

2006-08-04



TÜV Rheinland Group

Automation, Software and Information Technology

**Report of the approval of SafeNet
and different changes of
Safety Manager**

**Report-No.: 968/EZ 195.03/06
Date: 2006-08-04**

**Report of the approval of SafeNet
and different changes of
Safety Manager**

Report-No.: 968/EZ 195.03/06

Date 2006-08-04

Pages: 8

Test objects: Safety Manager V110.2

Customer/Manufacturer: Honeywell Safety Management Systems
Rietveldenweg 32A
NL-5222 AR 's-Hertogenbosch
The Netherlands

Order-No./Date: Project 740105 dated 2005-09-20

Test Institute: TÜV Rheinland Industrie Service GmbH
Automation, Software and Information Technology
Competence Center Safeguards and Safety Components
Am Grauen Stein
D-51105 Köln

TÜV-Offer-No./Date: 968/175/05 dated 2005-09-06

TÜV-Order-No./Date: 9365358 dated 2005-09-29

Inspectors: Dipl.-Ing. Andreas Hesse
Dipl.-Ing. Gernot Klaes

Test location: see Test Institute and customer/manufacturer

Test duration: June 2006 to August 2006

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. Test object.....	5
3.1 History and test objects.....	5
3.2 Product and test documents	5
3.3 Test samples.....	5
3.4 Test reports and protocols	5
4. Approval of the SafeNet protocol	6
4.1 SafeNet	6
4.1.1 General remarks	6
4.1.2 Protection measures for SafeNet.....	6
4.1.3 Calculation of the residual error rate.....	6
4.1.4 Results of the inspection	7
4.2 Additional changes.....	7
4.2.1 Documentation of the changes	7
4.2.2 Assessment of the changes	7
5. Conclusion	8

1. Scope

In the following report the results of the approval of the safe protocol SafeNet and changes to the Safety-Manager are presented.

The report is based on the previous reports listed in chapter 3.4.

It is described, which tests were performed, who performed them and which results were obtained.

2. Standards forming the basis for the requirements

Functional Safety

- [S1] IEC 61508, Parts 1 - 7:2000 Functional safety of electrical/electronic/programmable electronic safety-related systems
- [S2] EN 954-1/1996 Safety of machinery, Safety related parts of control systems Part 1: General principles of design

Application specific

- [S3] EN 50156-1:2004 Electrical Equipment for Furnaces
- [S4] IEC 61511:2004 Safety Instrumented Systems for the process industry sector
- [S5] NFPA 72:2002 National Fire Alarm Code Handbook
- [S6] NFPA 85:2001 Boiler and Combustion Systems Hazards Code
- [S7] EN 54-2:1997 Fire Detection and Fire Alarm Systems Control and indicating equipment
- [S8] EN 54-4:2003 Fire Detection and Fire Alarm Systems
- [S9] EN 298:2003 Automatic gas burner control systems for gas burners and gas burning appliances with or without fans

Electrical safety and resistance against environmental conditions

- [S10] IEC 61131-2:2003 Programmable Controllers
- [S11] IEC 61010-1:2001 Safety requirements for electrical equipment for measurement, control, and laboratory use

Climate

- | | |
|--|----------------------|
| [S5] IEC 61131-2:2003 Programmable Controllers | |
| IEC 60068-2-1 Test Ab and Ad: Cold | (part of EN 61131-2) |
| IEC 60068-2-2 Test Bb and Bd: Dry heat | (part of EN 61131-2) |
| IEC 60068-2-14 Test N: Change of temperature | (part of EN 61131-2) |
| IEC 60068-2-30 Test Db: Damp heat, cyclic | (part of EN 61131-2) |
| IEC 60068-2-32 Test Ed. Free fall | (part of EN 61131-2) |

Shock/Vibration

[S5]	IEC 61131-2:2003 Programmable Controllers	
	IEC 60068-2-6 Test Fc: Vibration	(part of EN 61131-2)
	IEC 60068-2-27 Test Ea: Shock	(part of EN 61131-2)

EMC/EMI

[S5]	IEC 61131-2:2003 Programmable Controllers	
	EN 55011	(part of EN 61131-2)
	IEC61000-4-2, ESD	(part of EN 61131-2)
	EN 61000-4-3, RFI	(part of EN 61131-2)
	EN 61000-4-4, Burst	(part of EN 61131-2)
	EN 61000-4-5, Surge	(part of EN 61131-2)
	EN 61000-4-6, cond. RFI	(part of EN 61131-2)
	EN 61000-4-8, Magnetic	(part of EN 61131-2)

[S12] The German Safety Bus Committee: "Principle rules for test and certification of "bus systems for the transmission of safety relevant messages"
BG Fachausschuß Elektrotechnik GS-ET-26/05.02

3. Test object

3.1 History and test objects

In the initial certification of the Safety Manager documented in [T2] V 100.3 was reviewed.

After that some changes have been carried out to improve the systems' behaviour, which are reported in [T4], [T4].

In the next step the protocol SafeNet has been implemented to exchange data between Safety Managers in a safe way.

3.2 Product and test documents

The documentation has been provided to the Test Institute electronically on a CD.

The key document for SafeNet was the

[T1] SafeNet Whitepaper / Doc-No. FSC.WP.6481
Version: 1.1 dated 2006-07-13

Any change to the System has been documented in a Product Anomalie Report (PAR).

The document CDs are stored at the Test Institute.

3.3 Test samples

No test samples were required.

3.4 Test reports and protocols

[T2] Report of the type approval of Safety Manager; Report-No.: 968/EZ 195.00/05
Date: 2005-03-04

[T3] Report of the approval of different changes of Safety Manager;
Report-No.: 968/EZ 195.01/05, Date: 2005-07-15

[T4] Report of the approval of different changes of Safety Manager;
Report-No.: 968/EZ 195.02/05, Date: 2005-10-04

[T5] Test Result of Fault Insertion Test for SafeNET
Rev. 1.2 dated 2006-07-20

4. Approval of the SafeNet protocol

4.1 SafeNet

4.1.1 General remarks

SafeNet is a high-level protocol for safe data exchange between several Safety Manager PLC via various physical layers.

The basic concept is that a Safety Manager packs its safety relevant data into a special protocol, which is protected by several measures listed in chapter 4.1.2.

The protected data will be transferred to the communication module, which sends the data over a physical layer.

4.1.2 Protection measures for SafeNet

The protection mechanisms are the following:

- CRC32 over data
- Double transmission of data with cross comparison
- Sequence number of messages
- Sender and receiver address
- Timeout
- Age Timer

The Safety Managers must receive at least one healthy message within a configured timeout.

4.1.3 Calculation of the residual error rate

The residual error rate has been calculated by the manufacturer with the following assumptions:

- maximum number of bytes per message: 2000
- maximum number of safety relevant messages per second: ≤ 10
- maximum number of number of safety relevant nodes: ≤ 62
- bit error probability: 10^{-2}
- hamming distance of the used CRC polynomial: 4 to 5 (depending on the block size)

The calculation were reviewed by the Test Institute and discussed with the manufacturer.

It has been shown that the residual error rate is less than 1 % of SIL 4.

The results were accepted by the Test Institute.

4.1.4 Results of the inspection

The implemented safety measures for SafeNet provide sufficient protection of safety relevant data according to [S12].

The effectiveness of the measures has been verified partially together with the manufacturer at his premises.

The results are documented in [T5].

All implemented faults have been detected and failure messages were generated as expected.

4.2 Additional changes

Since the last certification some changes had to be made.

4.2.1 Documentation of the changes

Each change has been documented in a PAR. The report contains information about:

- Reason of change
- Impact analysis
- Test result (if required).

The documents contain the necessary information to understand the reason for change.

The way of documentation fulfils the requirements of IEC 61508.

4.2.2 Assessment of the changes

Most of the changes were carried out to increase availability. Only 1 item has been found, that may affect safety.

All items were solved either by change of the software or by description of a workaround. All items were retested.

The results are accepted by the Test Institute.

5. Conclusion

During the evaluation of the SafeNet and the additional changes for the Safety Manager no infringement of the functional and safety-related requirements in the applied standards could be found.

Therefore the Safety Manager can be used in safety related applications for SIL 1, SIL 2 or SIL 3 according to IEC 61508 or Category 1 to 4 according to EN 954-1.

Observance must be given to the installation conditions and application notes defined in the Operating and Instruction Manuals.

The additional requirements as listed in [T1] have to be taken into consideration.

Actual information about the certification status of the Safety Manager and actual releases of HW and SW components can be obtained from the homepage of the Test Institute. Please refer to the "List of type approved PES" published on: <http://www.tuvasi.com/>.

Cologne, 2006-08-04
TIS/ASI/Kst. 968 he-kg-nie

The inspectors

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

Dipl.-Ing. Andreas Hesse

A handwritten signature in blue ink that reads 'Gernot Klaes'.

Dipl.-Ing. Gernot Klaes