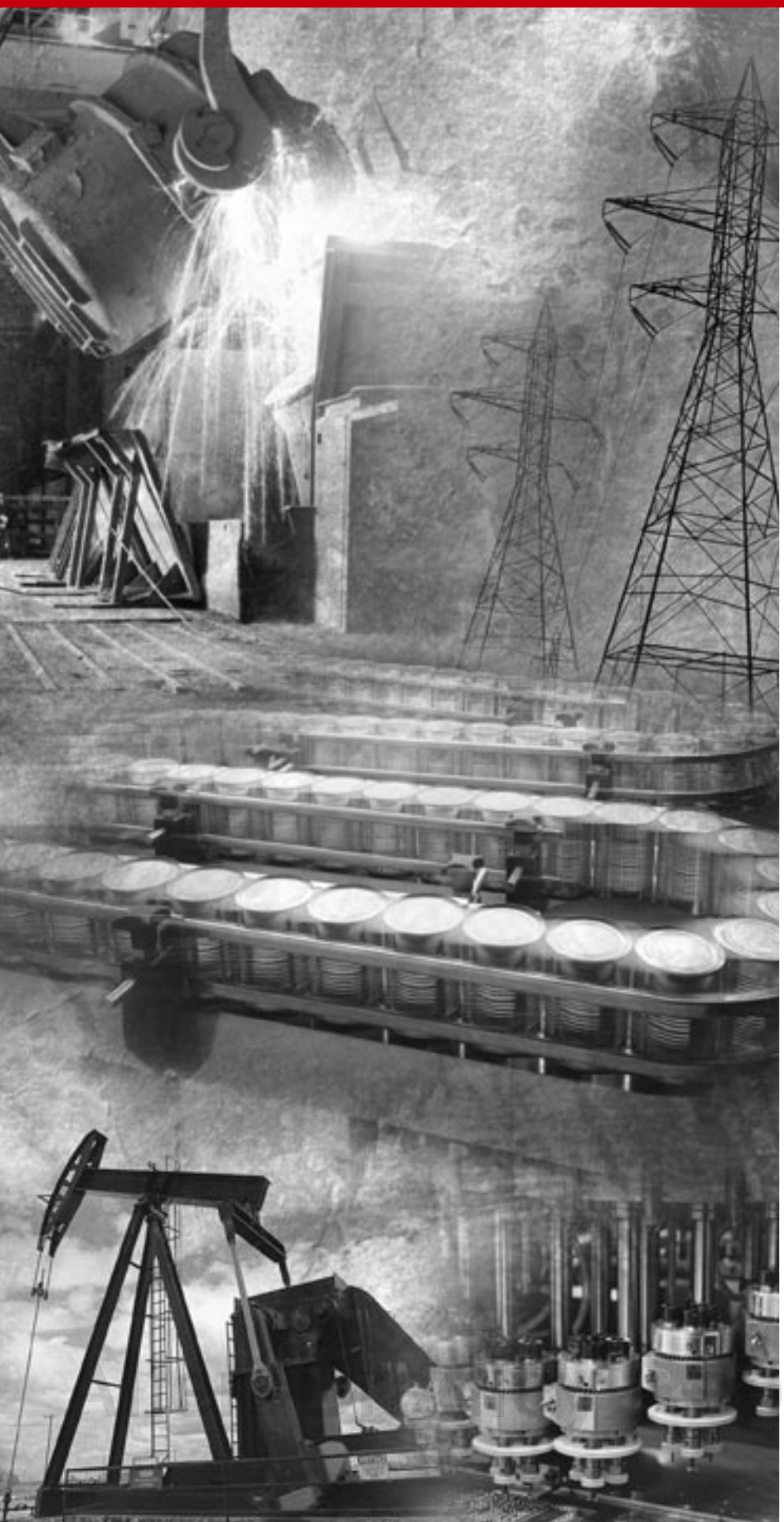


Allen-Bradley

GuardPLC 1200 and GuardPLC 2000

1754 and 1755

Safety Reference Manual

Rockwell Automation

Important User Information

Because of the variety of uses for the products described in this publication, those responsible for the application and use of this control equipment must satisfy themselves that all necessary steps have been taken to assure that each application and use meets all performance and safety requirements, including any applicable laws, regulations, codes and standards. Personnel responsible for the application of safety-related PES shall be aware of the safety requirements in the application of the system and shall be trained in using the system.

The illustrations, charts, sample programs and layout examples shown in this guide are intended solely for purposes of example. Since there are many variables and requirements associated with any particular installation, Allen-Bradley does not assume responsibility or liability (to include intellectual property liability) for actual use based upon the examples shown in this publication.

Allen-Bradley publication SGI-1.1, *Safety Guidelines for the Application, Installation and Maintenance of Solid-State Control* (available from your local Allen-Bradley office), describes some important differences between solid-state equipment and electromechanical devices that should be taken into consideration when applying products such as those described in this publication.

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

ATTENTION

Identifies information about practices or circumstances that can lead to personal injury or death, property damage or economic loss

Attention statements help you to:

- identify a hazard
- avoid a hazard
- recognize the consequences

IMPORTANT

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

European Communities (EC) Directive Compliance

If this product has the CE mark it is approved for installation within the European Union and EEA regions. It has been designed and tested to meet the following directives.

EMC Directive

This product is tested to meet the Council Directive 89/336/EC Electromagnetic Compatibility (EMC) by applying the following standards, in whole or in part:

- EN 50081-2 EMC — Generic Emission Standard, Part 2 — Industrial Environment
- EN 50082-2 EMC — Generic Immunity Standard, Part 2 — Industrial Environment
- EN 61131-2 — Programmable Controllers — Part 2: Equipment Requirements and Tests
- EN 61000-6.2 EMC — Part 6-2: Generic Standards — Immunity for Industrial Environments

This product is intended for use in an industrial environment.

Low Voltage Directive

This product is not required to meet Council Directive 73/23/EEC Low Voltage, because it is rated <50V ac and <75V dc.

This equipment is classified as open equipment and must be mounted in an enclosure during operation to provide safety protection.

Safety Policy

Chapter 1

Introduction 1-1
- Introduction to Safety. 1-1
- Safety Times 1-2
- Safety Restrictions 1-3

Terminology 1-4

Central Functions

Chapter 2

Chapter Introduction 2-1
Power Supply Module 2-1
Functional Description of the Central Processing Unit. 2-2
Self-Test Routines 2-3
- Microprocessor-Test. 2-3
- Test Memory Sectors 2-3
- Fixed Memory Sectors 2-3
- RAM-Test. 2-3
- Watchdog-Test. 2-3
- Test of the I/O Bus Within the System 2-4
- Reactions to Detected Errors in the CPU 2-4

Error Diagnostics. 2-4

Input Channels

Chapter 3

Chapter Introduction 3-1
Overview of GuardPLC 1200 and 2000 Input Modules 3-1
General Information on Safety-Related Input Modules 3-2
Safety of Sensors, Encoders, and Transmitters. 3-2
Safety-Related Digital Inputs and Input Modules. 3-2
- General 3-2
- Test Routines. 3-3
- Reaction To Error. 3-3
- Block Diagram of Digital Inputs With GuardPLC 2000 As Example: 3-3

Analog Inputs (Only In GuardPLC 2000) 3-4
- General 3-4
- Test Routines. 3-5
- Reaction In Case of Fault 3-5
- Block Diagram of Analog Inputs of the AB-AI Module. . 3-5

Counter Module 3-6
- General 3-6
- Test Routines. 3-6
- Reaction In Fault Condition 3-7
- Block Diagram of Counter Inputs With CO of the GuardPLC 2000 As Example: 3-7

Checklist for Safety-Related Inputs 3-8

Chapter 4

Output Channels

Chapter Introduction 4-1
Overview of GuardPLC 1200 / 2000 Signal Outputs 4-1
General Safety Information On Safety-Related Output Modules 4-2
Digital Outputs 4-2
Test Routines 4-2
Reaction In Case of Error 4-3
Block Diagram of Digital Outputs With AB-DIO of the GuardPLC 2000 As Example: 4-3
Safety-Related Analog Output Module 4-4
General 4-4
Test Routines 4-4
Reaction To Error 4-5
Block Diagram of Analog Outputs With AB-AO of the GuardPLC 2000 As Example: 4-5
Checklist for Safety-Related Outputs 4-6

Chapter 5

GuardPLC 1200/2000 Operating System

Chapter Introduction 5-1
Software for GuardPLC 1200 / 2000 Safety-Related Systems . 5-1
Technical Safety for the Operating System 5-2
Operation Mode and Functions of the Operating System . . 5-2
Technical Safety for Programming 5-3
Safety Concept of RSLogixGuard 5-3
Check the Created Application Program 5-3
Creation of a Program Backup 5-4
Possibilities of Program Identification 5-5
Parameters of the Automation System 5-5
Forcing 5-6
Protection Against Manipulation 5-7
Checklist for the Creation of an Application Program 5-8

Chapter 6

Technical Safety for the Application Program

Chapter Introduction 6-1
General Procedure 6-1
Safety-Related Applications Frames 6-1
Basis of Programming 6-2
Variable Declaration and I/O Name Input 6-3
Functions of the Application Program 6-4
Program Documentation for Safety-Related Applications 6-9
Configuration of COM 6-10

Conditions for Use

Chapter 7

Chapter Introduction 7-1
Climatic Conditions 7-2
Mechanical Conditions 7-2
EMC Conditions 7-3
Power Supply Conditions 7-3

Safety Policy

Introduction

This chapter introduces you to the safety policy.

For information about:	See page:
general safety	1-1
safety times	1-2
restrictions	1-3

Introduction to Safety

The Programmable Electronic System (PES) for the Rockwell Automation GuardPLC 1200 and 2000 family modules is safety-related, based on the 1oo2 microprocessor structure for one central module. These modules are safety-related up to safety requirement class 6 according to DIN V 19250, SIL 3 according to IEC 61508 respectively 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 comprise 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 creation of safety-related programs, use a PADT (Programming and Debugging Tool) with the programming tool RSLogixGuard, according to IEC 61131-3. (PADT is defined in IEC 61131-1.)

The PES has been designed for the dormant current principle. This requires that systems be designed in such a way that the “normally closed” or “on” state of external sensors and actuators be the normal run condition. The “off” or “normally open” state is the safe state. That is, in the event of a fault or safety trip, all elements should go to the “off” (no current flow) state.

Safety Times

Individual errors, that may lead to a dangerous operating condition are detected by the self-tests within the safety time of the PES and lead to defined error reactions which transfer the faulty modules into the safe condition. 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 admitted 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 in which the PES has to react in RUN mode 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 of input signals.

Multiple Error Occurrence Time (MOT):

The occurrence time for multiple faults is the time span 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 systems is the double cycle time of these systems. The cycle time of a system consists of the following parts:

- Read inputs
- Process of application program
- Write outputs
- Test routines

In addition, when considering the worst case of the system, the switching times of the inputs and outputs are taken in consideration.

Watchdog Time of the CPU (in the PES):

The watchdog time of the CPU is a value depending on system ability.

The watchdog time of the CPU is a default time in the menu for the setting of the controller attributes. 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. The watchdog time of the CPU must be within the setting ≥ 10 ms and ≤ 0.5 safety time of the PES.

The maximum permissible value will be 5,000 ms. The Default setting is 500 ms.

Safety Restrictions

For restrictions on the use of GuardPLC 1200 and GuardPLC 2000, see the following certification report.

Report to the Certificate Z2 01 03 43246 001
Safety Related Programmable Electronic System
GuardPLC 1200, GuardPLC 2000
No. 70001328

TÜV Product Service

Contact your Rockwell Automation representative for a copy of this report.

Terminology

The following table defines 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
PADT	Programming and Debugging Tool
PES	Programmable Electronic System
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

Central Functions

Chapter Introduction

This chapter discusses the power supply for the GuardPLC 2000 and the central module and self-test routines for both the GuardPLC 1200 and GuardPLC 2000.

For information about:	See page:
the power supply	2-1
functional description of the central module	2-2
self-test routines	2-3
error diagnostics	2-4

GuardPLC 1200 are compact systems which cannot be modified.

GuardPLC 2000 are modular systems in which - within one system - a power supply module, a CPU module and up to 6 I/O modules can be used.

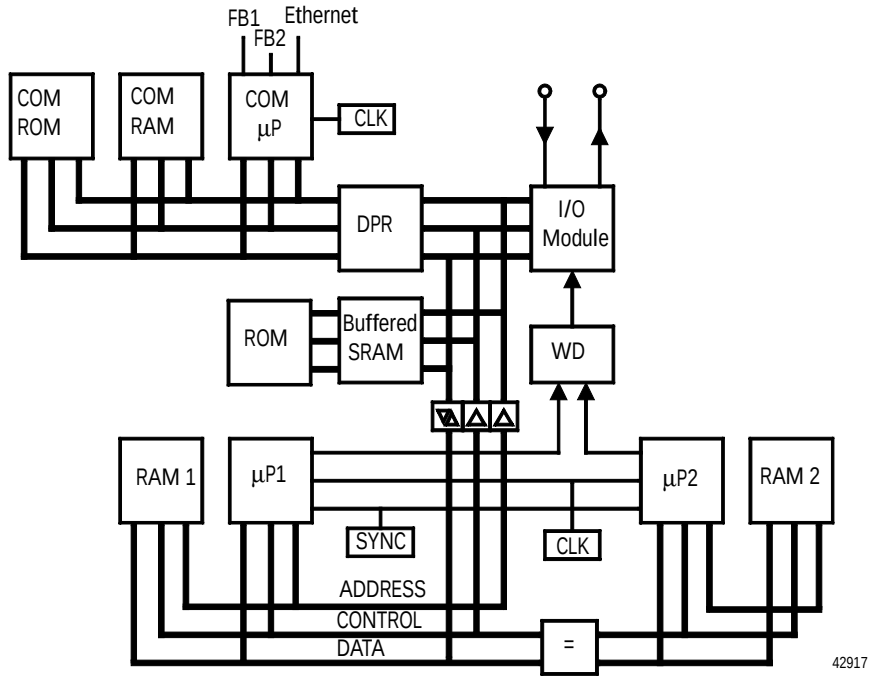
Power Supply Module

A power supply module is only available in the GuardPLC 2000. This function has already been integrated in the GuardPLC 1200 system and cannot be considered modular. The power supply module, respective of the integrated function, transforms the system supply voltage from 24V to 3.3V dc/5V dc (used for internal I/O Bus).

Functional Description of the Central Processing Unit

The central processing unit of the AB-CPU in the GuardPLC 2000 and the compact system GuardPLC 1200 respectively, consists of the following function blocks:

Display of the Function Blocks (GuardPLC 2000 As Example):



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 1200/2000 and PADT (PC) based on Ethernet.
- additional interface(s) for data exchange by field bus (FB2 only in GuardPLC 2000)
- 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 2000 RA-CPU central processing unit and for the GuardPLC 1200 system, and the interface to the I/O level are described under the keywords below.

Microprocessor-Test

The following 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 register

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

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 are tested with a Write/Read test, particularly for stuck at and cross coupling.

Watchdog-Test

The watchdog will be switched off if it is not triggered by the two CPUs in a defined time window. The same applies if the test of the hardware comparators fails. The possibility of switching off the watchdog signal is checked in a later test.

Test of the I/O Bus Within the System

The connection between the CPU and the related I/Os 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 the microprocessor system 1 are identical to the data of the microprocessor system 2. If this is not given, or if the test routines in the central area are negative, the system automatically goes into ERROR STOP and the watchdog signal will be switched off. This means that the outputs go to the de-energized, switched off condition and input signals will no longer be processed.

Error Diagnostics

Each GuardPLC 2000 module has its own LED to display errors in case of module failures. This provides a quick error diagnosis in case of failure in a module.

Error diagnostics are summarized in a collective error message in the GuardPLC 1200 - as it is a compact system.

The evaluation of various system variables, which 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 the communication with the CPU, that is, an evaluation via the CPU is still possible.

Input Channels

Chapter Introduction

This chapter discusses GuardPLC 1200 and GuardPLC 2000 input channels.

For information about:	See page:
input module capabilities	3-1
general safety-related information	3-2
safety of sensors, encoders, and transmitters	3-2
input modules safety-related digital inputs	3-2
analog inputs (GuardPLC 2000 only)	3-4
counter module	3-6
checklist for safety-related inputs	3-8

Overview of GuardPLC 1200 and 2000 Input Modules

See the table below for an overview of GuardPLC 1200 capabilities.

GuardPLC 1200		
System shares	Safety-Related	Non-Interacting
Digital Inputs		
20 Digital Inputs	**X**	**X**
2 Counter with 24-bit	**X**	**X**
Analog Inputs		
none		

See the table below for an overview of GuardPLC 2000 capabilities.

GuardPLC 2000			
Modules		Safety-Related	Non-Interacting
Digital Inputs			
AB-DIO	24-fold Digital Inputs	**X**	**X**
AB-CO	2 Counter with 24 bit	**X**	**X**
Analog Inputs			
AB-AI	8-fold Analog Inputs	**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 2000 safety-related input modules have a diagnostic LED, quick error detection, and error localization.

In addition, the systems for the user program offer status messages that can be evaluated. I/O errors stored in the diagnostic buffer can be read via RSlogixGuard.

Safety-related input modules are automatically subjected to a high-grade, cyclical self-test in the GuardPLC 1200 and 2000 during operation. These test routines are TÜV approved and ensure the safe function of the respective module.

When an error is detected, the application is provided with an "0" signal, and a detailed error message is generated optionally. If there are minor failures in the module (no affect on the safety function), no user diagnostic information is generated.

Safety of Sensors, Encoders, and Transmitters

In a safety-related application the sensors have to meet the same target SIL as the PES.

The sensors, encoders, or transmitters with the necessary SIL can be connected to the inputs of the PES.

If no sensors, encoders, or transmitters with the specific SIL are available, the sensors, encoders, or transmitters can be connected without specific SIL. The linking and monitoring of the signals then have to be programmed in the application program.

Notes on achieving the necessary SIL can be found, for example, in IEC 61511-1, Clause 11.4 and Table 5.

Safety-Related Digital Inputs and Input Modules

The items listed in the following section apply both to the GuardPLC 2000 1755-IB24XOB16 AB-DIO module digital input channels (see publication number 1755-IN003A-EN-P) and to the GuardPLC 1200 system digital input channels, if no specific module is named.

General

The digital inputs will be read once in every cycle and internally stored. 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 function 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.

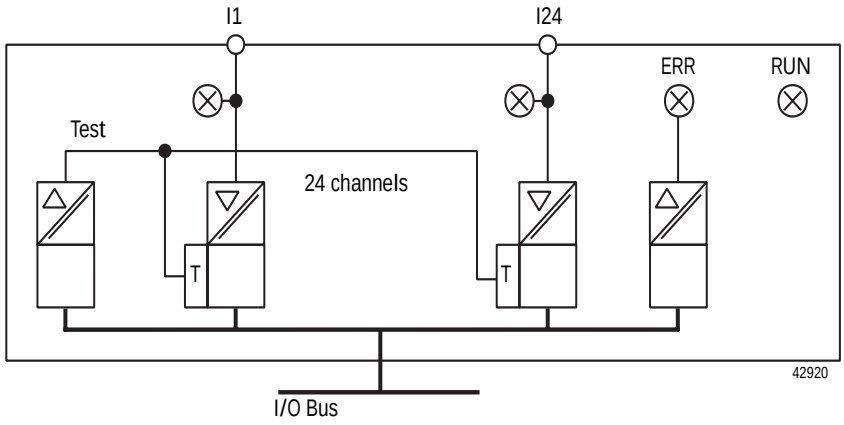
As the PES has been designed for the dormant current principle, an "0" signal is processed for the digital inputs in case of error. (See page 1-1 for an explanation of the dormant current system principle.)

Reaction To Error

If an error is found by the test routines for digital inputs, an "0" signal is processed in the application program for the faulty channel, and in the case of the GuardPLC 2000, the LED "ERR" is activated.

In addition to the signal value of the channel, the corresponding channel status signal has to be taken into account. When using the channel status signal in the application program, the user has additional possibilities to configure an error reaction in his program.

Block Diagram of Digital Inputs With GuardPLC 2000 As Example:



This display does not represent the data sheet of the related module.

Analog Inputs (Only In GuardPLC 2000)

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 then can be used in the user program.

The following input values are possible:

Number of Input Channels	Polarity	Current/Voltage	Value Range In Application
8	single ended	0 ... ±10V dc	0 ... ±1000
8	single ended	0/4 ... 20mA	0 ... 1000*
4	differential	-10V dc ... +10V dc	-1000 ... +1000

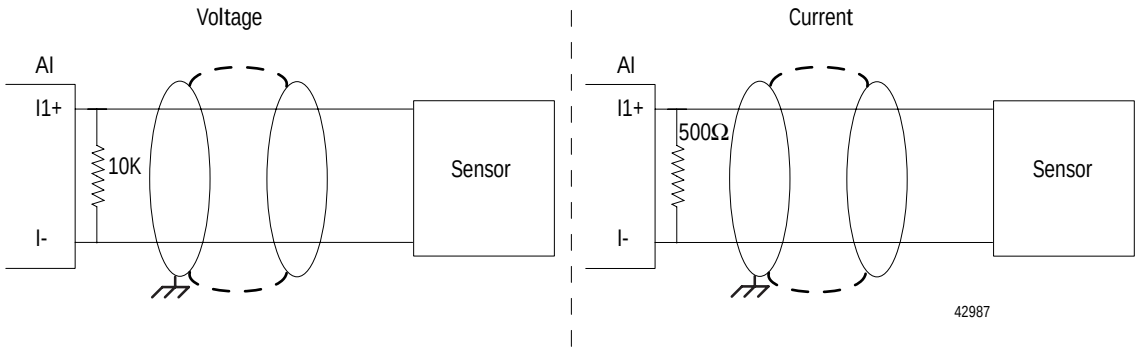
* by external 500Ω shunt

The AI module can be configured as either 8 single-ended channels or 4 differential channels. No mixing is allowed.

All of the channels default to voltage mode. On a channel by channel basis, a 500Ω shunt resistor can be added in parallel with the analog device if the current mode is requested. In current mode, the 10K resistor specified below is not required.

There is no live monitoring by the AI module; so in the event of a wire break, an input signal is still processing.

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



Unused AB-AI channels must be short-circuited.

Test Routines

The analog values are processed 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 in digital values and compared with a default value.

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

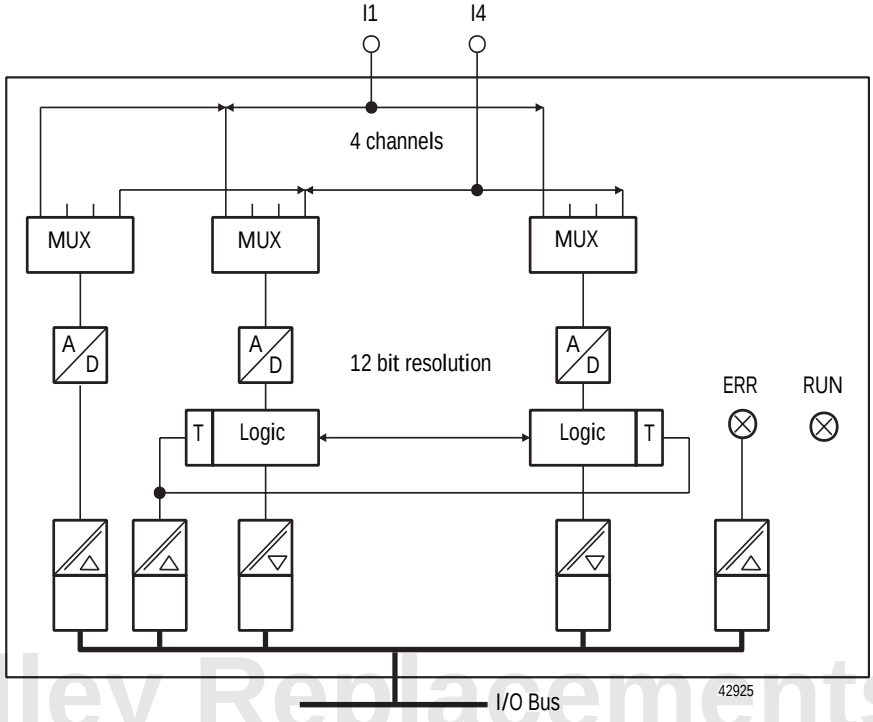
Reaction In Case of Fault

If the test routines for analog inputs detect an error, the value “0” is processed for the faulty channel in the application program and the LED "ERR" illuminates.

A status signal “≠ 0” is generated in addition for the application program. This can be taken into account for reactions in the application program by using in the logic.

Block Diagram of Analog Inputs of the AB-AI Module

The display does not represent the data sheet of the related module.



Counter Module

The items listed in the following sections apply for both the GuardPLC 2000 AB-CO module and for the GuardPLC 1200 system digital Counter input channels, if no explicit naming is effected.

General

Depending on the parameters in the user program, the counter can be operated as fast forward/backward counter with a resolution of 24-bit or as encoder in the Gray Code (4 respectively 3-bit or 8 respectively 6-bit).

When being used as quick forward/backward counter, the signals of the impulse input and the counter direction are necessary in the application. A reset is only effected in the program.

The encoder resolution 4- or 8-bit applies for the module AB-CO of the GuardPLC 2000; for the GuardPLC 1200, the encoder has a resolution of 3- or 6-bit. A reset is possible.

The link of 2 independent 4-bit-inputs to one 8-bit input (example of the GuardPLC 2000) is effected exclusively by the program. A switching possibility is not available for the purpose.

The encoder function monitors the modification of the bit pattern at the input channels. The bit patterns pending at the channels are directly transferred to the application program. The display in the PADT is effected in the form of a decimal figure corresponding to the bit pattern.

Depending on the application, this figure that corresponds to the Gray-Code bit pattern, for example, can be converted in BCD code.

Test Routines

When operated as encoder in the Gray code in the GuardPLC 2000, a value modification on only one bit input at the same time may be effected to the 4- or 8-bit inputs respectively (the 3- or 6-bit inputs of the GuardPLC 1200 respectively).

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

Reaction In Fault Condition

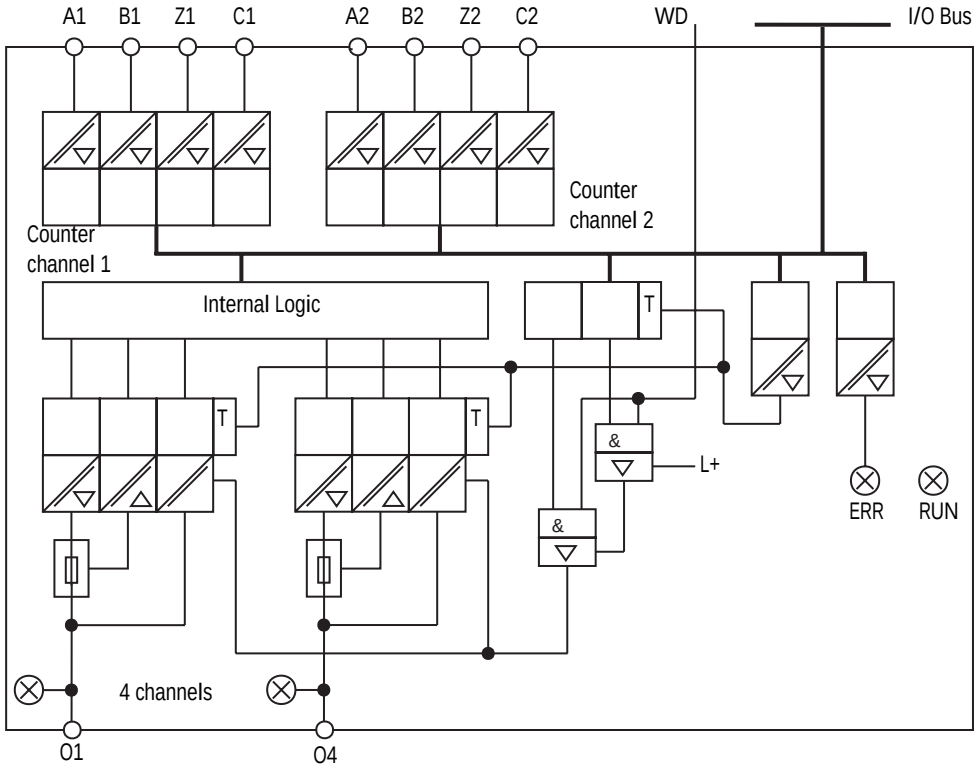
If an error is detected in the counter part of the module, the error message must be evaluated in the application program.

The respective channel status signal must be considered.

The user can configure and lay down the error reaction in the logic with the channel status signal.

Block Diagram of Counter Inputs With CO of the GuardPLC 2000 As Example:

This display does not represent the data sheet of the related module.



Checklist for Safety-Related Inputs

The following checklist is recommended for projecting, 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.

For projection or start-up, an individual checklist can be filled in for every single safety-related input channel in a system. This is the only way to make sure that the requirements were fully and clearly acquired. This checklist can also be used as documentation on the connection of external wiring to the application program.

Checklist for Projecting, Programming, and Start-up
Safety Manual GuardPLC 1200 and 2000

Company:	
Site:	
Loop definition:	

Safety-related input channels in the: ☐ GuardPLC 1200 ☐ GuardPLC 2000

No.	Requirements	Fulfilled		Comment
		Yes	No	
1	Is this a safety-related input?	☐	☐	
2	Is this input digital?	☐	☐	
3	Is this input analog?	☐	☐	
4	unipolar 0 - ±10V dc?	☐	☐	
5	unipolar 0-20mA?	☐	☐	
6	bipolar ±10V dc?	☐	☐	
7	Is the voltage input terminated or with error exclusion?	☐	☐	
8	Do the ranges of the sensors set fit the channel configuration?	☐	☐	
9	Are the analog inputs not used short-circuited?	☐	☐	
10	Is this input a counter?	☐	☐	
11	Function: Pulse counter?	☐	☐	
12	Function: Encoder (Gray-code)?	☐	☐	
13	Has a safety-related encoder/sensor been provided for this input?	☐	☐	
14	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.

For information about:	See page:
output module capabilities	4-1
general safety-related information	4-2
digital outputs	4-2
safety-related analog output module	4-4
checklist for safety-related outputs	4-6

Overview of GuardPLC 1200 / 2000 Signal Outputs

See the table below for an overview of GuardPLC 1200 capabilities.

GuardPLC 1200		
System share	Safety-Related	Non-Interacting
Digital outputs		
8 Digital outputs	**X**	**X**
Analog outputs		
none		

See the table below for an overview of GuardPLC 2000 capabilities.

GuardPLC 2000			
Modules	Safety-Related		Non-Interacting
Digital output modules			
AB-DIO	16-fold Digital Outputs	**X**	**X**
AB-CO	4-fold Digital Outputs	**X**	**X**
Analog Output modules			
AB-AO	8-fold Analog Outputs	**X**	**X**

General Safety Information On Safety-Related Output Modules

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

For outputs, the status "0" is the safe condition.

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

This so-called integrated safety switch-off, safely shuts down all channels of the defect output module in case of error (de-energized condition).

In addition, the watchdog signal from the CPU module also affects the safety-related switch-off. The cessation of the WD signal results in the immediate move to the safe condition. The WD function as described is only valid for the AB-DIO.

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

Digital Outputs

The items listed in the following section apply for both the GuardPLC 2000 AB-DIO and AB-CO modules digital output channels and for the GuardPLC 1200 system digital output channels, if no explicit naming is effected. For information about digital inputs, see publication number 1755-IN003A-EN-P.

Test Routines

The modules are automatically tested when in 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 a 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 in the AB-DIO and AB-CO modules will be turned off for 200µs each (200*10E-6 sec).

Reaction In Case of Error

The following conditions may occur as a result of errors.

If a faulty "1" signal has been detected, all outputs of the module are set to the safe "0" condition via the safety switches. In the GuardPLC 2000, this also is displayed by the diagnosis LED.

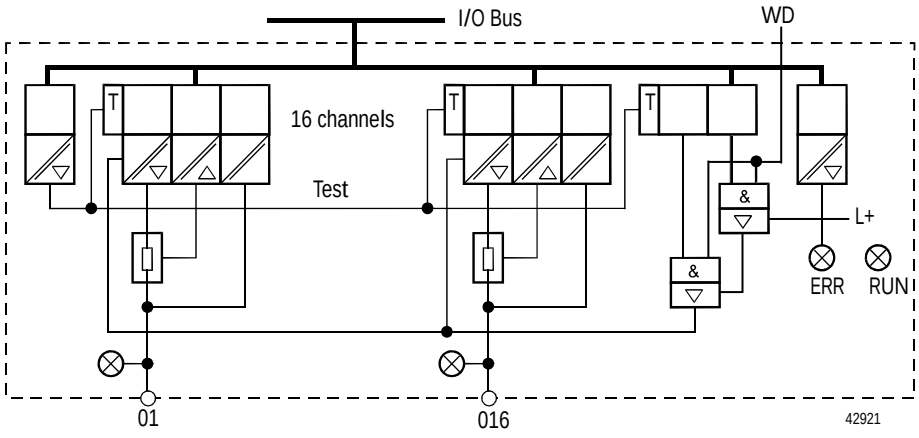
The testability in GuardPLC 1200/2000 of the module is maintained when there is a short circuit at an output. It is not necessary to switch off via safety shut-down.

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 "0" state.

In case of error, the output, along the rules of dormant current principles, is set to zero voltage.

Block Diagram of Digital Outputs With AB-DIO of the GuardPLC 2000 As Example:

This illustration does not show the data sheet of the related module.



Safety-Related Analog Output Module

Only available in GuardPLC 2000.

General

The analog outputs are written once per cycle and stored internally. This functionality is tested by the module itself.

The safety-related analog output modules can be set per DIP switches on the module as voltage or current output.

ATTENTION

Check the switch settings before inserting the module into the chassis.

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

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

The analog output module can be configured for current or voltage output. Hardware configuration is carried out on the module via DIP switches.

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 will result in erroneous behavior of the module.

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 signal.

3. Test for cross talk between the outputs.

4. Check of the integrated safety switch-off.

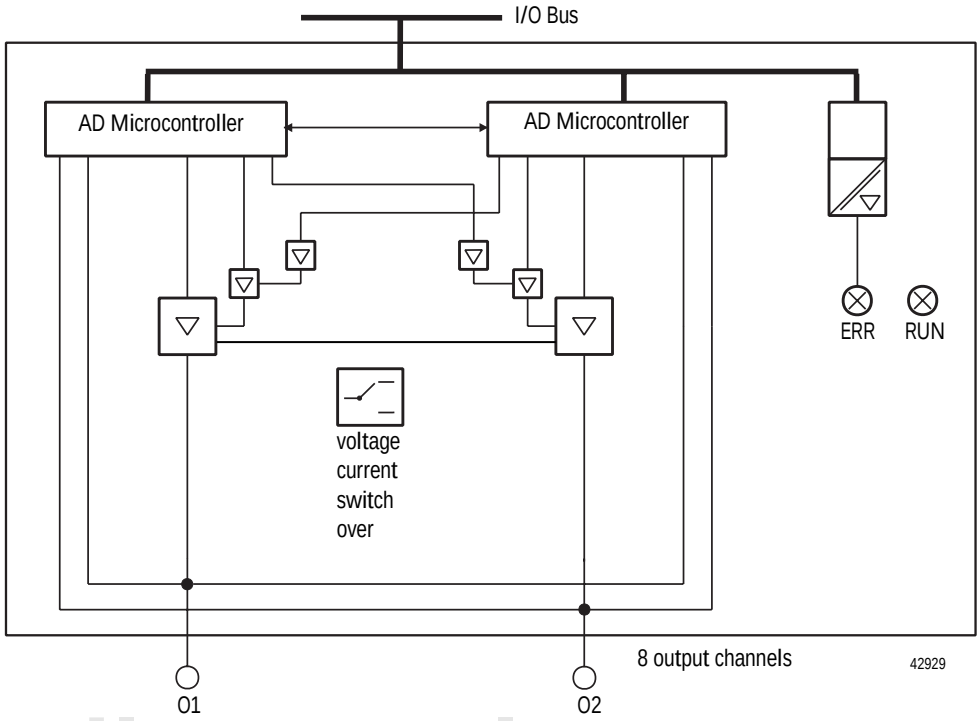
Reaction To Error

The output signals are read back once per cycle and compared with the internally stored output signals of the intelligent module 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 ERROR LED.

For the worst case reaction time of the analog outputs, the double watchdog time (WDZ_{CPU}*2) has to be added to the double watchdog time of the AO-CPU ($WDZ_{AO\text{-}\mu C}$*2). See the data sheet for the worst case reaction time.

Block Diagram of Analog Outputs With AB-AO of the GuardPLC 2000 As Example:

This illustration does not show the data sheet of the related module.



Checklist for Safety-Related Outputs

The following checklist is recommended for projecting, 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.

In the scope of projecting or start-up, an individual checklist for controlling the requirements to be considered can be filled in for every single safety-related output channel in a system. This is the only way to make sure that the requirements are fully and clearly acquired. This checklist can also be used as documentation on the connection of external wiring to the application program.

Check List for Projecting, Programming, and Start-up
Safety Manual GuardPLC 1200/ 2000

Company:	
Site:	
Loop definition:	
Safety output channels in the:	☐ GuardPLC 1200 ☐ 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 max. permissible value?	☐	☐	
4	Is load of system/module corresponding to the max. permissible value?	☐	☐	
5	Are free-wheeling circuits provided on the control elements?	☐	☐	
6	Is this output analog?	☐	☐	
7	Voltage outputs (switch positions checked?)	☐	☐	
8	Current output? (switch positions checked?)	☐	☐	
9	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 1200/2000 Operating System

Chapter Introduction

This chapter discusses the details of the GuardPLC 1200 and GuardPLC 2000 operating system.

For information about:	See page:
software	5-1
technical safety	5-2
operating mode and functions	5-2
technical safety for programming	5-3
parameterizing the automation module	5-5
forcing	5-6
protection against manipulation	5-7
checklist for the creation of an application program	5-8

Software for GuardPLC 1200 / 2000 Safety-Related Systems

The software for the GuardPLC 1200 and GuardPLC 2000 safety-related automation systems is arranged in the following three blocks:

- operating system,
- application program, and
- programming tool (RSLogixGuard™) according to IEC 61131-3

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

The *application program* has to be created by the programming tool RSLogixGuard and contains the specific equipment functions that are to be carried out by the automation module. Parameters for the operating function are also entered into the system using RSLogixGuard. 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, and the CPU module of the GuardPLC 2000, respectively.

The essential functions of the operating system and the connections 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 1200 or 2000 controller
CPU test	---
I/O module tests (depending on type)	Depends on the I/O modules used (only for GuardPLC 2000)
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 /CPU
Communication via Ethernet interface or ASCII protocol	Data exchange via COM is effected via a non-safe protocol: no writing of relevant safety tag
PADT interface: permissible actions	Fixed in RSLogixGuard: Configuration of protection functions, User login

Technical Safety for the Operating System

Every licensed operating system is identified by its name. For better distinction purposes, the revision and CRC signature are given. The respective applicable versions of the operating system and the related signatures (CRCs), approved by the TÜV for safety-related automation systems, are subject to revision controls and are documented on a list compiled together with the TÜV.

Use RSLogixGuard to read the current operating system version. A verification is required. See the checklist on page 5-8.

Operation Mode and Functions of the Operating System

The operating systems processes the application program in cycles. The following functions, in greatly simplified form, are executed:

- read input data
- processing 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
- diagnosis

Technical Safety for Programming

Safety Concept of RSLogixGuard

The safety concept of RSLogixGuard warranties, that:

- the PS works correctly, that is, programming system errors can be detected.
- the user applies the PS correctly, that is, 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 function test. To guarantee safety, the following three steps must be carried out:

1. Double compilation of the application program followed with 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 function test of the logic (see the next section, Check the Created Application Program).

Check the Created 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. RSLogixGuard and the measures defined in the safety manual make it sufficiently impossible that a semantic and syntactic correct code is generated that can contain undetected systematic errors from the process of code generation.

A suitable test set must also be generated for the numeric evaluation of formulas. Equivalent range tests are acceptable. These are tests within the defined value ranges, at the limits, or in impermissible value ranges. The test cases must be selected to prove the correctness 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 this is the only means of detecting correct wiring of the sensors and actuators to the system. Furthermore, this is the only means of testing the system configuration.

Creation of a Program Backup

When creating a program backup, the following steps should be carried out.

1. Printout 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 Configuration Control Center and use the context menu About Configuration to display versions. The important versions to verify include:
   - /config/rootcpu.config (“Configuration CRC of the CPU”). This indicates the overall configuration part of the CPU that is safety-related.
   - /config/rootcom.config which indicates the overall configuration part of the COM which is not safety-related.

4. Backup on memory medium and we also recommend that you 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.

Possibilities of Program Identification

The application program is clearly identified by the "Configuration CRC of the CPU". The related backup can thus be determined clearly. The identification of a backup should contain the "Configuration CRC of the CPU".

To make sure that the used backup is unmodified, the backup is first compiled and then this newly generated code version is compared with the code version of the program loaded in the controller. The comparison can be displayed with RSLogixGuard.

Parameters of the Automation System

The following parameters determine the behavior of the automation system in operation and are set in RSLogixGuard.

The available options when using the programming tool RSLogixGuard in the safety-related operation of the automation system are determined here and in the safety-related parameter preset.

The seizures possible in safety-related operation are not inflexibly bound to a certain requirement class, but have to be set up for every implementation of the automation system to the applicable approving board.

Safety-Related Parameter CPU	Safe
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 has to ensure sufficient safety technical monitoring of the process by other technical and organization measures.

The following forcing possibilities are available:

- Forcing can be prohibited by configuration. The PES then no longer accepts force values defined specifically by the application. In this case, new force values can only be set again after enabling the force system.
- A "Select All" can be effected via the Force Editor in RSLogixGuard.
- All forced inputs or outputs can be reset by STOP force command in the Force Editor in RSLogixGuard. All individual force values and switches are kept in their state. This means that after you start forcing again, these become active again.

More details about forcing can be found in the Application Manual.

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

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

Protection Against Manipulation

The user, together with the approving board in charge, must define what measures are to be applied for the protection against manipulation.

In the PES and in RSLogixGuard, protection mechanisms are integrated that prevent unintentional or unauthorized modifications to the safety system:

- A modification to the application program generates a new version number. These modifications can only be transferred to the PES by downloading (PES must be in STOP).
- Operator options are set up per user login in PES.
- RSLogixGuard has a password link to the PES upon user login.
- The link between PADT 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 in the operator's field of competence.

ATTENTION

Protect the password against unauthorized access. The default setting for both the login and password must be modified.

The PES data is only accessible if the PADT used has a programming tool and the application project is the currently running version (backup maintenance). The link between PADT and PES is only necessary for the download of the application program or for reading out variable statuses. In normal operation, the PADT is not required. A physical separation of PADT and PES in the standard operation phase protects against unauthorized access.

Checklist for the Creation of an Application Program

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

Checklist for Creation of an Application Program Safety Manual GuardPLC 1200/ 2000			
Company:			
Site:			
Project definition:			
File definition / Archive number:			
Notes / Checks	**Yes**	**No**	**Comment**
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?	☐	☐	
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?	☐	☐	
After a Modification - After Loading			
Was 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

Chapter Introduction

This chapter discusses technical safety for the application program.

For information about:	See page:
general procedure	6-1
safety-related applications frames	6-1

General Procedure

The general procedure for programming the GuardPLC 1200 and 2000 automation module for technical safety applications is listed below.

- Specification of the control function.
- Writing the application program.
- Compiling the application program with the C-code generator.
- Translate twice the C-code and compare the results.
- The program is created without errors and operable.
- Verification and validation.

The program can then be tested and the PES can start up safe operation.

Safety-Related Applications Frames

(This section contains defaults and rules, requirements from sample construction surveys, etc.)

The application program is created with the programming tool RSLogixGuard for personal computers using the operating system Windows NT® or Windows 2000®.

RSLogixGuard contains the following features:

- Input (function module editor), monitoring and documentation
- Variables with symbolic names and variable type (BOOL, UINT etc.)
- Assignment of the controllers (GuardPLC 1200/2000)
- Code generator (Translation of the application program into the machine code)

Basis of Programming

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 type of presentation of the specification depends on the task to be carried out. This can be:

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
- Procedure plans
- 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 equipment must contain the analysis of field circuits, that is, the type of sensors and actuators:

Sensors (Digital or Analog)

- Signal in standard operation (dormant current principle for digital sensors, life-zero for analog sensors)
- Signal for error
- Determination of redundancies required for safety technical 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, power failure respectively.

The targets when programming the application program should be:

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

Variable Declaration and I/O Name Input

With the help of the variable declaration editors, the variable names and their data type are defined. Symbolic names are assigned to all variables of the application program. These symbolic names can consist of a maximum of 256 characters.

Symbolic I/O names are used for physical inputs and outputs; here again they can consist of a maximum of 256 characters.

The use of symbolic names instead of a physical address has two essential advantages:

- In the application program, the equipment definitions of inputs and outputs can be used.
- 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

The measuring point list, a list of the sensors and actuators respectively., 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/channels are automatically executed by the operating system.

Types of Variables

Depending on the program organization unit (POU) - program or function module - different types of variables can be defined. An overview of these variable is in the following table.

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

*Tags: - Variables that can either be attached to hardware or, for example, be used as "flags" on program level.
**CONSTANT: - Constant that cannot be overwritten by the application program (e.g., switching point).

The essential characteristic is the capsulation of functions in self-created function modules and functions from the standard functions. 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 the modules into a large module or 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, care must be taken that the dormant current principle for the physical inputs and outputs is taken into account. This is best used in combination with the I/O module channel[nn] state.

Exclusively elements according to IEC 61131-3 with their corresponding function conditions are used with the logic.

- The application program can contain the sensible logic and/or arithmetical functions without taking account of the external dormant current principle.
- The I/O uses the dormant current principle which requires the safe state of the inputs and outputs to be “0”. The logic in the controller does not rely on the dormant current principle, so you can determine the safe state for connections between function blocks to be “0” or “1”. But, it is recommended that you use a safe state of “0” between function blocks.
- The logic should be effectively designed and documented for easy troubleshooting. This includes using flow charts and writing good documentation of the logic in the program. This does not replace any of the documentation requirements for your applications. Flow charts and logic documentation should be included if it is 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 analog, safety-related input modules, defined values can be further processed in an error case.

In a digital safety-related I/O module, the input is set to a safe "0" and the digital output module is switched off by 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 PADT in the safety-related operation of the automation module and the safety-related parameters are preset.

Switch	Function	Default Value	* Setting for Safe Operation
Master	The following switches/parameters can be modified in operation of PADT.	ON	**OFF**
Autostart	Automatic start after initializing the CPU.	OFF	**** ON/OFF**
Restart/Start	Coldstart, warmstart or hotstart by PADT in the condition RUN or STOP.	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 hardware 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 approval board**

Further switches and parameters can be preset for forcing (See the Loading and Starting the Application Program section, page 6-8)
* the setting to the values only applies when you are online
** configuration ON or OFF depends on the application

Procedure for "Disabling" the PES

"Disabling" the PES means locking functions and intervention possibilities from the user while in operation. A manipulation of the application program is thus prevented. The amount of disablings is to be seen in relation to the safety requirements on the use of PES, can however, also be executed as per consultation with the approving board in charge for site acceptance.

The following procedure has to be followed for "Disabling" PES:

1. The following values have to be set at the controller:

Main Enable	TRUE
Force	FALSE
Freeze	FALSE
Start/Restart	TRUE
Loading	TRUE
Autostart	FALSE

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

   a. Start / Restart to FALSE and
      Loading to FALSE

ATTENTION

Only upon consultation with the approving board, the following switches can be set at other values

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

   b. Main Enable to FALSE

ATTENTION

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

Procedure for "Enabling" the PES

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

The prerequisite for putting "Main Enable" to ON is the condition STOP of the PES. An **Activating** "Main Enable" is **not** possible when PES is running (in RUN condition). **Deactivating** “Main Enable” **is** possible while in RUN.

For a restart after an initialization of the CPU (after voltage failure), the following steps have to be taken to "Enable" the PES:

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

Code Generation

The code is generated after complete input of the application program and the I/O assignment of the controllers. Thereby the "Configuration CRC of the CPU" is formed.

The "Configuration CRC of the CPU" is a signature on the entire configuration of the CPU and the output is a Hex-Code in the 32-bit format. All configurable or modifiable elements such as logic, variables, switch settings are involved.

Loading and Starting the Application Program

The loading process of a control GuardPLC 1200 or GuardPLC 2000 can only be effected if the control had been set to STOP before.

Online loading processes are not possible.

Only one application program can be loaded into the respective CPU. The complete loading of an application program is monitored. Then the application program is started, that is, the cyclical process of the routine.

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 logic link.

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 makes sure that sufficient technical safety process monitoring is effected by other technical and structural measures during forcing.

Forcing can be limited by time. This maximum force time is given in seconds. If the force time is exceeded, it can be determined whether the CPU goes to STOP or the force value is no longer valid and the standard operation is proceeded. Exceeding the force time always has effects on the application program.

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

It is possible to automatically printout the documentation of a project using RSLogixGuard. 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

The documentation is a constituent of a function acceptance of a site subject to approval by an approving board (e.g. TÜV). The function acceptance only refers to the application function, not however, to the safety-related automation modules, GuardPLC 1200 and GuardPLC 2000, that are type tested.

In the case of sites subject to acceptance, it is recommended that you involve the approval authorities in projecting as early as possible.

Configuration of COM

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 with RSLogixGuard in the COM area. This data exchange can read as well as in written.

When configuring the 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 effected via a non-safe protocol (NSP).

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

ATTENTION

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

Conditions for Use

Chapter Introduction

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

For information about:	See page:
climatic conditions	7-2
mechanical conditions	7-2
EMC conditions	7-3
power supply conditions	7-3

The PES GuardPLC 1200 and GuardPLC 2000 were developed to meet the following standards for the EMC, climate, and environment regulations.

IEC61131-2, (1992 .. 2000)	Programmable Controllers Part 2: Equipment requirements and tests
IEC61000-6-2 (1999)	EMC Part 6-2: generic standards - immunity for industrial environments
EN 50081-2 (1993)	EMC Part 2: generic emission standard - industrial environments

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 .. 60°C (Test limits -10 .. 70°C)
	Storage Temperature -40 .. 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 .. 500°Hz/2g
	Shock test operating 30g
	Shock test non operating 50g
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, 11ms, EUT operating, 2 x cycles per axis)

EMC Conditions

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

EN 61131-2 Paragraph 6.3.6.2	Test: Noise immunity test / EMC
6.3.6.2.1	ESD test (4 kV contact / 8 kV air discharge)
6.3.6.2.2	RFI test (10 V/m) 26MHz to 1GHz, 80%AM
6.3.6.2.3	Bursts test (2KV Power supply / 1KV Signallines)
6.3.6.2.4	Damped oscillatory wave immunity test (1 kV)
IEC / EN 61000-6-2	Radio frequency common mode, 10 V, 150 kHz - 80 MHz, AM
IEC / EN 61000-6-2	900 MHz-Pulses
IEC / EN 61000-6-2	Surge 2 kV, 1 kV, 0,5 kV
EN 50081-2 EN 50011	Emission test 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	Test: Verification of DC Power Supply Characteristics
6.3.7.1.1	Voltage range test dc, -20%, +25% (19,2 V to 30,0 V)
6.3.7.2.1	Momentary interruption immunity test dc, PS2: 10 ms
6.3.7.4.1	Reversal of dc powers supply polarity test Application note in the system manual
6.3.7.5.1	Back-up duration withstand test (Test B: 1000 h) Lithium-battery is used for back-up

Notes:

A

application program
- technical safety 6-1

C

central module
- functional description 2-2

checklist
- creation of an application program 5-8
- safety-related inputs 3-8
- safety-related outputs 4-6

climatic conditions 7-2
conditions for use 7-1
- climatic conditions 7-2
- EMC conditions 7-3
- mechanical conditions 7-2
- power supply conditions 7-3

counter module 3-6
- block diagram 3-7
- general 3-6
- reaction in fault condition 3-7
- test routines 3-6

E

EMC conditions 7-3
error diagnostics 2-4

F

forcing 5-6
functions of the operating system 5-2

I

input modules
- analog inputs 3-4
  - block diagram 3-5
  - general information 3-4
  - reaction in case of fault 3-5
  - test routines 3-5
- counter module 3-6
  - block diagram 3-7
  - general 3-6
  - reaction in fault condition 3-7
  - test routines 3-6
- overview 3-1
- safety-related digital inputs 3-2
  - block diagram 3-3
  - general 3-2
  - reaction to error 3-3
  - test routines 3-3
- safety-related general information 3-2

M

manipulation
- protection against 5-7

mechanical conditions 7-2

O

operation mode of the operating system 5-2
output channels
- analog output module, safety-related 4-4
  - block diagram 4-5
  - general 4-4
  - reaction to error 4-5
  - test routines 4-4
- digital outputs 4-2
  - block diagram 4-3
  - reaction in case of error 4-3
  - test routines 4-2
- general safety information 4-2
- overview 4-1

P

parameterizing the automation module 5-5
power supply 2-1
power supply conditions 7-3

S

safety policy
- general safety information 1-1
- restrictions 1-3
- safety times 1-2
  - fault tolerance time 1-2
  - multiple error occurrence time 1-2
  - reaction time 1-2
  - safety time 1-2
  - watchdog time of the CPU 1-3

selt-test routines 2-3
- CPU-test 2-3
- fixed memory sectors 2-3
- I/O bus 2-4
- RAM-test 2-3
- reactions to detected errors in CPU 2-4

test memory sectors 2-3
watchdog-test 2-3
software
GuardPLC 1200/2000 safety-related systems 5-1

T

technical safety
application program 6-1
general procedure 6-1
safety-related applications frames 6-1
application program functions 6-4
programming basis 6-2
program documentation for safety-related applications 6-9
variable declaration and PLT name input 6-3
technical safety for programming 5-3
check the created application program 5-3
creation of a backup program 5-4
program identification 5-5
safety concept of RSLogixGuard 5-3
technical safety for the operating system 5-2

Allen-Bradley
Publication Problem Report

If you find a problem with our documentation, please complete and return this form.

Pub. Title/Type GuardPLC 1200 and GuardPLC 2000 Safety Reference Manual

Cat. No. 1754 and 1755 Pub. No. 1755-RM001A-EN-P Pub. Date September 2001 Part No. 957564-33

Please complete the sections below. Where applicable, rank the feature (1=needs improvement, 2=satisfactory, and 3=outstanding).

Overall Usefulness	1 2 3	How can we make this publication more useful for you?
Completeness (all necessary information is provided)	1 2 3	Can we add more information to help you? ☐ procedure/step ☐ illustration ☐ feature ☐ example ☐ guideline ☐ other ☐ explanation ☐ definition
Technical Accuracy (all provided information is correct)	1 2 3	Can we be more accurate? ☐ text ☐ illustration
Clarity (all provided information is easy to understand)	1 2 3	How can we make things clearer?
Other Comments		You can add additional comments on the back of this form.

Your Name _____ Location/Phone _____

Your Title/Function _____ Would you like us to contact you regarding your comments?

___No, there is no need to contact me

___Yes, please call me

___Yes, please email me at _____

___Yes, please contact me via _____

Return this form to: Allen-Bradley Marketing Communications, 1 Allen-Bradley Dr., Mayfield Hts., OH 44124-9705

Phone: 440-646-3176 Fax: 440-646-3525 Email: RADocumentComments@ra.rockwell.com

PLEASE FASTEN HERE (DO NOT STAPLE)

Other Comments

PLEASE FOLD HERE

PLEASE REMOVE

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL
FIRST-CLASS MAIL PERMIT NO. 18235 CLEVELAND OH

POSTAGE WILL BE PAID BY THE ADDRESSEE

Rockwell Automation

1 ALLEN-BRADLEY DR
MAYFIELD HEIGHTS OH 44124-9705

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-RM001A-EN-P - September 2001

PN 957564-33