Automation, Functional Safety

Test report on the supplementary approval of the Safety Related Programmable Electronic System ControlLogix of Rockwell Automation

Report-No.: 968/EZ 135.07/12
Date: 2012-09-27
Test report on
the supplementary approval of the
Safety Related Programmable Electronic System
ControlLogix of Rockwell Automation

Report-No.: 968/EZ 135.07/12

Date: 2012-09-27

Pages: 9

Test object: Safety Related Programmable Electronic System
ControlLogix

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

Order-No./Date: 7000123343 dated 2012-06-17

Test Institute: TÜV Rheinland Industrie Service GmbH
Automation, Functional Safety
Am Grauen Stein
51105 Köln
Germany

TÜV-Offer-No./Date: 968/192/12 dated 2012-04-18

TÜV-Order-No./Date: 10883414 dated 2012-06-18

Inspector: Dipl-Ing Andreas Hesse

Test location: see Test Institute

Test duration: June 2012 to September 2012

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Scope</td>
<td>4</td>
</tr>
<tr>
<td>2.</td>
<td>Standards forming the basis for the requirements</td>
<td>4</td>
</tr>
<tr>
<td>3.</td>
<td>Identification of the test object</td>
<td>4</td>
</tr>
<tr>
<td>3.1.</td>
<td>Description of the device under test</td>
<td>4</td>
</tr>
<tr>
<td>3.2.</td>
<td>Documents</td>
<td>5</td>
</tr>
<tr>
<td>3.3.</td>
<td>Test samples</td>
<td>5</td>
</tr>
<tr>
<td>3.4.</td>
<td>Previous test reports</td>
<td>6</td>
</tr>
<tr>
<td>3.5.</td>
<td>Terms and definitions</td>
<td>6</td>
</tr>
<tr>
<td>4.</td>
<td>Tests and test results</td>
<td>6</td>
</tr>
<tr>
<td>4.1.</td>
<td>General</td>
<td>6</td>
</tr>
<tr>
<td>4.2.</td>
<td>Proof of interference freeness</td>
<td>6</td>
</tr>
<tr>
<td>4.3.</td>
<td>Test sequence, results of the functional insertion testing</td>
<td>7</td>
</tr>
<tr>
<td>4.3.1.</td>
<td>Performance testing</td>
<td>7</td>
</tr>
<tr>
<td>4.3.2.</td>
<td>Electrical safety</td>
<td>7</td>
</tr>
<tr>
<td>4.3.3.</td>
<td>Temperature and supply voltage interference</td>
<td>7</td>
</tr>
<tr>
<td>4.3.4.</td>
<td>Electromagnetic interference / compatibility</td>
<td>8</td>
</tr>
<tr>
<td>4.3.5.</td>
<td>Mechanical interference</td>
<td>8</td>
</tr>
<tr>
<td>4.4.</td>
<td>User documentation</td>
<td>8</td>
</tr>
<tr>
<td>4.5.</td>
<td>Application specific requirements</td>
<td>8</td>
</tr>
<tr>
<td>5.</td>
<td>Summary</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Statement of the certification body</td>
<td>9</td>
</tr>
</tbody>
</table>
1. **Scope**

Within this type approval it was investigated whether the new Redundancy Module 1756-RM2 Series A, as part of the approved ControlLogix System, can be classified as interference free to the safety system.

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

**Functional safety**

[N1] IEC 61508, parts 1 - 7:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems

**Application specific**

[N2] EN 50156-1:2004
Electrical Equipment for Furnaces

[N3] IEC 61511-1:2004
Safety Instrumented Systems for the process industry sector

National Fire Alarm Code Handbook

Boiler and Combustion Systems Hazards Code

Fire Detection and Fire Alarm Systems Control and indicating equipment

Programmable Controllers

[N8] IEC 61326-3-1:2008
Electrical equipment for measurement, control and laboratory use - EMC requirements
Part 3-1: Immunity requirements for equipment performing or intended to perform safety related function (functional safety) - Industrial applications with particular EM environment

3. **Identification of the test object**

3.1. **Description of the device under test**

The device under test is a new version of Redundancy Module (1756-RM2 / RM2XT Series A) as part of the ControlLogix system.

The ControlLogix system is a Programmable Logic Controller system including Controller, different I/O-modules, Racks and communication modules. It is approved for the use in low demand applications up to SIL2 (for details see the Safety reference manual).

The Redundancy Module inside a ControlLogix provides a communication channel between two ControlLogix Controllers. These controllers run in parallel for availability purposes (see Figure 1)

One of these controllers (“Primary” controller) has access to the I/O area while the other controller (“Secondary” controller) runs in standby mode. At specified intervals the Primary Controller sends its I/O-data via the Redundancy Module to the Secondary. In case of a fault in the Primary controller the Secondary can take the control of the I/O-modules.

The Redundancy Module shall be considered “Interference Free”.

The tested version is Rev. 20.4.6
3.2. Documents

<table>
<thead>
<tr>
<th>No.</th>
<th>Document</th>
<th>Document-No.</th>
<th>Rev.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D2]</td>
<td>1756-RM Series C Functional Specifications</td>
<td>FSX0466</td>
<td>06</td>
<td>2012-05-23</td>
</tr>
<tr>
<td>[D3]</td>
<td>High Level Design Document of RM2 for SIL assessment</td>
<td>N/A</td>
<td>1.0</td>
<td>2012-07-11</td>
</tr>
<tr>
<td>[D4]</td>
<td>RM2 Diagnostic Coverage</td>
<td>N/A</td>
<td>2.0</td>
<td>2012-07-26</td>
</tr>
<tr>
<td>[D5]</td>
<td>Proposal for (SIL2) Data Integrity Diagnostics in RM2</td>
<td>N/A</td>
<td>N/A</td>
<td>2012-06-27</td>
</tr>
</tbody>
</table>

3.3. Test samples

For this evaluation no test samples were used.
3.4. Previous test reports

<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Document-No.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>[P1]</td>
<td>Type approval of Safety Related Programmable Electronic System Control Logix</td>
<td>968/EZ 135.00/02</td>
<td>2002-09-30</td>
</tr>
<tr>
<td>[P2]</td>
<td>Type approval of Safety Related Programmable Electronic System Control Logix</td>
<td>968/EZ 135.01/04</td>
<td>2004-03-02</td>
</tr>
<tr>
<td>[P3]</td>
<td>Type approval of Safety Related Programmable Electronic System Control Logix</td>
<td>968/EZ 135.02/04</td>
<td>2004-03-31</td>
</tr>
<tr>
<td>[P4]</td>
<td>Type approval of Safety Related Programmable Electronic System Control Logix</td>
<td>968/EZ 135.03/05</td>
<td>2005-01-31</td>
</tr>
<tr>
<td>[P5]</td>
<td>Type approval of Safety Related Programmable Electronic System Control Logix</td>
<td>968/EZ 135.04/06</td>
<td>2006-11-27</td>
</tr>
<tr>
<td>[P6]</td>
<td>Report about the type approval of the Safety Related Programmable Electronic System Control Logix of Rockwell Automation</td>
<td>968/EZ 135.05/09</td>
<td>2009-09-16</td>
</tr>
<tr>
<td>[P7]</td>
<td>Test report on the type approval of the Safety Related Programmable Electronic System ControlLogix of Rockwell Automation</td>
<td>968/EZ 135.06/12</td>
<td>2012-08-29</td>
</tr>
</tbody>
</table>

3.5. Terms and definitions

**Interference Free**

A module is considered “Interference Free” if it cannot prevent a safety action.

4. Tests 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 uncertainty 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. Proof of interference freeness

The Redundancy Module itself is not part of the safety loop. But it transfers safety data from the Primary to the Secondary Controller.

The following possible influences on the safety where identified:

1. The Redundancy Module may cause failures in the communication between the controllers. Therefore, data may be wrong or were not sent in time.

2. The Redundancy Module may try to switch both controllers to the active mode.
In addition the normative requirements (IEC 61508-3:2010 Chapter 7.2.2.9, 7.4.2.8, 7.4.2.9 and Annex B-Table B.1 and Table B.6) were analyzed in view of the Redundancy Module.

Result:

1. The transfer of the I/O data image was checked against the requirements of IEC 61508-2:2010-4-7.4.11.1. The transfer of the I/O data image is protected by a CRC (for details on the mechanisms see [D3], [D5]), a sequence number and a timeout that is checked by the safety related controllers. The Redundancy Module cannot create a valid I/O data image-message. It can also not create valid I/O-data messages. Therefore, the possible communication errors (transmission errors, repetition, deletion, insertion, re-sequencing, corruption delay and masquerade) are detected by the safety system.

2. The situation of activating both controllers for I/O access is prevented by design even if more than one considered failure occurs (see [D2] chapter 13.1.3).

In addition the following normative requirements regarding interfere checked:

4.3. Test sequence, results of the functional insertion testing

The Redundancy Module is classified as “Interference Free”. Therefore, the test sequence is set with the following items:

- Functional Tests
- Temperature / Humidity Tests
- EMC Tests using a Safety Standard

Result:

All required tests (functional and system verification/validation) have been completed successfully. The test reports were handed over to the Test Institute. The results of the assessment are summarized in particular within the following subchapters:

4.3.1. Performance testing

During the verification activities all properties of the Redundancy Module and the requirements of the specification were checked as a functional verification) in the manufacturer's laboratories.

The Fault Insertion Tests confirmed the effectiveness of the realized measures to detect and to control faults.

Result:

All necessary tests were carried out at the manufacturer’s laboratory. The tests were finished with a positive result.

4.3.2. Electrical safety

The device is powered by 24V DC SELV/PELV supply.

Result:

There are no additional requirements regarding electrical safety.

4.3.3. Temperature and supply voltage interference

The tests have been carried out by the manufacturer according to the IEC 61131-2. The results are documented in several test reports.

Result:

The tests were finished with a positive result. The results are accepted by the Test Institute based on a positive laboratory assessment. The requirements of IEC 61131-2 are met.
4.3.4. Electromagnetic interference / compatibility

The EMC / EMI tests have been carried out at manufacturer according to the IEC 61131-2 and IEC 61326-3-1. The results are documented in several test reports.

Result:
The tests were finished with a positive result.
The results are accepted by the Test Institute based on a positive laboratory assessment.
The requirements of IEC 61131-2, IEC 61326-3-1 are met.

4.3.5. Mechanical interference

The tests have been carried out by the manufacturer according to the IEC 61131-2. The results are documented in several test reports.

Result:
The tests were finished with a positive result.
The results are accepted by the Test Institute based on a positive laboratory assessment.
The requirements of IEC 61131-2 are met

4.4. User documentation

To ensure the safe usage of the Redundancy Module in all of the relevant life cycle phases (installation, maintenance, decommissioning) it is necessary that the user has all important information available. This includes among others warnings, installation hints, advice for the calculation of reaction time, and requirements for the cyclic maintenance procedures.

The Installation and Operating Manual [D1] was checked according to the requirements of the relevant standards.

Result:
The user documentation was checked in form and content for the safe usage of the product.
It fulfills the requirements according to the relevant standards and to the specifications. All relevant information for identification and safe use is in its appropriate place.

4.5. Application specific requirements

The 1756-RM2 Series A Module is “Interference Free” to the safety system.
Therefore, no additional evaluation regarding the application specific standards were considered necessary.

Result:
The previous results remain valid.

5. Summary

Based on the results of the inspection / review of the submitted documents it can be confirmed that the product can be considered as interference free.

Hence it can be used in ControlLogix safety up to SIL 2 according to IEC 61508 to provide high availability applications.

The instructions of the associated Installation and Operating Manual shall be considered.
Statement of the certification body:

According to the test results documented in this report and the shown conformity to the relevant and applied standards respectively to their protection goals it is confirmed, that the certificate with the No. 968/EZ 135.05/09, dated 2009-09-16, remains further valid.

The associated "Revision List" is updated accordingly.

Cologne, 2012-08-29
TIS/A-FS/Kst. 970 ga-nie

Certification body

Dipl.-Ing. Heinz Gall