

2005-01-31



**TÜV Rheinland Group**

**Automation, Software and Information Technology**

**Type approval report of Safety Related Programmable  
Electronic System Control Logix  
of Rockwell Automation**

**Report-No.: 968/EZ 135.03/05  
Date: 2005-01-31**

**Type approval of Safety Related Programmable  
Electronic System Control Logix  
of Rockwell Automation**

**Report-No.:** 968/EZ 135.03/05

**Date** 2005-01-31

**Pages:** 21

**Test object:** Safety Related Programmable Electronic System Control Logix

**Manufacturer:** Rockwell Automation Inc.

**Customer:** Rockwell Automation Inc.  
Automation Control & Information Group  
1 Allen-Bradley Drive  
USA-Mayfield Heights, OH 44124-6118  
United States of America

**Order-No./Date:** 76-519-000-T2221 dated 2004-09-02

**Test Institute:** TÜV Industrie Service GmbH  
Automation, Software and Information Technology (ASI)  
Am Grauen Stein  
D-51105 Köln (Poll)

**TÜV-Offer-No./Date:** 968/114/04 dated 2004-05-19

**TÜV-Order-No./Date:** 9108971 dated 2004-08-17

**Inspectors:** Dipl.-Ing. Andreas Hesse

**Test Location:** see Test Institute

**Test Duration:** June 2004 - January 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.

<b>Contents</b>	<b>Page</b>
1. Scope .....	4
2. Basic standards for the type approval .....	4
3. Test objects and manufacturer documentation .....	5
3.1 Documentation .....	5
3.2 Test object .....	5
3.3 Classification of the test object .....	8
4. Test and test results .....	8
4.1.1 Concept review .....	8
4.2 Functional safety management .....	9
4.3 Inspection of the measures to avoid and control systematic failures .....	10
4.4 Hardware inspection .....	10
4.4.1 Description of the hardware .....	11
4.4.2 Theoretical hardware inspections .....	11
4.4.2.1 Inspection of the documentation .....	11
4.4.2.2 Inspection of the design .....	12
4.4.2.3 Inspection of the electrical safety .....	12
4.4.2.4 Review of environmental and noise tests .....	12
4.4.2.5 Results of the hardware inspection .....	12
4.4.3 Inspection of the reliability data and PFD calculations .....	13
4.5 Inspection of the software .....	13
4.5.1 Description of the software .....	13
4.5.2 Software requirements .....	14
4.5.3 Theoretical software inspection .....	14
4.5.3.1 Inspection of the documentation .....	14
4.5.3.2 Inspection of measures to avoid failures .....	14
4.5.3.3 Analysis of the measure to control failures .....	14
4.5.3.4 Review of software tests .....	14
4.5.4 Results of the software inspection .....	15
4.6 Redundancy .....	15
4.7 Module specific inspection .....	15
4.7.1 Controller .....	15
4.7.1.1 General remarks .....	15
4.7.1.2 L55-Controller .....	15
4.7.1.3 L6xB-Controller .....	16
4.7.2 Digital I/O-components .....	16
4.7.3 Diagnostic output module OB16D, OA8D .....	16
4.7.4 Analog I/O-components .....	17
4.7.5 ControlNet-modules .....	17
4.7.6 Ethernet-modules .....	17
4.7.7 DH+/RIO-modules .....	17
4.7.8 Redundancy module .....	18
4.7.9 Sync Link module .....	18
4.7.10 Power supplies .....	18
4.7.11 Chassis .....	18
4.7.12 Chassis adapter .....	19
4.8 Function tests .....	19
4.9 Application program .....	19
4.10 PC-based software .....	19
4.11 System tests .....	20
4.12 Conditions for applications .....	20
5. Summary of results .....	21

## 1. Scope

The report is basically a summary of the results of the type approval 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 USA-Mayfield Heights.

This type approval is an enhancement of a previous certification documented in report-no. 968/EZ 135.02/04. It has to clarify, that the parts of the ControlLogix-System are described in chapter 3.2 fulfill 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] DIN EN 61131-2  
Programmable Controllers  
Part 2/ 2004, 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 61000-6-2/1999  
Electromagnetic compatibility (EMC)  
Generic standards - Immunity for industrial environments
- [5] IEC 61000-6-4/1997  
Electromagnetic compatibility (EMC)  
Emission standard for industrial environments
- [6] DIN EN 50178/1998  
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  
Fire detection and Alarm Systems -  
Part 2: Control and Indicating Equipment

**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-RM001D-EN-P	January 2005
/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 electronically form by the Test Institute.

**3.2 Test object**

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

For safety relevant applications the following specifically approved hardware components may be used.

Catalog Number	Description / System	Series:	Firmware Revision
1756-A4. A7. A10. A13 & A17	ControlLogix Chassis	B	NA
1756-PA75	AC Power supply	A	NA
1756-PB75	DC Power supply	A	NA
1756-PA75R	AC Redundant power supply	A	NA
1756-PB75R	DC Redundant power supply	A	NA
1756-PA75	AC Power supply	B	NA

Catalog Number	Description / System	Series:	Firmware Revision
1756-PB75	DC Power supply	B	NA
1756-PC75	DC Power supply	B	NA
1756-PH75	DC Power supply	B	NA
1756-PSCA <sup>1</sup>	Redundant Power Supply Chassis Adapter Module	A	NA
1756-PSCA <sup>2</sup>	Redundant Power Supply Chassis Adapter Module	A	NA
1756-L55M13	Logix processor w/ 1.5Mb memory	A	10.27 <sup>1</sup> 11.32 <sup>1</sup> 13.31 <sup>2</sup> 13.53.30 <sup>3</sup>
1756-L55M16	ControlLogix 7.5Mb Controller	A	10.27 <sup>1</sup> 11.32 <sup>1</sup> 13.31 <sup>2</sup> 13.53.30 <sup>3</sup>
1756-L61	ControlLogix 2 Mb Controller	B	13.40
1756-L62	ControlLogix 4 Mb Controller	B	13.40
1756-L63	ControlLogix 8 Mb Controller	B	13.40
1756-IA16I	AC Isolated Input Module	A	2.2
1756-IA8D	AC Diagnostic Input Module	A	2.6
1756-IB16D	DC Diagnostic Input Module	A	2.6
1756-IB16I	DC Isolated Input Module	A	2.2
1756-IB32	DC Input - 32pt	B	3.5
1756-IB16ISOE	24/48VDC Sequence of Events Input	A	1.5
1756-IH16ISOE	125VDC Sequence of Events Input	A	1.5
1756-OA16I	AC Isolated Output Module	A	2.1
1756-OA8D	AC Diagnostic Input Module	A	2.4
1756-OB16D	DC Diagnostic Output Module	A	2.3
1756-OB16I	DC Isolated Output Module	A	2.1
1756-OB32	DC Output - 32pt	A	2.4
1756-OB8EI	DC Isolated Output Module	A	2.3
1756-OX8I	Isolated Relay Output Module	A	2.1
1756-OW16I	N.O. Isolated Relay Output - 16Pt	A	2.1

Catalog Number	Description / System	Series:	Firmware Revision
1756-IF8	Analog Input Module	A	1.5
1756-IF16	Single-ended analog input module - 16pt	A	1.5
1756-IF6I	Isolated analog input module - 6pt	A	1.9 <sup>1</sup> 1.12 <sup>2</sup>
1756-IF6CIS	Isolated sourcing analog input module - 6pt	A	1.12
1756-IR6I	RTD Input module	A	1.9 <sup>1</sup> 1.12 <sup>2</sup>
1756-IT6I	Thermocouple Input module	A	1.9 <sup>1</sup> 1.12 <sup>2</sup>
1756-IT6I2	Enhanced Thermocouple Input Module	A	1.11 <sup>1</sup> 1.12 <sup>2</sup>
1756-OF8	Analog Output Module	A	1.5
1756-OF6VI	Isolated analog output module-Voltage - 6pt	A	1.9 <sup>1</sup> 1.12 <sup>2</sup>
1756-OF6CI	Isolated analog output module-Current - 6pt	A	1.9 <sup>1</sup> 1.12 <sup>2</sup>
1756-CNB	ControlNet Communication Module	D	5.27 <sup>1</sup> 5.38.40 <sup>1</sup> 5.45 <sup>2</sup>
1756-CNBR	Redundant ControlNet Communication Module	D	5.27 <sup>1</sup> 5.38.40 <sup>1</sup> 5.45 <sup>2,3</sup>
1756-ENBT	EtherNet Communication Module	A	1.33 <sup>1</sup> 3.4 <sup>2,3</sup>
1756-DHRIO	DH+/RIO bridge / scanner module	C	5.03
1757-SRM	Redundancy Module	A	3.37.5 <sup>3</sup>
1756-Sync	Synclink Module	A	2.18

<sup>1</sup> These versions can be used as a replacement in existing systems

<sup>2</sup> These versions are recommended for new implementation

<sup>3</sup> This version is required for the redundancy System

**Table 2: Identification of the test object**

Rockwell Automation has a quality assurance system according to ISO 9001 which is registered under the number 98-HOU-AQ-9379 by DNV Certification, Inc.

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

### 3.3 Classification of the test object

The ControlLogix-System has the following safety parameters:

Average probability of failure to perform its design function on demand:

$$\text{PFD} \geq 10^{-3} \text{ to } < 10^{-2}$$

The HFT is 0 which results in a safe failure fraction of

$$\text{SFF} \rightarrow 90 \% - < 99 \%$$

Modules which are used in a redundant configuration will have a HFT = 1 which results in a safe failure fraction of

$$\text{SFF} \rightarrow 60 \% - < 90 \%$$

## 4. Test and test results

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 discussed and 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 figures.

### 4.1.1 Concept review

The safety concept of the ControlLogix-System is based on 4 parts as documented in the SRM /1/:

1. Implemented (diagnostic) features of some modules, see the following sections
2. Predefined safety system structure and functionality, detailed in the following list:
  - Within the safety application 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 (redundant) input-modules, or standard output modules will be read back by an 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.
  - It is recommended to use ladder logic for safety application programming. Only a limited instruction set as defined in the SRM /1/ may be used.
  - For a commissioned safety application the RUN-Mode is the only allowed operation mode. Programming terminals have to be disconnected.
3. Predefined ladder logic structures for comparing redundant module I/O information.
  4. 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, there are additional structural considerations to be taken into account (see SRM /1/).

#### 4.2 Functional safety management

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

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

In addition the manufacturer discussed and 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 E<sup>2</sup>L in Mayfield Heights, 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.

#### **4.3 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 partial 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.

#### **4.4 Hardware inspection**

Based on the result 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 partial during the main inspection by the following procedures/methods:

- The behavior 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.

#### **4.4.1 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.

#### **4.4.2 Theoretical hardware inspections**

##### **4.4.2.1 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.

#### **4.4.2.2 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/.

#### **4.4.2.3 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 creeping distances and components.

High voltage tests were carried out by the manufacturer.

All tests were passed with a positive result.

#### **4.4.2.4 Review of environmental and noise tests**

The environmental and noise tests has been carried out in the Environmental Test-Laboratory E<sup>2</sup>L of Allen Bradley.

The Test laboratory is accredited for EMC tests by TÜV Product Services and for EMC and the other tests by Bureau Veritas.

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 were accepted by the Test Institute.

#### **4.4.2.5 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 4.7.

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

#### **4.4.3 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 modules 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/.

#### **4.5 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
- analyze of the measures to control failures in hardware
- review of the software tests

##### **4.5.1 Description of the software**

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

- Firmware of the controller which will handle communication to the modules, perform diagnostic and run the user application
- Firmware of the I/O-Modules which carries out I/O-handling and communication to the controller
- Firmware of the CNB-Module which carries out the remote I/O communication
- Firmware of the DH+/RIO - Module which carries out non safety related communication
- Firmware of the Ethernet - Module 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

#### **4.5.2 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.

#### **4.5.3 Theoretical software inspection**

##### **4.5.3.1 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.

##### **4.5.3.2 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 fulfill the requirements of the related standards.

##### **4.5.3.3 Analysis of the measure 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 4.7 which describes module specific items.

##### **4.5.3.4 Review of software tests**

The quality test plans and test results were partly checked.

All necessary information was provided by Rockwell on a CD.

#### **4.5.4 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 4.7.

#### **4.6 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 feed 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.

#### **4.7 Module specific inspection**

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

##### **4.7.1 Controller**

###### **4.7.1.1 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 fulfills 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.

###### **4.7.1.2 L55-Controller**

The L55-Controller can be used in safety relevant applications with either V10.27, V11.32, V13.31 or V13.53.30.

V13.53.30 is required for the Controller Redundancy system (see chapter 4.6 for information on redundancy).

V13.31 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.

#### **4.7.1.3 L6xB-Controller**

The L6xB-Controller can be used in safety relevant applications with V13.40.

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

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.

#### **4.7.2 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 redundant configuration.

This structural measure is necessary to fulfill 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.

#### **4.7.3 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.

#### 4.7.4 Analog I/O-components

In this inspection the firmware version 1.12 has been added. The V 1.12 is recommended to be used in a safety system. For the replacement in existing systems V 1.9 or V1.11 (only IT6I) may be used.

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

#### 4.7.5 ControlNet-modules

During the qualification CNBR-modules (redundant communication channels, only for availability) and CNB-module were used.

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 (5.45) in safety systems.

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

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

#### 4.7.6 Ethernet-modules

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

The 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.

#### 4.7.7 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.

#### **4.7.8 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 fulfills the requirements for SIL2 according to IEC61508 [1].

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

#### **4.7.9 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.

#### **4.7.10 Power supplies**

The new series B power supplies will have tighter tolerances for overvoltage and undervoltage monitoring.

It is recommended to use the Revision B Power Supplies 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.

#### **4.7.11 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.

#### **4.7.12 Chassis adapter**

The Power supply chassis adapter PSCA and PSCA-2 are different in the gender of the chassis adapter connector.

These changes do not have influence on the functional safety, so the PSCA-2 can be used in SIL2-applications.

#### **4.8 Function tests**

The functions of the I/O blocks as specified in the data sheets were partial 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.

#### **4.9 Application program**

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

For a SIL 2-Application program users shall only use a limited instruction set (see SRM /1/ chapter 8).

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

#### **4.10 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.

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 (see SRM /1/).

Engineering PCs have to be disconnected during SIL 2 operation.

#### **4.11 System tests**

During the type approval a application program, `Toyoto_SIL2_Slot4_Rev_1.ACD`, was developed by Rockwell Automation according to the requirements of TÜV. This program is described in a test report. The program is designed to use and to check the features of a typical ControlLogix application:

- Digital voting
- Analog voting
- Digital discrepancy checking
- Analog discrepancy checking
- Correct fault bit generation
- Correct shut down application program execution
- Loss of module communication

Additionally the Test Institute has written PLC-programs to test special functions of the system:

- software/hardware watchdogs
- RPI-mechanism (heartbeat between the modules and the controller)
- use of the redundancy system

All test programs and test results are deposited at the Test Institute.

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

#### **4.12 Conditions for 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 CLX-system fulfills 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.

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

The requirements are similar to the IEC 61508-requirements.

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

## 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 SIL2 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 according 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 state can be used where required in an application. The conditions of the Safety Reference Manual /1/ must be considered.

Cologne, 2005-01-31  
ASI/Kst. 968-hu-he-nie

The inspector

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

Dipl.-Ing. Andreas Hesse