Technical Report
MTP300i-SIL-*

Client: Mütec Instruments GmbH
Bei den Kämpen 26
D-21220 Seevetal-Ramelsloh
Products: MTP300i-SIL-*
Number: 4.139.18
Revision: 1.1
Date: 2013-08-17

Author(s): W. Velten-Philipp, Dr. M. Houtermans

Risknowlogy Germany GmbH
Unterreut 6
76135 Karlsruhe
Germany
www.risknowlogy.com

Revisions

Revision	Date	Who	Description
0	2013-07-15	WVP	Draft
1	2013-08-08	WVP	Release
1.1	2013-08-17	WVP	Minor modifications

Table of Contents

List of Tables

List of Figures

Terms and Definitions

Term	Definition
Dangerous failure	An internal failure that prevents the product from carrying out its safety function upon demand. See also safe failure
Detected failure	An internal failure that is detected by built-in diagnostics. Because of the diagnostics the product can act upon the failure. See also undetected failure
FMEDA	Failure mode, effects and diagnostics analysis
Functional safety	A product is functionally safe if random, systematic and common cause failures do not lead to malfunctioning of the system and do not result in injury or death of humans, spills to the environment, or loss of equipment or production
Hardware fault tolerance	Hardware fault tolerance indicates the number of failures the product or subsystem can withstand without losing the safety function
HFT	See hardware fault tolerance
PFD	The probability that the safety function has failed upon demand
PFS	The probability that the safety function causes a spurious trip of the process
Safe failure	An internal failure where a product carries out its safety function without a demand from the process. This failure can lead to a spurious trip. See also dangerous failure
Safety function	Function implemented in the product required to achieve a safe state of the process
SFF	Safe failure fraction
SIL	Safety Integrity Level
STL	Spurious Trip Level®
Type	The complexity of a product is designated by Type A or Type B. See IEC 61508, part 2, clause 7.4.3.1.2 and 7.4.3.1.3
Undetected failure	An internal failure that is not detected by built-in diagnostics. See also detected failure
FIT	Unit to express failure rates Failure in Time [FIT], 1 FIT = 10^{-9} /h

1 Introduction

1.1 Objective

The objective of this report is to document the IEC 61508, SIL 2 certification carried out for the Mütec MTP300i-SIL-* safety related temperature transmitter.
The MTP300i-SIL-* (* - TC type, e.g. K, E or J) is available in variants for different thermocouple linearization.

1.2 About Mütec

Mütec Instruments was founded in 1970 and offers solutions for complicated 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.
At Mütec Instruments, engineers do all the work from the initial concept to the finished product. This means that all new developments comply with the strictest criteria and have been optimized for performance and functionality.

1.3 About Risknowlogy

Risknowlogy is an international operating company that offers services, consulting, certification and training in the field of risk, reliability and safety. Risknowlogy was established in 2002 and has offices in Switzerland, Argentina, Germany, United Arab Emirates and The Netherlands. We consider the world as our work area and each location has obliged to maintain the same quality standards, rules, and business practices.
The headquarters of the Risknowlogy Corporation is located in Switzerland. Here we perform business development, market our products and services, create new products and services, train our employees and service any country in the world that is not serviced by a local organization.

1.4 Basis for testing

N1 IEC 61508: 2010 (ED 2)
Functional Safety of Electrical, Electronic, Programmable Electronic Safety Related Systems

N2 IEC 61511: 2003 (ED1)
Functional safety - Safety instrumented systems for the process industry sector

N3 SN 29000: 1996
Failure Rates of Components

2 Product Description

2.1 MTP300i-SIL-*

The product subject to the certification is the temperature transmitter MTP300i-SIL-*. The product is shown in Figure 1.

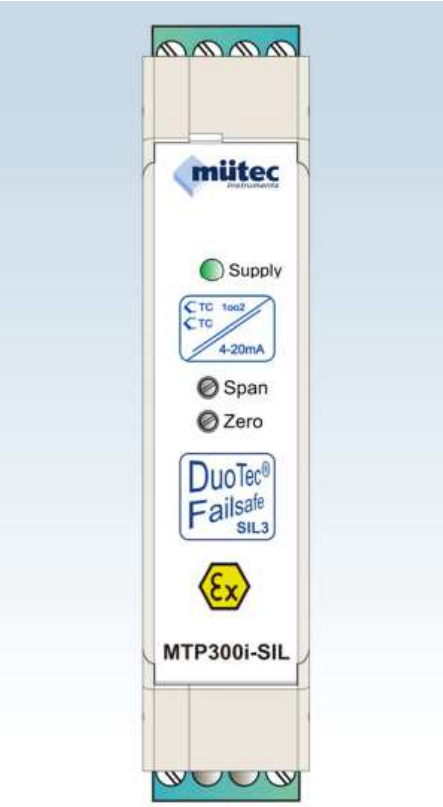

Figure 1 MTP300i-SIL-*

Main area of application for the product is safety related temperature measurement in explosive environment.

The safety function according to IEC 61508 is:

- Measurement of the temperature within an safety accuracy of 5% of the maximum value
- The signal pass-trough time is 2ms without filter or 38ms with Butterworth filter.
- Safe state of the output signal is a current below 3.6mA

The safety integrity level according to IEC 61508 is SIL 2. The safety function is a low demand mode function.

2.2 Architecture

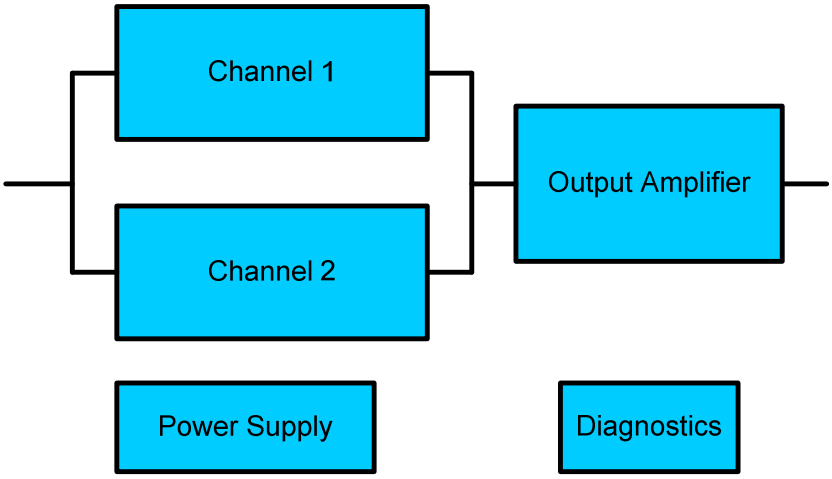

Figure 2 MTP300i-SIL-* architecture

The MTP300i-SIL-* consists of two independent measurement channels and cold-junction temperature compensation. The input channels are galvanic isolated from the output stage. The diagnostic circuit supervises power supplies, amplifier parameters and compares the two measured temperature values.
In case of failures the output current goes below 3.6 mA.
The diagnostic circuit of MTP300i-SIL-* uses a microcontroller to perform the diagnostics. The microcontroller is also responsible for the TC linearization. The linearization itself does not impact the safety function.

Target of the evaluation is SIL 2. The safety function of the device is performed by Type A components, the requirements for the SFF (IEC 61508-2) are < 60% per channel and 60%-90% for the single channel part.

3 Evaluation Results

3.1 Functional safety management

Mütec is an ISO 9001:2008 certified company [4]. Their quality system is also complaint with the ATEX directive [5]. Mütec implemented a project based functional safety management system to assure that the development was carried out in line with the management of functional safety requirements according to IEC 61508. This project based functional safety management system is described in the safety plan [1].
The safety plan describes the lifecycle phases, the managerial and technical activities to avoid systematic failures during the project, the people responsible for carrying out and documenting these activities. Supplementary a verification and validation plan [7] describes when and who will carry out which verification activities.
Risknowlogy reviewed the two documents for completeness and correctness. The review of the documentation did not lead to any objections.

3.2 Software

Software is involved to perform the diagnostics for the two channels:

- Compare of the two analogue values for 2.5% difference
- Detection of sensor or cable interruption
- Supervision of cold junction temperature sensors
- Supervision of power supplies
- Supervision of clock frequency
- Supervision of output current
- Feedback of the shut down path

The microcontroller itself is supervised by a hardware watchdog circuit which realises an independent shut down path.

The software documentation [11] was reviewed without objections.

3.3 Hardware

The basic measure to control the effects of random hardware failures is the 1oo2 architecture for the temperature measurement. The temperatures are compared by a microcontroller which shut down the output in case of discrepancy or other detected failures.

3.4 Reliability analysis

A qualitative and quantitative FMEDA analysis [3] was carried out to analyze the failure behaviour and the effectiveness of the measures to control failures. The failure rates for the different blocks from the FMEDA were used to calculate the PFD for the MTP300i-SIL-*.
The following is an overview of the functional safety characteristics of the product:
The SFF for the different blocks for the system exceeds the target values for the required SIL (SFFavg 93%). The architectural constraint for fault tolerance and SFF complies with IEC 61508-2.

The following table represents the overall calculation result for the PFD value using a MTTR of 72h and a beta factor of 2% which was derived from IEC 61508-6, Annex D.

Table 1 Average probability of failure on demand

T1	**1**	**2**	**5**	**10**	**15**	**20**
PFDG	5,63E-05	1,11E-04	2,77E-04	5,54E-04	8,30E-04	1,11E-03
%SIL2	0,56%	1,11%	2,77%	5,54%	8,30%	11,07%

T1: Proof Test Interval in years

The average probability to fail safe PFSavg(1Y) is 2.63E-5.

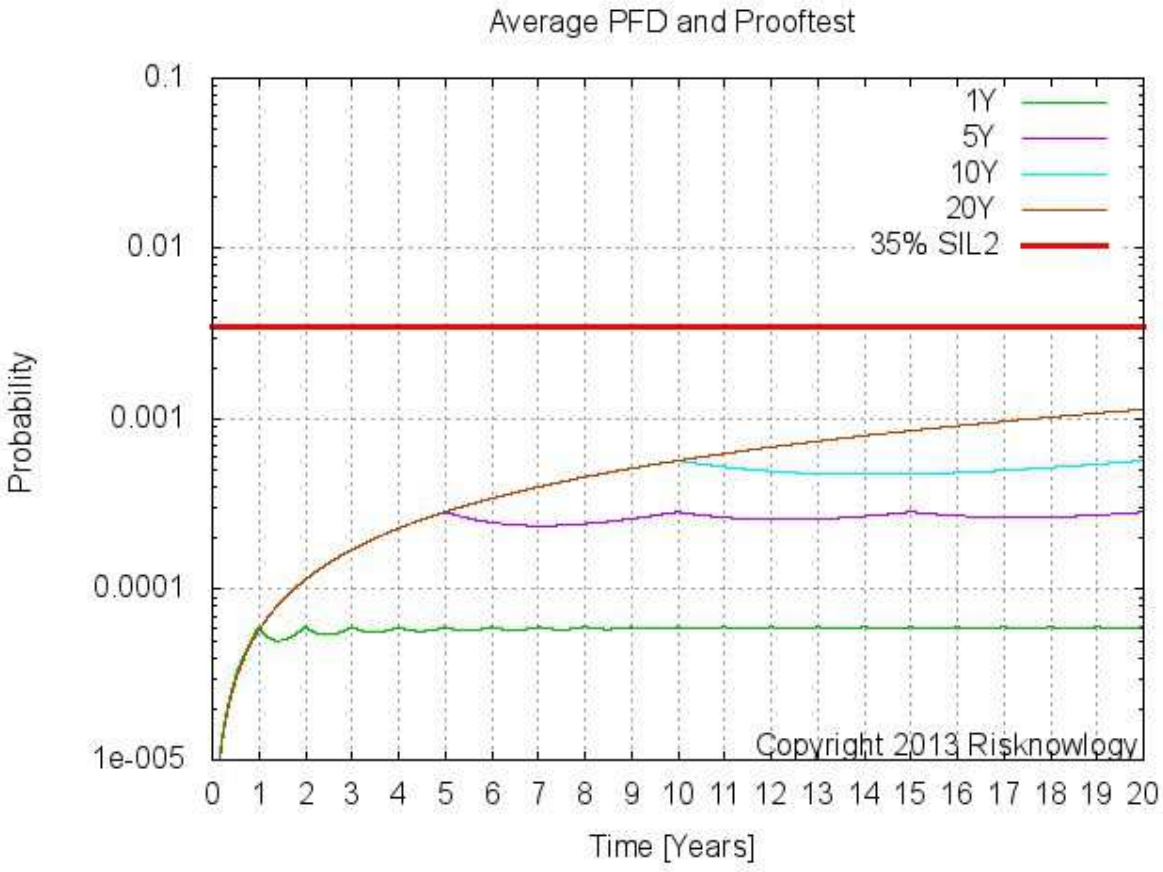

Figure 3 PFDG of MTP300i-SIL-*

3.5 Fault Injection Test

Fault injection testing was carried out to simulate the effects of all relevant failures. The failure effects and the related diagnostic measures were compared with the assumptions used for the FMEDA.
The fault injection test [8] was passed without objections.

3.6 Product Safety

The product complies to EN 60079-0 and EN 60079-11 and fulfils the ATEX Directive 94/9/EG [6].
The requirements for basic product safety are thus fulfilled.

3.7 EMC

EMC testing was carried out according to EN 61000-6-3: 2007 for emission and EN 61326-3-2: 2008 for immunity.
The EMC tests are suitable for a safety related device used in the process industry.

3.8 User Documentation

The user documentation [10] contains the necessary information for use of the product in safety related environments.

4 Conclusion

The MTP300i-SIL-* is suitable for safety related function up to SIL 2 according to IEC 61508 and IEC 61511.

5 References

The following references have been used during the project:

1. Safety Plan, rev 1.1, 2013-06-15, Mütec Instruments GmbH
2. Circuit Diagram
   Schaltung_GP_MTP300i_SIL, Rev 2.4
   Schaltung_ASP_MTP300i_SIL, Rev 2.0
   Stückliste_MTP300i_SIL_ASP, Rev 2.0
   Stückliste_MTP300i_SIL_GP, Rev 2.3
3. FMEDA, FMEA-Muetec_MTP300i_WVP_2013-07-09, Risknowlogy GmbH
4. ISO 9001: 2008 Certificate, A1047GER, QAS International
5. ATEX BVS 12 ATEX ZQS /E164, 2012-02-02, Dekra Exam GmbH
6. ATEX Certificate BVS 08 ATEX E 082 X, 2013-04-24, Dekra Exam GmbH
7. V&V Plan, rev 1.1., 2013-07-18, Mütec
8. Fault Injection Test Protocol FIT-Muetec_MTP300i_WVP_2013-07-09
9. EMC Test report No 10/1133-1, TÜV Nord
10. User Data Sheet 3001210_en, 2013-07, Mütec
11. Software documentation
    MTP300i-SIL_src_20130513
    I_Diff_Check.pdf
    I_Mirror_Check.pdf
    MAIN_LOOP.pdf