Allen-Bradley

DeviceNet Safety Scanner for GuardPLC™ Controllers

Catalog Number 1753-DNSI

User Manual

Rockwell Automation

Important User Information

Solid state equipment has operational characteristics differing from those of electromechanical equipment. *Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls* (Publication SGI-1.1 available from your local Rockwell Automation sales office or online at http://www.ab.com/manuals/gi) describes some important differences between solid state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

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.

IMPORTANT

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

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
- recognize the consequence

SHOCK HAZARD

Labels may be located on or inside the equipment (e.g., drive or motor) to alert people that dangerous voltage may be present.

BURN HAZARD

Labels may be located on or inside the equipment (e.g., drive or motor) to alert people that surfaces may be at dangerous temperatures.

Preface

Who Short Use this Manual P-1
Purpose of This Manual. P-1
Related Documentation P-2
Common Techniques Used in This Manual. P-2
Understanding Terminology P-3

Chapter 1

Before You Begin

Safety Concept 1-1
DeviceNet Safety Scanner Communications 1-2
How the 1753-DNSI Communicates 1-2
Understand Data Signals. 1-3
How Data Tables Work 1-4
How to Distinguish Between Standard Data and Safety Data in RSLogix Guard PLUS! 1-4
Role of RSNetWorx for DeviceNet and RSLogix Guard PLUS! 1-5
DeviceNet Safety Scanner Features. 1-6
Hardware Overview. 1-6
Supported Connections 1-7
Physical Layout of the DeviceNet Safety System 1-8
DeviceNet Safety I/O Performance Factors 1-8
Choose a Communication Rate for the Network 1-9
Assign an Address to Each Device 1-10

Chapter 2

Install the 1753-DNSI

General Safety Information 2-1
Preventing Electrostatic Discharge 2-2
Mount the Scanner 2-2
DIN Rail Mounting. 2-3
Panel Mounting 2-4
Ground the Scanner 2-4
Connect Power Source 2-5
Make Communication Connections 2-5
DeviceNet Connections 2-6
High-speed Safety Protocol (HSP) Connections 2-7

Chapter 3

Set Up Your DeviceNet Network

Connect a Computer to the DeviceNet Network 3-1
Configure a Driver for the Network 3-1
Make Sure the Driver Works. 3-2
Commission All Nodes 3-2
Browse the Network 3-3
Safety Reset (Optional) 3-4
Set Passwords (Optional). 3-5
Set or Change a Password 3-5

To set a password for a module: 3-5
Forgotten Passwords 3-6

Chapter 4

Manage the Safety Network Number

SNN Formats. 4-1
Time-based SNN (Recommended) 4-1
Manual SNN 4-2
Assignment of the SNN 4-2
Automatic (Time-based). 4-2
Manual 4-3
Set the SNN in All Safety Nodes. 4-3
SNN Mismatch 4-5
Safety Network Number Mismatch Dialog 4-5
SNN and Node Address Changes 4-6

Chapter 5

Configure DeviceNet Nodes and Connections

Configuration Signature. 5-1
Configure DeviceNet Safety I/O Target Nodes 5-2
1791DS DeviceNet Safety I/O Module Parameters 5-2
Configure the DeviceNet Safety Scanner’s Safety Connections 5-3
Configure DeviceNet Standard Slave I/O Nodes 5-6
Configure the DeviceNet Safety Scanner’s Standard Connections 5-6
Standard Communication Properties 5-6
Create a Scanlist. 5-8
Configure Standard Inputs 5-10
Configure Standard Outputs 5-11
Configure GuardPLC Controller Settings. 5-12

Chapter 6

Create a GuardPLC Project with High-Speed Safety Protocol

Create or Open a GuardPLC Project 6-1
Add High-Speed Safety Protocol to the GuardPLC Controller Resource. 6-3
Review the GuardPLC Controller’s Communication Settings 6-5

Chapter 7

Associate the Scanner and Controller and Download the DeviceNet Network Configuration

Scanner Signals File. 7-1
Target Connections File. 7-2
Automatically Update Signals. 7-2
Manually Associate the Scanner and Controller. 7-4
Download the DeviceNet Network Configuration 7-5

Chapter 8

Develop Your GuardPLC Application

Define Signals for Your GuardPLC Application 8-1
Define Signals for Safety Data. 8-1
Configure HSP Connection. 8-3
Create Application Program Logic 8-4
Save and Compile Application Logic 8-4
Download the Project to the Controller 8-4
Place the Controller in Stop Mode (if necessary) 8-4
Download the Project 8-4

Chapter 9

Verify Your DeviceNet Safety Configuration

Start the Safety Device Verification Wizard. 9-1
Determine if Devices Can Be Verified 9-1
Select Devices to Verify. 9-3
Review the Safety Device Verification Reports 9-5
Lock Safety Devices 9-6
View the Safety Device Verification Wizard Summary 9-7

Chapter 10

Monitor Status

LED Status Indicators. 10-1
Alphanumeric Display. 10-2
At Power Up 10-2
During Operation 10-2
Connection Status 10-9
DeviceNet Connection Status Bit Behavior 10-9
DeviceNet Safety Connection Status 10-10
Standard DeviceNet Connection Status 10-11
DeviceNet Interface Status 10-12

Appendix A

Specifications

General A-1
Environmental A-1
Electrical/EMC A-2
Certifications. A-3

Appendix B

Configure Peer-to-Peer DeviceNet Communications

Plan Your Peer-to-Peer Communications B-2
Commission a Peer Scanner. B-2
Add a Peer Controller B-3
Define Target Connections for Standard and Safety Data. . . B-4
Create Required Signals B-5
Define Standard Target Connections. B-6
Define Safety Connections B-7
Configure Peer-to-Peer Connections. B-8

Associate the Peer Safety Scanner and GuardPLC Controller B-8
Add the Peer Scanner to the Scanlist. B-9
Configure Safety Connections. B-10

Appendix C

DeviceNet Class Codes

DeviceNet Object C-1
Identity Object C-1
Safety Supervisor Object C-1

Appendix D

Calculate Safety Connection Bandwidth

Single-cast Inputs D-1
1 to 2 Bytes D-1
3 to 250 Bytes D-1
Single-cast Outputs D-2
1 to 2 Bytes D-2
3 to 250 Bytes D-2
Multicast Connections D-2
1 to 2 Bytes D-2
3 to 250 Bytes D-3

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
- related documentation
- common techniques used in this manual
- terminology used in this manual

Who Should Use this Manual

Use this manual if you are responsible for designing, installing, programming, or troubleshooting a safety control system that includes a GuardPLC controller communicating on a DeviceNet Safety network through a 1753-DNSI module.

We assume that you:

- have a basic understanding of electrical circuitry
- are trained and experienced in the creation, operation, and maintenance of safety systems.
- know each of your device's I/O parameters and requirements.

Purpose of This Manual

This manual only briefly describes the safety concept of the DeviceNet Safety Scanner for GuardPLC Controllers. Its purpose is to provide information on installing, operating, and maintaining your 1753-DNSI in a GuardPLC controller system.

For detailed information on safety system requirements regarding the DeviceNet Safety Scanner for GuardPLC Controllers, refer to the GuardPLC Controller Systems Safety Reference Manual, publication number 1753-RM002.

Related Documentation

The table below provides a listing of publications that contain important information about GuardPLC Controller systems.

For	Read this document	Publication
Information on installing, programming, operating, and troubleshooting a GuardPLC Controller	GuardPLC Controller User Manual	1753-UM001
Detailed requirements for achieving and maintaining SIL 3 applications with the GuardPLC Controller System	GuardPLC Controller Systems Safety Reference Manual	1753-RM002
Information on installing the DeviceNet Safety Scanner for GuardPLC Controllers	DeviceNet Safety Scanner for GuardPLC Installation Instructions	1753-IN009
Information on installing DeviceNet Safety I/O Modules	DeviceNet Safety I/O Installation Instructions	1791DS-IN001
Information on configuration and programming for DeviceNet Safety I/O Modules	DeviceNet Safety I/O User Manual	1791DS-UM001

If you would like a manual, you can:

- download a free electronic version from the internet at www.rockwellautomation.com/literature.
- purchase a printed manual by contacting your local Allen-Bradley distributor or Rockwell Automation sales office.

Common Techniques Used in This Manual

The following 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.

Understanding Terminology

The following table defines acronyms used in this manual.

Acronym:	Full Term:	Definition:
1oo2	One Out of Two	A safety architecture consisting of two channels connected in parallel, such that either channel can perform the safety function.
CAN	Controller Area Network	The networking standard that defines the physical layer of DeviceNet.
COS	Change of State	A type of I/O data communication in which the interface module can send and receive data with slave devices whenever a data change occurs in the configured slave device.
EDS	Electronic Data Sheet	A vendor-supplied template that specifies how device configuration information is displayed as well as what is an appropriate entry (value).
EPR	Expected Packet Rate	The rate at which packets are expected to be received by a device.
HSP	High-Speed Safety Protocol	A high-speed, high-integrity protocol designed to transfer both safety and standard data between the GuardPLC controller and the DeviceNet Safety Scanner for GuardPLC Controllers.
MAC ID	Media Access Identifier	The network address of a DeviceNet node.
MTBF	Mean Time Between Failures	Average time between failure occurrences.
MTTR	Mean Time to Restoration	Average time needed to restore normal operation after a failure has occurred.
PC	Personal Computer	Computer used to interface with, and control, a controller-based system via programming software.
PFD	Probability of Failure on Demand	The average probability of a system to fail to perform its design function on demand.
PFH	Probability of Failure per Hour	The probability of a system to have a dangerous failure occur per hour.
Rx	Receive	—
SNN	Safety Network Number	A unique number that identifies a safety network, or safety sub-net, across all networks in the safety system.
Tx	Transmit	—

Before You Begin

This chapter provides an overview of communication between the 1753-DNSI and the GuardPLC controller. Before configuring your 1753-DNSI module, you must understand:

- the safety concept of the system
- the data exchange between the GuardPLC controller and DeviceNet devices through the 1753-DNSI module
- the roles of RSNetWorx for DeviceNet and RSLogix Guard PLUS! software in the safety system
- the features of the DeviceNet Safety Scanner
- the physical layout of your network

Safety Concept

The DeviceNet Safety Scanner for GuardPLC Controllers is certified for use in GuardPLC safety applications up to and including Safety Integrity Level (SIL) 3, according to IEC 61508, and Category (CAT) 4, according to EN 954-1, in which the de-energized state is the safety state.

IMPORTANT For SIL 3 and CAT 4 safety system requirements, including proof test intervals, system reaction time, and PFD/PFH calculations, refer to the GuardPLC Controller Systems Safety Reference Manual, publication number 1753-RM002. You must read, understand, and fulfill these requirements prior to operating a GuardPLC controller-based SIL 3 or CAT 4 safety system.

The DeviceNet Safety Scanner and the GuardPLC system use the following mechanisms to support the integrity of the data they exchange:

- **Safety Network Number** – A unique number that identifies the Safety Network. Each DeviceNet sub-network that contains safety nodes must have one unique Safety Network Number.
- **Configuration Signature** – The combination of an ID number, date, and time that uniquely identifies a specific configuration for a safety device.

- **HSP (High-speed Safety Protocol) Signature** – This is a read-only value that represents the data exchanged between the GuardPLC controller and the safety scanner. The HSP Signature is calculated based on the Scanner Configuration Signature and changes only when the data exchanged by the controller and the safety scanner changes. The HSP Signature is sent to the controller configuration software and helps ensure the integrity of the data.
- **Controller ID (SRS)** – A unique identifier for every GuardPLC controller and GuardPLC Ethernet Distributed I/O module in a system, the Controller ID must be a unique number from 1 to 65,535. The default is 60000.
- **Safety-Lock** – The safety scanner and DeviceNet safety I/O modules must be Safety-Locked to prevent their configurations from being unintentionally modified. Safety-Lock all DeviceNet Safety devices by running the Safety Device Verification Wizard in RSNetWorx for DeviceNet before placing the safety application into service.
- **Password protection** – The configuration of the safety scanner can be protected by the use of an optional password. If you set a password in a safety device, the download, Safety-Reset, Safety-Lock and Safety-Unlock operations will require a password.

DeviceNet Safety Scanner Communications

The 1753-DNSI provides DeviceNet access for GuardPLC 1600 and GuardPLC 1800 controllers. These GuardPLC controllers support communications via High-Speed Safety Protocol (HSP). The 1753-DNSI reads and writes data from DeviceNet nodes and exchanges this aggregate data with the GuardPLC controller via HSP.

The 1753-DNSI scanner communicates with DeviceNet devices over the network to:

- read inputs from a device
- write outputs to a device
- monitor device status

How the 1753-DNSI Communicates

For **standard data**, the safety scanner communicates with a device via strobe, poll, change of state, and/or cyclic messages. It uses these messages to solicit data from or deliver data to each device in its scanlist.

For **safety data,** the scanner communicates with safety devices via cyclic messages only. You configure input and output connections in the DeviceNet safety scanner to transfer input and output data to and from DeviceNet safety I/O modules and the GuardPLC controller.

The scanner can make data available to other DeviceNet scanners using Target connections. When Target connections are enabled, the safety scanner looks like a standard I/O device that can be added to another scanner's scanlist,or a safety target device allowing another safety scanner to connect to the safety data by adding a safety connection. This allows for the transfer of data signals between two GuardPLC controllers for safety interlocking and distributed safety control. Standard data signals can also be exchanged with PLCs, HMIs, or a ControlLogix system with a 1756-DNB scanner on the DeviceNet network. For more information on Target connections, see Appendix B.

Understand Data Signals

In order to understand how to use data signals from the safety scanner in your GuardPLC application logic, you must know:

- whether the signal data is regarded as safety or standard data in the end device, and
- whether the signal data was transferred over a safety connection or a standard connection.

The following table defines permitted uses of safety and standard signals based on connection and signal type.

End Device Signal Definition	Connection Type	Permitted Use in Application
Safety	Safety	Safety
	Standard	Standard
Standard	Safety	Standard
	Standard	Standard

IMPORTANT Only safety signal data transmitted over safety connections may be used as safety data in safety application logic.

How Data Tables Work

To exchange data, the GuardPLC controller and the 1753-DNSI use two pairs of data tables: one pair for safety input and output data and one pair for standard input and output data.

Connection Type		Scanner Inputs	Scanner Outputs
Safety	Scanner is the originator.	Data the scanner reads from its target nodes. The data layout is defined by the target node's configuration.	Data the scanner writes to its target nodes. The data layout is defined by the target node's configuration.
	Scanner is the target.	Data that one other CIP Safety originator may write on the scanner's target output connection point. The data signals to be written are selected in RSLogix Guard PLUS!.	Data that one or more other CIP Safety originators may read from the scanner's target input connection point. The data signals to be read are selected in RSLogix Guard PLUS!.
Standard	Scanner is the master.	Data the scanner reads from its standard DeviceNet slaves. The data layout is defined by the target node's configuration.	Data the scanner writes to its standard DeviceNet slaves. The data layout is defined by the target node's configuration.
	Scanner is the slave.	Data that one other standard DeviceNet master can write on the scanner's slave mode outputs. The data signals are selected in RSLogix Guard PLUS!.	Data that one or more other standard DeviceNet master can read from the scanner's slave mode inputs. The data signals are selected in RSLogix Guard PLUS!.

Standard DeviceNet Explicit Messaging connections are limited to read-only access to safety data.

ATTENTION

To maintain the safety integrity level (SIL) of your system, you must ensure that safety data read by Explicit Messaging is used only as standard data in your application.

How to Distinguish Between Standard Data and Safety Data in RSLogix Guard PLUS!

In the HSP Signal Connection dialogs (in RSLogix Guard PLUS!), signals that are transferred over safety connections are shown in white text on a red background. Signals transferred over a standard connection are shown in blue text on a gray background.

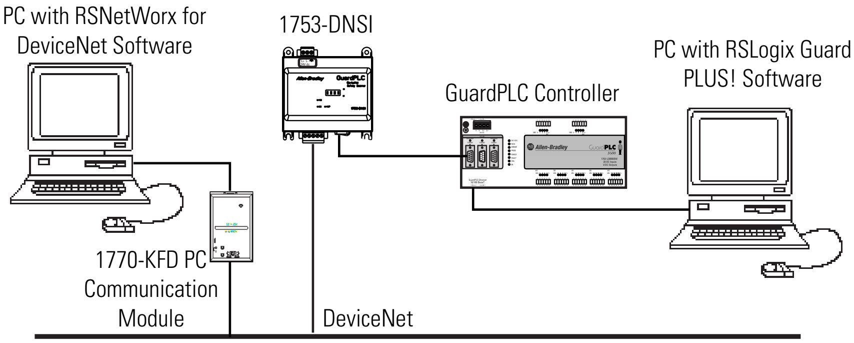
Since this colorization only applies to the Connect Signals dialogs available from the HSP protocol context menu, we strongly recommend that when using both standard and safety signals in your application, you use a naming convention to visually distinguish between standard and safety signals throughout the RSLogix Guard PLUS! programming environment. For example, use a prefix of 'std_' for any signals that are standard and a prefix of 'safe_' for any signals that are safety-related.

IMPORTANT

The red/blue colorization is not a guarantee that a signal is a safety signal. It only indicates which type of connection the signal was transferred over. The classification of the end node must also be considered. Any signal that appears in the (blue) standard Connect Signals window and is regarded as safety at the end device must be treated as standard in your application. Any signal that appears in the (red) safety Connect Signals window and is regarded as standard at the end device must be treated as standard in your application. In order for a signal to be regarded as a safety value in your application, the end device configuration must treat it as safety and it must be transferred over a DeviceNet Safety connection.

Role of RSNetWorx for DeviceNet and RSLogix Guard PLUS!

RSNetWorx for DeviceNet, version 6.x or higher, is the configuration tool for the 1753-DNSI on the DeviceNet Safety network. RSNetWorx for DeviceNet can connect to the safety scanner directly over the DeviceNet network via an RS-232 interface (1770-KFD module) or PC card (1784-PCD or -PCID) or through another network using a bridge device. A bridge can be either a single device with communication ports for two different networks, or separate communication devices in the same chassis.


PC with RSNetWorx for DeviceNet Software
1753-DNSI
GuardPLC Controller
PC with RSLogix Guard PLUS! Software
1770-KFD PC Communication Module
DeviceNet

RSNetWorx for DeviceNet exchanges signal information with RSLogix Guard PLUS!, the configuration and programming tool for the GuardPLC controller. The Scanner Signals and Target Connections

Files enable RSNetWorx for DeviceNet and RSLogix Guard PLUS! to share the same view of the individual signals available on all of the DeviceNet connections present in a specific DeviceNet Safety Scanner configuration.

TIP

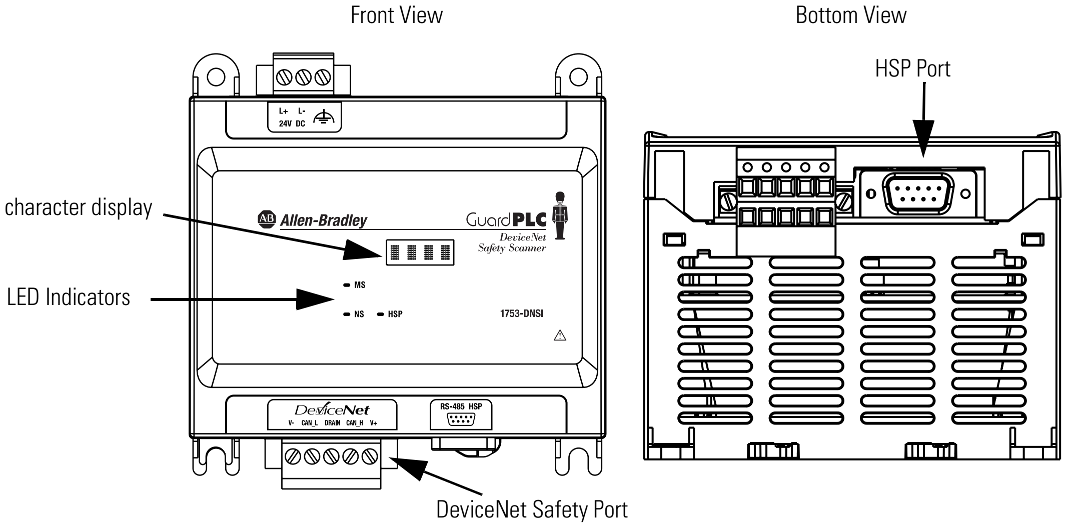
If you install RSLogix Guard PLUS! and RSNetWorx for DeviceNet on the same PC, you can take advantage of the ‘Automatically Update Signals’ feature. Otherwise, you must manually import and export the Scanner Signals and Target Connections files. See Chapter 7, Associate the Scanner and Controller and Download the DeviceNet Network Configuration, for more information.

The following table lists the software and revision level required to operate with the 1753-DNSI scanner.

Function	Software	Revision
Communications	RSLinx	2.42 or higher
DeviceNet Configuration	RSNetWorx for DeviceNet	6.x or higher
Programming Application Logic	RSLogix Guard PLUS!, Program Management	4.0 or higher
	RSLogix Guard PLUS!, Hardware Management	6.x or higher

DeviceNet Safety Scanner Features

Hardware Overview



The 1753-DNSI features two communication ports; one for DeviceNet communications and one for High-Speed Safety Protocol (HSP) communication with a GuardPLC controller. The HSP port is a 1 Mbps, full-duplex RS-485 interface.

The safety scanner also features a 4-character dot-matrix display, which provides status and error codes. Status LEDs on the safety scanner indicate module, network, and HSP connection status. See Chapter 10 for more information.

Supported Connections

The DeviceNet Safety port supports a maximum of 32 DeviceNet Safety input connections, 32 DeviceNet Safety output connections, and standard connections for up to 63 nodes.

The safety scanner does not support Quick Connect, Auto Device Replacement or Autoscan.

Safety Connections

The safety scanner supports single-cast producing or consuming connections and multi-cast consuming connections as a DeviceNet Safety originator. Up to 32 producing and 32 consuming safety connections can be made. These connections are used when the safety scanner is communicating to distributed safety I/O modules.

The safety scanner also supports the use of two safety targets, defined by RSLogix Guard PLUS! and made available via the Target Connections File. One target may be a single- or multi-cast producer, the other may be a single-cast consumer. These connections allow the safety scanner to look like safety I/O to another safety scanner on the network, and can be used for interlocking of safety data between two GuardPLC systems.

Standard Connections

The safety scanner supports the following standard DeviceNet connection types:

Standard Master Connections	Standard Slave Connections
Polled	Polled
Change of State (COS)	—
Cyclic	—
Bit Strobe	—

Communication Rate

The safety scanner supports the following communication rates, but does not support autobaud:

- 125 Kbps (default)
- 250 Kbps
- 500 Kbps

Physical Layout of the DeviceNet Safety System

Planning your system helps ensure that you can:

- meet safety times
- use memory and bandwidth efficiently
- fulfill device-specific requirements
- leave room for system expansion

Before configuring your 1753-DNSI scanner, you should be familiar with each of the DeviceNet devices on your network. You should know each device's:

- system safety time requirements
- communication requirements
- I/O size
- frequency of message delivery

You must also understand and define which data elements can be treated as safety and which as standard in your intended configuration.

DeviceNet Safety I/O Performance Factors

Safety nodes have priority on a DeviceNet network, but the performance of DeviceNet Safety I/O modules can be affected by the:

- baud rate of the network (Lower baud rates mean slower transmissions and slower responses.)
- packet size for the various connections (Bigger packets may result in fragmented messages and slower responses than single-packet messages, but use fewer resources.)
- type and number of connections used (Using point-to-point connections to make multiple connections to an input node uses more resources than a multicast connection.)
- RPI of the devices (Lower RPIs consume more bandwidth but lower system reaction time.)

Choose a Communication Rate for the Network

The default communication rate for a DeviceNet network is 125K bit/s. This is the easiest communication rate to use.

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

Communication Rate	Maximum Distance			Cumulative Drop Line Length
	flat cable	thick cable	thin cable	
125K bit/s	420 m (1378 ft)	500 m (1640 ft)	100 m (328 ft)	156 m (512 ft)
250K bit/s	200 m (656 ft)	250 m (820 ft)	100 m (328 ft)	78 m (256 ft)
500K bit/s	75 m (246 ft)	100 m (328 ft)	100 m (328 ft)	39 m (128 ft)

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.

Set the baud rate of the DeviceNet Safety Scanner using the Node Commissioning tool in RSNetWorx for DeviceNet. See Commission All Nodes on page 3-2.

The following table lists the most common methods for setting communication rates for other DeviceNet devices.

Method	Description
autobaud	At power up, the device automatically sets its communication rate to the baud rate of the first device it finds on the network. The device remains set until it powers up again. The network requires at least one device with a fixed communication rate so that the autobaud devices have something against which to set. Typically, scanners and network interfaces have a fixed communication rate.
switches or pushbuttons on the device	Some devices have switches or a pushbutton that sets the communication rate. Typically, the switch or pushbutton lets you select either autobaud or a fixed communication rate (125K, 250K, or 500K bit/s). The device reads the switch setting at power up. If you change the setting, you must cycle power for the change to take effect.
software	Some devices require a programming device to set its address and communication rate. For example, you can use the Node Commissioning tool in RSNetWorx for DeviceNet to set the communication rate of a device.

Assign an Address to Each Device

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.

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 to 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.

Standard DeviceNet assigns communication priority based on the device's node number. The lower the node number, the higher the device's communications 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 communications from devices with lower node numbers have priority over DeviceNet Safety communications from devices with higher node numbers.

Install the 1753-DNSI

General Safety Information

ATTENTION ⚠

Safety Applications

Personnel responsible for the application of safety-related Programmable Electronic System (PES) shall be aware of the safety requirements in the application of the system and shall be trained in using the system.

ATTENTION ⚠

Environment and Enclosure

This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC publication 60664-1), at altitudes up to 2000 meters 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 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.

See NEMA Standards publication 250 and IEC publication 60529, as applicable, for explanations of the degrees of protection provided by different types of enclosure. Also, see the appropriate sections in this publication, as well as the Allen-Bradley publication 1770-4.1 (Industrial Automation Wiring and Grounding Guidelines), for additional installation requirements pertaining to this equipment.

ATTENTION ⚠

Protective Debris Strip

Do not remove the protective debris strip until after the module and all other equipment in the panel near the module 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.

Preventing Electrostatic Discharge

ATTENTION ⚠

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 grounding wrist-strap.
- Do not touch connectors or pins on component boards.
- Do not touch circuit components inside the equipment.
- If available, use a static-safe workstation.
- When not in use, store the equipment in appropriate static-safe packaging.

Mount the Scanner

IMPORTANT

For effective cooling:

- Because of thermal considerations, mount the module horizontally only.
- Provide a gap of at least 100 mm (3.94 in.) above, below, and on each side of the module.
- Provide a gap of at least 51 mm (2.0 in.) from the front face of the module to the door of the enclosure.
- Select a location where air flows freely or use an additional fan.
- Do not mount the module over a heating device.

The module can be DIN rail or panel-mounted as described in the following sections.

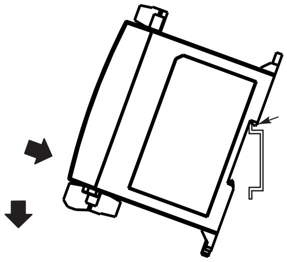
ATTENTION

Be careful of metal chips when drilling mounting holes for your module or other equipment within the enclosure or panel. Drilled fragments that fall into your module could cause damage.

DIN Rail Mounting

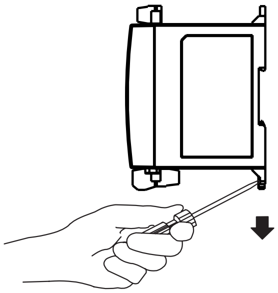
Mount the module to a EN50022-35x7.5 or EN50022-35x15 DIN rail by following the steps below:

1. Close the DIN latches, if they are open.
2. Hook the top slot over the DIN rail.
3. While pressing the module down against the top of the rail, snap the bottom of the module into position.



TIP

To remove the module from the DIN rail, insert a flathead screwdriver into the gap between the housing and each latch and pull the latch downward. When both DIN latches are open, lift the module off of the rail.



The maximum extension of each DIN rail latch is 14 mm (0.55 in) in the open position.

Panel Mounting

Mount the scanner directly to a panel using 4 screws. The preferred screws are #8 (M4); however, #6 (M3.5) may be used.

1. Use the mounting template provided in the module's installation instructions, publication number 1753-IN009.
2. Space your module properly to allow for adequate cooling. See page 2-2.
3. Secure the template to the mounting surface.
4. Drill holes through the template.
5. Remove the mounting template.
6. Secure the module to the panel using 4 screws.

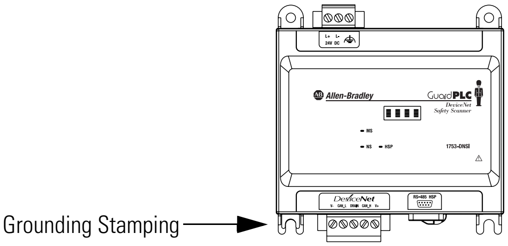
Ground the Scanner

This product is intended to be mounted to a well grounded mounting surface such as a metal panel. Refer to the Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1, for additional information.

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 (e.g. aluminum, plastic, etc.) that can corrode, oxidize, or are poor conductors, can result in improper or intermittent grounding.

Functionally ground the module through its DIN rail connection or through the mounting foot, if panel-mounted.



You must always connect the power supply functional ground screw when connecting the power supply.

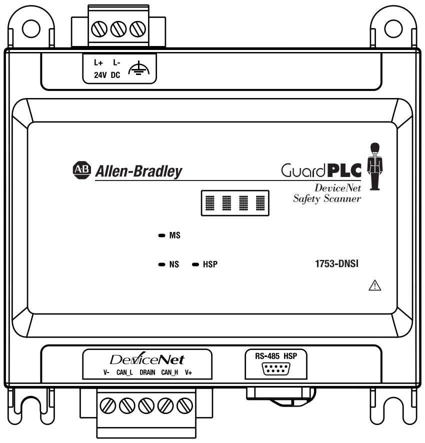
You must provide an acceptable grounding path for each device in your application. For more information on proper grounding guidelines, refer to the Industrial Automation Wiring and Grounding Guidelines, publication number 1770-4.1.

Connect Power Source

Power for the module is provided via an external 24V dc power source as well as from the DeviceNet cable. In North America, you must use a power supply that is marked CLASS 2 per the requirements of NFPA (National Electric Code) or CSA 22.1 (Canadian Electric Code, Part 1). Outside of North America, you must use a Safety Extra Low Voltage (SELV), or a Protected Extra Low Voltage (PELV) power supply to power this module. A SELV supply cannot exceed 30V rms, 42.4V peak, or 60V dc under normal conditions and under single fault conditions. A PELV supply has the same rating and is connected to protected earth.

Tighten power supply terminal screws to 0.5 to 0.6 Nm (4.4 to 5.3 in-lb.).

While some power is drawn from the DeviceNet network, the main power source is the external power supply.

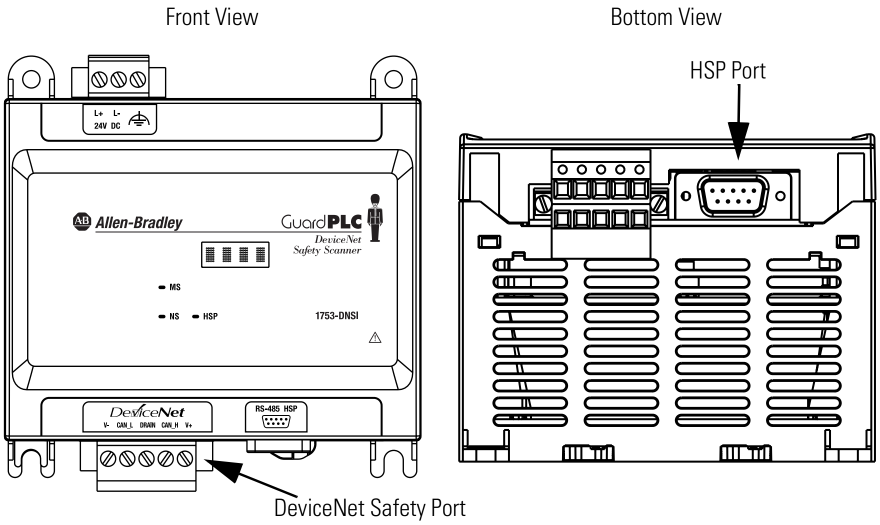


Make Communication Connections

ATTENTION

Do not connect or disconnect either communications cable with power applied to this module or any device on the network, because an electrical arc can occur. This could cause an explosion in hazardous location installations.

The scanner has two communication ports. The DeviceNet port is for communicating on DeviceNet, allowing connections to up to 63 standard DeviceNet nodes and 32 DeviceNet Safety nodes. The HSP port lets you communicate with a single GuardPLC 1600 or 1800 controller via a 1753-CBLDN cable.



DeviceNet Connections

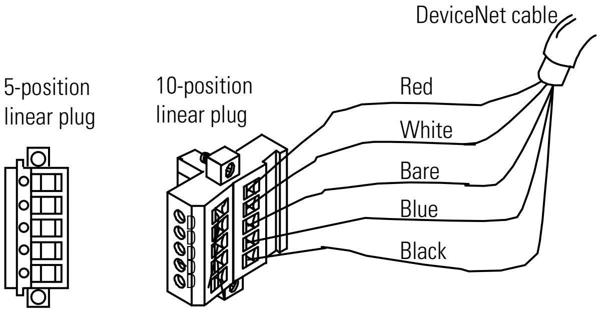
Wire the DeviceNet Connector

Use an open-style 5- or 10-position linear plug to connect to the DeviceNet network.

IMPORTANT For detailed DeviceNet connection information, refer to the DeviceNet Cable System Planning and Installation Manual, publication DN-6.7.2. Also refer to the Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1.

Wire the connector according to the following illustrations:

Connect	To
Red Wire	V+
White Wire	CAN High
Bare Wire	Shield
Blue Wire	CAN Low
Black Wire	V-



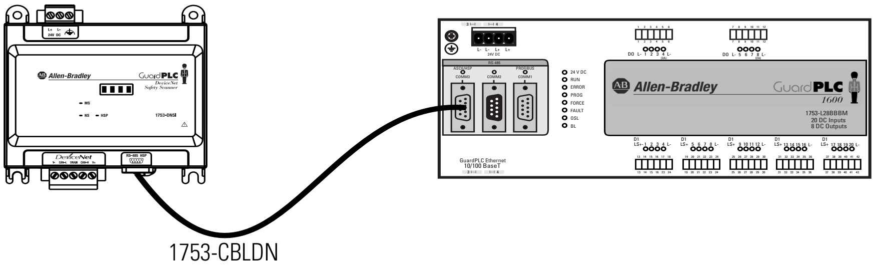
Connect to the DeviceNet Network

Attach the connector to the module’s DeviceNet port. Tighten the screws on the connector to 0.6 to 0.7 Nm (5 to 6 in-lb).

High-speed Safety Protocol (HSP) Connections

The module ships with the cable used to connect its HSP port to the GuardPLC controller’s COMM3 (ASCII/HSP) port. The minimum bend radius of the 1753-CBLDN is:

- 30 mm (1.18 in.) when the cable is permanently restrained by the use of a wire tie, cable trough, or other means.
- 60 mm (2.36 in.) when unrestrained.



IMPORTANT The maximum length of the cable connection between the module and the GuardPLC controller is 0.75 m (2.46 ft). To achieve a SIL 3 rating, you must use the 1753-CBLDN cable, which is shipped with the module.

Set Up Your DeviceNet Network

To set up devices on the DeviceNet network, follow the procedures listed below in order:

Procedure	page
1. Connect a Computer to the DeviceNet Network	3-2
2. Commission All Nodes	3-2
3. Browse the Network	3-3
4. Safety Reset (Optional)	3-4
5. Set Passwords (Optional)	3-5

Connect a Computer to the DeviceNet Network

To access a network, either:

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

TIP RSLinx provides online help for configuring drivers and using linking (bridge) devices.

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 using the correct cable.

Configure a Driver for the Network

1. Start RSLinx® software.

2. Click on the Configure Driver button.

3. Pull down the list of Available Driver Types and add the driver for your network.

For this network	Select this driver
RS-232	RS-232 DF1 Devices
EtherNet/IP	Ethernet devices
DeviceNet	DeviceNet drivers…

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 to make sure that the driver is running.
2. Close the dialog.
3. Open the RSWho window.
4. Double-click on the driver to see the network.

Commission All Nodes

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 to set the node address and/or baud rate of the DeviceNet Safety Scanner and other DeviceNet devices.

Follow the guidelines on page 1-10 when selecting node addresses for your DeviceNet network.

TIP

You can set the node address of a DeviceNet Safety I/O module by setting the rotary switches to a value between 0 and 63. Or, set the switches to a value between 64 and 99 to allow the node address to be set using the Node Commissioning tool in RSNetWorx for DeviceNet.

Refer to the DeviceNet Safety I/O Modules User Manual, publication number 1791DS-UM001, for information on commissioning 1791DS I/O modules.

To use the Node Commissioning tool:

1. Within RSNetWorx for DeviceNet, select Tools > Node Commissioning.
2. Click on the Browse button on the Node Commissioning dialog to select a device by browsing the network.
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. If you want to change the baud rate of the device, select the desired value.

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

6. On the Node Commissioning dialog, 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 SNN to an uninitialized state by selecting the SNN and performing a Safety Reset as described on page 3-4.

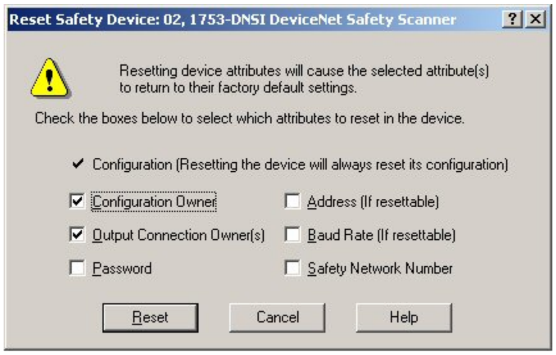
Browse the Network

1. Browse the network by clicking on the online button 🖧.
2. On the Browse for Network dialog, select the DeviceNet network.
3. Wait for the Browse Network operation to complete. As the network is browsed, all of the devices on the network will show up in RSNetWorx for DeviceNet.
4. Verify that all your nodes are visible.
5. Save your project in RSNetWorx for DeviceNet.

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.

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



Reset Safety Device: 02, 1753-DNSI DeviceNet Safety Scanner

Resetting device attributes will cause the selected attribute(s) to return to their factory default settings.

Check the boxes below to select which attributes to reset in the device.

✓ Configuration (Resetting the device will always reset its configuration)

☑ Configuration Owner □ Address (If resettable)

☑ Output Connection Owner(s) □ Baud Rate (If resettable)

□ Password □ Safety Network Number

1. Open the Reset Safety Device dialog by clicking on the device in the RSNetWorx for DeviceNet 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 checkbox is always checked to indicate that 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 next device that attempts to configure the device following the safety reset becomes the configuration owner.
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.
Address	Check this checkbox to reset the device's software-configured node Address to 63. NOTE: If the device's node Address has been set using DIP switches, the reset operation has no effect on the node Address.
Baud Rate	Check this checkbox to reset the device's baud rate to 125 kbps. NOTE: If the device's baud rate has been set using DIP switches, the reset operation has no effect on the baud rate.
Safety Network Number	Check this checkbox to reset the device's Safety Network Number.

3. Click on the Reset button.

4. 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.

5. If you have set a password for the device, enter the password when prompted.

Set 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 entered:

- download
- Safety-Reset
- Safety-Lock
- Safety-Unlock

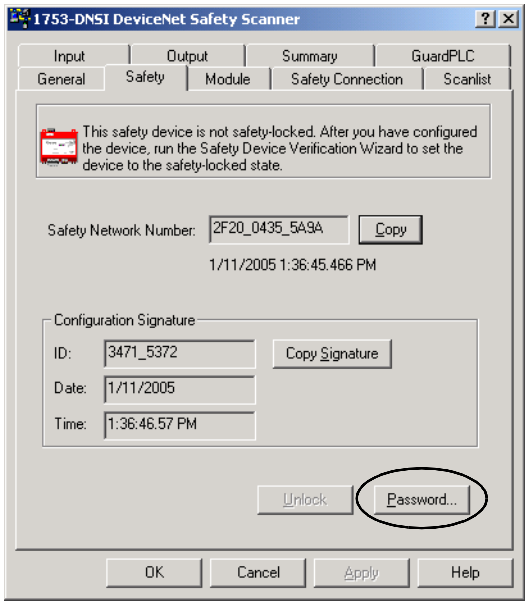
Set or Change a Password

To set a password for a module:

1. Double-click on the module to open the Device Properties dialog.

2. Select the Safety tab.

3. Click on the Password… button.



1753-DNSI DeviceNet Safety Scanner

This safety device is not safety-locked. After you have configured the device, run the Safety Device Verification Wizard to set the device to the safety-locked state.

Safety Network Number: 2F20_0435_5A9A

1/11/2005 1:36:45.466 PM

Configuration Signature

ID: 3471_5372

Date: 1/11/2005

Time: 1:36:46.57 PM

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

- clicking on the module and choosing Set Password… from the Device menu, or
- right-clicking on the module and selecting Set Password….

4. Enter the Old Password, if one exists.

5. Enter and confirm the new password.

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

6. Click OK.

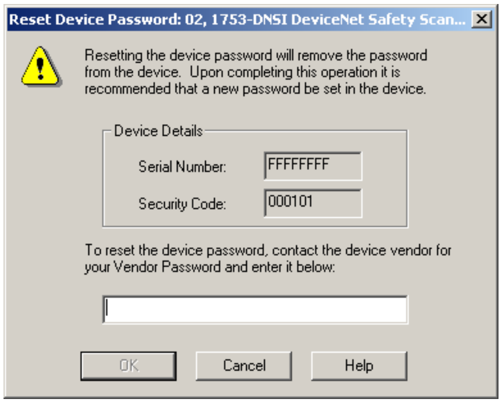
Forgotten Passwords

If you forget the password, you can reset it.

1. On the Safety tab of the Device Properties dialog, click on the Password… button to open the Set Device Password dialog.

2. Click on the Reset Password… button.

3. Contact Rockwell Automation Technical Support and provide the device Serial Number and Security Code from the Reset Password dialog.



Reset Device Password: 02, 1753-DNSI DeviceNet Safety Scan...

Resetting the device password will remove the password from the device. Upon completing this operation it is recommended that a new password be set in the device.

Device Details

Serial Number: FFFFFFFF

Security Code: 000101

To reset the device password, contact the device vendor for your Vendor Password and enter it below:

4. Enter the Vendor Password obtained from Rockwell Automation Technical Support on the Reset Device Password dialog and click OK.

Chapter 4

Manage the Safety Network Number

Safety Network Numbers assigned to each safety network or network sub-net must be unique. You must ensure that a unique Safety Network Number (SNN) is assigned to each DeviceNet network that contains safety nodes.

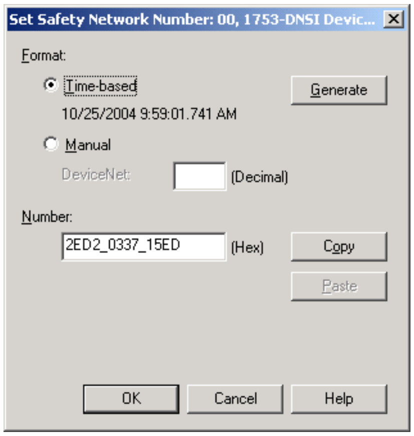
Each DeviceNet Safety device must be configured with an SNN. The combination of SNN and DeviceNet node address provides a unique identifier for every safety node in a complex industrial network. This unique identifier prevents data intended for a specific target node address on one DeviceNet subnet from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

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 SNN (Recommended)

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



Set Safety Network Number: 00, 1753-DNSI Devic...

Format:

● Time-based

10/25/2004 9:59:01.741 AM

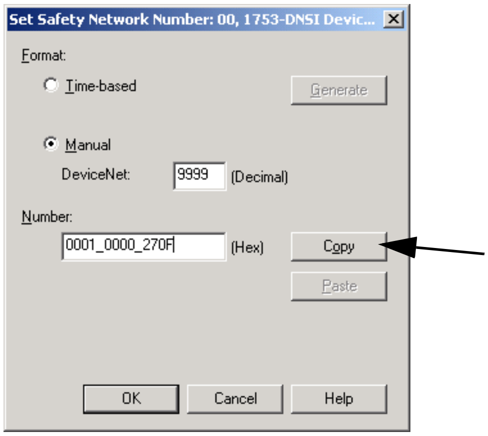
○ Manual

DeviceNet: (Decimal)

Number: 2ED2_0337_15ED (Hex)

Manual SNN

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



Set Safety Network Number: 00, 1753-DNSI Devic...

Format:

○ Time-based

● Manual

DeviceNet: 9999 (Decimal)

Number: 0001_0000_270F (Hex)

TIP You can use the Copy button on the Set Safety Network Number dialog to copy the SNN to the Windows® clipboard.

Assignment of the SNN

SNNs can be generated automatically via RSNetWorx for DeviceNet or manually assigned by the user. Automatically generated SNNs are 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:

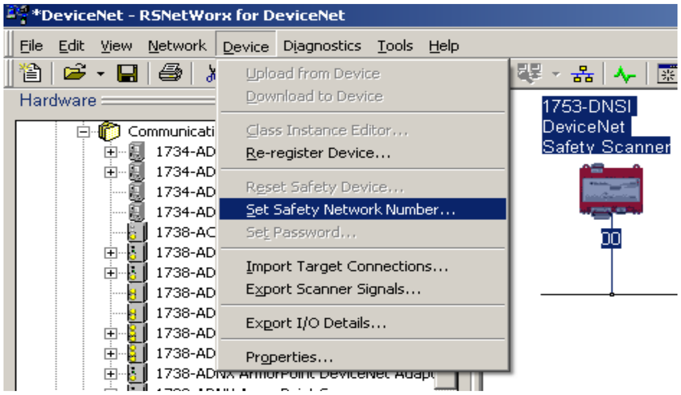
- If at least one safety device already exists in the DeviceNet network configuration, subsequent safety additions to that network configuration are assigned the same SNN as the lowest addressed safety device.
- If no other safety devices exist in the DeviceNet network configuration, a time-based SNN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

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 SNNs in a logical manner pertaining to their specific application.

IMPORTANT If you assign SNNs manually, take care to ensure 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, select the device in the hardware graphic view and choose Set Safety Network Number from the Device menu.



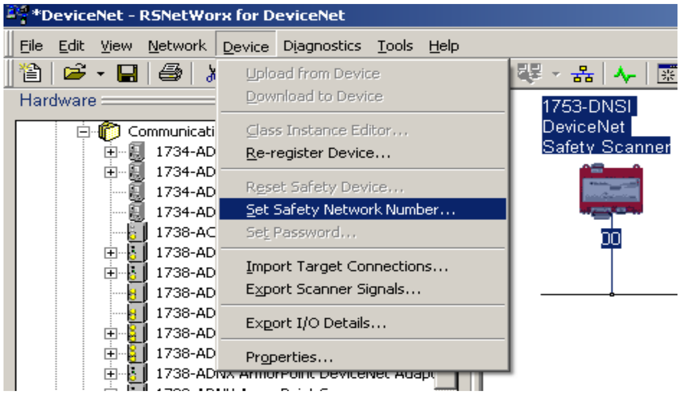
IMPORTANT When you set the SNN, the device is returned to its factory default configuration.

Set the SNN in All Safety Nodes

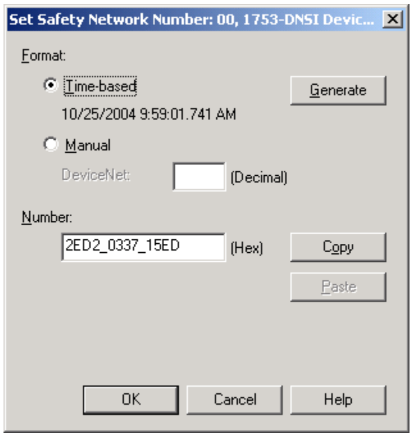
A time-based SNN is automatically generated when the first new safety device is added to the network. Subsequent additions to the network are assigned the same SNN as the lowest-addressed safety device. This automatic, time-based SNN is sufficient and recommended for most applications.

If you need to set the SNN for a particular device, follow the steps below:

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



2. Select Time-based and click the Generate button, or select Manual and fill in a Decimal number from 1 to 9999. Click OK.



Set Safety Network Number: 00, 1753-DNSI Devic...

Format:

● Time-based

10/25/2004 9:59:01.741 AM

○ Manual

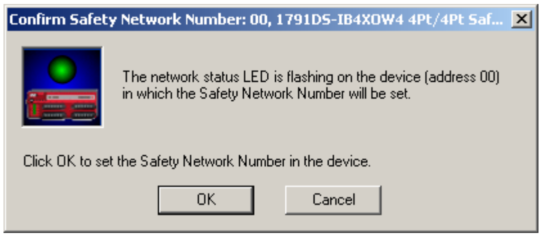
DeviceNet: (Decimal)

Number:

2ED2_0337_15ED (Hex)

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

3. Verify that the Network Status LED is rapidly alternating between red and green on the correct device and click OK.



Confirm Safety Network Number: 00, 1791DS-IB4XOW4 4Pt/4Pt Saf...

The network status LED is flashing on the device (address 00) in which the Safety Network Number will be set.

Click OK to set the Safety Network Number in the device.

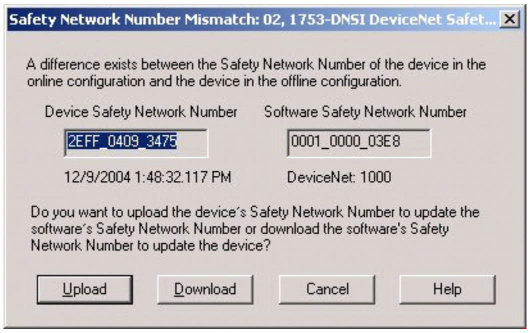
SNN Mismatch

RSNetWorx for DeviceNet 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 indicates an error with the SNN. The hardware graphic view displays the ! symbol over the safety device icon. You can resolve the SNN error from the Safety Network Number Mismatch dialog, as described on page 4-5.

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

Safety Network Number Mismatch Dialog

This dialog 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.



Safety Network Number Mismatch: 02, 1753-DNSI DeviceNet Safet...

A difference exists between the Safety Network Number of the device in the online configuration and the device in the offline configuration.

Device Safety Network Number: 2EFF_0409_3475
12/9/2004 1:48:32.117 PM

Software Safety Network Number: 0001_0000_03E8
DeviceNet: 1000

Do you want to upload the device's Safety Network Number to update the software's Safety Network Number or download the software's Safety Network Number to update the device?

TIP 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 disabled.

SNN and Node Address Changes

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

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 and click on Reset.

   Only the attributes selected on the dialog 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 3-4 for more information on the Safety Reset function.

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

Configure DeviceNet Nodes and Connections

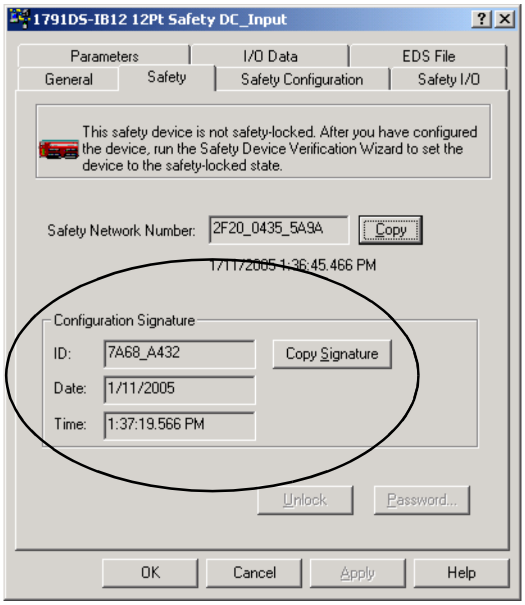
To configure standard, safety, and peer-to-peer connections, follow the procedures listed below in order:

Procedure	page
1. Configure DeviceNet Safety I/O Target Nodes	5-2
2. Configure the DeviceNet Safety Scanner's Safety Connections	5-3
3. Configure DeviceNet Standard Slave I/O Nodes	5-6
4. Configure the DeviceNet Safety Scanner's Standard Connections	5-6
5. Configure GuardPLC Controller Settings	5-12

Configuration Signature

Each safety device has a unique Configuration Signature, which identifies its configuration to ensure 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 when a configuration update is applied to the device. The Configuration Signature is found on the Safety tab of the Device Properties dialog.



1791DS-IB12 12Pt Safety DC_Input

This safety device is not safety-locked. After you have configured the device, run the Safety Device Verification Wizard to set the device to the safety-locked state.

Safety Network Number: 2F20_0435_5A9A

1/11/2005 1:36:45.466 PM

Configuration Signature

ID: 7A68_A432

Date: 1/11/2005

Time: 1:37:19.566 PM

The Configuration Signature is read during each browse and whenever the Device Properties dialog is launched while the software is in Online mode. RSNetWorx for DeviceNet 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.

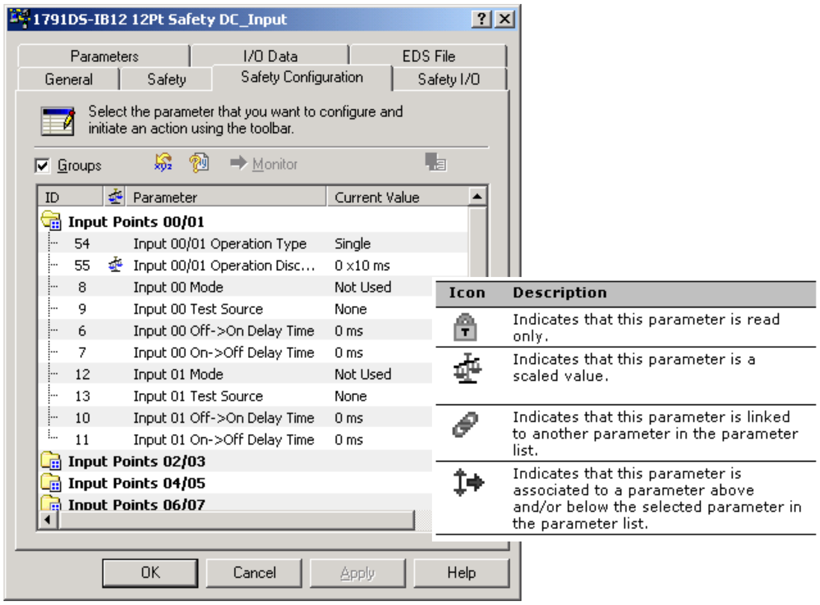
Configure DeviceNet Safety I/O Target Nodes

1791DS DeviceNet Safety I/O Module Parameters

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

Safety Input, Output, and Test Parameters

Safety parameters are configured using the Safety Configuration tab on the Module Properties page.



Select the parameter that you want to configure and initiate an action using the toolbar.

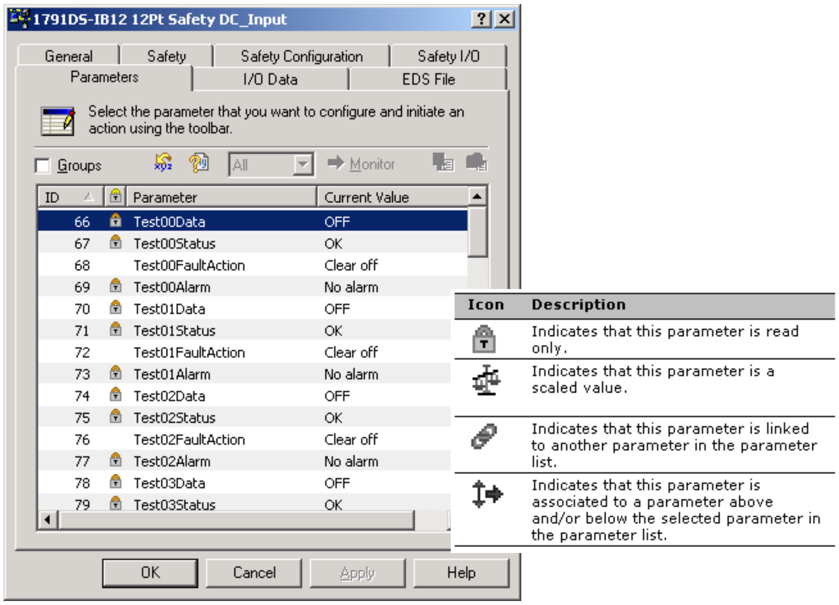
☑ Groups

ID		Parameter	Current Value
Input Points 00/01			
54		Input 00/01 Operation Type	Single
55	⚖	Input 00/01 Operation Disc...	0 x10 ms
8		Input 00 Mode	Not Used
9		Input 00 Test Source	None
6		Input 00 Off->On Delay Time	0 ms
7		Input 00 On->Off Delay Time	0 ms
12		Input 01 Mode	Not Used
13		Input 01 Test Source	None
10		Input 01 Off->On Delay Time	0 ms
11		Input 01 On->Off Delay Time	0 ms
Input Points 02/03			
Input Points 04/05			
Input Points 06/07			

Icon	Description
🔒	Indicates that this parameter is read only.
⚖	Indicates that this parameter is a scaled value.
🔗	Indicates that this parameter is linked to another parameter in the parameter list.
↕	Indicates that this parameter is associated to a parameter above and/or below the selected parameter in the parameter list.

Standard Input and Output Parameters

1791DS modules support standard data as well as safety data. Configure standard input and output parameters using the Parameters tab on the module properties page.



Select the parameter that you want to configure and initiate an action using the toolbar.

□ Groups

ID	🔒	Parameter	Current Value
66	🔒	Test00Data	OFF
67	🔒	Test00Status	OK
68		Test00FaultAction	Clear off
69	🔒	Test00Alarm	No alarm
70	🔒	Test01Data	OFF
71	🔒	Test01Status	OK
72		Test01FaultAction	Clear off
73	🔒	Test01Alarm	No alarm
74	🔒	Test02Data	OFF
75	🔒	Test02Status	OK
76		Test02FaultAction	Clear off
77	🔒	Test02Alarm	No alarm
78	🔒	Test03Data	OFF
79	🔒	Test03Status	OK

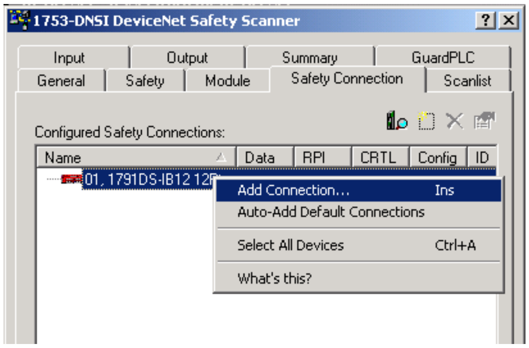
Icon	Description
🔒	Indicates that this parameter is read only.
⚖	Indicates that this parameter is a scaled value.
🔗	Indicates that this parameter is linked to another parameter in the parameter list.
↕	Indicates that this parameter is associated to a parameter above and/or below the selected parameter in the parameter list.

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

Configure the DeviceNet Safety Scanner's Safety Connections

Configure DeviceNet Safety communications by configuring the scanner's connections to safety targets.

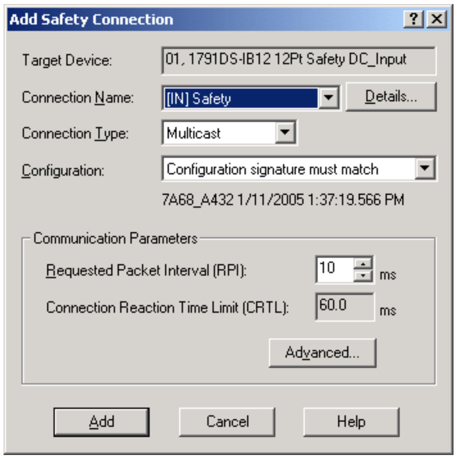
On the Safety Connections tab, right-click on the I/O module and select Add Connections to display all of the available connections.



Configured Safety Connections:

Name	Data	RPI	CRTL	Config	ID
01, 1791DS-IB12 12P					

The Add Safety Connection dialog allows you to configure a connection.



Add Safety Connection

Target Device: 01, 1791DS-IB12 12Pt Safety DC_Input

Connection Name: [IN] Safety

Connection Type: Multicast

Configuration: Configuration signature must match

7A68_A432 1/11/2005 1:37:19.566 PM

Communication Parameters

Requested Packet Interval (RPI): 10 ms

Connection Reaction Time Limit (CRTL): 60.0 ms

1. Select the desired connection by choosing the Connection Name.

2. Select a type of connection, either Multicast (input connections only) or Point-to-point (input or output connections).

3. Select 'Configuration signature must match'. This selection directs the scanner to ensure that the target safety device contains the correct configuration before opening the safety connection.

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

4. Review the Connection Reaction Time Limit.

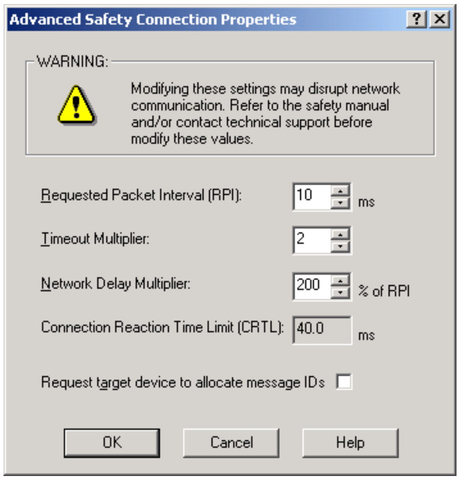
   The Connection Reaction Time Limit is the maximum age of safety packets on the associated connection. If the age of the data used by the consuming device exceeds the Connection Reaction Time Limit, a connection fault occurs. Adjust the Connection Reaction Time Limit by changing the RPI or the Advanced Communication Properties as described in steps 5 and 6.

5. Set the Requested Packet Interval (RPI).

   The RPI specifies the period at which data updates over a connection. The RPI is entered in 1 millisecond increments, and the scanner supports a valid range of 5 to 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, use the Advanced… button to further adjust the timing values affecting the Connection Reaction Time Limit as described below.

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



Advanced Safety Connection Properties

WARNING:

Modifying these settings may disrupt network communication. Refer to the safety manual and/or contact technical support before modify these values.

Requested Packet Interval (RPI): 10 ms

Timeout Multiplier: 2

Network Delay Multiplier: 200 % of RPI

Connection Reaction Time Limit (CRTL): 40.0 ms

Request target device to allocate message IDs □

- 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 communications 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.

Configure DeviceNet Standard Slave I/O Nodes

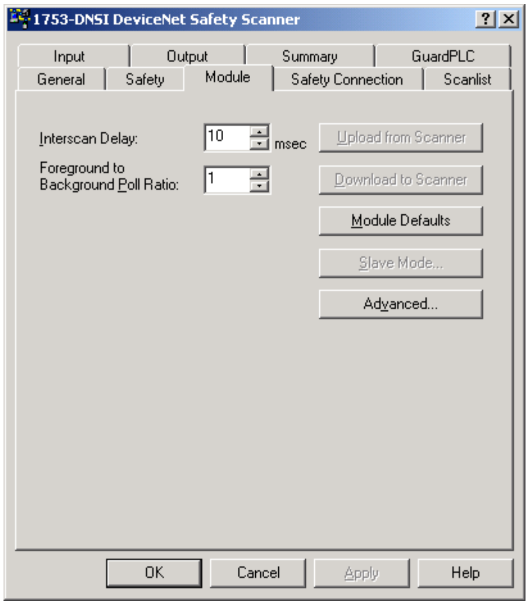
To configure your module, double-click on the module in the graphic view or right-click on the module and select Properties. Navigate through the available tabs to review and modify the module's configuration. Refer to the user manual for the module for additional information on how to set up the module's configuration.

Configure the DeviceNet Safety Scanner's Standard Connections

To configure the safety scanner for standard communications, you set up a scanlist and define the memory locations for the standard data of each device.

Standard Communication Properties

Configure the standard communication properties of the safety scanner on the Module tab of the Scanner Properties page. You can use the Module Defaults button to return the safety scanner to the default settings, which are shown below.



1753-DNSI DeviceNet Safety Scanner

Interscan Delay: 10 msec

Foreground to Background Poll Ratio: 1

Interscan Delay

This parameter defines the delay time the scanner uses between scans of the DeviceNet network. If you have slave devices configured for Polled behavior in the scanner's scanlist, Interscan Delay (ISD) defines the amount of time the scanner waits between writing outputs to the polled devices.

Increasing the ISD time causes a longer network scan, which adversely affects overall input-to-output performance. However, the increase allows lower priority messages to get more network access. These lower priority messages include those used to do network browsing and configuration upload and download functions. So, if these network functions are sluggish on your system, increasing the ISD time is one way to make more bandwidth available for lower priority messages.

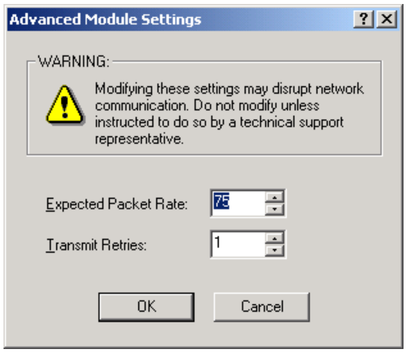
In addition, if the last node in your scan list produces a large amount of polled data, you may want to increase the ISD time to ensure that the entire response is received before the next poll request is sent to that node.

Foreground to Background Poll Ratio

Devices set for polled behavior can be polled on every I/O scan (foreground) or they can be polled less frequently (background). Setting a device for foreground or background behavior is done when you configure each device on the Scanlist tab, from the Edit I/O Parameters dialog. A ratio of 2 means that any nodes included on the background list are polled every other scan cycle. A ratio of 3 means they are polled on every third cycle, etc.

Advanced Module Settings

Clicking on the Advanced… button lets you to set the Expected Packet Rate (EPR) and the Transmit Retries as described below.


Advanced Module Settings

WARNING:

Modifying these settings may disrupt network communication. Do not modify unless instructed to do so by a technical support representative.

Expected Packet Rate: 75

Transmit Retries: 1

- Expected Packet Rate (EPR) – When the scanner opens a polled or strobed I/O connection, it uses this value as a maximum timeout (Expected Packet Rate) with the device. If the *device* does not receive a packet from the scanner within 4 times the EPR value, the slave device drops the connection. If the *scanner* does not receive a packet from the slave within 4 times the EPR value, it drops the connection and periodically attempts to reopen the connection.

When a standard connection is dropped, status bits in the scanner identify that the slave is not online. Slave behavior when a connection is dropped is a function of the slave device. If the slave is an I/O device, the standard outputs will be cleared, held at last state, or set to a fault condition (refer to the slave device’s documentation for actual I/O behavior when a connection is dropped).

When an input connection is dropped, the scanner sets the corresponding data in the data tables sent to the GuardPLC controller via the HSP connection to the safety state (0).

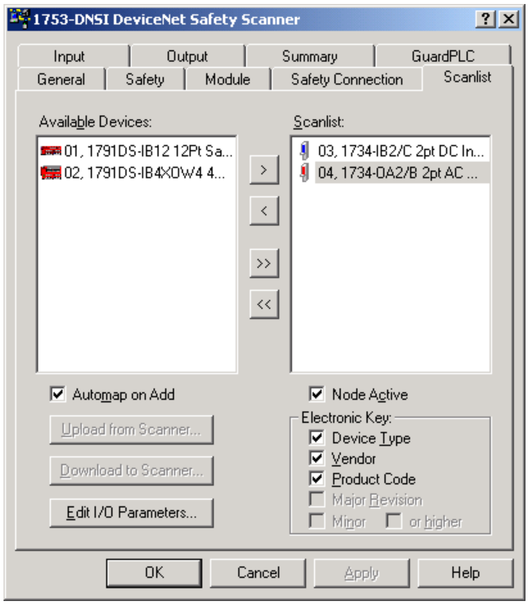
The EPR default value is 75 milliseconds.

IMPORTANT Changing the EPR number should be done carefully because it effects how long it takes the scanner to detect a missing device.

- Transmit Retries – Transmit Retries specifies the number of times the scanner attempts to retransmit a change of state or cyclic message that has not been acknowledged by the slave device before dropping the connection.

Create a Scanlist

The scanlist defines the standard devices (nodes) with which the scanner is configured to exchange I/O data.



1753-DNSI DeviceNet Safety Scanner

Available Devices:
01, 1791DS-IB12 12Pt Sa...
02, 1791DS-IB4XOW4 4...

Scanlist:
03, 1734-IB2/C 2pt DC In...
04, 1734-OA2/B 2pt AC ...

☑ Automap on Add

☑ Node Active

Electronic Key:
☑ Device Type
☑ Vendor
☑ Product Code
□ Major Revision
□ Minor □ or higher

Available Devices

These are the devices on the network that have the ability to be standard slave I/O devices. The DeviceNet Safety Scanner, as well as any other scanners that have been configured to support a standard slave-mode interface will also appear in this list. Slave-capable devices do not have to be used as slave I/O by a scanner. They may alternately be used as slave I/O by another scanner on the same network, or they may have dual functionality.

Scanlist

These devices have been assigned to be slave I/O to this scanner. The outputs of a slave device on DeviceNet can only be owned by one master at a time. Data mappings for each device in the scanlist are configured using the input and output tabs. Add an available device by selecting the device and clicking on the add arrow >. The double-arrow >> adds all the available devices to the scanlist.

It is not necessary to enter safety nodes into the safety scanner's scan list. All safety connections are configured on the Safety Connections tab. You only need to put a safety device into the safety scanner's scanlist if you are communicating with that device via a standard connection and exchanging standard data with it.

Automap on Add

Automap allows a slave's I/O to be automatically mapped into the scanner's input or output image tables when the slave device is added to the scanlist. DO NOT check this box if you intend to map a slave device into a particular input or output memory location.

Edit I/O Parameters

These parameters will vary depending upon the slave device. Information on configurable parameters is usually provided in the device's documentation.

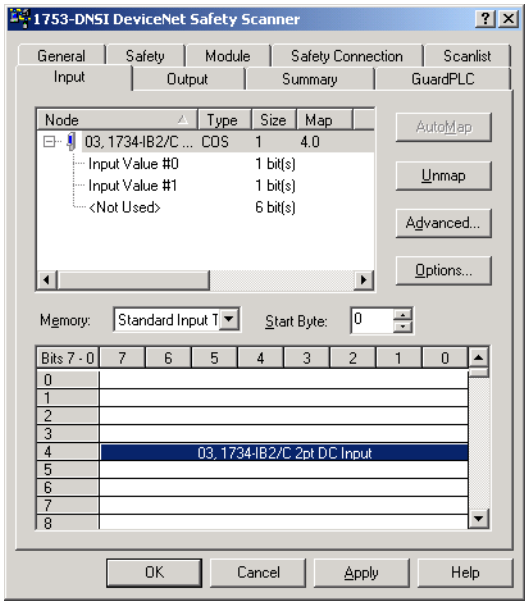
Electronic Key

The electronic key is used to ensure that a particular slave device always matches the intended device when the scanner initiates a connection to it. When one of the devices in the Scanlist section is highlighted, these boxes may be checked to indicate to what extent the key parameters must match the actual device on the network. A match of just Device Type can be selected or the additional parameters of Vendor ID and Product Code may be incrementally added.

Should the scanner detect a mismatch with any of the key parameters checked, an Electronic Key failure (status code 73) will occur for that slave device and the scanner will abort the connection establishment process.

Configure Standard Inputs

The Input tab lets you define how standard data from all of the scanner's slave devices are mapped into the input image of the controller.



Node	Type	Size	Map
03, 1734-IB2/C ...	COS	1	4.0
Input Value #0		1 bit(s)	
Input Value #1		1 bit(s)	
<Not Used>		6 bit(s)	

Memory: Standard Input T

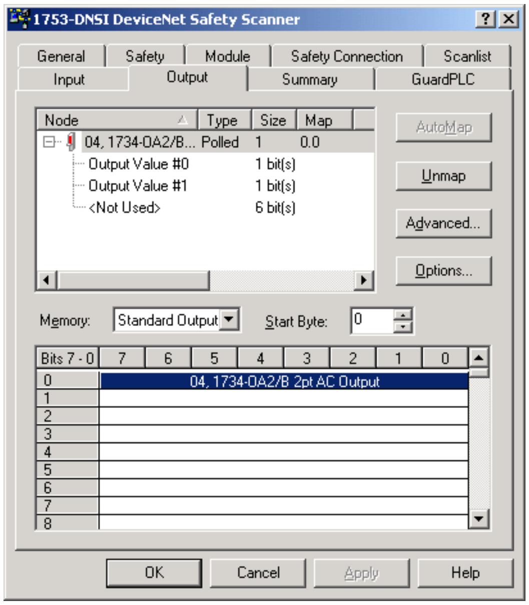
Start Byte: 0

Bits 7 - 0	7	6	5	4	3	2	1	0
0								
1								
2								
3								
4	03, 1734-IB2/C 2pt DC Input							
5								
6								
7								
8								

The graphical window at the top shows each device's node number, catalog number, type of connection that is used between the scanner and the slave device (strobed, polled, cyclic or change of state), the amount of data that will be exchanged (in bytes), and the location of the data within the controller's scanner's standard input image.

Configure Standard Outputs

The Output tab screen allows you to define how data from the scanner is mapped to the outputs of the slave devices.



Node	Type	Size	Map
04, 1734-OA2/B...	Polled	1	0.0
Output Value #0		1 bit(s)	
Output Value #1		1 bit(s)	
<Not Used>		6 bit(s)	

Memory: Standard Output

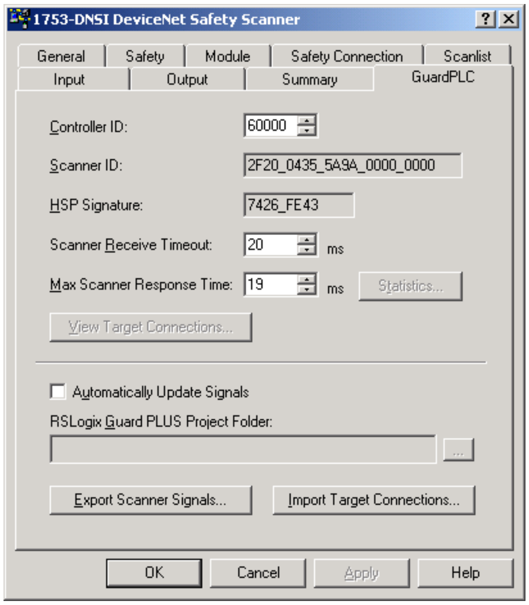
Start Byte: 0

Bits 7 - 0	7	6	5	4	3	2	1	0
0	04, 1734-OA2/B 2pt AC Output							
1								
2								
3								
4								
5								
6								
7								
8								

The graphical window at the top shows each devices node number, catalog number, type of connection that is used between the scanner and the slave device (strobed, polled, cyclic or change of state), the amount of data that will be exchanged (in bytes), and the location of the data within the controller's scanner's standard output image.

Configure GuardPLC Controller Settings

Use the GuardPLC tab to configure the scanner's HSP connection parameters.


1753-DNSI DeviceNet Safety Scanner

Controller ID: 60000

Scanner ID: 2F20_0435_5A9A_0000_0000

HSP Signature: 7426_FE43

Scanner Receive Timeout: 20 ms

Max Scanner Response Time: 19 ms

□ Automatically Update Signals

RSLogix Guard PLUS Project Folder:

Controller ID

The Controller ID (SRS) uniquely identifies a particular GuardPLC controller within a network of controllers. Its use ensures that this configuration is applied to the correct controller. Specify the Controller ID of your selected GuardPLC controller, or this will automatically be provided when you associate the scanner and controller as described in Chapter 7.

Scanner ID

The scanner ID is a read-only value which uniquely identifies the scanner and is required to connect the GuardPLC controller to the scanner. The scanner ID is automatically generated by RSNetWorx for DeviceNet using the SNN and DeviceNet address of the scanner. It is exported in the Scanner Signals file and is viewable in the associated RSLogix Guard PLUS! project.

HSP Signature

The HSP Signature is a read-only value that is unique to each layout of the signals within the data exchanged between the GuardPLC controller and the 1753-DNSI. The HSP Signature is calculated based on the scanner's configured safety and standard connections and any target connections defined in RSLogix Guard PLUS!. It is passed to RSLogix Guard PLUS! via the Scanner Signals File. The HSP signature changes only when a modification occurs in the layout of the signals exchanged between the controller and scanner.

Scanner Receive Timeout

The Scanner Receive Timeout is the amount of time (in milliseconds) that the scanner waits for a request from the GuardPLC controller before timing out the HSP connection. If the scanner does not receive a message from the GuardPLC controller within this time, all output connections are transitioned to the idle state, causing the safety outputs to transition to the safety state and standard outputs to follow the behavior dictated by their configuration.

Set the Scanner Receive Timeout equal to the Watchdog Timeout specified on the Properties dialog of the controller resource in RSLogix Guard PLUS! Hardware Management. Refer to the GuardPLC Controller Systems User Manual, publication number 1753-UM001, for information on setting the Watchdog Time.

Max. Scanner Response Time

The Max Scanner Response Time is the maximum amount of time (in milliseconds) allotted for the scanner to process an HSP request from the controller, and then format and send a proper response. If the scanner cannot respond within this time frame, then all output connections transition to the idle state, causing the safety outputs to transition to the safety state and standard outputs to follow the behavior dictated by their configuration.

The Max Scanner Response Time should be set to a value that includes the maximum observed statistical scanner response time over several hours of operation, plus a Margin of Safety equal to 3 ms or 10% of the maximum observed scanner response time. When online, you can view the Minimum, Maximum, and Average Observed Scanner Response Times by selecting the Statistics… button.

Create a GuardPLC Project with High-Speed Safety Protocol

To configure the GuardPLC controller to communicate with the DeviceNet Safety Scanner for GuardPLC Controllers, follow the procedures listed below in order:

Procedure	page
1. Create or Open a GuardPLC Project	6-1
2. Add High-Speed Safety Protocol to the GuardPLC Controller Resource	6-3
3. Review the GuardPLC Controller's Communication Settings	6-5

For detailed information on creating a GuardPLC controller project in RSLogix Guard PLUS!, refer to the GuardPLC Controller Systems User Manual, publication number 1753-UM001.

Create or Open a GuardPLC Project

TIP To optimize performance and minimize compilation time, create and store your projects on a local drive.

1. In RSLogix Guard PLUS!, either open an existing GuardPLC 1600 or GuardPLC 1800 controller project or create a new project by selecting Project>New from the main menu.

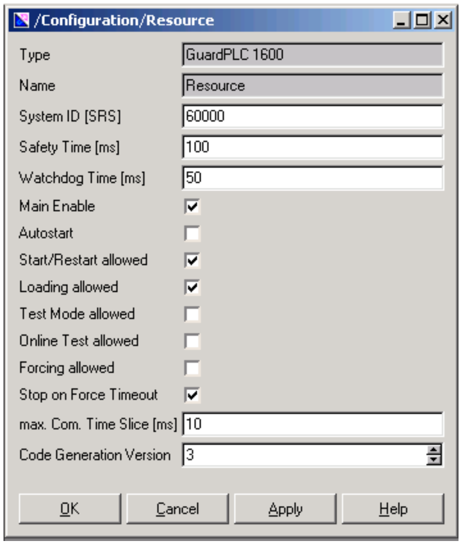
   If the project is new, enter the name of the project in the Object Name field and click OK. RSLogix Guard PLUS! automatically creates a single resource in a new project.

   TIP You can rename the controller Resource in the Project Management window by right-clicking on the Resource and selecting Rename from the context menu.

If you are opening an existing project, created in a prior version of RSLogix Guard PLUS!, the software automatically converts the project to the new version.

TIP Make a backup copy of your existing RSLogix Guard PLUS! project before opening it in the latest version, since the latest version automatically converts the existing project.

2. In the Hardware Management dialog, right-click on the controller Resource and select Properties.



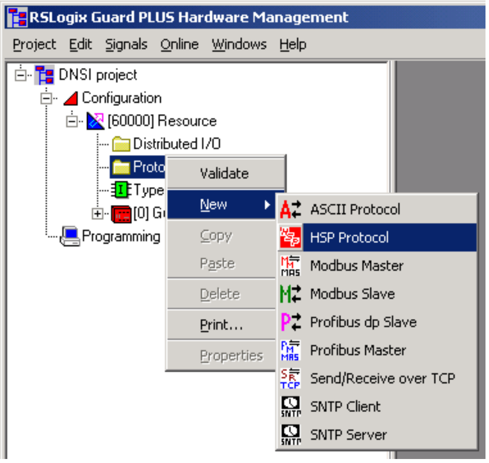
Type	GuardPLC 1600
Name	Resource
System ID [SRS]	60000
Safety Time [ms]	100
Watchdog Time [ms]	50
Main Enable	☑
Autostart	□
Start/Restart allowed	☑
Loading allowed	☑
Test Mode allowed	□
Online Test allowed	□
Forcing allowed	□
Stop on Force Timeout	☑
max. Com. Time Slice [ms]	10
Code Generation Version	3

3. Specify the controller type (GuardPLC 1600 or GuardPLC 1800 controllers only for HSP) and enter the System ID (SRS) of the controller. If you do not know the SRS, you need to connect the controller directly to your computer’s Ethernet port and use the Communication Settings dialog to retrieve the SRS. See step 1 on page 6-5.

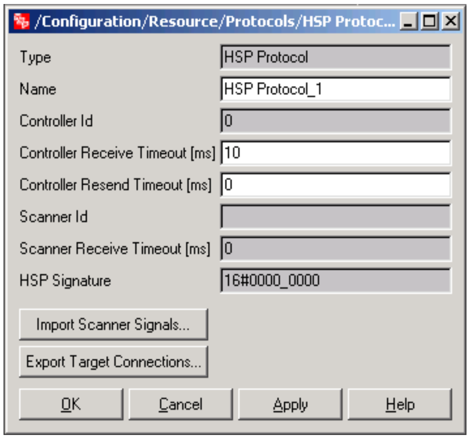
Add High-Speed Safety Protocol to the GuardPLC Controller Resource

To add High-Speed Safety Protocol (HSP) to your GuardPLC controller:

1. Right-click on the Protocols folder under your Resource and select New>HSP Protocol.



2. Configure HSP communications. Right-click on HSP Protocol and select Properties.


/Configuration/Resource/Protocols/HSP Protoc...

Type	HSP Protocol
Name	HSP Protocol_1
Controller Id	0
Controller Receive Timeout [ms]	10
Controller Resend Timeout [ms]	0
Scanner Id	
Scanner Receive Timeout [ms]	0
HSP Signature	16#0000_0000

The Controller Receive Timeout is the amount of time that the controller waits to receive an HSP response from the scanner before closing the HSP connection.

Controller Resend Timeout is the amount of time that the controller waits for the acknowledgement of a message before it resends it.

Use the following guidelines when setting the Controller Receive Timeout and Controller Resend Timeout:

- In environments where no HSP retries are required, set the Controller Receive Timeout to the amount of time required for the controller to send the HSP request, for the scanner to process the request, and for the scanner to send a response back to the controller. This value can be determined by observing the Response Time values displayed on the HSP protocol tab of the Resource Control Panel.

  Set the Controller Receive Timeout to be greater than or equal to the maximum value reported plus a margin of safety (3 ms or 10% of the maximum value reported). The Controller Resend Timeout should be set to zero.
- In electrically noisy environments, configuring retries on the HSP link may be required. Set the Controller Resend Timeout to be equal to or greater than the Max Response Time value reported on the HSP Protocol tab of the Resource Control Panel plus a margin of safety (3 ms or 10% of the maximum value reported). To enable a single retry, the Controller Receive Timeout must be 2 times the Controller Resend Timeout. To enable 2 retries, the Conroller Receive Timeout must be 3 times the Controller Resend Timeout.
- The controller's Communications Time Slice, found on the Properties dialog of the controller Resource, must be greater than the Controller Receive Timeout to enable proper HSP operation. If other protocols are in use on the controller Resource, then the Communications Time Slice should be increased to accommodate their use in conjunction with HSP. The Maximum Communication Time Slice setting on the Device Properties page should be set to the Maximum Communication Time Slice observed on the Control Panel's Statistics tab plus a margin of safety (6 ms or 10% of the maximum value reported).

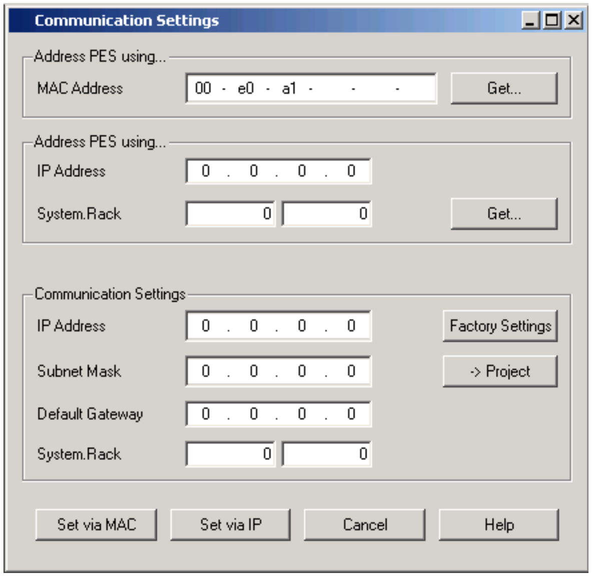
TIP

The Controller Id, Scanner Id and Scanner Receive Timeout values are shown here for reference. These values are set following a successful Scanner Signals File (.ssf) import process. For the import process to succeed, the Controller Id must match the System ID (SRS) of the controller Resource.

Refer to the GuardPLC Controller Systems User manual, publication 1753-UM001, for more information on configuring communications for GuardPLC controllers.

Review the GuardPLC Controller's Communication Settings

1. Retrieve or confirm the communication settings by selecting Communication Settings from the Online menu.



Communication Settings

Address PES using...

MAC Address: 00 - e0 - a1 - - -

Address PES using...

IP Address: 0 . 0 . 0 . 0

System.Rack: 0 0

Communication Settings

IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

System.Rack: 0 0

a. If you know the current IP Address, SRS and Administrator password, you can fill in the IP Address and SRS and select Get. This retrieves and confirms the communication settings. If you want to modify the current settings, see step 2.

b. If you do not know the current settings, you must connect your GuardPLC controller directly to your computer's Ethernet port and fill in the last three digits of the controller's MAC Address. The MAC Address is located on a label above the controller's lower Ethernet ports. Select Get to retrieve the current settings.

TIP The MAC Address lookup function can fail if there is an Ethernet switch between the PC running RSLogix Guard PLUS! and the GuardPLC controller.

2. You can now enter the desired settings for the IP Address and SRS.

3. To apply the new settings to the controller, click on either the Set via IP or Set via MAC buttons, depending on whether you use the IP Address or MAC Address in step 1.

4. Click the ->Project button to send the settings to the project.

Associate the Scanner and Controller and Download the DeviceNet Network Configuration

To allow the scanner and the controller to communicate you can associate their configurations using the Automatically Update Signals feature or you can manually manage the association. Both options are found on the GuardPLC tab of the Scanner Properties page in RSNetWorx for DeviceNet.

TIP We recommend using the Automatically Update Signals feature because it eliminates the need to manually import signals and export connections after every configuration change.

Once you've made the association between the scanner and controller, download the DeviceNet network configuration.

This chapter covers:

- the Scanner Signals File
- the Target Connections File
- the Automatically Update Signals procedure
- the manual association procedure
- downloading the DeviceNet network configuration

Scanner Signals File

The Scanner Signals File (.ssf) contains standard and safety level input and output data. RSNetWorx for DeviceNet creates a Scanner Signals File to define the layout of the data tables exchanged with the controller via HSP, including detailed signal information[1] and the HSP Signature. The data table contents include the data areas allocated to the DeviceNet I/O nodes to which the scanner connects, as well as data areas allocated to RSLogix Guard PLUS! application signals that are identified in the controllers Target Connections file (.tcf) and made available to DeviceNet peers that connect to the scanner.

[1] Not all standard I/O devices may provide these detailed I/O assembly definitions. Contact your device vendor for updated EDS files.

Standard devices that do not support these detailed I/O assembly definitions may include an UNKNOWN data type. Use the Define Data button on the Standard Data, Signal Connections screen in RSLogix Guard PLUS! to define these data types.

The Scanner Signals File separates data transferred on safety connections from data transferred over standard connections.

Signals created in the RSLogix Guard PLUS! Signal Editor can be assigned to scanner I/O data signals, allowing them to be used by the GuardPLC application logic.

Target Connections File

RSLogix Guard PLUS! generates the Target Connections File (.tcf) to inform RSNetWorx for DeviceNet which application signals should be exposed on the scanner's DeviceNet slave mode or target interfaces. As described in the Scanner Signals Files section, RSNetWorx for DeviceNet chooses locations for these target signals within the data tables that are exchanged over the HSP connection. See 'How Data Tables Work' on page 1-4 for more information on how safety and standard data is organized in a GuardPLC system that uses the safety scanner.

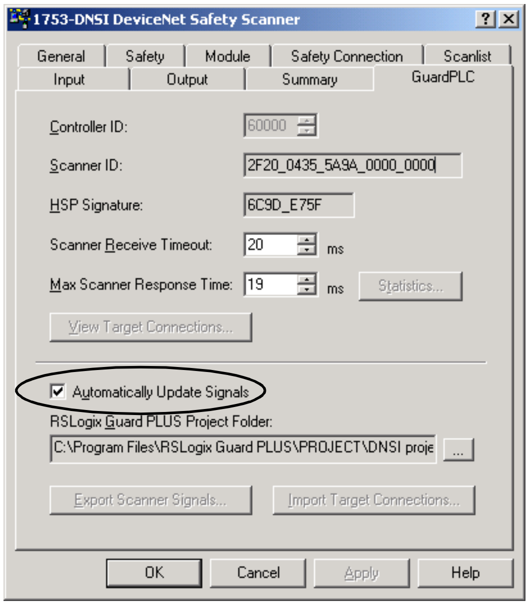
Automatically Update Signals

The simplest way to associate the 1753-DNSI and the GuardPLC controller is to select Automatically Update Signals on the safety scanner's GuardPLC tab. This option is only available when RSLogix Guard PLUS! and RSNetWorx for DeviceNet are installed on the same computer.

1. Open the Device Properties dialog by double-clicking on the scanner you want to associate.

2. Select the GuardPLC tab.

3. Select the Automatically Update Signals option.



1753-DNSI DeviceNet Safety Scanner
? X
General
Safety
Module
Safety Connection
Scanlist
Input
Output
Summary
GuardPLC
Statistics...
View Target Connections...
...
Export Scanner Signals...
Import Target Connections...
OK
Cancel
Apply
Help

Controller ID: 60000

Scanner ID: 2F20_0435_5A9A_0000_0000

HSP Signature: 6C9D_E75F

Scanner Receive Timeout: 20 ms

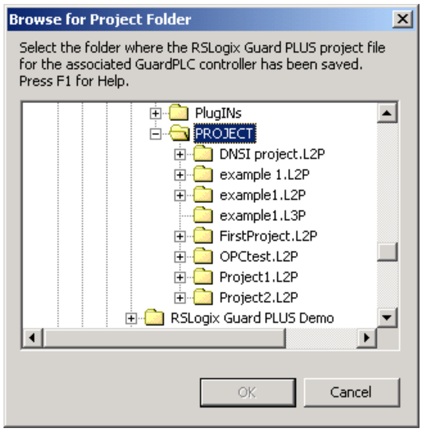
Max Scanner Response Time: 19 ms

☑ Automatically Update Signals

RSLogix Guard PLUS Project Folder: C:\Program Files\RSLogix Guard PLUS\PROJECT\DNSI proje

4. Select your RSLogix Guard PLUS! project.

   a. If you have multiple RSLogix Guard PLUS! projects, use care to select the correct one.

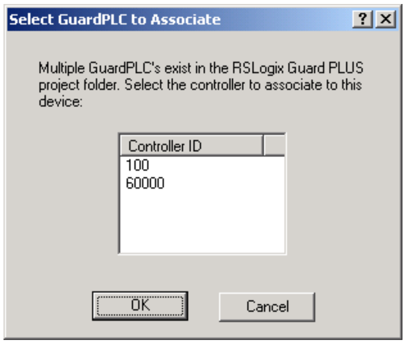


Browse for Project Folder

Select the folder where the RSLogix Guard PLUS project file for the associated GuardPLC controller has been saved. Press F1 for Help.

TIP	Only RSLogix Guard PLUS! projects that have at least one resource with HSP communications enabled can be selected.

   b. If you have multiple controller resources in your RSLogix Guard PLUS! project, RSNetWorx prompts you to select the correct resource.



Select GuardPLC to Associate

Multiple GuardPLC's exist in the RSLogix Guard PLUS project folder. Select the controller to associate to this device:

Controller ID
100
60000

5. RSNetWorx for DeviceNet automatically updates the Controller ID and imports the Target Connections File from the associated RSLogix Guard PLUS! project.

6. Click OK to establish the association.

Whenever the safety scanner configuration changes, RSNetWorx for DeviceNet automatically generates or updates the Scanner Signals file.

TIP	If RSLogix Guard PLUS! is open to the associated project, then it automatically imports the Scanner Signals file.

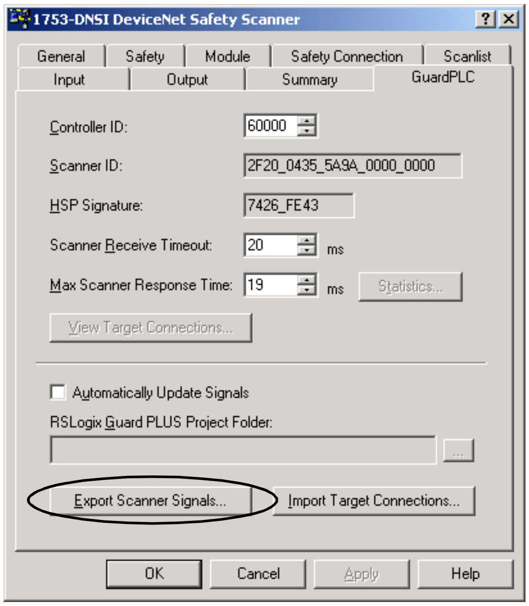
Manually Associate the Scanner and Controller

If you manually associate the scanner and controller, you must repeat this procedure whenever you make a change to the DeviceNet connections.

To manage the association between the safety scanner and the GuardPLC controller manually:

1. On the GuardPLC tab of the Device Properties dialog, verify that the Controller ID matches the GuardPLC controller to which you want the scanner associated.

2. Click on the Export Scanner Signals… button.


1753-DNSI DeviceNet Safety Scanner
General
Safety
Module
Safety Connection
Scanlist
Input
Output
Summary
GuardPLC
Statistics...
View Target Connections...
...
Export Scanner Signals...
Import Target Connections...
OK
Cancel
Apply
Help

Controller ID: 60000

Scanner ID: 2F20_0435_5A9A_0000_0000

HSP Signature: 7426_FE43

Scanner Receive Timeout: 20 ms

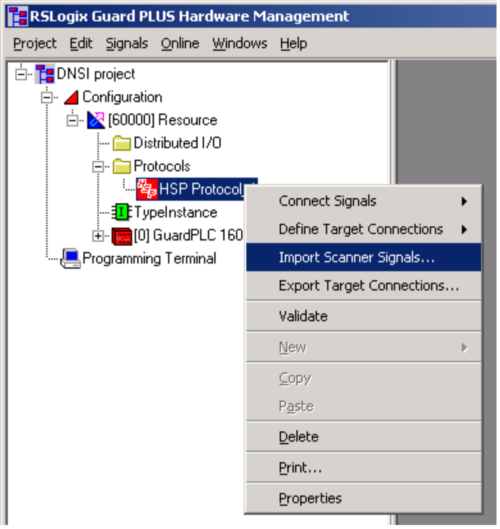
Max Scanner Response Time: 19 ms

□ Automatically Update Signals

RSLogix Guard PLUS Project Folder:

3. Save the Scanner Signals file. The Scanner Signal file's extension is .ssf.

4. Import the Scanner Signals file into your GuardPLC project.
   a. In RSLogix Guard PLUS! Hardware Management, right-click on the instance of the HSP protocol for your GuardPLC controller resource and select Import Scanner Signals…



   b. Browse to the correct .ssf file and select Open.

Download the DeviceNet Network Configuration

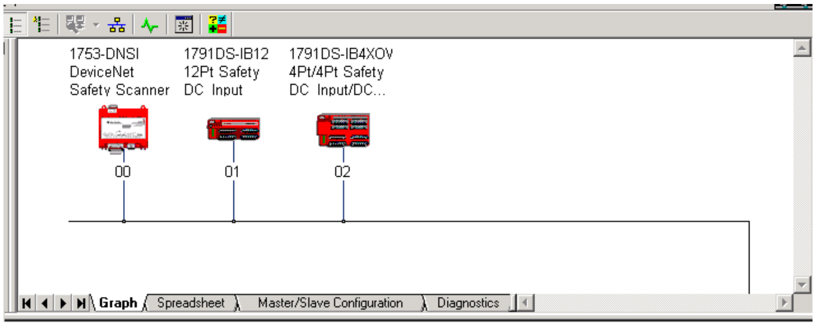
Before you download, you must go online to the DeviceNet network using RSNetWorx for DeviceNet. Your computer and the devices you wish to communicate with must be connected to the DeviceNet network.

When you go online to a DeviceNet network, RSNetWorx for DeviceNet 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.

1. Go online by selecting the online button.

2. Browse to the DeviceNet network and click OK at the prompt.



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

Safety Attribute	Description
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 4-5 for information on resolving an SNN mismatch error.
Configuration Signature	RSNetWorx for DeviceNet 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 selecting the device and choosing Download to Device from the Device menu or by right-clicking on the device and selecting Download to Device.

4. Confirm your intent to download by clicking Yes.

   If a device is password-protected, RSNetWorx for DeviceNet prompts you to enter 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 select 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.

Develop Your GuardPLC Application

To define your application signals and use them in your program logic, follow the procedures listed below in order:

Procedure	page
1. Define Signals for Your GuardPLC Application	8-1
2. Create Application Program Logic	8-4
3. Save and Compile Application Logic	8-4
4. Download the Project to the Controller	8-4

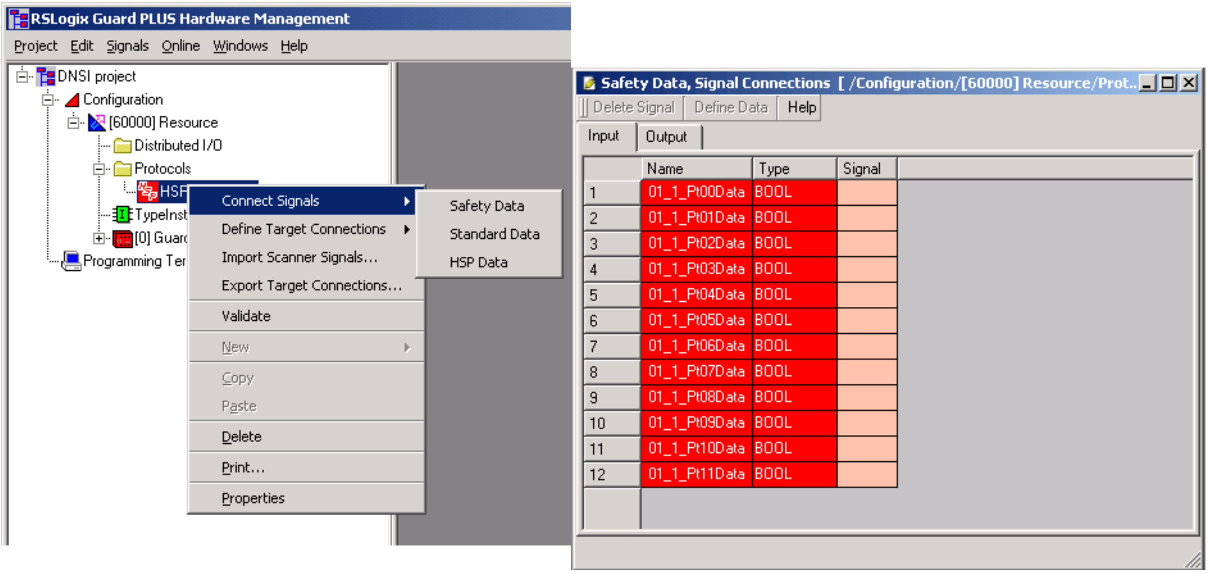
Define Signals for Your GuardPLC Application

Once the association between the scanner and controller is established, you can configure signals which allow you to use the safety or standard data in your GuardPLC application.

Review the guidelines for creating a distinction between safety and standard signals on page 1-4.

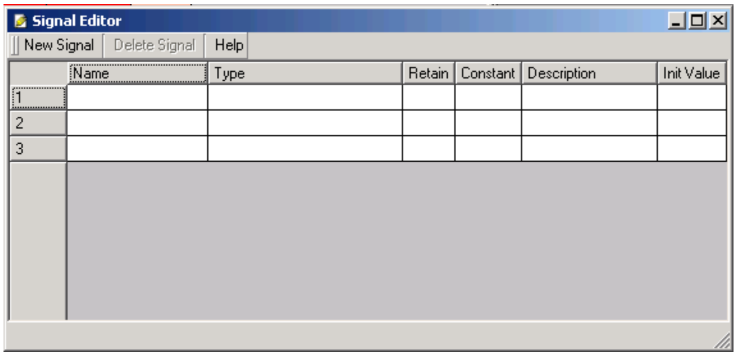
Define Signals for Safety Data

1. In your RSLogix Guard PLUS! project, right-click on the HSP icon and choose Connect Signals > Safety Data.



	Name	Type	Signal
1	01_1_Pt00Data	BOOL	
2	01_1_Pt01Data	BOOL	
3	01_1_Pt02Data	BOOL	
4	01_1_Pt03Data	BOOL	
5	01_1_Pt04Data	BOOL	
6	01_1_Pt05Data	BOOL	
7	01_1_Pt06Data	BOOL	
8	01_1_Pt07Data	BOOL	
9	01_1_Pt08Data	BOOL	
10	01_1_Pt09Data	BOOL	
11	01_1_Pt10Data	BOOL	
12	01_1_Pt11Data	BOOL	

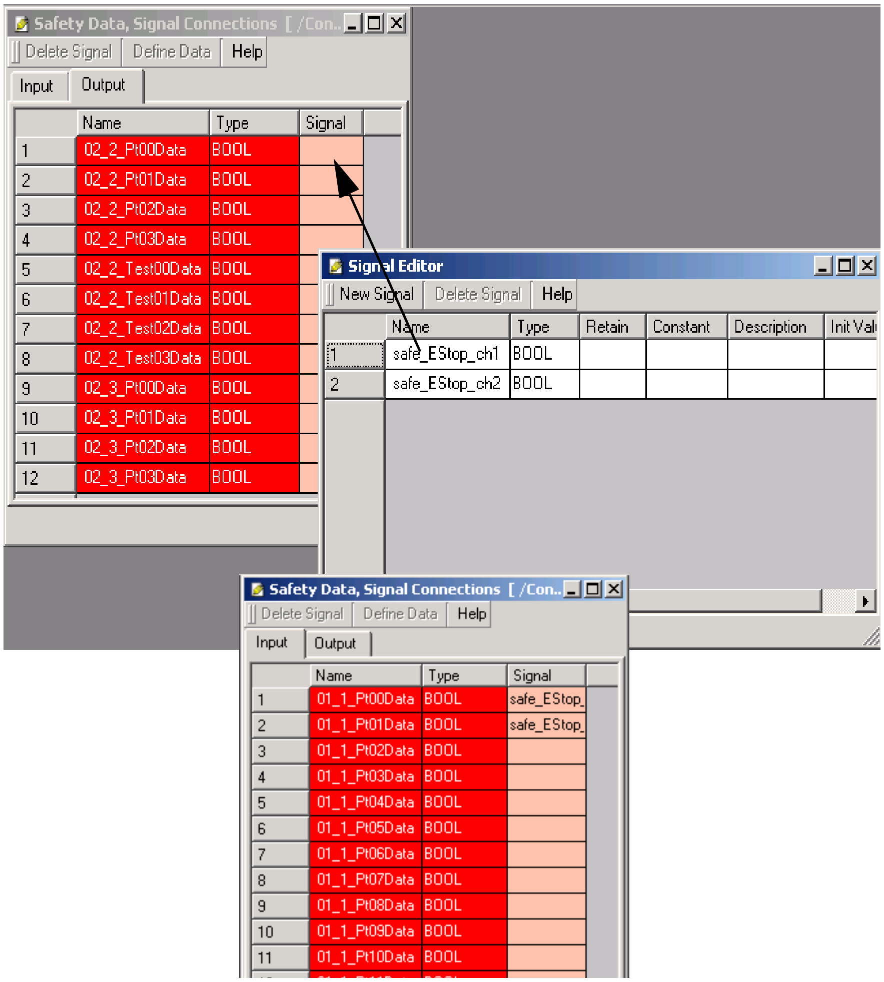
2. Open the Signal Editor by selecting Editor from the Signals menu.



	Name	Type	Retain	Constant	Description	Init Value
1						
2						
3						

3. Create a new signal by selecting New Signal or clicking in an empty signal Name field.

4. With the Safety Data, Signal Connections dialog visible and the Signal Editor dialog open, drag your application signals to the desired device data signals.



	Name	Type	Signal
1	02_2_Pt00Data	BOOL	
2	02_2_Pt01Data	BOOL	
3	02_2_Pt02Data	BOOL	
4	02_2_Pt03Data	BOOL	
5	02_2_Test00Data	BOOL	
6	02_2_Test01Data	BOOL	
7	02_2_Test02Data	BOOL	
8	02_2_Test03Data	BOOL	
9	02_3_Pt00Data	BOOL	
10	02_3_Pt01Data	BOOL	
11	02_3_Pt02Data	BOOL	
12	02_3_Pt03Data	BOOL	

	Name	Type	Retain	Constant	Description	Init Val
1	safe_EStop_ch1	BOOL				
2	safe_EStop_ch2	BOOL				

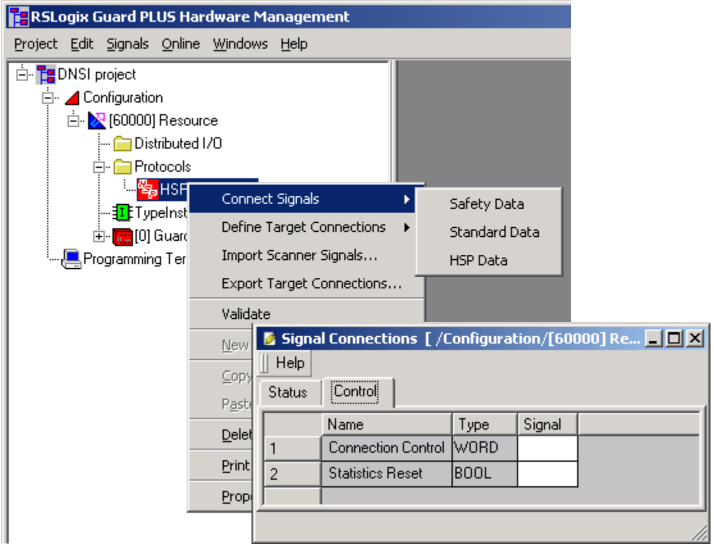
	Name	Type	Signal
1	01_1_Pt00Data	BOOL	safe_EStop_
2	01_1_Pt01Data	BOOL	safe_EStop_
3	01_1_Pt02Data	BOOL	
4	01_1_Pt03Data	BOOL	
5	01_1_Pt04Data	BOOL	
6	01_1_Pt05Data	BOOL	
7	01_1_Pt06Data	BOOL	
8	01_1_Pt07Data	BOOL	
9	01_1_Pt08Data	BOOL	
10	01_1_Pt09Data	BOOL	
11	01_1_Pt10Data	BOOL	

Configure HSP Connection

The safety scanner closes the HSP connection whenever either an HSP error occurs or the safety scanner diagnostic reports an error. Individual DeviceNet safety or standard connection errors do not cause the HSP connection to close. In the case of a faulted DeviceNet connection, any input data associated with that connection is forced to zero before being transmitted to the GuardPLC controller over HSP.

Your GuardPLC application logic can control the operation of the HSP connection, by writing a value to the signal associated with the HSP Connection Control Word.

To connect a signal to the HSP Connection Control Word, right-click on your HSP protocol in the RSLogix Guard PLUS! Hardware Management window and choose Connect Signals>HSP Data.


RSLogix Guard PLUS Hardware Management
Project Edit Signals Online Windows Help
DNSI project
Configuration
[60000] Resource
Distributed I/O
Protocols
HSP
TypeInst
[0] Guard
Programming Ter
Connect Signals
Define Target Connections
Import Scanner Signals...
Export Target Connections...
Validate
New
Copy
Paste
Delete
Print
Prop
Safety Data
Standard Data
HSP Data
Signal Connections [/Configuration/[60000] Re...
Help
Status
Control

	Name	Type	Signal
1	Connection Control	WORD	
2	Statistics Reset	BOOL	

The following table describes the possible mode settings for the HSP connection.

Connection Control Word Value	Mode	Description
0x8000	Disabled	HSP communication disabled.
0	Autoconnect	If communication is lost, open it automatically in the next cycle.
0x100	Toggle_Mode_0	If the connection is lost, do not reopen it until Toggle_Mode_1 is written.
0x101	Toggle_Mode_1	If the connection is lost, do not reopen it until Toggle_Mode_0 is written.

Create Application Program Logic

Create application program logic using the signals you defined.

Drag and drop the application signals, which are now connected (mapped) to DeviceNet data signals, into the appropriate application Type Instances and create your program logic.

Save and Compile Application Logic

Save and compile your application logic.

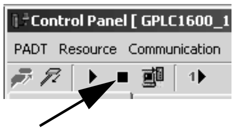
Compiling the application logic and controller hardware configuration results in a high-integrity computation of the HSP signature.

Refer to the GuardPLC Controller Systems User Manual, publication number 1753-UM001, for details on creating, saving, and compiling program logic.

Download the Project to the Controller

Place the Controller in Stop Mode (if necessary)

Before you can download to the GuardPLC controller, the controller must be in Stop mode. In RSLogix Guard PLUS! Hardware Management, left-click on the stop icon on the Control Panel and confirm the action by selecting Yes to the warning prompt.



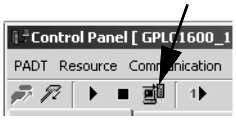
Download the Project

In RSLogix Guard PLUS! Hardware Management:

1. Right-click on the controller resource.
2. Select Online > Control Panel.
3. Fill in your user name and password on the login screen. The default username is Administrator with no password. Click OK.

TIP Enter Ctrl-A to automatically fill in the default username and access type.

4. Click the download icon and confirm the action by selecting Yes to the warning prompt.



TIP If this is the first time the application has been downloaded, you may want to adjust the timing parameters artificially high and allow the project to run for several hours. This lets you gather statistics on the system's operation before refining the timing parameters.

Set this parameter	Using
Controller Resend Timeout	RSLogix Guard PLUS! Hardware Management
Controller Receive Timeout	
Communications Time Slice	
Watchdog Time	
Safety Time	
Scanner Receive Timeout	RSNetWorx for DeviceNet
Max. Scanner Response Time	
Individual Safety/Standard connection Timing parameters	

Verify Your DeviceNet Safety Configuration

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

Refer to the GuardPLC Controller Systems Safety Reference Manual, publication number 1753-RM002 for information on verification testing for safety applications.

The Safety Device Verification Wizard, accessed from RSNetWorx for DeviceNet, 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 configuration file. The configuration is displayed in a report to facilitate visual verification and record keeping.

IMPORTANT Some devices 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

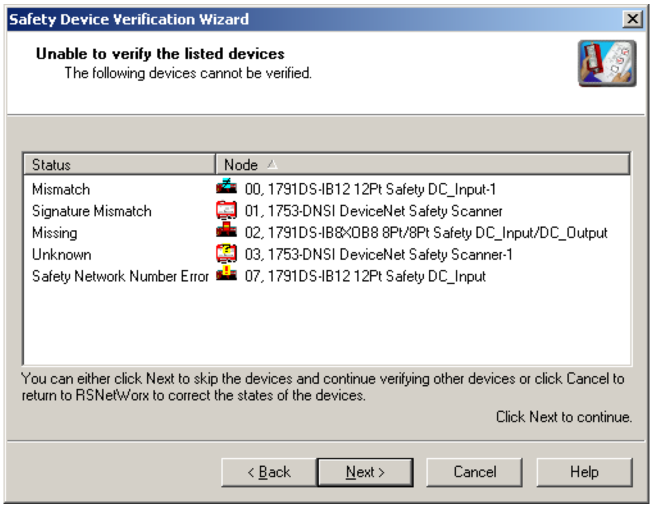
To run the Safety Device Verification Wizard, select Network > Safety Device Verification Wizard. The Welcome page, which describes the verification process, appears.

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



Unable to verify the listed devices

The following devices cannot be verified.

Status	Node
Mismatch	00, 1791DS-IB12 12Pt Safety DC_Input-1
Signature Mismatch	01, 1753-DNSI DeviceNet Safety Scanner
Missing	02, 1791DS-IB8XOB8 8Pt/8Pt Safety DC_Input/DC_Output
Unknown	03, 1753-DNSI DeviceNet Safety Scanner-1
Safety Network Number Error	07, 1791DS-IB12 12Pt Safety DC_Input

You can either click Next to skip the devices and continue verifying other devices or click Cancel to return to RSNetWorx to correct the states of the devices.

Click Next to continue.

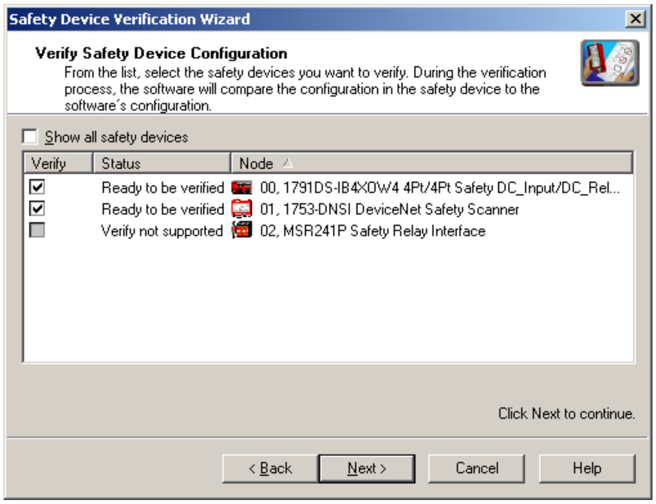
Status	Icon Overlay	Description
Missing	⛔	The device is part of the network configuration, but was not found during the browse operation.
Mismatch	≠	The device identity in the network configuration does not match the identity of the online device.
Unknown	?	The device is in the configuration, but has not been detected on the network yet.
Safety Network Number Error	!	The Safety Network Number in the device is either invalid or does not match the Safety Network Number 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 so that you can correct the status of the indicated devices, close the Safety Device Verification Wizard by clicking on 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 using the checkboxes in the Verify column of the Verify Safety Device Configuration dialog. You can select only the devices whose status is ‘Ready to be verified’.



Safety Device Verification Wizard

Verify Safety Device Configuration

From the list, select the safety devices you want to verify. During the verification process, the software will compare the configuration in the safety device to the software´s configuration.

☐ Show all safety devices

Verify	Status	Node
☑	Ready to be verified	00, 1791DS-IB4XOW4 4Pt/4Pt Safety DC_Input/DC_Rel...
☑	Ready to be verified	01, 1753-DNSI DeviceNet Safety Scanner
☐	Verify not supported	02, MSR241P Safety Relay Interface

Click Next to continue.

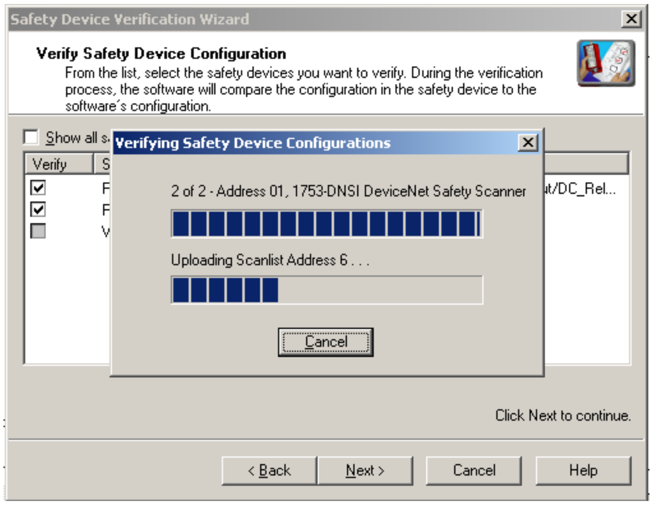
If the Show all safety devices checkbox is checked, the dialog lists all of the safety devices on the network and shows their current status. If it is unchecked, which is the default, only devices with the following status are shown:

- Verify FAILED
- Ready to be verified
- Verify not supported

These states are described in the following table.

Status	Description
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 on Next to begin the upload and compare process.



Safety Device Verification Wizard

Verify Safety Device Configuration

From the list, select the safety devices you want to verify. During the verification process, the software will compare the configuration in the safety device to the software's configuration.

Verifying Safety Device Configurations

2 of 2 - Address 01, 1753-DNSI DeviceNet Safety Scanner

Uploading Scanlist Address 6 . . .

Click Next to continue.

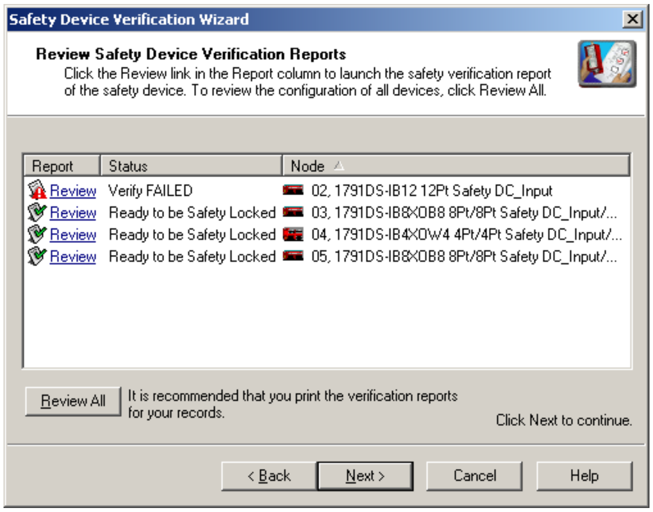
TIP

If you click on 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 page listing those devices
devices are ready to be Safety-Locked	the Lock page listing those devices
no devices were verified	the Finish page
no devices are ready to be Safety-Locked	the Finish page

Review the Safety Device Verification Reports

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



Review Safety Device Verification Reports

Click the Review link in the Report column to launch the safety verification report of the safety device. To review the configuration of all devices, click Review All.

Report	Status	Node
Review	Verify FAILED	02, 1791DS-IB12 12Pt Safety DC_Input
Review	Ready to be Safety Locked	03, 1791DS-IB8XOB8 8Pt/8Pt Safety DC_Input/...
Review	Ready to be Safety Locked	04, 1791DS-IB4XOW4 4Pt/4Pt Safety DC_Input/...
Review	Ready to be Safety Locked	05, 1791DS-IB8XOB8 8Pt/8Pt Safety DC_Input/...

It is recommended that you print the verification reports for your records.

Click Next to continue.

1. Click on the Review hyperlink in the Report column to launch the device’s HTML report in your default browser.

2. Click the Review All button 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.

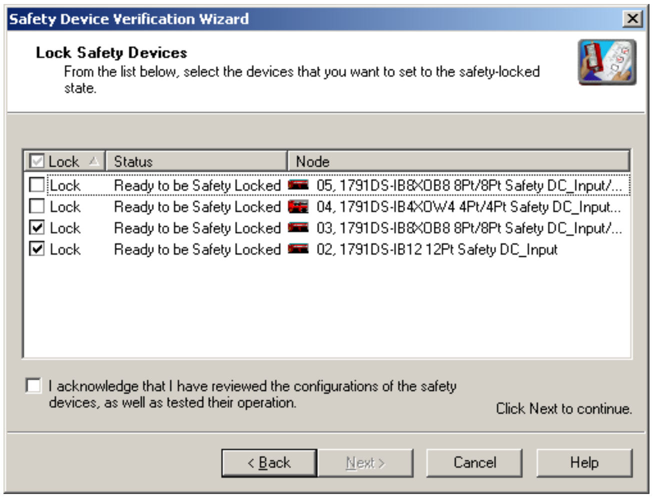
3. Review and print the verification reports for your records.

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 selecting the checkbox in the Lock column for each device that is ready to be Safety-Locked.



Safety Device Verification Wizard

Lock Safety Devices

From the list below, select the devices that you want to set to the safety-locked state.

☑ Lock	Status	Node
□ Lock	Ready to be Safety Locked	05, 1791DS-IB8XOB8 8Pt/8Pt Safety DC_Input/...
□ Lock	Ready to be Safety Locked	04, 1791DS-IB4XOW4 4Pt/4Pt Safety DC_Input...
☑ Lock	Ready to be Safety Locked	03, 1791DS-IB8XOB8 8Pt/8Pt Safety DC_Input/...
☑ Lock	Ready to be Safety Locked	02, 1791DS-IB12 12Pt Safety DC_Input

□ I acknowledge that I have reviewed the configurations of the safety devices, as well as tested their operation.

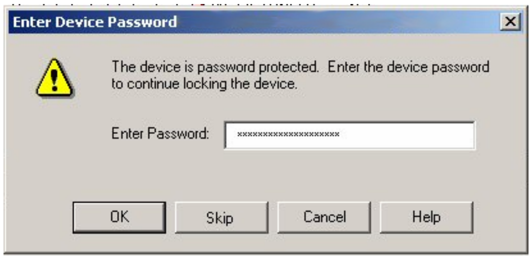
Click Next to continue.

2. You must check the acknowledgement box before the locking process can continue.

3. Click Next.

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

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



Enter Device Password

The device is password protected. Enter the device password to continue locking the device.

Enter Password: xxxxxxxxxxxxxxxxxxxx

If you want to skip the device and allow the locking process to continue for other devices, click on 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 on Finish to close the wizard.

Monitor Status

To assist you in monitoring the status of devices on the DeviceNet Safety network, the DeviceNet Safety Scanner provides:

- LED status indicators
- an alphanumeric status display.

You can also monitor the status of HSP, DeviceNet Safety and standard connections, and the DeviceNet interface via connection status bits and the corresponding GuardPLC application signals.

LED Status Indicators

The scanner has 3 LEDs which allow you to monitor module, DeviceNet network, and High Speed Protocol (HSP) status.

LED	Color/State	Description
Module Status	Off	No power.
	Green, On	Operating under normal conditions.
	Green, Flashing	Device is Idle.
	Red, Flashing	A recoverable fault exists.
	Red, On	An unrecoverable fault exists.
	Red/Green, Flashing	Self-tests in progress or the device needs commissioning due to configuration or unique node identifier missing, incomplete, or incorrect.
Network Status	Off	Device is not online or may not have DeviceNet network power.
	Green, On	Device is online; one or more connections are established.
	Green, Flashing	Device is online; no connections established.
	Red, Flashing	Communication timeout.
	Red, On	Communication failure. The device has detected an error which has prevented network communication.
	Red/Green, Flashing	The SNN is being set.

LED	Color/State	Description
HSP Status	Off	The module has not received any messages on the serial interface.
	Green, On	The module is transmitting data over the serial communication interface.
	Green, Flashing	The serial interface is ready for communication, but the controller is sending messages that do not match the safety scanner's current configuration.
	Red, Flashing	The connection to the controller was lost after being established at least once since power up.

Alphanumeric Display

At Power Up

When you apply power to the 1753-DNSI safety scanner, check the scanner's alphanumeric display to determine if the module is operating properly. It displays the following:

- firmware revision
- MAC ID
- DeviceNet communication rate

During Operation

Following power up, the alphanumeric display on the safety scanner displays the following information:

Display	Description
A#xx	'xx' is the MAC ID of the scanner. A status string follows.
IDLE	The scanner is in idle mode.
RUN	The scanner is in run mode.
Duplicate Node Failure	The address of the scanner is already in use by another device on the network. Change the address to an unused address.

Display	**Description**
Bus Off Detected	A bus off condition (communication problem) exists. 1. Cycle power to the device or disconnect and reconnect the DeviceNet cable. 2. Make sure all devices are at the same communication rate. 3. Make sure a short-circuit does not exist between the CAN line and a power or shield line. 4. Check for any of the following sources of noise: • Close proximity to a high voltage power cable • Improper or no termination resistor • Improper grounding 5. Check for a device that is producing noise or inappropriate data on the network.
No Network Power	The DeviceNet cable is not supplying power to the communication port. Make sure the network has 24V dc power. Check the connection to the scanner.
Faulted, must issue Safety Reset	The scanner encountered an internal critical fault. 1. Issue a Safety Reset and download the configuration using RSNetWorx for DeviceNet. 2. If the problem continues to occur, the safety scanner may need to be replaced. Contact your Rockwell Automation representative.
NVS Xfer Main	The module is in the process of having its non-volatile memory updated. The new image for the main processor is currently being transferred to the module.
NVS Xfer Peer	The module is in the process of having its non-volatile memory updated. The new image for the peer processor is currently being transferred to the module.
Main Save	The new non-volatile memory image for the main processor has been transferred and is now being saved to memory.
Peer Save	The new non-volatile memory image for the peer processor has been transferred and is now being saved to memory.
NoRx	No direct traffic for the scanner has been detected. This can be caused by not having a scanlist entered in the scanner, or simply that the scanner has not received communication from any other device. See status codes 75 and 76 on page 10-4.
NoTx	The scanner has failed to transmit a message. See Status code 79 on page 10-4.
N#xx	Another device has a problem, where ‘xx’ is the node address of the device. • For safety connections, the status code ‘S#ee’ or extended error code ‘G#gg<:nnnn>’ follows. • For standard connections, the status code ‘E#ee’ follows.

Display	Description
S#ee	Status code for safety connections, where 'ee' is the decimal error code listed on page 10-4.
G#gg<:nnnn>	Extended error code for safety connections, where: • 'gg' indicates the hexidecimal general status error code as listed in the Safety Connection General Status Error Codes table on page 10-5, and • 'nnnn' indicates the hexidecimal extended error code as listed in the table Safety Connection Extended Error Codes on page 10-7.
E#ee	Status code for standard connections, where ee is the decimal error code listed in the Status Codes table on page 10-4.

Status Codes

Status Code (ee)	Description	Recommended Action
70	The address of the device is already in use by another device on the network.	Change the address of the device to an unused address.
71	Illegal data in scan list.	Reconfigure the scan list and remove any illegal data.
72	*No* communication with the device.	Inspect the device and verify connections.
73	Device's identity information does not match electronic key in scanner	• Make sure that the correct device is at this address. • Make sure that the device matches the specified electronic key (vendor, product code, product type).
75	Either or both of the following: • The device does *not* have a scan list. • The device has *not* received communication from any other device	Check that the device has: • scan list • properly wired connection to the network
76	No direct network traffic for scanner.	None. The scanner hears other network communication but does **not** hear any directed to it.
77	During initialization, the data size expected by the device does *not* match the scan list entry.	Check the device and the scan list for the correct input and output size for the device.
78	Device is *not* communicating or communication is intermittent.	• Check that the device has a properly wired connection to the network. • Check that the device has power. • If the device is polled, make sure the interscan delay is long enough for the device to return its data.
79	Scanner has failed to transmit a message.	• Make sure that your scanner is connected to a valid network. • Check for disconnected cables.
80	Scanner is in idle mode.	1. Put controller in run mode. 2. Make sure 1753-CBLDN is connected properly. 3. Make sure the scanner and the controller have the same HSP signature.

Status Code (ee)	Description	Recommended Action
82	Error detected in sequence of fragmented I/O messages from device.	• Check scan list device to make sure that its input and output data sizes are correct. • Check the configuration of the device.
83	Device returns error responses when the scanner attempts to communicate with it.	• Check the accuracy of the scan list. • Check the configuration of the device. The device may be in another scanner's scan list. • Cycle power to the device.
84	Scanner is initializing the DeviceNet network.	None. This code clears itself once the scanner attempts to initialize all the devices on the network.
85	During runtime, the device is sending the wrong size of data.	Contact Rockwell Automation support. See the back of this publication.
86	Device is in idle state/mode (*not* producing data) while the scanner is in run mode.	• Check the configuration and status of the device. • If you set up an interlock between 2 scanners (controllers), make sure both scanners are in run mode.
92	The DeviceNet cable is *not* supplying power to the communication port.	• Make sure the network has 24V dc power. • Check the connection to the device.
95	The firmware of the device is currently being updated.	None. Do not disconnect the device while the update is in progress. You will lose any existing data in the device's memory.

Safety Connection General Status Error Codes

General Status Error Code (00gg)	Description
0001	Connection failure occurred. See the extended error codes on pages 10-7 to 10-8.
0002	Resources required for the requested services were unavailable.
0003	Invalid value.
0004	Internal Object Identifier syntax error. See the extended error codes on pages 10-7 to 10-8.
0005	Destination unknown, class unsupported, instance undefined, or structure element undefined. See the extended error codes on pages 10-7 to 10-8.
0006	Packet space is insufficient.
0007	Connection was lost.
0008	Service is unsupported.
0009	An error occurred in a data segment or an attribute value is invalid.
000A	Attribute list error occurred.
000B	This state already exists.
000C	Object state conflict occurred.
000D	This object already exists.
000E	Attribute is not settable.

General Status Error Code (00gg)	Description
000F	Permission denied. See the extended error codes on pages 10-7 to 10-8.
0010	Device state conflict occurred.
0011	Reply will not fit.
0012	Fragmentation of a primitive value. For example, the service specified an operation that is going to fragment a primitive data value, such as half a REAL data type.
0013	Command data is insufficient.
0014	Attribute is not supported.
0015	Too much data present.
001A	Bridge request is too large.
001B	Bridge response is too large.
001D	Attribute list is invalid.
001E	Embedded service error occurred.
001F	Connection related failure occurred. See the extended error codes on pages 10-7 to 10-8.
0022	Invalid reply received.
0025	Key segment error occurred.
0026	Path size is invalid. Either the size of the path was not large enough, or too much data was included.
0027	An unexpected attribute was encountered in the list.
0028	DeviceNet error, member ID is invalid.
0029	DeviceNet error, member is not settable.
00D1	The module is not in the run state.
00FB	The message port is not supported.
00FC	The message data type is unsupported.
00FD	The message is uninitialized.
00FE	The message has timed out.
00FF	A general error occurred. See the extended error codes on pages 10-7 to 10-8.

Safety Connection Extended Error Codes

General Status Error Code (00gg)	Extended Error Code (nnnn)	Description
0001	0100	The connection is in use.
0001	0103	Transport is not supported.
0001	0106	Ownership conflict occurred.
0001	0107	The connection was not found.
0001	0108	Connection type is invalid.
0001	0109	Connection size is invalid.
0001	0110	The module is not configured.
0001	0111	Expected Packet Rate value is not supported.
0001	0114	This is the wrong module.
0001	0115	Device type is incorrect.
0001	0116	Module revision is incorrect.
0001	0118	The configuration format is invalid.
0001	011A	The application is out of connections.
0001	0203	The connection has timed out.
0001	0204	An unconnected message has timed out.
0001	0205	Unconnected send parameter error occurred.
0001	0206	The message is too large.
0001	0301	There is no buffer memory.
0001	0302	Bandwidth is not available.
0001	0303	Dynamic I/O resources are not sufficient.
0001	0305	Signatures match.
0001	0311	The port is not available.
0001	0312	A link address is not available.
0001	0x0315	Safety Connection Type name is invalid (not equal to 0x50).
0001	0317	The connection is not scheduled.
0001	0x0801	The RPI is not compatible with previously established multicast connections. All multi-cast consumers must request the same RPI.
0001	0x0802	Safety connection size is invalid.
0001	0x0803	Safety connection format is invalid.
0001	0x0805	Ping interval EPI multiplier was out of range (10 to 10000).
0001	0x0806	Time Coordination Message Minimum Multiplier was out of range (10 to 10000).
0001	0x0807	Time Expectation Multiplier was out of range (0 to 42969).
0001	0x080A	CPCRC value in Safety Open and calculated CPCRC value.
0001	0x080B	Time Correction Connection ID is invalid.
0001	0x080C	Configuration Signatures do not match. The Configuration Signature was non-zero and did not match the value in the target.

General Status Error Code (00gg)	Extended Error Code (nnnn)	Description
0001	0x080D	The target's unique node identifier was not set.
0001	0x080E	The target's unique node identifier does not match. The message was likely routed to this node in error.
0001	0x080F	The configuration operation was not allowed.
0004 0005	0000	Extended status is out of memory.
0004 0005	0001	Extended status is out of instances.
000F	0203	The connection has timed out.
00FF	2001	One or more of the system address segments that a device must interpret to direct a message to its destination object is excessive.
00FF	2002	A parameter value is bad.
00FF	2018	Semaphore reject occurred.
00FF	201B	Size is too small.
00FF	201C	Size is invalid.
00FF	2100	Privilege failure occurred.
00FF	2102	Password is invalid.
00FF	2103	No password was issued.
00FF	2104	The address is out of range.
00FF	2106	Data is in use.
00FF	2107	Type is invalid and not supported.
00FF	2108	The controller is in the upload and download mode.
00FF	2109	An attempt was made to change the number of array dimensions.
00FF	210A	The symbol name is invalid.
00FF	210B	The symbol does not exist.
00FF	210E	The search failed.
00FF	210F	The task cannot start.
00FF	2110	Unable to write.
00FF	2111	Unable to read.
00FF	2112	The shared routine is not editable.
00FF	2113	The controller is in fault mode.
00FF	2114	Run mode is inhibited.

Connection Status

You can monitor the HSP and DeviceNet Safety and standard connection status using the scanner's connection status bits and the related GuardPLC application signals as discussed in the following sections.

DeviceNet Connection Status Bit Behavior

The following table describes the combined operation of the DeviceNet connection status bits.

Connection Fault	Idle Mode	Safety Connection Operation	Standard Connection Operation
0 = Valid	0 = Run	Data is actively being controlled by the producing device. The producing device is in the Run mode.	
0 = Valid	1 = Idle	The connection is active and the producing device is in the Idle state. The safety data sent to the controller from this connection is reset to zero.	The connection is active and the producing node is in the Idle state. The data sent to the controller for this connection is 'hold last state'.
1 = Faulted	1 = Idle[1]	The connection is faulted. The state of the producing device is unknown. The safety data sent to the controller from this connection is reset to zero. A safety connection status bit is set to Faulted any time the connection is not established or not operating error-free.	Not applicable.
1 = Faulted	0 = Run[1]	Not applicable.	The connection is faulted. The state of the producing device is unknown. The data sent to the controller for this connection is reset to 0. At start up, the standard fault bit defaults to 0. If the first attempt to connect to the slave device is not successful, then the connection will be reported as faulted. When one or more of the standard connections to the slave node timeout, the corresponding fault bit is set. When all of the connections to a slave node are in the established state, the fault bit is set to 0. The fault bit for the slave-mode interface is not used; it is always 0.

[1] This value is meaningless when the Connection Fault bit is 1 (Faulted).

IMPORTANT The bits in the table above are only accurate if the HSP connection is established.

IMPORTANT As with any communications channel, you must use the connection status bits in your application program logic to achieve a SIL 3 system.

HSP Connection State Signal

The HSP connection status may be monitored via the HSP Protocol>Connect Signals>HSP Data>Connection State controller signal in RSLogix Guard PLUS! Hardware Management.

Signal	State of the Connection
Connection State	0 = closed. The active end point is not attempting to open the connection. 1 = try_open. The active endpoint is attempting to open the connection, but the connection is not yet open. 2 = connected. The connection is established and normal functions, such as data transfer and time monitoring, are occuring.

DeviceNet Safety Connection Status

The Safety connection fault and idle status tables are only available as signals in the RSLogix Guard PLUS! application. Each table is presented as a collection of 66 bits contained within 3 DWORD device signals, as shown in the following table. The left column shows the signal names as they appear in RSLogix Guard PLUS!.

_Safe_FaultTable_1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	Connection Number
_Safe_FaultTable_2	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	Connection Number
_Safe_FaultTable_3	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	RESERVED																														66	65	Connection Number
_Safe_IdleTable_1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	Connection Number

_Safe_IdleTable_2	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	Connection Number
_Safe_IdleTable_3	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	RESERVED																														66	65	Connection Number

User application logic only needs to consider status bits associated with connections present in the scanner's configuration. The list of configured connections can be obtained from the RSNetWorx for DeviceNet report feature by selecting File>Generate Report.

Standard DeviceNet Connection Status

The Faulted Node Table and Idle Node Table attributes of the Scanner Configuration Object (class 0x90) contain standard DeviceNet connection status information as described in the following table.

Name	Attribute	Data Type	Access	Attribute Value Description[1]
Faulted Node Table	0x10 a	Array of BOOL	Get	0 = The device is not faulted or is not configured. 1 = The device is faulted.
Idle Node Table	0x11 b	Array of BOOL	Get	0 = The device is not in Idle mode or the device is not configured. 1 = The Device is in Idle mode.

[1] The bit offset in the table corresponds to the node number. For example, bit 0 corresponds to node 0…bit 15 corresponds to node 15.

For nodes with more than one connection type enabled (that is, connections with both an input and output connection configured), the status bit reflects the logical 'OR' of the status for each configured connection.

User application program logic only needs to consider status bits associated with nodes that have one or more connections. The status bits of nodes without any connections may be ignored. The list of configured connections can be obtained from the RSNetWorx for DeviceNet report feature by selecting File>Generate Report.

Connection Status Signals

Each standard status table is presented as a collection of 64 bits, contained within 2 DWORD device signals, as shown in the table below. The left column shows the signal names as they appear in RSLogix Guard PLUS!.

_Std_FaultTable_1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Node Address
_Std_FaultTable_2	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	Node Address
_Std_IdleTable_1	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Node Address
_Std_IdleTable_2	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit Position
	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	Node Address

DeviceNet Interface Status

The DeviceNet Interface Status bits provide general status information for the scanner's DeviceNet Interface, as described in the table below.

Status Bit	Data Type	Attribute Value Description
Communications Failure	BOOL	0 = Normal 1 = Bus Off condition is present
DeviceNet Power Failure	BOOL	0 = Normal 1 = No DeviceNet power.
Duplicate MAC Failure	BOOL	0 = Normal 1 = Duplicate MAC Failure

Status Signals

The one WORD _DNet_StatusTable GuardPLC signal indicates the status of the DeviceNet interface as show in the following table.

_Dnet_StatusTable	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
	RESERVED													Dup Mac Fail	Power Fail	Comm Fail

Specifications

General

Dimensions (H x W x D)	90 mm$^{(2)}$ x 110 mm x 87 mm$^{(3)}$ (3.5 in.$^{(2)}$ x 4.33 in. x 3.43 in.$^{(3)}$)
Weight	400 kg (0.882 lb)
DeviceNet Current Load, Max.	90 mA maximum @ 24V dc
Power Consumption	10 W maximum (on external power connection)
Response Overload	shut down of the concerned output with cyclic reconnecting
Isolation Voltage	30V continuous Tested to withstand 500V dc for 60 seconds
HSP Cable	1753-CBLDN (ships with safety scanner)
Wire Type	Copper
Wiring Category[1]	2 - on power and communication ports

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

[2] Height does not include DIN rail latches or mounting feet.

[3] Depth does not include communication cable.

Environmental

Storage Temperature	-40°C to +85°C (-40°F to +185°F)
Operating Temperature	0°C to +60°C (+32°F to +140°F)
Relative Humidity	IEC 60068-2-30 (Test Db, Un-packaged Non-operating Damp Heat): 5% to 95% noncondensing
Vibration	IEC60068-2-6 (Test Fc, Operating): 2g at 10 to 500 Hz
Operating Shock	IEC60068-2-27 (Test Ea, Unpackaged Shock): 30g
Non-operating Shock	IEC60068-2-27 (Test Ea, Unpackaged Shock): 50g
Enclosure Type Rating	none (open-style)

Electrical/EMC

Emissions	CISPR 11: Group 1, Class A
ESD Immunity	IEC 61000-4-2: • 6 kV contact discharges • 8 kV air discharges
Radiated RF Immunity	IEC 61000-4-3: • 10V/m with 1 kHz sine-wave 80% AM from 30 MHz to 2000 MHz • 10V/m with 200 Hz 50% Pulse 100% AM at 900 MHz • 10V/m with 200 MHz 50% Pulse 100% AM at 1890 MHz • 3V/m with 1 kHZ sine-wave 80% AM from 2000 MHz to 2700 MHz
EFT/B immunity	IEC 61000-4-4: • ±2 kV at 5 kHz on power ports • ±2 kV at 5 kHz on communications ports
Surge Transient Immunity	IEC 61000-4-5: • ±1 kV line-line (DM) and ±2 kV line-earth (CM) on power ports • ±2 kV line-earth (CM) on communications ports
Conducted RF Immunity	IEC 61000-4-6: • 10Vrms with 1 kHz sine-wave 80% AM from 150 kHz to 80 MHz

Certifications

When marked, the components have the following certifications. See the Product Certification link at www.ab.com for Declarations of Conformity, Certificates, and other certification details.

Certification[1] (when product is marked)	**Description**
c-UL-us	UL Listed Industrial Control Equipment, certified for US and Canada
	UL Listed for Class I, Division 2 Group A,B,C,D Hazardous Locations, certified for US and Canada
CE	European Union 89/336/EEC EMC Directive, compliant with: • EN 61000-6-4; Industrial Emissions • EN 50082-2; Industrial Immunity • EN 61326; Meas./Control/Lab., Industrial Requirements • EN 61000-6-2; Industrial Immunity • EN61131-2; Programmable Controllers (Clause 8, Zone A, B, & C)
C-Tick	Australian Radiocommunications Act, compliant with: AS/NZS CISPR 11; Industrial Emissions
TÜV	Functional Safety: SIL 1 to 3, according to IEC 61508; Category 1 to 4, according to EN954-1; NFPA79; when used as described in the GuardPLC Controller Systems Safety Reference Manual, publication 1753-RM002.
ODVA	ODVA conformance tested to DeviceNet Safety specifications.

[1] See the Product Certification link at www.ab.com for Declarations of Conformity, Certificates, and other certifications details.

Configure Peer-to-Peer DeviceNet Communications

This appendix provides instructions on how to set up peer-to-peer communications to share application signals between two GuardPLC controller/1753-DNSI scanner pairs or to other standard masters or safety originators on the DeviceNet network.

IMPORTANT Complete the procedures in this chapter before making safety connections via the Safety Connections tab or standard connections via a scanlist in RSNetWorx for DeviceNet, steps 2 and 4 in Chapter 5.

Use the slave mode for standard connections to allow standard devices such as standard PLCs (ControlLogix, CompactLogix, SLC 500, and others) or HMIs to exchange data with the GuardPLC controller. Use the safety target interface for safety connections to allow multiple GuardPLC controllers to perform safety interlocking over DeviceNet.

To add peer-to-peer connections, follow the procedures listed below in order.

Procedure	page
1. Plan Your Peer-to-Peer Communications	B-2
2. Set Up Your DeviceNet Network	3-1
3. Commission a Peer Scanner	B-2
4. Create a GuardPLC Project with High-Speed Safety Protocol	6-1
5. Add a Peer Controller	B-3
6. Define Target Connections for Standard and Safety Data	B-4
7. Configure Peer-to-Peer Connections	B-8
8. Configure DeviceNet Nodes and Connections (non-peer-to-peer)	5-1
9. Associate the Scanner and Controller and Download the DeviceNet Network Configuration	7-1
10. Develop Your GuardPLC Application	8-1
11. Verify Your DeviceNet Safety Configuration	9-1

Plan Your Peer-to-Peer Communications

If your application requires peer-to-peer DeviceNet communications, you must:

- determine which RSLogix Guard PLUS! application signals each controller and scanner combination needs to make available to peer controllers, and
- determine whether the chosen signals should be made available on standard or safety connections.

Only the following data types are supported:

Type	Size in bits	Description
BOOL	1	true or false, on or off
USINT	8	unsigned byte
INT	16	signed word
UINT	16	unsigned word
DINT	32	signed double word
UDINT	32	unsigned double word
SINT	8	signed byte
REAL	32	float, IEC559 single precision format
LREAL	64	double, IEC559 double precision format
BYTE	8	string of 8 bits
WORD	16	string of 16 bits
DWORD	32	string of 32 bits

The next steps are to set up your DeviceNet Network as discussed in Chapter 3.

Commission a Peer Scanner

1. Connect the scanner to the network following the installation instructions in Chapter 2.

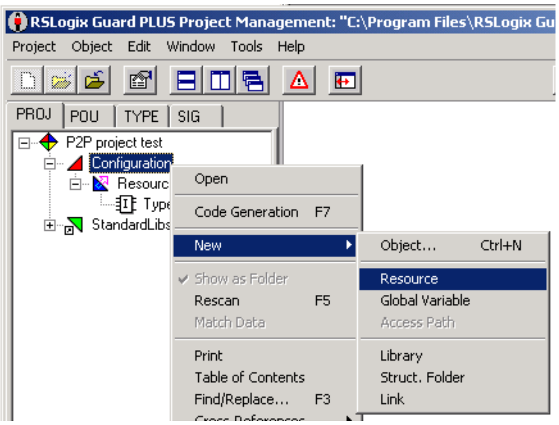
2. Commission the scanner, following the instructions in Chapter 3 to set the node address, baud rate, SNN, and password, if desired.

The next step is to create a GuardPLC controller resource with HSP protocol as described in Chapter 6.

Add a Peer Controller

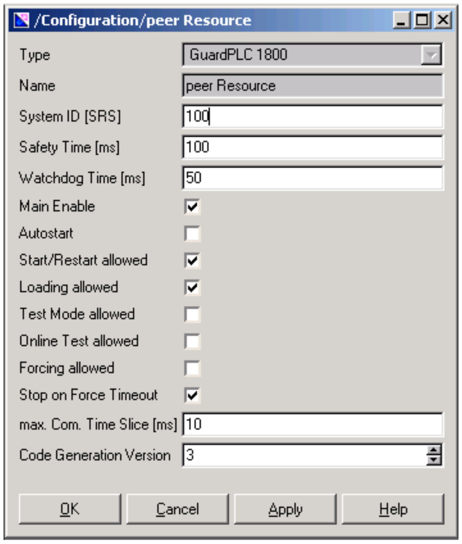
To add a peer controller Resource to the project:

1. In RSLogix Guard PLUS! Project Management, right-click on Configuration and select New>Resource.



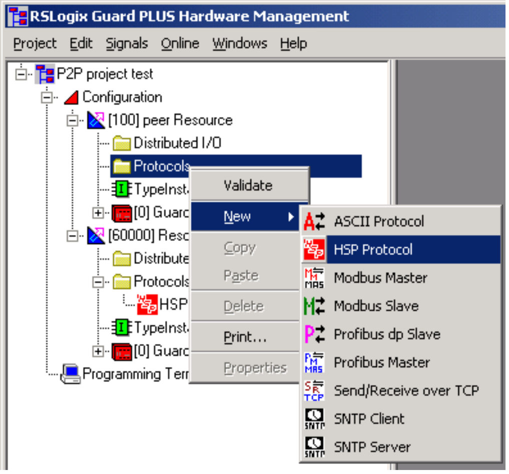
2. Name the resource.

3. In RSLogix Guard PLUS! Hardware Management, configure the resource properties by right-clicking on the resource and selecting Properties.

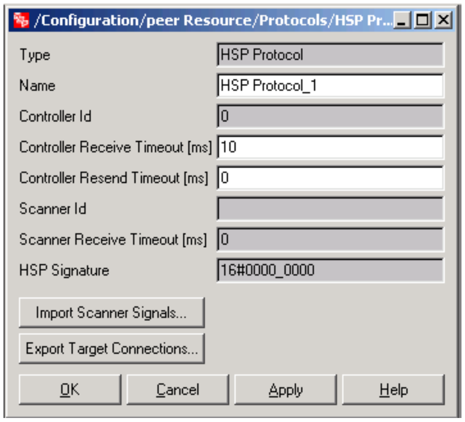

/Configuration/peer Resource

Type	GuardPLC 1800
Name	peer Resource
System ID [SRS]	100
Safety Time [ms]	100
Watchdog Time [ms]	50
Main Enable	☑
Autostart	☐
Start/Restart allowed	☑
Loading allowed	☑
Test Mode allowed	☐
Online Test allowed	☐
Forcing allowed	☐
Stop on Force Timeout	☑
max. Com. Time Slice [ms]	10
Code Generation Version	3

4. Add HSP protocol to the peer resource.



5. Configure HSP communications. Right-click on the peer HSP Protocol and select Properties.


/Configuration/peer Resource/Protocols/HSP Pr...

Type	HSP Protocol
Name	HSP Protocol_1
Controller Id	0
Controller Receive Timeout [ms]	10
Controller Resend Timeout [ms]	0
Scanner Id	
Scanner Receive Timeout [ms]	0
HSP Signature	16#0000_0000

See page 6-3 for an explanation of the HSP communication parameters.

6. Review the peer controller's communication settings. See page 6-5.

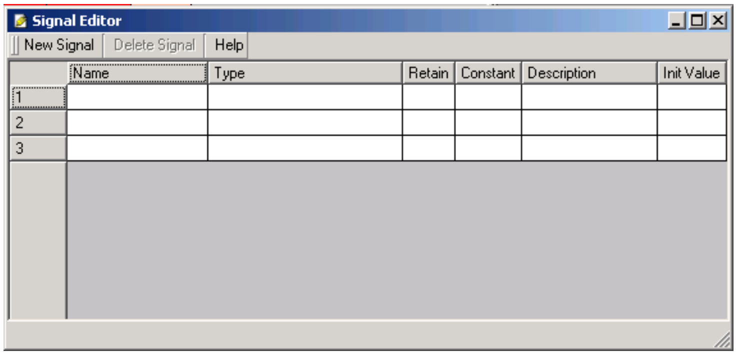
Define Target Connections for Standard and Safety Data

To support peer-to-peer communication, you must assign application signals to define target connections to which a peer scanner or other CIP Safety originator or standard master will connect. Review the guidelines for creating a distinction between safety and standard signals on page 1-4.

Create Required Signals

Using RSLogix Guard PLUS! Hardware Management, create the signals that will be made available to peers on the DeviceNet Safety network via the Target Connections file.

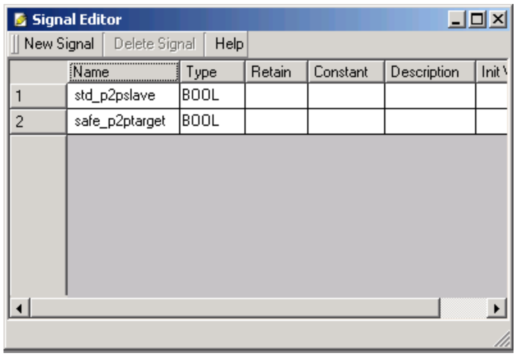
1. Open the Signal Editor by selecting Editor from the Signals menu.



	Name	Type	Retain	Constant	Description	Init Value
1						
2						
3						

2. Click on the New Signal button to add new signal.

3. Name the signal and configure its properties.



	Name	Type	Retain	Constant	Description	Init
1	std_p2pslave	BOOL				
2	safe_p2ptarget	BOOL				

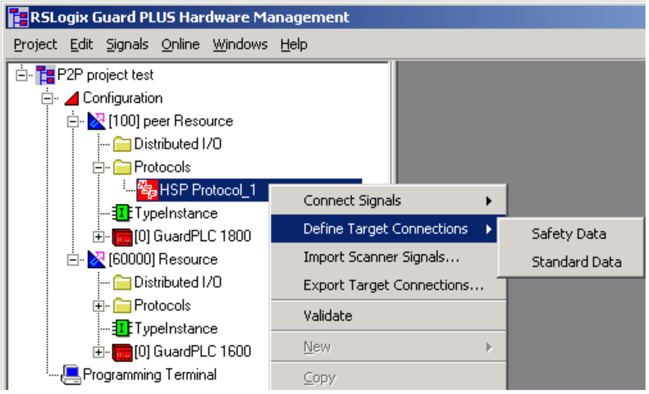
4. Leave the Signal Editor open.

For more information on using the Signal Editor, refer to the GuardPLC Controller Systems User Manual, publication 1753-UM001.

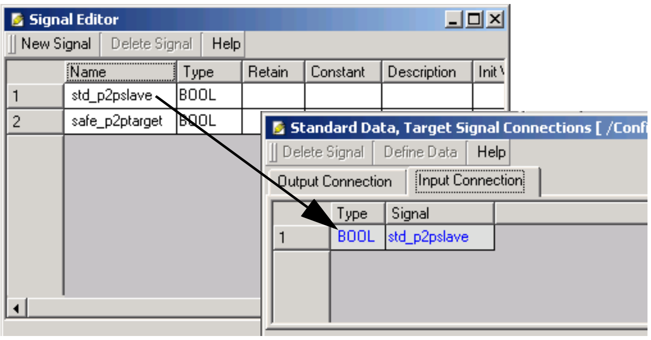
Define Standard Target Connections

To define the signals that will be available to another standard master on the network:

1. Right-click on the HSP Protocol instance of the target resource and select Define Target Connections>Standard Data.



2. Drag the Standard signals from the Signal Editor to the Standard Data, Target Signal Connections dialog.



	Name	Type	Retain	Constant	Description	Init V
1	std_p2pslave	BOOL				
2	safe_p2ptarget	BOOL				

	Type	Signal
1	BOOL	std_p2pslave

The signal names in the Target Signal Connections dialog are named from the perspective of the peer controller that is connecting to this target. Signals dropped into the Input Connection tab are read by the peer/connecting controller. Signals dropped into the Output Connection tab will be written by the peer/connecting controller.

You may drop safety signals into the Standard Target Connection's Input tab so that they may be read by the peer, but they may only be regarded as standard signals in the peer's application. Do not drop safety signals into the Standard Target Connection's Output tab.

A signal may be dropped into only one of the four Target Connections tabs (Safety Input, Safety Output, Standard Input, or Standard Output). If a signal appears in more than one Target

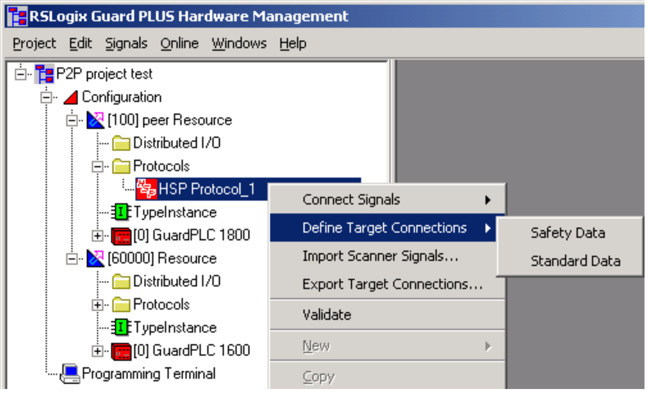
Connections tab, RSNetWorx for DeviceNet will reject the Target Connections file when it is imported.

3. RSLogix Guard PLUS! automatically generates a Target Connections file within its project folder. When you use the Automatically Update Signals option in RSNetWorx for DeviceNet, that software automatically imports any updates when the scanner's property page is displayed. You can also manually export the Target Connections file to a specific location at any time by right-clicking on the HSP Protocol and selecting Export Target Connections.

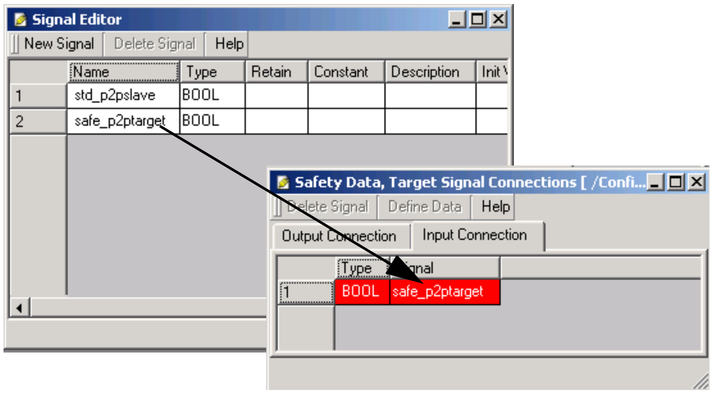
Define Safety Connections

To define safety target connections:

1. Right-click on the HSP Protocol instance of the peer resource and select Define Target Connections>Safety Data.



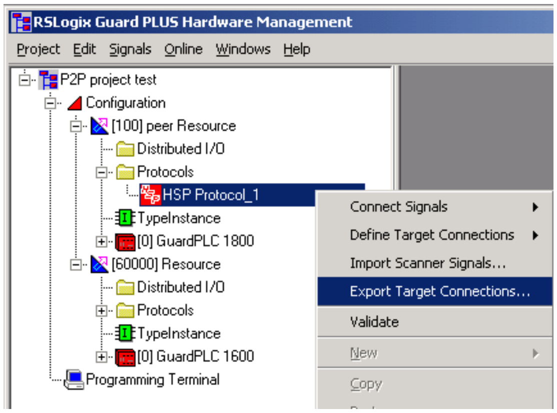
2. Drag the Safety signals from the Signal Editor to the Safety Data, Target Signal Connections dialog.



	Name	Type	Retain	Constant	Description	Init V
1	std_p2pslave	BOOL				
2	safe_p2ptarget	BOOL				

	Type	Signal
1	BOOL	safe_p2ptarget

3. RSLogix Guard PLUS! automatically generates a Target Connections file within its project folder. When you use the Automatically Update Signals option in RSNetWorx for DeviceNet, that software automatically imports any updates when the scanner's property page is displayed. You can also manually export the Target Connections file to a specific location at any time by right-clicking on the HSP Protocol and selecting Export Target Connections.



Configure Peer-to-Peer Connections

You must associate target scanners with their GuardPLC controller before you can configure the peer-to-peer standard and safety connections.

Associate the Peer Safety Scanner and GuardPLC Controller

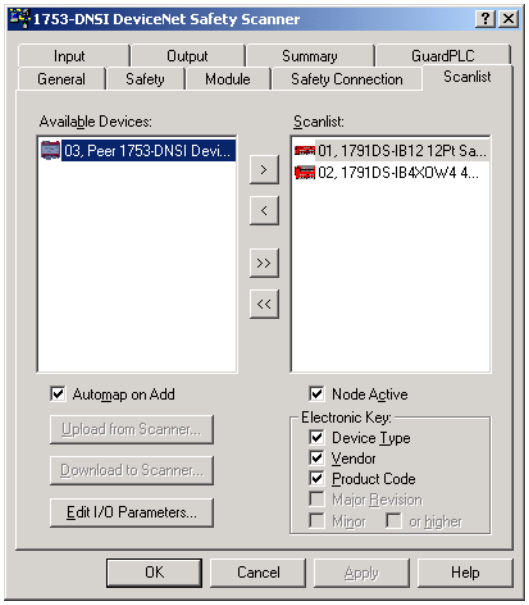
Follow the procedure in Chapter 7 to associate the peer safety scanner to its GuardPLC controller and configure the peer scanner's GuardPLC connection.

View the application signals imported via the association by clicking on the View Target Connections… button on the GuardPLC tab in RSNetWorx for DeviceNet. The signals should match the definitions made in RSLogix Guard PLUS!.

Add the Peer Scanner to the Scanlist

To configure standard peer-to-peer communications:

1. Open the DeviceNet Properties dialog for the DeviceNet Safety Scanner and select the Scanlist tab.



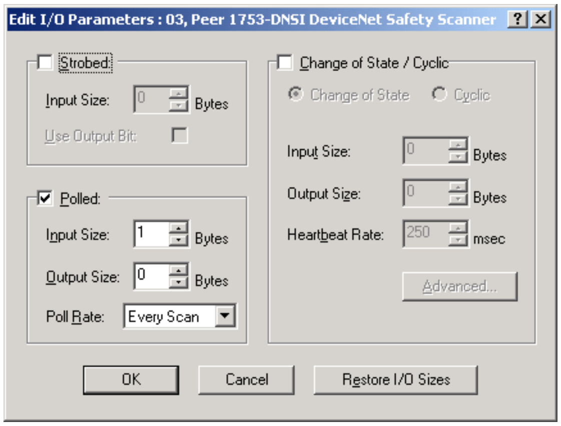
☑ Automap on Add

☑ Node Active

Electronic Key:
☑ Device Type
☑ Vendor
☑ Product Code
□ Major Revision
□ Minor □ or higher

2. Add the peer scanner to the scanlist by clicking on the > button.

3. Configure the I/O parameters of the peer scanner by clicking on the Edit I/O Parameters button.


Edit I/O Parameters : 03, Peer 1753-DNSI DeviceNet Safety Scanner
Advanced...
OK
Cancel
Restore I/O Sizes

□ Strobed:
Input Size: 0 Bytes
Use Output Bit: □

☑ Polled:
Input Size: 1 Bytes
Output Size: 0 Bytes
Poll Rate: Every Scan

□ Change of State / Cyclic
● Change of State ○ Cyclic
Input Size: 0 Bytes
Output Size: 0 Bytes
Heartbeat Rate: 250 msec

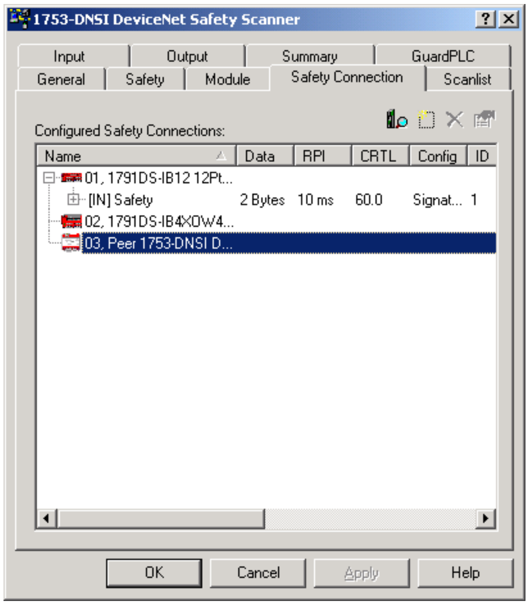
The target safety scanner only supports the polled connection on its slave mode interface.

4. Specify the Poll Rate, either Every Scan or Background.

Configure Safety Connections

To configure a safety connection to the peer scanner:

1. On the Device Properties dialog, select the Safety Connections tab.

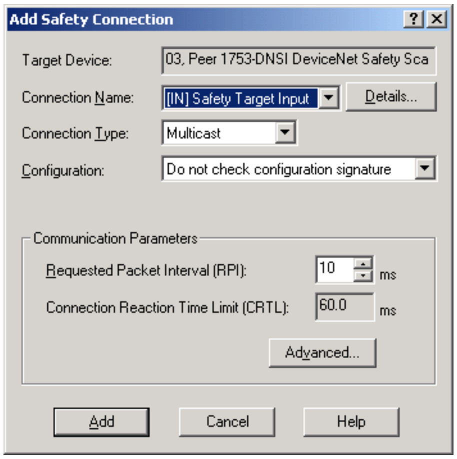


Configured Safety Connections:

Name	Data	RPI	CRTL	Config	ID
01, 1791DS-IB12 12Pt...					
[IN] Safety	2 Bytes	10 ms	60.0	Signat...	1
02, 1791DS-IB4XOW4...					
03, Peer 1753-DNSI D...					

2. Right-click on the peer scanner and select Add Connections to display the available connections.

3. Configure the safety connection.



Target Device: 03, Peer 1753-DNSI DeviceNet Safety Sca

Connection Name: [IN] Safety Target Input

Connection Type: Multicast

Configuration: Do not check configuration signature

Communication Parameters

Requested Packet Interval (RPI): 10 ms

Connection Reaction Time Limit (CRTL): 60.0 ms

For a description of the Safety Connection parameters, see pages 5-4 to 5-5.

TIP For peer-to-peer safety connections, you can only select ‘Do not check configuration signature’.

Make non-peer-to-peer connections, following steps 2 and 4 in Chapter 5. Then, continue with the process described in Chapters 7, 8, and 9.

DeviceNet Class Codes

This appendix contains the most commonly used class codes for the 1753-DNSI DeviceNet Safety Scanner for GuardPLC Controllers.

DeviceNet Object

Name	Class	Instance	Attribute	Data Size	Access
MAC ID	0x03	0x01	0x01	1 byte	Get/Set
Baud Rate	0x03	0x01	0x02	1 byte	Get/Set
SNN	0x03	0x01	0x0B	6 bytes	Get/Set

Identity Object

Name	Class	Instance	Attribute	Data Size	Access
Vendor ID	0x01	0x01	0x01	2 bytes	Get
Device Type	0x01	0x01	0x02	2 bytes	Get
Product Code	0x01	0x01	0x03	2 bytes	Get
Revision	0x01	0x01	0x04	2 bytes	Get
Serial Number	0x01	0x01	0x06	4 bytes	Get
Product Name	0x01	0x01	0x07	23 bytes	Get

Safety Supervisor Object

Name	Class	Instance	Attribute	Member Size	Access
Safety Supervisor	0x39	1	11	8 bits	Get

Calculate Safety Connection Bandwidth

This appendix provides equations for calculating the amount of system bandwidth consumed by an individual safety input or output connection.

In the equations below,

- RPI is in milliseconds
- data sizes are in bytes
- Baud_Rate is in bits per second

The bit_stuffing_factor is the percentage of bandwidth estimated to be used by bit stuffing. We used 15% for our calculations.

Single-cast Inputs

1 to 2 Bytes

In the equation below:

A = 1 ÷ Data_RPI ÷ 0.001
B = Safety_Data_Size + 6
C = (B x 8 x bit_stuffing_factor) rounded to the nearest whole number
D = 1 ÷ (Data_RPI x 100) ÷ 0.001

%Bandwidth = 100 x {[A x (57 + B x 8 + C) + (D x 115)] ÷ Baud_Rate}

3 to 250 Bytes

In the equation below:

A = 1 ÷ Data_RPI ÷ 0.001
B = (2 x Safety_Data_Size) + 8
C = (B ÷ 8) rounded to the nearest whole number
D = 1 ÷ (Data_RPI x 100) ÷ 0.001
E = (B x 8 x bit_stuffing_factor) rounded to the nearest whole number

%Bandwidth =
100 x ({A x [(57 x C) + (B x 8) + E] + (D x 115)} ÷ Baud_Rate)

Single-cast Outputs

1 to 2 Bytes

In the equation below:

$A = 1 \div \text{Data\_RPI} \div 0.001$
$B = \text{Safety\_Data\_Size} + 6$
$C = (B \times 8 \times \text{bit\_stuffing\_factor})$ rounded to the nearest whole number
$D = 1 \div (\text{Data\_RPI} \times 19) \div 0.001$

$\%\text{Bandwidth} = 100 \times \{[A \times (57 + B \times 8 + C) + (D \times 115)] \div \text{Baud\_Rate}\}$

3 to 250 Bytes

In the equation below:

$A = 1 \div \text{Data\_RPI} \div 0.001$
$B = (2 \times \text{Safety\_Data\_Size}) + 8$
$C = (B \div 8)$ rounded to the nearest whole number
$D = 1 \div (\text{Data\_RPI} \times 19) \div 0.001$
$E = (B \times 8 \times \text{bit\_stuffing\_factor})$ rounded to the nearest whole number

$\%\text{Bandwidth} =$
$100 \times \big(\{A \times [(57 \times C) + (B \times 8) + E] + (D \times 115)\} \div \text{Baud\_Rate}\big)$

Multicast Connections

1 to 2 Bytes

In the equation below:

$A = 1 \div \text{Data\_RPI} \div 0.001$
$B = \text{Safety\_Data\_Size} + 6$
$C = (B \times 8 \times \text{bit\_stuffing\_factor})$ rounded to the nearest whole number
$D = 1 \div (\text{Data\_RPI} \times 100) \div 0.001$

$\%\text{Bandwidth} =$
$100 \times \{[A \times (57 + B \times 8 + C) + 2 \times (D \times 115 \times \text{Number\_of\_Consumers})]$
$\div \text{Baud\_Rate}\}$

3 to 250 Bytes

In the equation below:

A = 1 ÷ Data_RPI ÷ 0.001
B = (2 x Safety_Data_Size) + 8
C = (B ÷ 8) rounded to the nearest whole number
D = 1 ÷ (Data_RPI x 100) ÷ 0.001
E = (B x 8 x bit_stuffing_factor) rounded to the nearest whole number

%Bandwidth =
100 x ({A x [(57 x C) + (B x 8) + E] +
2 x (D x 115 x Number_of_Consumers)} ÷ Baud_Rate)

Change of State (COS)

A type of standard I/O communication in which the interface module 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.

CIP Safety Protocol

A network communications method designed and certified for transport of data to assure SIL 3 requirements.

Configuration Signature

The combination of an ID number date and time that uniquely identifies a specific configuration for a device.

Controller ID (SRS)

A value required to uniquely identify a particular GuardPLC controller within a network of controllers. Refer to the GuardPLC Controller Systems User Manual, publication number 1753-UM001.

Controller Receive Timeout

The amount of time that the controller waits to receive an HSP response from the scanner before closing the HSP connection.

Controller Resend Timeout

The amount of time that the controller waits for the acknowledgement of a message before it resends it.

Cyclic

A type of standard I/O data communication in which the interface module can send and receive data with slave devices that support the cyclic feature. Data is only sent at the user-specified rate.

Electronic Data Sheet (EDS)

A vendor-supplied template that RSNetWorx for DeviceNet uses to display the configuration parameters, I/O data profile, and connection type support for a given DeviceNet or DeviceNet Safety module.

Explicit Messaging

A type of messaging used for lower priority tasks, such as configuration and status monitoring.

Heartbeat Rate

Devices that are configured for change of state data can also send a 'heartbeat' signal to keep the connection active during periods when the data is not changing.

HSP Signature

A read-only value that represents the data exchanged between the GuardPLC controller and the 1753-DNSI. The HSP Signature is calculated based on the scanner's configured safety and standard connections and is passed to RSLogix Guard PLUS! via the Scanner Signals File.

Implicit Messaging

The type of messaging used for high priority I/O control data (e.g. change of state, cyclic, polled, strobed, or safety).

Node

Hardware that is assigned a single address on the network (also referred to as device or module).

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).

Requested Packet Interval (RPI)

When communicating over a network, this is the maximum amount of time between subsequent production of input 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 ensure 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 sub-net within a system. The Safety Network Number makes up part of the Unique Node Identifier (UNID).

Scanlist

The list of devices (nodes) with which the scanner is configured to exchange I/O data.

Scanner ID

A read-only value which uniquely identifies the scanner and is required to connect the GuardPLC controller to the scanner. The scanner ID is automatically generated by RSNetWorx for DeviceNet using the SNN and DeviceNet address of the scanner.

Scanner Signals File

A file which defines the layout of the data passed via HSP, including signals and the HSP Signature value.

SRS (System, Rack, Slot)

See Controller ID.

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 one 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.

Target Connections File

A file used to pass target connection information for data the user wants to make available from the GuardPLC controller to another safety originator or standard master on the DeviceNet network.

Timeout Multiplier

This value determines the number of messages that may be lost before declaring a connection error.

Symbols

.ssf
  See scanner signals file.
.tcf
  See target connections file.

Numerics

1753-CBLDN 2-7
1770-KFD module 1-5
1784-PCD 1-5
1784-PCID 1-5

A

A#xx 10-2
add connections 5-3
add devices
  available devices list 5-9
advanced safety connection properties 5-5
associate 7-1–7-5
  manually 7-4–7-5
automap 5-9
automatically update signals 7-2–7-3
available devices list 5-9
  add devices 5-9

B

baud rate
  reset 3-4
  See communication rate.
bridge device 1-5
bus off detected 10-3

C

change of state
  definition
  messages 1-2
CIP safety protocol
  definition G-1
COMM3 port 2-7
communication connections 2-5
communication rate 1-8
  choose 1-9
  set 1-9
compile logic 8-4
configuration
  DeviceNet Safety I/O target nodes 5-2
  DeviceNet Safety Scanner safety connections 5-3
  DeviceNet Safety Scanner standard connections 5-6
  DeviceNet Safety target nodes 5-1
  DeviceNet Standard slave nodes 5-6
  GuardPLC controller connections 5-12
  HSP connnection 8-3
  safety parameters 5-2
  signals 8-1
  standard inputs 5-10
  standard outputs 5-11
  standard parameters 5-3
  standard scanner inputs 5-10
  verify 9-1–9-7
configuration owner
  reset 3-4
configuration signature 1-1, 5-1
  comparison 9-6
  components 5-1
  definition 5-1, G-1
  mismatch 9-2
configure a driver 3-1
connect safety signals 8-2
connect signals 8-1
connection reaction time limit 5-4
  and network delay multiplier 5-5
  DeviceNet Safey I/O 5-4
connections
  add 5-3
controller ID 5-12, 7-4
  and system ID 6-4
  default 1-2
  definition G-1
controller receive timeout
  set 6-3
controller resend timeout
  definition G-1
  set 6-3, 6-4
cooling 2-2
COS
  See change of state.
create a GuardPLC project 6-1
create a scanlist 5-8
create a signal 8-2
create application program logic 8-4
cyclic
  definition G-1
  messages 1-2
cyclic messages 1-3

D

data tables 1-4, 7-1, 7-2
data types B-2
default
module defaults button 5-6
device status
monitoring 10-1
Safety Device Verification Wizard 9-1
verification 9-3
DeviceNet connections 2-6
DeviceNet network
configuration 3-1
configure a driver 3-1
connecting 3-1
DeviceNet Safety I/O
configuration signature 5-1
set node address 3-2
DeviceNet Safety Scanner
See scanner.
display
status 10-2
download DeviceNet configuration 7-5–7-7
download project to controller 8-4
driver types 3-2
duplicate node failure 10-2

E

E#ee 10-4
edit I/O parameters 5-9
EDS
See electronic data sheet.
electronic data sheet
definition
electronic key 5-9
electrostatic discharge
prevent 2-2
environment and enclosure 2-1
EPR
See expected packet rate.
expected packet rate 5-7
default 5-8
explicit messaging 1-4
definition G-1
export scanner signals 7-4
extended error code 10-4, 10-7

F

faulted, must issue safety reset 10-3
features 1-7

G

G#gg 10-4
grounding 2-4
GuardPLC controller
communication settings 6-5
configuration 6-1
properties 6-2
GuardPLC project
create 6-1
GuardPLC tab
associate automatically 7-2
associate manually 7-4
configure HSP connection 5-12

H

heartbeat rate
definition G-2
high-speed safety protocol 1-2
add to GuardPLC project 6-3
cable connections 2-7
configure communications 6-3
configure connections 8-3
signature 5-12
high-speed safety protocol signature 1-2
definition G-2
HSP
See high-speed safety protocol
HSP Connection Control Word 8-3
HSP connection control word 8-3
HSP signature
See high-speed safety protocol signature.

I

icon
device status 9-2
IDLE status 10-2
implicit messaging
definition G-2
import scanner signals 7-5
input tab 5-10
interscan delay 5-6
ISD
See interscan delay.

L

LED indicators 10-1
lock
  See safety-lock.
login screen 8-4

M

MAC address 6-5
  reset 3-4
Max Scanner Response Time 5-13
max scanner response time 5-13
mean time between failures (MTBF)
  definition P-3
mean time to restoration
  definition P-3
mismatch
  configuration signature 9-2
  SNN 4-5
missing device
  icon 9-2
module tab 5-6
mount the scanner 2-2
  DIN rail 2-3
  panel 2-4
multicast connections 5-4

N

N#xx 10-3
naming convention 1-5
network delay multiplier 5-5
network status LED
  flashing 4-4
no network power 10-3
node
  definition G-2
node address
  changes 4-6
  DeviceNet Safety I/O 3-2
  select 1-10
node commissioning 3-2–3-3
node commissioning tool 3-2

O

online button 7-6
output connection owners
  reset 3-4
output tab 5-11

P

parameters tab 5-3
password 1-2
  forgotten 3-6
  protected operations 3-5
  reset 3-4, 3-6
  set or change 3-5
  valid characters 3-6
point-to-point 5-4
poll messages 1-2
poll ratio 5-7
polled
  definition G-2
power supply 2-5
probability of failure on demand (PFD)
  definition P-3
probability of failure per hour (PFH)
  definition P-3
protective debris strip 2-2

R

ready to be safety locked 9-5
ready to be verified 9-3
requested packet interval
  and connection reaction time limit 5-5
  definition G-2
  set 5-4
reset
  configuration owner 3-4
reset safety attributes 3-4
reset safety device 3-4, 4-6
RPI
  See requested packet interval.
RSLinx 3-1
  revision level 1-6
RSLogix Guard PLUS
  create a project 6-1
  install 1-6
RSLogix Guard PLUS, Hardware Management
  revision level 1-6
RSLogix Guard PLUS, Program Management
  revision level 1-6
RSNetWorx for DeviceNet 1-5
  install 1-6
  node commissioning 3-2
  revision level 1-6
RUN status 10-2

S

S#ee 10-4
safety concept 1-1
safety configuration tab 5-2
safety connections 1-7
  colorization 1-4
safety connections tab 5-3
safety data
  communication 1-3
safety data, signal connections dialog 8-2
Safety Device Verification Wizard 3-5
  definition 9-1
  device status 9-1
  reports 9-5
  run 9-1
  safety-lock
  select devices 9-3
  summary 9-7
  upload and compare 9-4
  Welcome page 9-1
safety I/O
  definition G-2
safety information 2-1
safety integrity level 1-4, 2-7
safety network number 1-1, 4-1
  assignment 4-2–4-3
  automatic 4-2
  automatic assignment 4-2
  copy 4-2
  definition G-2
  formats 4-1
  managing 4-1
  manual 4-2, 4-3
  manual assignment 4-3
  mismatch 4-5
  mismatch dialog 4-5
  reset 3-4, 4-6
  time-based 4-1
safety network number error
  icon 9-2
safety reset 3-4
  when faulted 10-3
safety-lock
  devices
  during reset 3-5
  icon 9-2
save and compile logic 8-4
scanlist 5-8, 5-9
  definition G-3
scanner
  DeviceNet connections 2-6
  features 1-7
  ground 2-4
  hardware overview 1-6
  HSP connections 2-7
  mounting 2-2
  power supply 2-5
  reset 4-6
scanner configuration signature 1-2
scanner ID 5-12
  definition G-3
scanner receive timeout 5-13
scanner signals file 1-5, 6-4, 7-1
  definition G-3
  import 7-5
  save 7-4
signal
  create 8-2
signal editor 8-2
signals
  connect 8-1
  connect safety 8-2
  define 8-1–8-2
  export 7-4
  import 7-5
  safety data 8-1
SIL
  See safety integrity level.
software revision
  RSLogix Guard PLUS 1-6
  RSNetWorx for DeviceNet 1-6
software revisions
  RSLinx 3-1
SRS
  See controller ID.
standard connection 1-7
standard connections
  colorization 1-4
standard data
  communication 1-2
statistics button 5-13
status
  A#xx 10-2
  bus off detected 10-3
  display 10-2
  duplicate node failure 10-2
  E#ee 10-4
  extended error code 10-4
  faulted, must issue safety reset 10-3
  G#gg 10-4
  IDLE 10-2
  LEDs 10-1
  monitoring 10-1

N#xx 10-3
no network power 10-3
RUN 10-2
S#ee 10-4
status code
descriptions 10-4
general status error codes 10-5
safety connections 10-4
standard connections 10-4
status codes
extended error code 10-7
strobe messages 1-2
strobed
definition G-3
system ID (SRS) 6-2
system reaction time
definition G-3

T

target connections file 1-5, 7-2
definition G-3
terminology
used throughout manual P-3
timeout multiplier 5-5
definition G-3
timing parameters 8-5
transmit retries 5-7, 5-8

U

unique node identifier 4-1
unknown device
icon 9-2
update signals
automatically 7-2–7-3
upload and compare
Safety Device Verification Wizard 9-4
use data signals 1-3

V

verification failure report 9-5
verification reports
Safety Device Verification Wizard 9-5
verify
select devices 9-3
verify DeviceNet Safety configuration 9-1–9-7
verify FAILED 9-5
verify failed 9-3
verify not supported 9-3
view scanner response times 5-13

W

Watchdog Timeout 5-13
welcome page 9-1

Rockwell Automation Support

Rockwell Automation provides technical information on the web to assist you in using its products. At http://support.rockwellautomation.com, you can find technical manuals, a knowledge base of FAQs, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools.

For an additional level of technical phone support for installation, configuration and troubleshooting, we offer TechConnect Support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit http://support.rockwellautomation.com.

Installation Assistance

If you experience a problem with a hardware module within the first 24 hours of installation, please review the information that's contained in this manual. You can also contact a special Customer Support number for initial help in getting your module up and running:

United States	1.440.646.3223 Monday – Friday, 8am – 5pm EST
Outside United States	Please contact your local Rockwell Automation representative for any technical support issues.

New Product Satisfaction Return

Rockwell tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned:

United States	Contact your distributor. You must provide a Customer Support case number (see phone number above to obtain one) to your distributor in order to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for return procedure.

www.rockwellautomation.com

Corporate Headquarters
Rockwell Automation, 777 East Wisconsin Avenue, Suite 1400, Milwaukee, WI, 53202-5302 USA, Tel: (1) 414.212.5200, Fax: (1) 414.212.5201

Headquarters for Allen-Bradley Products, Rockwell Software Products and Global Manufacturing Solutions
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 SA/NV, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, 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

Headquarters for Dodge and Reliance Electric Products
Americas: Rockwell Automation, 6040 Ponders Court, Greenville, SC 29615-4617 USA, Tel: (1) 864.297.4800, Fax: (1) 864.281.2433
Europe/Middle East/Africa: Rockwell Automation, Herman-Heinrich-Gossen-Strasse 3, 50858 Köln, Germany, Tel: 49 (0) 2234 379410, Fax: 49 (0) 2234 3794164
Asia Pacific: Rockwell Automation, 55 Newton Road, #11-01/02 Revenue House, Singapore 307987, Tel: (65) 6356 9077, Fax: (65) 6356 9011