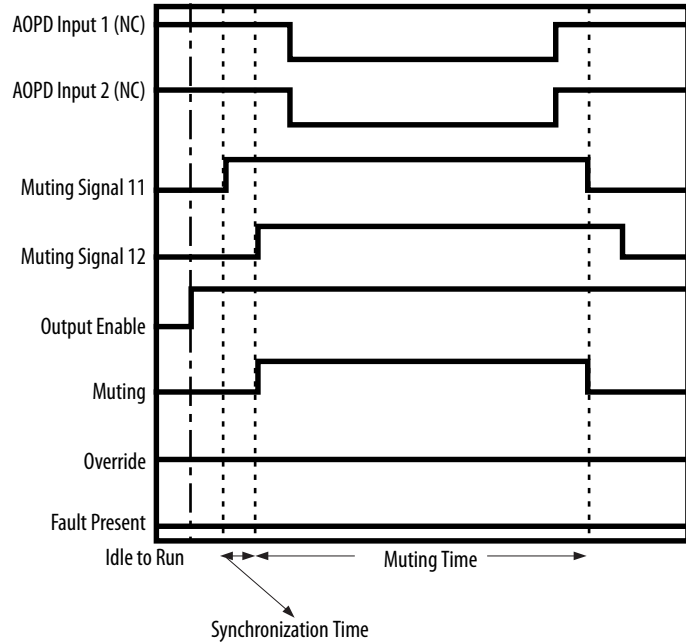


Figure 64 - Synchronization Error

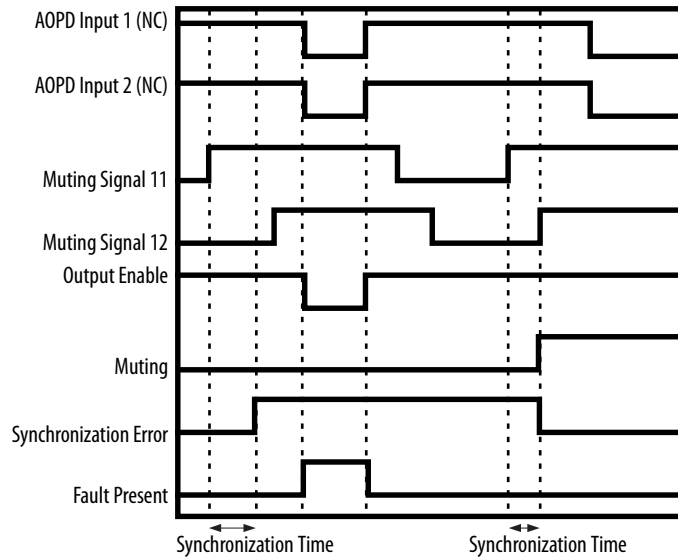
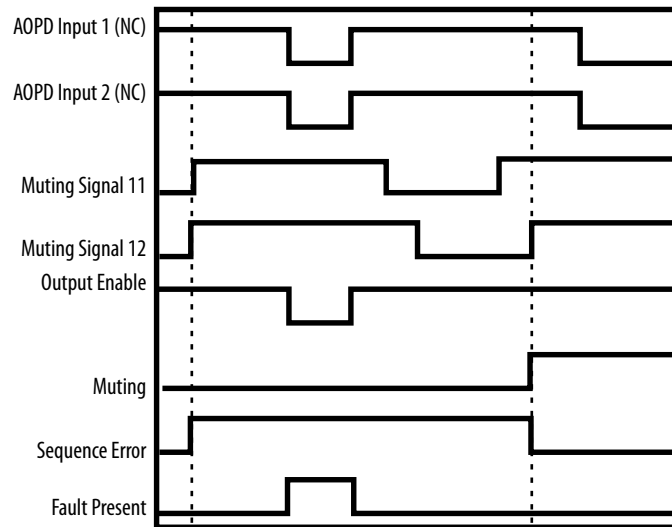


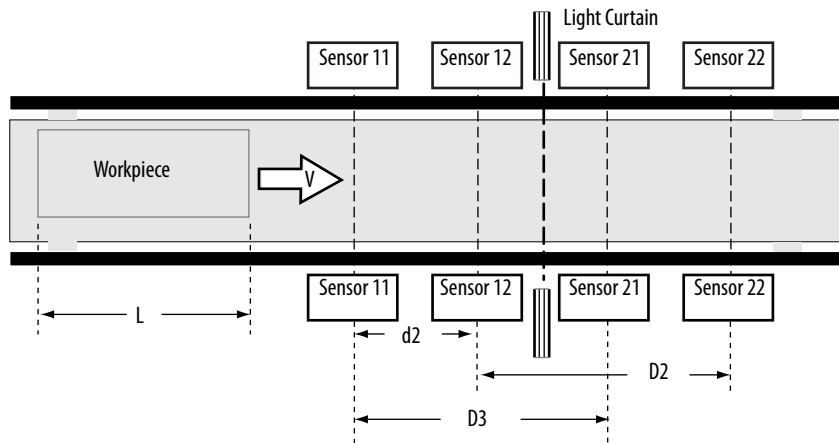
Figure 65 - Sequence Error



Example: Sequential Muting with Four Sensors (forward direction)

In this example, four through-beam photoelectric sensors are set up as the muting sensors with intersecting detection zones. Use this configuration when the length of the workpiece being transported is a fixed length long enough to activate sequentially-mounted muting sensors.

Figure 66 - Application Setup



Sensor 11 is connected to Muting Signal 11. Sensor 12 is connected to Muting Signal 12. Sensor 21 is connected to Muting Signal 21. Sensor 22 is connected to Muting Signal 22.

Muting Sequence

The muting sequence for this example is described below.

1. The light is not interrupted between sensors 11, 12, 21, and 22 and the light curtain, so the Output Enable signal is on.
2. As the workpiece moves to the right and sensors 11 and 12 go on in order, muting is enabled and the muting signal turns on.
3. As the workpiece continues to advance, the Output Enable signal is kept on even if the light curtain is obstructed.
4. As the workpiece continues to advance, the light from sensor 21 is no longer interrupted by the workpiece, the muting status is cleared, and the muting signal turns off.

Distance Settings

When setting up this type of muting application, the distance settings must prevent a passing person from enabling the muting function, and the light curtain and muting sensors must be set up so that a workpiece passes by all of the muting sensors before the next workpiece arrives at the muting sensors.

To calculate the appropriate setup distances for this example, use these formulas, where:

D2 and D3 = minimum distance required for muting sensor performance

d2 = maximum distance required for muting sensor performance

L = length of the workpiece

V = transit speed of the workpiece

T1min = controller cycle time

T1max = synchronization time setting (the default setting is 3 seconds)

Formula 3: $D2 < L$

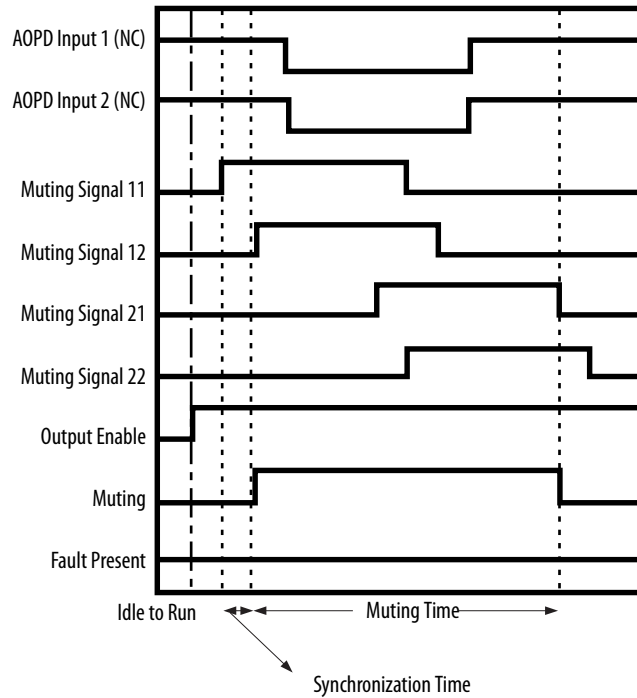
Formula 4: $D3 < L$

Formula 5: $V \times T1min < d2 < V \times T1max$

For the muting function to operate effectively, formulas 3, 4, and 5 must be satisfied.

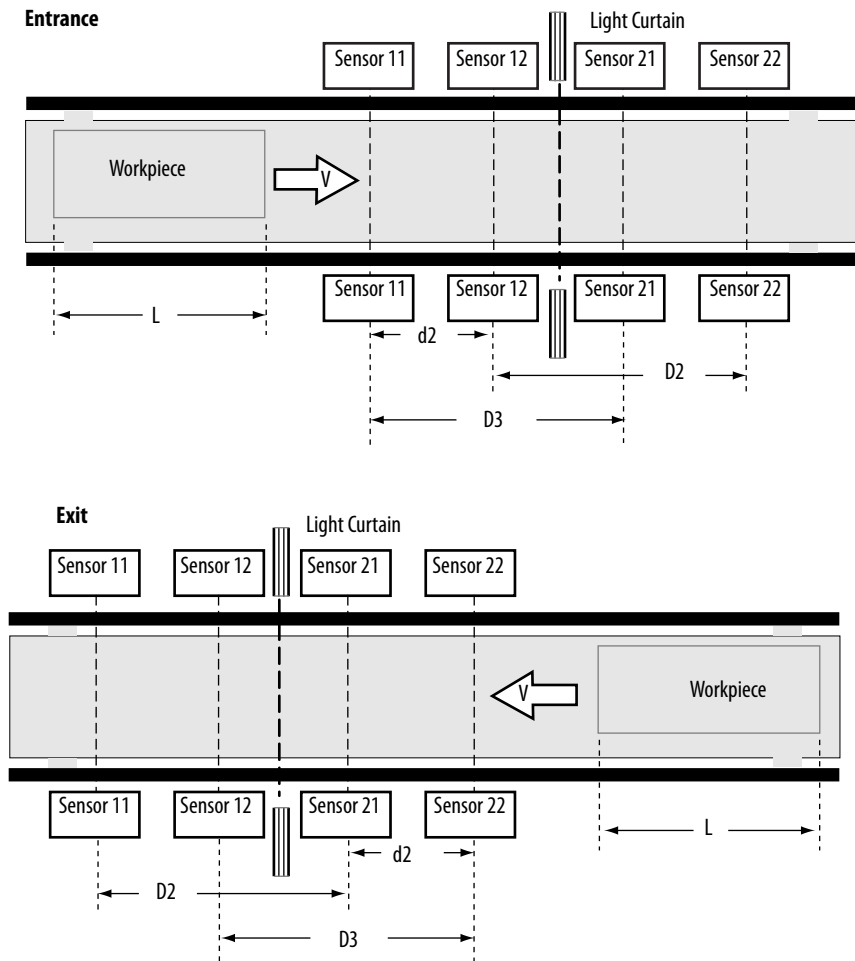
Sequential Muting (forward direction) Timing Chart

Figure 67 - Normal Operation



Example: Sequential Muting with Four Sensors (both directions)

In this example, four through-beam photoelectric sensors are set up as the muting sensors with intersecting detection zones.

Figure 68 - Application Setup

Sensor 11 is connected to Muting Signal 11. Sensor 12 is connected to Muting Signal 12. Sensor 21 is connected to Muting Signal 21. Sensor 22 is connected to Muting Signal 22.

Muting Sequence

The muting sequence for this example is described below.

1. The light is not interrupted between sensors 11, 12, 21, and 22 and the light curtain, so the Output Enable signal is on.
2. For the entrance, as the workpiece moves to the right and sensors 11 and 12 go on in order (sensors 21 and 22 go on as the workpiece exits), muting is enabled and the muting signal turns on.
3. As the workpiece continues to advance, the Output Enable signal is kept on even if the light curtain is obstructed.
4. As the workpiece continues to advance, the workpiece is no longer detected by sensor 21 at the entrance (sensor 12 during workpiece exit), the muting status is cleared, and the muting signal turns off.

Distance Settings

When setting up this type of muting application, the distance settings must prevent a passing person from enabling the muting function, and the light curtain and muting sensors must be set up so that a workpiece passes by all of the muting sensors before the next workpiece arrives at the muting sensors.

To calculate the appropriate setup distances for this example, use these formulas, where:

D2 and D3 = minimum distance required for muting sensor performance

d2 = maximum distance required for muting sensor performance

L = length of the workpiece

V = transit speed of the workpiece

T1min = controller cycle time

T1max = synchronization time setting (the default setting is 3 seconds)

Formula 3: $D2 < L$

Formula 4: $D3 < L$

Formula 5: $V \times T1min < d2 < V \times T1max$

For the muting function to operate effectively, formulas 3, 4, and 5 must be satisfied.

Sequential Muting (both directions) Timing Charts

Figure 69 - Entrance Timing Chart

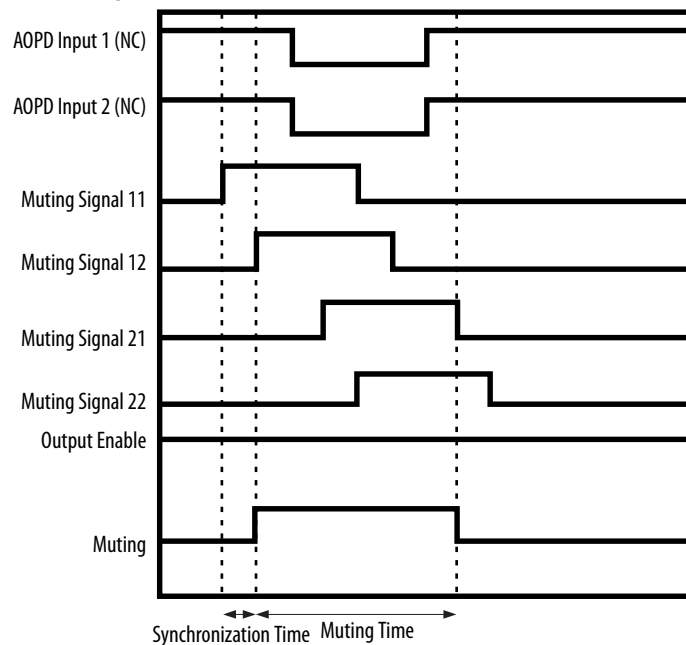
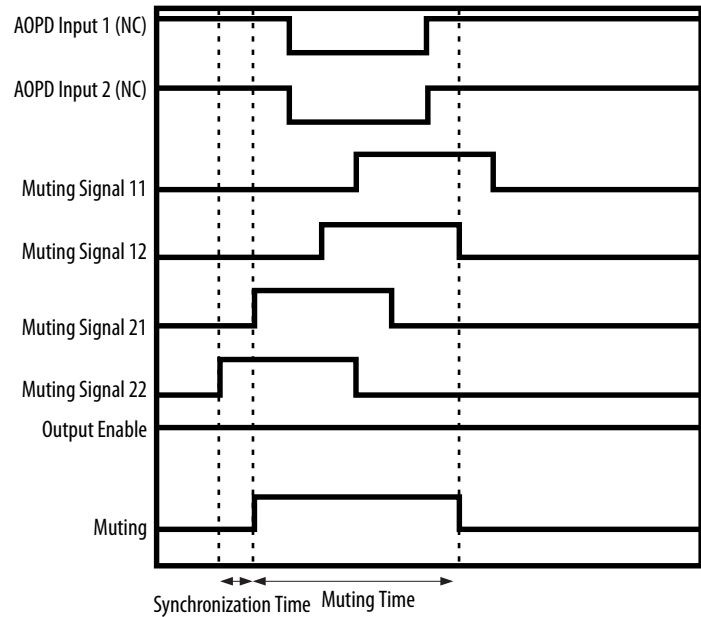


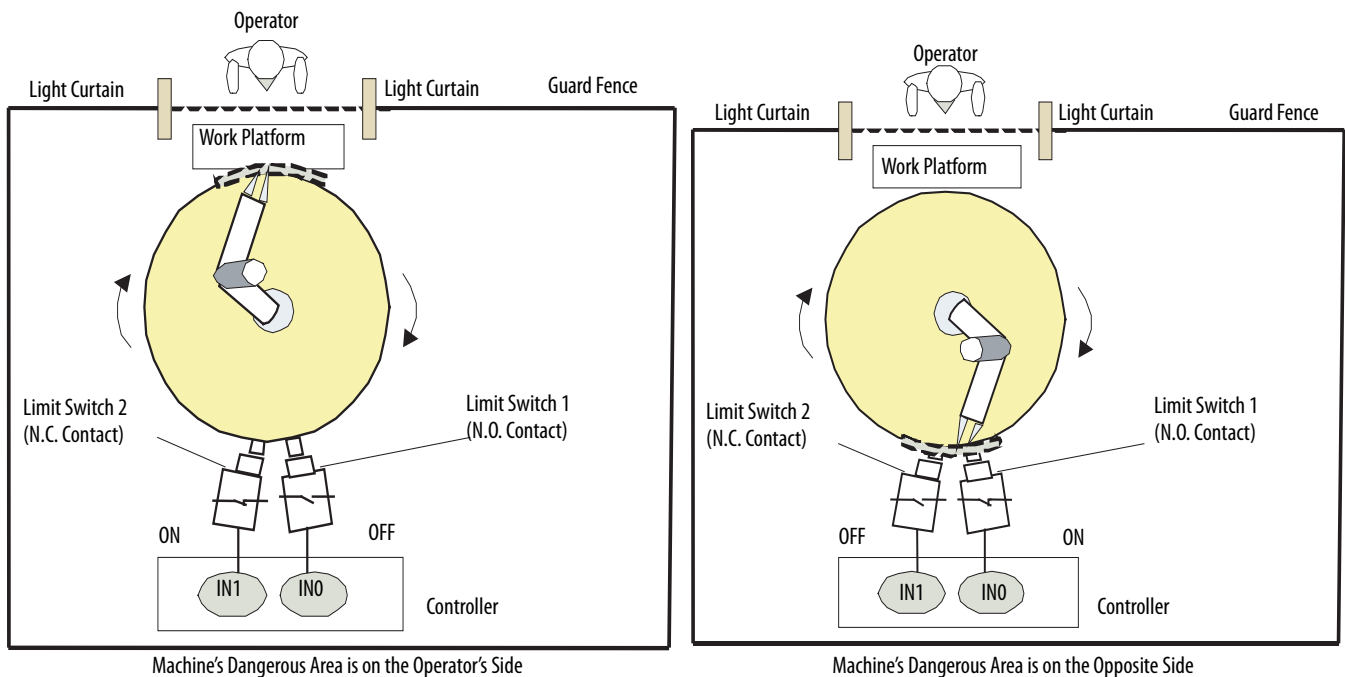
Figure 70 - Time-difference Input Pattern 2: Exit Timing Chart



Example: Position Detection

In this example application, the workpiece is mounted on a machine turntable surrounded by a guard fence. The operator can disable the light-interruption signal of the light curtain safety function to set a workpiece on the turntable when the machine’s dangerous area is on the opposite side of the operator.

Figure 71 - Application Setup

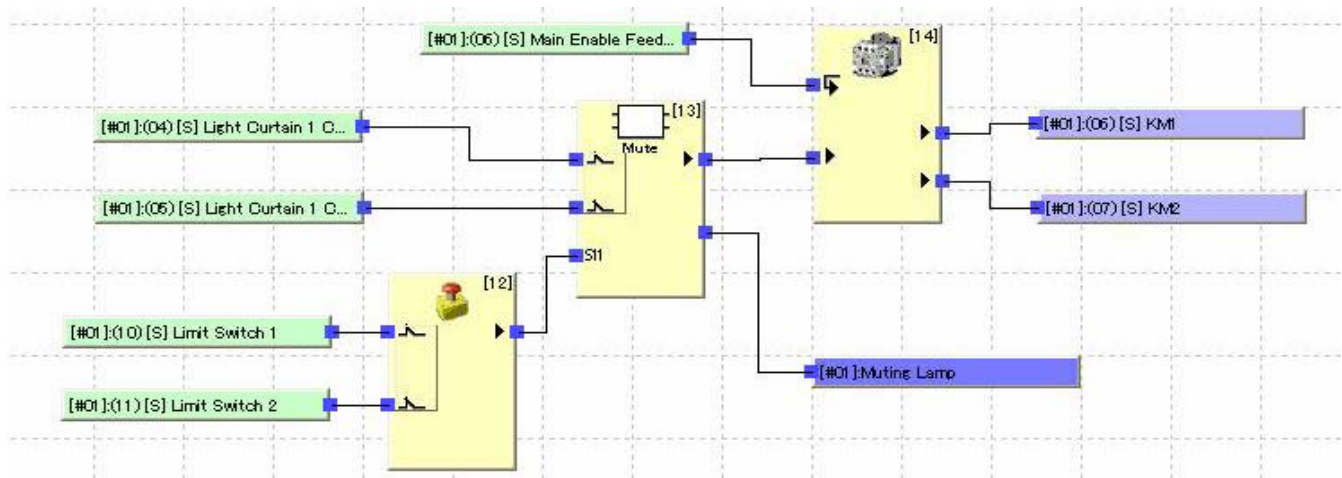


Configure the local input in the controller as dual channel complementary.

Program Example

Limit switches 1 and 2 connect to muting signal 11 of the muting function block using an Estop instruction. Limit switches 1 and 2 are set to dual channel complementary setting for local inputs to evaluate the input data from the two switches.

Figure 72 - Program Logic



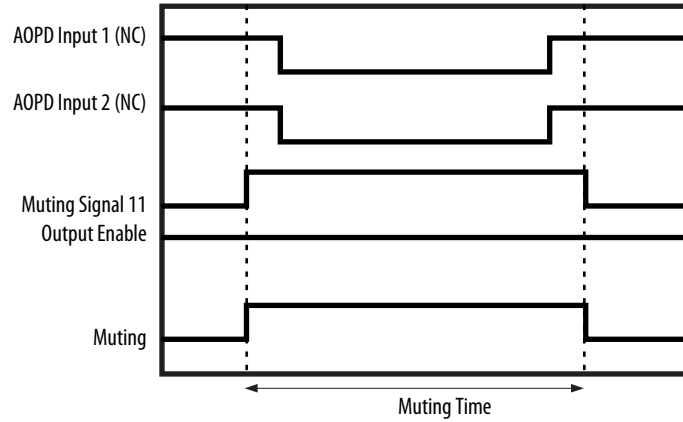
Muting Sequence

The muting sequence for this example is described below.

1. When the machine's dangerous area is on the same side as the operator, N.O. limit switch 1 is off and N.C. limit switch 2 is on. In addition, the light curtain is not obstructed, so the Output Enable signal is on. Muting Signal 11, which inputs the dual channel complementary signal for limit switches 1 and 2, goes off.
2. As the robotic arm rotates, limit switch 1 goes on and limit switch 2 goes off when the dangerous area is opposite the operator. The result of the Estop instruction, which inputs the dual channel complementary signal for limit switches 1 and 2, goes on, so muting is enabled, and the muting signal goes on.
3. At this point, the Output Enable signal is kept on even if the light curtain is obstructed so the operator can access the work platform.
4. When the operator completes his task and the light curtain is unobstructed as the robotic arm rotates, the result of the Estop instruction goes off, the muting status is cleared, and the muting signal goes off.

Timing Chart

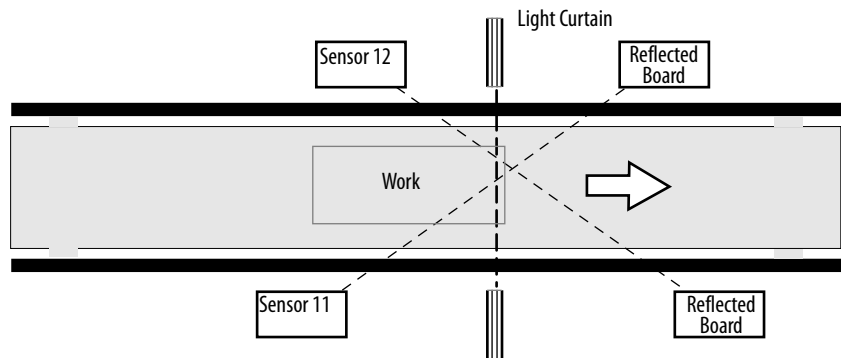
Figure 73 - Normal Operation



Example: Override Function

The override function can turn on the safety output even though the light-interruption signal of the light curtain is inactive. If a workpiece gets jammed during transit, the system cannot be returned to normal operation without forcibly removing the workpiece. In this type of situation, the override function can be used to move the workpiece out of the light curtain detection zone.

Figure 74 - Application Setup



Sensor 11 is connected to Muting Signal 11. Sensor 12 is connected to Muting Signal 12.

Override Sequence

The override sequence in this example is described below.

1. The Output Enable signal is off.
2. When the override inputs turn on, the override function starts and the overriding signal turns on. As long as the override inputs are on, the muting status is forcibly enabled, and both the muting and Output Enable signals are on.
3. When the workpiece moves to the right until it is no longer detected by the sensor (sensor 12 in this case), the muting status forced by the override function is cleared, and both the muting and Output Enable signals turn off.

Override Start Conditions

If the following conditions are met, the override function starts and the Output Enable, muting, and overriding signals turn on.

- At least one muting sensor is on.
- The light curtain is inactive (obstructed).
- The Output Enable is off.
- The override input signal is on (when set as a single input) or active (when set as dual inputs).

Override Stop Conditions

If any one of the following conditions is met, the override function stops and the muting and overriding signals turn off.

- The muting signals are all off.
- The maximum override time has elapsed.
- The Override Input signal is off (when set as a single input) or inactive (when set as dual inputs).

When the override function has stopped, the Output Enable turns off if the light curtain is obstructed.

Timing Chart

The muting mode in the following charts is parallel muting with 2 sensors.

Figure 75 - Normal Operation of the Override Function

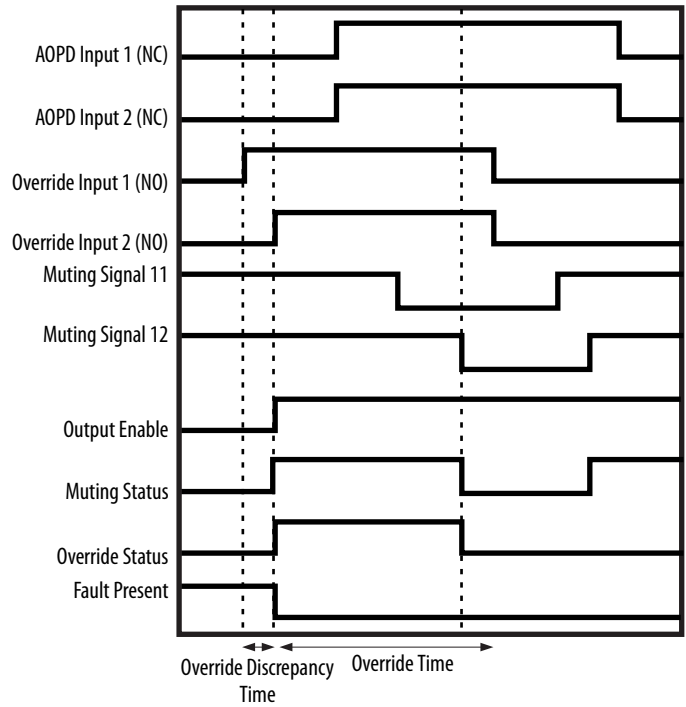


Figure 76 - Override Signal Goes Off During Override

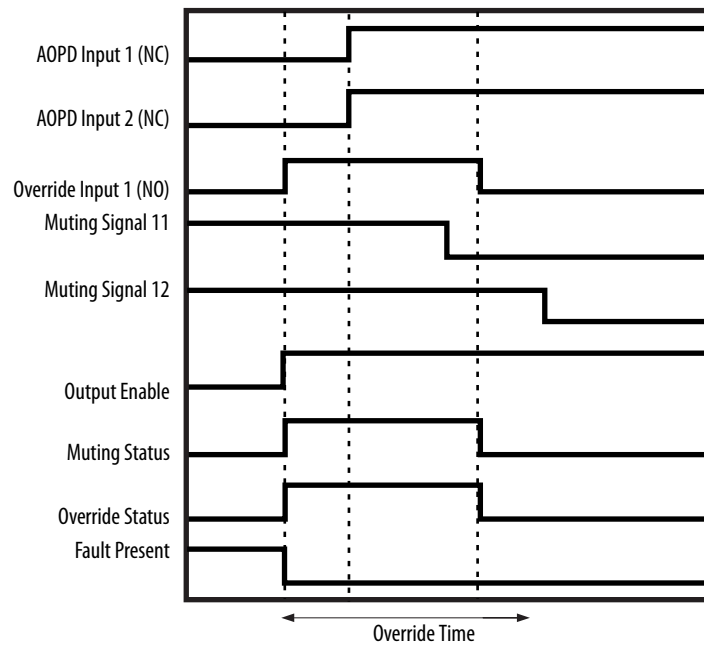
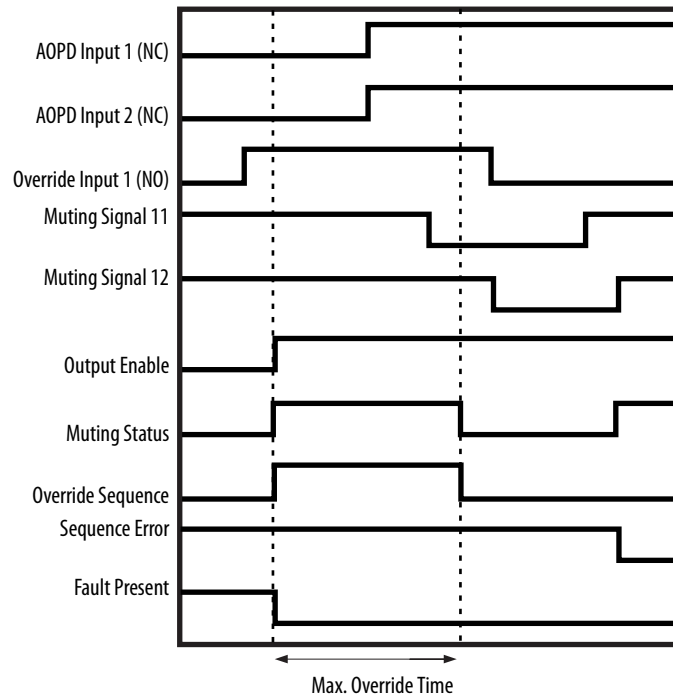
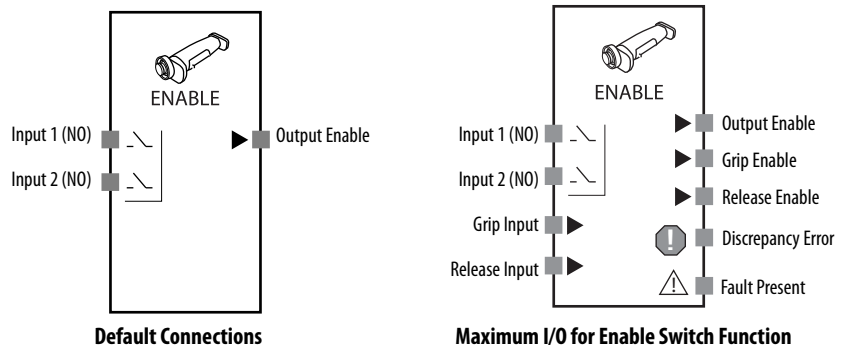


Figure 77 - Override Timeout During Override



Enable Switch

Figure 78 - Enable Switch Block Diagram



The enable switch function block monitors the status of the enable-switch device. The Output Enable signal is on when the inputs from the monitored enable-switch device are active. The Output Enable signal is off when the inputs are not active or an error is detected in the function block.

In addition, if the enable switch device is the type that outputs a grip signal and a release signal, the device's grip input and release input signal status can be monitored. The received grip input and release input signals do not affect the status of the Output Enable signal.

Enable Switch Function Block Parameters

Set these parameters for the Enable Switch function block.

Table 30 - Enable Switch Function Block Parameters

Parameter	Valid Range	Default Setting
Input Type	Single Channel Dual Channel Equivalent	Dual Channel Equivalent
Discrepancy Time	0...30 s in 10 ms increments. ⁽¹⁾ The discrepancy time must be equal to or greater than the cycle time of the controller.	30 ms

(1) A discrepancy time check is not performed when the discrepancy time is set to 0.

The number of inputs can be increased from two to four on the In/Out Settings tab of the Function Block Properties dialog box in RSNetWorx for DeviceNet software. There are two inputs even when the input type is set to Single Channel. The grip input and release input signals can be used when three or four inputs are set. The default setting is two.

Optional Outputs

Optional outputs may also be used in programming. To enable these optional outputs, check the output checkboxes on the Out point tab of the Function Block Properties dialog box.

- Grip enable
- Release enable
- Discrepancy error

Fault Present Output Setting

The Fault Present output can also be used in programming. To enable this output, check the Fault Present checkbox on the Out point tab of the Function Block Properties dialog box.

Enable Switch Function Block Error Handling

Use this table to diagnose and reset a discrepancy error in the Enable Switch function block.

Table 31 - Error Detection and Reset for Enable Switch Function Block

Error Condition	Status When an Error Occurs			To Reset the Error Condition
	Output Enable	Fault Present	Error Output	
Discrepancy error at input pair	OFF (safety state)	ON	Discrepancy Error: ON	Remove the cause of the error, then either: 1. Make both input pairs 1 and 2 inactive and active again. 2. Change the controller's operating mode to Idle and back to Run.

Enable Switch Function Block Timing Charts

Figure 79 - Normal Operation and Discrepancy Error

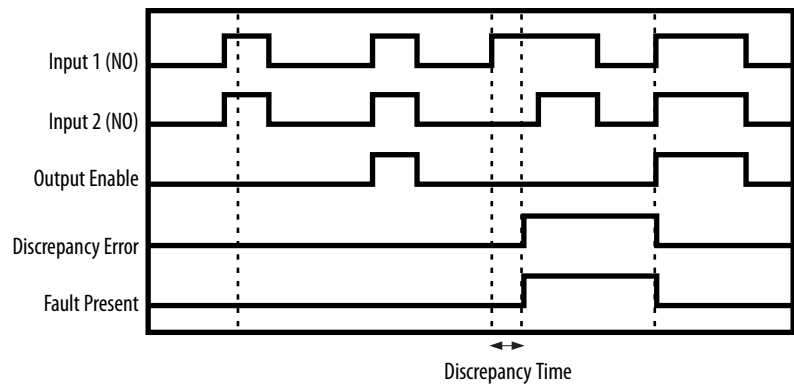
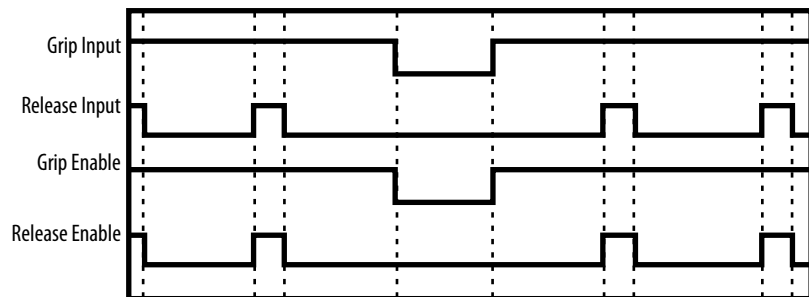
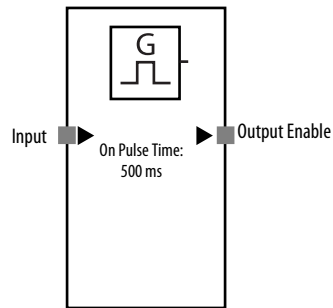


Figure 80 - Grip Signal and Release Signal



Pulse Generator

Figure 81 - Pulse Generator Function Block Diagram



The Pulse Generator function block generates an On/Off pulse output at the output enable signal while the function block's input signal is on.

The pulse's on-time and off-time can be set independently between 10 ms and 3 seconds in 10 ms increments. When the on-time is set to 100 ms and the off-time is set to 500 ms, the signal will be repeatedly turned on for 100 ms and then off for 500 ms.

The output pulse width will have a timing error equivalent to the cycle time of the SmartGuard controller. For example, if the SmartGuard controller's cycle time is 7 ms and the pulse width is set to 100 ms, the output pulse will be anywhere between 93 and 107 ms.

Pulse Generator Function Block Parameters

Set these parameters for the Pulse Generator function block.

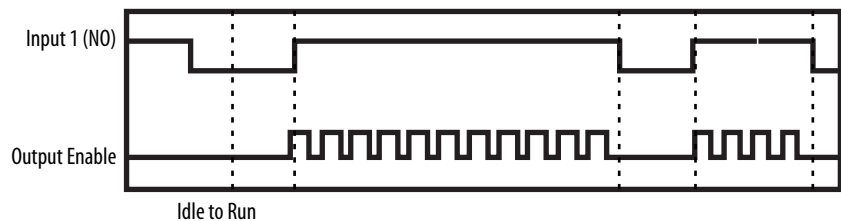
Table 32 - Pulse Generator Function Block Parameters

Parameter	Valid Range	Default Setting
On pulse time	10 ms...3 s in 10 ms increments ⁽¹⁾	500 ms
Off pulse time	10 ms...3 s in 10 ms increments ⁽¹⁾	500 ms

(1) The set value must be longer than the controller's cycle time.

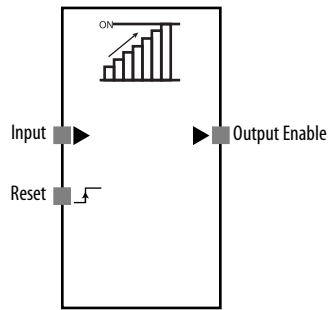
Pulse Generator Function Block Timing Chart

Figure 82 - Pulse Generator Timing Chart



Counter

Figure 83 - Counter Function Block Diagram



The counter function block counts the input pulses at an input and turns on the Output Enable signal when the count reaches a preset value. You set this value by using RSNetWorx for DeviceNet software.

When the input count reaches the preset value, the Output Enable signal turns on and is held on. To detect pulses in the input signal, the input pulse's off-time and on-time must be longer than the controller's cycle time. If the input pulse signal off-time and on-time are shorter than the controller's cycle time, pulses may be missed.

Counter Function Block Parameters

Set these parameters for the Counter function block.

Table 33 - Counter Function Block Parameters

Parameter	Valid Range	Default Setting
Reset condition	Auto reset Manual reset	Manual reset
Count type	Down counter (decrementing) Up counter (incrementing)	Down counter (decrementing)
Counter	1...65,535 counts	1 count

Reset Condition

The reset condition used to reset the input count can be set to manual or auto reset. When the reset condition is set to auto reset and the input count reaches the preset value, the Output Enable signal turns on and remains on as long as the input signal is on. When the input signal goes off, the input count is reset.

When the reset condition is set to manual reset, the input count is reset and the Output Enable signal is turned off when the reset signal goes on. Input pulses are not counted while the reset signal is on.

Count Type

The count type can be set to down counter (decrementing) or up counter (incrementing).

With a down counter, the preset value is the counter's initial value and the counter decrements by one count each time an input pulse is detected. The Output Enable signal turns on when the count reaches zero. This function block's preset value is stored in the function block's internal work area, and can be monitored from a programming device.

With an up counter, the counter's initial value is zero, and the counter increments by one count each time an input pulse is detected. The Output Enable signal turns on when the count reaches the preset value.

Counter Function Block Timing Charts

Figure 84 - Auto Reset Up Counter

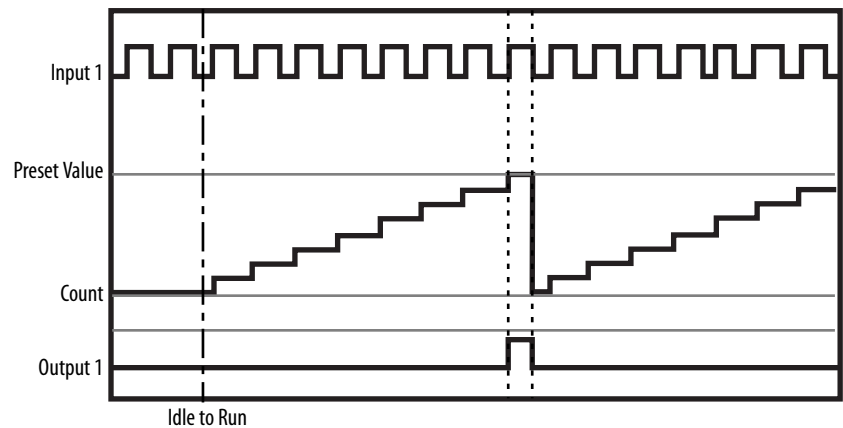


Figure 85 - Auto Reset Down Counter

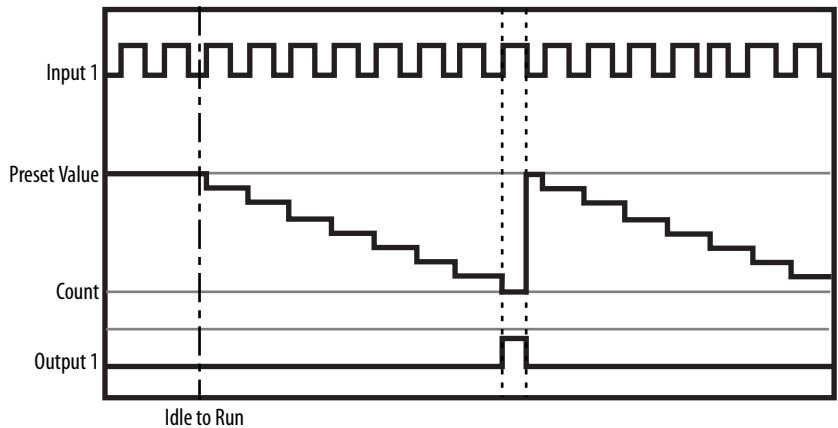


Figure 86 - Manual Reset Up Counter

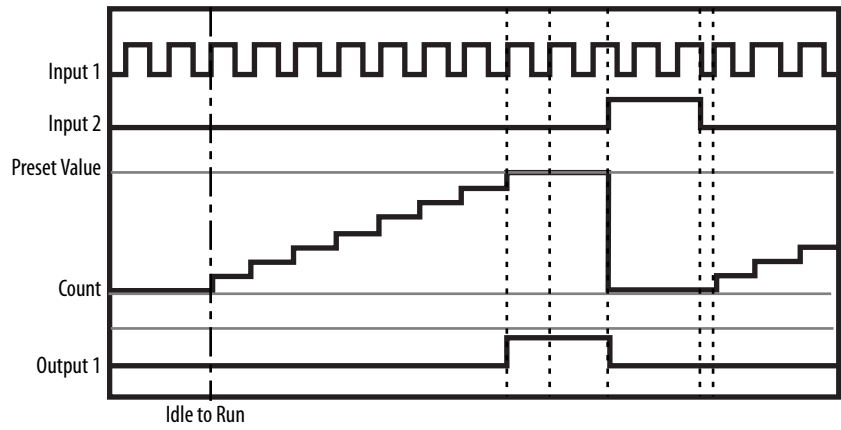
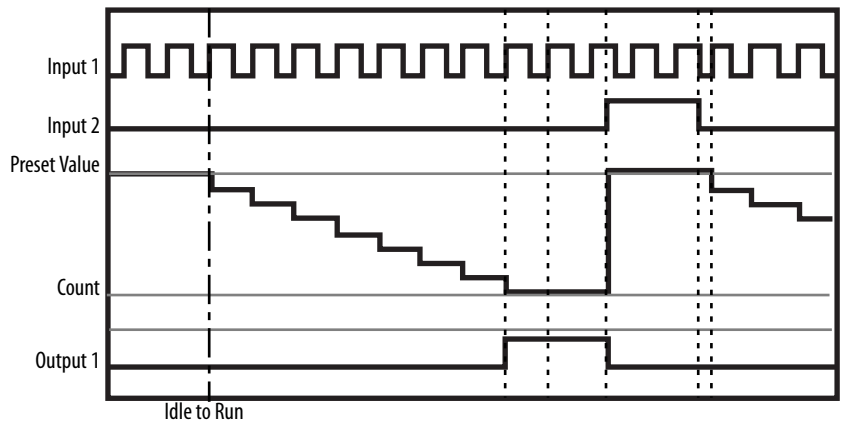


Figure 87 - Manual Reset Down Counter



Explicit Messages

Introduction

Topic	Page
Receiving Explicit Messages	261
Send Explicit Messages	264
Accessing Controller Parameters By Using DeviceNet Explicit Messages	265

Receiving Explicit Messages

Sending an explicit message from a standard DeviceNet master to the SmartGuard controller enables reading or writing any specified data or parameters of the SmartGuard controller. The controller performs according to a command sent from the master and returns a response.

A read command reads the SmartGuard local I/O or safety slave I/O area allocated to the SmartGuard controller from the master.

The basic format of the command and response are shown below.

Figure 88 - Command Format

Destination Node Address	Service Code	Class ID		Instance ID		Offset Address		Data Size	
	4B	03	56						

Figure 89 - Normal Response Format

Number of Receive Bytes	Originating Node Address	Service Code	Read Data						
		CB							

Figure 90 - Error Response Format

Number of Receive Bytes		Originating Node Address	Service Code	Error Code	
00	04		94		

Command Format

The Destination Node Address specifies, in 1 byte hexadecimal, the node address of the data to be read.

For commands, specify 4B (hex) for the Service Code.

Class ID is always 0356 for a SmartGuard controller.

The Instance ID is dependent upon the type of message.

Table 34 - Instance ID Values

Explicit Message Type	Service	Instance ID
Read Local Input Area	Read	0001 (hex)
Read Local Output Area	Read	0002 (hex)
Read Safety Remote Input Area	Read	0005 (hex)
Read Safety Remote Output Area	Read	0006 (hex)

The command data includes the offset size, and data size. The offset size specifies the address from which to start reading. This is an offset in bytes from the first line of the area. The data size specifies the number of bytes to be read from 1...256. The range values shown below should be used as a guide for setting the offset and size for the various data areas.

Table 35 - Range Values

Area	Range
Local Input Area	0 or 1
Local Output/Test Output Area	0 or 1
Safety Remote Input Area	0...551
Safety Remote Output Area	0...551

Response Format

The Number of Receive Bytes for responses indicates the number of bytes of receive data from the originating node address to the end of the returned response (in hexadecimal format).

The Originating Node for responses returns the node address of the responding SmartGuard controller in 1 byte hexadecimal.

For responses, the upper bit is turned on and CB hex is returned for the Service Code.

The Read Data for responses is the I/O data returned from the specified area. The address offsets and bit assignments for reading the local inputs, local outputs, and test outputs are shown below. For these bits, 1 equals normal and 0 equals an error.

Table 36 - Local Inputs (2 bytes)

Offset (bytes)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Safety Input Terminal Number 7	Safety Input Terminal Number 6	Safety Input Terminal Number 5	Safety Input Terminal Number 4	Safety Input Terminal Number 3	Safety Input Terminal Number 2	Safety Input Terminal Number 1	Safety Input Terminal Number 0
1	Safety Input Terminal Number 15	Safety Input Terminal Number 14	Safety Input Terminal Number 13	Safety Input Terminal Number 12	Safety Input Terminal Number 11	Safety Input Terminal Number 10	Safety Input Terminal Number 9	Safety Input Terminal Number 8

Table 37 - Local Outputs and Test Outputs (2 bytes)

Offset (bytes)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Safety Output Terminal Number 7	Safety Output Terminal Number 6	Safety Output Terminal Number 5	Safety Output Terminal Number 4	Safety Output Terminal Number 3	Safety Output Terminal Number 2	Safety Output Terminal Number 1	Safety Output Terminal Number 0
1	Reserved				Test Output Terminal Number 3	Test Output Terminal Number 2	Test Output Terminal Number 1	Test Output Terminal Number 0

Error Response Format

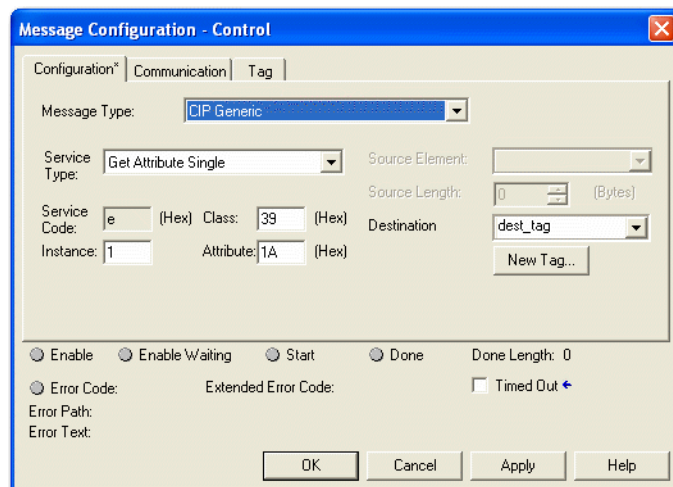
Like the normal response, the error response includes the Number of Receive Bytes, the Originating Node Address, and Service Code. It also includes these DeviceNet error codes.

Table 38 - DeviceNet Explicit Message Error Codes

Response Code	Error Name	Description
08FF	Service not supported	An error exists in the service code.
16FF	Object does not exist	The specified instance ID is not supported.
15FF	Too much data	The data is longer than the specified size.
13FF	Not enough data	The data is shorter than the specified size.
20FF	Invalid parameter	The specified operation command data is not supported.

Example Read Message from a GuardLogix Controller

This GuardLogix message instruction, programmed in RSLogix 5000 software by using the command format parameters on [page 261](#), reads the SmartGuard data.



Send Explicit Messages

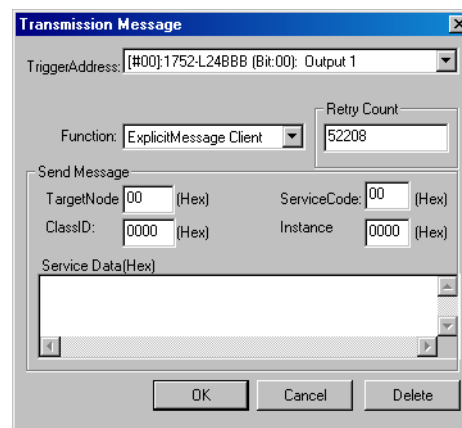
A SmartGuard controller can send explicit messages from a user application program. User-registered messages are sent over the network when user-specified trigger conditions are met. This can be used to notify monitoring and control devices or as a method for specifying outputs to display devices. Up to 32 bytes of explicit message data can be sent.

Table 39 - Explicit Message Data Format

Parameter Name	Data Size
MAC ID	1 byte
Service Code	1 byte
Class ID	2 bytes
Instance ID	2 bytes
Service Data	0...26 bytes

Follow these steps to send an explicit message by using the Logic Editor in RSNetWorx for DeviceNet software.

1. From the menu bar, choose Function>Transmission Message Setting.



2. Use the TriggerAddress pulldown to select the output tag you want to use 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.

3. In the Retry Count field, type the number of times to retry sending the transmission if it fails.

Type 0 for no retries.

4. Check the explicit message format of the destination node and created a send message based on the destination node's specifications, including TargetNode, ServiceCode, Class ID, and Instance ID.

Restrictions on Sending Explicit Messages

Explicit messages are subject to the following restrictions.

- One address can be set in the user program for the trigger address.
- The SmartGuard controller's internal I/O memory is sent as a response to an explicit message. Explicit messages can be sent from a user program in the controller, but internal information in the controller cannot be used as send message data.
- Response data to explicit messages cannot be used in a SmartGuard controller's use program.



ATTENTION: The data attributes handled by standard I/O communication and explicit message communication is non-safety data. The necessary measures for safety data are not taken during generation of standard or explicit message data. Do not use this data to operate a safety control system.

Accessing Controller Parameters By Using DeviceNet Explicit Messages

You can read and write to controller parameters by sending DeviceNet explicit messages to the SmartGuard controller. The controller processes the received messages and returns a response. The messages described in these tables are supported by the SmartGuard controller.

Table 40 - Reading General Status

Explicit Message	Service	Function	Command					Response
			Service Code	Class ID Hex	Instance ID Hex	Attribute ID	Data Size	
Read Unit General Status	Read	Reads the controller's general status	0E hex	39 hex	01 hex	6E hex	--	1 byte

Table 41 - Reading Safety Signature

Explicit Message	Service	Function	Command					Response
			Service Code	Class ID Hex	Instance ID Hex	Attribute ID	Data Size	
Read Unit Safety Status	Read	Reads the SmartGuard's Safety Signature and Time Stamp	0E hex	39 hex	01 hex	1A hex	--	10 bytes

Table 42 - Setting and Monitoring Safety Input Terminals

Explicit Message	Service	Function	Command				Response	
			Service Code	Class ID	Instance ID	Attribute ID		Data Size
Monitor Mode for Terminal Maintenance Information	Read	Reads the monitor mode of maintenance information for the input (1...16) specified by the Instance ID.	0E hex	3D hex	01 to 10 hex	65 hex	—	1 byte 00 hex: Total On Time mode 01 hex: Contact Operation Counter mode
	Write	Writes the monitor mode of maintenance information for the input (1...16) specified by the Instance ID.	10 hex	3D hex	01 to 10 hex	65 hex	1 byte 00 hex: Total On Time mode 01 hex: Contact Operation Counter mode	
SV for Input Total On Time or Contact Operation Counter	Read	Reads the SV of the total on time or contact operation counter for the input (1...16) specified by the Instance ID.	0E hex	3D hex	01 to 10 hex	68 hex	—	4 bytes 0000 0000 ... FFFF FFFF hex (0...4,294,967,295)
	Write	Writes the SV of the total on time or contact operation counter for the input (1...16) specified by the Instance ID.	10 hex	3D hex	01 to 10 hex	68 hex	4 bytes 0000 0000 ... FFFF FFFF hex (0...4,294,967,295)	—
Read Input Total On Time or Contact Operation Counter	Read	Reads the total on time or contact operation counter for the input (1...16) specified by the Instance ID.	0E hex	3D hex	01 to 10 hex	66 hex	—	4 bytes 0000 0000 ... FFFF FFFF hex (0...4,294,967,295)
Reset Input Total On Time or Contact Operation Counter	Reset	Resets to 0 the total on time or contact operation counter for the input (1...16) specified by the Instance ID.	05 hex	3D hex	01 to 10 hex	66 hex	—	—
Read Monitor Status of Input Total On Time or Contact Operation Counter	Read	Reads the monitor status of the total on time or contact operation counter for the input (1...16) specified by the Instance ID.	0E hex	3D hex	01 to 10 hex	67 hex	—	1 byte 00 hex: in range 01 hex: out of range (over monitor value)
Read Safety Input Normal Flag	Read	Reads the normal flag status of the number (1...16) specified by the Instance ID.	0E hex	3D hex	01 to 10 hex	04 hex	—	1 byte 00 hex: error 01 hex: normal

Table 42 - Setting and Monitoring Safety Input Terminals

Explicit Message	Service	Function	Command					Response
			Service Code	Class ID	Instance ID	Attribute ID	Data Size	
Read Safety Input Error Information Cause	Read	Reads the cause for the normal flag of the number (1...16) specified by the Instance ID being off (error).	0E hex	3D hex	01 to 10 hex	6E hex	—	1 byte 00 hex: no error 01 hex: invalid configuration 02 hex: test signal error 03 hex: internal circuit error 04 hex: discrepancy error 05 hex: error in other channel of dual channels
Read AND of Safety Input Normal Flags	Read	Reads the cause for the normal flag of the number (1...16) specified by the Instance ID being off (error).	0E hex	3E hex	01 hex	05 hex	—	1 byte 00 hex: error 01 hex: all normal
Read OR of Monitor Status of Input Total On Times or Contact Operation Counters	Read	Reads the logical OR of the monitor status of the total on time or contact operation counter for all inputs 1...16.	0E hex		01 hex	72 hex	—	1 byte 00 hex: all in range 01 hex: input out of range (over monitor value)

Table 43 - Setting and Monitoring Safety Output Terminals

Explicit Message	Service	Function	Command					Response
			Service Code	Class ID	Instance ID	Attribute ID	Data Size	
Monitor Mode for Terminal Maintenance Information	Read	Reads the monitor mode of maintenance information for the output (1...8) specified by the Instance ID.	0E hex	3B hex	01...08 hex	65 hex	—	1 byte 00 hex: Total On Time mode 01 hex: Contact Operation Counter mode
	Write	Writes the monitor mode of maintenance information for the output (1...8) specified by the Instance ID.	10 hex	3B hex	01...08 hex	65 hex	1 byte 00 hex: Total On Time mode 01 hex: Contact Operation Counter mode	—
SV for Output Total On Time or Contact Operation Counter	Read	Reads the SV of the total on time or contact operation counter for the input (1...8) specified by the Instance ID.	0E hex	3B hex	01...08 hex	68 hex	—	4 bytes 0000 0000... FFFF FFFF hex (0...4,294,967,295)
	Write	Writes the SV of the total on time or contact operation counter for the input (1...8) specified by the Instance ID.	10 hex	3B hex	01...08 hex	68 hex	4 bytes 0000 0000... FFFF FFFF hex (0...4,294,967,295)	—
Read Output Total On Time or Contact Operation Counter	Read	Reads the total on time or contact operation counter for the input (1...8) specified by the Instance ID.	0E hex	3B hex	01...08 hex	66 hex	—	4 bytes 0000 0000... FFFF FFFF hex (0...4,294,967,295)
Reset Output Total On Time or Contact Operation Counter	Reset	Resets to 0 the total on time or contact operation counter for the output (1...8) specified by the Instance ID.	05 hex	3B hex	01...08 hex	66 hex	—	—

Table 43 - Setting and Monitoring Safety Output Terminals

Explicit Message	Service	Function	Command					Response
			Service Code	Class ID	Instance ID	Attribute ID	Data Size	
Read Monitor Status of Output Total On Time or Contact Operation Counter	Read	Reads the monitor status of the total on time or contact operation counter for the output (1...8) specified by the Instance ID.	0E hex	3B hex	01...08 hex	67 hex	—	1 byte 00 hex: in range 01 hex: out of range (over monitor value)
Read Safety Output Normal Flag	Read	Reads the normal flag status of the number (1...8) specified by the Instance ID.	0E hex	3B hex	01...08 hex	05 hex	—	1 byte 00 hex: error 01 hex: normal
Read Safety Output Error Information Cause	Read	Reads the cause for the normal flag of the number (1...8) specified by the Instance ID being off (error).	0E hex	3B hex	01...08 hex	6E hex	—	1 byte 00 hex: no error 01 hex: invalid configuration 02 hex: overcurrent detection 03 hex: short-circuit detection 04 hex: high constant error 05 hex: error in either of dual channels 06 hex: internal relay circuit error 07 hex: relay error 08 hex: data error between dual channel outputs 09 hex: detection of short-circuit between wires
Read AND of Safety Output Normal Flags	Read	Reads the cause for the normal flag of the number (1...8) specified by the Instance ID being off (error).	0E hex	3C hex	01 hex	05 hex	—	1 byte 00 hex: error 01 hex: all normal
Read OR of Monitor Status of Output Total On Times or Contact Operation Counters	Read	Reads the logical OR of the monitor status of the total on time or contact operation counter for all outputs 1...8.	0E hex	3C hex	01 hex	72 hex	—	1 byte 00 hex: all in range 01 hex: input out of range (over monitor value)

Table 44 - Monitoring Test Output Terminals

Explicit Message	Service	Function	Command					Response
			Service Code	Class ID	Instance ID	Attribute ID	Data Size	
Monitor Mode for Terminal Maintenance Information	Read	Reads the monitor mode of maintenance information for the test output (1...4) specified by the Instance ID.	0E hex	35B hex	01...04 hex	83 hex	—	1 byte 00 hex: Total On Time mode 01 hex: Contact Operation Counter mode
	Write	Writes the monitor mode of maintenance information for the test output (1...4) specified by the Instance ID.	10 hex	35B hex	01...04 hex	83 hex	1 byte 00 hex: Total On Time mode 01 hex: Contact Operation Counter mode	—

Table 44 - Monitoring Test Output Terminals

Explicit Message	Service	Function	Command					Response
			Service Code	Class ID	Instance ID	Attribute ID	Data Size	
SV for Test Output Total On Time or Contact Operation Counter	Read	Reads the SV of the total on time or contact operation counter for the input (1...4) specified by the Instance ID.	0E hex	35B hex	01...04 hex	86 hex	—	4 bytes 0000 0000 to FFFF FFFF hex (0 to 4,294,967,295)
	Write	Writes the SV of the total on time or contact operation counter for the input (1...4) specified by the Instance ID.	10 hex	35B hex	01...04 hex	86 hex	4 bytes 0000 0000... FFFF FFFF hex (0... 4,294,967,295)	—
Read Test Output Total On Time or Contact Operation Counter	Read	Reads the total on time or contact operation counter for the input (1...4) specified by the Instance ID.	0E hex	35B hex	01...04 hex	84 hex	—	4 bytes 0000 0000... FFFF FFFF hex (0... 4,294,967,295)
Reset Test Output Total On Time or Contact Operation Counter	Reset	Resets to 0 the total on time or contact operation counter for the test output (1...4) specified by the Instance ID.	05 hex	35B hex	01...04 hex	84 hex	—	—
Read Monitor Status of Test Output Total on Time or Contact Operation Counter	Read	Reads the monitor status of the total on time or contact operation counter for the test output (1...4) specified by the Instance ID.	0E hex	35B hex	01...04 hex	85 hex	—	1 byte 00 hex: in range 01 hex: out of range (over monitor value)
Read Test Output Safety Flag	Read	Reads the normal flag status for the test output (1...4) specified by the Instance ID.	0E hex	35B hex	01...04 hex	68 hex	—	1 byte 00 hex: normal 01 hex: error
Read Test Output Error Information Cause	Read	Reads the cause for the normal flag of the test output (1...4) specified by the Instance ID being off (error).	0E hex	35B hex	01...04 hex	76 hex	—	1 byte 00 hex: no error 01 hex: invalid configuration 02 hex: overcurrent detection 05 hex: high constant error 06 hex: undercurrent detection
Read OR of Test Output Safety Flags	Read	Reads the logical OR of the normal flag for all test outputs (1...4).	0E hex	35C hex	01 hex	69 hex	—	1 byte 00 hex: all normal 01 hex: error
Read OR of Monitor Status of Test Output Total On Times or Contact Operation Counters	Read	Reads the logical OR of the monitor status of the total on time or contact operation counter for all test outputs (1...4).	0E hex	35C hex	01 hex	72 hex	—	1 byte 00 hex: all in range 01 hex: test output out of range (over monitor value)

Notes:

Application and Configuration Examples

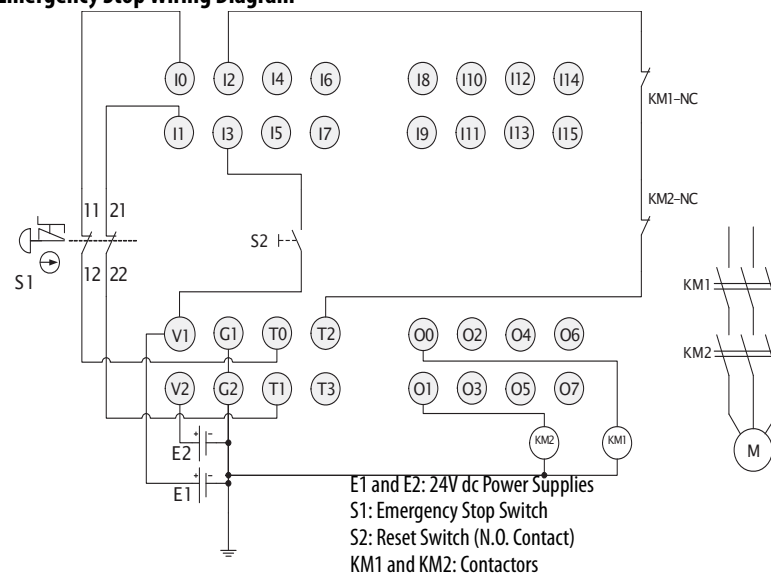
Introduction

Topic	Page
Emergency Stop Application	271
Safety Gate Application with Automatic Reset	273
Dual Zone Safety Gate Application Using Emergency Stop Switch with Manual Reset	274
Safety Mat Application	276
Light Curtain Application	279

Emergency Stop Application

This example shows a dual channel emergency stop switch with manual reset.

Figure 91 - Emergency Stop Wiring Diagram



Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 92 - Configuration

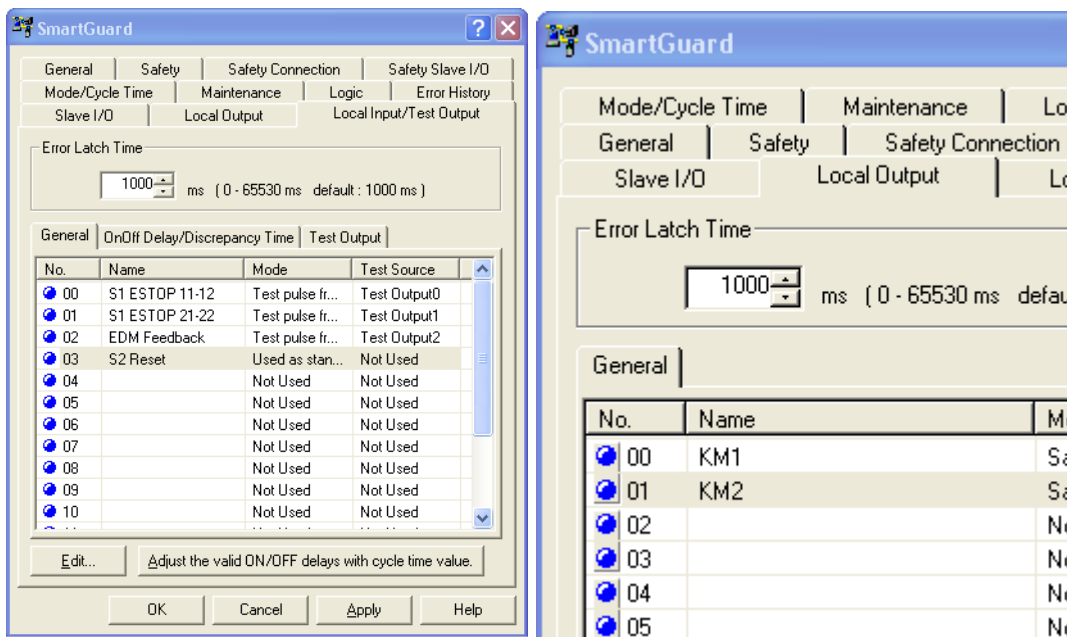


Figure 93 - Programming

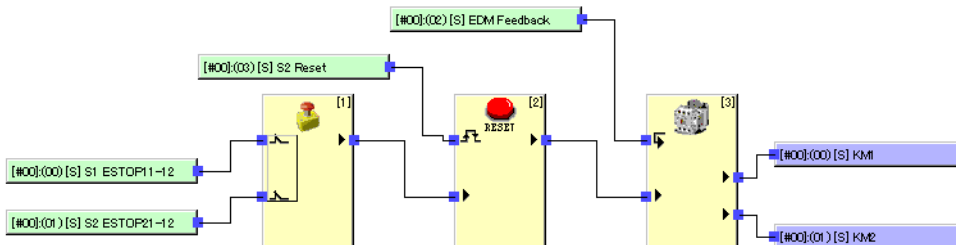
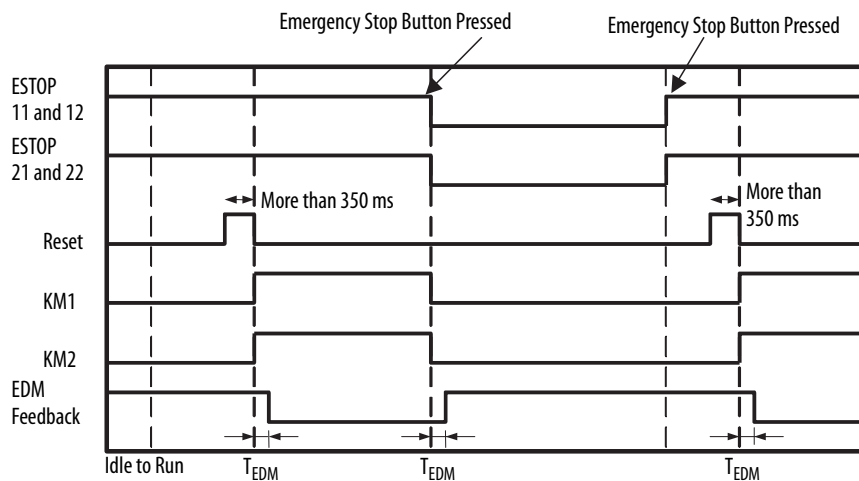


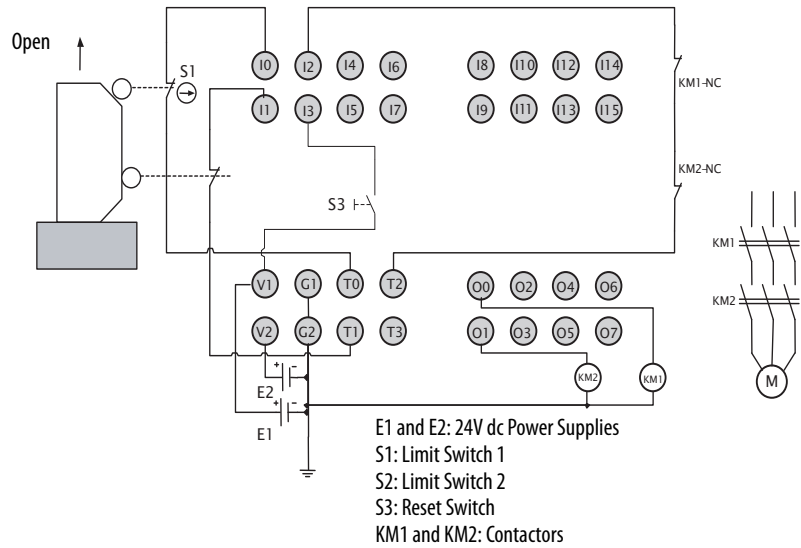
Figure 94 - Timing Diagram



Safety Gate Application with Automatic Reset

This example shows dual channel mode limit switches with automatic reset.

Figure 95 - Wiring Diagram



Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 96 - Configuration

SmartGuard Configuration - Left Screenshot

No.	Name	Mode	Test Source
00	S1 Limit Switch	Test pulse fr...	Test Output0
01	S2 Limit Switch	Test pulse fr...	Test Output1
02	EDM Feedback	Test pulse fr...	Test Output2
03	Reset	Used as stan...	Not Used
04		Not Used	Not Used
05		Not Used	Not Used
06		Not Used	Not Used
07		Not Used	Not Used
08		Not Used	Not Used
09		Not Used	Not Used
10		Not Used	Not Used

SmartGuard Configuration - Right Screenshot

No.	Name	Mode
00	KM1	Safety Pulse Test
01	KM2	Safety Pulse Test
02		Not Used
03		Not Used
04		Not Used
05		Not Used
06		Not Used
07		Not Used

Figure 97 - Programming

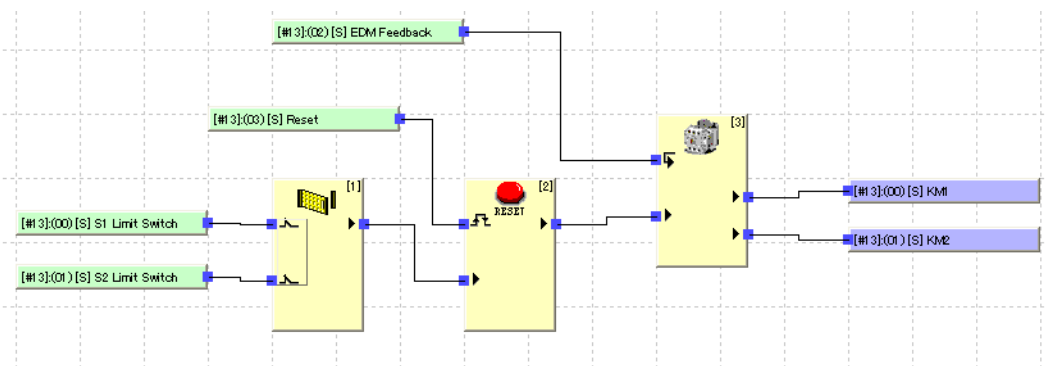
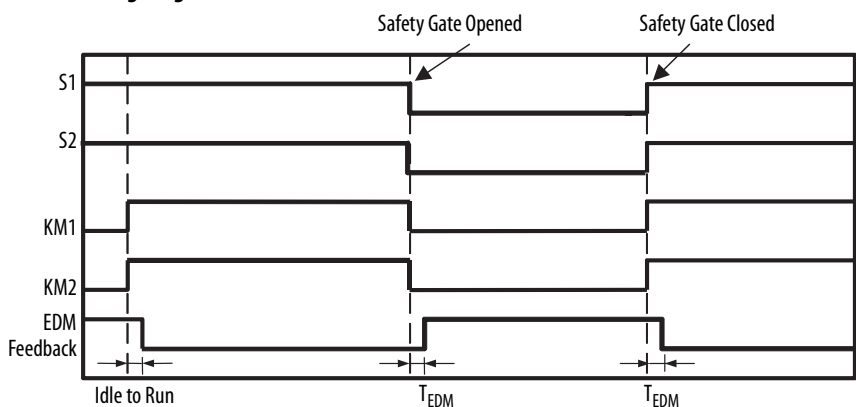


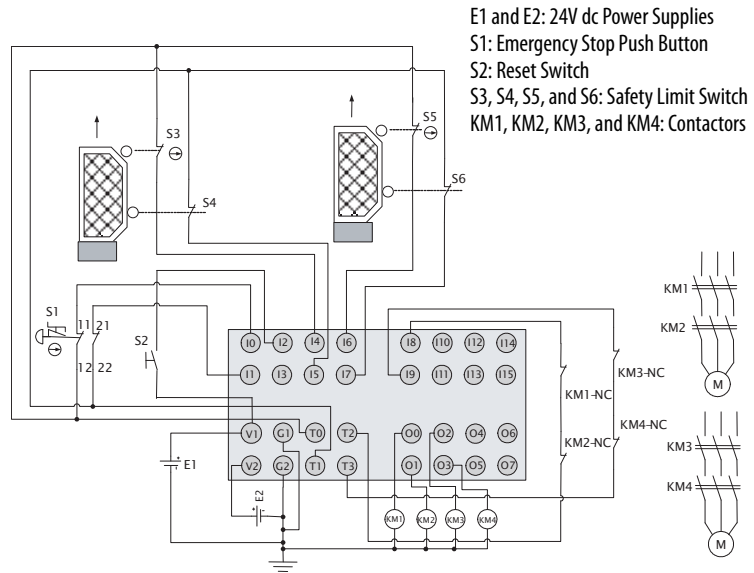
Figure 98 - Timing Diagram



Dual Zone Safety Gate Application Using Emergency Stop Switch with Manual Reset

This example shows dual channel door switches with automatic reset and a dual channel emergency stop switch with manual reset. Each pair of door switches controls a separate zone, so part of the machine can keep running if that part's door is closed. An E-stop will stop both zones.

Figure 99 - Wiring Diagram



Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 100 - Configuration

1752-L24BBB Configuration - Error Latch Time

Mode/Cycle Time | Maintenance | Logic | Error History
 General | Safety | Safety Connection | Safety Slave I/O
 Slave I/O | Local Output | Local Input/Test Output

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

No.	Name	Mode	Test Source
00	ESTOP1-1	Test pulse from test out	Test Output0
01	ESTOP1-2	Test pulse from test out	Test Output1
02	ResetSW	Test pulse from test out	Not Used
03		Used as standard i...	Not Used
04[e]	DoorSW1-1	Test pulse from test out	Test Output0
05[e]	DoorSW1-2	Test pulse from test out	Test Output1
06[e]	DoorSW2-1	Test pulse from test out	Test Output0
07[e]	DoorSW2-2	Test pulse from test out	Test Output1
08	FeedbackKM12	Test pulse from test out	Test Output2
09	FeedbackKM34	Test pulse from test out	Test Output3

1752-L24BBB Configuration - General

Mode/Cycle Time | Maintenance | Logic | Error History
 General | Safety | Safety Connection | Safety Slave I/O
 Slave I/O | Local Output | Local Input/Test Output

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

No.	Name	Mode
00	KM1	Safety Pulse Test
01	KM2	Safety Pulse Test
02	KM3	Safety Pulse Test
03	KM4	Safety Pulse Test
04		Not Used
05		Not Used
06		Not Used
07		Not Used

Figure 101 - Programming

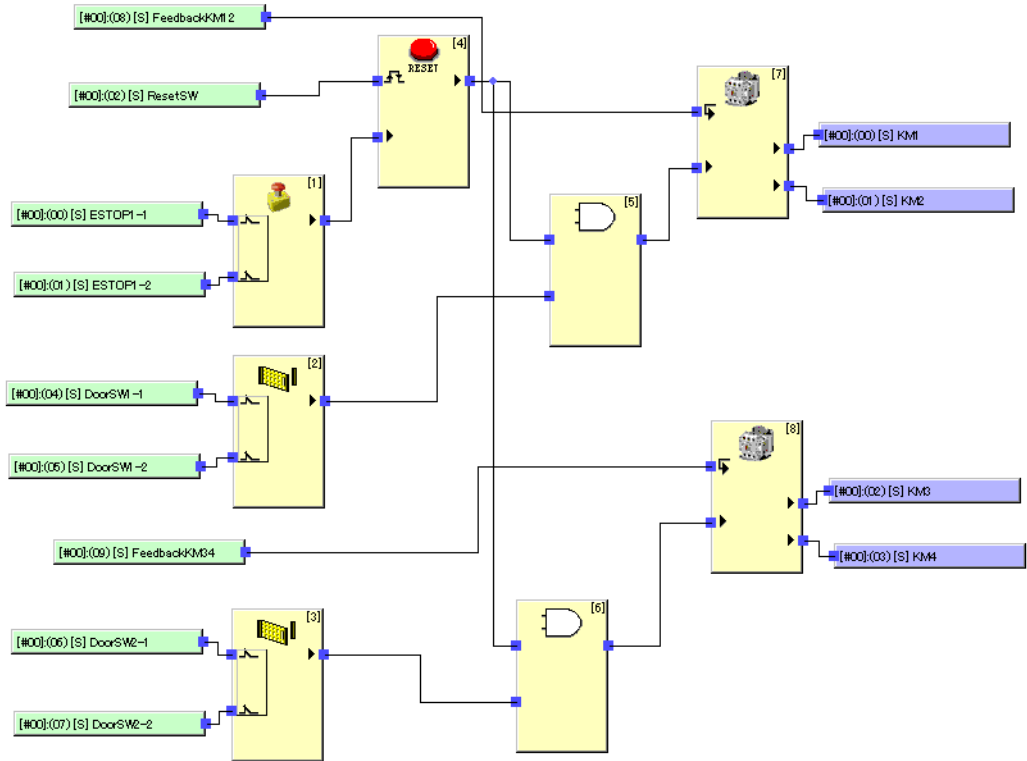
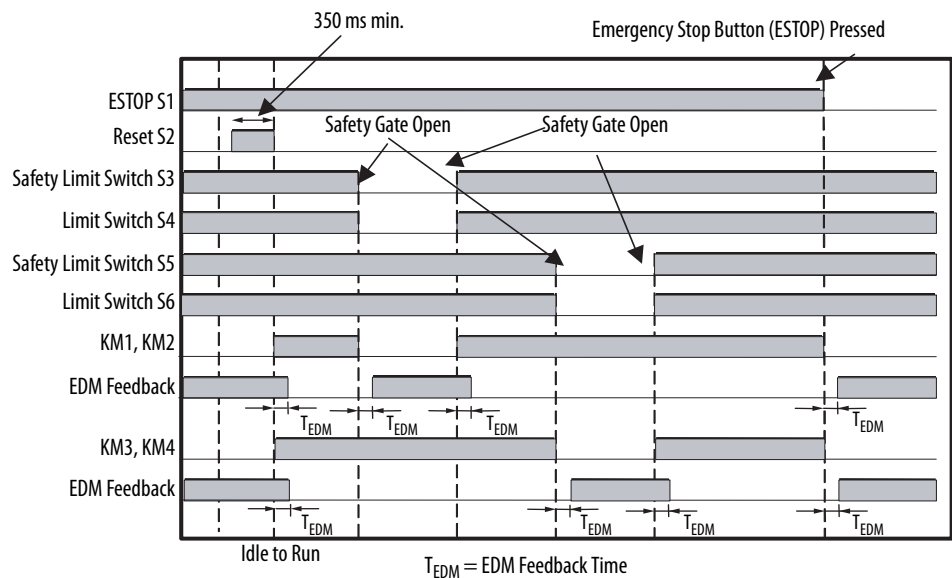


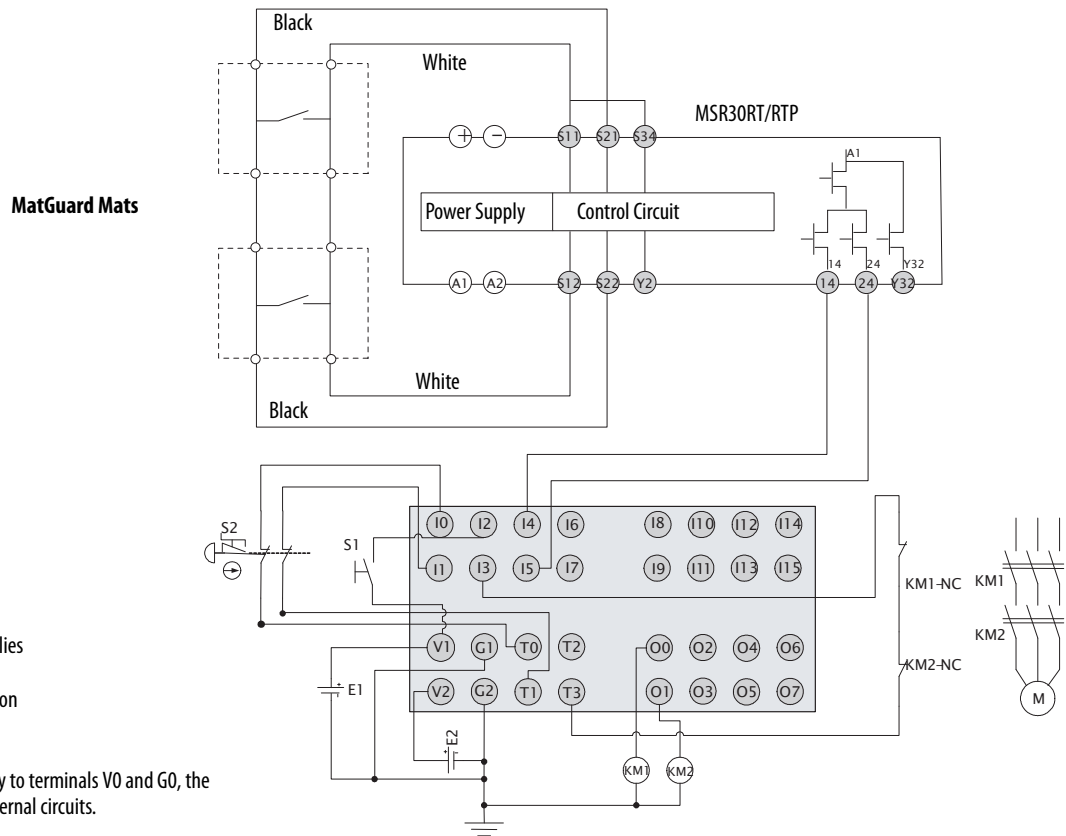
Figure 102 - Timing Diagram



Safety Mat Application

This example shows a dual channel safety mat with manual reset and a dual channel emergency stop switch with manual reset. This application uses a MSR30RT/RTP relay, which has its own pulsed outputs and inputs, so a test output from the SmartGuard controller is not used.

Figure 103 - Wiring Diagram



E1 and E2: 24V dc Power Supplies
 S1: Reset Switch
 S2: Emergency Stop Push Button
 KM1 and KM2: Contactors

Connect a 24V dc power supply to terminals V0 and G0, the power supply terminals for internal circuits.

Figure 104 - Configuration

The figure shows two screenshots of the 1752-L248BB configuration software. Both screenshots show the 'General' tab with an 'Error Latch Time' set to 1000 ms. The left screenshot shows a table of safety inputs and outputs, and the right screenshot shows a table of safety outputs.

No.	Name	Mode	Test Source
00[e]	Estop1	Test pulse from test out	Test Output0
01[e]	Estop2	Test pulse from test out	Test Output1
02	Reset	Not Used	Not Used
03	EDM Feedba...	Test pulse from test out	Test Output3
04[e]	Mat1	Used as safety input	Not Used
05[e]	Mat2	Used as safety input	Not Used
06		Not Used	Not Used
07		Not Used	Not Used
08		Not Used	Not Used
09		Not Used	Not Used

No.	Name	Mode
00	KM1	Safety Pulse Test
01	KM2	Safety Pulse Test
02		Not Used
03		Not Used
04		Not Used
05		Not Used
06		Not Used
07		Not Used

Figure 105 - Programming

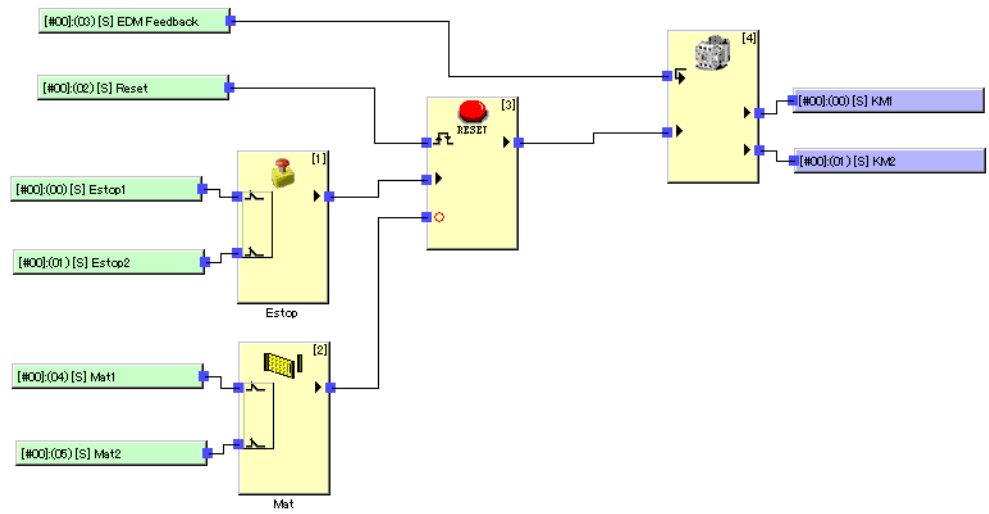


Figure 106 - Timing Diagram

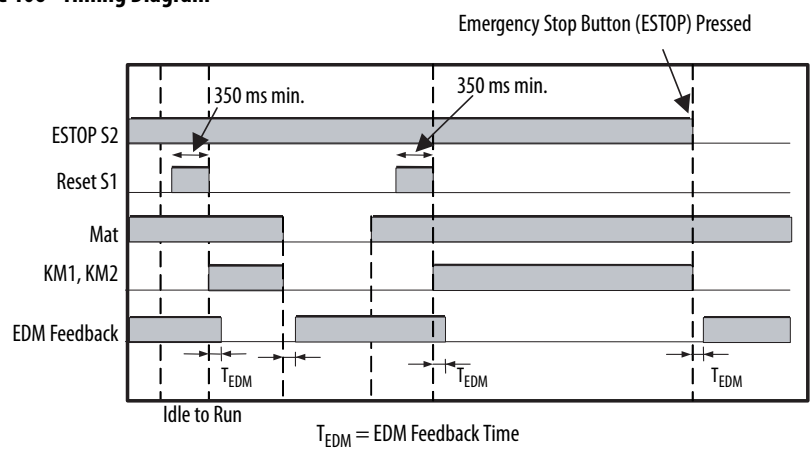


Figure 108 - Configuration

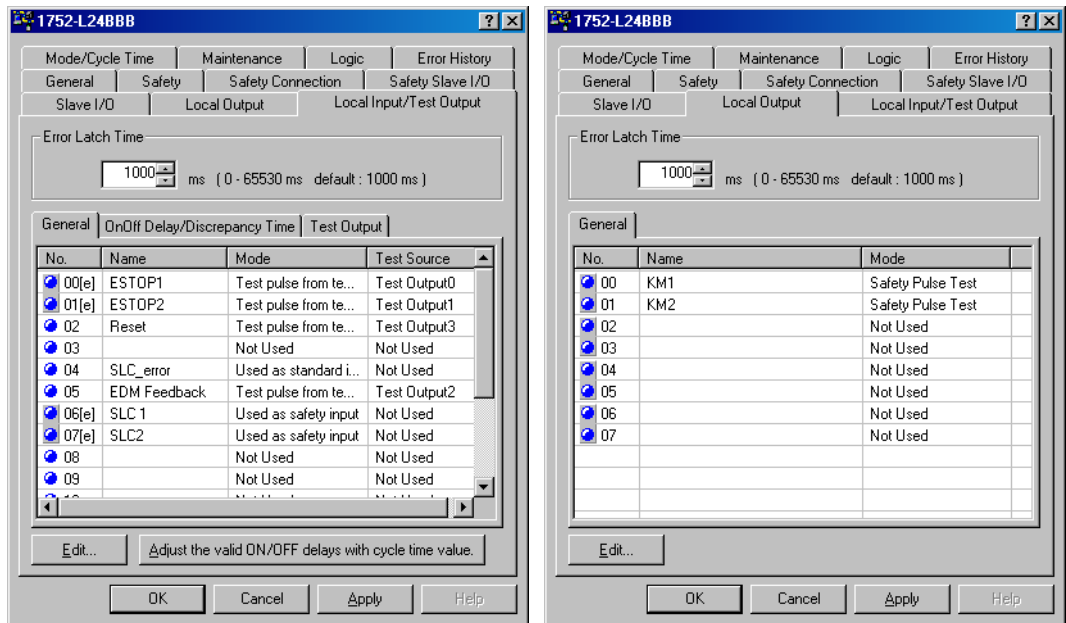


Figure 109 - Programming

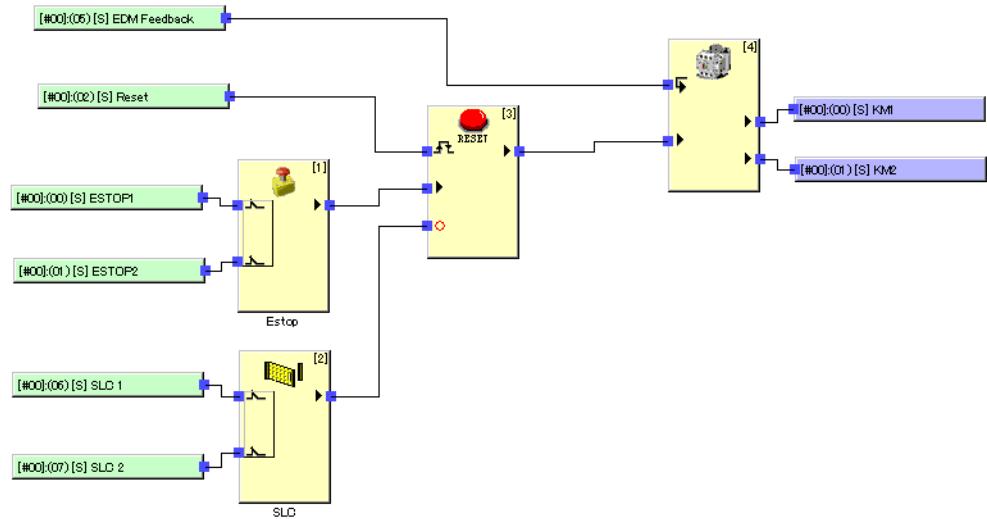
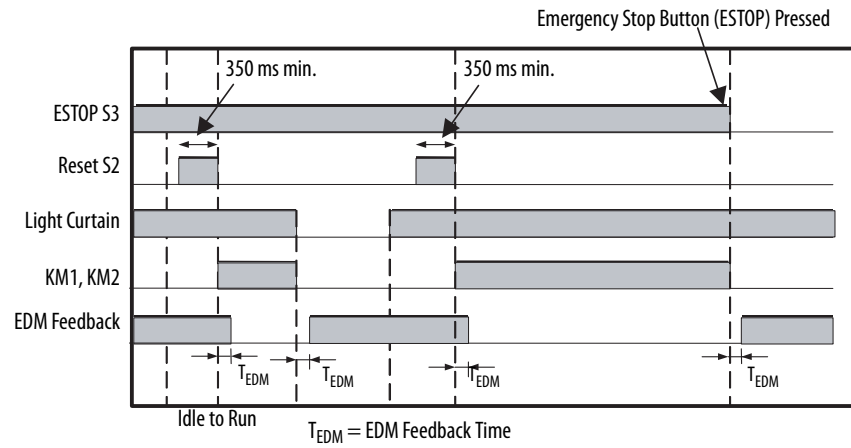


Figure 110 - Timing Diagram



Notes:

The following terms and abbreviations are used throughout this manual. For definitions of terms not listed here, refer to the Allen-Bradley Industrial Automation Glossary, publication [AG-7.1](#).

- 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 communication cable. An error is detected when the internal error counter exceeds a threshold value.
- change of state (COS)** A type of standard I/O communication in which the controller can send and receive data with slave devices whenever a data change occurs in the configured slave device or controller. Data is updated at the rate of the heartbeat.
- common industrial protocol (CIP)** A communication protocol designed for industrial automation applications.
- configuration signature** The combination of an ID number, date, and time that uniquely identifies a specific configuration for a device.
- cyclic** A type of standard I/O data communication in which the controller can send and receive data with slave devices that support the cyclic feature. Data is only sent at the user-specified rate.
- discrepancy time** The time period from a change in one or two inputs until the other input changes.
- Dual Channel** The use of two inputs or outputs as the input or output for redundancy.
- Dual Channel Complementary** A setting to evaluate whether two logic states are complementary.
- Dual Channel Equivalent** A setting to evaluate whether two logic states are equivalent.
- electronic data sheet (EDS)** A vendor-supplied template that RSNetWorx for DeviceNet software uses to display the configuration parameters, I/O data profile, and connection type support for a given DeviceNet or DeviceNet Safety module.
- error latch time** The time period to hold an error state (including the related control data, status data, and status indications).
- explicit messaging** A type of messaging used for lower priority tasks, such as configuration and status monitoring.
- node** Hardware that is assigned a single address on the network (also referred to as device or module).
- one out of two (1oo2)** Refers to the behavioral design of a multi-processor safety system.
- personal computer (PC)** Computer used to interface with a control system via programming software.

- polled** A type of standard I/O data communication in which a polled message solicits a response from a single, specified device on the network (a point-to-point transfer of data).
- probability of failure on demand (PFD)** The average probability of an operational system to fail to perform its design function on demand.
- probability of failure per hour (PFH)** The probability of an operational system to have a dangerous failure occur per hour.
- requested packet interval (RPI)** When communicating over a network, this is the expected rate in time for production of data.
- safety I/O** Safety I/O has most of the attributes of standard I/O except it features mechanisms certified to SIL 3 to verify data integrity and timeliness.
- safety network number (SNN)** Uniquely identifies a network across all networks in the safety system. The end user is responsible for assigning a unique number for each safety network or safety subnet within a system. The safety network number makes up part of the unique node identifier (UNID).
- standard** Any object, task, tag, program, or component in your project that is not a safety-related item.
- strobed** A type of standard I/O data communication in which a message solicits a response from each strobed device (a multi-cast transfer). It is a 64 bit message that contains 1 bit for each slave device on the network.
- Each slave node can return a maximum of 8 bytes in response to the master's strobe.
- system reaction time** The worst-case time from a safety-related event as input to the system or as a fault within the system, until the time that the system is in the safety state. System reaction time includes sensor and activator reaction times as well as the controller reaction time.
- test pulse** A signal used to detect when external wiring comes into contact with the power supply (positive), or to identify short-circuits between signal lines.

A

alphanumeric display
identify errors 199

B

baud rate
see communication rate

BOOTP
set the IP address 51
use the Rockwell Utility 52

bridge 56

C

CIP Safety I/O
configuration signature 44

communication rate
reset 46

configuration
DeviceNet Safety target nodes 44
reset 46
safety parameters 78
standard parameters 79
verify 161-167

configuration signature 44
comparison 166
components 45
definition 44
mismatch 162

configure a driver 41, 50

connection reaction time limit 81
and network delay multiplier 82
DeviceNet Safety I/O 81

D

device status
Safety Device Verification Wizard 161
verification 163

DeviceNet network
configure a driver 41, 50
connecting 41, 49

download DeviceNet configuration 159-160

driver types 42, 50

dual channel mode
inputs 67
outputs 73

E

error categories 179

error messages

communication 183
download errors 185
mode changes 188
power supply 184
reset errors 187
safety inputs 185
safety outputs 185
system failure 183
test outputs 185

EtherNet/IP module

bridging 56
configuration parameters 51

EtherNet/IP network

connect to a computer 49
parameters 51

examples

bridging 58
EtherNet/IP network to a DeviceNet network
57
EtherNet/IP network to a USB port 59
RSLinx bridging 57, 59

explicit message

receiving 261
restrictions 265
sending 264

F

function block 69

G

gateway 51

I

icon
device status 162

IP address
overview 51
use BOOTP to set 51
use RSLinx software to set 54

L

local
inputs 67-70
outputs 73-75

lock

See safety-lock

logic

functions 141

M**mismatch**

configuration signature 162
SNN 65

missing device
 icon 162
multicast connections 80
muting lamp
 status data 177

N

Network
 bridge 56
network delay multiplier 82
network status indicator
 flashing 196
node address 42
 changes 65
 reset 46
 select 25
node commissioning 42-43
 tool 42

O

off-delay 67
on-delay 67
online button 160
output connection owners
 reset 46
overcurrent detection
 outputs 73
 pulse test sources 71

P

parameters tab 79
password
 protected operations 47
 reset 46
 set or change 47
 valid characters 47
point-to-point 80
pulse test sources 71

R

ready to be safety locked 164
ready to be verified 163
related publications 13
requested packet interval
 and connection reaction time limit 81
 set 81
reset
 configuration owner 46
 safety attributes 46
 safety device 45, 65
Rockwell BOOTP utility 52
RPI
 See requested packet interval
RSLinux software
 bridging 57, 59
 configuring network parameters 54

RSLogix 5000 software
 software generic profile 130
RSNetWorx for DeviceNet software
 node commissioning 42

S

safety configuration tab 78
safety connections tab 80
Safety Device Verification Wizard 46
 definition 161
 device status 161
 reports 164
 run 161
 safety-lock
 select devices 163
 summary 167
 upload and compare 164
 Welcome page 161
safety network number 61
 assignment 62-63
 automatic 62
 automatic assignment 63
 copy 62
 error icon 162
 formats 61
 managing 61
 manual 62, 63
 manual assignment 63
 mismatch 65
 reset 46, 65
 time-based 62
safety reset 45
safety-lock
 devices
 during reset 46
 icon 162
scanner
 reset 65
specifications
 general 189
Status
 indicators 195
status data 175
 general 176
 local input 176
 local output 177
 muting lamp 177
 test output 177
subnet mask 51

T

test pulse sources
 with inputs 67
 with outputs 73
timeout multiplier 82

U

unique node identifier 61

unknown device

icon 162

upload and compare

Safety Device Verification Wizard 164

V**verification reports**

failure report 165

Safety Device Verification Wizard 165

verify

DeviceNet Safety configuration 161-167

FAILED 164

select devices 163

verify failed 163**verify not supported** 163**W****welcome page** 161

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products.

At <http://www.rockwellautomation.com/support> you can find technical and application notes, sample code, and links to software service packs. You can also visit our Support Center at <https://rockwellautomation.custhelp.com/> for software updates, support chats and forums, technical information, FAQs, and to sign up for product notification updates.

In addition, we offer multiple support programs for installation, configuration, and troubleshooting. For more information, contact your local distributor or Rockwell Automation representative, or visit <http://www.rockwellautomation.com/services/online-phone>.

Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/rockwellautomation/support/overview.page , or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to help ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication [RA-DU002](#), available at <http://www.rockwellautomation.com/literature/>.

Rockwell Automation maintains current product environmental information on its website at <http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page>.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1752-UM001E-EN-P - June 2014

Supersedes Publication 1752-UM001D-EN-P - April 2009

Copyright © 2014 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.