SIL Certification
HVT300-SIL-XX

Document type:	Certification report
Client:	Mütec Instruments GmbH, Seevetal-Ramelsloh, Germany
Project:	HVT300-SIL-XX
Report number:	123.542.13
Revision:	1
Status:	Released
Date:	2022-08-05

Version Control

Quality Assurance

QMT4-2 - 2020-04-26 - Released

Author(s)

Revision	Date	Author(s)	Reviewer(s)	Approver
0	2022-08-05	Michel Houtermans	Ricardo Vittoni	Frank Kozole

Document History

Revision	Date	Description
0	2022-08-05	Original issue
1	2022-08-05	Removed absoleet paragraph

Parties

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, 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

List of Figures

List of Tables

Terms and Definitions

Term	Definition
DC	Diagnostic coverage
DD	Dangerous detected failure rate
DU	Dangerous undetected failure rate
NE	No effect failure rate
NP	No part failure rate
PFDavg	Average probability of failure on demand
SC	Systematic capability
SD	Safe detected failure rate
SF	Safety Function
SFF	Safe failure fraction
SIL	Safety integrity level
STL	Spurious trip level
SU	Safe undetected failure rate
T1	Proof Test Interval

1. Introduction

1.1. Purpose

The purpose of this report is to document the functional safety certification of the HVT-300-SIL-XX series. These products are designed, developed and manufactured by Mütec Instruments, Germany (Mütec). The certification process is carried out to demonstrate that these products meet the applicable SIL requirements according to IEC 61508 [1].

1.2. About the Project

Mütec, is the designer and manufacturer of the HVT300-SIL-XX series. These devices are used as part of safety functions according to IEC 61508 [1] and IEC 61511 [2].

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].

1.4. Certification scope

The certification scope of Risknowlogy, as agreed upon with Mütec, is limited to the product(s) listed in Chapter 2, is based on proven in use (route 2h and 2s) and addresses the following subject matters:

- Management of functional safety;
- Hardware requirements;
- Hardware architecture;
- Hardware reliability;
- Software;
- Basic safety;
- User documentation;

1.5. History

HVT300-SIL-XX is not a new device. It is derived from and rebranded from the MSK200-SIL-DX. The development of MSK 200-SIL-DX itself is based on the MSK200 development from 1998. MSK200 owned a certificate according to DIN V VDE 0801 and DIN V 19250 for AK4 from TÜV Nord e.V. The MSK 200-SIL-DX includes a safety-related architecture and sufficient diagnostic

coverage. The MSK200-SIL-DX device was re-certified according to IEC 61508 [1] and IEC 61511 [2] for SIL2. The latter certification is documented in [3].

2. Product description

2.1. About the HVT300-SIL-XX

The products subject to the analysis are the HVT300-SIL-XX series. The HVT300-SIL-XX is a Balance Voltage Supervisor for Chlorine-Alkali electrolysis. Furthermore, it is used for voltage monitoring in test systems which are used in the automotive sector. The HVT300-SIL-XX measures input voltages, with absolute or differential mode. Output is a 4-20mA analogue signal and an alarm signal. An example of the product is shown in Figure 1.

Figure 1 - HVT300-SIL-DX

The product subject to the analysis documented in this report and available for safety-related applications consists of the configuration listed in Table 1.

Table 1 - Configuration subject to analysis

Configuration	HW Version	SW Versions
HVT300-SIL-XX*	3.3.0	msk_dx_20210412.s2
* XX represents the variations DX, DP, DU, DV		

2.2. Differences Between MSK200-SIL-DX and HVT300-SIL-XX

The HVT300-SIL-XX design is based on the certified MSK200-SIL-DX [3]. The main difference between the HVT300-SIL-XX and the MSK200-SIL-DX is the power supply. The power supply of the HVT300-SIL-XX has been redesigned to guarantee an isolation voltage up to 1000V. Furthermore, the MSK200-SIL-DX has a digital output which has been removed from the HVT300-SIL-XX. These differences do not affect the actual design of the safety functionality. The main body of evidence for this certification is based on the MSK200-SIL-DX documentation.

2.3. Safety function and functional safety parameters

A single HVT300-SIL-XX carries out two safety functions:

> *Safety function 1:*
> *Measure the input voltage and set the output of a 4-20mA current signal within a specified accuracy of 0.2-5%. When the accuracy cannot be maintained, de-energise the alarm relays (REL3 and REL4).*

> *Safety function 2:*
> *Upon demand (violation of configured limit value) open the limit relay**s** (REL1 or REL2). When the limit relay cannot be switched or in case of an internal failure, de-energize the alarm relays (REL3 and REL4)*

The implementation of the above safety functions takes into account the following functional safety parameters according to IEC 61508 [1] and the existing certification [3]:

- Type B;
- HFT = 0 - Low demand;
- HFT = 1 - Low or High demand;
- Safe state safety function 1: REL3 and REL4 open, and the alarm output current to <3.6 mA;
- Safe state safety function 2: REL1 or REL2 open, and REL3 and REL4 open.

3. Certification results

3.1. Quality management

Mütec has a certified ISO 9001 quality management system [4].

3.2. Functional safety management

Mütec holds a valid Functional Safety Management certificate [5] according to the requirements of IEC 61508 [1]. Nevertheless, the device is certified [3] according to route 2h (hardware integrity) and 2s (systematic integrity) of IEC 61508 [1] and meets the systematic capability SC2 in 1oo1.

3.3. Restricted functionality

The purpose of the HVT300-SIL-XX series is to monitor voltage [6]. The functionality of HVT300-SIL-XX is restricted to this purpose. There are no other functions available.

3.4. Conditions of use

The HVT300-SIL-XX series subject to this proven in use study has been used in similar environments. These include over 10 typical process industry environments [7].

3.5. Field data

Mütec has collected 10+ years of operational field data for the HVT300-SIL-XX series, since 2010 [7]. The typical operating time in the process industry is 24 hours per day. From these operational hours, 25% has been excluded to take into account non-operating hours due to, for example, storage time, non-operating time, maintenance downtime, etc. This resulted in a total of 23.800.000 operating hours for this proven in use study.

Mütec has collected and stored customer feedback and repair data [8]. This data demonstrates that for the above claimed operating hours, 72 failures have occurred. 41 of these failures are classified as dangerous failures related to the safety function. None of the failures is related to systematic failures. See Table 2.

Table 2 - Collected field data

Product(s)	Operating hours	Dangerous failures	Safe failures
HVT300-SIL-XX	23.800.000	41	31

3.6. Modifications

During the above period, the hardware and software have been modified. The hardware was released in 2006 (version 1.0), and in 2008, a minor modification was performed (v1.01) [9]. Since 2008 the hardware circuitry has been unmodified, except for modifications of component values to adapt the input measurement circuitry to different measurement ranges (version 1.10, 1.11, 3.3.0) and modifications of the power supply (version 2.2.1 and 3.0.9) [9]. The hardware modifications are not in contradiction with the proven in use verification process because they are limited and minor.

The firmware was released in 2006, and the last modification was introduced in 2015, which led to version 4.04. Since 2015 the firmware is unmodified [10]. The 4 modifications in the time span of 2006 to 2015 were related to product improvements and bug fixes. Summarised, the modifications are classified as limited, traceable and minor. The modifications are not in contradiction with the proven in use verification process. The systematic capability is sufficient for route 2s according to IEC 61508-7, Annex D with 99% confidence for SIL 2.

3.7. Reliability analysis

A reliability study has been carried out in line with the proven in use requirements of the IEC 61508 standard. The reliability study consists of a statistical proven in use study and a failure mode and effects analysis (FMEDA) [11]. Table 3 depicts the statistical analysis of the proven in use data for the stated operating hours in paragraph 3.5 [12].

Table 3 - Statistical analysis results

Property	Failure rate	90% upper confidence limit failure rate
Dangerous failure rate	172 FIT	223 FIT
Safe failure rate	134 FIT	180 FIT

For Type B products, IEC 61508 requires a minimum diagnostic coverage (DC) of 60%. In order to obtain the DC value, an FMEDA has been carried out. The FMEDA uses the component failure rates from SN29500 [13] and the failure models from IEC 62061: 2005, Annex D [14]. For the analyses, an environmental temperature of 40 °C was assumed.

The results of the FMEDA are presented in the next table.

Table 4 - FMEDA analysis

Property	HVT300-SIL-XX
Type	B
Safe detected failure rate	0 FIT
Safe undetected failure rate	331 FIT
Dangerous detected failure rate	325 FIT
Dangerous undetected failure rate	37 FIT
Safe failure fraction	95%
Diagnostic coverage	90%

The FMEDA analysis, which represents design expectations, corresponds with the data from the proven in use data, which represents operational experience. The hardware reliability analysis demonstrates that the product meets the SIL 2 requirements for proven in use.

3.8. PFD

For the product HVT300-SIL-XX, the PFD has been calculated over a period of 1, 5 , and 10 years without proof testing and an expected repair time of 72 hours [12]. The results are listed in the table below.

Table 5 - PFDavg calculations

Property	1 Year	5 Years	10 Years
PFDavg	1.9E-04	8.4E-04	1.7E-03
%SIL 2	1.9%	8.4%	17%

The PFH for a single device is 2.1E-8. From a hardware probability point of view, the product can be used in a SIL 2 application.

3.9. Basic safety evaluation

The HVT300-SIL-XX complies with

- EMC directive 2014/30/EU [15];
- LVD directive 2014/35/EU [16].

The LVD testing was performed according to IEC 61010-1. EMC testing was performed according to IEC 61326-3-1.

3.10. User documentation evaluation

The conditions of use and constraints are described by the safety manual [6].

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

4.3. Conclusions

It is the conclusion of Risknowlogy that the products listed in Table 1 of paragraph 2.1, summarised as HVT300-SIL-XX series, meet the applicable hardware integrity requirements of IEC 61508 according to the certification basis, the certification scope and the safety requirements specification. The products can be used in applications that need to comply with IEC 61508 and/or IEC 61511 taking into account the restrictions in paragraph 4.1.

In summary, the HVT300-SIL-XX meets the hardware and systematic integrity requirements of SIL 2. For low demand mode applications, the products can be used in HFT=0 or HFT=1. For high demand mode applications, the products must be used in HFT=1.

On behalf of Risknowlogy,

Dr Michel Houtermans
Author

Richard Vittoni
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. Mütec, SIL Certificate MSK 200-SIL-DX. Number 123.493.11. Issued 2020-06-29
4. Mütec, Quality Management Certificate. Number A1047GER, expiry 2024-08-28, issued 2021-08-28
5. Mütec, Functional Safety Management Certificate. Number 123.202.7-2. Valid until 2024-08-11
6. Mütec, Safety Manual HVT300-SIL- DX / DP / DU / DV. Number 441, revision 1.0, 2022-07-25
7. Mütec, Betriebsstunden_DuoTec.xlsx
8. Mütec, Reparaturhistorie 2010-2017.xlsx
9. Mütec, Versionen des MSK200.pdf
   20200508_Unterschiede-DPVX-VK.pdf
   MSK200_DB 4-20mA.pdf
   MSK200_DP -10V to +10V.pdf
   MSK200_DP_-250V to +250V.pdf
   MSK200_DP_-5V to +5V.pdf
   MSK200_DV 0-70mV.pdf
   MSK200_DX 0-1000V.pdf
   MSK200_DX 0-1200V.pdf
   MSK200_VK_7 to 1.pdf
10. Mütec, Firmware-Versionen_MSK200-SIL-XX.pdf
11. Risknowlogy, FMEDA - HVT300-SIL-XX - ISO. Document 123.542.5, revision 3, 2022-06-14
12. Risknowlogy, Hardware Reliability Analysis. Document 123.542.6, revision 1, 2022-07-15
13. Siemens, SN29500: 2013 - Failure Rates of Components
14. IEC 62061: 2005, Annex D - Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
15. TUV NORD, EMC Test Report HVT 300-SIL-DX. Number 21077-2, revision 0, 2021-10-13

16. TUV NORD, LVD - Electrical Safety Test Report HVT 300-SIL-DX. Number 21077-1, revision 1, 2021-12-14

Appendix A - Modifications

As of the release of this document, no modifications have taken place. Future modifications to the hardware need to go through an IEC 61508 [1] compliant modification procedure and are subject to re-verification, re-validation and/or certifications.