

Automation, Software and Information Technology

**Test report on the type approval of the
“Safe Speed Monitor Option S1” and
“Safe Torque Off Option S” within
the frame 8 of the PowerFlex 750 AC Drive
of Rockwell Automation**

**Report-No.: 968/M 262.00/10
Date: 2010-07-29**

Test report on the type approval of the “Safe Speed Monitor Option S1” and “Safe Torque Off Option S” within the frame 8 of the PowerFlex 750 AC Drive of Rockwell Automation

Report-No.: 968/M 262.00/10

Date: 2010-07-29

Pages: 11

Test object: Safe Torque Off Option-S [20-750-S] and
Safe Speed Monitor Option-S1 [20-750-S1] used within
Allen-Bradley PowerFlex 755 20G and 21G 400-480V, Frame 8

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: Approval form dated 2009-02-17
Email dated 2009-02-18

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: 968/59/09 dated 2009-02-09

TÜV-Order-No./Date: 10160996 dated 2009-02-24

Inspector: Dipl.-Ing.Thomas Steffens

Test location: see Test Institute

Test duration: February 2009 to July 2010

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 forming the basis for the requirements | 4 |
| 3. Identification of the test object | 4 |
| 3.1 Technical data | 4 |
| 3.2 Documents | 4 |
| 3.3 Test sample, test set-up | 5 |
| 3.4 Revisions | 5 |
| 4. Tests and test results | 5 |
| 4.1 General | 5 |
| 4.2 Description and judgment of the safety structure | 5 |
| 4.3 Measures for the avoidance of faults according to the relevant standards | 8 |
| 4.4 Measures for the detection and control of faults | 8 |
| 4.5 Electrical safety | 9 |
| 4.6 Environmental tests | 9 |
| 4.7 EMC/EMI contemplation | 9 |
| 4.8 User documentation and markings for a safe use | 9 |
| 4.9 Determination of the safety parameters | 10 |
| 5. Summary | 11 |

Annex to Report-No.: 968/M 262.00/10:
Summary of the characteristic data for use of the product in safety-related applications

1. Scope

The Frame 8 of the PowerFlex 750 AC Drives shall be used in conjunction with the already certified safety options “Safe Speed Monitor Option S1” and “Safe Torque Off Option S”.

This report documents the type approval of the safety circuits as a required interface for the use of the above safety options.

On this way the comprehensible proof shall be established, that the safety options “Safe Speed Monitor Option S1” and “Safe Torque Off Option S” in conjunction with the Frame 8 of the PowerFlex 750 AC Drives fulfil 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 61800-5-2:2007
Adjustable speed electrical power drive systems
Part 5-2: Safety requirements-Functional
- [N2] EN 61800-5-1:2007
Adjustable speed electrical power drive systems
Part 5-1: Safety Requirements - Electrical, thermal and energy
- [N3] EN 61800-3:2004
Adjustable speed electrical power drive systems -
Part 3: EMC product standard including specific test methods
- [N4] EN 62061:2005
Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
- [N5] EN ISO 13849-1:2008 + AC:2009
Safety of machinery - Safety-related parts of control systems
Part 1: General principles for design
- [N6] EN 60204-1:2006 + A1:2009 (in extract)
Safety of machinery - Electrical equipment of machines
Part 1: General requirements
- [N7] IEC 61508 Part 1-7:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems

3. Identification of the test object

3.1 Technical data

The device under test is described in detail in the documents listed in “Latest Documents Sent to TÜV_2010_0728.xls”.

3.2 Documents

The documents used for the assessment are listed in in “Latest Documents Sent to TÜV_2010_0728.xls”.

Following documents have been produced or extended during the type approval by the Test Institute:

- [D1] Rhino_HiHP_Safety-FMEA-Rev_02_stf 2010-07-28.xls
- [D2] TÜV Rheinland Fault Insertion test plan “2010-06-22 FIT HIHOPO.doc”

[D3] TÜV Rheinland test plan "Test plan Rhino HIHOPO - 2010-07-29.xls"

[D4] Schematic „10000083255_02_sch FIB stf 2010-06-23.pdf“

[D5] Schematic „10000089235_00_SCH CB stf 2010-06-24.pdf“

[D6] Schematic „10000103446_00_sch PLI stf 2010-06-24.pdf“

3.3 Test sample, test set-up

Selected tests have been performed or witnessed at the Rockwell site in Mequon dated 28th June 2010 to 30 June 2010.

The test have been performed at a test sample built according to the schematics "10000089235_00_SCH.pdf", "10000083255_02_sch.pdf" and "10000103446_00_sch.pdf"

Revisions of safety FPGAs populated on the PCBs and the PCBs:

PCB: Main Control Board (P/N-46629/ ECN-10016647)
Main FPGA (MCB) 2.001.97 (App), Bootloader: 1.002.06, Diag FPGA 2.001.97

PCB: Fiber Interface Board (PN-40886/ ECN 10013958)

PCB: Power Layer Interface Board (PN-45734/ ECN 10017762)
Main FPGA (PLI) / Diag FPGA: 1.001.51

3.4 Revisions

PCB: Main Control Board (P/N-46629/ ECO-10016647)
Main FPGA (MCB) 2.001.110 (App), Bootloader: 1.002.06, Diag FPGA 2.001.110

PCB: Fiber Interface Board (PN-40886/ ECO 10017371)

PCB: Power Layer Interface Board (PN-45734/ ECO 10016747)
Main FPGA (PLI) / Diag FPGA: 1.002.02

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 Description and judgment of the safety structure

The frame 8 of the PowerFlex 750 AC Drives provides an interface for the connection of the safety options "Safe Torque Off Option S" and "Safe Speed Monitor Option-S1". With the safety circuits of the frame 8 of the PowerFlex 750 AC Drives the safety function "Safe Torque Off" (STO) is realized. For the realization of the safety function following PCBs are involved:

Main Control Board (MCB) , Fiber Interface Board (FIB) and Power Layer Interface Board (PLI), Backplane PCB (BP).

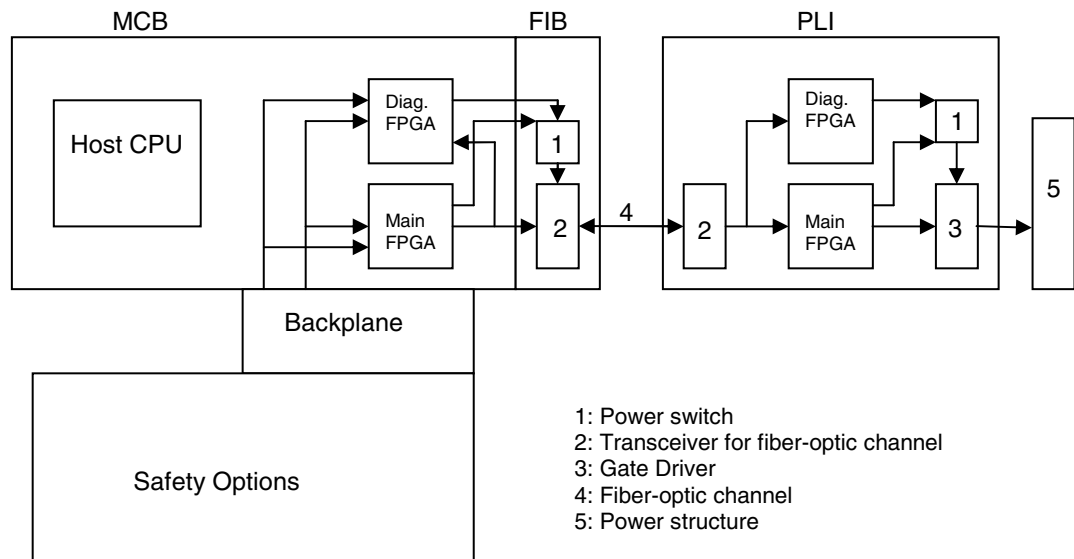


Figure 1: Safety Structure

The Backplane serves as interface to the above mentioned safety options and the MCB and the FIB is the bus interface between PLI board and MCB. For future setup up to five PLI board can be connected to the fiber-optic channel bus. In this project only one PLI board connected to the fiber-optic channel bus will be assessed.

The safety structure of all PCBs is described in detail in the documentation mentioned in chapter 3.2. Following the main items of the safety structure for the MCB, FIB and PLI board will be depicted.

Safety structure of the MCB and FIB

The MCB consists of a Main-FPGA and a Diagnostic-FPGA. The safety signals from the safety option will be routed via the BP to both FPGAs on the MCB. Both FPGAs have the knowledge about the safety signals. The Main-FPGA is interfaced to the FIB that comprises among others the transceivers and the power switch for controlling the supply of the fiber-optic transceivers.

Both FPGAs on the MCB control the power switch on the FIB and can switch off the power supply in case of any detected failure.

The Diagnostic FPGA monitors the behaviour of the Main-FPGA and acts as a Watchdog (WD) and vice versa. Moreover the Diagnostic FPGA is listening to the safety data that the Main-FPGA transmits to the PLI Board. In case that these data are not plausible, the Diagnostic FPGA switches off the power switch on the FIB. The switch off capability of both FPGA is tested cyclically. Both FPGAs are supplied by a common power supply. The safety related supplies are monitored by separate monitoring circuits. The monitoring circuits control the power switch for the transceiver supply and switch off the power switch in case that a supply is out of its specified range.

Both FPGAs have an independent time base.

Safety Bus communication MCB to PLI Board

The FIB serves as interface for the fiber-optic channel bus. By means of this bus the safety data from the MCB will be transmitted to the PLI Board. For the safety data communication suitable measures for fault detection have been realized in order to control the defined failures according to IEC 61508.

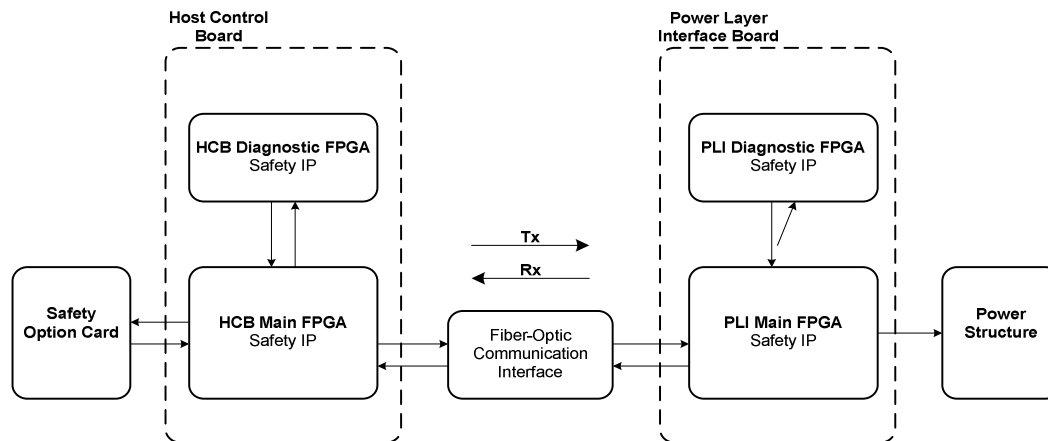


Figure 2: Fiber-optic Communication Structure

Safety structure of the PLI Board

The PLI Board comprises among other transceivers for the fiber-optic channel communication, a main FPGA, diagnostic FPGA, power switch to control the supply for the PWM driver circuitry, monitoring circuit for the safety related power supplies, two independent time base. The safety structure is comparable with the safety structure of the MCB. Both FPGAs receive the safety data from the fiber-optic channel bus. The diagnostic FPGA serves as WD for the main FPGA and vice versa. The diagnostic FPGA monitors the output information of the main FPGA and switches off the power supply of the PWM driver circuitry in case that the information are not plausible. Both FPGAs control the power switch and the capability to switch off the power switch will be tested cyclically. The main FPGA controls the gate driver IC and the switch off capability will be tested cyclically. Both FPGAs have an independent time base.

Configuration of the MCB FPGAs

The FPGAs will be configured during power by means of the Host CPU (Power-PC). Each FPGA has 4 Bit identification tag. This ID tag serves to guarantee that the right FPGA will be addressed and that the configuration is compatible with the HW. The configuration data are stored on the Host control board in a non volatile memory protected by a CRC32. After configuration the CRC of the configuration data will be verified. In case that the CRC calculation fails the power switch will be switched off. The CRC of the configuration will be verified cyclically.

Configuration of the PLI Board FPGAs

The configuration data are stored on the PLI board in a non volatile memory protected by a CRC32. After configuration the CRC of the configuration data will be verified. In case that the CRC calculation fails the power switch will be switched off. The CRC of the configuration will be verified cyclically.

Tests provided by the safety option S and S1

In case that the “Safe Speed Monitor Option S1” is installed, the tests provided by this safety option will be routed to the safety circuits situated on the PLI board for execution. Due to this the whole safety chain, beginning by the safety option and finishing by the disabling circuitry of the PLI board, is covered by these tests.

If the safety option “Safe Torque Off Option S” is used no tests will be provided by the safety option. The tests of the chain will be initiated by the FPGAs on the MCB and PLI board in order to achieve the same safety integrity.

The details to the safety structures are described in the documentation mentioned in chapter 3.2

Result: The system architecture and safety structure fulfils the requirements for PL e / Cat. 4 in accordance with EN ISO 13849-1 as well as for a device conforming to SIL 3 / SIL CL 3 in accordance with EN 61800-5-2/ EN 62061/ IEC 61508.

4.3 Measures for the avoidance of faults according to the relevant standards

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

The measures for fault avoidance for the different life cycle phases at the manufacturer have been inspected by the Test Institute during the present type approval. The Safety Plan “RHP_Functional Safety Plan 02.pdf” contains all relevant information for the project organization and responsibilities. Planning for Verification and Validation Testing was carried out establishing various test plans in order to provide a reproducible verification of the defined requirements. The plan for verification and validation is documented in the V&V Plan “RHP_Functional Safety V&V Plan 02.pdf”.

In order to ensure the systematic integrity during the development of the FPGAs the measures recommended in annex F.2 of IEC 61508-2 have been considered.

The process of the FPGA development and the planned measures are described in detail in “706_RHP_ProjectFpgaSafetyIpdDevProcessSpec_03.doc”.

Result: The measures for fault avoidance over the whole life cycle of the safety related system as well as the Documentation Management System installed and used at the manufacturer for all projects has been assessed with the result that they were carried out in accordance to the requirements for the Functional Safety Management (FSM) of IEC 61508 and meet even more than the requirements for SIL 3 applications.

4.4 Measures for the detection and control of faults

In a common review with the developer the safety of design has been analyzed and the required measures for fault control have been agreed for achieving the target safety integrity level SIL 3 and PL e. In order to determine the required measures the system has been separated in functional blocks and after for each of the functional blocks involved in the safety chain, a system level FMEA was carried out. The results of this analysis has been documented as requirements within the safety requirement specification.

As far as applicable, the design uses the most appropriate diagnostic measures of tables A.1 to A.15 of IEC 61508-2 as mitigations. Additionally, various other measures depending on the technical realization were implemented to achieve the highest possible diagnostic coverage on each function block.

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 by Rockwell.

The results of these tests are present at the Test Institute. The results show that all tests are passed and the target safety integrity is kept.

The results are accepted by the Test Institute.

Additionally to this the results of these tests have been verified by “spot checks” in co-operation with the Test Institute in the manufacturer’s laboratories.

Result: The effectiveness and suitability of the implemented measures is given for the required fault tolerance, safe failure fraction (SFF) and diagnostic coverage (DCavg) for a device conforming to SIL 3 / SIL CL 3 in accordance with EN 61800-5-2 / EN 62061 / IEC 61508 and PL e / Cat. 4 in accordance with EN ISO 13849-1. This was proven by various tests as described below.

4.5 Electrical safety

The electrical safety has been assessed in relation to the safety circuits and touchable user interfaces. The power supply concept of the PF753/PF755 has been already assessed during the type approval of “Safe Torque Off Option S”. The safety circuit is a protection class III device, which requires that the safety circuit must be supplied by a SELV/PELV supply.

In order to show conformity to the protection goals of EU Low Voltage Directive (LVD) Rockwell has carried out the required tests according to EN 61800-5-1. The results are documented in the compliance report “PF755 20G 21G Fr8 61800-5-1 Compliance Rept R1.0 28Jun10.pdf” and confirm, that the requirements according to the EU Low Voltage Directive (LVD) and to EN 61800-5-1 are fulfilled.

The results are accepted by the Test Institute.

4.6 Environmental tests

The environmental tests according to EN 61800-5-1 have been performed in the labs of Rockwell.

All tests have been passed. The test reports are present at Test Institute.

The results are accepted by the Test Institute.

4.7 EMC/EMI contemplation

The tests according to the standard EN 61800-3 have been performed in the labs of Rockwell.

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

The results are summarized in “PF755 Fr 8 61800-3 Compliance Rept r1 28Jun2010.xls”.

All tests have been passed.

The results are accepted by the Test Institute.

4.8 User documentation and markings for a safe use

To ensure the safe usage of the Product in all of the relevant life cycle phases (development, 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.

Result: The user documentation was checked in form and content for the safe usage of the product. It fulfils the requirements according to the relevant standards and to the specifications which were defined during the concept phase. The user manual and installation handbook contain the required information for a safe use of the integrated safety according to EN 61800-5-2.

4.9 Determination of the safety parameters

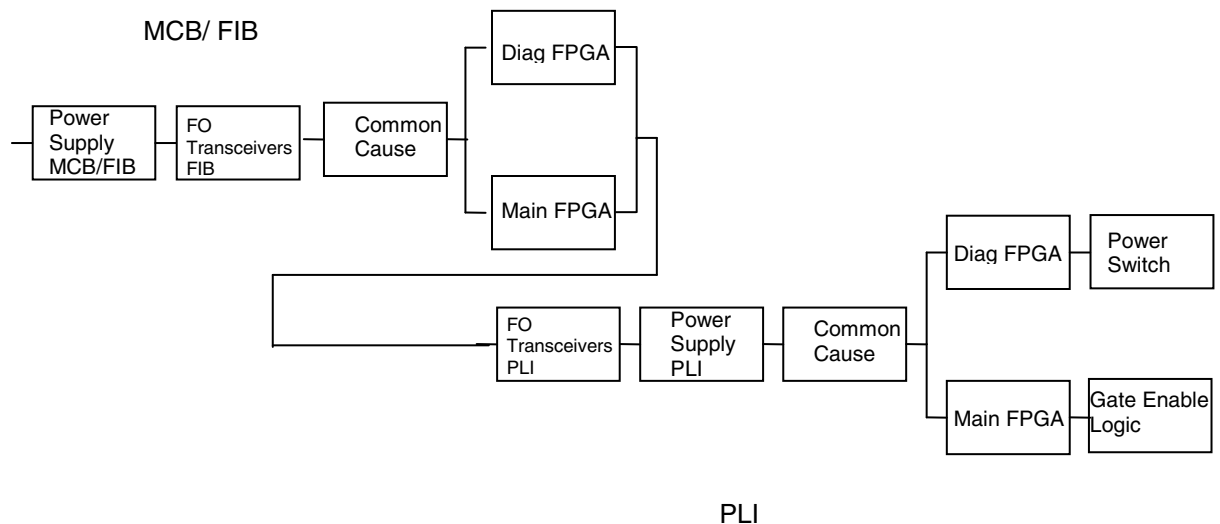
The determination and calculation of the safety parameters for the safety function realized by the Frame 8 of the PowerFlex 750 AC Drive is documented in the Excel file "Rhino_HiHP_Safety-FMEA-Rev_02_stf 2010-07-29.xls".

The determination of the residual failure rate for the fiber-optic communication is documented in "706_RHP_FiberOpticCommIntegrity_00.doc". Details to the calculation can be found in this document.

The residual failure rate is determined to $8.8 \cdot 10^{-16} \text{ h}^{-1}$.

This value is much less 1 % of SIL 3 and therefore the bus system can be neglected for further calculation.

The determination of the safety parameter for the safety function realized by the Frame 8 of the PowerFlex 750 AC Drive has been done based on the following "Reliability Block Diagram":



The calculations have been performed considering the following prerequisites and assumptions:

- Source of the reliability data of the components: Siemens SN 29500.
- The failure rate data from the SIEMENS Standard SN 29500 is based on a maximum average temperature of 40°C. It is assumed, that the Test Object is mostly operated under these conditions although it is specified for operating at higher ambient temperatures.
- It is assumed that the failure rate of the components remains constant over the period of use and the early phase of higher failure rates has been passed when the systems goes into operation.
- It is assumed, that 50 % of all type B-component failures are in the safe direction and the remaining 50 % of the failures are in the unsafe direction. This assumption is in accordance with annex C of IEC 61508-6.
- Each detected failure results in a shut-down of the system (both or at least one OSSD off). Therefore the MTTR value (mean time to restoration) is set to 0 h.
- All external elements such as buttons, contacts, switches, valves, motors, etc. as well as external cabling were not considered within the failure rate calculation.
- For this system the Common Cause factors $\beta = 2 \%$ and $\beta_d = 1 \%$ were used.

The calculation was done by Rockwell and has been verified by the Test Institute.

The Proof test interval (PTI) is determined to 20 years. Within this time interval the values for PFD_{av} and PFH for the safety circuit for realization of the safety function "Safe Torque Off" within the frame 8 of the PowerFlex 750 AC Drive are as follow:

$$PFD_{av} = 3.5 \cdot 10^{-4}$$

$$PFH = 4.1 \cdot 10^{-9} \text{ 1/h (calculated according to IEC 61508)}$$

$$MTTFD = 88 \text{ high}$$

$$DCav = 98 \% \text{ (medium)}$$

The frame 8 of the PowerFlex 750 AC Drive can be used with the safety options "Safe Speed Monitor Option S1" and "Safe Torque Off Option S". By using these option the safety parameter for PFD_{av} and PFH are as follow:

PowerFlex 750 AC Drive Frame 8 with Safety option "Safe Torque Off Option S"

$$PFD_{av} = 3.81 \cdot 10^{-4}$$

$$PFH = 4.46 \cdot 10^{-9} \text{ 1/h}$$

PowerFlex 750 AC Drive Frame 8 with Safety option "Safe Speed Monitor Option S1"

$$PFD_{av} = 5.83 \cdot 10^{-4}$$

$$PFH = 6.75 \cdot 10^{-9} \text{ 1/h}$$

The results are summarized within the appended page (SIL-Sheet).

Result: The safety parameters for SIL 3 according to IEC 61508 and PL e according to EN ISO 13849-1 are met for the PowerFlex 750 AC Drive Frame 8 using the safety options "Safe Speed Monitor Option S1" and "Safe Torque Off Option S".

5. Summary

Based on the results of the inspection of the submitted documents and the test sample it can be confirmed that the product complies with the requirements of the relevant standards:

EN ISO 13849-1: Cat. 4 / PL e (Safe Speed Monitor Option-S1)
 EN ISO 13849-1: Cat. 3 / PL e (Safe Torque Off Optino-S)
 EN 61800-5-2: SIL 3
 EN 62061: SIL CL 3
 IEC 61508: SIL 3

Hence it is suitable for the use in applications up to PL e acc. to EN ISO 13849-1 and SIL 3 acc. to EN 62061 / IEC 61508 depending on the configuration and parameterization.

The instructions of the associated Installation and Operating Manual shall be considered.

Cologne, 2010-07-29
 TIS/ASI/Kst. 968-stf-nie

The expert

Report released after review
 Date: 2010-07-29



Dipl.-Ing. Thomas Steffens



Dipl.-Ing. Stephan Hüb