

2009-01-20

Automation, Software and Information Technology

**Report on the type approval of the
Safe Speed Monitor Option - S1
used within PowerFlex 750-Series AC Drives
of Rockwell Automation Inc.**

**Bericht-Nr.: 968/EZ 341.00/09
Datum: 2009-01-20**

**Report on the type approval of Safe Speed Monitor Option Module
used in PowerFlex 750-Series AC Drives of Rockwell Automation Inc.**

Report-No.: 968/EZ 341.00/09

Date: 2009-01-20

Pages: 10

Test object: Safe Speed Monitor Option - S1 used within the adjustable
Frequency Drive Allen Bradley PowerFlex 753
and PowerFlex 755
Frame 2-7, 400V- 480V

Customer: Rockwell Automation
6400 West Enterprise Drive
Mequon, WI 53092
United States of America

Manufacturer: Rockwell Automation
6400 West Enterprise Drive
Mequon, WI 53092
United States of America

Order-No./Date: H046287 dated 2007-03-26
H046287 und 7000012819 (30.03.2007 und 06.06.2008)

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

Department: Automation, Software and Information Technology (ASI)

TÜV-Offer-No./Date: 968/15/07 dated 2007-01-19

TÜV-Order-No./Date: 9719447 dated 2007-04-02

Inspector: Dipl.-Ing. Thomas Steffens

Test location: see Test Institute

Test duration: October 2005 to January 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.

1. **Scope**

This report documents the type approval of the Safe Speed Monitor Option - S1 used within the adjustable Frequency Drive Allen Bradley PowerFlex 753 and PowerFlex 755.

On this way the comprehensible proof shall be established, that the device under test meets the functional and safety related requirements of the product specification and fulfils the requirements up to PL e and category 4 according to EN ISO 13849-1 as well as SIL 3 according to IEC 61508 / EN 62061.

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

- [N1]** EN ISO 13849-1:2008
Safety of machinery - Safety-related parts of control systems
Part 1: General principles for design
- [N2]** EN 60204-1:2006
Safety of machinery - Electrical equipment of machines
Part 1: General requirements
- [N3]** EN 61800-5-1:2007
Adjustable speed electrical power drive systems
Part 5-1: Safety Requirements - Electrical, thermal and energy
- [N4]** EN ISO 13850:2006
Safety of machinery; Emergency stop, Principles for design
- [N5]** EN 62061:2005
Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
- [N6]** IEC 61508 Part 1-7:1998 and 2000
Functional safety of electrical/electronic/programmable electronic safety-related systems.
- [N7]** IEC 61800-5-2:2007
Adjustable speed electrical power drive systems
Part 5-2: Safety requirements-Functional

3. **Test object**

3.1 **Identification of the test object**

The Safe Speed Monitor Option - S1 as a safety option board will be used within the adjustable Frequency Drive Allen Bradley PowerFlex 753 and PowerFlex 755.

The safety and monitoring functions of the Safe Speed Monitor Option - S1 are configurable.

The Safe Speed Monitor Option - S1 provides following interfaces to the user:

Six redundant safety inputs for the safety functions:

- Safe Stop (SS)
- Safety Limited Speed Monitoring (SLS)
- Door Monitoring (DM)
- Enabling Switch Monitoring (ESM)
- Lock Monitoring (LM)

Three sets of redundant safety outputs:

- SS_Out
- SLS_Out
- DC_Out (configurable as bipolar outputs)

Two Encoder interfaces:

- Encoder 1
- Encoder 2

One additional input:

- Reset Input (Fault reset)

Two pulse outputs for diagnosis:

- Test_Out_0
- Test_Out_1

The Safe Speed Monitor Option - S1 is cascadable and can be configured as Master or as Slave.

Following safety modes are configurable:

0	All safety function are disabled
1	Master- Safe Stop
2	Master- Safe Stop with Door Monitoring
3	Master- Safe Limited Speed
4	Master- Safe Limited Speed with Door Monitoring
5	Master- Safe Limited Speed with Enabling Switch Control
6	Master- Safe Limited Speed with Door Monitoring and Enabling Switch
7	Master- Safe Limited Speed Status Only
8	Slave-Safe Stop
9	Slave- Safe Limited Speed
10	Slave- Safe Limited Speed Status Only

The test object as well as the functionality is described in detail in the documents provided to the Test Institute.

The latest version of the software and hardware is as follows:

SW: V1.004.001

HW: V 01

3.2 Documentation

The documents that are the basis for the type approval are listed in „Document Reference List_0p15.xls “. The latest version is 0.15.

2009-01-20

3.3 Test sample

Selected tests have been performed or witnessed at the Rockwell site in Mequon dated 1st December 2008 to 4th December 2008.

The test have been performed based on the schematics "394530-2_R-Version7prelim.pdf" and "312321_R-Version2_stf.pdf"

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 Illustration of the inspection process

The type approval has been executed in the following main steps:

- Kick-off Meeting in 2005-10-06 at Rockwell Automation in Wuppertal. Presentation of concept.
- 1. Detailed review of the concept at Rockwell Automation in Wuppertal from 2006-03-09 to 2006-03-10. Analysis of the safety function und planned measures for fault control according to the applied standards. Inspection and judgement of the intended and applied measures for fault avoidance according to the relevant life cycle phases of the device according to IEC 61508. Verification of the required documents with relation to completeness according to the requirements of IEC 61508.
- 2. Detailed review of the concept at TÜV Rheinland Industrie Service in Cologne in 2006-08-23. Review of the concept of the MSR57P (SMSC).
- 3. Detailed review of the concept at Rockwell Automation in Wuppertal from 2006-10-26 to 2006-10-27. Review of the relevant documents of the concept (FRS, Safety Plan, FW Architecture, Schematics, FMEA, Configuration).
- Phone conference in 2007-01-16. Discussion about the adapted documents of the concept.
- Phone conference and concept meeting at Rockwell Automation in Wuppertal in 2007-04-16.
- 4. Detailed review of the concept at Rockwell Automation in Wuppertal in 2007-06-20. Review of the documents for the approval of the MSR57P in preparation for the practical test.
- 5. Detailed review and practical tests at BBH in Weiden from 2007-07-24 to 2007-07-27. Verification of the implemented measures for fault control. Performing of fault injection tests. Review of the documents according to the relevant life cycle phases.
- 6. Practical tests at Rockwell Automation in Wuppertal in from 2007-08-02 to 2007-07-27. Repetition of practical tests as a result of the practical tests at the 5. Detailed review and practical tests at BBH in Weiden from 2007-07-24 to 2007-07-27.

- 7. 2008-12-01 to 2008-12-04 at Rockwell Automation in Mequon. Performing of additional fault injection tests for the SMSC in order to cover the additional safety circuits of the enhanced safety board. Review of the documents according to the relevant life cycle phases
- 8. Review of the provide documents of the different life cycle phases from 2007-12-06 to 2009-01-16.
Review of the provided documents with following main focus:
 - User documentation
 - Test plan (Module tests for software, Integration tests for Software- and Hardware)
 - Reports of test results (Module tests for software, Integration tests for Software- and Hardware)
 - Verification of the environmental tests, EMC tests, mechanical tests

4.3 Description and judgment of the safety structure

The safety structure of the enhanced safety board for the realization of the "Safe Speed Monitor Option - S1" is almost technically identical to the already type approved Speed Monitoring Safety Relay MSR57P (Report-No.: 968/EZ 335.00/08).

In contrast to the MSR57P, no external motion power outputs exist.

The safety function "Safe Torque Off" is realized by two independent channel. The first channel switches off the supply of the gate driver and the pull-up resistors and the second channel disables the gate driver outputs. Both channels are tested periodically. These tests cannot be disabled.

In contradiction to the MSR57P the safety structure of the power supply is as follow:

- Power Supply 24 V serves for the supply of the outputs and is not monitored.
- 12 V power supply is provided by the control board and is not monitored. The maximum voltage in case of failure is 22 V. Protection for this over voltage condition is considered. From the 12 V the 3,3 V and 5 V are derived and from the 3,3 V the 1,8 V is derived.
- The 5 V, 3,3 V and 1,8 V are monitored by both μ C via the ADC.
- 3,3 V serves for the supply of the peripheral and is monitored for over voltage condition.
- 1,8 VDC serves for the supply of the cores of the μ Cs and is monitored for over voltage condition and under voltage condition by an independent monitoring circuit with an independent switch off circuit for the outputs. The voltage monitoring circuit is tested cyclically.
- Additionally two Reset devices exist that monitor the 3,3VDC and 1,8 VDC for under voltage condition.

A safety Integrity Level of 3 as well as PL e can be reached by using at least two independent encoders installed in a manner that common cause effects do not affect the safety of both feedback systems.

By using a certified sin/cos-encoder type SIL 3 can be reached if the conditions described in the user manual are kept. Among others a fault exclusion for shaft slippage and shaft breakage is required.

Safety Integrity for Configuration process

The Safe Speed Monitor Option - S1 can be configured by means of the following tool:

- "Drive Explorer" in combination with an anaCANda converter
- "HIM" a kind of portable Drive Explorer

For the communication during configuration a third μC is used. This μC serves as black channel and does not affect the configuration data. It handles the configuration process between the safety controllers and the configuration tools. The configuration data are solely verified by both safety controllers.

Following measures insure the integrity of the configuration process:

- configuration is protected by crc32 signature calculated in the device
- comparison of the signature with signature calculated in configuration tool
- configuration must be tested by the user as instructed in the user manual
- configuration must be verified by visual inspection after uploading from the device
- configuration must be locked for protection against unauthorised changes
- unlocked condition can be verified by checking the Guard status parameter P68
- optional password protection can be used
- protection against unauthorised use is also given due to the requirements of the use of personal computer , special adapter cable for connection and special configuration software
- detailed procedures for configuration are described in the user manual

The process of configuration and parameterization meets the requirements according EN 62061 chapter 6.11.2.

Fault behaviour

In case of a fault where the safety integrity is in question (Safe state fault) all outputs are set to their safe state, all communications are stopped and reset is carried out and a completed power up diagnostics. The other faults lead to a defined fault behaviour (i. e. execution of the stop function) that is described in detail in the documents mentioned in chapter 3 and in the user documentation.

Whether a fault is resettable or not depends on the fault type.

Response time

The response time of an input event is determined to 16 ms. The response time of a speed monitoring event is mainly depending on the configurable "Overspeed Response time" and varies from 48 ms to 420 ms. Both response times are described in detail in the belonging user manual.

With this safety structure the Safe Speed Monitor Option - S1 can be used in applications up to Safety Integrity Level 3 according to EN 61508 / EN 62061 as well as up to category 4 and PL e according to EN ISO 13849-1 depending on the configuration and parameterization.

4.4 Results of the functional and safety analyses

In common reviews together with the developer the safety of design of the Hardware and the Software has been analyzed. All safety related functions and the measures for fault detection and control have been verified by practical tests.

In these tests the effectiveness of the measures as well the temporal requirements for fault detection and control have been verified.

Additionally the aspects of electrical safety, completeness of the requested documents and the user documentation were also subject of inspection and testing.

Besides of these tests comprehensive tests for the hardware and software have been performed by Rockwell or on behalf of Rockwell by BBH and Patny according to the test plans, which have been agreed with Rockwell. The results of these tests are present at the Test Institute. The results show that all tests were passed and the target safety integrity is kept.

The results are accepted by the Test Institute.

The summary result of all these tests is that the requirements according to EN ISO 13849-1 category 4 and PL e and according to IEC 61508, EN 62061 and EN 61800-5-2 SIL 3 are fulfilled.

All the required information for a safe use can be found in the belonging user documentation.

4.5 Electrical safety

TÜV Rheinland of North America (TRNA) has performed the electrical safety certification according to EU Low Voltage Directive (LVD) and to EN 61800-5-1 for the PF753/PF755 in conjunction with certification of integrated safety function "Safe Torque Off".

The results are documented in the summary report-no.: 30771465.004 dated 2008-11-10 and confirm, that the PF753/PF755 fulfils requirements according to the EU Low Voltage Directive (LVD) and to EN 61800-5-1 for the above mentioned models.

On the enhanced safety board for the realization of the Safe Speed Monitor Option - S1 no voltage exists higher than 24 VDC. Therefore the results of the electrical safety certification can be taken over for the PF753/PF755 with Safe Speed Monitor Option - S1.

The results are accepted by the Test Institute.

4.6 Environmental tests

The environmental tests have not been repeated for the PF753/PF755 with implemented enhanced safety board.

Solely an extended temperature test with an ambient temperature of 90°C has been executed. No failures occur during this tests.

The enhanced safety board is installed in a POD, which is used to mount the various option boards within drive. According to a statement of Rockwell (Internal Department letter, dated 2009-01-16) the maximum ambient temperature within this POD has been determined to 65°C. The De-rating of the components have been done based on this temperature. Additionally a thermal scan has been done in order to confirm that all components are in their specified ratings. The hottest point on the board is 50°C.

Due to this analysis the Test Institute agree that an additional temperature testing is not required for the PF753/PF755 with implemented enhanced safety board.

The mechanical tests have not been repeated since the mounting method of the enhanced safety board is not different to the other option boards which are mounted in the POD and the components of the enhanced safety board has no significant mass.

The mechanical tests for the PF753/PF755 have been performed during the certification of integrated safety function "Safe Torque Off" by TRNA. The results of these tests are documented in the summary 30771465.004 dated 2008-11-10. During these tests option boards with significant mass were installed.

Due to the fact that the components of the enhanced safety board has no significant mass, no other results are expected by a repetition of the mechanical tests where this board is installed.

Therefore the Test Institute agree that a repetition of the mechanical tests where this board is installed is not required.

4.7 EMC/EMI contemplation

The tests according to the standards EN 61000-4-4, EN 61000-4-2, EN 61000-4-5, and EN 61000-4-6 have been performed in the labs of Rockwell. All tests have been passed. The results are documented in the reports DE1001-006, DE1002-001, DE1002-002, DE1002-003 and DE1002-004.

The results are accepted by the Test Institute.

The tests according to EN 61000-4-3 and the measurements of radiated emission have been performed in an accredited Test Institute (LS Research, W66N220 Commerce Court, Cedaburg, WI 53012). The results of these tests are documented in the reports no.: DE1002-005, DE1002-004 and 280097.

Additionally the increased levels according to EN 62061 have been tested and passed.

The results are accepted by the Test Institute.

4.8 Measures for the avoidance of faults according to IEC 61508

The IEC 61508 requires the realization and the verification of measures for the fault avoidance over the whole life cycle process of the safety system, beginning with the specification and finishing with the decommissioning of the safety system.

The volume of the measures, which have to be performed according to the IEC 61508, is depending on the target safety integrity level.

The measures for the fault avoidance, which have been carried out by Rockwell during the different life cycle phases, are documented. These documents are present at the Test Institute.

The measures for the fault avoidance, which have been carried out by Rockwell, are sufficient to fulfil the requirements for SIL 3 according to the IEC 61508.

4.9 Determination of the safety parameters

The determination and calculation of the safety parameters is documented in the Excel file "Rhino_Adv_Safety-FMEA-Rev0_4.xls". For the determination and calculation of the safety parameters a "worst case" configuration has been assumed (standalone, all inputs, all outputs, single encoder mode). The safety parameters for SIL 3 according to IEC 61508 and PL e according to EN ISO 13849-1 are met.

The Proof test interval (PTI) is determined to **20 years**. Within this time interval the values for PFD_{av} and PFH are as follow:

$$PFD_{av} = 2.35 * 10^{-4}$$

$$PFH = 2.67 * 10^{-9} \text{ 1/h (calculated according to IEC 61508)}$$

$$PFH_D = 1.17 * 10^{-8} \text{ (calculated according to EN 62061)}$$

$$MTTF_D = 143 \text{ years}$$

$$DC_{av} = \text{High}$$

2009-01-20

5. Summary

The type approval of the Safe Speed Monitor Option - S1, manufactured by Rockwell Automation, came to the result, that the requirements of the applicable standards, which are listed in clause 2, are met.

Hence the Safe Speed Monitor Option - S1 can be used in applications up to SIL 3 according IEC 61508 / EN 62061 / 61800-5-2 as well as up to category 4 and PL e according to EN ISO 13849-1 depending on the configuration and parameterization.

The information for a safe use is present in the belonging user documentation.

Cologne, 2009-01-20
TIS/ASI/Kst. 968-stf-nie

The expert



Dipl.-Ing. Thomas Steffens

Report released after review
Date: 2009-01-20



Dipl.-Ing. Stephan Hüb