

2005-01-31



TÜV Rheinland Group

Automation, Software and Information Technology

**Type approval report of
Safety Related Programmable I/O-System FLEX-I/O
(in combination with ControlLogix-System)
of Rockwell Automation**

**Report-No.: 968/EZ 188.01/05
Date: 2005-01-31**

**Type approval report of
Safety Related Programmable I/O-System FLEX-I/O
(in combination with ControlLogix-System)
of Rockwell Automation**

Report-No.: 968/EZ 188.01/05

Date 2005-01-31

Pages: 12

Test object: FLEX-I/O System as extension of the ControlLogix-System

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

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: F649934 dated 2003-09-10

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

TÜV-Offer-No./Date: 968/95/03 dated 2003-05-13

TÜV-Order-No./Date: 968/386205 dated 2003-09-11

Inspectors: Dipl.-Ing. Andreas Hesse

Test Location: see Test Institute

Test Duration: September 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.

Contents	Page
1. Scope	4
2. Standards	4
3. Test object	5
3.1 Description of the test object	5
3.2 Documentation of the test object	6
3.3 Classification of the test object	6
4. Test and test results	7
4.1 Safety requirements	7
4.1.1 General safety requirements - FSM	7
4.1.2 Avoidance of systematic failures	7
4.1.3 Control of failures	7
4.2 Review and results of the inspection	7
4.2.1 Review of the documentation	7
4.2.2 Review of the safety architecture	7
4.3 General hardware requirements	8
4.3.1 Environmental requirements	8
4.3.2 Reliability data and PFD calculations	9
4.3.3 Power supply	9
4.4 Review of the different modules	9
4.4.1 Terminal base	9
4.4.2 I/O-components	10
4.4.3 ControlNet-Adapter	10
4.5 Configuration and Programming of the FELX-I/O	10
4.6 System tests	10
4.7 Conditions for applications	11
5. Summary	11

1. Scope

Object of the inspection is the FLEX-I/O-System from Rockwell Automation Inc. Automation Control & Information Group USA-Mayfield Heights.

The parts of the system are described in chapter 3.

Purpose of the approval is to clarify, under which conditions FLEX-I/O-System together with the ControlLogix-System can be used for applications with the requirements for safety equipment up to and including SIL 2 in accordance to the standard IEC 61508.

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

2. Standards

- [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

3. Test object

3.1 Description of the test object

The FLEX-I/O-System is a modular I/O-System with the option to connect to different networks (e.g. ControlNet).

The FLEX-I/O-System consists of different I/O-components, communication modules and Terminal Bases.

For safety relevant applications it is intended to use the FLEX-I/O-System together with the ControlLogix-System and a ControlNet-Connection.

The following modules are selected to be used in safety relevant applications:

No.	Rockwell Automation Catalog Number	Description	Revision	
			HW	FW
Terminal Base				
1	1794-TB3	Terminal Base, 3 wire, screw	A	N/A
2	1794-TB3G	Terminal Base, Gnd, 3 wire, screw	A	N/A
3	1794-TB3GS	Terminal Base, Gnd, 3 wire, spring	A	N/A
4	1794-TB3S	Terminal Base, 3 wire, spring	A	N/A
5	1794-TB3T	Terminal Base, Temp, 3 wire, screw	A	N/A
6	1794-TB3TS	Terminal Base, Temp, 3 wire, spring	A	N/A
7	1794-TBNF	Terminal Base, Fused Nema	A	N/A
Communication Modules				
8	1794-ACN15	ControlNet Adapter	C	4.3
9	1794-ACNR15	Redundant ControlNet Adapter 1.5	C	4.3
I/O-Modules				
10	1794-IB10X0B6	DC Combo 10 in 6 out	A	N/A
11	1794-IB16	DC Sinking Input 16 pt.	A	N/A
12	1794-IE8	Analog Input 8 pt.	B	N/A
13	1794-IF2X0F2I	Isolated Analog Combo 2 in 2 out	A	F
14	1794-IF4I	Isolated Analog Input 4 pt.	A	F
15	1794-IJ2	High Resolution Freq. 2 channel	A	D
16	1794-IP4	Pulse counter 4 channel	B	4
17	1794-IR8	RTD input 8 pt.	A	K
18	1794-IRT8	non isolated Thermo input 8 pt.	B	B
19	1794-IT8	Thermo input 8 pt.	A	K
20	1794-OB16	DC Output Source 16 pt.	A	N/A
21	1794-OB16P	DC Protected Output Source 16 pt.	A	N/A

No.	Rockwell Automation Catalog Number	Description	Revision	
			HW	FW
22	1794-OB8EP	DC Elec Fused Output Source 8 pt.	A	N/A
23	1794-OE4	Analog Output 12 bit, 4 pt.	B	N/A
24	1794-OF4I	Isolated Analog Output 4 pt.	A	F
25	1794-OW8	Relay Contact 8 pt.	A	N/A

Table 1: Identification of the test object

3.2 Documentation of the test object

All necessary documentation for the concept review regarding the FLEX I/O-System was provided by Rockwell Automation.

No.	Description	Revision	Date	Remark/Doc-No.
/1/	FLEX-I/O System Specification	4	1997-03-27	FE-001/4
/2/	FLEX-I/O Technical Data Manual	E	1999-07-15	ER#X6664
/3/	Safety Reference Manual - ControlLogix	--	2005-01-31	1756-RM001D-EN-P
/4/	Safety Reference Manual - FLEXLogix (hereafter SRM)	A	2005-01-31	1791-RM001A-EN-P

Table 2: Documentation for the concept review

In addition the following documents were used:

- Module specific documentation was provided by Rockwell. Those documents were also used during the qualification.
- Documents of the Type Approval of the ControlLogix-System (TÜV-Report-No. 968/EZ 135.03/05 dated 2005-01-31) were used where required.

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

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:

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

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

$$SFF \rightarrow 90 \% - < 99 \%$$

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

$$SFF \rightarrow 60 \% - < 90 \%$$

4. Test and test results

4.1 Safety requirements

4.1.1 General safety requirements - FSM

The manufacturer (Rockwell Automation) maintains a project specific functional safety management system which fulfils the general requirements of the IEC 61508-1 in order to manage and specify all technical activities during the safety lifecycle phases which are necessary to achieve the required safety integrity level (SIL) of a safety related system.

4.1.2 Avoidance of systematic failures

To avoid systematic failures in the specification, in the design of the architecture and the hardware/software modules as well as in the test and integration phase Rockwell Automation uses techniques and measures according to Annex B of IEC 61508-2 and Annex A and Annex B of IEC 61508-3 with reference to the required SIL.

The same techniques and measures are used as for the previously certified ControlLogix-System are valid for the FLEX-I/O-System.

These measures are sufficient for the required SIL-level.

4.1.3 Control of failures

To control failures during operation, different techniques and measures according to Annex A of IEC 61508-2 with reference to the required SIL are implemented.

For more detailed information see chapter 4.2.2 and 4.3.

These measures are sufficient for the required SIL-level.

4.2 Review and results of the inspection

4.2.1 Review of the documentation

The documentation as listed in chapter 3.1 were used during the concept review.

In detail the following documents were reviewed:

- ASIC-Design specifications
- Hardware Design Specifications of the different modules
- User documentation

The review of the documents has shown that the formal requirements regarding the standard IEC 61508 are fulfilled by documents in general.

4.2.2 Review of the safety architecture

In safety related systems up to SIL2 a minimum of 2 FLEX-I/O groups must be used.

The following general principal safety loop structures must be fulfilled:

1. Safety critical inputs are connected to 2 input-modules located in different FLEX I/O-lines. The two FLEX I/O-Lines will communicate with the Owner Controller via a CNB-Module (see Figure 1).

2. Safety critical outputs are connected to 1 output-module and will be read back by an input modules located in the different FLEX I/O-line. A secondary shutdown path (e.g. external relay) is required. The secondary shutdown path must be controlled by a different output module located in the CLX-system or by a different output module located in the other FLEX-I/O line.
A relay module can be substituted for the external relay. Also, the external relay can be placed in series either before or after the output module.
3. Safety critical analog outputs normally have no predefined safe state. Because of this analog outputs must be read back by an analog input. The location of the analog output and analog input must be in different FLEX I/O-Lines. A faulty compare must result in a failure message to the operator. The following fault reaction must be an organizational one, described within the safety manual, or also covered by a secondary control path.

Additional application specific structures may be possible, but need to be inspected separately.

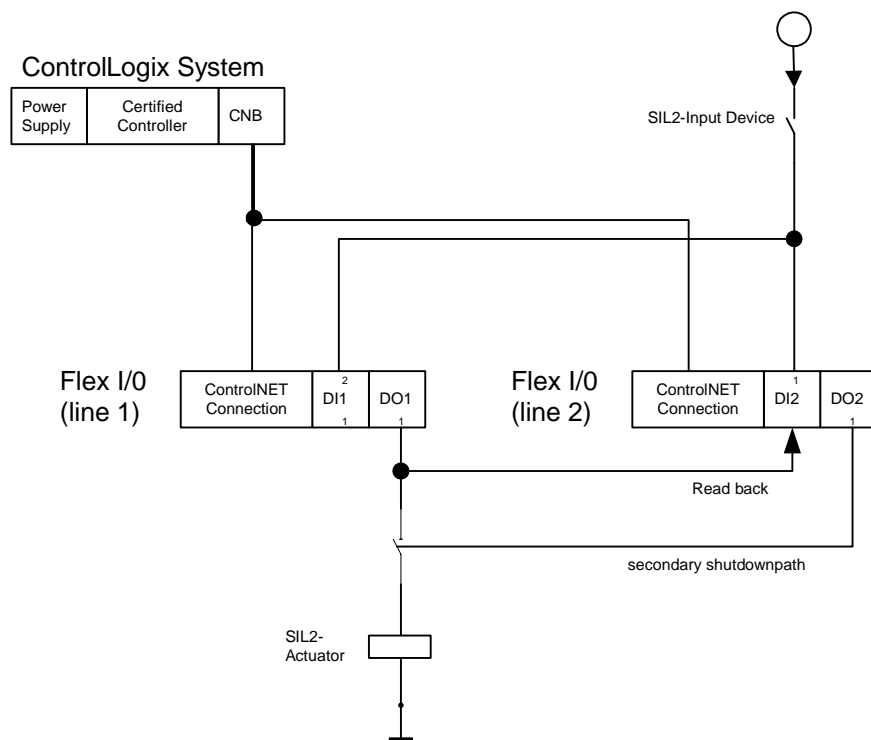


Figure 1: Example for Digital I/O wiring

4.3 General hardware requirements

4.3.1 Environmental requirements

All modules fulfil the requirements of IEC 61131 part 2 regarding the environmental conditions.

These measures are sufficient for the certification.

The tests were carried out in the Rockwell laboratory which is accredited to IEC 17025. The results were accepted by the Test Institute.

4.3.2 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/.

4.3.3 Power supply

The FLEX I/O-System gets its power supply from external units.

It is required that the power supply of the logic, connected via the ControlNet adapter, is strictly separated from the field power.

The following additional measurements must be applied:

- over voltage protection
- a detection of under voltage
- no auto restart

Field power is wired via the I/O-connectors only. The field power supply

- must be sufficient blocked by protecting measures to avoid e.g. surge or burst interference
- must be interference free between the relating FLEX I/O-Lines
- must fulfil the requirements for electrical safety
- must fulfil a detection of under- and over voltage

4.4 Review of the different modules

4.4.1 Terminal base

The terminal bases provide the field power connection, FLEX-Bus connection and I/O-signal connection for different I/O modules. The terminal bases will not contain any logic. Failures in the terminal bases are covered by the serial protocol between a communication adapter and the slave modules.

Therefore the terminal bases are useful for SIL 2.

4.4.2 I/O-components

All I/O-modules listed in chapter 3.1 have a SFF of > 60 % due to internal diagnostics and due to system safety concept aspects.

A FMEA on Function Block level was used to verify that the requirements of a SFF > 60 % is fulfilled.

The I/O-components have to be used according to the structures described in chapter 4.2.2 and the SRM /4/.

4.4.3 ControlNet-Adapter

The ControlNet-Adapter is the key module for the safety concept. It will handle:

- communication to the main processor via ControlNet
- continuous collection and storage of the states of its submodules
- handling of RPI-mechanism of its submodules

The ControlNet-Adapter fulfils a SFF of > 60 %.

- The communication is under the control of the ControlLogix - processor module.
- All necessary information (diagnostics, errors, I/O-data, data-echo) of all slave-modules will be send to the controller within the predefined RPI, so the controller can compare all relating and actual data.
- The communication protocol between the controller and ControlNet-Adapter has the same safety quality than between a CLX main and remote rack.
- A loss of communication will be detected and leads to a predefined safe state of the outputs.

FLEX-Bus:

- The ControlNet-Adapter refreshes all signal information (Diagnostics, Errors, I/O-Data, data echo) continuously.
- Detected communication faults will be reported to the ControlLogix - processor module.
- A loss of communication will be detected and leads to the safe state of the actuators.

Details on this will be discussed in the associated FLEX I/O SIL 2 Safety Manual.

4.5 Configuration and Programming of the FELX-I/O

The same configuration software and configuration procedures are used as for the CLX-system (see also Report of the Test Institute No.: 968/EZ 135.03/05 dated 2005-01-31).

4.6 System tests

During the type approval application programs were developed by TÜV. The programs were designed to use and to check the features of a typical FLEX-I/O - System in conjunction with ControlLogix - System (consisting of a certified controller, a CNB Module and different ControlLogix-I/O components).

The programs were used to test

- 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)

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.

4.7 **Conditions for applications**

For the use of the FLEX I/O-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 the SRM /4/.

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

For full compliance the following conditions must be observed:

- Additional testing may be necessary.
- The conditions of the SRM /4/ 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**

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 FLEX-I/O-System that are certified for SIL2 are listed in Chapter 3.1.

The FLEX-I/O-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 FLEX-I/O-System must be checked within the commissioning.

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].

2005-01-31

Therefore the ControlLogix-System is appropriate for the use in safety relevant applications up to an including SIL 2 of IEC 61508 [1]. For all applications the de-energised state must be the safe-state (ESD). The conditions of the SRM /4/ must be respected.

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

The inspector



Dipl.-Ing. (FH) Andreas Hesse