RISKNOWLOGY
Experts in Risk, Reliability, Safety and Security

Technical Report
Reliability Analyses

Client: Mütec Instruments GmbH, Seevetal-Ramelsloh, Germany
Product(s): MSK200…, MTP200…
Number: 123.101.2
Version: 1.2
Date: 2013-05-28

Author(s): Dr. M.J.M. Houtermans

Risknowlogy B.V.
Brunner bron 2
6441 GX Brunssum
The Netherlands
www.risknowlogy.com

RISKNOWLOGY
Experts in Risk, Reliability, Safety and Security

Client: Mütec Instruments GmbH, Seevetal-Ramelsloh, Germany
Product(s): MSK200…, MTP200…
Number: 123.101.2
Version: 1.2
Date: 2013-05-28

Author(s): Dr. M.J.M. Houtermans

Revision History

Revision	Date	By	Reason
1.0	2005-06-10	MH	First release
1.1	2006-09-08	MH	Updated STL, MTTF, DDC, Type
1.2	2013-05-28	WVP	Update of safety function definition

Summary

Mütec Instruments has requested Risknowlogy to carry out a reliability study on the products MSK200 and MTP200. Risknowlogy has carried out an FMEA and Markov study to determine the most important reliability properties of the product. These studies have been carried out following the rules of IEC 61508 and 61511.

To fully understand the calculation results it is necessary to read the complete report. Table 1 summarizes the functional safety results. Table 2 and Table 3 summarize the results for sample calculations that have been carried out on the following reliability properties:

- PFD: The probability that the safety function has failed upon demand
- PFDavg: The average probability that the function has failed upon demand
- PFS: The probability that the safety function causes a spurious trip of the process
- FO: The probability that the product has failed but can still carry out its function
- AV: The probability that the function of the product is available
- UP: The probability that the product is running without any internal failures

Table 1 – Functional safety summary results

Properties	MSK200	MTP200
Mixed type	B	B
Hardware fault tolerance	0	0
Safe failure fraction	91.6%	90.1%
Safe detected failure rate [1/h]	8.59E-07	8.75E-07
Safe undetected failure rate [1/h]	1.27E-06	1.15E-06
Dangerous detected failure rate [1/h]	6.86E-07	1.11E-06
Dangerous undetected failure rate [1/h]	2.59E-07	3.47E-07
Dangerous diagnostic coverage	72.6%	76.2%
MTTFd [y]	120.7	78.5
MTTFs [y]	53.6	56.3
Fit for use in Safety Integrity Level	2	2
Fit for use in Spurious Trip Level™	4	4

Table 2 – Sample probability calculations MSK200

	Standalone connected to standard PLC		Standalone connected to smart PLC	
Property	**Value**	**Value**	**Value**	**Value**
Mission time	1 year	10 years	1 year	10 years
Periodic testing	None	1 per 5 years 100% coverage	None	1 per 5 years, 100% coverage
PFD	2.342e-003	1.136e-002	2.355e-003	1.137e-002
PFDavg	1.174e-003	5.751e-003	1.187e-003	5.763e-003
PFS	6.651e-005	6.259e-005	2.819e-005	2.652e-005
FO	1.279e-002	6.202e-002	1.279e-002	6.202e-002
AV	9.976e-001	9.886e-001	9.976e-001	9.886e-001
UP	9.848e-001	9.266e-001	9.848e-001	9.266e-001

Table 3 – Sample probability calculations MTP200

	Standalone connected to standard PLC		Standalone connected to smart PLC	
Property	**Value**	**Value**	**Value**	**Value**
Mission time	1 year	10 years	1 year	10 years
Periodic testing	None	1 per 5 years 100% coverage	None	1 per 5 years, 100% coverage
PFD	3.049e-003	1.473e-002	3.072e-003	1.475e-002
PFDavg	1.529e-003	7.468e-003	1.552e-003	7.491e-003
PFS	9.702e-005	9.060e-005	2.733e-005	2.552e-005
FO	1.394e-002	6.733e-002	1.394e-002	6.733e-002
AV	9.969e-001	9.852e-001	9.969e-001	9.852e-001
UP	9.829e-001	9.179e-001	9.830e-001	9.179e-001

Table of Contents

List of Figures

List of Tables

Terms and Definitions

Term	Definition
AV	See availability.
Availability	The probability that function of the product (or process) is available
Coverage	The percentage of potential failures detected by a test
Dangerous failure	An internal failure that prevents the product from carrying out its safety function upon demand. See also safe failure.
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.
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.
Undetected failure	An internal failure that is not detected by built-in diagnostics. See also detected failure.
Diagnostic test	A built-in test, frequently and automatically carried out, to determine whether the product could carry out its (safety) function without problems.
FMEA	Failure mode and effects analysis.
FO	The probability that the product has failed but can still carry out its function.
FS	The probability that the function causes a spurious trip of the process.
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.
Mission time	Time period over which an analysis is carried out.
Periodic test	A test that is initiated by hand on a periodic basis, e.g., once per year, to determine whether the product can carry out its (safety) function without problems. See also diagnostic test.
PF	The probability that the function has failed upon demand.
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.
Proof test	See periodic test.
Safety function	Function implemented in the product required to achieve a safe state of the process.
SIL	Safety Integrity Level
Safety support function	Function implemented in the product which is not required to achieve a safe state of the process but which enhances the

Term	Definition
	functionality of the product.
STL	Spurious Trip Level
SFF	See safe failure fraction.
TÜV	Technischer Überwachungs Verein
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.
UP	The probability that the product is functioning without any internal failures.

1 Introduction

1.1 Objective

The objective of this report is to document the results of the reliability analyses that have been carried out on the MSK200 and MTP200 products developed and manufactured by Mütec Instruments.

1.2 About Mütec Instruments

Mütec Instruments was founded in 1970 and offers solutions for even the most complicated problems. Mütec's team of highly experienced technical sales 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, we do all the work ourselves-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. Worldwide, our customers benefit from this standard.

1.3 About Risknowlogy

Risknowlogy is a leading provider of technical risk management solutions including knowledge, services, and products in the functional safety industry. Our key focus is on those clients in need of risk, reliability and safety solutions. Through the Risknowlogy Network of Experts (RNE), the Risknowlogy Reseller Associate Program (RRAP) and the Risknowlogy Affiliate Program (RAP) we are able to offer local services and products globally. Risknowlogy has a working agreement with TUV Rheinland, which assures that all our functional safety services are in line with the latest safety procedures of TUV.

1.4 References

The references in Table 4, Table 5, Table 6, and Table 7 have been utilized and/or created during this project:

Table 4 – Basis of the analysis

1.	IEC 61508-2, Functional Safety of Electrical, Electronic, Programmable Electronic Safety Related Systems, 1999
2.	IEC 61511, Functional safety - Safety instrumented systems for the process industry sector, 2003
3.	DIN 19250, Control Technology; Fundamental Safety Aspects To Be Considered for Measurement and Control Equipment, 1994
4.	DIN 19251, MC Protection Equipment, 1995
5.	DIN V VDE 0801, Principles for computers in safety-related systems and Amendment A1, 1984
6.	Siemens SN 29500 Part 1-14 1996-1999, Failure rates of components
7.	ANSI/IEC/ASQC D601165-1997: Application of Markov Techniques
8.	Rouvroye, J.L., Enhanced Markov analysis as a method to assess safety in the process industry, Eindhoven University of Technology, 2001
9.	US MIL-STD-1629, Failure Mode and Effects Analysis, National Technical Information Service, VA: Springfield, MIL1629
10.	Billinton R., Allan R.N., Reliability Evaluation of Engineering Systems, Concepts and Techniques. Pitman Books Limited, London, 1983

Table 5 – Client documentation

11. Mütec Instruments GmbH, Circuit Diagram MSK200iEx, Document number M. 3.03.202, revision 2.0 2003-03-30
12. Mütec Instruments GmbH, Circuit Diagram MTP200iEx, Document number M. 3.03.201, revision 1.1, 2003-03-10
13. Mütec Instruments GmbH, Betriebsanleitung des MSK200(iEx), 2003-11-1
14. Mütec Instruments GmbH, Betriebsanleitung des MTP200(iEx), 2004-5-5
15. Mütec Instruments GmbH, Stückliste des MSK200(iEX), Document number M 2.08.101, revision 2, 2002-08-10
16. Mütec Instruments GmbH, Stückliste des MTP200(iEX), Document number M 2.10.101, revision 1, 2002-10-10
17. TUV Nord e.V, Bericht zür AK4-Prüfung des 19”-Transmitter-Speisegerates MSK200/AK4, rev 1.0, 1999-10-15
18. TUV Nord e.V, Bericht zür AK4-Prüfung des Meßumformers MTP200/AK4, rev 1.0, 1998-08-24
19. Mütec Instruments GmbH, Hardware –Implementierungs Dokumentation, MSK 200, 1999-07-20
20. Mütec Instruments GmbH, Hardware –Implementierungs Dokumentation, MTP 200, 1998-07-10

Table 6 – Risknowlogy documentation

21. Risknowlogy, Failure modes and effects analysis MSK200, Report number 123.101.1, version 1.0, 2005-04-17
22. Risknowlogy, Failure modes and effects analysis MTP200, Report number 123.101.3, version 1.0, 2005-04-30
23. Risknowlogy, Markov analysis MSK200 and MTP200, Report number 123.101.2, version 1.0, 2005-05-01

Table 7 – Other

24. Risknowlogy Markov Modeling and Calculation Engine
25. Risknowlogy Failure Rate Collection Database

2 Product Description

2.1 Introduction

The products subject to hardware reliability analyses are the MSK200 and MTP200 smart transmitters. Examples of the products are given in Figure 1. The products are described in detail in [13,14]. Both products are certified by TUV Nord e.V. for AK 4 taking into account DIN 19250 [3], DIN 19251 [4] and DIN V VDE 0801 [5]. The certification is documented in [17,18].

The measures to control and avoid failures for AK 4, as required by DIN 19250 and DIN V VDE 0801, are equivalent to measures to control and avoid failures in IEC 61508 for SIL 2. To demonstrate compliance with the IEC 61508 SIL 2 requirements it is therefore in addition necessary to perform reliability analysis and calculations.

Figure 1 – Product: MSK200 and MTP200

2.2 Product: MSK200

The MSK200 is a universal 1-channel measuring transmitter supply unit in DuoTec-Failsafe Technology with self-monitoring for supply of 2-wire transmitter.

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

The functional safety properties of the product according to IEC 61508 are:

- Output of the analogue 4-20mA current with an accuracy of 0.2 to 5%
- measurement and supervision of the loop resistance (0 to 2 KOhm)
- Supervision of the accuracy of the analogue output (1%)
- Upon demand open the relays or open the alarm relay in case of an internal failure
- Internally the MSK200 can be divided into a Type A sub module and a Type B sub module. The overall product is a type B;
- Hardware fault tolerance is 0.

2.3 Product: MTP200

The MTP200 is a universal measuring transmitter in DuoTec-Failsafe Technology with self-control.

The functional safety properties of the product according to IEC 61508 are:

- temperature measurement within specified accuracy of 0.2 to 5% for the resistor input
- temperature measurement within specified accuracy of 0.2 to 5mV for the thermocouple input
- measurement and supervision of the loop resistance (0 to 2 KOhm)
- Output of the analogue 4-20mA current with an accuracy of 0.2 to 5%
- Supervision of the accuracy of the analogue output (1%)

- Upon demand open the relays or open the alarm relay in case of an internal failure
- Internally the MTP200 can be divided into a Type A sub module and a Type B sub module. The overall product is a type B;
- Hardware fault tolerance 0.

2.4 Alarm Relay and output loop connection

In case parameters are exceeding the accuracy settings the analogue output current of the device switches to the alarm setting (0 mA or 22 mA). The alarm relay (REL3) indicates the internal status of the diagnostics. The safety function consists of the logical combination of output signal and REL3 status. It is mandatory that both signals are used by control logic or that the analogue signal is connected by REL3 to the control system (see figure below).

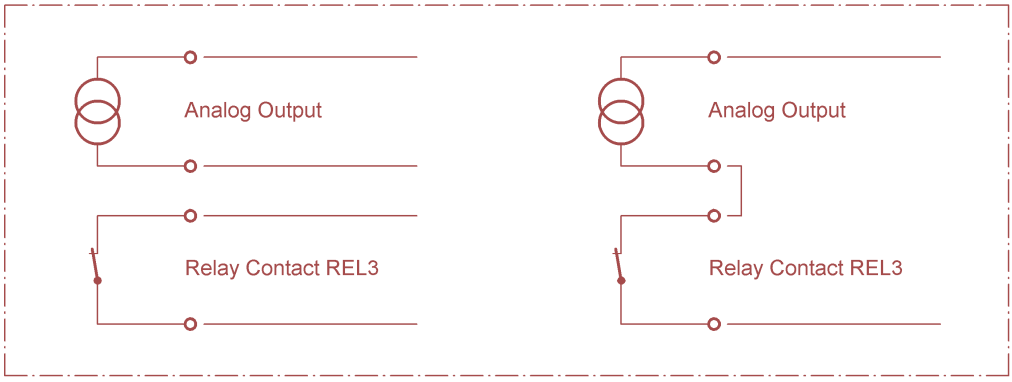

Figure 2 Safety function signalling to control system

3 Reliability Analysis

3.1 Introduction

A qualitative and quantitative reliability study has been carried out in line with the requirements of the IEC 61508 [1] standard and the TUV functional safety procedures. The reliability study consists of failure mode and effects analyses (FMEA) and Markov analyses.

3.2 FMEA

The FMEA is a widely used and effective safety analysis technique. The standard reference for this method is US MIL-STD-1629 [9]. Engineers have always performed an FMEA type of analysis on their design and manufacturing processes, but the first formal applications of the FMEA can be found in the mid-1960 in the American aerospace industry. Today different variations of the FMEA technique exist, which differ in focus but not in their approach.

An FMEA is carried out for two reasons. First of all to evaluate the failure behavior of the product(s) in terms of single failure modes and their effect on the product and the process the product is trying to protect. Second, to determine the existence and effectiveness of internal diagnostics and the safe failure fraction of the product(s) according to the applicable functional safety standard.

3.3 Results FMEA

The results of the FMEA(s) are documented in [21,22] taking into account [11,12,13,14,15,16,17,18,19,20,6,25]. During the FMEA each product was internally divided into type A and type B subsystems. The overall product is a Type B. Table 8 and Table 9 present a summary of the functional safety calculation results for each sub module of the products.

Table 8 – Results FMEA study MSK200

Property	Type B
Safe failure fraction	91.6%
Safe detected failure rate [h]	8.59E-07
Safe undetected failure rate [h]	1.27E-06
Dangerous detected failure rate [h]	6.86E-07
Dangerous undetected failure rate [h]	2.59E-07
Don't care rate [h]	4.11E-08

Table 9 – Results FMEA study MTP200

Property	Type B
Safe failure fraction	90.1%
Safe detected failure rate [h]	8.75E-07
Safe undetected failure rate [h]	1.15E-06
Dangerous detected failure rate [h]	1.11E-06
Dangerous undetected failure rate [h]	3.47E-07
Don't care rate [h]	7.75E-08

3.4 Markov

The Markov approach or Markov modeling technique comes originally from the Russian mathematician A.A. Markov (1856 - 1922) [10]. Markov was engaged in research on mathematically describing random processes. With the years, that work has been extensively developed and the Markov technique has received more and more attention and use.

The basic principle of Markov analysis is that a system can exist in different states. Each state is defined by (a combination of) one or more internal failures in the system. The Markov technique is a straightforward and systematic technique to determine the quantitative behavior of systems. The standard reference for Markov is [7] and in several research projects it has been identified as the ultimate technique to carry out safety analysis [8]. The Markov calculations are performed with [24].

The Markov technique is used to carry out quantitative reliability and availability calculations on the product(s). The following reliability properties are calculated:

- PFD: The probability that the safety function has failed upon demand
- PFDavg: The average probability that the safety function has failed upon demand
- PFS: The probability that the safety function causes a spurious trip of the process
- FO: The probability that the product has failed but can still carry out its function
- AV: The probability that the function of the product is available
- UP: The probability that the product is running without any internal failures

The following paragraphs summarize the results from the detailed analyses performed in [23].

3.5 Results Markov analysis

The calculation results of the two functions of the products are presented in the following tables and figures. For each product the calculations are performed twice. The first calculation represents products purely as standalone devices. This means in practice that they would be connected to a PLC application that cannot differentiate 0-4mA from 4-20mA signals. The second set of calculations represents products that are connected to a smart PLC application that can differentiate the 0-4mA from the 4-20mA output signals.

3.5.1 Calculations for standalone products connected to standard PLC

The following tables and figures show the calculation results for the standalone products connected to a standard PLC application. The results are for the products only, i.e., the values are excluding the PLC hardware.

Table 10 – Results safety function MSK200

Property	Value	Value
Mission time	1 year	10 years
Periodic testing	None	1 per 5 years, 100% coverage
PFD	2.342e-003	1.136e-002
PFDavg	1.174e-003	5.751e-003
PFS	6.651e-005	6.259e-005
FO	1.279e-002	6.202e-002
AV	9.976e-001	9.886e-001
UP	9.848e-001	9.266e-001

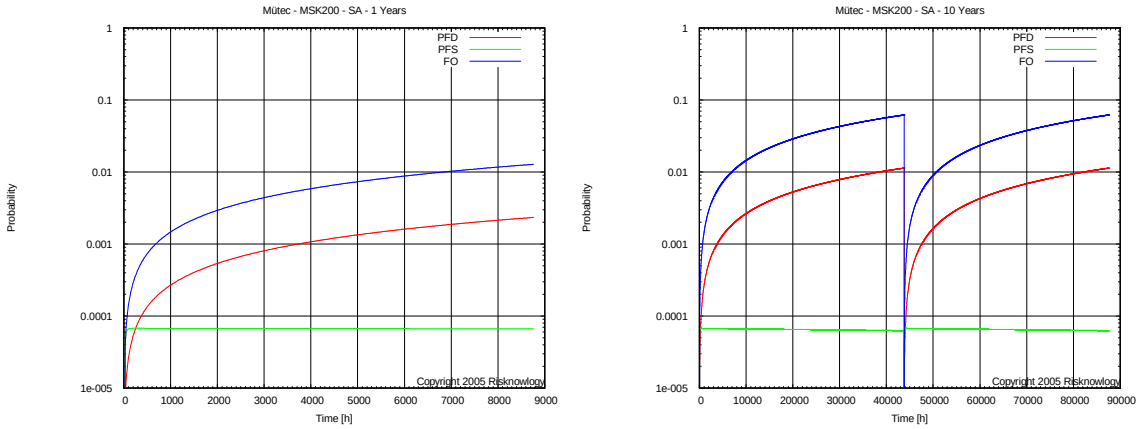

Figure 2 – PFD, PFS, FO – Safety Function MSK200 – 1 Year, 10 Years

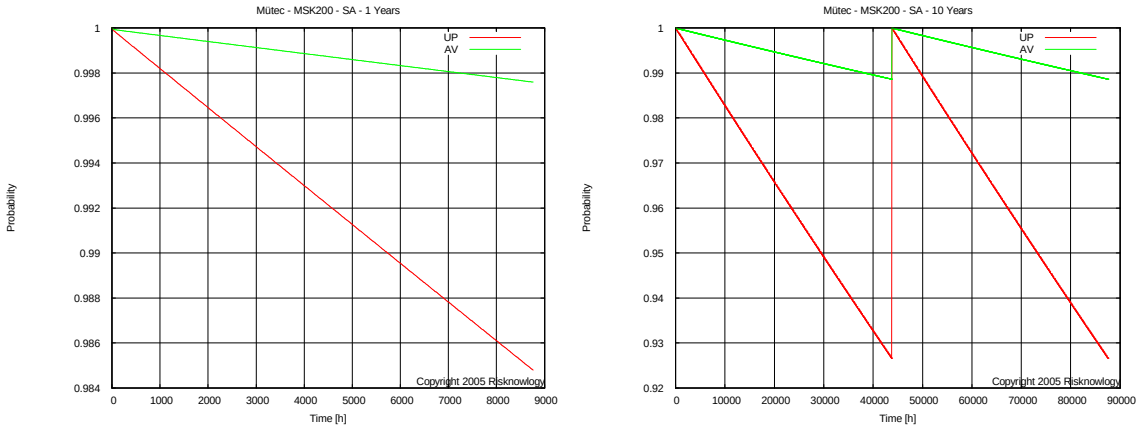

Figure 3 – AV, UP – Safety Function MSK200 – 1 Year, 10 Years

Table 11 – Results safety function MTP200

Property	Value	Value
Mission time	1 year	10 years
Periodic testing	None	1 per 5 years, 100% coverage
PFD	3.049e-003	1.473e-002
PFDavg	1.529e-003	7.468e-003
PFS	9.702e-005	9.060e-005
FO	1.394e-002	6.733e-002
AV	9.969e-001	9.852e-001
UP	9.829e-001	9.179e-001

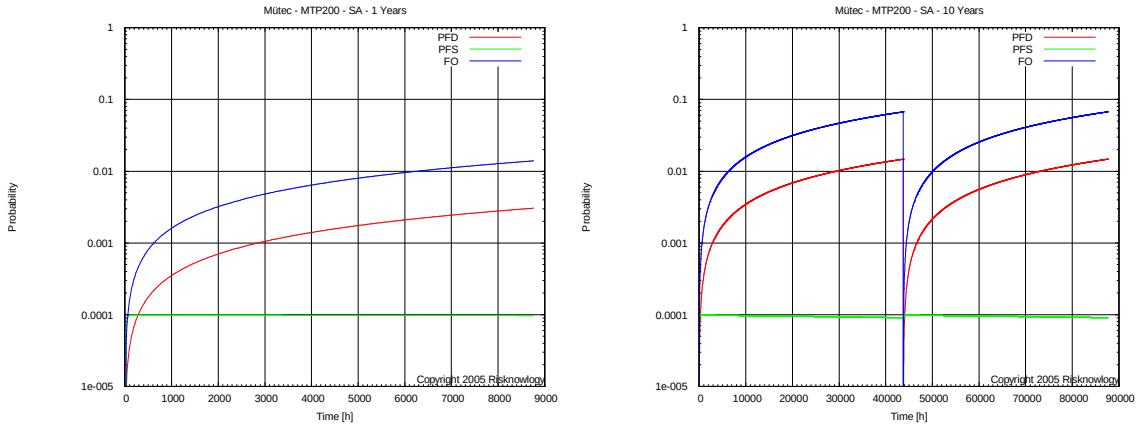

Figure 4 – PFD, PFS, FO – Safety Function MTP200 – 1 Year, 10 Years

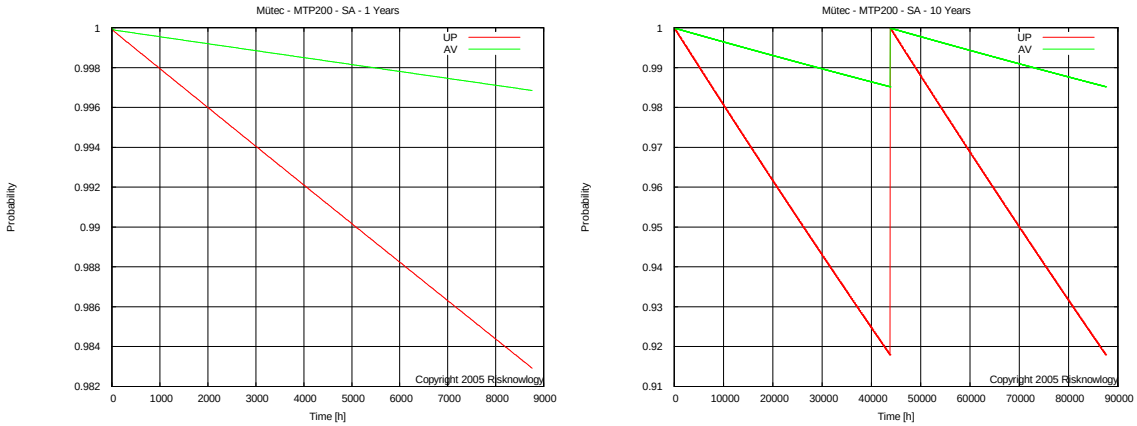

Figure 5 – AV, UP – Safety Function MTP200 – 1 Year, 10 Years

3.5.2 Calculations for standalone products connected to smart PLC

The following tables and figures show the calculation results for the standalone products connected to a smart PLC application. The results are for the products only, i.e., the values are excluding the PLC hardware.

Table 12 – Results safety function MSK200

Property	Value	Value
Mission time	1 year	10 years
Periodic testing	None	1 per 5 years, 100% coverage
PFD	2.355e-003	1.137e-002
PFDavg	1.187e-003	5.763e-003
PFS	2.819e-005	2.652e-005
FO	1.279e-002	6.202e-002
AV	9.976e-001	9.886e-001
UP	9.848e-001	9.266e-001

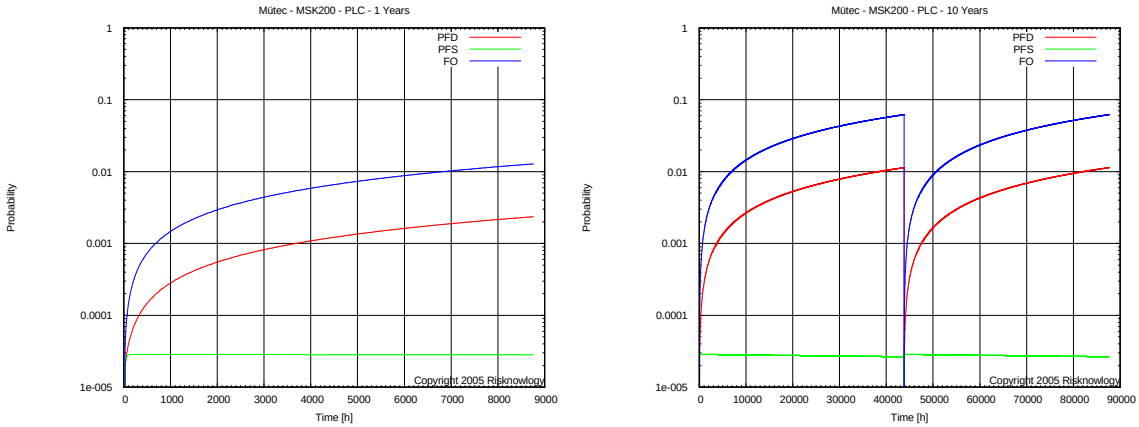

Figure 6 – PFD, PFS, FO – Safety Function MSK200 – 1 Year, 10 Years

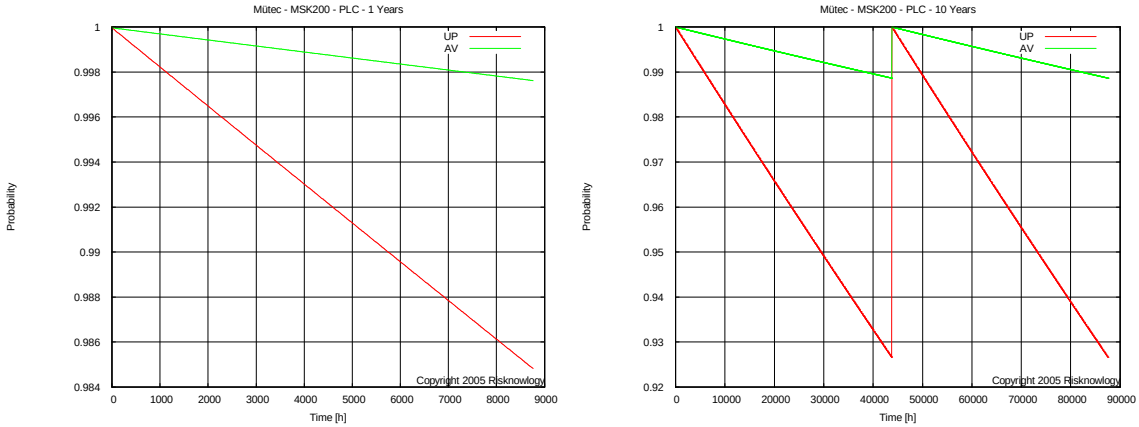

Figure 7 – AV, UP – Safety Function MSK200 – 1 Year, 10 Years

Table 13 – Results safety function MTP200

Property	Value	Value
Mission time	1 year	10 years
Periodic testing	None	1 per 5 years year, 100% coverage
PFD	3.072e-003	1.475e-002
PFDavg	1.552e-003	7.491e-003
PFS	2.733e-005	2.552e-005
FO	1.394e-002	6.733e-002
AV	9.969e-001	9.852e-001
UP	9.830e-001	9.179e-001

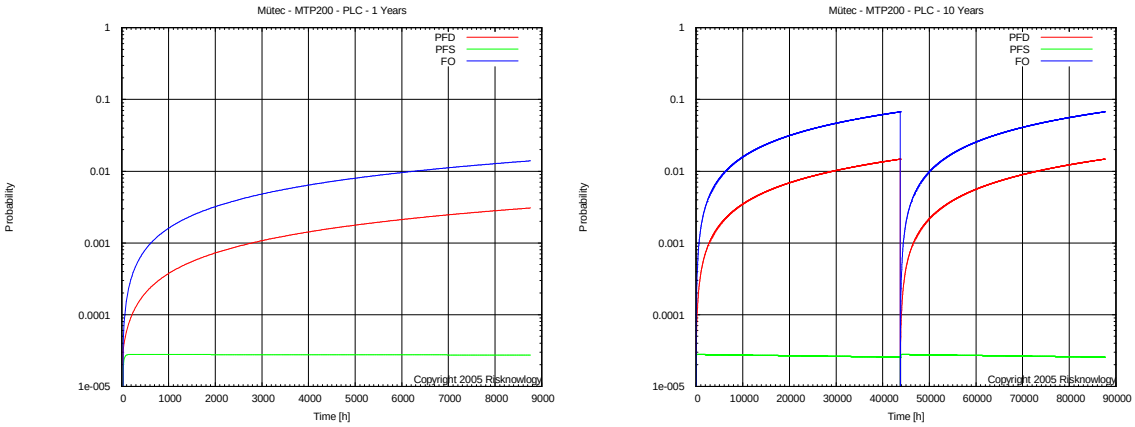

Figure 8 – PFD, PFS, FO – Safety Function MTP200 – 1 Year, 10 Years

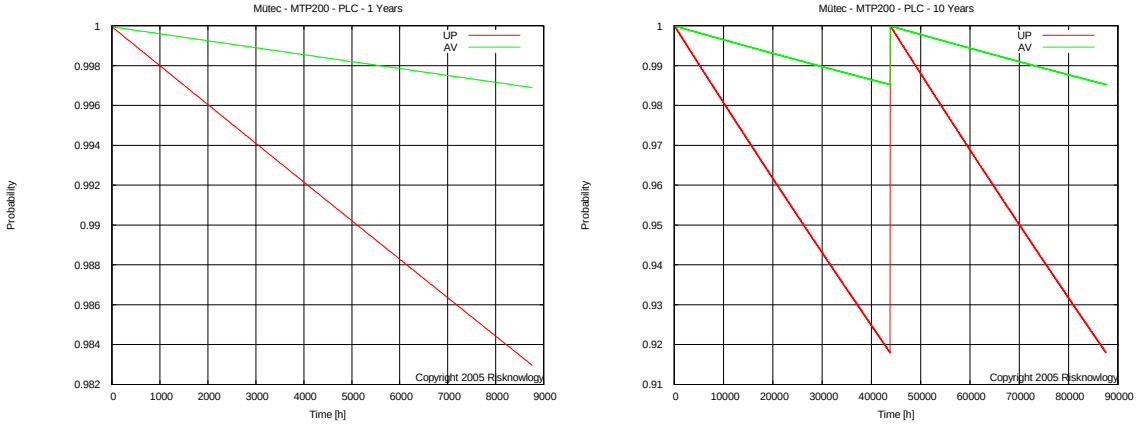

Figure 9 – AV, UP – Safety Function MTP200 – 1 Year, 10 Years

4 Conclusions

Based on the description of the product in chapter 2, the reliability analyses and sample calculations in chapter 3 and the applicable functional safety standards listed in Table 4 the functional safety results are summarized in Table 14. Additional Table 14 gives the MTTF, the dangerous diagnostic coverage and the spurious trip level. The end-user can use the results presented in this report to calculate the PFD of the safety loop taking into account all components of the loop. Depending the application program of the connected PLC, the common cause factor and the periodic proof testing by the end user it is possible to use this product in a 1oo1 architecture up to the PFD requirements according to SIL 2 or in a 1oo2 architecture up to the PFD requirements according to SIL 3.

The end-user can improve the performance of the products in terms of the probability of fail safe by writing an application program that differentiate the 0-4mA from the 4-20mA output signals. See calculation examples in paragraph 3.5.2.

Table 14 – Functional safety summary results

Properties	MSK200	MTP200
Type	B	B
Hardware fault tolerance	0	0
Safe failure fraction	91.6%	90.1%
Safe detected failure rate [1/h]	8.59E-07	8.75E-07
Safe undetected failure rate [1/h]	1.27E-06	1.15E-06
Dangerous detected failure rate [1/h]	6.86E-07	1.11E-06
Dangerous undetected failure rate [1/h]	2.59E-07	3.47E-07
Dangerous diagnostic coverage	72.6%	76.2%
MTTFd [y]	120.7	78.5
MTTFs [y]	53.6	56.3
Fit for use in Safety Integrity Level	2	2
Fit for use in Spurious Trip Level™	4	4