Certification
SpeedSys 200, SpeedSys300

Document Type	Technical Report
Client	Istec International BV Meer en duin 8 2163 HA Lisse Netherlands
Manufacturer	Mütec Instruments GmbH Bei den Kämpen 26 21220 Seevetal-Ramelsloh Germany
Authors	Dipl.-Ing. Wolfgang Velten-Philipp
Verifier	dr.ir. Michel Houtermans
Report	123.508.18 - Revision 1.2
Status	Released
Date	2021-04-27

Quality Assurance

Template	Date	Status
QMT4-1	2020-04-08	Released

Authors

Revision	Date	Authors	Reviewers	Assessors
0	2021-03-14	WVP		
1	2021-03-23	WVP	MH	MH
1.1	2021-04-19	WVP	MH	MH
1.2	2021-04-27	WVP	MH	MH

Document History

Revision	Date	Description
0	2021-03-14	initial
1	2021-03-23	release after review
1.1	2021-04-19	introduced SC2 for SpeedSys 200
1.2	2021-04-27	Manufacturer added on title page

Contents

List of Tables

List of Figures

Terms and Definitions

Term	Definition
PFDG	Average PFD
PFSavg	Average probability to fail to safe state
SFF	Safe failure fraction
DC	Diagnostic coverage
SC	Systematic capability
Type A circuit	non complex circuitry (e.g. relays, transistors, discrete components)
Type B circuit	complex circuitry (e.g. micro controller, FPGA, ASIC)

Parties

About Istec International

Istec International was founded in 1973 and is a family owned business. The company offers systems and services for functional safety and advanced condition monitoring for heavy industrial equipment, and supports its customers with a team of highly certified and experienced experts.

About Mütec Instruments

Mütec Instruments was founded in 1970 and offers solutions for complex and safety critical problems. Mütec's team of highly experienced professionals and engineers works closely with each client to design a perfectly tailored solution and often forms a close and long-term working relationship with those customers.

About Risknowlogy

Risknowlogy was founded in 2002 and is a family owned business. We offer products, services,consulting, certification and training. Risknowlogy certifies hardware, software, solutions, sites,management systems, organisations, and professionals.

1 Introduction

1.1 Objective and scope

The objective of this report is to document the type approval according to IEC 61508, route 1 carried out for the SpeedSys 200, SpeedSys300 modules. Application of SpeedSys 200, SpeedSys300 is the measurement of turbine speed using speed probes that are not the scope of this type of approval. The target of the evaluation is SIL 2 according to IEC 61508, route 1. This target allows to use the device within applications according to IEC 61511 [1, 2].

1.2 Product description

The product subject to the evaluation is the SpeedSys 200, SpeedSys300 . Figure 1 shows the products.

Figure 1: SpeedSys 200, SpeedSys300

The SpeedSys 200, SpeedSys300 measures the time between input pulses from connected speed probes. The input circuitry is galvanic isolated from the controller part. The time between the detected input pulses is converted into speed and acceleration values.
The speed and acceleration values can be compared to limit values, triggering a safety relay action. The calculated speed value is additionally converted into a safety relevant 4..20mA signal.
The SpeedSys 200, SpeedSys300 is configurable by parametrisation in the associated software.

SpeedSys 200 and SpeedSys300 have similar circuits. The SpeedSys300 owns a read-only RS485 (Modbus RTU) and a proof test input/output interfacing.

The versions of SpeedSys 200, SpeedSys300 available for safety related use are listed by Table 1.

Table 1: SpeedSys 200, SpeedSys300 variants for safety related use

Hardware Version	0.14.0
Software Version	Master 1.20 (CRC 0x32fe) Slave 1.0 (CRC 0x5269)
Parameterisation Tool	1.0

1.3 Functional safety properties

The functional safety properties according to IEC 61508 are:

Safety function:

- Measure the frequency of the input signal with an accuracy of 0.05% and derive a speed value. SpeedSys 200, SpeedSys300 compares the speed with configurable limits and provides the status of the limits by use of the two relay outputs.
- Measure the frequency of the input signal with an accuracy of 0.05% and derive an acceleration value. Output of this safety function are the two relays with configurable alarm set points.
- Measure the frequency of the input signal with an accuracy of 0.05% and derive a speed value. Output of this safety function is the 4-20mA current signal. The accuracy of the 4-20mA output is 0.1% of the measured speed pulses.
- All safety functions are operating in "Low Demand Mode".

The safety manual [5] describes the different configurations of the device and also the different possible redundant use cases. In principle the following architectures are available:

- HFT 0: 1oo1, 2oo2, low demand mode, SIL 2
- HFT 1: 1oo2, 2oo3, low and high demand mode, SIL 3, only SpeedSys300

Note: Configurations with more redundancy are available but not listed here.
Scope of this report is the SIL2 (HFT 0) configuration.

2 Assessment Results

2.1 Functional safety management

Mütec is an ISO 9001:2008 certified company [6] and has a certified functional safety management system [7]. Their quality system is also compliant with the ATEX directive [8].
Mütec followed their certified functional safety management system to assure that the development was carried out in line with the functional safety requirements according to IEC 61508. The functional safety management system requires a functional safety plan [9]. The required systematic capability for hard- and software development is SC3 for SpeedSys300 and SC2 for SpeedSys 200. The measures to avoid systematic failures during the hard- and software development are detailed by the tables from IEC 61508-2, Annex B and IEC 61508-3, Annex A, B. The measures are described in document [10].

Results

The functional safety plan [9] and the verification plan [11] describe the life cycle and the necessary activities. Risknowlogy performed a life cycle audit during the project to verify that the measures to avoid systematic failures during hard- and software development are applied. The lifecycle audit [12] did not lead to objections. The measures applied are suitable for SC3 for SpeedSys300 and SC2 for SpeedSys 200.
Note: SC3 allows to use SpeedSys300 for SIL 3 applications in redundant configurations. This is not dedicated for SpeedSys 200.

2.2 System architecture

The system uses a 1oo1 single channel architecture with diagnostics. The design uses two microcontrollers to enable galvanic isolation between the input and output side. Figure 2 shows the basic principle of the device.

For SIL 2 the Safe Failure Fraction (SFF) shall exceed 90% in case of a hardware fault tolerance of zero. For the following diagnostics are implemented to achieve this target:

- Redundant input circuits, pulse discriminators and compare of measured pulse counts.
- Redundant relay outputs.
- Microcontroller self test (RAM ROM, test of calculation units, stack supervision, logical sequence).
- Watchdog and second independent shut down path.
- Feedback of the 4-20mA current and shut down path for the current.
- Interrupt supervision.

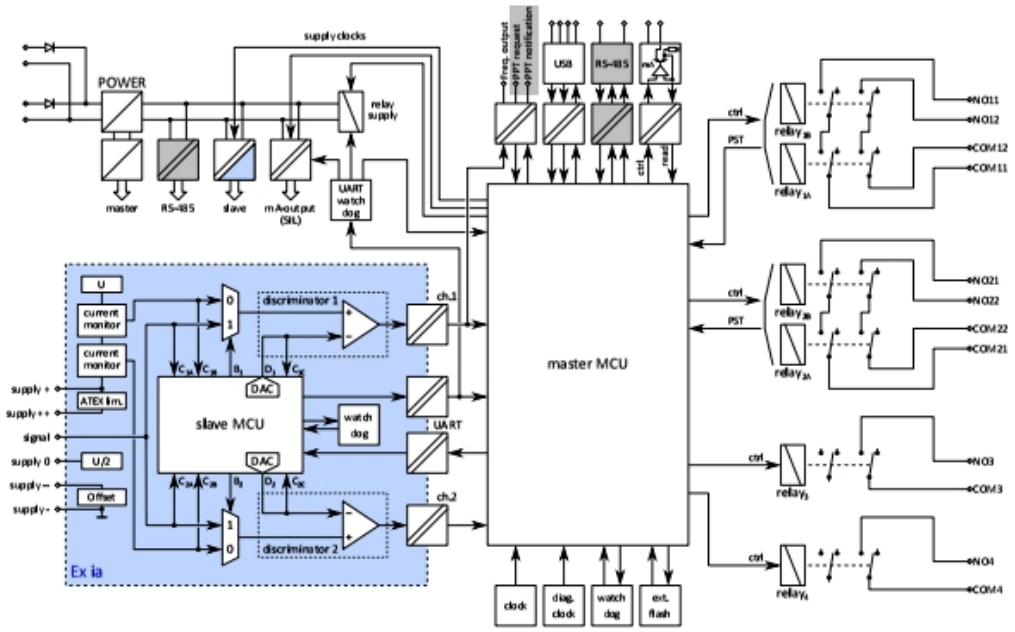

Figure 2: Architecture of SpeedSys 200, SpeedSys300

Results

The architecture is decribed by the SRS [13] and the more detailed description [14].
The diagnostic measures mentioned before are sufficient to provide a diagnostic level which is sufficient for a SFF of more than 90%. The effectiveness of the measures have been demonstrated during fault injection testing.

2.3 Reliability Analysis (FMEDA)

A failure mode and effect analyse (FMEDA) in line with the requirements of the IEC 61508 standard was carried out [15]. The FMEDA uses the component failure rates from SN29500 [3] and the failure models from IEC 62061: 2005, Annex D [4]. For the analyses environmental temperatures of 40 °C and 60 °C were assumed.

Table 2 presents a summary of the reliability data derived from the FMEDA.
Figure 3 and Table 3 are showing the average PFD (PFDG) results depending from the intended proof test intervals.

Table 2: Functional safety data for SpeedSys 200, SpeedSys300

Properties	40 °C 3-wire	2-wire	60 °C 3-wire	2-wire
Safe failure rate	479	479	944	944
Dangerous detected failure rate	608	615	1305	1320
Dangerous undetected failure rate	28	39	59	82
SFF	97%	97%	97%	97%

Notes:
Failure rates are in FIT $10^{-9}1/h$.
3-wire voltage and current sensor
2-wire voltage sensor

Table 3: PFDG for SpeedSys 200, SpeedSys300 , 2-wire voltage sensor

Proof Test (Years)	1	5	10	20
PFDG(40 °C, MTTR 72h)	2.1E-4	8.9E-4	1.7E-3	3.4E-3
%SIL 2	2%	9%	17%	34%
PFDG(60 °C, MTTR 72h)	4.6e-4	1.9E-3	3.7E-3	7.3E-3
%SIL 2	5%	19%	37%	73%

Table 4: PFDG for SpeedSys 200, SpeedSys300 , 3-wire voltage and current sensor

Proof Test (Years)	1	5	10	20
PFDG(40 °C, MTTR 72h)	1.7E-4	6.6E-4	1.3E-3	2.5E-3
%SIL 2	2%	7%	13%	25%
PFDG(60 °C, MTTR 72h)	3.5E-4	1.4E-3	2.7E-3	5.3E-3
%SIL 2	4%	14%	27%	53%

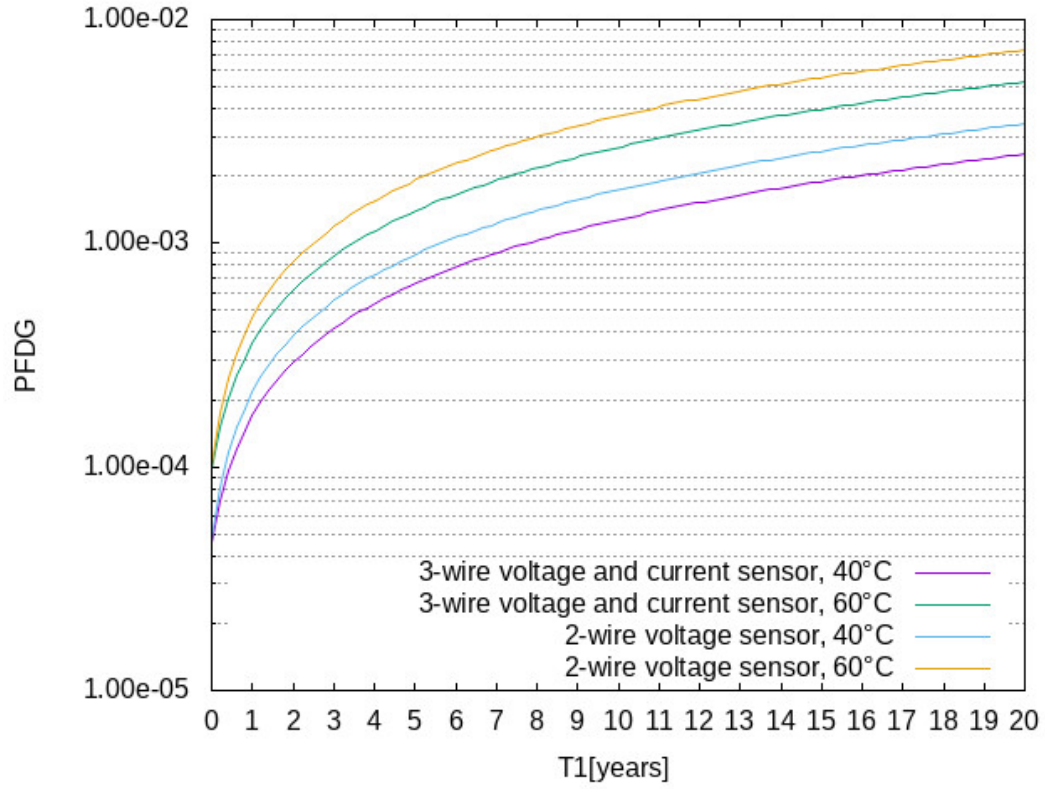

Figure 3: PFDG for SpeedSys 200, SpeedSys300

2.4 Hardware test and fault injection test

Hardware tests were performed by Mütec and reviewed by Risknowlogy. The tests are using fault models which are defined by ISO 13849-1 and IEC 61508 (DC fault model). The fault models are covering component failures (open, stuck-at, drift), failures of power supplies and references (under- and over voltages), sensor failures etc. The tests were planned by test plans and documented by test reports [16], [17].

Results

All tests passed without objections. The effectiveness of the diagnostic measures were confirmed by the tests.

2.5 Software development and software test

The software development was performed according to the measures which were defined by IEC 61508-3, Annex A for SIL2/SIL 3. During the software development Mütec performed software reviews to confirm the measures and to review the code. The MISRA-C coding rules [18] were applied and static code analyses [19] were performed.

Results

The software development process was reviewed by Risknowlogy and a life cycle audit was performed. The development tools are described and classified by document [20]. The software development process is suitable up to SIL3 and the effectiveness of the diagnostic measures are confirmed by the test results.

2.6 Parameterisation

For parametrisation the software "Parameter Software, Version 1.00" is used. The program is connected by a serial interface to SpeedSys 200, SpeedSys300 . The parameter setting can be accessed after submitting a password. The software has different access/read/write levels and supports a parameter verification process [21].

Results

The requirements of IEC 61508 and IEC 61511 for the parameterisation of safety related equipment are fulfilled.

2.7 EMC, Basic Safety and Environmental Testing

The product complies [22] with

- EMC directive 2014/30/EU
- ATEX directive 2014/34/EU
- LVD directive 2014/35/EU

3 User Documentation

The safety manual [5] provided by Istec provides all necessary information for usage of the product. The safety manual was reviewed without any objections.

4 Conclusions

The evaluation documented in this report demonstrates that the specified safety function of SpeedSys 200, SpeedSys300 , used in HFT=0, is suitable for SIL 2 safety properties according to IEC 61508, route 1 and IEC 61511.

Risknowlogy

Wolfgang Velten-Philipp
Author

dr.ir. Michel Houtermans
Verifier

5 Standards

[1] IEC 61508: 2010
Functional safety of electrical/electronic/programmable electronic safety related systems.

[2] IEC 61511: 2016
Functional safety: Safety instrumented systems for the process industry sector.

[3] SN29500: 2013
Failure Rates of Components.

[4] IEC 62061: 2005, Annex D
Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems.

6 References

[5] MSSY00039-nr-SpeedSys300 - Functional Safety Manual.

[6] ISO 9001: 2008 Certificate, A1047GER, 2017-08-28, QAS International.

[7] FSM Certificate, 123.202.07, 2016-06-13, Risknowlogy.

[8] MSSY00034-10-IBExU19ATEX1121_N0_SSY200300_en
MSSY00034-10-IECEx_IBE_19.0030_000_signed
MSSY00034-10-IB-19-3-0155_Pruefberich_SSY200300.

[9] MSSY00001-02-SpeedSys300 - Safety Plan
MSSY00002-03-SpeedSys300 - Roles and responsibilities.

[10] MSSY00008-05-SpeedSys300 - Failure Control.

[11] MSSY00003-03-SpeedSys300 - Verification Plan.

[12] FSM_Audit_20210216.

[13] MSSY00012-06-SpeedSys300 - SRS.

[14] MSSY00018-07-SpeedSys300 - Hardware Concept.

[15] Summary_FMEA_20210307.

[16] Hardware test documentation
MSSY00019-02-SpeedSys300 - Hardware Test Plan
MSSY00026-02-SpeedSys300 - Hardware Test Protocol
SSY300_schematic_FIT_comment.

[17] HW/SW Integration test
MSSY00017-05-SpeedSys300 - HWSW Integration Test Plan
MSSY00028-01-SpeedSys300 - HWSW Integration Test Protocol.

[18] MDGL00058-10-C-coding guideline.

[19] Code Analyse
MSSY00025-01-SpeedSys300 - Static code analysis report
MSSY00040-01-SpeedSys300 - Code Coverage Protocol.

[20] MSSY00009-03-SpeedSys300 - Tools List.

[21] MSSY00020-07-SpeedSys300 - Software Concept.

[22] MSSY00032-00-SpeedSys300 - EMC test report (20025-1-R00)
MSSY00034-10-IBExU19ATEX1121_N0_SSY200300_en
MSSY00034-10-IECEx_IBE_19.0030_000_signed
G0M-2002-8842-SCM001X-V001
DE-6-G5210004_CB Cert.

[23] Schematics
SSY300_schematic_0140.

[24] Software test documentation
MSSY00021-03-SpeedSys300 - Software Test Plan
MSSY00027-02-SpeedSys300 - Software Test Protocol.