TÜVRheinland®
Precisely Right.

Automation, Software and Information Technology

Report about the type approval of the Safety Related Programmable Electronic System Control Logix of Rockwell Automation

Report-No.: 968/EZ 135.05/09
Date: 2009-09-16

**Report about the type approval of the
Safety Related Programmable
Electronic System Control Logix
of Rockwell Automation**

Report-No.:	968/EZ 135.05/09
Date	2009-09-16
Pages:	21
Test object:	Safety Related Programmable Electronic System Control Logix
Customer/Manufacturer:	Rockwell Automation Inc. Automation Control & Information Group 1 Allen-Bradley Drive Mayfield Heights, OH 44124-6118 United States of America
Order-No.:	76-519-000-T4328 / PAR 4328 (email) dated 2005-12-09
Test Institute:	TÜV Rheinland Industrie Service GmbH Automation, Software and Information Technology (ASI) Am Grauen Stein 51105 Köln Germany
TÜV-Offer-No./Date:	968/177/05 dated 2005-09-07
TÜV-Order-No./Date:	9411235 dated 2005-12-12
Inspectors:	Dipl.-Ing. Andreas Hesse
Test Location:	see Test Institute
Test Duration:	Januar 2008 - July 2009

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**

Contents **Page**

1. Scope

The report is basically a summary of the results of the type approvals with regards to the application. This report must also be considered for design, installation and setting into operation of all safety related applications.

Object of the inspection is the Safety Related Programmable Electronic System ControlLogix from Rockwell Automation Inc. Automation Control & Information Group, Mayfield Heights, United States of America.

This type approval is an enhancement of previous certifications documented in the test reports listed in chapter 3.4. It has to be clarified, that the parts of the ControlLogix-System described in chapter 3.2 fulfil the requirements for safety equipment up to and including SIL 2 in accordance to the standard IEC 61508. Modules have to be integrated into the safety concept described in the safety manual /1/.

The basic assumption is, that the process or plant under the control of the PLC has a safe state. The safe state is low-signal, that means the de-energized state.

Therefore the system can be used as an emergency shutdown system (ESD).

It is also possible to use the “Hold-Last-State” where required in an application.

2. Basic standards for the type approval

[1] IEC 61508:2000, parts 1 - 7
Functional safety of electrical/electronic/programmable electronic safety related systems

[2] IEC 61131-2:2007
Programmable Controllers - Equipment requirements and tests

[3] IEC 60068
2-1 Environmental testing - Tests A: Cold
2-2 Environmental testing - Tests B: Dry heat
2-6 Environmental testing - Test Fc: Vibration (sinusoidal)
2-14 Environmental testing - Test N: Change of temperature
2-27 Environmental testing - Test Ea and guidance: Shock
2-30 Environmental testing - Test Db and guidance: Damp heat, cyclic (12 + 12-hour cycle)

[4] IEC 61000-6-2:2005
Electromagnetic compatibility (EMC)
Generic standards - Immunity for industrial environments

[5] IEC 61000-6-4:2006
Electromagnetic compatibility (EMC)
Emission standard for industrial environments

[6] EN 50178:1997
Electronic Equipment for use in power installations

[7] EN 50156-1:2004
Electrical Equipment for Furnaces
Part 1: Requirements for Application Design and Installation

[8] EN 54-2:1997 / A1:2006
Fire detection and Alarm Systems
Part 2: Control and Indicating Equipment

[9] EN 954-1:1996
Safety of machinery, Safety related parts of control systems
Part 1: General principles of design

[10] IEC 61511-1:2004
Safety Instrumented Systems for the process industry sector

[11] NFPA 72:2007
National Fire Alarm Code Handbook

[12] NFPA 85:2007
Boiler and Combustion Systems Hazards Code

Table 1: Standards

3. Test objects and manufacturer documentation

3.1 Documentation

No.	Document name	Document no.	Date
/1/	Safety Reference Manual (hereafter SRM)	1756-RM001F-EN-P	June 2009
/2/	SRS and V&V-Plan	Document-CD: CLX-SIL 2 SRS Validation_Verification_Final.doc Document-CD: SIL 2 Follow-Up Documentation June 2002	20. March 2002

Table 2: Documentation used for the qualification

Module specific documentation was provided by Rockwell. Those documents were also used during the qualification.

All necessary documentation used for the type approval was provided by Rockwell Automation and is archived in electronical format by the Test Institute.

3.2 Test object

The ControlLogix-System is a field approved Standard PLC-System.

For safety relevant applications the specifically approved hardware components listed in Annex A may be used.

The complete documentation of the Rockwell components are controlled by the change control procedure as defined in Product Change Procedure /2/.

In this qualification the following items were added:

- ControlLogix Analog modules with HART
- X-Scale based communication modules
- ControlLogix modules with extended temperature range

3.3 Classification of the test object

The ControlLogix-System has to fulfil the following safety parameters:

Average probability of failure to perform its designed safety function on demand:

$PFD_{avg} \geq 10^{-3}$ to $< 10^{-2}$

In HFT = 0 configuration: SFF -> 90 % - < 99 %

In HFT = 1 (1oo2) configuration: SFF -> 60 % - < 90 %.

3.4 Previous test reports

[T1] Type approval of Safety Related Programmable Electronic System Control Logix Report-No.: 968/EZ 135.00/02; Date: 2002-09-30

[T2] Type approval of Safety Related Programmable Electronic System Control Logix Report-No.: 968/EZ 135.01/04; Date: 2004-03-02

[T3] Type approval of Safety Related Programmable Electronic System Control Logix Report-No.: 968/EZ 135.02/04; Date: 2004-03-31

[T4] Type approval of Safety Related Programmable Electronic System Control Logix Report-No.: 968/EZ 135.03/05; Date: 2005-01-31

[T5] Type approval of Safety Related Programmable Electronic System Control Logix Report-No.: 968/EZ 135.04/06; Date: 2006-11-27

4. Test and test results

4.1 General

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.

4.2 General remarks

The ControlLogix-PLC (CLX-PLC) is a system which has been developed before the standard IEC 61508 was published.

The difference between the requirements of the standard and the design of the ControlLogix PLC (e. g. diagnostic) is described in

- the Safety Requirements Specification (SRS)
- the Verification and Validation Plan (V&V)

In addition the manufacturer documented all measures for failure avoiding regarding the tables included in the IEC 61508, Part 2 and 3.

A database of Rockwell Automation gives also information about the number of modules in the field and the number of returned modules from customers. These data were used to calculate the Probability of Failure on Demand.

4.3 Concept review

The safety concept of the ControlLogix-System is based on 3 parts as documented in the SRM /1/:

1. Implemented (diagnostic) features of modules, see the following sections

2. Predefined safety system structure and functionality, detailed in the following list:

   - Within the safety task it is not allowed to implement non-safety functions
   - A safety loop only contains safety related parts
   - A safety application consists of only one controller
   - Any module has to broadcast its data within a specified time (RPI)
   - Any output modules provide the Data Echo feature
   - The use of Digital- and Analog - I/O-Modules must be done in the way described in the SRM /1/, e. g. one safety relevant input has to be wired to two (1oo2) input-modules, or standard output modules will be read back by a corresponding input module.
   - The main rack, which is the location of the processor, can be extended by remote racks. The communication between the racks has to be done by using ControlNet (direct connections) and only for safety communication.
   - The communication to non safety parts has to be done via an independent ControlNet-Node from the main rack. Non safety parts are only allowed to have Read-Only-Access to the safety part of the application.
   - For communication with the Human-Machine-Interface (HMI), Ethernet can be used.
   - For application language recommendations refer to chapter 10 of the Safety Manual /1/.
   - For a commissioned safety application the RUN-Mode is the only allowed operation mode, see Safety Reference Manual /1/.

3. An independent switch, e.g. external relay, is required to switch off the output field voltage supply for de-energized state as safe state applications.

As a result of the review of the safety concept for a CLX-PLC SIL 2 application, additional structural considerations are to be taken into account (see SRM /1/).

4.4 Functional safety management

The listed measures below are basic measures referenced by the manufacturer and items of the concept review for the ControlLogix-System.

These measures are described in the SRS, V&V-Plan /2/.

In addition the manufacturer documented all measures for failure avoiding regarding the tables included in the IEC 61508, Part 2 and 3.

- All ControlLogix hard- and software modules are designed, developed and produced in accordance with the quality management system of Rockwell Automation. The development of the CLX-PLC follows a company specific lifecycle procedure.

- The quality management system is certified and registered according to the standard ISO 9001 under the no. 98-HOU-AQ-9379 by DNV Certification INC.

- Configuration and modification during and after production of the ControlLogix modules and PLC related documentation are considered in the procedures of the change control as defined in the quality management system of Rockwell Automation.

- The functional-specification, the design-specification and the data sheet of the test objects were reviewed by the Test Institute.

Selected measures to control systematic failures:

- The compliance of the ControlLogix modules with the environmental condition as specified in the data sheets and user's manuals were reviewed by the Test Institute. The tests were carried out at the Allen Bradley Lab E²L in Mayfield Heigths, Ohio, USA, which is accredited to IEC 17025.

- A temporary monitoring of the application program is achieved by controlling of the program cycle time in combination with the setting of a watch-dog timer.

The measures are sufficient for the required SIL level.

4.5 Inspection of the measures to avoid and control systematic failures

The effectiveness of the selected measures to avoid and control systematic failures were theoretically inspected during the concept review and partially tested during the main inspection by the following procedures and methods.

- A test system including all documentation was made available to TÜV for carrying out the system tests.

- The validity of the safety concept as documented in the SRM /1/ was inspected by analyzing the specified measures and by comparing the expected reactions with the reactions resulting from the system.

The measures are sufficient for the required SIL level.

4.6 Hardware inspection

Based on the results of the concept review the following steps were carried out during the main inspection:

- Review of manufacturing documents versus the requirements of the standard [1]
- Review of the diagnostic features to control failures of the hardware
- Review and test of the measures to control systematic failures
- Review of the internal and external communication measures between the I/O-modules
- Calculate the Probability of Failure on Demand (PFD) based on the field data provided by Rockwell Automation

As a result of the main inspection the SRM /1/, was issued. The SRM contains all necessary information applying the PLC as a SIL 2 safety system.

The effectiveness of the selected measures to control failures, see the following chapters, were tested partially during the main inspection by the following procedure/method:

The behaviour of the system was checked and inspected by using a ControlLogix-test system. This test system was configured and assembled by Rockwell Automation according to the test requirements of TÜV. The test system executes a test program, which enables it to test the basic features of the ControlLogix operation. The test program is based on the ladder logic language used for ControlLogix-Systems. The test system including all documentation was made available to TÜV for carrying out the system tests.

4.7 Description of the hardware

The ControlLogix-system used in safety relevant applications consists of one CPU, power supplies, digital I/O-Modules, analog I/O-Modules, communication modules and multislot chassis.

Each module (except Racks, Power-Supplies and Chassis adapter)

- includes a communication interface to the backplane in a chassis
- is microprocessor controlled and self-contained in standardized enclosures
- will use the same backplane protocol to communicate with each other. A loss of communication of a certain module will lead to a safe state of the module

The main rack can be extended via the communication bridge modules, using ControlNet, by remote racks.

Each chassis will be supplied by at least one of the certified power modules. Additionally it is possible to connect a second redundant power supply to a rack to increase availability.

The hardware is described in detail in the handbooks/user's manuals published by the manufacturer.

4.7.1 Theoretical hardware inspections

4.7.1.1 Inspection of the documentation

The documentation as listed in chapter 3.1 has been checked for its completeness, consistency and comprehensibility.

Furthermore the documentation has been checked for conformity with the realized boards. The following types of documents were checked as needed:

- functional specification
- design description
- user manual
- schematics
- layouts
- component location diagrams
- part list
- test procedures and results
- quality assurance procedure for the documentation

The documentation of the hardware components is complete, consistent and comprehensible.

The conformity with the realized components is given.

All the documentation is under quality assurance controlled by the manufacturer.

4.7.1.2 Inspection of the design

The modules used for the ControlLogix-System were designed and developed in accordance with the Rockwell Automation QM-System. The whole procedure is defined in the TQCS-Policy and the related documents.

The design of the modules were inspected with respect to the modules qualified in a previous certification. Main point of these inspections were, e. g. electrical safety, consistency with the manufacturing documents, electronic devices, manufacturing quality, etc.

The results of the inspection of the hardware structure and diagnostic measures for each type of module are summarized in the following chapters.

The results of the design inspection were particularly considered within the safety concept with a final description of the safety structure in the SRM /1/.

4.7.1.3 FMEA for new modules

For new modules (1756-EN2T, 1756-CN2, 1756-CN2R and 1756-RM) a FMEA has been carried out by the Test Institute.

The FMEA showed that the requirements for SIL 2 are fulfilled.

The PFD figures are documented in the safety manual.

4.7.1.4 Inspection of the electrical safety

The electrical safety was partially checked according to the requirements of IEC 61131 [2].

The inspection was done on theoretical base for safe isolation areas, clearance and creepage distances and components.

High voltage tests were carried out by the manufacturer.

All tests were passed with a positive result.

4.7.1.5 Review of environmental and EMC tests

The environmental and noise tests have been carried out in the Environmental Test-Laboratory E²L of Allen Bradley.

The Test Laboratory was positively assessed by the Test Institute.

The following tests were carried out:

- Climatic tests
- Vibration/shock-tests
- EMC-tests

The results of the environmental and noise tests are documented by the reports of Rockwell Automation. Parts of the reports and documentations have been handed over to TÜV.

As a result all modules meet the requirements of IEC 61131 [2].

The test results are accepted by the Test Institute.

4.7.1.6 Extended temperature modules

The following modules are used with an extended temperature range:

1756-CN2RXT
1756-EN2TXT/B
1756-EN2T series B butlower temp
1756-L63XT/B
1756-PBXT/B
1756-A7LXT/B
1756-A5XT

There are only few hardware changes to the already certified modules. Additional testing to check functionaliy under higher temperature has been carried out by the manufacturer.

The results are accepted by the Test Institute.

4.7.1.7 Results of the hardware inspection

The hardware inspection was carried out as described before and successfully conducted according to the standards in chapter 2.

For module specific details please refer to chapter 4.10.

The detailed results of the inspection are deposited at the Test Institute.

4.7.2 Inspection of the reliability data and PFD calculations

The manufacturer provides the PFD data for all suitable configuration options needed for the calculation of the PFD of a complete system. The PFD data are based on reliability data which are based on module returns. The procedure for the data collection is part of the QM-System of the manufacturer.

The validation of the reliability data was done by comparing the listed data of the shipped modules with the recorded data of the modules coming back from the field.

The common cause failure as defined in IEC 61508 has been demonstrated by the manufacturer to be 2 % or less for the redundant parts of the system.

The manufacturer has calculated the Probability of Failure on Demand (PFD) based on a proof period of one year and a Mean Time to Repair (MTTR) of 10 hours.
The method of calculation has been approved by the Test Institute.

The manufacturer has provided sufficient data to allow PFD calculations based on end user requirements and desired configurations. The PFD-values are documented in the SRM /1/.

4.8 Inspection of the software

The software approval was divided in a review of the manufacturer’s software documents (listed in chapter 3.1) and in an analysis of all safety related software functions.

The review of the documentation and the software analysis was carried out partially in co-operation with the manufacturer and partly as soon as a desk checking with static analysis of the source code. During the software approval the avoidance and control of failures were considered regarding the standards listed in chapter 2.

The software inspection was divided into the following parts:

- inspection of the documentation
- inspection of program and data structures
- inspection of the measures to avoid failures
- analysis of the measures to control failures in hardware
- review of the software tests

4.8.1 Description of the software

The software, which is running on a ControlLogix, is divided in the following parts:

- Firmware of the controller, which handles communication to the modules, performs diagnostic and runs the user application
- Firmware of the I/O-Modules, which carries out I/O-handling and communication to the controller
- Firmware of the communication modules for safety related communication between controller and I/O-modules
- Firmware of the communication modules for non safety related communication (e.g. DH+/RIO), which carries out non safety related communication

The Firmware is mainly developed with the Programming Language “C” and special parts are realized in Assembler.

During the inspection, PC-based toolset were used to

- create, compile and download PLC application programs
- configure the ControlNET-network
- Flash firmware into a module

4.8.2 Software requirements

The standard IEC 61508 [1] defines in part 3 the requirements for software to be used in systems, which provide functional safety.

Within the scope of the IEC 61508 the V-model (IEC 61508, part 3, figure 5) is used to describe the lifecycle model of software development.

4.8.3 Theoretical software inspection

4.8.3.1 Inspection of the documentation

The examination of the documents listed in chapter 3 took place in an inspection with regard to the standards listed in chapter 2.

Beside the specifications and users manuals for the software the source code of all Firmware was available for the analysis.

For parts of the software also internal review documents and test reports were available. These review documents were also considered.

Open points were described and the manufacturer carried out the related changes in the documents. The examination on the documents was finished with a positive result.

4.8.3.2 Inspection of measures to avoid failures

Similar measures as described in the “V”-Model were established in the design and development process.

Additionally Rockwell uses commercially available tools “Clearquest” and “Clearcase” for code management and defect tracking.

The software product specific and higher manufacture measures to avoid failures are sufficient and fulfil the requirements of the related standards.

4.8.3.3 Analysis of the measures to control failures

The implementation of modules specific diagnostic (e.g. watchdog) and overall system measures (RPI) was carried out on a theoretical and a practical base.

For further details see chapter 4.10 which describes module specific items.

4.8.3.4 Review of software tests

The quality test plans and test results were partly checked.

All necessary information was provided by Rockwell in electronical format.

4.8.4 Results of the software inspection

The safety relevant parts of the software are in agreement with the tasks, which they shall perform.

The effectiveness of the measures to avoid systematic software failures are in accordance with SIL 2 according to [1].

The inspections of the software were finished with positive results.

For further module specific details see chapter 4.10.

4.9 Redundancy

The redundancy system provides a hot swap between 2 controllers that are running quasi parallel. 1 of the 2 controllers is called primary and is responsible for running the application and feeds its partner (secondary) controller with actual application data.

In case that the primary controller detects an internal failure of any module in the chassis, the redundancy system is able to initiate a switchover to the secondary (which has the same application program as its partner controller).

The redundancy system is for availability only. It is required to test both controllers during a proof test. It is sufficient to test half of the safety functions with 1 controller, then initiate a switchover, test the rest of the safety functions with second controller and initiate a switchover again.

4.10 Module specific inspection

The details of module configuration are described in the safety manual (e.g. use of single or redundant configuration).

4.10.1 Controller

4.10.1.1 General remarks

The controller is the central part of the safety system. It is responsible for running the application program.

The controller handles:

- failures caused by modules
- reactions on application specific events
- internal diagnostics

The controller fulfils the requirements of Safe Failure Fraction SFF > 90 %. The results of the controller diagnostic features are documented in the controller specific documentation that is archived in the Test Institute.

4.10.1.2 L55-Controller

The L55-Controller can be used in safety relevant applications with the versions listed in Annex A.

V15.57 is recommended for new implementations using the Controller Redundancy system (see chapter 4.9 for information on redundancy).

V16.21 is recommended for the use in new implementations that do not use Controller Redundancy.

The inspection of the L55-controller was finished with positive results.

For further detail on the use of the controller see the SRM /1/ and the user documentation.

4.10.1.3 L6xB-Controller

The L6xB-Controller can be used in safety relevant applications with the versions listed in Annex A.

V16.54 is recommended for new implementations using the Controller Redundancy system (see chapter 4.9 for information on redundancy).

V16.21 is recommended for the use in new implementations that do not use Controller Redundancy.

It is required to use series B standard power supplies when using the L6xB-Controller in SIL 2-systems or use redundant power supplies.

The inspection of the L6xB-controller was finished with positive results.

For further detail on the use of the L6xB-controller see the SRM /1/ and the user documentation.

4.10.2 Digital I/O-components

All digital I/O-Modules listed in paragraph 3 - except of the Diagnostic Output Module OB16D and OA8D - must be used in a 1oo2 configuration.

This structural measure is necessary to fulfil the SFF/HFT requirement for a SIL 2 application.

For further details on the Digital I/O-components see the SRM /1/ and module related user documentation.

4.10.3 Diagnostic output module OB16D, OA8D

The diagnostic output modules have additional diagnostic measures.

These measures are:

- Pulse-test
- Short Circuit Protection/Thermal Shutdown
- Output Verification
- No Load-Detection

Also the Output Data Echo feature is used to acknowledge output commands for verification done by the controller.

With these features it is possible to use only one diagnostic output module to switch safety actuators. To make sure that it can be switched off in the case of a fault, an additional relay has to be wired to switch off the field side power of the modules outputs.

For further details on the diagnostic output module see the SRM /1/ and module related user documentation.

4.10.4 Analog I/O-components

The analog I/O-components can be used in safety systems in the versions listed in Annex A.

All analog I/O-modules listed in paragraph 3 must be used in a 1oo2 configuration.

It is recommended to use the latest qualified firmware-version in safety systems.

Previously qualified firmware versions may be used in existing safety systems.

For further details on Analog I/O-components see the SRM /1/ and module related user documentation.

4.10.5 ControlNet-modules

In this inspection the new software and hardware revision of the ControlNet modules have been added. Additionally ControlNET modules based on a new hardware-platform have been added.

Under respect of the requirements described in the SRM, /1/, the CNB-module can be used in a one single channel configuration.

It is recommended to use the latest qualified firmware-version in safety systems.

Previously qualified firmware and hardware versions may be used in existing safety systems.

For further details on ControlNet-modules see the SRM /1/ and module related user documentation.

Users are allowed to use ControlNet repeater as listed in Annex A in safety systems up to and including SIL 2.

4.10.6 Ethernet-modules

4.10.6.1 1756-EN2T

A EtherNET module based on a new hardware-platform has been added.

The new EtherNET module 1756-EN2T (new Hardwareplatform) is basically the same module as the new ControlNet module. The basic difference is the physical layer.

Therefore, the new Ethernet module may also be used for safety related applications. The same conditions as used for the ControlNET modules have to be observed.

4.10.6.2 1756-ENBT

In this inspection the new software revision of the EtherNet modules 1756-ENBT has been added.

These Ethernet-modules will be used for non-safety communication (eg. to a Human and Machine Interface (HMI)). Parameter changes via the HMI are only permitted if the restrictions described in the SRM /1/ are followed.

This Ethernet module was inspected to be interference free within the safety related applications.

It is recommended to use the latest qualified firmware-version in safety systems.

Previously qualified firmware versions may be used in existing safety systems.

For further details on Ethernet -modules see the SRM /1/ and module related user documentation.

4.10.7 DH+/RIO-modules

DH+/RIO-modules will be used for non-safety communication interface. This interface must have solely **Read-Only** access to the safety system as it has been defined for the Ethernet module in the previous qualification.

The DH+/RIO-module was inspected to be interference free within the safety related applications.

For further details on DH+/RIO-modules see the SRM /1/ and module related user documentation.

4.10.8 Redundancy module

The redundancy module is used to communicate between two controller chassis that provide controller redundancy.

The redundancy modules have been inspected in view of their safety relevance. The modules are not involved in safety loops. Safety relevant data that were sent between the two controllers are packed in a CRC and have time expectation.

The redundancy module maintains cyclic heartbeat signals to modules located in its chassis. Any switchover is divided in number of phases that must be completed by both redundancy modules in a redundancy system.

The redundancy module fulfils the requirements for SIL 2 according to IEC61508 [1].

For further details on the use of the redundancy module see the SRM /1/ and module related documentation.

4.10.9 Sync Link module

The Sync Link module provides time synchronization between multiple racks. This is required e.g. for sequence of event inputs.

The Sync Link module does not have a safety function. It has been inspected to be interference free within the safety related applications.

For further details on the use of the Sync Link Module see the SRM /1/ and module related documentation.

4.10.10 Power supplies

The series B power with tighter tolerances for overvoltage and undervoltage monitoring are recommended to be used in Safety systems.

Previously qualified Revision A Power Supplies may be used in existing safety systems.

The measures for overvoltage and undervoltage are sufficient for SIL 2 according to IEC 61508 [1].

Redundant power supplies can be used to increase availability of the system.

For further details on the use of the Power supplies see the SRM /1/ and module related documentation.

4.10.11 Chassis

The chassis provide the slots for the modules. The chassis does not provide any diagnostics. Failures on the Backplane will result in a communication error which is recognized by the participating modules.

During the Qualification only the 1756-A10 was used in tests at TÜV. All other Chassis were qualified with respect to the similar construction.

For further details on Chassis see the SRM /1/ and Chassis related documentation.

4.10.12 Chassis adapter

Either the Power supply chassis adapter PSCA or PSCA-2 can be used in SIL 2-applications.

4.11 Function tests

The functions of the I/O blocks as specified in the data sheets were partially tested under different conditions of the following parameters:

- input signal
- supply voltages
- output loadings

Additionally the Test Institute carried out the following tests:

- exceptional failure injection tests
- test of the communication between racks
- test of the communication between safety and non-safety area
- test of the redundancy system (switchover, fault handling)

The functions of the modules were tested within the test system also used for the system and software tests.

All tests were passed with a positive result.

4.12 Application program

The test of the application program was mainly done in the system integration tests.

The requirements of application programming is listed in the SRM /1/ chapter 8.9.

4.13 PC-based software

The RS-Logix 5000 software was used to compile and download user programs. Most of the functions of RS-Logix 5000 are local to the PC to help during the development of an application program unless performing online modifications.

During all practical software tests the RS-Logix 5000 software was used.

Integrated in the RS-Logix is the possibility, to read back programs from PLCs in the field to the PC. With this feature it is possible to compare programs in a PLC with a given program.

The RS-Networx-Software for ControlNet was used to establish communication between the Racks via the Controlnet-Modules.

The PC-based toolset is an engineering environment. It was not part of the certification.

Users shall use PC-based Software only during commissioning of a project or when performing online edits as described in the Safety Reference Manual /1/.

4.14 System tests

During the type approval the following items have been verified by practical tests:

- Digital voting
- Analog voting
- Digital discrepancy checking
- Analog discrepancy checking
- Correct fault bit generation
- Correct shut down application program execution
- Loss of module communication
- Software/hardware watchdogs
- RPI-mechanism (heartbeat between the modules and the controller)
- Use of the redundancy system

The test results are deposited at the Test Institute.

The system tests of the ControlLogix-System were finished with a positive results.

4.15 Use of ControlLogix-System in EN 54-2 applications

The CLX-system fulfils the requirements of EN 54-2 in view of the environmental conditions.

For full compliance the following conditions must be observed:

- Additional testing may be necessary.
- The conditions of the SRM /1/ must be taken into consideration.
- Application specific requirements have to be taken into consideration during integration.

4.16 Use of ControlLogix-System in EN 50156 applications

For the use of the ControlLogix-System in safety relevant applications up to the SIL 2 of IEC 61508 [1], module selection, installation, configuration, programming and operation have to be observed. These conditions are included in SRM /1/.

The EN 50156-1 lists additional requirements for the application of protective systems.

The requirements are similar to the IEC 61508-requirements.

- The conditions of the SRM /1/ must be taken into consideration.

Application specific requirements have to be taken into consideration during integration.

4.17 Use of ControlLogix-System in machinery applications

The subset of ControlLogix modules listed in Annex A can be used to build up safety systems requiring category 1 according to EN 954-1.

- The conditions of the SRM /1/ must be taken into consideration.

4.18 Requirements according to IEC 61511:2004

The ContolLogix-System fulfils the requirements for safety integrity level 2 in accordance with IEC 61508. Hence, the system can be used within the scope of IEC 61511.

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 safety reference manual /1/.

4.19 Requirements according to NFPA 72:2007

The ContolLogix-System meets the additional requirements imposed by the application standards NFPA 72 [11].

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 safety reference manual /1/.

4.20 Requirements according to NFPA 85:2007

The ContolLogix-System meets the applicable requirements for logic solvers as defined by the application standard NFPA 85 [12]. The test results were positive and are documented in the inspectors documentation.

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 safety manual /1/.

5. Summary of results

The type approval was performed according to the test plan as documented in the chapters before, which is based on the relevant standards listed in chapter 2.

The modules of the ControlLogix-System that are certified for SIL 2 are listed in chapter 3.2.

The ControlLogix-System must be used only within the specified environmental conditions. These conditions are documented in the user manuals. The compliance of the existing conditions for an application with the specified conditions for ControlLogix-System must be checked within the commissionary.

All tests were passed. The detailed results and documents are archived in the Test Institute.

During the type approval no deviations were observed, which are in conflict with the requirements of SIL 2 of IEC 61508 [1].

Therefore the ControlLogix-System is appropriate for the use in safety relevant applications up to and including SIL 2 of IEC 61508 [1]. For all applications the de-energized state must be the safe-state (ESD). Additionally the hold last value state can be used where required in an application. The conditions of the Safety Reference Manual /1/ must be considered.

Cologne, 2009-09-16
TIS/ASI/Kst. 968 he-nie

Report released after review:
Date: 2009-09-16

The inspector

Dipl.-Ing. Andreas Hesse

Dipl.-Ing. Heinz Gall