Allen-Bradley

GuardPLC™ Controller Systems

Bulletin 1753, 1754, and 1755

Safety Reference Manual

Rockwell Automation

Important User Information

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

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

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

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

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

WARNING

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

IMPORTANT

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

ATTENTION

Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you:

- identify a hazard
- avoid a hazard
- recognize the consequence

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

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

Information regarding GuardPLC 1600 and GuardPLC 1800 controllers, GuardPLC Distributed I/O, and RSLogix Guard PLUS programming software has been added throughout the manual. The table below summarizes other changes since the last publication.

For information about	See
List of catalog numbers covered by this safety reference manual	page 1-1
Certification	page 1-2
PFD and PFH calculations	page 1-3
Safety requirements	page 1-3
Programming requirements	page 1-4
Communication requirements	page 1-5
Maintenance override	page 1-5
Updated power supply requirements	page 2-1
Updated table of GuardPLC input capabilities	page 3-1
Preventing surge impulses on digital inputs	page 3-4
Configurable digital inputs	page 3-4
Line control for inputs	page 3-4
Analog input values for GuardPLC 1800	page 3-6
Revised checklist for safety-related inputs	page 3-10
Updated table of GuardPLC output capabilities	page 4-1
Line control for outputs	page 4-3
Revised checklist for safety-related outputs	page 4-6
Revised checklist for creation of the application program	page 5-8
Configuring communications	Chapter 7
Use in central fire alarm systems	Appendix B

Chapter 1

Safety Concept

Chapter 2

Central Functions

Chapter 3

Input Channels

Chapter 4

Output Channels

Chapter 5

GuardPLC Controller Operating System

Chapter 6

Technical Safety for the Application Program

Chapter 7

Configuring Communications

Appendix A

Specifications

Appendix B

Use in Central Fire Alarm Systems

Safety Concept

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

Catalog Number	Description
1753-L28BBB-M	GuardPLC 1600 controller with Modbus Communications
1753-L28BBB-P	GuardPLC 1600 controller with Profibus-DP Communications
1753-L32BBBM-8A	GuardPLC 1800 controller with Modbus Communications
1753-L32BBBP-8A	GuardPLC 1800 controller with Profibus-DP Communications
1753-IB16	GuardPLC 16-point Input Module (for GuardPLC 1600 or 1800 controllers)
1753-IB20XOB8	GuardPLC I/O Module (for GuardPLC 1600 or 1800 Controllers)
1753-OB16	GuardPLC 16-point Output Module (for GuardPLC 1600 or 1800 Controllers)
1754-L28BBB	GuardPLC 1200 Controller
1755-L1	GuardPLC 2000 Controller
1755-A6	GuardPLC 2000 I/O Chassis
1755-IB24XOB16	GuardPLC 2000 Digital I/O Module
1755-IF8	GuardPLC 2000 Analog Input Module
1755-HSC	GuardPLC 2000 High Speed Counter Module
1755-OF8	GuardPLC 2000 Analog Output Module
1755-PB720	GuardPLC 2000 Power Supply Module

Certification

Certificate No. 968/EZ164.00/04
TÜV Rheinland/Berlin-Brandenburg
TÜV Anlagentechnik GmbH
Automation, Software, and Informatinstechnologie

Safety restrictions can be found in this manual. See Safety Requirements on page 1-3.

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-related up to safety requirement class 6 according to DIN V 19250, SIL 3 according to IEC 61508 and category 3,4 according to EN 954-1.

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 safe function for existing systems, making the PES suitable for the Safety Machinery Market.

For support in the creation of safety-related programs, use the programming software RSLogix Guard PLUS, according to IEC 61131-3. (Programming software is defined in IEC 61131-1.)

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 system in accordance with IEC 61508. For SIL 3, IEC 61508-1 sets the following PFD and PFH values:

Type	SIL3 value per IEC61508-1:
PFD	10^{-4} to 10^{-3}
PFH	10^{-8} to 10^{-7} per hour

The Proof Test interval is set at 10 years.

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

Safety Requirements

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

Hardware Configuration

Product Independent

- To ensure safety-related operation, use only GuardPLC hardware (see the GuardPLC Version List available at **www.ab.com/certification/safety/**) and RSLogix Guard PLUS software.
- The specified operating conditions listed in Appendix A must be followed.
- Hardware modules and software components which are not fail-safe, but do not cause any adverse reactions, can be used to process non-safety-related signals. However, they cannot be used to carry out safety-related tasks.
- The closed-circuit current principle should be used 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- and SELV-compliant power supplies may be used. See Appendix A or page 2-1 for details on power supply requirements.

Programming Requirements

Product Independent

For safety-relevant applications, ensure that the safety-relevant system variables are correctly configured. Pay particular attention to the maximum cycle time and the safety time.

Product Dependent

- You must use RSLogix Guard PLUS to program the system.
- After creating the application, check that it was compiled correctly by manually compiling and comparing the CRCs.
- The correct conversion of the application specification should be validated using a complete test of the logic for verification.
- Each time a modification is made, the application must be re-checked as described above.
- When a fault occurs in the fail-safe input and output modules, the error response of the system must be determined by the user program according to site-specific safety criteria.

Communication

- When safety-related communication occurs between different devices, the total response time of the system must not exceed the fault tolerance time. See Calculating Worst-Case Reaction Time on page 7-2.
- Safety-related data cannot be transferred over public networks (e.g. the Internet).
- If the data will be transferred across company/factory networks, ensure that sufficient protection is provided against manipulation. For example, use a firewall to separate the safety-relevant portion of the network from standard use portions.
- Serial interfaces should be used only for non-safety-relevant purposes.
- Equipment connected to communication devices should feature safe electrical isolation.

Maintenance Override

When using “Maintenance Override”, follow the requirements of the most recent version of the Maintenance Override document from TÜV Product Service. The document is available from the TÜV website: www.tuv-fs.com (TÜV Süddeutschland).

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 which transfer the faulty modules into the safe condition within the safety time of the PES. The following section describes 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.

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.

Reaction Time

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

- Reading inputs
- Processing the application program
- Writing outputs
- Testing routines

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

Watchdog Time of the CPU (in the PES)

The watchdog time of the CPU is dependent upon system capabilities.

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 I/O modules is 10 ms.

Terminology

The following table defines the acronyms and terms used in this manual.

Term	Definition
EN	EuroNorm. The official European Standard
IEC	International Electrotechnical Commission
Non-Interacting	Does not interfere or affect functions of the safety system
NSP	Non-Safe Protocol
PES	Programmable Electronic System
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
POU	Program Organization Unit
PS	Programming System
SIL	Safety Integrity Level
SRS	System, Rack, Slot (This number is used as the System ID)
TÜV	Technischer Überwachungs-Verein (Technical Inspection Association)
WD	Watchdog Time

Central Functions

Chapter Introduction

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

GuardPLC 1200 is a compact system which 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.

GuardPLC 1600 and GuardPLC 1800 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.

GuardPLC 2000 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

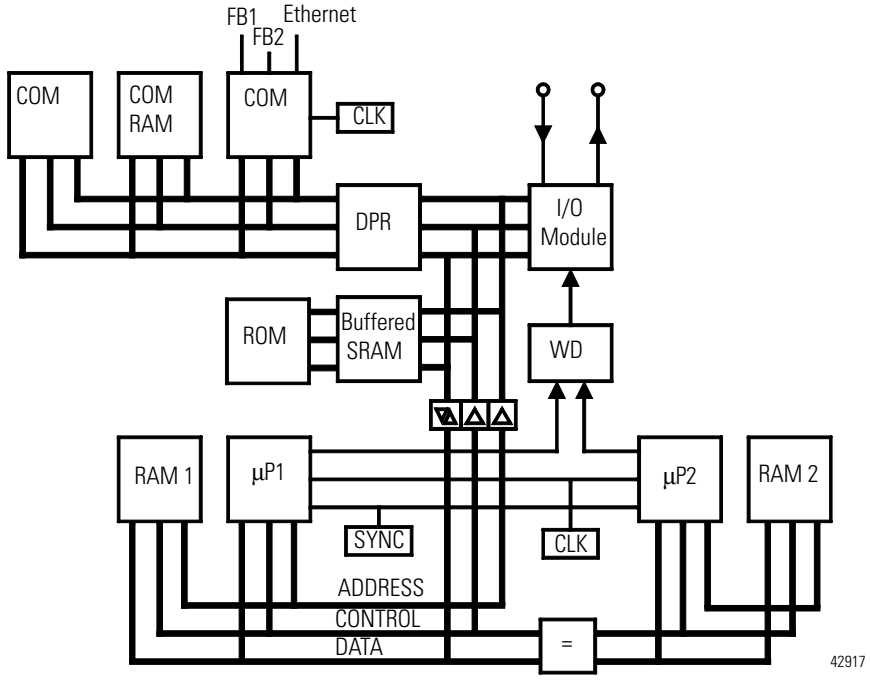
The power supply transforms the system supply voltage from 24V to 3.3V dc/5V dc (used for internal I/O Bus).

The power supply used with the GuardPLC 1200, 1600 or GuardPLC 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 2.1 Display of the Function Blocks (Using GuardPLC 2000):



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 comparator for all external access of both microprocessors
- in case of an error, the watchdog (WD) is set in the safe condition
- Flash EPROMs of the program memory for the operating system and user 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 interface(s) for data exchange by field bus
- system condition indicated by LEDs
- I/O-Bus-Logic for the connection with I/O modules
- safe 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-related 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:

- 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 user 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, user 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

If it is not triggered by the two CPUs within a defined time window, the watchdog is switched off. 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.

Error Diagnostics

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

Each GuardPLC distributed I/O module has its own LED 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 only transmitted 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.

Input Channels

Chapter Introduction

This chapter discusses GuardPLC controllers and I/O module input channels.

Overview

See the table below for an overview of GuardPLC 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 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

General Information on Safety-Related Input Modules

The safety-related input modules can be used both for safety-related and non-safety-related inputs.

The GuardPLC safety-related input modules have a diagnostic LED, quick error detection, and error localization.

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

Safety-related 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 ensure the safe function 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 which do not affect the safety function, user diagnostic information is not generated.

Safety of Sensors, Encoders, and Transmitters

In a safety-related application, the sensors and the PES must meet the same target SIL.

In this case, the safety-related 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.

Safety-Related Digital Inputs and Input Modules

The items listed in the following section apply to all of the digital input channels listed in the Overview on page 3-1, 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 safe 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 (safe condition) is processed in the application program for every error in the input module.

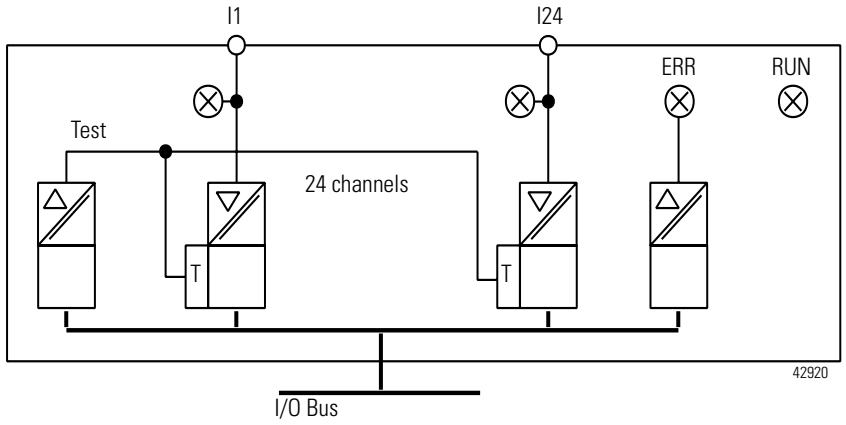
Because the PES has been designed to the closed-circuit current principle, a “0” signal is processed for the digital inputs in case of error. (See page 1-2 for an explanation of the closed-circuit current system principle.)

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” LED (“ERR” on GuardPLC 2000) 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 3.1 Example Block Diagram of Digital Inputs (Using GuardPLC 2000):



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.

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 3-6 to 3-8, also apply to the configurable digital inputs on the GuardPLC 1800.

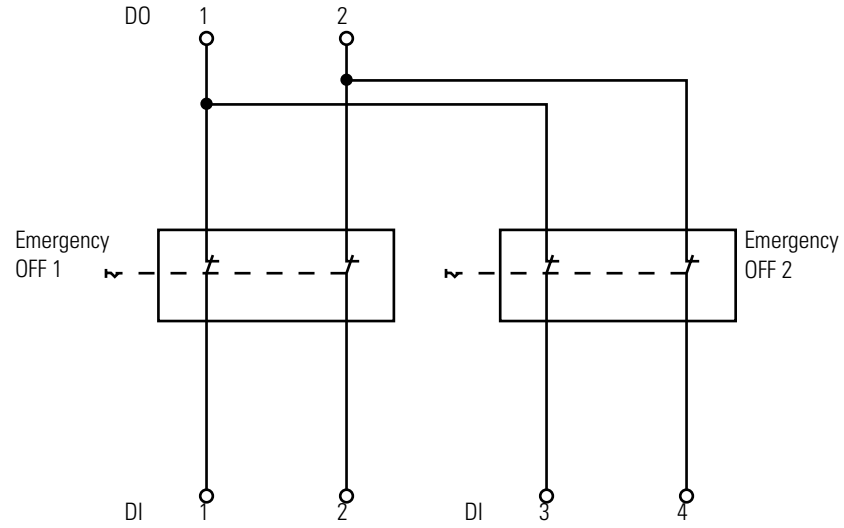
Line Control

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. As a result, line control is not available on GuardPLC 1800.

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

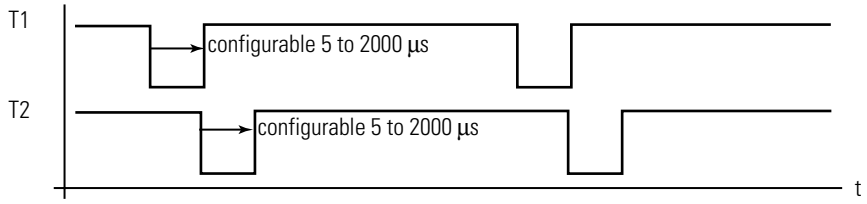
In addition, digital outputs are connected to the digital inputs of the same system, as shown in Figure 3.2.

Figure 3.2 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.

Figure 3.3 Digital Input Monitoring



The FAULT LED on the front plate of the controller/module flashes, the inputs are set to 0 and an error code is generated when the following 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

General

In the 8 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 user program.

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

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

(1) with scale factor 1000 selected in RSLogix Guard PLUS.
(2) with scale factor 2000 selected in RSLogix Guard PLUS.
(3) by external 250Ω shunt
(4) by external 500Ω shunt
(5) Safety 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 8 single-ended channels or 4 differential channels. No mixing is allowed. The following input values are possible:

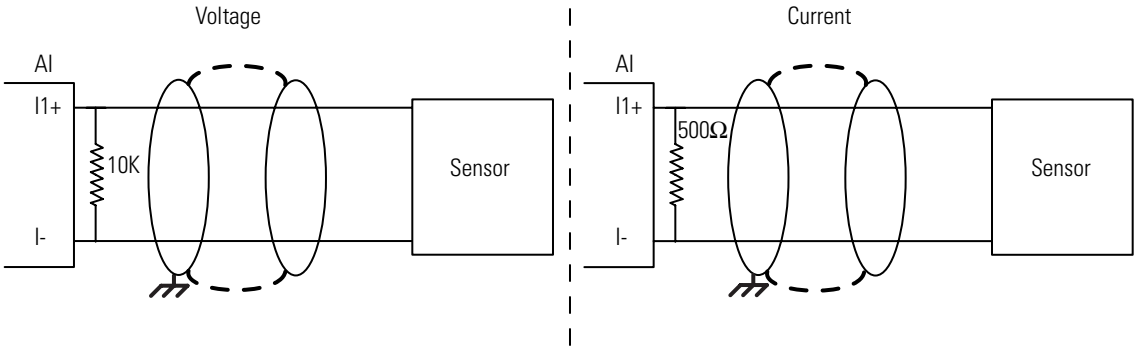
Number of Input Channels	Polarity	Current/Voltage	Value Range In Application	Safety Accuracy(5)
8	single-ended	0 to +10V dc	0 to 1000(1) 0 to 2000(2)	1%
8	single-ended	0/4 to 20 mA	0 to 500(1)(3) 0 to 1000(1)(4) 0 to 1000(2)(3) 0 to 2000(2)(4)	1%
4	differential	-10V dc to +10V dc	-1000 to +1000(1) -2000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

(1) with scale factor 1000 selected in RSLogix Guard PLUS.
(2) with scale factor 2000 selected in RSLogix Guard PLUS.
(3) by external 250Ω shunt
(4) by external 500Ω shunt
(5) Safety 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.

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 10K 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 10KΩ resistor parallel to the sensor. The internal resistance of the source must be taken into account.



IMPORTANT Unused analog input channels must be short-circuited.

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 which are then compared with a default value.

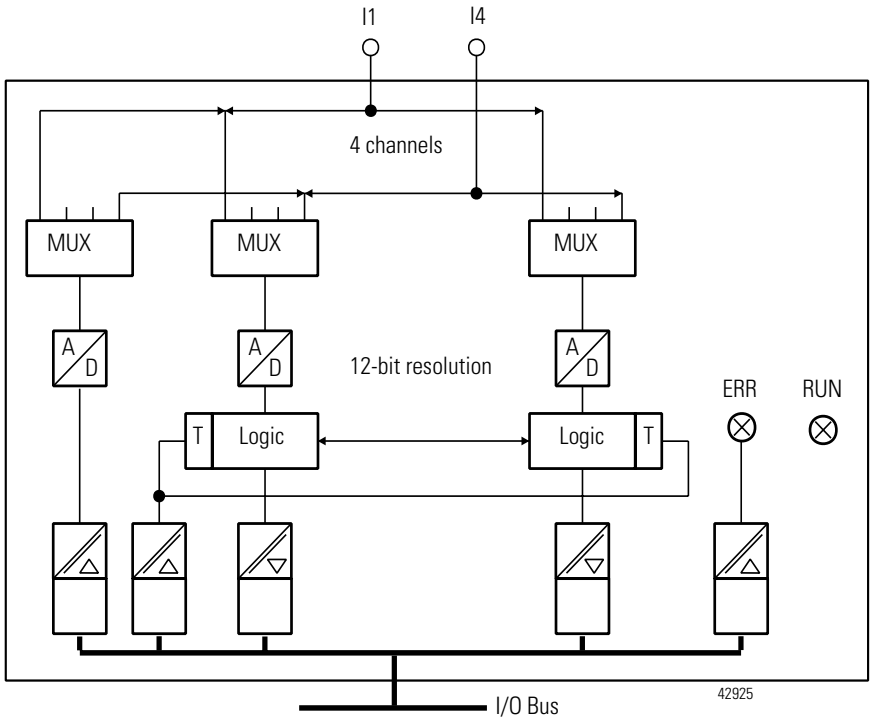
When faults are detected, the analog inputs are set to the "0" value in the application program.

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” LED 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 3.4 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 following sections 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 user 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 only be accomplished via the user program.

The 1755-HSC module features 4- or 8-bit encoder resolution. In the GuardPLC 1200 and 1800, 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.

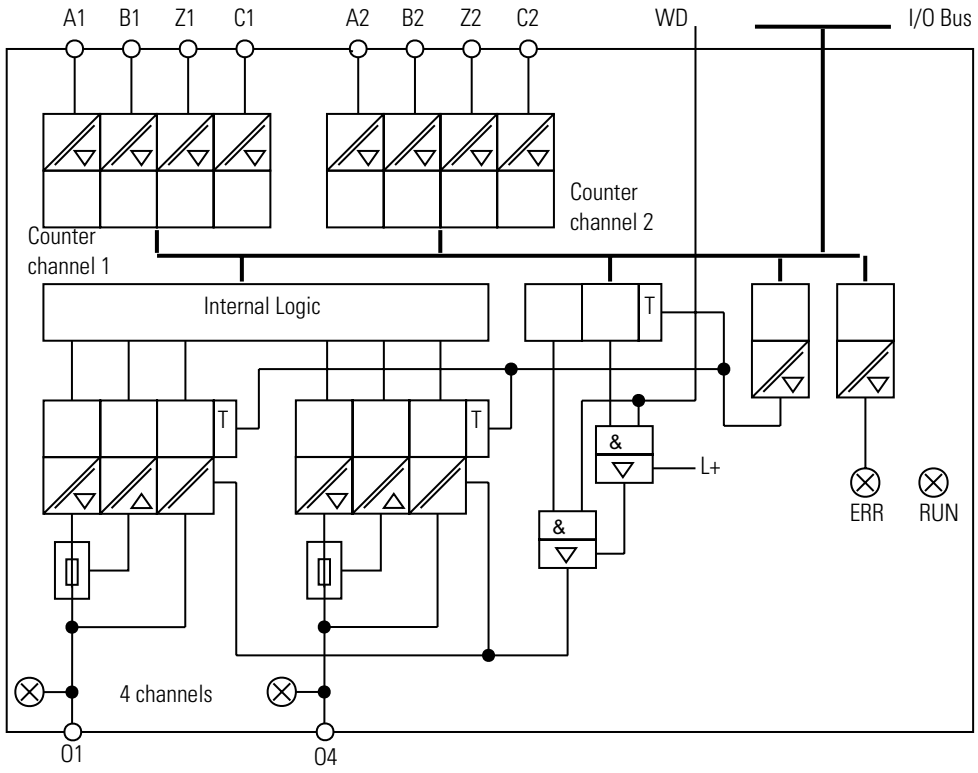
Reaction In Fault Condition

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 3.5 Example Block Diagram of Counter Inputs (Using 1755-HSC of the GuardPLC 2000):



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

Checklist for Safety-Related Inputs

Use the checklist on the following page for system configuration, programming and start-up of safety-related 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-related 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 Start-up of Safety Manual GuardPLC System

Company:	
Site:	
Loop definition:	

Safety-related input channels in the:

☐ GuardPLC 1200 ☐ GuardPLC 1800

☐ GuardPLC 1600 ☐ GuardPLC 2000

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

Output Channels

Chapter Introduction

This chapter discusses 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 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

General Safety Information On Safety-Related Output Modules

The safety-related 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 safe condition.

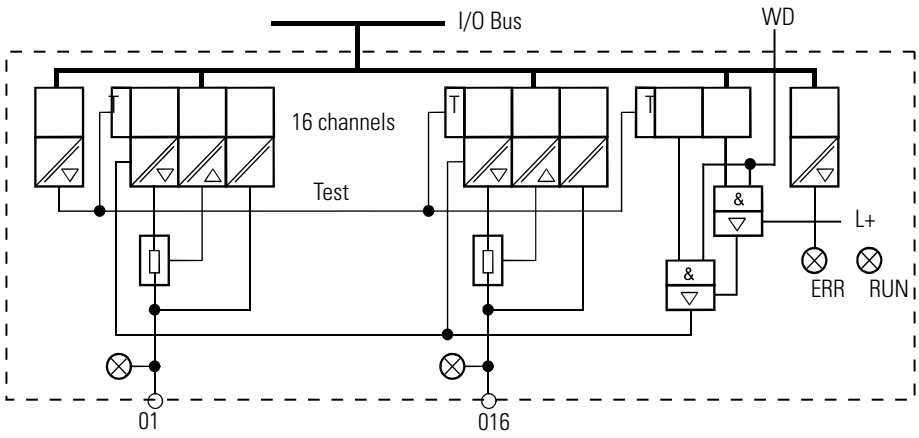
Three testable semi-conductor switches have been integrated, in series, into the safety-related output modules. Thus, the second independent switch-off, required for safety technical reasons, has been integrated on the output module.

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-related switch-off. The cessation of the WD signal results in the immediate transition to the safe condition.

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

Figure 4.1 Example Block Diagram of Digital Outputs (Using AB-DIO of the GuardPLC 2000)



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

Digital Outputs

Test Routines

The modules are automatically tested during operation. The essential test functions are:

1. Read back 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.

2. Check the integrated double-safety switches.

3. Low supply voltage protection. If the supply voltage drops below 13V, you will not be able to turn on any outputs.

4. At a minimum interval of 20 seconds, digital outputs are turned off for a maximum of 200 µs each (200 x 10E-6 sec).

Reaction To Error

The following conditions may occur as a result of errors.

Faults

If an output is incorrectly "HI" (1), all outputs of the module are set to the safe (0) condition via the safety switches. This is also indicated by the diagnostic LED.

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 safe 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-related digital outputs can be cycled with the safety-related digital inputs of the same system to allow short-circuit or line-break monitoring using Emergency shut-off devices (according to Category 4 in EN954-1). See Line Control on page 3-4.

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

Analog Outputs in the 1755-OF8 (AB-AO)

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.

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

Test Routines

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

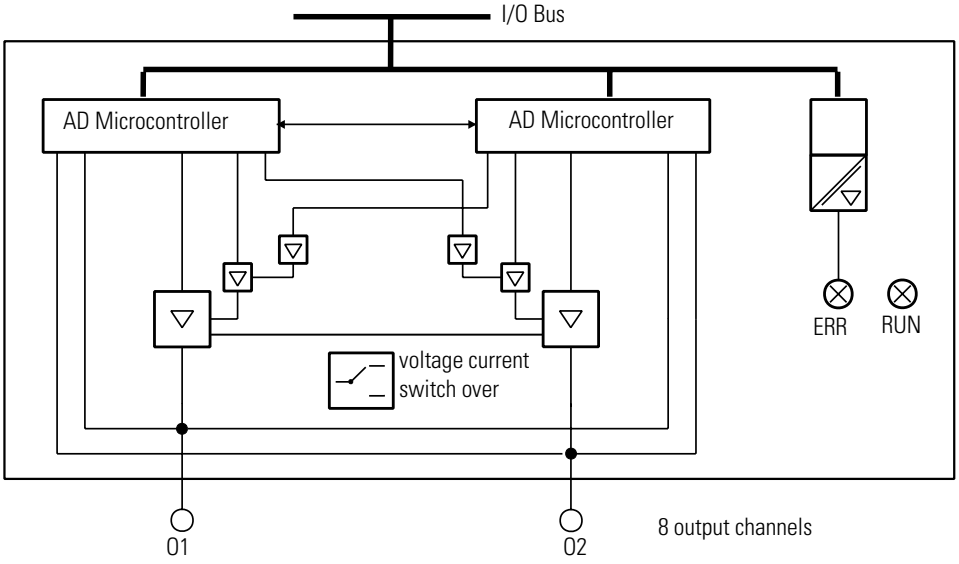
1. Safety-related 1oo2 A/D Microprocessor system.
2. Double read back of output signals.
3. Test for cross-talk between the outputs.
4. Check of the integrated safety switch-off.

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 LED.

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 ($WDZ_{AO-\mu C}$ x 2). See the specifications for the worst-case reaction time.

Figure 4.2 Example Block Diagram of Analog Outputs (Using 1755-OF8)



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

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

Checklist for Safety-Related Outputs

Use the following checklist for system configuration, programming and start up of safety-related 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 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-related 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-related 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-related output?	☐	☐	
2	Is this a digital output?	☐	☐	
3	Is the channel load corresponding to the maximum permissible value?	☐	☐	
4	Is load of system/module corresponding to the maximum permissible value?	☐	☐	
5	Are RC circuits provided on the control elements?	☐	☐	
6	Has the actuator been connected according to specifications?	☐	☐	
7	Is this output analog?	☐	☐	
8	Voltage outputs (DIP switch positions checked?)	☐	☐	
9	Current output? (DIP switch positions checked?)	☐	☐	
10	Have unused analog voltage outputs been left open?	☐	☐	
10	Have unused analog current outputs been short-circuited?	☐	☐	
11	Is a safety-related actuator planned for this output?	☐	☐	
12	Is the error message processed in the application program?	☐	☐	

GuardPLC Controller Operating System

Chapter Introduction

This chapter discusses the details of the GuardPLC controllers, their operating system and RSLogix Guard PLUS software.

Software for GuardPLC Safety-Related Systems

The software for the GuardPLC safety-related automation systems is arranged in the following three blocks:

- operating system
- application program
- programming tool (RSLogix Guard PLUS™) according to IEC 61131-3

The *operating system* is loaded in the central unit of the PES and must be applied in the corresponding applicable safety-related application certified by the TÜV.

The *application program* must be created using the programming tool RSLogix Guard PLUS 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. The application program is translated into machine code with the code generator. This machine code is transferred via an Ethernet interface into the Flash EPROMs of the GuardPLC 1200, 1600, 1800 controllers and the CPU module of the GuardPLC 2000, 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	---
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 LEDs	---
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 interface or serial line	Data exchange via COM (serial) is effected via a non-safe protocol: no writing of relevant safety signal
programming software interface: permissible actions	Fixed in RSLogix Guard PLUS: 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-related automation systems, are subject to revision controls and are documented on a list compiled in conjunction with TÜV.

Use RSLogix Guard PLUS to read the current operating system version. Verification is required. See the checklist on page 5-8.

Operation 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

Safety Concept of RSLogix Guard PLUS

The safety concept of RSLogix Guard PLUS 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-related PES or after a modification of the application program, the safety of the entire system must be checked by a complete functional test. To guarantee safety, the following 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 the created 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 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.

Creation of a Backup Program

When creating a backup program, follow the steps below in order.

1. Print out the application program to compare the logic with 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. To do this, select a controller in the Hardware Management Window and use the context menu About Configuration to display versions. The important versions to verify include:
   - root.config/rootcpu.config ("Configuration CRC of the CPU"). This indicates the overall configuration portion of the CPU that is safety-related.
   - root.config/rootcom.config, which indicates the overall configuration portion of the COM which is *not* safety-related.
   - root.config for each distributed I/O module.

4. Backup on memory medium and name it the application program, "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 using RSLogix Guard PLUS.

Parameters of the Automation System

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

The available options when using RSLogix Guard PLUS in the safety-related operation of the automation system are determined here and in the safety-related parameter preset.

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

Safety-Related Parameter CPU	Safe Setting
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	Reset/off
Main Enable (modification of the safety parameters)	Reset/Off (can only be set to OFF in RUN mode of the CPU)
Freeze	Reset/off

Forcing

Forcing is only permissible after consulting the approving board responsible for site approval. During forcing, the person in charge must ensure 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 only be set after re-enabling the force system.
- A “Select All” can be effected via the Force Editor in RSLogix Guard PLUS. 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. All individual force values and switches are held in their current state. Once you re-start forcing, they become active again.

More information about forcing can be found in the *GuardPLC Controller Systems User Manual*, publication 1753-UM001.

Basic information about forcing can be found in the TÜV document “Maintenance Override”. To access the document on the Internet, see the following websites:

- TÜV-Product-Service (www.tuvglobal.com), or
- TÜV-Rheinland (www.tuv-fs.com)

Protection Against Manipulation

The user, in conjunction with the approving board, must define what measures will be applied to protect against manipulation.

Protection mechanisms are integrated in the PES and in RSLogix Guard PLUS 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).
- The user must be logged in to the PES to access operating options.
- RSLogix Guard PLUS 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 only accessible if the PC uses RSLogix Guard PLUS, and the application project is the currently running version (backup maintenance). The link between programming software and PES is only necessary for the download of the application program or for reading out variable status. 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 on the basis of safety aspects?	☐	☐	
Are programming guidelines used for the creation of the application program?	☐	☐	
Are functionally independent sections of the program capsuled in functions and function modules?	☐	☐	
Were only safe signals used for all safety functions?	☐	☐	
Does each safety-related signal source correction (also via communication) reach the user program?	☐	☐	
Is each safety-related 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)?	☐	☐	
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 default for maximum/defined protection?	☐	☐	
Verify that the CPU operating system and the CRC are official licensed versions approved by TÜV	☐	☐	

Technical Safety for the Application Program

Introduction

This chapter discusses technical safety for the application program.

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

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

RSLogix Guard PLUS contains the following features:

- Input (function block editor) monitoring and documentation
- Variables with symbolic names and variable types (BOOL, UINT etc.)
- Assignment of the controllers (GuardPLC 1200, 1600, 1800 or 2000)
- 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 safe 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, EMERGENCY STOP, etc.

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 standard 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, Transmitters section, page 3-2.)
- Discrepancy monitoring and reaction

Actuators

- Position and activation in standard operation
- Safe 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 test routines for safety-related 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 (e.g., switching point).

The essential characteristic is the encapsulation of the standard 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. This is best used in combination with the I/O module channel[nn] state.

Only components which 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 uses the closed-circuit principle which requires the safe 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 safe state for connections between function blocks to be “0” or “1”. However, we recommend that you use a safe 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-Related Inputs and Outputs

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

In a digital safety-related I/O module, the input is set to a safe “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-related operation of the automation module and the safety-related parameters are preset.

Switch	Function	Default Value	Setting for Safe Operation[1]
Main Enable	The following switches/parameters can be modified during operation of the programming software.	ON	**OFF**
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**
Freeze	No further processing of the application program.	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**
Additional switches and parameters can be preset for forcing (See the Loading and Starting the Application Program section, page 6-8).			

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

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

Procedure for "Disabling" the PES

"Disabling" 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.

Follow the procedure below to “disable” the PES:

1. The following values must be set in the controller:

Main Enable	TRUE
Force Enable	FALSE (application-dependent)
Freeze	FALSE
Start/Restart	TRUE
Load Enable	TRUE
Autostart Enable	TRUE/FALSE
Stop during Force Timeout	TRUE (application-dependent)

2. After loading and starting, the following switches can be modified in the controller in the following sequence:

   a. Start / Restart to FALSE, and
   Load 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	to	TRUE
Autostart Enable	to	TRUE

   b. Main Enable to FALSE

ATTENTION

The “Freeze” switch must never be set to TRUE for safe operation.

Procedure for “Enabling” the PES

“Enabling” the PES means removing the active disable, for example, to execute measures to the PES.

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 the steps below to "Enable" the PES:

1. Set Main Enable switch to TRUE.
2. Set Start/Restart switch to TRUE.
3. Start the application program.
4. Then "Disable" the PES again (see the Procedure for "Disabling" the PES on page 6-6).

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.

Loading and Starting 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.

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.

Forcing 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 following table describes Forcing of Switches and Parameters.

Switches or Parameters	Function	Default Value	Setting for Safe Operation
Force Release	Enable the Force function	OFF	ON(1)
Force Timeout	Stop the CPU after exceeding the Force time	Stop	Stop(1)
Forcing Master	Forcing active	OFF	ON(1)
Force Time	Timeout of the Force value	0	Time in sec(1)

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

Forcing can be limited by time. The maximum force time is given in seconds. 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.

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

Program Documentation for Safety-Related Applications

You can print out the documentation of a project using RSLogix Guard PLUS. 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 (e.g. TÜV). The functional acceptance refers only to the application function, not to the safety-related 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.

Configuring Communications

Non-Safety-Related Communication

Apart from the input/output signals, signal statuses can also be exchanged via a data link with another system. To achieve this, the variables are declared in the COM area using RSLogix Guard PLUS. This data exchange can be read/write.

When configuring communication, the IP address serves as access safety. In addition, the SRS value of the CPU with a value divergent to the system ID offers a safe identification of the PES.

The data exchange between CPU (application program) and COM (bus variables) is currently accomplished via a non-safe protocol (NSP).

Therefore, only non-safety-relevant signals may be written as input variables in the COM field. They are also used as such in the application program.

ATTENTION

Any data imported from non-safe sources may not be used for the safety functions of the application program.

Depending on the controller, the following options are available for non-safety-related communication: Modbus, OPC, Profibus-DP, and ASCII read-only.

Safety-Related (Peer-to-Peer) Communication

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

ATTENTION

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

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

If safety-related 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.

ATTENTION

ReceiveTMO is a safety-related parameter.

Calculating Worst-Case Reaction Time

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.

Between PES and Remote I/O Modules

The worst-case reaction time between changing a transmitter of the first remote I/O module and the reaction of the outputs of the second remote 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 = $ReceiveTMO_2 + WDZ_{PES}$
$t_7 = 2 \times WDZ_{I/O-2}$

Terms

ReceiveTMO

The monitoring time, within which a valid response must be received. Safe 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.

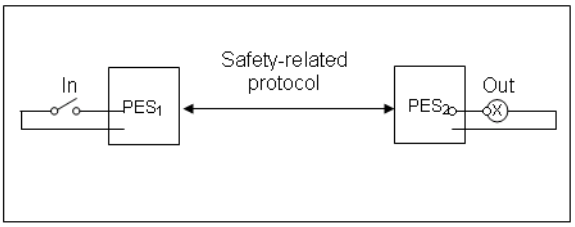
Watchdog

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-related protocols.



Specifications

Chapter Introduction

This chapter discusses climate, mechanical, and EMC environmental regulations.

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

IEC61131-2	Programmable Controllers Part 2: Equipment requirements and tests
IEC61000-6-2	EMC Part 6-2: Generic Standards - Immunity for Industrial Environments
IEC61000-6-4	EMC Generic Emission Standard - Industrial Environments

When using GuardPLC systems in safety-related applications, the following criteria must be met:

- Protection Class II, according to IEC/EN6661131-2
- Polution 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:

EN 61131-2 Paragraph 6.3.4	Test: Climatic Tests
	Temperature operating 0 to 60°C (Test limits -10 to 70°C)
	Storage Temperature -40 to 85°C (Battery only -30°C)
6.3.4.2	Dry heat and cold resistance test (70°C / -25°C, 96h, EUT Power supply unconnected)
6.3.4.3	Change of temperature, resistance and immunity test (25°C / 70°C, EUT Power supply unconnected and 0°C / 55°C, EUT)
6.3.4.4	Cyclic damp heat resistance test (25°C / 55°C, 95%r.F., Power supply unconnected)

Mechanical Conditions

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

EN 61131-2 Paragraph 6.3.5	Test: Mechanical Tests
	Vibration test operating 10 to 500Hz/2g
	Shock test operating 30g
	Shock test non operating 50g
6.3.5.1	Immunity vibration test (10 to 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 table:

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

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

Standard(s)	Noise Emission Tests
IEC/EN61000-6-4 EN50011, Class A	Radiated Conducted

Power Supply Conditions

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

EN 61131-2 Paragraph 6.3.7	Verification of DC Power Supply Characteristics
6.3.7.1.1	Voltage range test dc, -20%, +25% (19.2V to 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)

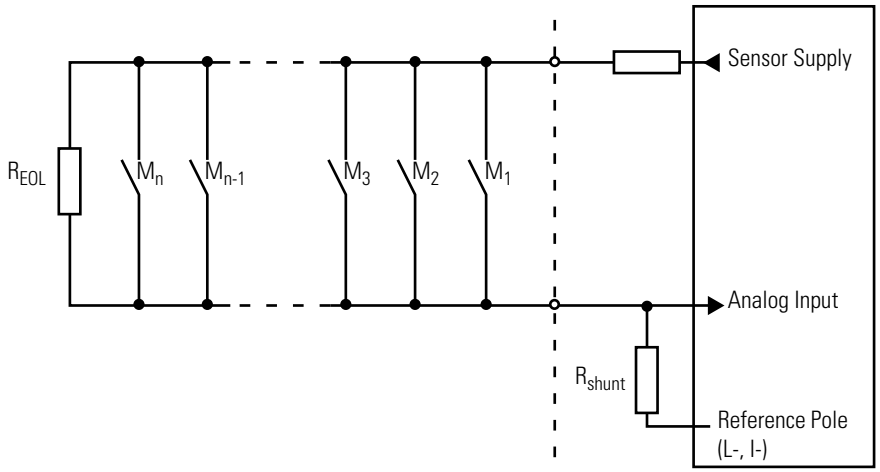
Use in Central Fire Alarm Systems

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.

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.

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 B.1 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

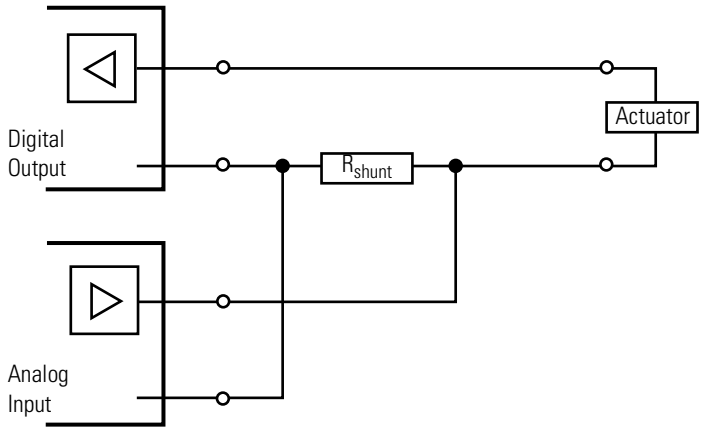
For the application, the resistance of R_{EOL}, R_L and R_{shunt} should be calculated based on the sensors used and the number of sensors per

alarm loop. The required data is contained in the relevant specifications from the sensor manufacturer.

The alarm outputs, used for activating lamps, sirens, horns, etc., 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, as shown below.

Figure B.2 Monitoring Actuator Current



Visual display systems, indicator light panels, LED displays, alphanumeric displays, audible alarms, etc., 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 using the closed-circuit current principle.

Fire alarms can be transmitted from one GuardPLC system to another using the standard Ethernet communications 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-related inputs, and all the channels of faulty safety-related outputs are switched off.

P

R

S

T

W

Reach us now at www.rockwellautomation.com

Wherever you need us, Rockwell Automation brings together leading brands in industrial automation including Allen-Bradley controls, Reliance Electric power transmission products, Dodge mechanical power transmission components, and Rockwell Software. Rockwell Automation's unique, flexible approach to helping customers achieve a competitive advantage is supported by thousands of authorized partners, distributors and system integrators around the world.

Americas Headquarters, 1201 South Second Street, Milwaukee, WI 53204, USA, Tel: (1) 414 382-2000, Fax: (1) 414 382-4444
European Headquarters SA/NV, avenue Herrmann Debroux, 46, 1160 Brussels, Belgium, Tel: (32) 2 663 06 00, Fax: (32) 2 663 06 40
Asia Pacific Headquarters, 27/F Citicorp Centre, 18 Whitfield Road, Causeway Bay, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1755-RM001B-EN-P – March 2004
Supersedes Publication 1755-RM001A-EN-P – September 2001
PN 957678-74