

2005-07-26



TÜV Rheinland Group

Automation, Software and Information Technology

**Report of the type approval of
GuardPLC Safety Scanner
of Rockwell Automation, Inc.**

**Report-No.: 968/EZ 200.00/05
Date: 2005-07-26**

**Report of the type approval of
GuardPLC Safety Scanner
of Rockwell Automation, Inc.**

Report-No.:	968/EZ 200.00/05
Date:	2005-07-26
Pages:	14
Test object:	GuardPLC Safety Scanner 1753 - DNSI
Customer:	Rockwell Automation Inc. Automation Control & Information Group 1 Allen-Bradley Drive USA-Mayfield Heights, OH 44124 United States of America
Manufacturer:	see customer
Order-No./Date:	PAR 2375 dated 2003-04-04
Test Institute:	TÜV Industrie Service GmbH Automation, Software and Information Technology (ASI) Am Grauen Stein D-51105 Köln (Poll)
Department:	Automation, Software and Information Technology (ASI)
TÜV-Offer-No./Date:	968/76/03 dated 2003-04-14
TÜV-Order-No./Date:	9066569 dated 2003-04-09 (former no. 968/386096)
Inspectors:	Dipl.-Ing. Matthias Haynl Dipl.-Ing. Andreas Hesse
Test location:	see Test Institute
Test duration:	April 2003 to July 2005

The test results are exclusively related to the test samples.

This report must not be copied **in an abridged version** without the written permission of the Test Institute.

Contents	Page
1. Scope	4
2. Standards forming the basis for the requirements	4
3. Test object	5
3.1 History and test objects	5
3.2 Product and test documents	5
3.3 Test samples	6
3.4 Description and result of the inspection of the safety structure	6
4. Protocol and results type approval	6
4.1 Overview	6
4.2 Requirements in accordance with IEC 61508	7
4.2.1 General requirements	7
4.2.2 Assessment of the management of functional safety	7
4.2.3 Documentation over the entire life cycle	7
4.2.4 Assessment of the measures for controlling failures in hardware	7
4.2.5 Assessment of the measures for failure avoidance in hardware/software	8
4.2.6 Determination of PFD/PFH/SFF	8
4.3 Requirements in accordance with EN 954-1	8
4.4 Electrical safety	8
4.5 Environmental tests	9
4.6 Accompanying documents	9
4.7 Application specific considerations	9
4.7.1 Requirements according to EN 50156-1/ 2004	9
4.7.2 Requirements according to ANSI/RIA R15.06 - 1999	9
4.7.3 Requirements according to ANSI B11.19 - 2003	10
4.7.4 Requirements according to NFPA 79 - 2002	11
4.7.5 Requirements according to EN 54-2/ 2004	11
4.7.6 Use of the GuardPLC Safety Scanner in machinery applications	13
4.8 Programming and configuration	13
4.8.1 Programming and configuration tools	13
4.9 Communication requirements	13
4.10 DeviceNet Safety Conformance	13
5. Conclusion	14

1. **Scope**

In the following report the results of the type approval of the GuardPLC Safety Scanner for safety application are presented.

This test report is to provide traceable evidence, that the test object complies with the functional and safety-related requirements of the product specification, satisfies the requirements of the relevant regulations, and thus can be used as component for emergency shutdown and fire and gas applications.

Besides several application standards, the GuardPLC Safety Scanner has been subject to an assessment in accordance with EN 954-1 category 4 and IEC 61508 Safety Integrity Level 3 (SIL 3).

This test report contains the essential safety engineering aspects, that were assessed during the concept and test phases, and identifies the various test steps, that were performed to provide evidence, that the test object complies with the safety-relevant requirements of the product specification and the relevant regulations.

It is described, which tests were performed, who performed them and which results were obtained.

2. **Standards forming the basis for the requirements**

Functional Safety

- [S1] IEC 61508, parts 1 - 7:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems
- [S2] EN 954-1:1996 Safety of machinery, Safety related parts of control systems, Part 1: General principles of design

Application specific

- [S3] EN 50156-1:2004 Electrical Equipment for Furnaces
- [S4] IEC 61511:2004 Safety Instrumented Systems for the process industry sector
- [S5] NFPA 79:2002 Electrical Standard for Industrial Machinery
- [S6] EN 54-2:1997 Fire Detection and Fire Alarm Systems Control and indicating equipment
- [S7] EN 60204-1:1997 Safety of machinery; Electrical equipment of machines
- [S8] ANSI B11.19:2003 American National Standard for Machine Tools - Performance Criteria for Safeguarding
- [S9] ANSI/RIA R15.06:1999 American National Standard for Industrial Robots and Robot Systems - Safety Requirements

Electrical safety and resistance against environmental conditions

[S10] IEC 61131-2:2003 Programmable Controllers

[S11] EN 61000-6-2:2001 Generic Standards; Immunity for industrial environments

[S12] EN 61000-6-4:2001 Generic standards; Emission standard for industrial environments

3. Test object

3.1 History and test objects

The GuardPLC Safety Scanner is a microcontroller based system to connect a DeviceNET Network to a GuardPLC-Controller.

The parts of the system are listed in Appendix 1.

3.2 Product and test documents

The complete documentation was provided by the customer. The complete set of documentation is available to the inspectors and will not be listed here. They are stored in the Test Institute. Only the documents which were discrete given to the inspectors are mentioned here.

The documentation was provided by Rockwell Automation as an electronic file-image. The following list includes selected documents which were used for this inspection.

- [D1] DeviceNet Safety Scanner SRS Document
Rev.3.4 dated 2005-04-25
- [D2] Validation_Verification_plan (part of SRS)
Rev.3.4 dated 2005-04-25
- [D3] DeviceNet Safety Scanner Project Plan
Rev.1.1 dated 2003-09-16
- [D4] Safety Reference Manual (hereafter: SRM)
Doc: 1753-RM002A-EN-P dated 2005-04-25
- [D5] Installation Manual
Doc: 1753-IN009A-EN-P dated 2005-04-25
- [D6] User Manual
Doc: 1753-UM002A-EN-P dated 2005-04-25
- [D7] DeviceNet Safety Scanner FMEA Report
Rev.1.1 dated 2003-08-29
- [D8] Fault Insertion of Scanner
Rev. 1.1 dated 2005-05-28

Furthermore the source-codes of the GuardPLC Safety Scanner are available within the inspectors documentation.

Test reports of the Test Institute:

- [T1] Test report about the Safety Network
Report No. 968/EL 335.00/05 dated 2005-07-30
- [T2] Test report on the type approval of 1791DS Series DeviceNet Safety I/O Modules
1791DS-IB12, 1791DS-IB8XOB8 and 1791DS-IB4XOW4
Report No. 968/EZ 190.01/05 dated 2005-08-02

3.3 Test samples

The necessary tests of the GuardPLC Safety Scanner system were carried out at the Rockwell facilities in Cleveland.

Additionally Rockwell provided a test system to the Test Institute. It is used to partly verify the tests carried out at Rockwell and to incorporate additional tests.

3.4 Description and result of the inspection of the safety structure

The GuardPLC Safety Scanner consists of two similar controller boards (main and peer-controller) which build up a redundant system. The main controller will handle safety and non safety messages, communication to (external) devices (e.g. I/O-components) and communication to the peer controller. The peer controller itself will only handle safety messages and report its result to the main controller for comparison and completing safety messages.

For a complete safety system DeviceNet safety I/O-components (see [T2]) and a GuardPLC-Controller can be used to build up safety loops.

For safety messages the CIP-Safety protocol will be used which has been tested separately. The test results are documented in [T1].

Sending out safety messages:

A safety message that will be sent out by the GuardPLC Safety Scanner is composed of the data generated by the main controller and the data of the peer controller. The main controller generates the true data, the peer controller generates the false data. Any receiver can check the safety information.

Receiving safety messages:

All the safety messages will be received by the main controller and will be directly transferred to the peer controller. The main controller has no affect to these data.

4. Protocol and results type approval

4.1 Overview

The measuring and test equipment, which has been used by the TÜV Rheinland Group in the tests described in the following, is subject to regular inspection and calibration. Only devices with valid calibration have been used. The devices used in the various tests are recorded in the inspector's documentation.

All considerations concerning tolerance of the measurements, so far applicable, are stated in the inspector's documentation, too.

In cases where tests have been executed in an external test lab or in the test lab of the manufacturer and where the results of these tests have been used within the here documented approval, this has occurred after a positive assessment of the external test lab and the achieved test results in detail according to the Quality Management procedure QMA 3.310.05.

The testing has been carried out to show that the GuardPLC Safety Scanner complies with the requirements for Safety Integrity Level 3 (SIL 3) as per IEC 61508 and the general requirements for fail-safe controls in accordance with EN 954-1 for safety category 4.

The devices used in the various tests are recorded in the inspectors' documentation.

4.2 Requirements in accordance with IEC 61508

4.2.1 General requirements

For the GuardPLC Safety Scanner Safety Integrity Level 3 (SIL 3) is sought.

Due to the technology in the device and the intended application it is considered as a type B subsystem in accordance with IEC 61508-2. It operates beside as a component for a protective device in a "Low Demand Mode of Operation" also in "High Demand Mode of Operation" applications.

Along with the probabilistic requirements IEC 61508 the following points have to be judged:

- documentation
- measures for the avoidance of failures (QM) as well as
- measures for controlling failures in each case over the entire life cycle of the product

4.2.2 Assessment of the management of functional safety

Rockwell maintains a project related functional safety management system according to IEC 61508. The functional safety management system has been audited by the Test Institute on project level.

The functional safety management fulfils the requirements of IEC 61508.

4.2.3 Documentation over the entire life cycle

The extensive documentation provided by Rockwell is listed in chapter 3.2. They have been prepared to suit the individual phases of the life cycle and are available to the Test Institute.

The test results and assessment of the documentation on the GuardPLC Safety Scanner demonstrated, that they satisfy to the requirements in accordance with IEC 61508.

4.2.4 Assessment of the measures for controlling failures in hardware

To achieve the level of failure detection required in accordance with SIL 3 the safe failure fraction measures for controlling failures must be taken for hardware failures given in a defined failure model. The used failure model corresponds to the requirements in table A.1 in annex A of IEC 61508-2. The effectiveness of the taken measures has been analysed by the manufacturer. They have been documented and verified by module and system tests.

In addition the measures for the detection of failures and controlling failures were analysed in joint reviews with the Test Institute. The effectiveness was partly verified based on selected practical tests, which are documented in [D8].

Any detected fault will result in the configured fault reaction which by default is the deactivation of the output values or loss of communication to I/O-components. The I/O-components are responsible to reach the defined safe state.

The safety structure, diagnostics and the detection of failures comply to the requirements of [S1].

4.2.5 Assessment of the measures for failure avoidance in hardware/software

The assessment of failure avoidance was part of the functional safety management (see chapter 4.2.2 and 4.2.3). The applied measures were partly verified by the Test Institute during several meetings on project level.

4.2.6 Determination of PFD/PFH/SFF

The target values of PFD/PFH and SFF are specified for SIL 3.

The PFD, PFH and SFF data were derived from and documented in the FMEA [D7].

The FMEA-results were supplemented with failure injection tests to verify diagnostic functions and the failure reaction of the system.

Diagnostic elements and electronic devices used in non safety related functions were not included in failure rate calculations.

The basic failure rates are based on values taken from SN 29500 as well as manufacturer data for some components.

Failure modes assumed during the FMEA and the calculation method for PFD/PFH values were agreed with the Test Institute.

The PFD-values are documented in the SRM [D4].

The FMEA analysis and the PFD/PFH/SFF calculation were finished with a positive result.

4.3 Requirements in accordance with EN 954-1

All single failures will be detected by appropriate diagnostic measures. The effectiveness of these diagnostics were already assessed during [S1] assessment. A failure accumulation need not to be considered due to the fact that each failure leads into the configured fault reaction of the system.

The safety structure, diagnostics and the detection of failures comply to the requirements in [S2].

4.4 Electrical safety

A power supply that will be used for a GuardPLC Safety Scanner in safety application needs to fulfil the requirements according to EN50178 or similar standards. Power supplies must fulfil the requirements for Protective Extra-low-Voltage (PELV) and Safety Extra Low Voltage (SELV).

4.5 Environmental tests

The environmental tests temperature and climate are performed at Rockwell's internal test laboratories. This laboratory is accredited to ISO17025.

The results are accepted by the Test Institute with some restrictions:

The present climate test results are not fully compliant with [S6] chapter 15.14. These tests might be carried out additionally if required in an application.

4.6 Accompanying documents

The SRM [D4], the Installation Manual [D5] and the User Manual [D6] for the GuardPLC Safety Scanner has been reviewed. It contains the necessary information for the correct installation and safe operation.

4.7 Application specific considerations

4.7.1 Requirements according to EN 50156-1/ 2004

The EN 50156-1 lists beside the application specific requirements also system specific requirements which are in accordance with IEC 61508 and EN 954-1. Therefore, the system specific requirements are fulfilled.

The user still needs to comply with all other requirements from the standard including requirements that have an effect on the operation of the safety system. The end-user should refer to the SRM [D4].

4.7.2 Requirements according to ANSI/RIA R15.06 - 1999

This American National Standard applies beside the manufacture, remanufacture, rebuild, installation, maintenance, testing, start-up and training also to the safeguarding requirements for industrial robots and robot systems.

It defines methods of safeguarding to enhance the safety of personnel associated with the use of robots and robot systems.

In the following clauses, relevant general and specific requirements are defined. These requirements are applied to the GuardPLC Safety Scanner and it is described, if they are applicable and how they are fulfilled:

Clause	Requirements	Result
4.5.3	Single channel with monitoring safety circuits shall include the requirements for single channel, shall be safety rated, and shall be checked (preferably automatically) at suitable intervals.	The safety scanner is partly built as single channel. The single channel parts are covered by the safety protocol (block channel).
4.5.4	Control reliable safety circuitry shall be designed, constructed and applied such that any single component failure shall not prevent the stopping action of the robot.	This requirement is fulfilled. See previous chapters.
5.3	General requirements for safeguarding devices that signal a stop: <ul style="list-style-type: none"> - Accompanying documents, - Indicators, that the device is operating - Not adversely affected by environmental conditions - Maximum response time must not be affected by object sensitivity and environmental changes - Provide means for secure attachment - Provide means to restrict unauthorized adjustments or settings 	Fulfilled, see the previous chapters of this report.

Clause	Requirements	Result
6.4	<p>Software and firmware-based controllers used in place of hardware based components with safety-related devices shall:</p> <ul style="list-style-type: none"> a) be designed such that any single safety related component or firmware failure shall: <ul style="list-style-type: none"> 1) lead to the shutdown of the system in a safe state and 2) prevent subsequent automatic operation until the component failure has been corrected b) supply the same degree of safety achieved by using hardwired/ hardware components per 4.5.4. For example, this degree of safety may be achieved by using microprocessor redundancy, microprocessor diversity, and self-checking c) be certified by a National Recognized Testing Laboratory (NRTL) to an approved standard applicable for safety devices. 	<p>Fulfilled, see the previous chapters of this report.</p> <p>This Test Institute is not listed as a National Recognized Testing Laboratory (NRTL). Despite this matter of fact, the test objects are in accordance with approved standards for safety devices.</p>
10.1	Requirements for safety circuit performance	Fulfilled
11.3	<p>Requirements for safeguarding devices that signal a stop</p> <ul style="list-style-type: none"> - Interface to the robot - Installation so that over- and under reaching of the safeguard is not possible - Start/Restart required from outside the safeguarded space - Provision of control over adjustments or settings being made by others than authorized personnel - Indication on if the device is functioning 	<p>Not quite applicable to the GuardPLC Safety Scanner; most of the requirements concern the installation. The Manual provides sufficient information to perform a correct installation. An indication, that the device is functioning, is available.</p>

4.7.3 Requirements according to ANSI B11.19 - 2003

This standard contains requirements for the design, construction, care and operation of safeguards used at the other ANSI B11 machine tools. The selection and the application of the safeguarding system is provided in the appropriate B11 safety standard for the particular machine tool.

The B11.19 standards provides requirements for different types of safeguards (fixed and movable guards, presence sensing devices, two hand operating control devices, probe protection devices and others).

In the following tables the relevant general and specific requirements are defined. These requirements are applied to the GuardPLC Safety Scanner and it is described, if they are applicable and how they are fulfilled:

Clause	Requirements	Result
6.1	<p>Performance of the safety related function(s):</p> <p>When a component, module, device or system failure occurs, such that it or a subsequent failure of another component, module, device or system would lead to the inability of the safety-related function(s) to respond to a normal stop command or an immediate stop command, the safety-related function shall:</p> <ul style="list-style-type: none"> • prevent initiation of hazardous machine motion (or situation) until the failure is corrected or until the control system is manually reset; or 	<p>Fulfilled, see the previous chapters of this report</p>

Clause	Requirements	Result
6.1 cont.	<ul style="list-style-type: none"> initiate an immediate stop command and prevent re-initiation of hazardous machine motion (or situation) until the failure is corrected or until the control system is manually reset; or prevent re-initiation of hazardous machine motion (or situation) at the next normal stop command until the failure is corrected or until the control system is manually reset. 	

4.7.4 Requirements according to NFPA 79 - 2002

This standard from the National Fire Protection Association contains the electrical requirements for industrial machinery.

In the following tables the relevant general and specific requirements are defined. These requirements are applied to the GuardPLC Safety Scanner and it is described, if they are applicable and how they are fulfilled:

Clause	Requirements	Result
9.4.3	Control Systems Incorporating Software and Firmware Based Controllers.	
	<p>Control systems incorporating software and firmware based controllers performing safety-related functions shall conform to all of the following:</p> <p>(1) In the event of any single failure perform as follows:</p> <ul style="list-style-type: none"> (a) Lead to the shutdown of the system in a safe state (b) Prevent subsequent operation until the component failure has been corrected (c) Prevent unintended startup of equipment upon correction of the failure <p>(2) Provide protection equivalent to that of control systems incorporating hardwired / hardware components.</p> <p>(3) Be designed in conformance with an approved standard that provides requirements for such systems</p>	Fulfilled, see the previous chapters of this report
11.2.3	<p>Electrical Noise and Transient Suppression.</p> <p>Transient suppression, isolation, or other appropriate means shall be provided where the electronic equipment generates electrical noise or transients, which can affect the operation of equipment.</p>	Fulfilled
11.2.4	<p>Output Protection.</p> <p>Outputs controlled by programmable electronic systems shall be protected from overload and short-circuit conditions.</p>	Must be fulfilled by the used I/O-components

The user still needs to comply with all other requirements from the standard including requirements that have an effect on the operation of the safety system. The end-user should refer to the SRM [D4].

4.7.5 Requirements according to EN 54-2/ 2004

The GuardPLC Safety Scanner meets the additional requirements imposed by the application standard EN 54-2 [S6].

The table below shows only those product requirements which have not yet performed by the manufacturer. Requirements which can be reached by planning or projecting measures, e.g. power supply, installation etc are not considered. Only the following test has not been carried out and is still pending.

Clause	Requirement	Results
13.5	The storage of programs and data	
13.5.1	All executable code and data necessary to comply with this European Standard shall be held in memory which is capable of continuous, unmaintained, reliable operation for a period of at least 10 years.	Fulfilled. The contents of Flash memory is secured by a CRC32-signature. It will be checked during runtime.
13.5.2	The program shall be held in non-volatile memory, which can only be written to at access level 4. Each memory device shall be identifiable such that its contents can be uniquely cross-referenced to the software documentation.	The program is stored in the Flash memory. Access level can be defined in the configuration software or must be defined on a higher level. This is a application requirement and therefore not relevant here.
13.5.3	For site specific data, the following requirements shall apply:	
	a) alteration shall not be possible at access levels 1 or 2;	Access level can be defined in the configuration software or must be defined on a higher level.
	b) the alteration of site specific data shall not affect the structure of the program;	Fulfilled.
	c) if stored in volatile memory, the site-specific data shall be protected against power loss by a back-up energy source which can only be separated from the memory at access level 4, and which is capable of maintaining the memory contents for at least 2 weeks;	Fulfilled. Configuration data is stored within FLASH memory.
	d) if stored in read-write memory, there shall be a mechanism which normally prevents the memory being written to during program execution, such that its contents may be protected in the event of a failure in program execution.	Fulfilled.
13.6	The monitoring of memory contents	
	The contents of the memories containing the program and the site specific data shall be automatically checked at intervals not exceeding 1 hour. The checking device shall signal a system fault if a corruption of the memory contents is detected.	Fulfilled. Complete tests for the RAM and Flash are within 8 hours. But due to the fact that the GuardPLC Safety Scanner is a redundant system with permanent crosschecking of data and watchdog between main and peer controller this requirement is fulfilled.
15.3	Environmental tests	
15.4	Cold (operational)	Fulfilled as part of EN61131-2.
15.5	Damp heat, steady state (operational)	Fulfilled as part of EN61131-2
15.6	Impact (operational)	Fulfilled as part of EN61131-2
15.7	Vibration, sinusoidal (operational)	Fulfilled as part of EN61131-2
15.8	Electrostatic discharges (operational)	Fulfilled as part of EN61131-2
15.9	Radiated electromagnetic interference (operational)	Fulfilled as part of EN61131-2

Clause	Requirement	Results
15.10	Voltage transients - fast transient bursts (operational)	Fulfilled as part of EN61131-2
15.11	Voltage transients - slow high energy transients (operational)	Fulfilled as part of EN61131-2
15.12	Mains voltage dips and interruptions (operational)	Fulfilled as part of EN61131-2
15.13	Supply voltage variation (operational)	Fulfilled as part of EN61131-2
15.14	Damp heat, steady state (endurance)	Not performed
15.15	Vibration, sinusoidal (endurance)	Fulfilled as part of EN61131-2

The user still needs to comply with all other requirements from the standard including requirements that have an effect on the operation of the safety system. The end-user should refer to the SRM [D4] .

4.7.6 Use of the GuardPLC Safety Scanner in machinery applications

If the GuardPLC Safety Scanner is used for safety of machinery users should refer to the SRM [D4] and the Installation Manual [D5].

Users must implement application specific requirements such as e.g. emergency stop or warm restart in the application logic.

4.8 Programming and configuration

4.8.1 Programming and configuration tools

For the GuardPLC Safety Scanner mainly 2 parts of software will be used:

- RSGuard+ programming software for configuring the connection between a GuardPLC-controller and the GuardPLC Safety Scanner
- RSNetworks Network configuration software

Both parts of software are not safety relevant. The special requirements for the PC-based Software when using it for safety systems are clearly described in the SRM [D4] and must be observed.

4.9 Communication requirements

The GuardPLC Safety Scanner uses the CIP-safety protocol, to communicate to safety devices. Due to the quality of the CIP-safety protocol any safety device on the network can detect data corruption caused on the transmission network.

It is also allowed to handle standard communication in safety systems. For further details users shall refer to the SRM [D4].

4.10 DeviceNet Safety Conformance

The communication with other DeviceNet components is performed using the generic driver from DeviceNet Safety. A conformance test procedure in accordance with the DeviceNet Safety specification is installed within the ODVA (Open DeviceNet Vendor Association).

The test specification and the results are available to the Test Institute.

The test has been performed at ODVA-Laboratory.

5. Conclusion

During the correctly performed test no infringement of the functional and safety-related requirements in the applied standards could be found. Observance must be given to the installation conditions and application notes defined in the user documentation.

The additional application specific requirements as listed in the related chapters above must be taken into consideration.

It was demonstrated, that the GuardPLC Safety Scanner complies with the requirements of IEC 61508 for SIL 3 and EN 954-1 Cat. 4. The safety related parameters are specified within the SRM [D4]. The resistance against the specified environment conditions are mostly given, exceptions are mentioned in chapter 4.5 and 4.7.

Therefore the GuardPLC Safety Scanner can be used in applications up to and including SIL 3/Cat. 4.

Cologne, 2005-07-26
TIS/ASI/Kst. 968 he-nie

The inspectors

A handwritten signature in black ink that reads 'Mathias Haynl'.

Dipl.-Ing. Mathias Haynl

A handwritten signature in blue ink that reads 'Andreas Hesse'.

Dipl.-Ing. Andreas Hesse

SIL3 - certified - Components:

Catalog Number	Description / System	Series:	Firmware Revision
1753-DNSI	DeviceNet Safety Scanner	A	1.2
1791DS-IB12	DeviceNet Safety Input Module	B	1.1
1791DS-IB8XOB8	DeviceNet Safety Input/Solid-State Output Module	B	1.1
1791DS-IB4XOW4	DeviceNet Safety Input/Relay	B	1.1