Safety Reference Manual

Allen-Bradley

GuardPLC Controller Systems

Catalog Numbers 1753, 1754, and 1755

Allen-Bradley • Rockwell Software

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.rockwellautomation.com/literature/) 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.
	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence
	**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
	**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

This manual contains new and updated information. Changes throughout this revision are marked by change bars, as shown to the right of this paragraph.

New and Updated Information

This table contains the changes made to this revision.

Topic	Page
Updated PFD and PFH data tables	15
Added Functional Verification Tests section	21
Added Project Verification Test section	22
Updated EN954-1 to ISO 13849-1	various
Changed Cat. 4 to PLe/Cat. 4	various

Table of Contents

Chapter 5

GuardPLC DeviceNet Safety Scanner

Chapter 6

DeviceNet Safety I/O for the GuardPLC Control System

Chapter 7

GuardPLC Controller Operating System

Chapter 8

Technical Safety for the Application Program

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

- the purpose of this manual.
- list of abbreviations.
- additional resources.

Purpose of This Manual

This manual explains how the GuardPLC Control System, including the GuardPLC controllers and distributed I/O, DeviceNet safety scanner, and DeviceNet safety I/O, can be used in safety applications up to and including SIL 3 according to IEC 61508, and applications up to and including Performance Level e/Category (Cat.) 4, according to ISO 13849-1.

IMPORTANT	You must read and understand the safety concepts and requirements presented in this manual prior to operating a GuardPLC controller-based safety system.

List of Abbreviations

The following table defines terms or abbreviations used in this manual.

Term	Definition
1oo2	One Out of Two Safety Architecture. Consists of 2 channels connected in parallel, such that either channel can process the safety function. Thus, a dangerous failure would have to occur in both channels before a safety function failed on demand
2oo3	Two out of Three Safety Architecture. Consists of 3 channels connected in parallel with a majority voting arrangement for the output signals, such that the output state is not changed if only 1 channel gives a result that disagrees with the other 2 channels
CRC	Cyclic Redundancy Check. A number derived from and stored or transmitted with a block of data in order to detect corruption
EMC	Electromagnetic Compatibility
EN	European Norm. The official European Standard
EPROM	Erasable Programmable Read-only Memory
ESD	Electrostatic Discharge
HFT	Hardware Fault Tolerance
HSP	High-speed Safety Protocol
IEC	International Electrotechnical Commission Standard
MAC ID	Media Access Identifier. A node's address on a network or subnet
MOT	Multiple Error Occurrence Time
MTTF	Mean Time to Failure
MTTFd	Mean Time to Dangerous Failure
Non-interacting	Does not interfere or affect functions of the safety system
PES	Programmable Electronic System
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
POU	Program Organization Unit
PS	Programming System
RFI	Radio Frequency Interference
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SNN	Safety Network Number
SRS	System, Rack, Slot (This number is used as the System ID)
Standard	Any object, task, tag, or program, that is not marked as being a safety item
TÜV	Technischer Überwachungs-Verein (Technical Inspection Association)
UNID	Unique Node Identifier
WD	Watchdog Time

Additional Resources

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

Resource	Description
GuardPLC Controller Systems User Manual, publication 1753-UM001	Information on configuration and operation for a GuardPLC Controller System
Using RSLogix Guard PLUS! Software with GuardPLC Controllers Programming Manual, publication 1753-PM001	Procedural information on programming a GuardPLC Controller System with RSLogix Guard PLUS! software
CompactBlock Safety I/O Modules on DeviceNet Series 1791DS Installation Instructions, publication 1791DS-IN001	Information on installing CompactBlock Safety I/O modules on DeviceNet networks
Guard I/O DeviceNet Safety Modules User Manual, publication 1791DS-UM001	Information on configuration and programming on DeviceNet networks for ArmorBlock and CompactBlock Guard Safety I/O Modules
GuardPLC Certified Function Blocks - Basic Suite Safety Reference Manual, publication 1753-RM001	Information on programming with GuardPLC Certified Function Blocks
CompactBlock Guard I/O DeviceNet Safety Modules Installation Instructions, publication 1791DS-IN002	Information on Installing 1791DS-IB8XOBV4 modules
ArmorBlock Guard I/O DeviceNet Installation Instructions, publication 1732DS-IN001	Installing ArmorBlock Guard I/O modules on DeviceNet networks
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	In-depth information on grounding and wiring Allen-Bradley programmable controllers
Application Considerations for Solid-State Controls, publication SGI-1.1	A description of important differences between solid-state programmable controller products and hard-wired electromechanical devices
National Electrical Code - Published by the National Fire Protection Association of Boston, MA.	An article on wire sizes and types for grounding electrical equipment
Allen-Bradley Industrial Automation Glossary, publication AG-7.1	A glossary of industrial automation terms and abbreviations

If you would like a manual, you can:

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

Safety Concept for GuardPLC Controllers and GuardPLC I/O

This chapter introduces you to the safety concept for the following GuardPLC products.

Catalog Number	Description
1753-DNSI	DeviceNet Safety Scanner for GuardPLC
1753-IB16	GuardPLC 16-point Input Module
1753-IB20XOB8	GuardPLC I/O Module
1753-IB8XOB8	GuardPLC I/O Module
1753-IB16XOB8	GuardPLC I/O Module
1753-IF8XOF4	GuardPLC Analog I/O Module
1753-L28BBBM	GuardPLC 1600 controller with Modbus Communication
1753-L28BBBP	GuardPLC 1600 controller with Profibus-DP Communication
1753-L32BBBM-8A	GuardPLC 1800 controller with Modbus Communication
1753-L32BBBP-8A	GuardPLC 1800 controller with Profibus-DP Communication
1753-OB16	GuardPLC 16-point Output Module
1753-OW8	GuardPLC Relay Output Module
1754-L28BBB	GuardPLC 1200 Controller
1755-A6	GuardPLC 2000 I/O Chassis
1755-L1	GuardPLC 2000 Controller
1755-HSC	GuardPLC 2000 High-Speed Counter Module
1755-IB24XOB16	GuardPLC 2000 Digital I/O Module
1755-IF8	GuardPLC 2000 Analog Input Module
1755-OF8	GuardPLC 2000 Analog Output Module
1755-PB720	GuardPLC 2000 Power Supply Module

Certification

Certificate No. 968/EZ164.10/09
TÜV Rheinland Group
TÜV Industrie Service GmbH
Automation, Software, and Informatinstechnologie

Safety restrictions can be found in this manual. See Safety Requirements on page 17.

For a listing of TÜV certified product and software versions, refer to:
http://www.rockwellautomation.com/products/certification/safety/

Introduction to Safety

The Programmable Electronic System (PES) for the Allen-Bradley GuardPLC system is safety-related, based on the 1oo2 microprocessor structure for one central module. These controllers are safety-rated up to and including Safety Integrated Level (SIL) 3 according to IEC 61508 and PLe (Cat. 4) according to ISO13849-1, except for the 1754-L28BBB which is safety-rated up to and including Safety Integrity Level (SIL) 3 according to IEC 61508 and Category 4 according to EN 954.

Safety tests are based on the safety standards current at the time of certification. These safety tests consist of test routines that are run during the entire operating phase. The routines are guaranteed to the highest degree of integrity for existing systems, making the PES suitable for the Safety Machinery Application.

Safety State

The PES has been designed to the closed-circuit current principle, which requires that systems be designed so that the normally closed or on state of external sensors and actuators is the normal run condition. The off or normally open state is the safe state. This means that in the event of a fault or safety trip, all inputs and outputs revert to the off (current-free/voltage-free) state.

PFD and PFH Calculations

The average probability of a system to fail to satisfactorily perform its safety function on demand is called Probability of Failure on Demand (PFD). The probability of a system to have a dangerous failure occur per hour is called Probability of Failure per Hour (PFH).

PFD and PFH calculations have been carried out for the GuardPLC controllers and GuardPLC I/O system in accordance with IEC 61508. For SIL 3, IEC 61508-1 sets the following minimum PFD and PFH values.

Table 1 - PFD and PFH Values

Type	SIL 3 value per IEC 61508-1
PFD	10^{-4}…10^{-3}
PFH	10^{-8} …10^{-7} per hour

Table 2 - GuardPLC Controllers

Module	MTTF (in years)	MTTFd (in years)	PFD	PFH	Safe Failure Fraction
GuardPLC 1200 Controllers(1)	19.84	n/a	1.451664E-04	3.094950-E9	99.8779%
GuardPLC 1600 Controllers(1)	17.69	102.44	4.158987E-05	3.926815E-09	99.8626%
GuardPLC 1800 Controllers(1)	14.58	84.45	5.460105E-05	5.665043E-09	99.8636%

(1) The PFD and PFH data is based on a functional verification test interval of 10 years.

Table 3 - GuardPLC 2000

Module	MTTF (in years)	MTTFd (in years)	PFD	PFH	Safe Failure Fraction
Chassis(1)	704.66	1409.32	4.195800E-06	8.10000E-11	99.9500%
L1(1)	44.03	122.78	4.884170E-05	4.36713E-09	99.7699%
IF8(1)	73.12	252.52	1.746768E-05	4.14836E-09	99.6233%
HSC(1)	45.33	239.18	5.993297E-05	3.28725E-09	99.6623%
IB24XOB16(1)	34.28	352.58	3.710908E-05	1.09636E-09	99.874%
OF4(1)	94.26	250.23	2.682039E-05	1.83623E-09	99.8899%
PB720(1)	20.73	980.88	6.028484E-06	1.16380E-10	99.9892%

(1) The PFD and PFH data is based on a functional verification test interval of 10 years.

Table 4 - GuardPLC I/O

Module	MTTF (in years)	MTTFd (in years)	PFD	PFH	Safe Failure Fraction
1753-IB16(1)	45.02	198.48	3.684285E-05	2.772601E-09	99.7946%
1753-OB16(1)	15.22	177.84	3.625669E-05	3.902687E-09	99.7734%
1753-IB20XOB8(1)	20.48	163.50	5.107536E-05	4.247003E-09	99.7681%
1753-IB8XOB8(1)	19.02	122.55	4.603845E-05	6.581646E-09	99.7908%
1753-IB16XOB8(1)	12.38	121.08	6.655234E-05	6.189071E-09	99.7161%
1753-IF8XOF4(1)	35.01	117.75	8.575442E-05	5.159597E-09	99.7760%
1753-OW8(2)	34.16	159.41	2.240516E-05	1.730251E-09	99.7905%

(1) The PFD and PFH data is based on a functional verification test interval of 10 years.

(2) The PFD and PFH data is based on a functional verification test interval of 3 years.

The safety functions, consisting of a safety loop (input, processor, output, and communication between GuardPLC modules), fulfill the above requirements in any combination. These requirements are also met by the GuardPLC distributed I/O modules.

Safety requirements, including PFD and PFH, for the DeviceNet Safety Scanner are in Chapter 5.

Safety requirements, including PFD and PFH, for the DeviceNet Safety I/O are in Chapter 6.

Safety Requirements

The following safety requirements must be followed when using the safety PES of the GuardPLC system.

Hardware Configuration

There are product-independent and product-dependent hardware configurations for the GuardPLC system.

Product Independent

- Use only GuardPLC hardware and software that appear in the GuardPLC version list available at http://www.rockwellautomation.com/products/certification/safety/.
- Use RSNetWorx for DeviceNet software version 6.0 or later to configure the DeviceNet safety scanner and DeviceNet safety I/O module.
- Use RSLogix Guard PLUS! programming software, according to IEC 61131-3, for support in the creation of safety programs for GuardPLC controllers and GuardPLC I/O modules. Programming software is defined in IEC 61131-1.
- Follow the specifications listed in Appendix A.
- Hardware modules and software components that are not fail-safe, but do not cause any adverse reactions, can be used to process standard signals. However, they cannot be used to carry out safety tasks.
- Use the closed-circuit current principle in all external safety circuits connected to the system.

Product Dependent

Only equipment that can be safely isolated from the main power should be connected to the system.

The safe electrical isolation of the power supply must take place in the 24V DC power supply. Only PELV- or SELV-compliant power supplies may be used.

See Appendix A or page 23 for details on power supply requirements.

ATTENTION: Limit the use of standard devices in your GuardPLC application to standard critical components. If you choose to use standard devices in a safety critical fashion, you must ensure that the system design meets SIL 3 requirements.

Programming Requirements

There are product independent and product dependent programming requirements for the GuardPLC system.

Product Independent

Verify that the safety system variables are correctly configured for safety applications. Pay particular attention to the maximum cycle time and the safety time.

Product Dependent

- You must use RSLogix Guard PLUS! software to program the GuardPLC controller.
- You must follow the guidelines listed on page 78 for initial startup or after a modification to the application program.
- You must perform a complete check of program logic to verify that logic correctly and fully addresses the functional and safety requirements in your application specification.
- You must re-check the application as described above each time you make a modification.
- When a fault occurs in the fail-safe input and output modules, the error response of the system must be determined by the application program according to site-specific safety criteria.

Communication

- The total response time of the system must not exceed the fault tolerance time when safety communication occurs between devices.
- Safety data cannot be transferred over public networks (for example, the Internet).
- If the data is transferred across company/factory networks, verify that sufficient protection is provided against manipulation. For example, use a firewall or router to separate the standard or safety I/O subnets from office subnets in your environment. At this stage the serial interfaces should only be use for non-safety related purposes.

  Refer to Safety Concept of RSLogix Guard PLUS! Software on page 77 for more information.
- Equipment connected to communication devices should feature safe electrical isolation.
- Your application should monitor the status bits associated with safety network connections. Since connections often recover automatically, make sure this occurrence does not result in an unsafe machine state. Your application should drive safety outputs to their safe state when the connection faults or goes idle. Safety outputs remain in the safe state until a manual reset occurs. This prevents unexpected output transitions from low to high when a connection recovers from a faulted or idle state.

Maintenance Override

When using Maintenance Override, follow the requirements of the most recent version of the Maintenance Override document from the TÜV homepage: http://www.tuv-fs.com (TÜV Rheinland).

If necessary, the operator must consult the acceptance department responsible for the application to determine the administrative requirements to provide access protection for the system.

Safety Times

Individual errors that may lead to a dangerous operating condition are detected by the self-tests and trigger defined error reactions that transfer the faulty modules into the Safety state within the safety time of the PES. The following sections describe self-test safety times.

Fault Tolerance Time (FTT)

See DIN VDE 0801 Appendix A1 2.5.3

The fault tolerance time is an attribute of the process and describes the time span in which faulty signals can be tolerated in the process without a dangerous condition occurring. If the fault condition lasts longer than the FTT, the faulty signals can create a dangerous condition.

Safety Time (of the PES)

The safety time is the time within which the PES (while in RUN mode) must react after an internal error has occurred.

Seen from the process side, the safety time is the maximum amount of time in which the safety system must react (reaction time) to a change in the input signals or module or component failure.

Multiple Error Occurrence Time (MOT)

The occurrence time for multiple faults is the period of time in which the probability for the occurrence of multiple faults, which in combination are critical to safety, is sufficiently low.

The multiple fault occurrence time is defined at 24 hours in the operating system.

GuardPLC Reaction Time

The maximum reaction time of working GuardPLC systems is twice the cycle time of the system. The cycle time of a system consists of the following items.

- Reading local inputs
- Processing the application program
- Writing local outputs
- Testing routines
- Communication (for example, GuardPLC Ethernet, DeviceNet Safety, Profibus, Modbus networks)

In addition, when considering the worst case for the entire system, the switching times of the inputs and outputs must be taken into account.

When a network is used for communication data, reaction times are affected.

Refer to Chapter 9 for reaction time calculations.

Watchdog Time of the CPU (in the PES)

The watchdog time of the CPU depends on system configuration.

The watchdog time of the CPU is the maximum permissible time allowed for a RUN cycle (cycle time). If the cycle time exceeds the default watchdog time of the CPU, the CPU goes into FAILURE STOP mode. The watchdog time of the CPU must be a value between 2 ms and half the safety time of the PES. The maximum permitted value is 5000 ms. The default setting for controllers is 50 ms. The default for distributed GuardPLC I/O modules is 10 ms.

Functional Verification Tests

IEC 61508 requires the user to perform various functional verification tests of the equipment used in the system. Functional verificaiton tests are performed at user-defined times. For example, functional verification test intervals can be once a year, once every 15 years, or whatever timeframe is appropriate.

GuardPLC controllers have a functional verification test interval of up to 10 years. Other components of the system, such as Safety I/O modules, sensors, and actuators may have shorter functional verification test intervals. The controller should be included in the functional verification testing of the other components in the safety system.

IMPORTANT Your specific applications determine the timeframe for the functional verification test interval. However this is mainly related to Safety I/O modules and field instrumentation.

Project Verification Test

Project verification includes required functional verification tests of fault routines, input and output channels, to ensure that the safety system operates properly.

To perform a functional verification test on the GuardPLC controller you must perform a full test of the application. You must toggle each sensor and actuator involved in every safety function. From a controller perspective, this means toggling the I/O point going into the controller, not necessarily the actual activators. Be sure to test all shutdown functions, since these functions are not typically exercised during normal operation. Also, be aware that a functional verification test is only valid for the specific application tested. If the controller is moved to another application, you must also perform startup and functional verification testing on the controller in the context of its new application.

GuardPLC Central Functions

Chapter Introduction

This chapter gives information about the power supply, the CPU, and self-test routines for GuardPLC controllers.

The GuardPLC 1200 controller is a compact system that includes a CPU, 20 digital inputs, 8 digital outputs, 2 counters and communication ports in a single package. An external 24V DC power supply is required.

The GuardPLC 1600 and GuardPLC 1800 controller systems include an integrated CPU and on-board I/O, as well as optional distributed I/O. An external 24V DC power supply is required.

The GuardPLC 2000 controller is a modular system, in which a power supply module, a CPU module, and up to 6 local I/O modules comprise the system.

Power Supply Module

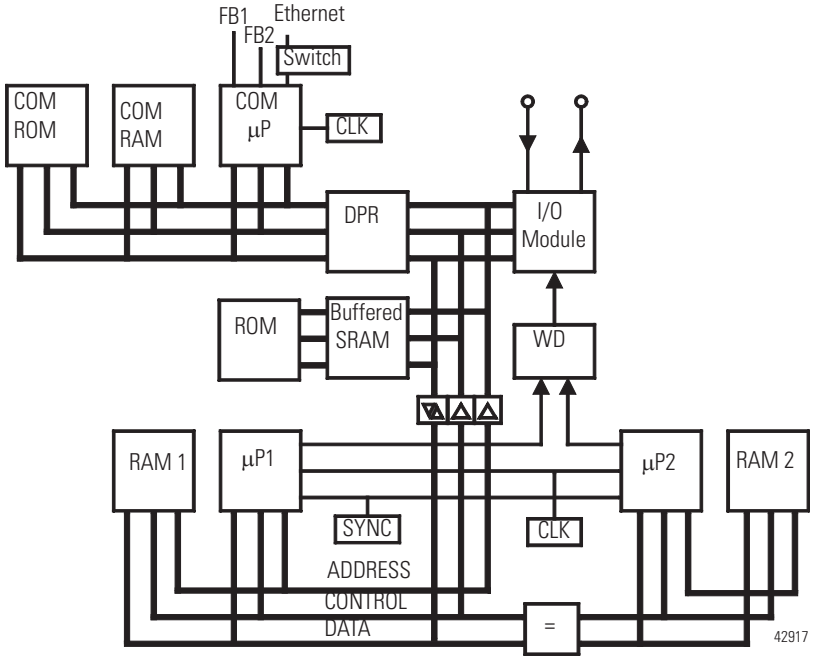
The power supply transforms the system supply voltage from 24V to 3.3V DC/ 5V DC (used for internal I/O Bus).

The power supply used with the GuardPLC 1200, 1600, or 1800 controllers must feature galvanic isolation since inputs and outputs are not electrically isolated from the processor. In addition, it must fulfill the requirements of IEC 61131-2 and SELV (Safety Extra Low Voltage) or PELV (Protective Extra Low Voltage).

Functional Description of the Central Processing Unit

The central processing unit of the GuardPLC controllers consists of the following function blocks.

Figure 1 - Display of the Function Blocks (Using GuardPLC 2000 Controller)



Features of the central module are listed below.

- Two cycle synchronous microprocessors (µP1 and µP2)
- Each microprocessor has its own memory (RAM 1 and RAM 2)
- Testable hardware comparators for all external access of both microprocessors
- The watchdog (WD) is set to the safety state in case of an error
- Flash EPROMs of the program memory for the operating system and application program - suitable for a minimum of 100,000 programming cycles
- Data memory in SRAM (Static RAM)
- Multiplexer for the connection of I/O bus, Dual Port RAM (DPR)
- Buffering for SRAMs via batteries
- Interface for data exchange between the GuardPLC controllers and programming software (PC) based on Ethernet
- Additional interfaces for data exchange by field bus
- System condition indicated by status indicators
- I/O-bus-logic for the connection with I/O modules
- Safety watchdog (WD)
- Power supply module monitor, testable (3.3V DC/5V DC system voltage)

Self-test Routines

The most important self-test routines for the safety GuardPLC controller's central processing unit and the interface to the I/O level are described in the following sections.

Microprocessor Test

The following items are checked during the microprocessor test.

- All used commands and addressing modes
- Write condition of the flags and the commands controlled by flags
- Write condition and the cross-linking of the registers

Test Memory Sectors

The operating system, the application program, the constants and parameters, and the variable data are stored in every central processing unit in both processor sectors and are tested by a hardware comparator.

Fixed Memory Sectors

The operating system, application program, and parameter sector are each filed in one memory. They are secured by write-protection and a CRC test.

RAM Test

The RAM sectors, particularly stuck-at and cross-coupling, are tested with a Write/Read test.

Watchdog Test

The watchdog is switched off if it is not triggered by the two CPUs within a defined time window. The same applies if the test of the hardware comparators fails. A separate test determines whether the watchdog signal is able to switch off.

Test of the I/O Bus Within the System

The connection between the CPU and the related I/O points or I/O modules is checked.

Reactions to Detected Errors in the CPU

A hardware comparator within the central area constantly compares whether the data of microprocessor system 1 are identical to the data of microprocessor system 2. If this is not the case, or if the test routines in the central area are negative, the system automatically goes into FAILURE_STOP mode and the watchdog signal is switched off. Input signals are no longer processed, and outputs go to the de-energized, switched-off condition.

GuardPLC Controllers and I/O Modules Error Diagnostics

Because the GuardPLC 1200, 1600, and 1800 controllers are compact systems, error diagnostics are summarized in a collective error status indicator.

Each GuardPLC distributed I/O module has its own status indicator to display errors in case of module failures or faults in the external wiring, providing a quick error diagnosis in case of module failure.

The evaluation of system variables that contain the status value of the I/O or the CPU can also be monitored in the application program.

An error signal is transmitted only if the error does not impede communication with the CPU, that is, an evaluation via the CPU is still possible.

An extensive diagnostic record of system performance and faults is stored in the diagnostic memory of the CPU and the COM. This record can be viewed in the programming software, even after a system fault.

GuardPLC Controller and GuardPLC I/O Module Input Channels

Chapter Introduction

This chapter gives information about GuardPLC controllers and GuardPLC I/O module input channels.

Overview

See the table below for an overview of GuardPLC controller input capabilities.

Controller/Module	Type	Quantity	Safety-Related	Electrically Isolated
GuardPLC 1200 Controller	Digital Input	20	X	—
	24-bit Counter	2	X	—
GuardPLC 1600 Controller	Digital Input	20	X	—
GuardPLC 1800 Controller	Digital Input	24	X	—
	24-bit Counter	2	X	—
	Analog Input	8	X	—
GuardPLC 16-point DC Input Module, 1753-IB16	Digital Input	16	X	—
GuardPLC 20/8 DC I/O Module, 1753-IB20XOB8	Digital Input	20	X	—
GuardPLC 8/8 DC I/O Module, 1753-IB8XOB8	Digital Input	8	X	—
GuardPLC 16/8 DC I/O Module, 1753-IB16XOB8	Digital Input	16	X	—
GuardPLC 2000 DIO,1755-IB24XOB16	Digital Input	24	X	X
GuardPLC 2000 CO, 1755-HSC	24-bit Counter	2	X	X
GuardPLC 2000 AI, 1755-IF8	Analog Input	8	X	X
GuardPLC Analog Input/Output Module, 1753-IF8XOF4	Analog Input	8	X	—

General Information on GuardPLC Safety Input Modules

The GuardPLC safety input modules can be used both for safety and standard inputs.

The GuardPLC safety input modules have a diagnostic status indicator, quick error detection, and error localization.

In addition, status messages can be evaluated in the application program. I/O errors stored in the diagnostic buffer can be read via RSLogix Guard PLUS! software.

Safety input modules are automatically submitted to a high-grade, cyclical self-test in the GuardPLC controller during operation. These test routines are TÜV-approved and help the high integrity operation of the respective module.

When an error is detected, a 0 signal is sent to the application, and a detailed error message can be generated. If there are minor failures in the module that do not affect the safety function, user diagnostic information is not generated.

Safety of Sensors, Encoders, and Transmitters

In a Safety application, the sensors and the PES must meet the same target SIL.

In this case, the safety sensors, encoders, or transmitters can be directly connected to the inputs of the PES.

If no sensors, encoders, or transmitters with the required SIL are available, sensors, encoders, or transmitters can still be connected. However, the connection and monitoring of the signals must be programmed in the application program.

Refer to IEC 61511-1, Clause 11.4 and Table 5 for information on achieving the necessary SIL.

Digital Inputs

The items listed in the following section apply to all of the digital input channels listed in the Overview on page 28, if no specific module is named.

General

The digital inputs are read once in every cycle and values are stored internally. The inputs are tested cyclically for safety function. Input signals, whose pulse width is shorter than two times the scan time, are not processed.

Test Routines

The online test routines perform a walking input test to check whether the input channels are able, independent of the pending input signals, to make a through-connection of both signal levels (L- and H- signal). This functional test is executed with every input signal reading. The 0 signal (safety state) is processed in the application program for every error in the input module.

Because the PES has been designed to the closed-circuit current principle, a 0 signal is processed for the digital inputs in case of error.

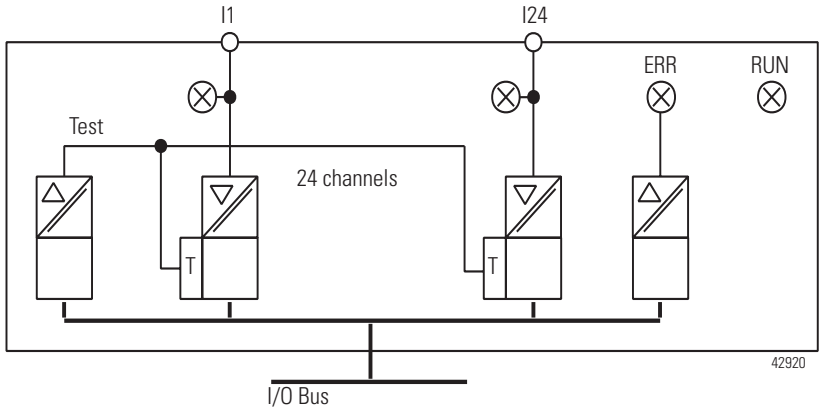
See page 14 for an explanation of the closed-circuit current system principle.

Reaction To Error

If the test routines detect an error in digital inputs, a 0 signal is processed in the application program for the faulty channel. The FAULT indicator (ERR on the GuardPLC 2000 controller) is activated.

In addition to the signal value of the channel, the corresponding channel status signal must be taken into account. When using the channel status signal in the application program, you have additional options to configure an error reaction in your program.

Figure 2 - Example Block Diagram of Digital Inputs (Using GuardPLC 2000 Controller)



The illustration above does not represent the specifications of the related module.

Surge on Digital Inputs

An EN61000-4-5 surge impulse can be read as a short-time H signal, caused by the short cycle time of the GuardPLC system. To avoid errors of this type, use one of the following preventative measures.

- Install shielded input lines to eliminate the effects of surges in your system.
- Use fault masking in your user program so that a signal must be present for at least two cycles before being evaluated. Be aware that this increases the system's reaction time.

ATTENTION: The mentioned measures can be neglected if surges in the system can be excluded by the construction of the plant. The construction includes especially protection measures concerning overvoltage, lightning strike, earthing and wiring on base of manufacturers instructions and relevant standards.

Configurable Digital Inputs

The digital inputs of the GuardPLC 1800 controller operate according to the principle of analog inputs, but are set to digital values by configuration of the operating points.

The test routines and safety functions of analog inputs, explained on pages 33...36, also apply to the configurable digital inputs on the GuardPLC 1800 controller.

Line Control

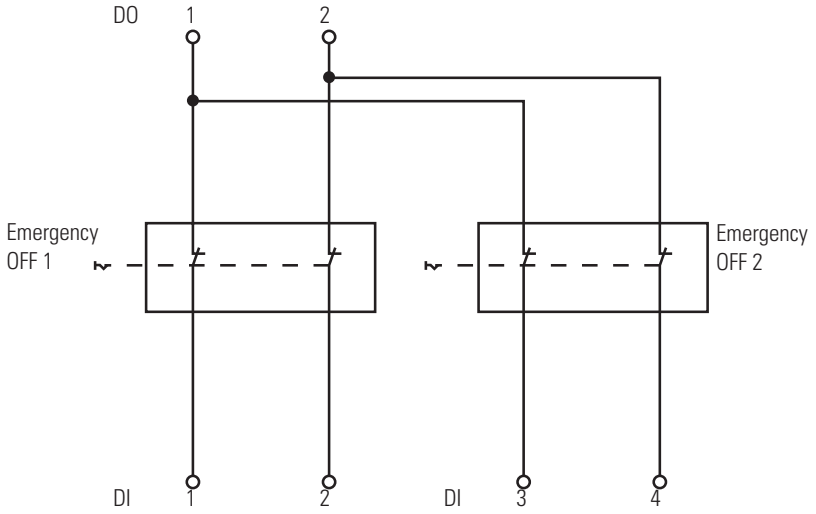
Line Control is an emergency short-circuit and line-break monitoring system of emergency stop devices, which can be configured on GuardPLC 1600 systems with digital inputs. This does not include configurable digital inputs.

TIP GuardPLC 1200 and GuardPLC 2000 systems require application programming for line control.

IMPORTANT This operation is not permissible for configurable digital inputs, like those on the GuardPLC 1800 system. Therefore, the type of line control described above cannot be configured for GuardPLC 1800 controllers.

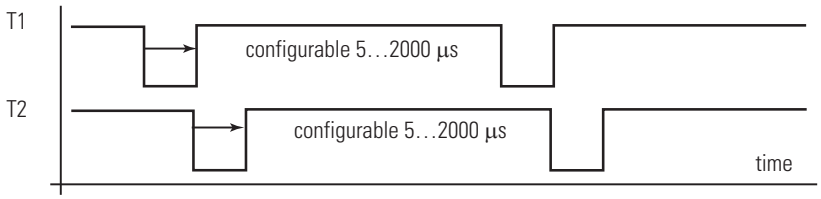
In addition, digital outputs are connected to the digital inputs of the same system, as shown in Emergency Off Switches on page 32.

Figure 3 - Emergency Off Switches



The digital outputs DO1 and DO2 are pulsed (T1 and T2 below). As a result, the connections to the digital inputs are monitored. The signals for the pulsed outputs must begin at DO1(01) and must be directly sequential.

Figure 4 - Digital Input Monitoring



The FAULT indicator on the front plate of the controller/module flashes, the inputs are set to 0 and an error code is generated when these faults occur.

- Short-circuit between two parallel connections
- Reversal of two connections
- Ground fault on one of the lines
- Line break (or opening of the contacts when one of the Emergency OFF switches is pressed)

Analog Inputs

The items listed in the following section apply to all of the analog input channels listed in the Overview on page 28, if no specific module is named.

General

IMPORTANT The safety-related accuracy is the guaranteed accuracy of the analog input without error reaction of the module. This value should be taken into account when the safety functions are configured.

In the eight analog input channels available in each module, the incoming signals are converted into an INTEGER value in 12-bit resolution. This value can then be used in the application program.

The following input values are possible for the GuardPLC 1800 controller.

Number of Input Channels	Polarity	Current/Voltage	Value Range In Application	Accuracy(5)
8	single-ended	0…10V DC	0…1000(1) 0…2000(2)	2%
8	single-ended	0/4…20 mA	0…500(1)(3) 0…1000(1)(4) 0…1000(2)(3) 0…2000(2)(4)	2%

(1) With scale factor 1000 selected in RSLogix Guard PLUS! software.
(2) With scale factor 2000 selected in RSLogix Guard PLUS! software.
(3) By external 250 Ω shunt.
(4) By external 500 Ω shunt.
(5) Accuracy is the guaranteed accuracy of the analog input without error reaction of the module. This value must be considered when safety functions are configured.

The 1755-IF8 (AI module) can be configured as either eight single-ended channels or four differential channels. No mixing is allowed. The following input values are possible.

Number of Input Channels	Polarity	Current/Voltage	Value Range In Application	Accuracy[5]
8	single-ended	-10…10V DC	0…1000[1] 0…2000[2]	1%
8	single-ended	0/4…20 mA	0…500[1][3] 0…1000[1][4] 0…1000[2][3] 0…2000[2][4]	1%
4	differential	-10…10V DC	-1000…1000[1] -2000…2000[2]	1%

(1) With scale factor 1000 selected in RSLogix Guard PLUS! software.
(2) With scale factor 2000 selected in RSLogix Guard PLUS! software.
(3) By external 250 Ω shunt.
(4) By external 500 Ω shunt.
(5) Accuracy is the guaranteed accuracy of the analog input without error reaction of the module. This value must be considered when safety functions are configured.

The following input values are possible for the 1753-IF8XOF4 module.

Number of Input Channels	Polarity	Current/Voltage	Value Range In Application	Accuracy
8	Uni-polar	0…10V DC	0…2000	2%
8	Uni-polar	0/4…20 mA	0…1000[1] 0…2000[2]	2%

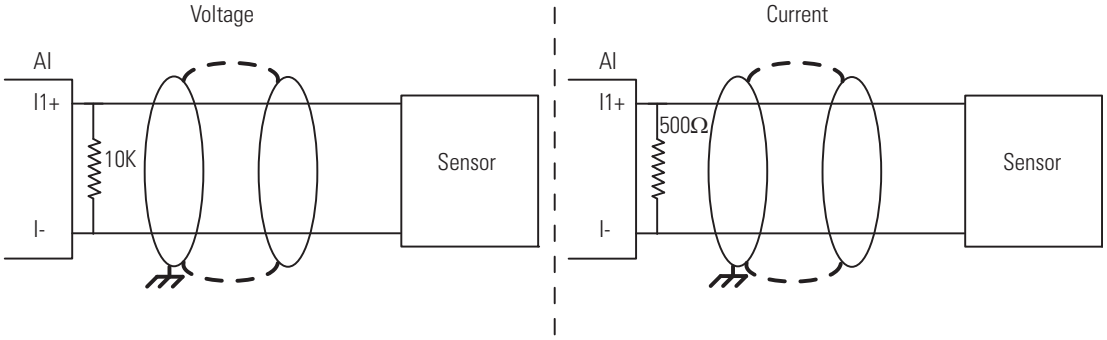
(1) By external 250 Ω shunt.
(2) By external 250 Ω shunt.

All of the channels default to voltage mode. On a channel-by-channel basis, a shunt resistor can be added in parallel with the analog device if current mode is requested. In current mode, the 10 K resistor specified below is not required.

The 1755-IF8 AI module does not perform line monitoring. Therefore, in the event of a wire break, an input signal continues to process.

In the event of an error line break, the input voltage floats and the resulting value is not reliable. The inputs must be terminated with a 10 KΩ resistor parallel to the sensor. The internal resistance of the source must be taken into account.

Figure 5 - Example Line Break Voltage



IMPORTANT Unused analog input channels must be short-circuited.

TIP For unused analog input channels, the corresponding signal AI[0x].Used must be set to the default value 0 (FALSE).

Test Routines

The analog values are processed in parallel via two multiplexers and two analog/digital converters with 12-bit resolution. The results are compared. In addition, test values are switched on via digital/analog converters and converted back again to digital values that are then compared with a default value.

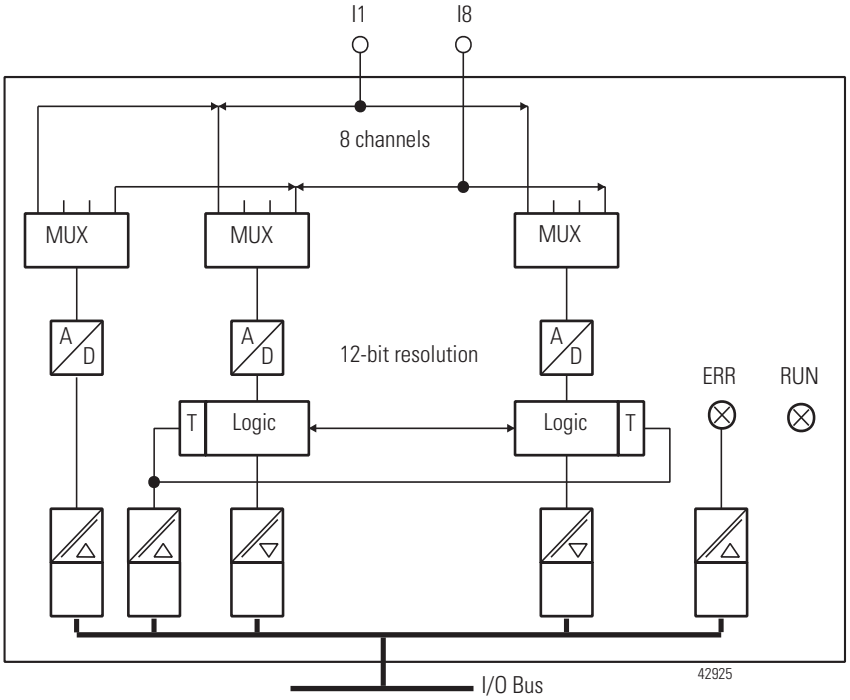
When faults are detected, the analog inputs are set to the 0 value in the application program.

Reaction In Case of Fault

If the test routines for analog inputs detect an error, a 0 value is processed for the faulty channel in the application program, and the FAULT status indicator illuminates.

In addition, a channel status signal greater than 0 is generated for the application program. The analog input value must be interlocked with this status information, allowing you to program additional fault handling in the applications and provide a means for evaluating the external wiring of the inputs.

Figure 6 - Block Diagram of Analog Inputs of the 1755-IF8 Analog Input Module



The illustration above does not represent the specifications of the related module.

Counter Module

The items listed in the sections starting on page 36 apply to the 1755-HSC module and to the GuardPLC 1200 and 1800 system digital counter input channels.

General

Depending on the parameters in the application program, the counter can be operated as a fast up/down counter with 24-bit resolution or as an encoder in the Gray code.

When used as a quick up/down counter, the signals of the impulse input and the counter direction are necessary in the application. A reset can be accomplished only via the user program.

The 1755-HSC module features 4- or 8-bit encoder resolution. In the GuardPLC 1200 and 1800 controller, the encoder has a resolution of 3- or 6-bit. Reset is possible.

Linking two independent 4-bit inputs to one 8-bit input (for example, in the 1755-HSC) is effected exclusively by the program. Switching is not available in this instance.

The encoder function monitors the change of the bit pattern at the input channels. The bit patterns pending at the channels are directly transferred to the application program. The programming software displays a decimal figure corresponding to the bit pattern. Depending on the application, this figure can be converted into BCD code.

Test Routines

When the counter is operated as an encoder in the Gray code, only one input bit may be modified at a time.

If there are faulty codes, the operating system sets a corresponding channel status signal.

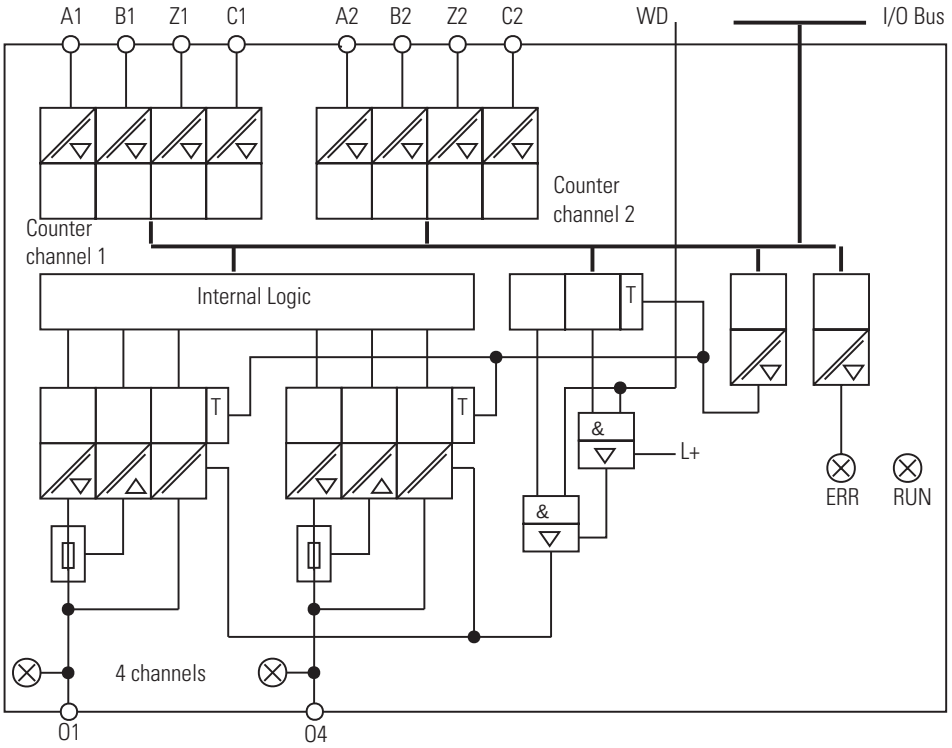
Reaction In Fault Condition

If an error is detected in the counter section of the module, the error message must be evaluated in the application program.

The respective channel status signal must be considered.

You can configure an error reaction in the logic and trigger it the with the channel status signal.

Figure 7 - Example Block Diagram of Counter Inputs (Using 1755-HSC Module of the GuardPLC 2000 System)



This display does not represent the specifications of the related module.

Checklist for Safety Inputs

Use the checklist on the following page for system configuration, programming and start-up of safety inputs.

It may be used as a planning draft as well as a proof. If used as a planning draft, the checklist can be saved as a record of the plan.

To ensure that the requirements are fully and clearly satisfied during system configuration or start-up, an individual checklist for controlling the requirements can be filled in for every single safety output channel in a system. This checklist can also be used as documentation on the connection of external wiring to the application program.

Checklist for Configuration, Programming, and Startup of Safety Manual GuardPLC System

Company:	
Site:	
Loop definition:	

Safety input channels in the:

☐ GuardPLC 1200 ☐ GuardPLC 1800

☐ GuardPLC 1600 ☐ GuardPLC 2000

No.	Requirements	Fulfilled		Comment
		Yes	No	
1	Is this a safety input?	☐	☐	
2	Is the error message processed in the application program? [VALUE=0] and [CHANNEL STATUS≠0]	☐	☐	
3	Is this a digital input?	☐	☐	If no, go to 6
4	Is the hysteresis for the digital inputs configured correctly? (GuardPLC 1800 and 2000)	☐	☐	
5	Is line control (pulse testing) used for this input?	☐	☐	
6	Is this an analog input?	☐	☐	If no, go to 15
7	unipolar 0…10V DC? unipolar 0…10V DC? (1755-IF8 only)	☐	☐	
8	unipolar 0…20mA?	☐	☐	
9	bipolar ±10V DC? (1755-IF8 only)	☐	☐	
10	Is the voltage input terminated or programmed for application fault handling?	☐	☐	
11	Do the ranges of the sensors set fit the channel configuration?	☐	☐	
12	Are the unused analog inputs short-circuited?	☐	☐	
13	Are the error code system signals for the used input channels evaluated in the logic?	☐	☐	
14	Has the AI[0x].Used signal been configured properly for used and unused analog inputs?	☐	☐	
15	Is this input a counter?	☐	☐	
16	Function: Pulse counter?	☐	☐	
15	Function: Encoder (Gray code)?	☐	☐	
16	Has a safety encoder/sensor been provided for this input?	☐	☐	

Notes:

GuardPLC Controller and GuardPLC I/O Output Channels

Chapter Introduction

This chapter gives information about GuardPLC 1200 and GuardPLC 2000 output modules.

Overview of GuardPLC Output Modules

See the table below for an overview of GuardPLC output capabilities.

Controller/Module	Type	Quantity	Safety-related	Electrically Isolated
GuardPLC 1200	Digital Output	8	X	—
GuardPLC 1600 Controller	Digital Output	8	X	—
GuardPLC 1800 Controller	Digital Output	8	X	—
GuardPLC 16-point DC Output Module 1753-OB16	Digital Output	16	X	—
GuardPLC 20/8 DC I/O Module 1753-IB20XOB8	Digital Output	8	X	—
GuardPLC 8/8 DC I/O Module 1753-IB8XOB8	Digital Output	8 (1-pole)	X	—
		2 (2-pole)	—	—
GuardPLC 16/8 DC I/O Module 1753-IB16XOB8	Digital Output	16 (1-pole)	X	—
		8 (2-pole)	X	—
GuardPLC 2000 DIO Module 1755-IB24XOB16	Digital Output	16	X	X
GuardPLC 2000 CO Module 1755-HSC	Digital Output	4	X	X
GuardPLC 2000 AO Module 1755-OF8	Analog Output	8	X	X
GuardPLC Relay Module 1753-OW8	Relay Output(1)	8	X	X
GuardPLC Analog Input/Output Module, 1753-IF8XOF4	Analog Output	4	X(2)	—

(1) Relay outputs cannot be used as pulsed outputs.

(2) The analog outputs may be used only as safety-related outputs if the output values are read back to safety-related analog inputs and evaluated in the user program.

General Safety Information on GuardPLC Safety Outputs

The GuardPLC safety output modules are written to once in every cycle. The output signals are read back and compared with the output data given by the application logic.

For outputs, 0 is the safety state (or an open relay contact).

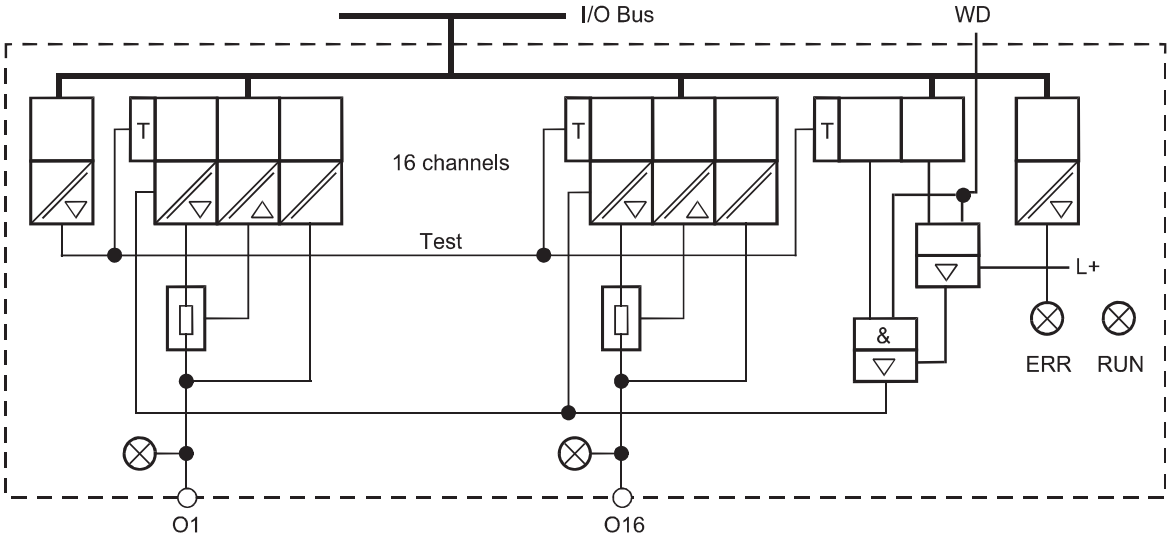
Three testable semi-conductor switches have been integrated, in series, into the safety output modules. Thus, the second independent switch-off, required for safety technical reasons, has been integrated on the output module.

This integrated safety switch-off safely shuts down all channels of the output module (de-energized condition) if an error occurs.

In addition, the watchdog (WD) signal from the CPU module also affects the safety switch-off. The cessation of the WD signal results in the immediate transition to the safety state. This function is effective only for all digital outputs and relay outputs of the controller.

In addition, the respective channel status signals can be evaluated in the application program.

Figure 8 - Example Block Diagram of Digital Outputs (Using AB-DIO of the GuardPLC 2000 System)



The illustration above does not represent the specifications of the related module.

Digital Outputs for Non-relay Output Modules

Non-relay output modules have these types of digital outputs.

Test Routines

The modules are automatically tested during operation. These are the essential test functions.

- Read back of the output signal of the output amplifiers. The switching threshold for a read back 0 signal is 2V. The diodes provided prevent feedback of signals.
- Check the integrated double-safety switches.
- Low supply voltage protection. If the supply voltage drops below 13V, you cannot turn on any outputs.
- Digital outputs are turned off for a maximum of 200 µs each (200 x 10E-6 s) at a minimum interval of 20 seconds.

Reaction to Error

The following conditions may occur as a result of errors.

Faults

If an output fault is detected, the affected output of the module is set to a safety, de-energized state via the safety switches. In case of a module fault, all outputs are switched off. Both faults are indicated via the FAULT indicator.

External Short-circuit or Overload

Module tests can still be performed, even when there is a short-circuit at an output. It is not necessary to switch off via a safety shut-down.

The total current draw of the module is monitored. If the threshold is exceeded, all channels of the output module are set to the Safety state (0).

If an error occurs, the output, in accordance with the rules of the closed-circuit principle, is set to zero voltage. Outputs continue to be monitored at intervals of several seconds to determine if the overload is still present. When normal state resumes, outputs are re-connected to the load.

Line Control

Safety digital outputs can be cycled with the safety digital inputs of the same system to allow short-circuit or line-break monitoring using Emergency Stop devices (according to Ple/Cat. 4 in ISO 13849-1).

See Line Control on page 31.

IMPORTANT	This operation is not permissible for configurable digital inputs, like those on the GuardPLC 1800 controller. Therefore, the type of line control described above cannot be configured for GuardPLC 1800 controllers.

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

Safety-related Two-pole Digital Outputs

The information in this section applies to the two-pole digital outputs of the 1753-IB16XOB8 and 1753-IB8XOB8 modules.

Test Routines for Two-pole Digital Outputs

The modules are automatically tested during operation. These are the essential test functions.

- Read-back of the output signal of the switching amplifier. The switching threshold for a read-back signal is 2V. Diodes are used to prevent a feedback of signals.
- Check the integrated (redundant) safety shutdown.
- Perform a shutdown test of the outputs within the multiple fault occurrence time for a max. of 200 µs. The minimum time between two tests is 20 seconds.
- Monitor line at two-pole connection
  - short-circuit to L+, L-
  - short-circuit between two-pole connections (1753-IB16XOB8 only)
  - line break in one of the two-pole lines (1753-IB16XOB8 only)
- Test L- switch capability at two-pole connection with line monitoring (1753-IB16XOB8 only)
- Monitor the output current of the device

The operating voltage of the entire system is monitored. All outputs are de-energized at an undervoltage of < 13V.

One-pole / Two-pole Connection

The digital outputs can be configured as follows:

- Digital output with two-pole connection with line monitoring
- Digital output with two-pole connection without line monitoring
- One-pole positive-switching digital output (DO+)
- One-pole negative-switching digital output (DO-)

Two-pole Connection

ATTENTION: The status signal of the line monitoring must be used to switch off the outputs (DO+, DO-) in case of a fault for ISO 13849-1 PLe/Cat. 4 applications.

ATTENTION: A short-circuit between a negative switching output and L- can cause a relay to switch on or another actuator to be switched into another operating state.
During monitoring time of line monitoring a 24 V voltage (L+ reference pole) is impressed at the load (relay, actuator), so that the amount of electric energy is great enough to switch the load in another operating state.

ATTENTION: When the module is configured for two-pole operation, a DI input may not be connected to a DO output. This would prevent a detection of a line break.

ATTENTION: Inductive loads must be connected with a protection diode on the load.

Reaction in the Event of an Internal Fault

The module has negative-switching outputs and positive-switching outputs. This section describes how they react to an internal fault.

Negative-switching Outputs (DO-)

If a output fault is detected, the affected output of the module is set to a safety, de-energized state via the safety switches. In case of a module fault, all outputs are switched off. Both faults are indicated via the FAULT indicator.

Positive-switching Outputs (DO+)

If an output fault is detected, the affected output of the module is set to a safety, de-energized state via the safety switches. In case of a module fault, all outputs are switched off. Both faults are indicated via the FAULT indicator.

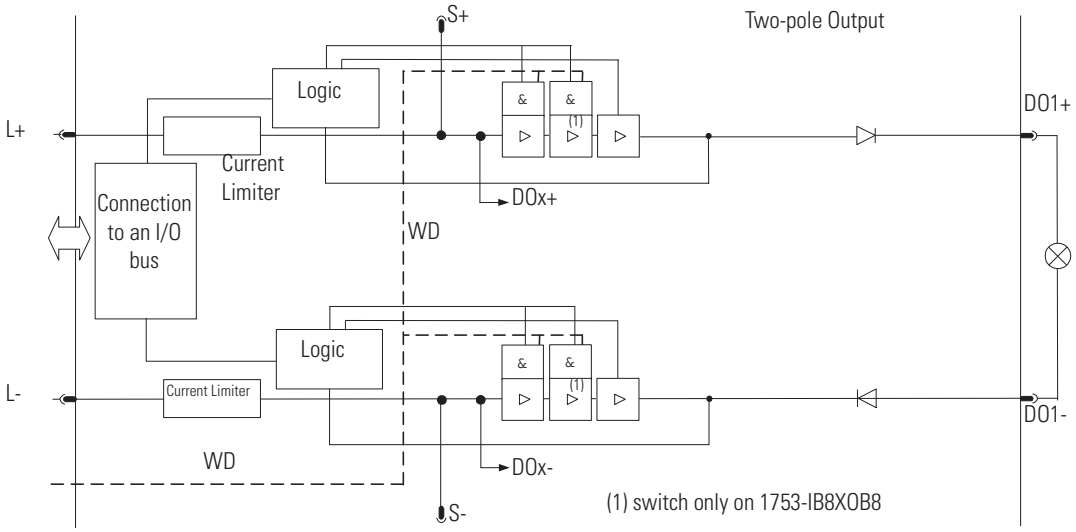
External Short Circuit or Overload Performance

If the output is short-circuited to L-, L+, or an overload condition exists, it is still possible to carry out tests on the module. A safety shutdown is not required.

The total current consumption of the module is monitored. If the threshold is exceeded, all the channels of the output module are set to the safety 0 state.

In this state the outputs are cyclically checked (in periods of several seconds) if the overload is still present. Once the short-circuit or overload condition is corrected, the outputs are activated according to the application program.

Figure 9 - Two-pole Digital Outputs in 1753-IB8XOB8 and 1753-IB16XOB8 Modules



Relay Outputs in the 1753-OW8 Module

The information in this section applies to the relay outputs of the 1753-OW8 module.

Test Routines

The modules are automatically tested during operation. These are the essential test functions.

- Read-back of the output signal of the switching amplifiers before the relays.
- Test the switching of the relays with positively guided contacts.
- Test the integrated redundant safety shutdown.

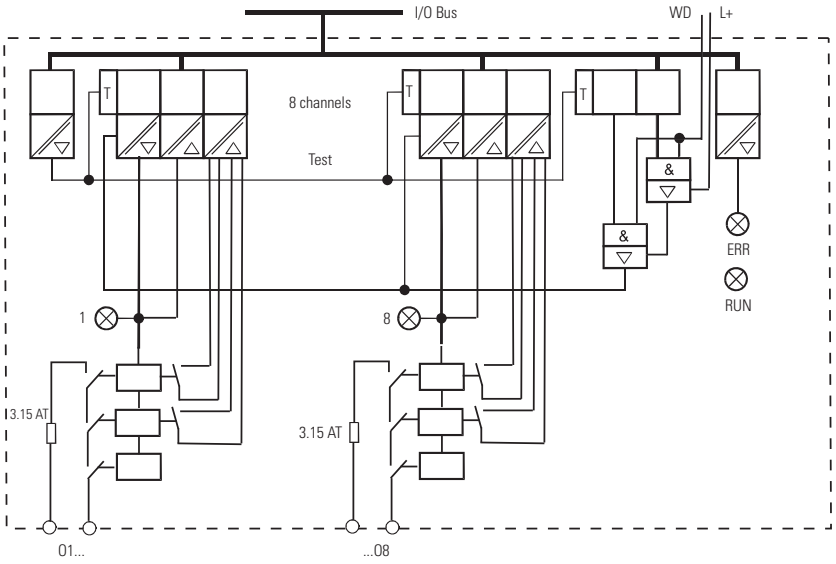
The operating voltage of the entire system is monitored, de-energizing all outputs at an undervoltage of <13V.

At the 1753-OW8 module, the outputs are equipped with three safety relays; two relays with positive guided contacts and one MSR type enabling the outputs to be used in safety shutdowns.

Reaction To Error

If a faulty signal is detected, all contact outputs of the module are set to the safety (0) state via the safety switches in accordance with the closed-circuit principle. This is also indicated by the FAULT diagnostic status indicator.

Figure 10 - Relay Outputs in the 1753-OW8



Analog Outputs in the 1753-IF8XOF4

The analog outputs are written once every cycle and the values are saved internally.

All the outputs are non-safety related but they can all be shut down safely.

To reach SIL 3, the outputs values must be read back via safety-related analog inputs and evaluated in the application program. There are also reactions to incorrect output values that must be specified.

Test Routines

Both the safety switches for the shutdown of all four outputs of the module are automatically tested during operation.

Reaction to Error

If a faulty signal is detected, all contact outputs of the module are set to the Safety (0) state via the safety switches in accordance with the closed-circuit principle. This is also indicated by the FAULT diagnostic indicator.

The error code signal enables you to provide additional fault handling in the application program.

Analog Outputs in the 1755-OF8 Module

The information in this section applies to the analog outputs of the 1753-OF8 module.

General

The analog outputs on the 1755-OF8 GuardPLC 2000 (AB-AO) module are written once per cycle and stored internally. This functionality is tested by the module itself.

The analog output module can be configured for current or voltage output via DIP switches on the module.

ATTENTION: Check the switch settings before inserting the module into the chassis, and make sure that the settings in the application program coincide with the hardware configuration. Configuring the hardware for current output and the application program for voltage output results in erroneous behavior of the module.

ATTENTION: Unused analog voltage outputs must be left open. Unused analog current outputs must be short-circuited.

The analog output circuits contain current/voltage monitoring, read back and testing of parallel output circuits, and two additional safety switches for the safe disconnection of the output circuit in the event of failure. Thus, the safe condition is achieved at an output current of 0 mA and an output voltage of 0V DC.

Respectively two analog outputs are DC coupled to each other (output 1 and 2, output 3 and 4, output 5 and 6, output 7 and 8).

In addition, the respective channel status signals can be evaluated in the application program.

Test Routines

The module is automatically tested in operation. These are the essential test functions.

- Safety 1oo2 A/D Microprocessor system.
- Double read back of output signals.
- Test for cross-talk between the outputs.
- Check of the integrated safety switch-off.

Reaction To Error

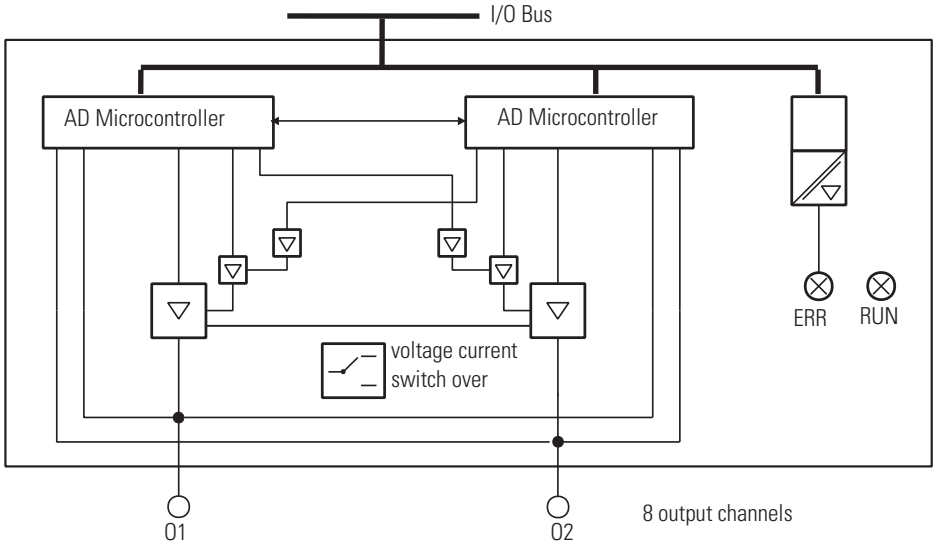
The output signals are read back once per cycle and compared with the internally stored output signals of the intelligent module 1755-OF8 (AB-AO). If a discrepancy is detected, the faulty output channel is switched off via the two safety switches, and the module failure is reported via the FAULT indicator.

The error code signal enables the user to provide additional fault handling in the application program.

For the worst case reaction time of the analog outputs, add double the watchdog time (WDZ_{CPU} x 2) of the controller to double the watchdog time of the output module ($WDZ_{AO\text{-}\mu C}$ x 2).

See the specifications for the worst-case reaction time.

Figure 11 - Example Block Diagram of Analog Outputs (Using 1755-OF8)



This illustration does not represent the specifications of the related module.

TIP The value of an analog output depends on the scaling factor selected in RSLogix Guard PLUS!.

Checklist for Safety Outputs

Use the following checklist for system configuration, programming and start up of safety outputs.

It may be used as a planning draft as well as a proof. If used as a planning draft, the checklist can be saved as a record of the plan.

To make sure that the requirements are fully and clearly satisfied during system configuration or start-up, an individual checklist for controlling the requirements can be filled in for every single safety output channel in a system. This checklist can also be used as documentation on the correlation of external wiring to the application program.

Check List for Configuration, Programming, and Start-up of Safety Manual GuardPLC Systems

Company:	
Site:	
Loop definition:	

Safety output channels in the:

☐ GuardPLC 1200 ☐ GuardPLC 1800

☐ GuardPLC 1600 ☐ GuardPLC 2000

No.	Requirements	Fulfilled		Comment
		Yes	No	
1	Is this output channel a safety output?	☐	☐	
2	Is the error message processed in the application program?	☐	☐	
3	Has the signal AO[0x].Used been configured properly for used and unused analog outputs?	☐	☐	
4	Is this a digital output?	☐	☐	If no, go to 10
5	Is the channel load corresponding to the maximum permissible value?	☐	☐	
6	Is load of system/module corresponding to the maximum permissible value?	☐	☐	
7	Are RC circuits provided on the control elements?	☐	☐	
8	Has the actuator been connected according to specifications?	☐	☐	
9	Is this output used exclusively for line control (pulse testing)?			
10	Is this an analog output?	☐	☐	
11	Voltage outputs DIP switch positions checked?	☐	☐	
12	Current output? DIP switch positions checked?	☐	☐	
13	Have unused analog voltage outputs been left open?	☐	☐	
14	Have unused analog current outputs been short-circuited?	☐	☐	
15	Is a safety actuator planned for this output?	☐	☐	

Chapter 5

GuardPLC DeviceNet Safety Scanner

Chapter Introduction

This chapter gives information about the GuardPLC DeviceNet Safety Scanner included in a GuardPLC Safety System.

Overview

Before operating a GuardPLC safety system containing a DeviceNet safety scanner, you must read, understand, and follow the installation, operation, and safety information provided in the publications provided in the following table.

The DeviceNet safety scanner provides DeviceNet access for GuardPLC controllers via High-speed Safety Protocol (HSP). The safety scanner supports standard DeviceNet Master and Slave connections as well as DeviceNet safety originator and target connections.

Catalog Number	Description	Installation Instructions	User Manual
1753-DNSI	DeviceNet Safety Scanner for GuardPLC	1753-IN009	1753-UM002

In addition, there are the following essential functions.

- Comprehensive self-tests
- Data transfer over DeviceNet Safety Network
- Diagnostics

Certification

Certificate No. 968/EZ 200.00/05
TÜV Rheinland Group
TÜV Industrie Service GmbH
Automation, Software, and Informatinstechnologie

Safety Requirements for DeviceNet Safety Scanner

The DeviceNet Safety Scanner is typed-approved and certified for use in applications up to and including SIL 3 according to IEC 61508, and applications up to and including Cat. 4 according to ISO 13849-1.

For configuring DeviceNet Safety Scanner use RSNetWorx for DeviceNet software version 6.00 or later.

The High-speed Safety Protocol (HSP) allows the exchange of safety and standard data between the DeviceNet safety scanner and GuardPLC 1600 and 1800 controllers. The DeviceNet safety scanner and GuardPLC controller interchange safety input and output data, and standard input and output data tables. Safety application data tables are protected from standard data.

Safety and Standard Data

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 by the end device.
- 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.

Commission Safety Devices

In the HSP signal connection dialogs (in RSLogix Guard PLUS! software), 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.

The colorization applies only to the Connect Signals dialogs available from the HSP protocol context menu. It is recommended that you use a naming convention to visually distinguish between standard and safety signals in the 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

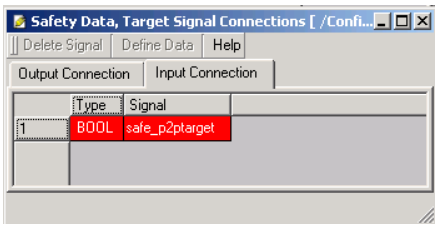
Any safety tags that appear in the Standard Connect Signals window must be treated as standard values in your application.

Any standard tags that appear in the Safety Connect Signals window must be treated as standard.

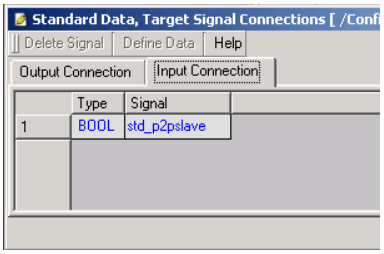
For a signal to be regarded as a safety value in your application, the end device configuration must treat the signal as safety and be transferred over a DeviceNet safety connection.

Figure 12 - Connect Signals Dialogs

Safety Connect Signals Dialog Box



Standard Connect Signals Dialog Box



You must commission all safety devices with the MAC ID and communication rate, if necessary, before their installation on the safety network. MAC ID and communication rate settings for the DeviceNet safety scanner are made via RSNetWorx for DeviceNet software.

A scanner can be configured by only RSNetWorx for DeviceNet software that automatically becomes its configuration owner.

PFD and PFH Calculations

Component	Functional Verification Test Interval	PFD
1753-DNSI	10 years	9.3E-06

Component	PFH
1753-DNSI	5.61E-10

The Functional Verification Test interval is set at 10 years for the GuardPLC DeviceNet safety scanner. The test does not apply to the DeviceNet safety I/O module.

The DeviceNet safety scanner is based on a 1oo2 microprocessor system for the control module.

SFF and HFT Calculations

Component	SFF	HFT
1753-DNSI	98.0%	1

Multiple Error Occurrence Time

The occurrence time for multiple faults is the period of time in which the probability for the occurrence of multiple faults, which in combination are critical to safety, is sufficiently low.

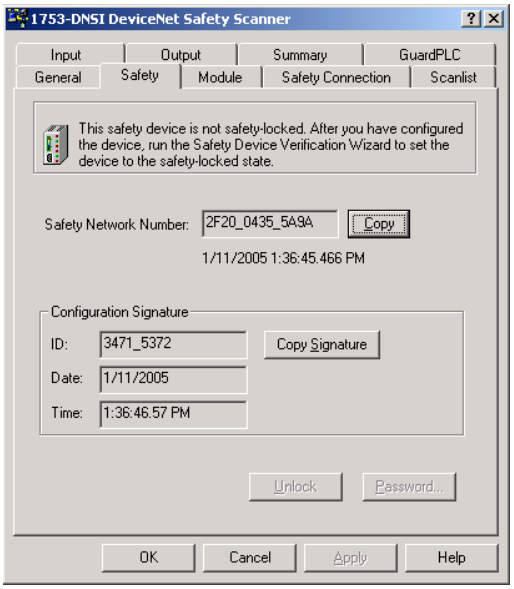
Faults that do not directly affect the safety function of the system unless they occur in combination with another fault are detected within the Multiple Error Occurrence Time, which is preset in the operating system of the safety scanner to eight hours.

Configuration Signature

The configuration signature uniquely identifies a particular module configuration. It is comprised of a checksum (ID) and the date and time that the configuration was created. The configuration signature is used in several operations.

- During download from a configuration tool, the configuration signature provides you with a means to check that the device and the configuration tool agree on the information downloaded.
- During connection establishment, the originator and the target devices use the Configuration Signature to ensure that both devices are using the expected configuration.

Figure 13 - Configuration Signature



Safety Network Number

The Safety Network Number (SNN) is a unique number that identifies the safety network sub-net. The SNN in conjunction with the target's node address, enables a target to determine with high integrity whether or not safety connection requests it receives have reached the correct destination.

Each end node within a DeviceNet safety control system must have a unique node identifier. The unique node reference for a DeviceNet safety node is a combination of a SNN and the node address of the node. It is used to precisely identify the intended target device during configuration and I/O connection establishment.

Any device that originates a safety connection to another safety device must be configured with the SNN of the target device.

The assignment of a time-based SNN is the default when adding a DeviceNet safety scanner or new DeviceNet safety I/O modules.

IMPORTANT	The automatic time-based SNN is generally adequate for most applications. If you assign SNNs manually, take care to ensure that system expansion does not result in duplication of SNN and node address combinations.

ATTENTION: If a safety project is copied to another project intended for a different hardware installation and that installation may reside within the same routable safety system, the SNN must be changed to ensure that the SNN is not repeated.

User Verification Procedure

Since RSNetWorx for DeviceNet software is not an SIL 3 certified application, the configuration values resulting from user operations and software computation are not considered to be of high-integrity until the download, read-back, and user testing is complete. Complete these steps to guarantee safety.

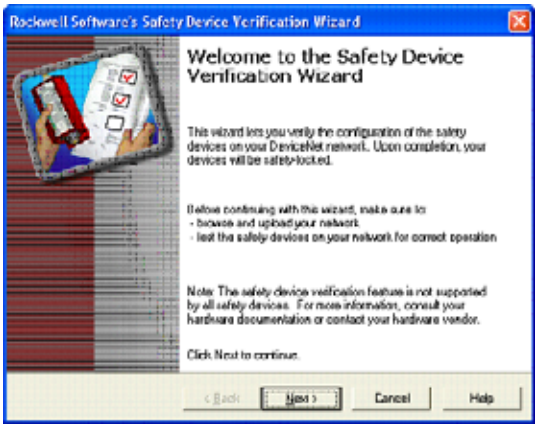
1. Assign SSN and configure devices using RSNetWorx for DeviceNet software.
2. Read back and print out the configuration from the device.
3. Compare the printed configuration to the configuration from RSNetWorx for DeviceNet software.
4. Compare printed values read back to application requirements.
5. Test the application.
6. Lock the device if errors do not occur.
7. Correct the configuration if errors occur.
8. Repeat these steps until all DeviceNet safety nodes are verified and locked.

Safety Lock with Password Protection

The configuration of the safety scanner can be protected by the use of an optional password. Download, Safety-reset, Safety-lock and Safety-unlock are password protected.

When applying functional safety, restrict access to qualified, authorized personnel who are trained and experienced. The safety-lock function, with passwords, is provided by the Safety Device Verification Wizard in RSNetWorx for DeviceNet software. You are responsible for controlling access to the safety system, including password use and handling.

After configuration data has been downloaded and verified, the configuration data within the module can be protected, using RSNetWorx for DeviceNet software. Run the Safety Verification Wizard to lock the scanner.



If you forget a password, you can reset passwords using the Vendor Password. Contact Rockwell Automation Technical Support and provide the device's serial number and security code to obtain the vendor password.

Refer to the DeviceNet Safety Scanner for GuardPLC User Manual, publication 1753-UM002, for information on the safety-lock feature or on setting a password using RSNetWorx for DeviceNet software.

Error Reaction

This section describes how the module reacts to HSP and DeviceNet connection losses and diagnostic test failure.

HSP Connection Loss

On the loss of HSP, all producing DeviceNet safety connections are transitioned to the Idle mode, resulting in the end device transitioning to its safety state. All standard DeviceNet I/O connections are likewise transitioned to Idle mode, resulting in the standard nodes transitioning to their Idle state. When the HSP connection is restored, the DeviceNet safety and standard connections are returned to Run mode with normal data production.

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 and the associated status bit is set to one.

DeviceNet Connection Loss

On the loss of a DeviceNet safety or standard connection, the data associated with connections for which the scanner is the consumer, are set to zero and the associated status bit is set to one. The scanner automatically attempts to re-establish any lost DeviceNet connections for which it is the originator. When the connection is recovered, the data is set to the values received from the producing node and the status bit is cleared.

When the safety scanner enters Configuration mode, all the DeviceNet connections are terminated and eliminated. The High-speed Safety Protocol connection is terminated. To restore connections, download and verify a new configuration.

Failure of Diagnostic Tests

If a diagnostic test fails, all application processing is stopped and High-speed Protocol, DeviceNet safety, and standard I/O connections are terminated.

Status Indicators

Options for viewing the DeviceNet safety scanner's status are listed in the following sections.

IMPORTANT	Status indicators and alphanumeric displays are not reliable indicators for safety functions. They should be used only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators as operational indicators.

Alphanumeric Display

When you apply power to the scanner, the alphanumeric display cycles through the following information.

- Firmware revision
- MAC ID
- DeviceNet communication rate

The scanner also displays status codes that provide diagnostic information. Refer to the DeviceNet Safety Scanner for GuardPLC User Manual, publication 1753-UM002, for information on status and error codes.

Status Indicators

The scanner has three status indicators that let you monitor module, DeviceNet network, and High-speed Protocol (HSP) status. The evaluation of system variables that contain the status value of the scanner can also be monitored in RSNetWorx for DeviceNet software.

For a detailed description of the status indicators, refer to the DeviceNet Safety Scanner for GuardPLC User Manual, publication number 1753-UM002.

Reaction Times

The system reaction time is the amount of time from a safety-related event as input to the system until the system is in the Safety state.

Refer to page 103 for reaction time information.

Connection Status

Your application should monitor the HSP and DeviceNet connection status bits. Since connections often recover automatically, make sure this occurrence does not result in an unsafe machine state. Your application should drive safety outputs to their safe state when the connection faults or goes idle, and remains in the safe state until a manual reset occurs. This prevents unexpected output transitions from low to high when a connection recovers from a faulted or idle state.

IMPORTANT	The DeviceNet connection status bits are accurate only if the HSP connection is in the established state.

DeviceNet Scanner Configuration Checklist

Use the checklist on the following page for configuration, programming and startup of the DeviceNet safety scanner.

It may be used as a planning draft as well as a proof. If used as a planning draft, the checklist can be saved as a record of the plan.

To ensure that the requirements are fully and clearly satisfied during system configuration or start-up, an individual checklist for controlling the requirements can be filled in for every single safety output channel in a system.

Checklist for Configuration, Programming, and Startup of DeviceNet Safety Scanner	
Company:	
Site:	
Loop definition:	

No.	Requirements	Fulfilled		Comment
		Yes	No	
After adding one or more nodes to the network				
1	Is each DeviceNet safety node commissioned with a unique node reference (combination of SNN and MAC ID) that is unique within your entire network? See page 58 for more information.	☐	☐	
2	Is each DeviceNet safety target correctly configured?	☐	☐	
3	Are the reaction times of each target known and suitable for the application?	☐	☐	
After adding one or more connections				
4	Are the safety connection timing parameters suitable for the capacity of all CIP safety links traversed?	☐	☐	
5	Is the reaction time of each DeviceNet safety connection suitable for the application?	☐	☐	
6	Are application signals correctly applied to device signals within RSLogix Guard PLUS! Hardware Management software?	☐	☐	
7	Is your site-selected naming convention applied to application signals mapped to standard device signals correctly and consistently? Refer to page 55 for more information.	☐	☐	
8	Did the scanner accept the configuration signature download by RSNetWorx for DeviceNet software?	☐	☐	
9	Did the GuardPLC controller accept the compiled application with matching HSP signature?	☐	☐	
10	Does your application logic monitor the HSP and DeviceNet connection status bits?	☐	☐	

Checklist for Configuration, Programming, and Startup of DeviceNet Safety Scanner				
After compiling and downloading the configuration into the GuardPLC controller and scanner				
11	Have all of the application-to-device signal mappings been verified functionally?	☐	☐	
12	Did the RSLogix Guard PLUS! software compilation process' calculation of the HSP signature match the value provided by RSNetWorx for DeviceNet software in the .ssf file?	☐	☐	
13	Has the system been run long enough under typical use for the statistics reported in RSLogix Guard PLUS! and RSNetWorx for DeviceNet software to be meaningful?	☐	☐	
14	Is the Max Scanner Response Time setting on the GuardPLC controller tab in RSNetWorx for DeviceNet software greater than the maximum value reported by the statistics feature?	☐	☐	
15	Have you set the Controller Receive Timeout as indicated in either 15a or 15b?	☐	☐	
15a	For environments with electrical noise characteristics that do not require HSP retires, for example, default Controller Resend Timeout of 0 is acceptable.	☐	☐	
	Is the Controller Receive Timeout setting on the HSP Properties dialog in RSLogix Guard PLUS! software greater than or equal to the maximum response time reported on the HSP Protocol tab of the control panel?	☐	☐	
15b	Controller Resend Timeout must be set greater than zero (HSP retries are necessary due to an electrically noisy environment):	☐	☐	
	Is the Controller Resend Timeout setting on the HSP Properties dialog in RSLogix Guard PLUS! software greater than or equal to the maximum response time reported on the HSP Protocol tab of the control panel?	☐	☐	
	Is the Controller Receive Timeout setting on the HSP Properties dialog in RSLogix Guard PLUS! software greater than or equal to N +1 times the Controller Resend Timeout, where N retries are desired?	☐	☐	
16	Is the number of communication time slices reported on the Statistics tab of the RSLogix Guard PLUS! software Control Panel equal to 1?	☐	☐	
17	Is the maximum Communication Time Slice value on the Resource Configuration dialog in RSLogix Guard PLUS! Hardware Management greater than or equal to the maximum Communication Time Slice value reported on the Statistics tab of the RSLogix Guard PLUS! Control Panel?	☐	☐	
18	Is the Watchdog Time (WDZ) value on the Resource Configuration dialog greater than or equal to the maximum Cycle Time value reported on the Statistics tab of the RSLogix Guard PLUS! control panel?	☐	☐	
19	Is the Safety Time value on the Resource Configuration dialog greater than twice the Watchdog Time Value?	☐	☐	

Checklist for Configuration, Programming, and Startup of DeviceNet Safety Scanner				
20	Is the Scanner Receive Timeout setting on the GuardPLC tab in RSNetWorx for DeviceNet equal to the WDZ time of the controller?	☐	☐	
21	Is the HSP connection establishment setting (auto/manual) properly configured and managed (if applicable) for the application?	☐	☐	
After adjusting all reaction time parameters based on statistics gathered during verification				
22	For each input-output chain, does the sum of the reaction times of all network links and modules traversed yield an acceptable input-output single-fault reaction time for the associated safety function of the application?	☐	☐	
23	Have you executed the Safety Device Verification Wizard?	☐	☐	
24	Did you review and print the verification report for your records?	☐	☐	

Chapter 6

DeviceNet Safety I/O for the GuardPLC Control System

Chapter Introduction

This chapter gives information about the DeviceNet Safety I/O.

Overview

Before operating a GuardPLC safety system containing DeviceNet safety I/O modules, you must read, understand, and follow the installation, operation, and safety information provided in the documentation for these products.

Refer to Additional Resources on page 11.

Field safety I/O modules can be connected to safety input and output devices, allowing these devices to be controlled by a GuardPLC and DeviceNet safety scanner control system. For safety data, I/O communication is performed through safety connections using the DeviceNet Safety Protocol; logic is processed in the GuardPLC controller.

Typical Safety Functions of DeviceNet Safety I/O Modules

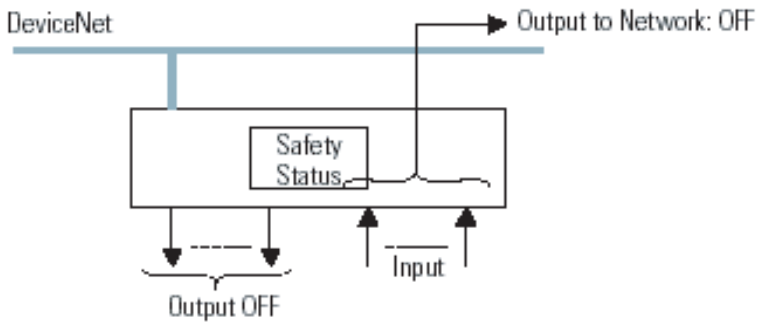
This section describes the module's safety functions.

Safe State

The following is treated as the safety state by safety I/O modules.

- Safety outputs: OFF
- Output data to network: OFF

Figure 14 - Safety State Representation



The DeviceNet safety I/O modules should be used for applications that are in the safety state when the safety output turns OFF and the output data to the network turns OFF.

Diagnostics

DeviceNet safety I/O modules perform self-diagnostics when the power is turned ON and periodically during operation. If a diagnostic failure is detected, the safety outputs and output data to the network are turned OFF.

Commission Safety Devices

You must commission all safety devices with the MAC ID, SNN, and communication rate, if necessary, before their installation on the safety network.

Ownership

A module can only be configured by one originator or by a tool, which automatically becomes the configuration owner for that module. No other device can send configuration data to the module, unless the module is first returned to the out-of-box condition.

TIP Ownership also applies to outputs. An output or output assembly can only have one owner, which is the first originator to establish a valid connection to the output or output assembly.

You can return the module to the out-of-box condition by selecting the Reset Safety Device from the Device menu in RSNetWorx for DeviceNet software.

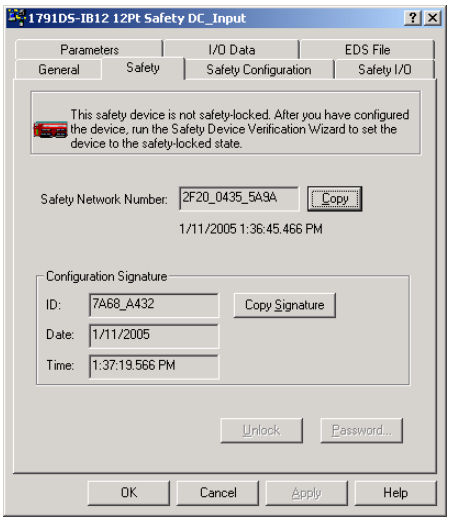
If there are multiple tools being used within the facility or on the network, you must use passwords to prevent unintended configuration changes.

Configuration Signature

The Configuration Signature uniquely identifies a particular module configuration. It is comprised of a checksum (ID) and the date and time that the configuration was created. The Configuration Signature is used in several operations.

- During download from a configuration tool, the Configuration Signature provides you with a means to check that the device and the configuration tool agree on the information downloaded.
- During connection establishment, the originator and the target devices use the Configuration Signature to ensure that both devices are using the expected configuration.

The Configuration signature is made up of ID number, Date, and Time.



Safety Network Number (SNN) Assignment

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.

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

Refer to the DeviceNet Safety Scanner for GuardPLC User Manual, publication number 1753-UM002, for information on managing the SNN.

Input and Output Line Conditioning

DeviceNet safety I/O modules provide pulse test and monitoring capabilities. If the module detects a failure, it sets the offending input or output to its Safety state and reports the failure to the controller.

The failure indication is made via the input or output point status, and is maintained for a configurable amount of time, or until the failure is repaired, whichever comes first.

IMPORTANT	Logic must be included in the application program to latch these I/O point failures and ensure proper restart behavior.

DeviceNet Connection Loss

This section describes input and output connection losses.

Input Connection

If an input connection loss is detected, the safety data is set to the defined safety state (0). The corresponding connection fault bits are set to one. The application logic must react appropriately to all safety data from a DeviceNet safety connection being set to the safety state fault. The scanner continuously attempts to reestablish the input connection.

Output Connection

If an output connection is lost, the connection is reported as faulted by the safety Scanner to the controller via the connection status bits. The application logic must react appropriately to the connection fault, and the output device must react appropriately to the loss of the connection and must perform its safety action. The scanner continuously attempts to reestablish the output connection.

Your application should monitor the HSP and DeviceNet connection status bits. Since connections often recover automatically, make sure this occurrence does not result in an unsafe machine state. Your application should drive safety outputs to their safe state when the connection faults or goes idle, and remains in the safe state until a manual reset occurs. This prevents unexpected output transitions from low/off to high/on when a connection recovers from a faulted or idle state.

Safety Considerations for I/O Module Replacement

The replacement of safety devices requires that the replacement device be configured properly and that the operation of the replacement device be user-verified.

ATTENTION: No safety function that includes any portion of the replaced module may be relied upon during the replacement and functional testing of the module.

When replacing a module, you cannot automatically recover the configuration signature. You need to set the Safety Network Number via RSNetWorx for DeviceNet software and re-load the configuration. Then drop and re-establish the I/O connection with the DeviceNet Safety Scanner module.

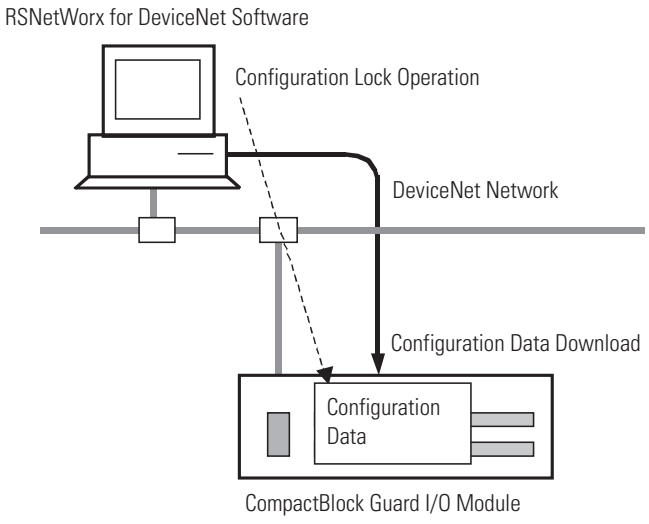
Safety-lock with Password Protection

When applying functional safety, restrict access to qualified, authorized personnel who are trained and experienced. The safety-lock function, with passwords, is provided by the Safety Device Verification Wizard in RSNetWorx for DeviceNet software. You are responsible for controlling access to the safety system, including password handling.

For information on the safety-lock feature or on setting a password using RSNetWorx for DeviceNet software, refer to the DeviceNet Safety Scanner for GuardPLC User Manual, publication 1753-UM002.

After configuration data has been downloaded and verified, the configuration data within the module can be protected, using RSNetWorx for DeviceNet software. Run the Safety Device Verification Wizard to lock the module.

Figure 15 - Safety-lock Application Process



Status Indicators

The DeviceNet safety I/O modules include status indicators.

Status Indicators

For details on status indicator operation, refer to the product documentation for your specific module.

IMPORTANT	Status indicators are not reliable indicators for safety functions. They should be used only for general diagnostics during commissioning or troubleshooting. Do not attempt to use status indicators as operational indicators.

Status Data

In addition to input and output data, some DeviceNet safety I/O modules support status data to monitor the I/O circuits. You can create an application program to monitor these variables and take appropriate action. Refer to your module's product documentation.

Reaction Time

The input reaction time is the time from when an input signal is changed to when network data is sent.

The output reaction time is the time from when a network signal is received to when the state of output terminal is changed.

Some DeviceNet safety I/O modules may support ON-delay and OFF-delay functions for input signals. You must include OFF-delay times when calculating system reaction time.

See page 103 for information on calculating reaction times.

For information on determining the input and output reaction times, refer to the product documentation for your specific DeviceNet safety I/O module.

Checklist for DeviceNet Safety I/O Modules

For programming or startup, an individual checklist can be filled in for every single safety input and output channel in a system. This is the only way to make sure that the requirements are fully and clearly implemented. This checklist can also be used as documentation on the connection of external wiring to the application program.

Checklist for DeviceNet Safety I/O Modules used in GuardPLC Systems			
Company:			
Site:			
Safety Function definition:			
SIL input channels in the:			
Notes / Checks	**Yes**	**No**	**Comment**
Have you followed installation instructions and precautions to conform to applicable safety standards?	☐	☐	
Have you verified that the electrical specifications of the sensor and input are compatible?	☐	☐	
Have you verified that the electrical specifications of the output and the actuator are compatible?	☐	☐	
Are modules wired in compliance with PLe/Cat. 4 according to ISO 13849-1(1) if required?	☐	☐	
Have you verified that test outputs are not used as safety outputs?	☐	☐	
Are control, diagnostics, and alarming functions performed in sequence in application logic?	☐	☐	
Are HSP and DeviceNet Connection Status Bits monitored in application logic?	☐	☐	
Have you uploaded and compared the configuration of each module to the configuration sent by configuration tool?	☐	☐	
Have you performed proof tests on the system and modules?	☐	☐	

(1) For information on wiring your DeviceNet Safety I/O module, refer to the product documentation for your specific module.

GuardPLC Controller Operating System

Chapter Introduction

This chapter gives information about the details of the GuardPLC controllers, their operating system, and RSLogix Guard PLUS! software.

Software for GuardPLC Controllers and I/O Modules

The software for the GuardPLC safety automation systems is arranged in these three blocks.

- Operating system
- Application program
- Programming tool (RSLogix Guard PLUS! software) according to IEC 61131-3

The operating system is loaded in the central unit of the GuardPLC controller and should be used in the valid, TUV-certified form required for safety-related applications.

The application program must be created by using the RSLogix Guard PLUS! programming tool and must contain the specific equipment functions to be performed by the automation module. Parameters for the operating function are also entered into the system using RSLogix Guard PLUS! software. The application program is translated into machine code with the code generator. This machine code is transferred via an Ethernet network interface into the Flash EPROMs of the GuardPLC 1200, 1600, 1800 controllers and the CPU module of the GuardPLC 2000 controller, respectively.

The essential functions of the operating system and their correlation to the application program are shown in the following table.

Functions of the Operating System	Connections to the Application Program
Cyclical processing of the application program	Acts on variables, function blocks
Configuration of the automation module	Fixed by the selection of the GuardPLC controller
CPU test	None
I/O module tests (depending on type)	Depends on the I/O modules used
Reaction in error case	Default setting
	Application program is responsible for process reaction
Diagnostic status indicators	None
Diagnostic possibilities of I/O and of the CPU	Use of the system variables for error messages of the I/O and CPU
Communication via Ethernet network interface or serial line	Data exchange via COM (serial) is effected via a standard protocol: no writing of relevant safety signal
Programming software interface: permissible actions	Fixed in RSLogix Guard PLUS! software: Configuration of protection functions, User login

Technical Safety for the Operating System

Every licensed operating system is identified by its name. To aid in identification, the revision, and CRC signature are provided. The applicable versions of the operating system and the related signatures (CRCs), approved by TÜV for safety automation systems, are subject to revision controls and are documented on a list compiled in conjunction with TÜV.

Use RSLogix Guard PLUS! software to read the current operating system version. Verification is required.

See the checklist on page 83.

Operating Mode and Functions of the Operating System

The operating systems process the application program in cycles. The following functions, described in simplified form, are executed.

- Read input data
- Process logic functions programmed according to IEC 61131-3
- Write output data

In addition, there are the following essential functions.

- Comprehensive self-tests
- Tests of the I/O modules while in operation
- Data transfer
- Diagnostics

Technical Safety for Programming

This section details what you need to do when programming using the software.

Safety Concept of RSLogix Guard PLUS! Software

The safety concept of RSLogix Guard PLUS! software warranties that:

- the programming system works correctly, meaning that programming system errors can be detected.
- the user applies the programming system correctly, and therefore, user operating errors can be detected.

For the initial start-up of a safety PES or after a modification of the application program, the safety of the entire system must be checked by a complete functional test. These three steps must be carried out.

1. Double compilation of the application program followed by comparison of the code versions (Configuration CRC of the CPU).
2. Check the correct encoding of the application based on the data and control flows.
3. Complete functional test of the logic.

   See the next section, Check the Created Application Program.

Check the Application Program

To check your application program for adherence to the specific safety function, you must generate a suitable set of test cases covering the specification.

As a rule, the independent test of each input and the important links from the application side should suffice. RSLogix Guard PLUS! software and the measures defined in this safety manual are designed to prevent the generation of a semantic and syntactically correct code that contains undetected systematic errors.

You must also generate a suitable test set for the numeric evaluation of formulas. Equivalent range tests are acceptable. These are tests within the defined value ranges, at the range limits, or using invalid value ranges. Select the test cases to prove the validity of the calculation. The necessary number of test cases depends on the formula used and must comprise critical value pairs.

However, active simulation with sources cannot be omitted as it is the only means of detecting correct wiring of the sensors and actuators and of testing the system configuration.

Create a Back-up Program

Follow these steps when creating a back-up program.

1. Print out the application program to compare the logic to the specifications.
2. Compile the application program to generate the Configuration CRC of the CPU.
3. Note the version of the Configuration CRC of the CPU by verifying the set of CRCs.
   a. Select a controller in the RSLogix Guard PLUS! software Hardware Management Window.
   b. Use the About Configuration context menu to display versions.

   The important versions to verify include:
   - rootcpu.config (Configuration CRC of the CPU). This indicates the overall configuration portion of the CPU that is safety-related.
   - rootcom.config, that indicates the overall configuration portion of the COM that is not safety-related.
   - root.config indicates the entire configuration including the remote I/O modules (CPU and COM).
4. Back up the project and make note of the user program name, Configuration CRC of the CPU and date it.

   This does not replace the user's documentation requirements.
5. Create a backup of every controller.

Program Identification

The application program is clearly identified by the top level root.config Controller Overview. The related backup can thus be clearly determined. The identification of a backup should contain the configuration CRC of the controller.

To make sure that the backup is unmodified, first compile the backup, and then compare this newly generated code version with the code version of the program loaded in the controller. The comparison can be displayed by using RSLogix Guard PLUS! software.

Parameters of the Automation System

The following parameters determine the operating behavior of the automation system and are set in RSLogix Guard PLUS! software.

The settings possible for safety operation are not inflexibly bound to a certain requirement class. However, they must be available to the applicable approving board for every implementation of the automation system.

Safety Parameter CPU	Setting for Safety Operation
Safety time in ms	Depends on process
Watchdog time in ms	Max. 50% of the safety time
Start/Restart	Reset/Off (can only be set to OFF in RUN mode of the CPU)
Force Enable (forcing)	Reset/off
Activate/Deactivate forcing in Force-Editor Window(1)	Reset/off
Main Enable (modification of the safety parameters)(1)	Reset/Off (can only be set to OFF in RUN mode of the CPU)
Test Mode(1)	Reset/off

(1) You cannot set this on distributed I/O modules, except for 1753-IB20XOB8.

Forcing

Forcing is only permissible after consulting the approving board responsible for site approval. During forcing, the person in charge must make sure sufficient safety technical monitoring of the process by other technical and structural measures.

The following forcing options are possible.

- Forcing can be prohibited by configuration. If it is prohibited, the PES no longer accepts force values defined specifically by the application. In this case, new force values can be set only after re-enabling the force system.
- A Select All can be effected via the Force Editor in RSLogix Guard PLUS! software. All displayed signals should be verified in the controller.
- All forced inputs or outputs can be reset by a STOP force command in the Force Editor in RSLogix Guard PLUS! software. All individual force values and switches are held in their current state. Once you restart forcing, they become active again.

More information about forcing can be found in the Using RSLogix Guard Plus! Software with GuardPLC Controllers Programming Manual, publication 1753-PM001.

General information about forcing can be found in the TÜV document Maintenance Override. To access the document on the Internet, see these websites.

- TÜV-Product-Service, http://www.tuvasi.com
- TÜV-Rheinland, http://www.tuv-fs.com

Protection Against Manipulation

You, in conjunction with the approving board, must define what measures are applied to protect against manipulation.

Guard PLC Controllers and GuardPLC I/O Modules

Protection mechanisms are integrated in the PES and in RSLogix Guard PLUS! software to prevent unintentional or unauthorized modifications to the safety system.

- A modification to the application program generates a new (CRC) version number. These modifications can only be transferred to the PES via download (PES must be in STOP).
- You must be logged in to the PES to access operating options.
- RSLogix Guard PLUS! software features a password link to the PES upon user login.
- The link between programming software and PES is not necessary during RUN operation.

The requirements of the safety and application standards regarding the protection against manipulations must be observed. The authorization of employees and the necessary protection measures are the responsibility of the operator.

ATTENTION: To protect the password against unauthorized access, modify the default settings for both the login and password.

PES data is accessible only if the computer uses RSLogix Guard PLUS! software, and the application project is the currently running version (back-up maintenance). The link between programming software and PES is necessary only for the download of the application program or for reading out variable status and performing a reboot of the controller to recover from a failure stop condition. The programming software is not required for normal operation. Disconnecting the programming software from the PES during standard operation protects against unauthorized access.

Checklist for the Creation of an Application Program

Use the following checklist to maintain safety technical aspects when programming, and before and after loading the new or modified program.

Checklist for Creation of an Application Program Safety Manual GuardPLC Systems			
Company:			
Site:			
Project definition:			
File definition / Archive number:			
Notes / Checks	**Yes**	**No**	**Comment**
Creation/Before a Modification			
Are the configuration of the PES and the application program created with safety in mind?	☐	☐	
Are programming guidelines used for the creation of the application program?	☐	☐	
Are functionally independent sections of the program encapsulated in functions and function modules?	☐	☐	
Were only safety signals used for all safety functions?	☐	☐	
Are HSP and DeviceNet Connection Status Bits monitored?	☐	☐	
Does each safety signal source correction (also via communication) reach the user program?	☐	☐	
Is each safety output signal correctly configured and is the output signal connected to a physical output channel?	☐	☐	
After a Modification - Before Loading			
Has a review of the application program with regard to the binding system specification been carried out by a person not involved in the program creation?	☐	☐	
Has the result of the review been documented and released (date/signature)?	☐	☐	
Have all force markers been removed before safety mode?	☐	☐	
Was a backup of the complete program created before loading a program in the PES?	☐	☐	
Has the user program been compiled twice with a subsequent comparison of both CPU configuration CRCs?	☐	☐	
After a Modification - After Loading			
Were a sufficient number of tests carried out for the safety relevant logical linking (including I/O) and for all mathematical calculations?	☐	☐	
Was all force information reset before safety operation?	☐	☐	
Do the settings of enable switches correspond to the settings for maximum/ specified protection?	☐	☐	
Verify that the CPU and scanner operating systems and the CRC are official licensed versions approved by TÜV.	☐	☐	

Notes:

Chapter 8

Technical Safety for the Application Program

Introduction

This chapter gives information about technical safety for the application program.

The following sections contain defaults, rules, and requirements developed from sample construction surveys.

You must create the application program by using the RSLogix Guard PLUS! programming tool for personal computers using the Windows XP, Windows NT, or Windows 2000 operating system.

RSLogix Guard PLUS! software contains these features.

- Input (function block editor) monitoring and documentation
- Variables with symbolic names and variable types (BOOL and UINT)
- Assignment of the controllers (GuardPLC 1200, 1600, 1800, or 2000 controllers)
- Code generator (translation of the application program into machine code)
- Hardware configuration
- Communication configuration

General Procedure

The general procedure for programming the GuardPLC control systems for technical safety applications is listed below.

- Specify the control function.
- Write the application program.
- Compile the application program with the C-code generator.
- Translate the C-code twice and compare the results.
- Generate an error-free, executable program.
- Verify and validate.

The program can then be tested by the user and the PES can initiate safety operation.

Basis of Programming

The application program should be:

- easy to understand.
- easy to trace.
- easy to change.
- easy to test.

The control task should be available as a specification or a performance specification. This documentation forms the basis for the check of correct transformation into the program. The presentation of the specification depends on the application task to be carried out. This can be:

- combinatory logic.
- sequential controls (step controls).
- digital or analog sensors.
- actuators.

Combinatory Logic

- Cause/effect diagram
- Logic of the link with functions and function modules
- Function blocks with specified characteristics

Sequential Controls (Step Controls)

- Verbal descriptions of the steps with step conditions and actuators to be controlled
- Flow charts
- Matrix or table form of stepped conditions and the actuators to be controlled
- Definition of marginal conditions, for example, operating modes, and EMERGENCY STOP

The I/O concept of the system must contain the analysis of field circuits, that is, the type of sensors and actuators.

Sensors (Digital or Analog)

- Signal in normal operation (closed-circuit principle for digital sensors, life-zero for analog sensors)
- Signals for error
- Determination of redundancies required for technical safety reasons (1oo2, 2oo3)

  See the Safety of Sensors, Encoders, and Transmitters section, page 29.
- Discrepancy monitoring and reaction

Actuators

- Position and activation in normal operation
- Safety reaction/positioning when switching OFF or power failure.

Variable Declaration and I/O Naming

The variable names and their data types are defined with the help of the variable declaration editors. Symbolic names, consisting of a maximum of 256 characters, are assigned to all variables of the application program.

Symbolic I/O names, consisting of a maximum of 256 characters, are also used for physical inputs and outputs.

The use of symbolic names instead of physical addresses has two essential advantages.

- The equipment definitions of inputs and outputs can be used in the application program.
- Modifications of the signal assignment in the input and output channels have no effect on the application program.

Assignment of I/O Names to Variable Names

A list of the sensors and actuators in the system should serve as basis for the assignment of I/O names (names used for hardware assignment).

For practical reasons, variable name and I/O name should be the same. The number of channels (names) per module depends on the type of module or system used.

The necessary diagnostic routines for safety I/O modules or channels are automatically executed by the operating system.

Types of Variables

Depending on the program organization unit (POU), either program, function block, or function module, different types of variables can be defined as described below.

	Program	Function Module	Application
Signals(1)	X (CONSTANT)(2)		Only on program level
VAR		X (CONSTANT)	Only within function module
VAR_INPUT		X	Input variable
VAR_OUTPUT		X	Output variable

(1) Signals are variables that can either be attached to hardware or used as flags on the program level.

(2) Constants cannot be overwritten by the application program (for example, switching point).

The essential characteristic is the encapsulation of the functions into self-created function modules. Thus a program can be clearly structured in modules (function modules). Every module can be seen individually and the final, complex function results from linking these modules into a larger module or ultimately into a program.

Functions of the Application Program

Programming is not subjected to any restrictions imposed by hardware. The functions of the application program are freely programmable.

When programming, follow the closed-circuit current principle for the physical inputs and outputs.

Only components that comply with IEC 61131-3, and their corresponding functional requirements, may be used with the logic.

- Appropriate logical and/or arithmetic functions are used by the application program, regardless of the closed-circuit principle of the physical inputs and outputs.
- The I/O module uses the closed-circuit principle that requires the safety state of the inputs and outputs to be 0. The logic in the controller does not rely on the closed-circuit principle, so you can determine the safety state for connections between function blocks to be 0 or 1. However, we recommend that you use a safety state of 0 between function blocks.
- Design and document the logic to simplify troubleshooting. Use flow charts and write good documentation of the program logic. This does not replace any of the documentation requirements for your applications. Flow charts and logic documentation should be included if they are not already required by your documentation procedures.
- Any number of negations are permissible.
- The programmer must evaluate input, output, and logic module error signals.

Safety Inputs and Outputs

In an analog GuardPLC safety input module, defined values can be further processed in the event of an error.

In a digital GuardPLC safety I/O module, the input is set to a 0 and the digital output module is switched off via the integrated safety switch-off.

Parameters of the Application Program

The parameters listed in the following table determine the behavior of the automation module while in operation and are set in the menu attributes of the controller.

Here the permissible actions are determined with the programming software in the safety operation of the automation module and the safety parameters are preset.

Switch	Function	Default Value	Setting for Safety Operation(1)
Main Enable	The following switches/parameters can be modified during operation of the programming software.	ON	OFF(1)
Autostart	Automatic start after initializing the CPU.	OFF	ON/OFF(2)
Restart/Start	Coldstart, warmstart, or hotstart using programming software in the RUN or STOP condition.	ON	OFF
Load Enable	Load release for an application program.	ON	ON
Test Mode allowed	Test Mode allowed or forbidden. At Test Mode the program execution will be frozen or stopped. The outputs remain actuated and the program execution can be done in single cycle steps.	OFF	OFF
Force Enable	Activation of values for the PES inputs or outputs, independent of the actual value of a signal from the linked process or the result of the logic link.	OFF	Determined by the approving board
Stop on Force Timeout	Stop during operation of forcing time	ON	Determined by the approving board
Additional switches and parameters can be preset for forcing (See the Loading and Starting the Application Program section, page 92).			

(1) The setting of the values only applies when you are online.

(2) Setting to ON or OFF is application-dependent.

Procedure for Locking the PES

Locking the PES means locking functions and access from the user during operation to prevent manipulation of the application program. The extent of disabling actions depends on the safety requirements for the particular application of the PES. Consult the approving board in charge of site acceptance for help in determining the safety requirements.

The only distributed I/O module that can be locked is the 1753-IB20XOB8.

Follow these procedure to lock the PES.

1. The following attribute values must be set in the controller before compilation.

Attribute	Value
Main Enable	True
Autostart	True/False
Start/Restart allowed	True
Forcing allowed	False (application-dependent)
Loading allowed	True
Test Mode allowed	False
Stop on Force Timeout	True (application-dependent)

2. After loading and starting, you can modify the following switches in the controller in the following sequence.
   a. Start / Restart allowed to FALSE, and Loading allowed to FALSE.
   b. Main Enable to FALSE.

ATTENTION: The following switches can be set at other values only upon consultation with the approving board:

Force Enable	to	TRUE
Stop on Force Timeout	to	TRUE/FALSE
Start / Restart allowed	to	TRUE
Autostart	to	TRUE

ATTENTION: The Test Mode switch must never be set to TRUE for safety operation.

Procedure for Unlocking the PES

Unlocking the PES means enabling functions and access to allow you to make changes to the safety system.

The controller must be in STOP mode in order to set the Main Enable switch to ON. Activating Main Enable is not possible when the PES is running (in RUN condition). Deactivating Main Enable is possible while in RUN.

To restart following initialization of the CPU (after power failure), follow these steps to Unlock the PES.

1. Set Main Enable switch to TRUE.
2. Set Start/Restart switch to TRUE.
3. Start the application program.
4. Then Lock the PES again.

See the Procedure for Locking the PES on page 91.

Code Generation

After input of the application program and completion of the I/O assignments, the code is generated, forming the Configuration CRC of the Controller.

The Configuration CRC of the Controller is a signature of the entire configuration of the controller. The output is a Hex-code in 32-bit format. All configurable or modifiable elements such as logic, variables, and switch settings are included.

Load and Start the Application Program

The application program can only be downloaded to the controller if the controller is in STOP mode. Downloading during RUN mode is not possible. The configuration CRC of the root.config is also created at this time. It must be compiled twice and the configuration CRC must be identical in both compile cycles.

Only one application program can be loaded into the respective CPU. Downloading of an application program is monitored. Once download is complete, the application program starts, and the cyclical process of the routine begins executing.

Force Inputs and Outputs

Forcing means activation of values for the hardware inputs or outputs, independent of the actual value of a signal from the linked process or the result of the program logic.

The only distributed I/O module that can be configured for forcing is 1753-IB20XOB8.

ATTENTION: Forcing is permissible only upon consultation with the approving board in charge of site acceptance. The person in charge must make sure that sufficient technical safety process monitoring is carried out by other technical and structural measures during forcing.

Switches or Parameters	Function	Default Value	Setting for Safety Operation
Forcing allowed (1)	Enables the Force function	OFF	ON
Stop on Force Timeout(1)	Stops the CPU after exceeding the Force time	ON	ON
Forcing activated	Forcing active	OFF	ON
Remaining Force Time	Time limit, in seconds, that Forces may be active	0	Time in sec

(1) This setting cannot be changed during operation with a locked PES.

Forcing can be limited by time. The maximum force time is given in seconds. For forcing without a time limit, set the Remaining Force Time to -1.

ATTENTION: Forcing without a time limit is only permissible after consultation with the approving board in charge of site acceptance.

The Forcing allowed switch enables forcing to be permitted or forbidden within the CPU. When Forcing allowed is set, forcing is allowed. The entered force values only become active if the relevant force switch is set for the data source. When Forcing allowed is not set, forcing is not possible. Any force values entered remain in the system but have no effect. After the force time has elapsed, or if forcing is stopped, the signals being forced revert to control by the user program.

If	Then
The Stop on Force Timeout switch is set in the controller properties	The controller transitions to the STOP mode when the force time expires. The signals being forced revert to control by the user program.
The Stop on Force Timeout switch is not set in the controller properties	The controller does not stop when the force time expires. The signals being forced revert to control by the user program.

If the force time is exceeded, the logic can determine whether the CPU goes to STOP or the force value is no longer valid, allowing standard operation to proceed. Exceeding the force time always has effects on the application program.

Pressing the Stop button in the Force Editor (found in RSLogix Guard PLUS! Hardware Management software) manually stops forcing. The controller remains in the RUN state, because the timeout was not reached and the Stop on Force Timeout switch was not set.

The force value is saved in the CPU. If the CPU moves from RUN to STOP, the Forcing activated switch is deactivated to prevent the controller from being started with active forcing.

Online Test

The Online Test function allows the online test (OLT) fields to be used within the application logic for displaying and for forcing signals and variables during operation of the controller.

If	Then
The Online Test allowed switch is set in the controller properties	The values of signals or variables can be displayed and forces in the OLT fields. The forced value is only valid until a function in the logic overwrites the value.
The Online Test allowed switch is not set in the controller properties	The values of signals or variables may be displayed in the OLT fields, but they cannot be changed.

The default for Online Test allowed switch is set.

Consult the online help for RSLogix Guard PLUS! software for more information about the OLT fields.

Program Documentation for Safety Applications

You can print out the documentation of a project using RSLogix Guard PLUS! software. The most important types of documentation are:

- Interface declaration.
- Variable list.
- Logic.
- Definition of data types.
- Configurations for system, modules and system parameters.
- I/O variable cross-reference.
- Code generator information.
- Network configuration.

Documentation is a component of a functional acceptance of a site subject to approval by an approving board (for example TÜV). The functional acceptance refers only to the application function, not to the safety modules and controllers, that are type tested.

In the case of sites subject to acceptance, you should involve the approval authorities in the project as early as possible.

Considerations for DeviceNet Safety Data

In the HSP Signal Connection dialog boxes (in RSLogix Guard PLUS! software), 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.

The colorization applies only to the Connect Signals dialog boxes available from the HSP protocol context menu. We recommend that you use a naming convention to visually distinguish between standard and safety signals in the 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	Any safety tags that appear in the Standard Connect Signals window must be treated as standard values in your application. Any standard tags that appear in the safety Connect Signals window must be treated as standard. In order for a signal to be regarded as a safety value in your application, the end device configuration must treat the signal as safety and be transferred over a DeviceNet safety connection.

Notes:

Configuring Communication

Introduction

Depending on the controller, the following options are available for safety or standard protocols: Modbus, OPC, Profibus-DP, and ASCII read-only.

Controller	GuardPLC 1200	GuardPLC 1600		GuardPLC 1800		GuardPLC 2000
	1754-L28BBB	1753-L28BBBM	1753-L28BBBP	1753-L32BBBMBA	1753-L32BBBP8A	1755-L1
Communication						
GuardPLC Ethernet	single port	4-port switch	4-port switch	4-port switch	4-port switch	single port
DeviceNet Safety	—	X	X	X	X	—
RS-232 Ports	8-pin mini DIN	—	—	—	—	9-pin mini DIN
RS-485 Ports	—	9-pin DIN	—	9-pin DIN	—	—
Modbus RTU Slave	—	X	—	X	—	—
PROFIBUS DP Slave	—	—	X	—	X	—
ASCII - Read Only	X	X	X	X	X	X
Ethernet IP	—	X	X	X	X	—

Standard Protocols

Apart from the local input/output signals, signal values and statuses can also be exchanged via a data link with another system (for example, Modbus, OPC, and Profibus). To achieve this, the variables are declared in the Protocols area using RSLogix Guard PLUS! software. This data exchange can be read/write.

Signals mapped to data points connected via standard protocols may only be used in standard application functions, not safety functions. They may also used in the application program.

ATTENTION: Any data imported from standard sources may not be used for the safety functions of the application program.

Peer-to-peer Safety Communication via GuardPLC Ethernet

GuardPLC controllers communicate safely with one another and with the programming software via GuardPLC Ethernet network.

ATTENTION: You must make sure that the network utilized for Peer-to-peer communication is sufficiently protected against manipulation (protection against hackers for example). The methods and extent of protective measures must be coordinated with the approving board.

Monitoring of safety communication must be configured in the Peer-to-peer Editor by specifying the Receive Timeout (ReceiveTMO).

If safety signals cannot be imported (received) within the ReceiveTMO, they are reset to their (user-configurable) initial values in the PES.

The value of the input signal must be present longer than the ReceiveTMO or be monitored via loopback, if each value has to be transferred.

ATTENTION: ReceiveTMO is a safety parameter.

Your application should monitor the GuardPLC Ethernet connection status. Since connections often recover automatically, make sure this occurrence does not result in an unsafe machine state. Your application should drive safety outputs to their safe state when the connection faults or goes idle, and remains in the safe state until a manual reset occurs. This prevents unexpected output transitions from low to high when a connection recovers from a faulted or idle state.

ReceiveTMO

ReceiveTMO is the monitoring time on PES_1, during which a correct response must be received from PES_2.

TIP ReceiveTMO also applies in the reverse direction, for example from PES_2 to PES_1

The ReceiveTMO (safety-related) is part of the Worst Case Reaction Time T_R. The ReceiveTMO must be calculated and entered via the peer-to-peer editor.

If the communication partner does not receive a correct answer within the ReceiveTMO, the safety related communication is closed and all signals imported over this communication channel are set to the initial values defined by you.

ReceiveTMO ≥ 2 x response time (minimum)

If the requirement is met, the loss of at least one data packet will not cause the peer-to-peer connection to be lost.

If the requirement is not met, the availability of a peer-to-peer connection is available in a network that is free of collisions and faults. However, the CPU safety is not affected.

TIP The maximum permitted value for Receive TMO depends on the application process and is set in the peer-to-peer editor together with the maximum expected response time and the profile.

Calculating Worst-case Reaction Time

Reaction times are calculated the following ways:

- Between PES and GuardPLC distributed I/O modules
- Between PES1 and PES2

Between PES and GuardPLC Distributed I/O Modules

The worst-case reaction time between changing a transmitter of the first distributed I/O module and the reaction of the outputs of the second distributed I/O module can be calculated as follows.

T_R = input path + output path, where:

T_R = Worst-Case Reaction Time
input path = $t_1 + t_2 + t_3 + t_4$
output path = $t_5 + t_6 + t_7$
WDZ = Watchdog Time
$ReceiveTMO_1$ = ReceiveTMO from I/O-1 to PES
$ReceiveTMO_2$ = ReceiveTMO from PES to I/O-2

$t_1 = 2 \times WDZ_{I/O-1}$
t_2 = 0 ms, if Production Rate = 0, (normal condition)
otherwise = $ReceiveTMO_1 + WDZ_{I/O-1}$
$t_3 = ReceiveTMO_{I/O-1}$
$t_4 = 2 \times WDZ_{PES}$
$t_5 = ReceiveTMO_2$
t_6 = 0 ms, if Production Rate = 0, (normal condition)
otherwise = $ReceiveTMO_2 + WDZ_{PES}$
$t_7 = 2 \times WDZ_{I/O-2}$

Between PES1 and PES2

The Worst-case Reaction Time, T_R, (maximum response time) from the occurrence of an input signal change at PES_1 to the reaction of the output signal at PES_2 can be calculated as follows:

$T_R = t_1 + t_2 + t_3 + t_4$, where:

T_R = Worst-Case Reaction Time
WDZ = Watchdog Time
$t_1 = 2 \times WDZ_{PES1}$
t_2 = 0 ms, if Production Rate = 0, “normal condition”
otherwise = ReceiveTMO + WDZ_{PES1}
t_3 = ReceiveTMO
$t_4 = 2 \times WDZ_{PES2}$

The Worst-Case Reaction Time, T_R, depends on the application and must be coordinated with the approving board.

T_R can be read in the Worst Case column of the Peer-to-Peer Editor.

Terms

Peer-to-peer communication uses the following terms.

ReceiveTMO

The monitoring time, within which a valid response must be received. Safety communication is terminated if the ReceiveTMO expires.

ResendTMO

The monitoring time after which a transmission is repeated, if its receipt has not been acknowledged.

Production Rate

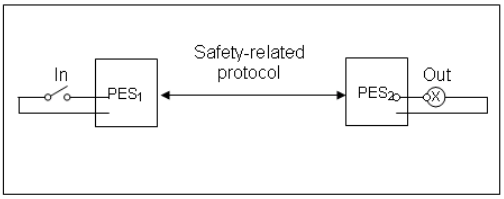
The minimum interval between two data transmissions.

Watchdog

The maximum permissible duration of a run cycle.

Worst-case Reaction Time

The maximum response time from the occurrence of a physical input signal change until the reaction of the physical output signal (see the illustration below). Data transfer is carried out by means of safety protocols.



High-speed Safety Protocol

The following characteristics of High-speed Safety Protocol let it exchange device signal layouts between RSLogix Guard PLUS! and RSNetWorx for DeviceNet software.

HSP Signature

The High-speed Signature is a read-only value that represents the layout of the device signals exchanged between the GuardPLC controller and the DeviceNet safety scanner. The HSP signature is calculated based on the layout of the device signals in RSNetWorx and is passed to RSLogix Guard PLUS! software via the Scanner Signals File. The HSP signature changes only when a modification occurs in the layout of the device signal exchanged between the controller and scanner.

Target Connections File

The Target Connections file is a file used to pass target connection information for application signals you want to make available for read or write access by the GuardPLC controller to another safety originator or standard master on the DeviceNet network.

Scanner Signals File

The Scanner Signals file defines the layout of the safety and standard device signals that the scanner makes available to the controller. This file is generated by RSNetWorx for DeviceNet and sent to RSLogix Guard PLUS! software.

Reaction Times for DeviceNet Safety Communication

The system reaction time is the amount of time from a safety-related event as input to the system until the system is in the Safety state. Each of the times listed is variably dependent on factors such as the type of DeviceNet Safety I/O modules and instructions used in the program. Faults within the system can also have an effect upon the reaction time of the system.

Between PES and DeviceNet Safety I/O Modules

The worst-case reaction time between changing a value on the first DeviceNet Safety I/O module and the reaction of the outputs of the second DeviceNet Safety I/O module can be calculated as follows.

T_R = input path + output path, where:

T_R = Worst-case Reaction Time
input path = $t_A + t_B + t_C$
output path = $t_D + t_E + t_F$
WDZ = Watchdog Time

t_A = Reaction time of DeviceNet Safety input node
t_B = Reaction time of DeviceNet Safety connection to input node
t_C = 2 x WDZ_{PES}
t_D = Max Scanner Response Time
t_E = Reaction time of DeviceNet Safety connection to output node
t_F = Time of DeviceNet Safety output node

An example of using an 1791DS-IB8XOB8:

t_A = 16.2 ms + setting time of 'ON/OFF delay time'
t_A = 16.2 ms + (0, 6, 12,...ms)
t_A = 16.2 ms + 0
t_A = 16.2 ms

t_B = CRTL = 24 ms default (12 ms in normal operation). The CRTL is based on 6 ms RPI, timeout multiplier of 2, network delay multiplier of 200%. You can find these values in RSNetWorx Adv. Safety Connections Property tab.

t_C = 2 x 50
t_C = 100 ms

t_D = 8 ms

t_E = 24 ms fault, 12 ms normal

t_F = 6.2 ms + relay response time
t_F = 6.2 ms + 0
t_F = 6.2 ms

Worst-case Reaction Times

System Reaction Time with no faults:

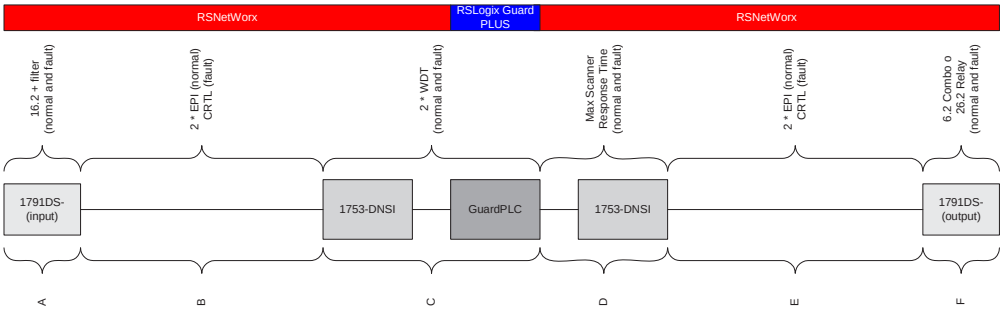
T_R = 16.2 + 12 + 100 + 8 + 12 + 6.2
T_R = 154.4 ms

System Reaction Time with a single fault:

T_R = 16.2 + 24 + 100 + 8 + 12 + 6.2
T_R = 166.4 ms

System Reaction Time with all faults:

T_R = 16.2 + 24 + 100 + 8 + 24 + 6.2
T_R = 178.4 ms



The basic equation is:

A + B + C + D + E + F = System Reaction Time (T_R)

The 2 x WDT term is valid as long as the scanner's Scanner Receive Timeout is set to the same value as the controller's Watchdog Timeout.

System Reaction Time with No Faults

Input + 2 x Expected Packet Interval + 2 x Watchdog Timeout + Max Scanner Reaction Time + 2 x Expected Packet Interval + Output

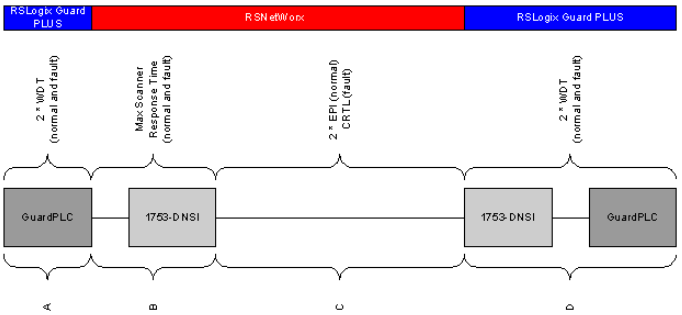
System Reaction Time with a Single Fault

Input + Max (CRTL) + 2 x Watchdog Timeout + Max Scanner Reaction Time + 2 x Expected Packet Interval + Output

System Reaction Time with Multiple Faults

Input + CRTL1 + 2 x Watchdog Timeout + Max Scanner Reaction Time + CRTL2 + Output

Peer-to-peer Reaction Time



The basic equation is:

$$A + B + C + D = \text{System Reaction Time } (T_R)$$

The 2 x WDT term is valid as long as the scanner's Scanner Receive Timeout is set to the same value as the controller's Watchdog Timeout.

System Reaction Time with No Faults

2 x Watchdog Timeout + Max Scanner Reaction Time + 2 x Expected Packet Interval + 2 x Watchdog Timeout

$$T_R = 2 \times 30 + 10 + 20 + 2 \times 30$$
$$T_R = 150 \text{ ms}$$

System Reaction Time with a Single Fault

2 x Watchdog Timeout + Max Scanner Reaction Time + Max (CRTL) + 2 x Watchdog Timeout

$$T_R = 2 \times 30 + 10 + 40 + 2 \times 30$$
$$T_R = 170 \text{ ms}$$

Notes:

Specifications

Chapter Introduction

This chapter gives information about climate, mechanical, and EMC environmental regulations.

The GuardPLC controllers were developed to meet the following standards for the EMC, climate, and environment regulations.

Standard	Description
IEC/EN61131-2	Programmable Controllers Part 2: Equipment requirements and tests
IEC/EN61000-6-2	EMC Part 6-2: Generic Standards - Immunity for Industrial Environments
IEC/EN61000-6-4	EMC Generic Emission Standard - Industrial Environments

When using GuardPLC controllers and I/O modules in safety applications, the following criteria must be met.

- Protection Class II, according to IEC/EN61131-2
- Pollution Degree II
- Altitude < 2000 m
- IP20 Enclosure for Standard Applications
  An alternate enclosure may be required, depending upon the standards relevant to your application.

Climatic Conditions

The most important parameters and tests for climatic conditions are listed in the following table.

IEC/EN 61131-2 Paragraph 6.3.4	Climatic Tests
	Temperature operating 0…60 °C (32…140 °F) (Test limits -10…70 °C (14…158 °F))
	Storage Temperature -40…85 °C (-40…185 °F)) (Battery only -30 °C (-22 °F))
6.3.4.2	Dry heat and cold resistance test (70 °C / -25 °C (158 °F/-13 °F), 96h, EUT Power supply unconnected)
6.3.4.3	Change of temperature, resistance and immunity test (-25 °C / 70 °C (-13 °F/158 °F), EUT Power supply unconnected and 0 °C / 55 °C (32 °F/131 °F), EUT)
6.3.4.4	Cyclic damp heat resistance test (25 °C / 55 °C (77 °F/131 °F), 95% relative humidity, EUT power supply unconnected)

Mechanical Conditions

The most important parameters and tests for mechanical conditions are listed in the following table.

IEC/EN 61131-2 Paragraph 6.3.5	Mechanical Tests
	Vibration test operating 5…9 Hz/3.5 mm 9…150 Hz/1g
6.3.5.1	Immunity vibration test (10…150 Hz, 1g, EUT operating, 10 cycles per axis)
6.3.5.2	Immunity shock test (15g, 11 ms, EUT operating, 2 cycles per axis)

EMC Conditions

The most important parameters and tests for EMC conditions are listed in the following tables.

IEC/EN 61131-2 Chapter 6.3.6.2	Noise Immunity Tests
6.3.6.2.1 IEC/EN61000-4-2	ESD(1) test (4 KV contact / 8 kV air discharge)
6.3.6.2.2 IEC/EN61000-4-3	RFI(2) test (10 V/m) 26MHz to 1GHz, 80%AM
6.3.6.2.3 IEC/EN61000-4-4	Burst tests (2 KV Power supply / 1 KV Signal lines)
6.3.6.2.4 IEC/EN61000-4-12	Damped oscillatory wave immunity test (1 KV)

(1) See List of Abbreviations on page 10.

(2) See List of Abbreviations on page 10.

IEC/EN 61000-6-2	Noise Immunity Tests
IEC/EN61000-4-6	Radio frequency common mode, 10V, 150 KHz…80 MHz, AM
IEC/EN61000-4-3	900 MHz-Pulses
IEC/EN61000-4-5	Surge 1 KV, 0,5 KV

IEC/EN 61000-6-4	Noise Emission Tests
EN50011 Class A	Emission test Radiated, conducted

Power Supply Conditions

The most important parameters and tests for power supply conditions are listed in the following table.

IEC/EN 61131-2 Paragraph 6.3.7	Verification of DC Power Supply Characteristics
6.3.7.1.1	Voltage range test 24V DC, -20%, +25% (19.2…30.0V)
6.3.7.2.1	Momentary interruption immunity test: DC, PS2: 10 ms
6.3.7.4.1	Reversal of DC power supply polarity test
6.3.7.5.1	Back-up duration withstand test (Test B: 1000 h) Lithium battery is used for back-up

The power supply must meet one of the following standards:

- IEC 61131-2
- Safety Extra Low Voltage, EN60950 (SELV)
- Protective Extra Low Voltage, EN60742 (PELV)

Use in Central Fire Alarm Systems

All GuardPLC systems with analog inputs can be used for control and indicating equipment in accordance with DIN EN 54-2 and NFPA 72. The user program must fulfill the functional requirements established for central fire alarm systems by the standards cited above.

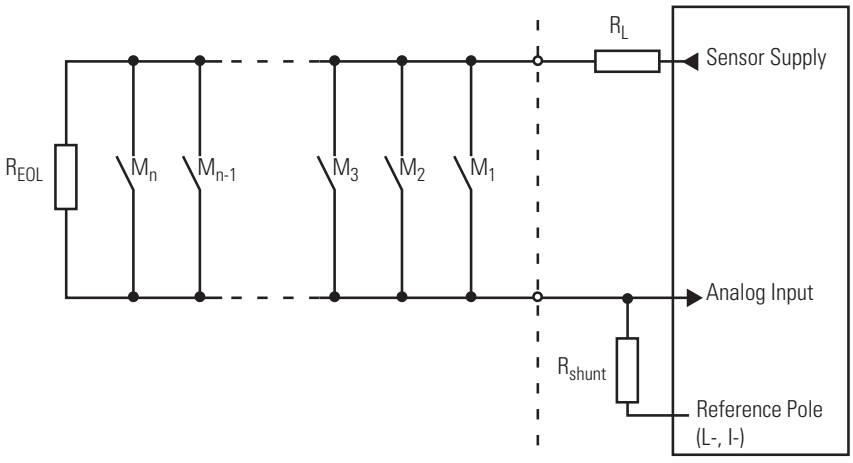
IMPORTANT DeviceNet Safety I/O modules are not appropriate for safety systems.

The required maximum cycle time of 10 seconds (DIN EN 54-2) for central fire alarm systems can be achieved with GuardPLC systems, whose cycle times can be measured in milliseconds. Similarly, the required 1 second safety time (error response time) can also be achieved, if necessary.

According to EN 54-2 the fire alarm system has to be in the fault report state within 100 seconds aftert he HIMatrix system has received the fault report.

The fire alarms are connected using the open-circuit principle with line control for the detection of short-circuits and line breaks. The digital and analog inputs of the GuardPLC 1800 and the analog inputs of the GuardPLC 2000 1755-IF8 module can be used. See the application example below.

Figure 16 - Wiring of Fire Alarms - Example



M = Fire alarm
R_{EOL} = Terminating resistor on the last sensor of the loop
R_L = Limitation of the maximum permitted current in the loop
R_{shunt} = Measuring resistor

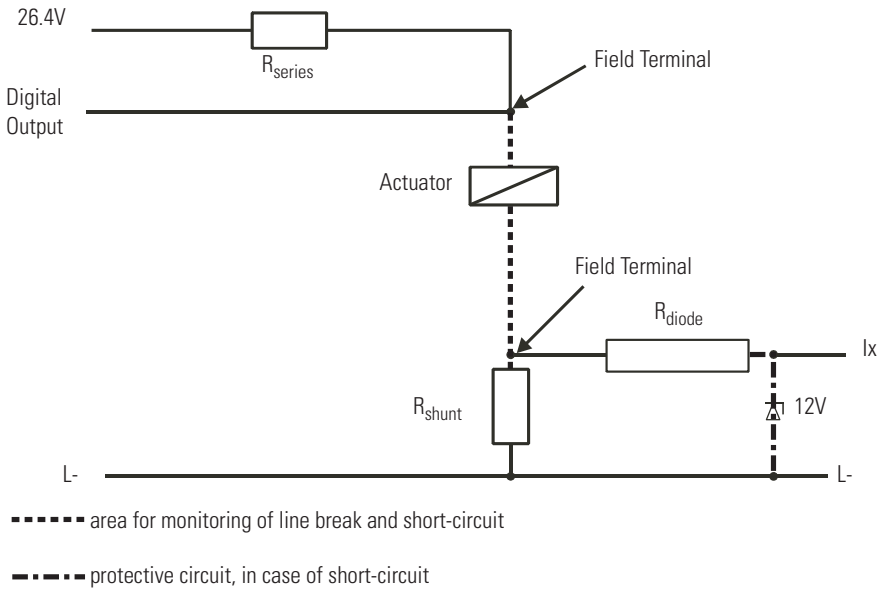
For the application, the resistance of R_{EOL}, R_L and R_{shunt} should be calculated based on the sensors used and the number of sensors per alarm loop. The required data is contained in the relevant specifications from the sensor manufacturer.

The alarm outputs, used for activating lamps, sirens, and horns, are operated using the open-circuit principle. These outputs must be monitored for line breaks and short-circuits. This can be accomplished by feeding back the output signals directly from the actuator to the inputs.

The current in the actuator should be monitored via an analog input with an appropriate shunt. A series connection of a zener diode protects the input over-voltage in case of a short-circuit.

For explicit line break monitoring (at de-energized outputs DO), a transmitter supply to the analog inputs is necessary, as shown below. For more information on line monitoring, refer to the GuardPLC Controller Systems User Manual, publication number 1753-UM001.

Figure 17 - Example for line break and short-circuit monitoring of digital outputs



Visual display systems, indicator light panels, status indicator displays, alphanumeric displays, and audible alarms, can all be controlled by the user program.

The routing of fault signals via input and output modules or to routing equipment must be accomplished by using the closed-circuit current principle.

Fire alarms can be transmitted from one GuardPLC system to another by using the standard Ethernet communication available. Any breakdown in communication must be signalled.

GuardPLC systems that are used as central fire alarm systems must have a redundant power supply. Precautions must also be in place to guard against power supply failure. Transition between the main and backup power supply must be without interruption. Voltage dips of up to 10 ms are permitted.

When there is a fault in the system, the system variables specified in the user program are written by the operating system, enabling error signalling for errors detected by the system. In the event of an error, zero signals are applied to the channels of faulty safety inputs, and all the channels of faulty safety outputs are switched off.

Symbols

Numerics

A

C

D

E

F

G

H

I

L

M

O

P

R

S

T

W

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products.
At http://www.rockwellautomation.com/support/, you can find technical 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://www.rockwellautomation.com/support/.

Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/support/americas/phone_en.html, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation 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, follow these procedures.

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

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation, 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

Publication 1753-RM002D - July 2010
Supersedes Publication 1753-RM002C-EN-P - September 2008