

SIL Certification of SpeedSys 200, SpeedSys 300, SpeedSys300

Document type:	Certification report
Client:	Istec International BV, Netherlands
Manufacturer:	Mütec Instruments GmbH, Germany
Project:	SIL Certification SpeedSys
Report number:	18.508.18
Revision:	3
Status:	Released
Date:	2023-12-07

© Copyright Risknowlogy® - All Rights Reserved.

LIMITATION OF LIABILITY - This report was prepared using best efforts. Risknowlogy does not accept any responsibility for omissions or inaccuracies in this report caused by the fact that certain information or documentation was not made available to us. Any liability in relation to this report is limited to the indemnity as outlined in our Terms and Conditions. A copy is available at all times upon request.

This document is the property of, and is proprietary to Risknowlogy®. The client has the right to duplicate this document in whole and to distribute it in whole. Third parties do not have the right to disclose in whole or in part and no portion of this document shall be duplicated by any third party in any manner for any purpose without Risknowlogy's expressed written authorisation.

Version Control

Quality Assurance

QMT4-2 - 2020-04-26 - Released

Author(s)

Revision	Date	Author(s)	Reviewer(s)	Approver
3	2023-12-07	Michel Houtermans	Ricardo Vittonic	Frank Kozole

Document History

Revision	Date	Description
0	2021-03-14	Original issue
1	2012-03-23	Release after review
1.1	2021-04-19	Introduced SC2 for SpeedSys 200
1.2	2021-04-27	Manufacturer added on title page
2	2023-06-12	Updated report template and added Modification 1
3	2023-12-07	Added SpeedSys 300 marketing name

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 Müttec Instruments

Müttec Instruments was founded in 1970 and offers solutions for complex and safety critical problems. Müttec'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, coaching, certification and training to business operators. Risknowlogy certifies hardware, software, solutions, sites, management systems, organisations, and professionals according to international standards.

Table of Contents

Version Control	3
Parties	4
About Istec International	4
About Müttec Instruments	4
About Risknowlogy	4
Table of Contents	5
List of Figures	6
List of Tables	6
Terms and Definitions	7
1. Introduction	8
1.1. Purpose	8
1.2. About the Project	8
1.3. Certification basis	8
1.4. Certification scope	8
1.5. History	9
2. Product Description	10
2.1. About the SpeedSys	10
2.2. Safety functions and functional safety parameters	11
3. Certification results	12
3.1. Functional safety management	12
3.2. Product architecture	12
3.3. hardware evaluation	13
3.4. Hardware test and Fault Injection tests	14
3.5. Software development and software test	14
3.6. Parameterisation	15
3.7. Basic safety evaluation	15
3.8. User documentation evaluation	15
4. Conclusions	16
4.1. End user responsibilities	16
4.2. Modifications	16
4.3. Conclusions	16
References	17
Appendix A - Modifications	19
Modification 1	19

List of Figures

Figure 1 - The SpeedSys 200 (l) and SpeedSys300 (r)	10
Figure 2 - Architecture of SpeedSys	12

List of Tables

Table 1 - SpeedSys Products subject to this certification	11
Table 2 - Hardware integrity evaluation for safety function #1.	13
Table 3 - Reliability Analysis - SpeedSys - 2-wire voltage sensor	14
Table 4 - Reliability Analysis - SpeedSys - 3-wire voltage and current sensor	14

Terms and Definitions

Term	Definition
DC	Diagnostic coverage
DD	Dangerous detected failure rate
DU	Dangerous undetected failure rate
NE	No effect failure rate
PFDG	Average probability of failure on demand
PFSavg	Average probability of fail safe
SC	Systematic capability
SD	Safe detected failure rate
SFF	Safe failure fraction
SIL	Safety integrity level
SU	Safe undetected failure rate

1. Introduction

1.1. Purpose

The purpose of this report is to document the functional safety certification of the SpeedSys 200, SpeedSys 300, and SpeedSys300 modules. The certification process is carried out to demonstrate that these products meet the applicable SIL requirements according to IEC 61508 [1] and can be used according to IEC 61511 [2].

1.2. About the Project

ISTEC International is the owner of the product. Müttec Instruments is the designer and manufacturer of the products. These products are used in the industry as part of safety (instrumented) functions according to IEC 61508 [1], IEC 61511 [2] and other functional safety standards.

1.3. Certification Basis

The following standard(s) have been used as the basis for the certification:

- ▶ IEC 61508 - Functional safety of E/E/PE safety-related systems [1].
- ▶ IEC 61511 - Functional safety: Safety instrumented systems for the process industry sector [2]

1.4. Certification Scope

The certification scope of Risknowlogy, as agreed upon with the client, is limited to the product(s) listed in Chapter 2 and addresses the following subject matters:

- ▶ Management of functional safety;
- ▶ Safety requirements specification;
- ▶ Hardware requirements (and embedded software where applicable);
- ▶ Hardware reliability;
- ▶ Fault injection testing;
- ▶ Software;
- ▶ Basic safety;
- ▶ User documentation;

Everything else is excluded from the certification scope.

1.5. History

The original certification took place in 2021.

Modification 1 has been added in 2023.

2. Product Description

2.1. About the SpeedSys

The product(s) subject to certification are identified as SpeedSys 200, SpeedSys 300 and SpeedSys300 and are referred to as SpeedSys in this report. Figure 1 shows the SpeedSys 200 and SpeedSys300. The SpeedSys is used to measure turbine speed using speed probes. The speed probes are not within the scope of this certification.



Figure 1 - The SpeedSys 200 (l) and SpeedSys300 (r)

The SpeedSys measures the time between input pulses from the 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 is configurable by parametrisation in the associated software.

SpeedSys 200 and the SpeedSys 300 and SpeedSys300 have similar circuits. The SpeedSys 300 and SpeedSys300 adds, in addition, a read-only RS485 (Modbus RTU) and a proof test input/output interface.

The SpeedSys products and their versions available for safety-related use are listed in Table 1.

Table 1 - SpeedSys Products subject to this certification

Products	Hardware	Software	Parameterisation Tool
SpeedSys 200	1.0.0	Master 1.20 (CRC 0x32fe) Slave 1.0 (CRC 0x5269)	1.0
SpeedSys 300 / SpeedSys300	1.0.0	Master 1.20 (CRC 0x32fe) Slave 1.0 (CRC 0x5269)	1.0

2.2. Safety Functions and Functional Safety Parameters

The SpeedSys carries out three safety functions [13]:

1. Measure the frequency of the input signal with an accuracy of 0.05% and derive a speed value. The SpeedSys compares the speed with configurable limits and provides the status of the limits by use of the two relay outputs.
2. 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.
3. 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.

The implementation of the above safety functions takes into account the following functional safety parameters:

- ▶ Type B
- ▶ Low demand
- ▶ Hardware fault tolerance is 0
- ▶ SIL is 2

3. Certification Results

3.1. Functional Safety Management

Mütec Instruments, the designer and manufacturer of the SpeedSys, holds a valid Functional Safety Management certificate [7] according to the requirements of IEC 61508 [2]. The SpeedSys products have been designed according to the Functional Safety Management system.

3.2. Product Architecture

The SpeedSys uses a 1oo1 single-channel architecture with diagnostics [13]. The design uses two microcontrollers to enable galvanic isolation between the input and output sides. Figure 2 shows the basic principle of the device.

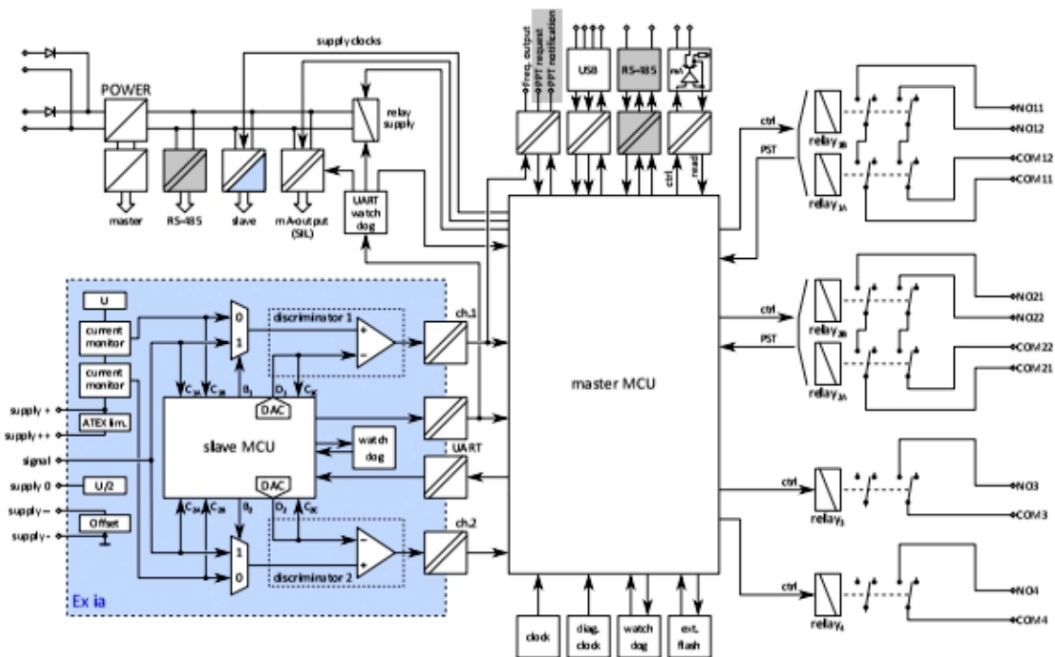


Figure 2 - Architecture of SpeedSys

For SIL 2, the Safe Failure Fraction (SFF) must 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 comparison 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 shutdown path for the current.
- Interrupt supervision.

Results

The architecture is described in the SRS [13] and a more detailed description in [14]. The diagnostic measures mentioned before are sufficient to provide a diagnostic level which is that achieves an SFF of more than 90%. The effectiveness of the measures has been demonstrated during fault injection testing.

3.3. Hardware Evaluation

A failure mode and effect analyse (FMEDA) were carried out [15] in line with the requirements of the IEC 61508 standard. The FMEDA uses the component failure rates from SN29500 [3] and the failure models from IEC 62061: 2005, Annex D [4]. Environmental temperatures of 40 °C and 60 °C were assumed for the analyses. Table 2 presents a summary of the reliability data derived from the FMEDA.

Table 2 - Hardware integrity evaluation for safety function #1.

#	Product	SD ¹	SU ¹	DD ¹	DU ¹	NE ¹	SFF
1	SpeedSys - 3 Wire - 40 °C	1	478	608	28	1568	97%
2	SpeedSys - 2 Wire - 40 °C	1	478	615	39	1571	97%
3	SpeedSys - 3 Wire - 60 °C	3	942	1304	59	2978	97%
4	SpeedSys - 2 Wire - 60 °C	3	942	1320	82	2986	96%

¹) Values are in FIT, 1 FIT = 1e-9 failures per hour

Table 3 and Table 4 show the average PFD (PFDavg) results based on different proof test intervals and for the different temperature ratings.

Table 3 - Reliability Analysis - SpeedSys - 2-wire voltage sensor

T1 (y)	1	2	5	10	20
PFDavg - 40°C	2.13E-04	3.82E-04	8.88E-04	1.73E-03	3.42E-03
% SIL 2	2.13%	3.82%	8.88%	17.30%	34.20%
PFDavg - 60°C	4.56E-04	8.17E-04	1.90E-03	3.70E-03	7.31E-03
% SIL 2	4.56%	8.17%	19.00%	37.00%	73.10%

Table 4 - Reliability Analysis - SpeedSys - 3-wire voltage and current sensor

T1 (y)	1	2	5	10	20
PFDavg - 40°C	1.67E-04	2.89E-04	6.58E-04	1.27E-03	2.50E-03
% SIL 2	1.67%	2.89%	6.58%	12.70%	25.00%
PFDavg - 60°C	3.53E-04	6.12E-04	1.39E-03	2.68E-03	5.27E-03
% SIL 2	3.53%	6.12%	13.90%	26.80%	52.70%

3.4. Hardware Test and Fault Injection Tests

Hardware tests were performed by Mütéc and reviewed by Risknowlogy. The tests use fault models defined by ISO 13849-1 and IEC 61508 (DC fault model). The fault models cover 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 was confirmed by the tests.

3.5. 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, Mütéc 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 for SIL 3, and the effectiveness of the diagnostic measures is confirmed by the test results.

3.6. Parameterisation

The software "Parameter Software, Version 1.00" is used for parameterisation. The program is connected by a serial interface to the SpeedSys. 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.

3.7. Basic Safety Evaluation

The SpeedSys complies [22] with

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

3.8. User Documentation Evaluation

The safety manual [5] provided provides all the necessary information for correctly using the SpeedSys. The safety manual describes the device's different configurations and 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 SpeedSys 300 and SpeedSys300

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

The safety manual was reviewed without any objections.

4. Conclusions

4.1. End User Responsibilities

To achieve SIL-compliant safety (instrumented) functions, it is the end user's responsibility to correctly design the final solution taking into account the products listed in Table 1 of paragraph 2.1. Furthermore, it is the responsibility of the end user:

- ▶ To perform their functional safety analysis according to the applicable functional safety standard (e.g., IEC 61511, IEC 61508).
- ▶ To install, commission and validate (SAT) the products correctly;
- ▶ To operate, maintain and repair the products according to the instructions given by the supplier;
- ▶ To operate the products in an environment that does not exceed the limits presented in the user documentation.

4.2. Modifications

Future modifications by Istec/Mütec Instruments to the products listed in Table 1 of paragraph 2.1 must go through an IEC 61508 compliant modification procedure and are subject to re-verification, re-validation, re-assessment and re-certification. Modifications that require re-certification are documented in Appendix A of this report.

4.3. Conclusions

Risknowlogy concludes that the safety functions of the products listed in Table 1 of paragraph 2.1, summarised as SpeedSys, meet the SIL 2 requirements for route 1 according to IEC 61508 according to the certification basis, the certification scope and the safety requirements specification.

On behalf of Risknowlogy,



Wolfgang Velten-Philipp†, Dr. Michel Houtermans
Authors



Frank Kozole
Verifier

References

1. IEC 61508:2010 - Functional safety of electrical / electronic / programmable electronic safety-related systems
2. IEC 61511:2003 - 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 pro- grammable electronic control systems.
5. MSSY00039-nr-SpeedSys300 - Functional Safety Manual.
6. QAS International, ISO 9001: 2015 Certificate, A1047GER, Valid 2024-08-28, issued 2021-08-28.
7. Risknowlogy, Functional Safety Management Certificate. Number 123.202.7-2. Valid until 2024-08-11
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. Risknowlogy, Summary FMEA. Document 18.508.34, revision 2, 2023-04-24.
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.
25. Mutec, SpeedSys 200/300 – Modification Form - fuse F810 / transistor T192. Document
MSSY000xx, revision 0.1, 2023-16-03

Appendix A - Modifications

Modification 1

During production and usage in the field, two systematic failures were revealed.

The modification was performed according to the modification procedure of the certified FSM system [7]. The modification was documented in [15]. The failures were investigated, and two design changes were proposed.

The modification was documented according to the requirements of the FSM system [7] in the modification Form [25]. The proposed modification included two changes. One was the increase of resistance values for four resistors. The second modification was to add three clipping diodes to the design.

The impact analysis demonstrated that no software modifications were needed, and only the hardware design was affected. This resulted in a revaluation of the FMEDA [15]. The hardware modifications were minor and did not significantly impact the resulting failure rates. All related documentation was updated, and where necessary new tests were performed.

Risknowlogy reviewed the modification documentation for completeness and correctness. The safety functionality of the product did not change, and the implementation followed the modification procedure correctly.