Failure Modes, Effects and Diagnostic Analysis

Project:

Temperature Transmitters
TT*200-*H with 4..20 mA output and
TSP*** with TTH200-*H and 4..20 mA output

Customer:

ABB Automation Products GmbH
Minden
Germany

Contract No.: ABB 12/04-016

Report No.: ABB 12/04-016 R023

Version V2, Revision R1; August 2016

Stephan Aschenbrenner, Jürgen Hochhaus

Management summary for TT*200-*H with 4..20 mA output

This report summarizes the results of the hardware assessment carried out on the Temperature Transmitters TT*200-*H with 4..20 mA output.

The Temperature Transmitters TT*200-*H are configurable single sensor channel (1 x RTD 2/3/4 wire, 1 x TC, 1 x mV) analog 4..20mA devices.

Table 1 gives an overview of the different types that belong to the considered Temperature Transmitters TT*200-*H with 4..20 mA output including hardware and software version.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Configuration overview

Type	Description	HW Version	SW Version
TTH200-*H	Head mounted temperature transmitter	1.12 and 1.13	2.01.00
TTR200-*H	Rail mounted temperature transmitter	1.12 and 1.13	2.01.00

For safety applications only the described versions were considered. All other possible output variants or electronics are not covered by this report.

The failure rates of the electronic components used in this analysis are the basic failure rates from the Siemens standard SN 29500. This failure rate database is specified in the safety requirements specification from ABB Automation Products GmbH for the Temperature Transmitters TT*200-*H with 4..20 mA.

The listed SN 29500 failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC (25°C ambient temperature plus internal self-heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed.

The failure rates for the Temperature Transmitters TT*200-*H with 4..20 mA output do not include failures resulting from incorrect use of the Temperature Transmitters TT*200-*H with 4..20 mA output, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The Temperature Transmitters TT*200-*H with 4..20 mA output are considered to be Type B[1] elements with a hardware fault tolerance of 0.

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the Temperature Transmitters TT*200-*H with 4..20 mA output communicate detected faults by an alarm output current ≤ 3,6mA or ≥ 21mA. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following table shows how the above stated requirements are fulfilled for the worst case configuration of the Temperature Transmitters TT*200-*H with 4..20 mA output.

[1] Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

Table 2: Summary – IEC 61508 failure rates

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**291**
Fail detected (detected by internal diagnostics)	182
Fail high (detected by safety logic solver)	23
Fail low (detected by safety logic solver)	86
Annunciation detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**27**
Annunciation undetected (λ_{AU})	4
No effect	153
No part	129
Total failure rate (safety function)	**318 FIT**
SFF	**91%**
DC	**91%**
MTBF	**190 years**
SIL AC [2]	**SIL2**

The failure rates are valid for the useful life of the Temperature Transmitters TT*200-*H with 4..20 mA output (see Appendix 2).

Appendix 3 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

[2] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

Assuming that the Temperature Transmitters TT*200-*H with 4..20 mA output will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution for the thermocouple or RTD in a **low stress environment** is as follows:

Table 3: TT*200-*H and TC (low stress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [3]
0 FIT	0 FIT	1191 FIT	127 FIT	90%

Table 4: TT*200-*H and TC (low stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [3]
0 FIT	0 FIT	386 FIT	32 FIT	92%

Table 5: TT*200-*H and 4-wire RTD (low stress – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [3]
0 FIT	0 FIT	786 FIT	32 FIT	96%

Table 6: TT*200-*H and 4-wire RTD (low stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [3]
0 FIT	0 FIT	338.5 FIT	29.5 FIT	91%

Table 7: TT*200-*H and 2/3-wire RTD (low stress – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [3]
0 FIT	0 FIT	671 FIT	122 FIT	84%

Table 8: TT*200-*H and 2/3-wire RTD (low stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [3]
0 FIT	0 FIT	330 FIT	36 FIT	90%

[3] The number listed assumes that the temperature sensing device and the transmitter together are considered to be an element according to IEC 61508:2010. However, it would also be possible to consider both parts as separate elements where each element has to fulfill the SFF by itself. See section 7.4.4.2.3 of IEC 61508-2.

Assuming that the Temperature Transmitters TT*200-*H with 4..20 mA output will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution for the thermocouple or RTD in a **high stress environment** is as follows:

Table 9: TT*200-*H and TC (high stress – with extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	18291 FIT	2027 FIT	90%

Table 10: TT*200-*H and TC (high stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	2191 FIT	127 FIT	94%

Table 11: TT*200-*H and 4-wire RTD (high stress – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	10191 FIT	127 FIT	98%

Table 12: TT*200-*H and 4-wire RTD (high stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	1241 FIT	77 FIT	94%

Table 13: TT*200-*H and 2/3-wire RTD (high stress – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	7891 FIT	1927 FIT	80%

Table 14: TT*200-*H and 2/3-wire RTD (high stress – close coupled)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	1078 FIT	200 FIT	84%

[4] The number listed assumes that the temperature sensing device and the transmitter together are considered to be an element according to IEC 61508:2010. However, it would also be possible to consider both parts as separate elements where each element has to fulfill the SFF by itself. See section 7.4.4.2.3 of IEC 61508-2.

Management summary for TSP*** with TTH200-*H

This report summarizes the results of the hardware assessment carried out on the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output.

The Temperature Transmitters TTH200-*H are configurable single sensor channel (1 x RTD 2/3/4 wire, 1 x TC, 1 x mV) analog 4..20mA devices.

Table 15 gives an overview of the different types that belong to the considered Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output including hardware and software version.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 15: Configuration overview

Type	Description	HW Version	SW Version
TSP***	Sensor TSP000 … TSP999 with TTH200-*H	1.12 and 1.13	2.01.00

For safety applications only the described versions were considered. All other possible output variants or electronics are not covered by this report.

The failure rates of the electronic components used in this analysis are the basic failure rates from the Siemens standard SN 29500. This failure rate database is specified in the safety requirements specification from ABB Automation Products GmbH for the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed.

The failure rates for the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output do not include failures resulting from incorrect use of the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output are considered to be Type B[5] elements with a hardware fault tolerance of 0.

It is assumed that the connected safety logic solver is configured as per the NAMUR NE43 signal ranges, i.e. the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output communicate detected faults by an alarm output current ≤ 3,6mA or ≥ 21mA. Assuming that the application program in the safety logic solver does not automatically trip on these failures, these failures have been classified as dangerous detected failures. The following tables show how the above stated requirements are fulfilled for the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output (complete temperature sensor assembly consisting of the Temperature Transmitters TTH200-*H and a thermocouple or RTD).

[5] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

The failure rates are valid for the useful life of the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output (see Appendix 2).

Appendix 3 gives typical failure rates and failure distributions for thermocouples and RTDs which were the basis for the following tables.

Assuming that the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution for the thermocouple or RTD in a **low stress environment** is as follows:

Table 16: TSP* with TTH200-*H and TC (low stress – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	386 FIT	32 FIT	92%

Table 17: TSP* with TTH200-*H and 4-wire RTD (low stress – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	338.5 FIT	29.5 FIT	91%

Table 18: TSP* with TTH200-*H and 2/3-wire RTD (low stress – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [4]
0 FIT	0 FIT	330 FIT	36 FIT	90%

Assuming that the Temperature Transmitters TSP*** with TTH200-*H and 4..20 mA output will go to the pre-defined alarm state on detected failures of the thermocouple or RTD, the failure rate contribution for the thermocouple or RTD in a **high stress environment** is as follows:

Table 19: TSP* with TTH200-*H and TC (high stress – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [5]
0 FIT	0 FIT	2191 FIT	127 FIT	94%

Table 20: TSP* with TTH200-*H and 4-wire RTD (high stress – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [5]
0 FIT	0 FIT	1241 FIT	77 FIT	94%

Table 21: TSP* with TTH200-*H and 2/3-wire RTD (high stress – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [5]
0 FIT	0 FIT	1078 FIT	200 FIT	84%

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA. Table 1 and Table 15 give an overview of the different configurations that belong to the considered Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output including hardware and software version.

The FMEDA builds the basis for an evaluation whether a sensor subsystem including the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

An FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

2 Project management

2.1 *exida*

exida is one of the world's leading product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

ABB Automation Products GmbH	Manufacturer of the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output.
exida	Performed the hardware assessment.

ABB Automation Products GmbH contracted *exida* in April 2012 with the FMEDA of the above mentioned devices.

2.3 Standards / Literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	SN 29500-1:01.2004 SN 29500-1 H1:07.2011 SN 29500-2:09.2010 SN 29500-3:06.2009 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 1SN 29500-11:07.2011 SN 29500-12:02.2008 SN 29500-15:07.2009 SN 29500-16:08.2010	Failure rates of components
[N3]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	*exida* L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N4]	EMCR Handbook, 2011 Update	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, 2011 Update

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	DS_TTH200-EN-02_2009[1].pdf	Data sheet „Head mounted Temperature Transmitter TTH200" of 4.11.2009
[D2]	DS_TTR200-EN-A-07_2008[1].pdf	Data sheet "Rail mounted Temperature Transmitter TTR200" of 4.11.2009
[D3]	670697_TTH200SE_SCH_V01.12	Circuit diagram "TTH200" PCB 670696; Rev. 1.12 of 14.09.12
[D4]	670697_TTH200SE_SCH_V01.13.pdf	Circuit diagram "TTH200" PCB 670696; Rev. 1.13 of 25.04.16
[D5]	IIM-A006_2012-TT_Fault Insertion Test.pdf	Test report "Fault Insertion Test TTH200" IIM-A006/2012-TT; 15.11.12
[D6]	IIM-FL-07-2016-TT TTX200 HW 1.13 Modification	Description of the hardware modification for v1.13 of 6.6.2016
[D7]	Change Impact Analysis TTx200_HW_1.12 HW_1.13	Analysis of the change for the impact on functional safety 12.6.2016
[D8]	IIM-A-20-2016-TT TTX200 Qualifikation Referenz HW-Rev. 1.13	Accuracy test report of the modified output, dated 15.6.2016

The list above only means that the referenced documents were provided as basis for the FMEDA but it does not mean that *exida* checked the correctness and completeness of these documents.

2.4.2 Documentation generated by *exida*

[R1]	FMEDA_V8_TTx200_V1R3.efm of 5.8.16
[R2]	Summary_with_Sensor_Element_V1R3.xls of 5.8.16

3 Description of the analyzed elements

3.1 System description

The Temperature Transmitters TSP*** and TT*2*0-*H are isolated two-wire 4...20 mA devices used in many different industries for both control and safety applications. Combined with a temperature sensing device, the temperature transmitters become a temperature sensor assembly.

The Temperature Transmitters TSP*** and TT*2*0-*H with 4..20 mA output are considered to be Type B subsystems with a hardware fault tolerance of 0.

The temperature sensing devices that can be connected to the Temperature Transmitters TSP*** and TT*2*0-*H are listed underneath:

- 2-, 3-, and 4-wire RTD
- Thermocouple

The FMEDA has been performed considering the worst-case input sensor configuration.

Figure 1 gives an overview of the Temperature Transmitters TSP*** and TT*2*0-*H with 4..20 mA output.

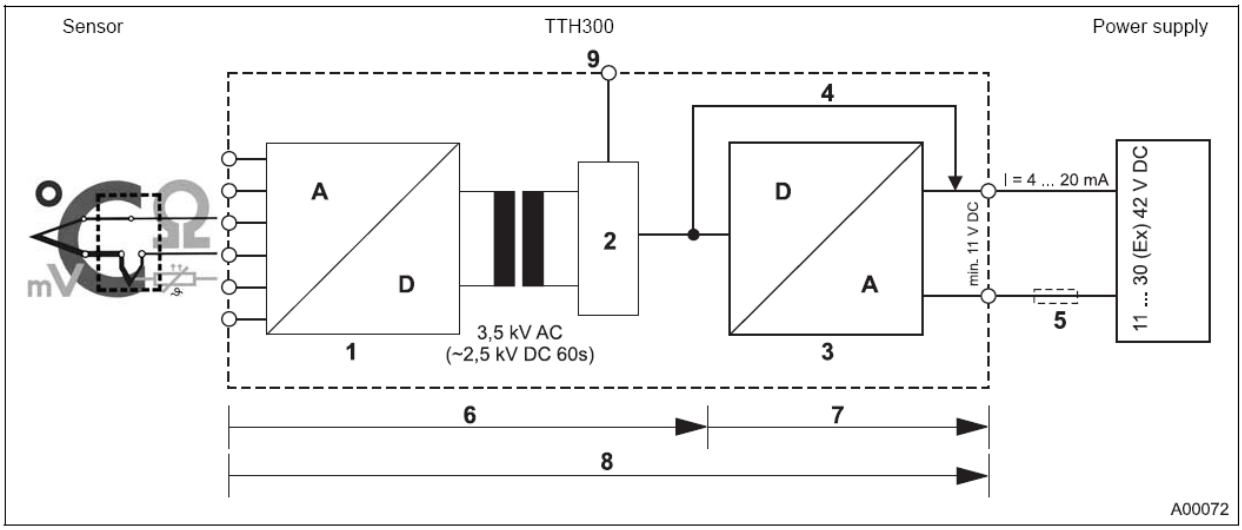


Fig. 1

1	24-bit A/D converter	6	Digital accuracy
2	Microcontroller	7	D/A accuracy
3	16-bit D/A converter	8	Overall accuracy
4	HART signal	9	Display interface
5	Load (observe voltage drop, refer to the section "Terminal connection diagrams")		

Figure 1: Temperature Transmitters TSP* and TT*2*0-*H with 4..20 mA output**

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was prepared by *exida* together with ABB Automation Products GmbH. The results are documented in [R1] and [R2]. When the effect of a certain component failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level (see fault insertion test report [D5]). This resulted in failures that can be classified according to the following failure categories.

4.1 Description of the failure categories

In order to judge the failure behavior of the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as the output reaching the user defined threshold vale.
Fail Safe	A safe failure (S) is defined as a failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) deviates the output current by more than 2% of full span or prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or, b) decreases the probability that the safety function operates correctly when required.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed.
Fail Dangerous Detected	Failure that is dangerous but is detected.
Fail High	A fail high failure (H) is defined as a failure that causes the output signal to go to the high alarm output current (> 21mA).
Fail Low	A fail low failure (L) is defined as a failure that causes the output signal to go to the low alarm current (< 3.6mA).
Annunciation	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures.
No effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.
No part	Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness.

4.2 Methodology – FMEDA, Failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Modes, Effects, and Diagnostic Analysis) is a FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA are the basic failure rates from the Siemens standard SN 29500. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

The listed SN 29500 failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC (25°C ambient temperature plus internal self-heating). For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation (daily fluctuation of > 15°C) must be assumed.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events, however, should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The HART protocol is only used for setup and diagnostics purposes, not during normal operation.
- The device is installed per manufacturer's instructions.
- Failures during parameterization are not considered.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- External power supply failure rates are not included.
- The worst case internal fault detection time is 5 minutes.
- The time of a connected safety PLC to react on a dangerous detected failure and to bring the process to the safe state is identical to MTTR.
- Only the current output 4..20mA is used for safety applications.
- Only one input and one output are part of the considered safety function.
- The application program in the safety logic solver is configured according to NAMUR NE43 to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- Materials are compatible with process conditions.
- The measurement / application limits (including pressure and temperature ranges) are considered.
- Short circuit and lead breakage detection are activated.
- The minimum supply voltage is 15 VDC.

4.3 Results

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

This assessment supports the 1_H approach.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$SFF = (\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg}) / (\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg} + \Sigma\lambda_{DU} \text{ avg})$

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{DU} = Fail Dangerous Undetected

$DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$

$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{AU} + \lambda_{no\ effect} + \lambda_{no\ part})) + 24\ h$

4.3.1 Temperature Transmitters TT*200-*H with 4..20 mA output

The FMEDA carried out on the worst-case configuration of the Temperature Transmitters TT*200-*H with 4..20 mA output leads under the assumptions described in section 0 to the following failure rates:

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**0**
Fail Dangerous Detected (λ_{DD})	**291**
Fail detected (detected by internal diagnostics)	182
Fail high (detected by safety logic solver)	23
Fail low (detected by safety logic solver)	86
Annunciation detected (λ_{AD})	0
Fail Dangerous Undetected (λ_{DU})	**27**

Annunciation undetected (λ_{AU})	4
No effect	153
No part	129

Total failure rate (safety function)	**318 FIT**
SFF	**91%**
DC	**91%**
MTBF	**190 years**

SIL AC [6]	**SIL2**

[6] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled.

5 Using the FMEDA results

The following section describes how to apply the results of the FMEDA.

5.1 Temperature sensing devices

The Temperature Transmitters TT*200-*H with 4..20 mA output together with a temperature sensing device become a temperature sensor assembly like the TSP*** with TTH200-*H and 4..20 mA output. Therefore when using the results of this FMEDA in a SIL verification assessment, the failure rates and failure modes of the temperature sensing device must be considered.

5.1.1 TSP*** with TTH200-*H or TT*200-*H with thermocouple (TC)

The failure mode distributions for thermocouples vary in published literature but there is strong agreement that open circuit or “burn-out” failure is the dominant failure mode. While some estimates put this failure mode at 99%+, a more conservative failure rate distribution suitable for SIS applications is shown in Table 22 and Table 23 when thermocouples are supplied with the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output. The drift failure mode is primarily due to T/C aging. The Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output will detect a thermocouple burn-out failure and drive their output to the specified failure state.

Table 22 Typical failure rates for thermocouples (with extension wire)

Thermocouple Failure Mode Distribution	***Low Stress (LS)***	***High Stress (HS)***
Open Circuit (Burn-out)	900 FIT	18000 FIT
Short Circuit (Temperature measurement in error)	50 FIT	1000 FIT
Drift (Temperature measurement in error)	50 FIT	1000 FIT

Table 23 Typical failure rates for thermocouples (close coupled)

Thermocouple Failure Mode Distribution	***Low Stress (LS)***	***High Stress (HS)***
Open Circuit (Burn-out)	95 FIT	1900 FIT
Short Circuit (Temperature measurement in error)	4 FIT	80 FIT
Drift (Temperature measurement in error)	1 FIT	20 FIT

TSP*** with TTH200-*H and 4..20 mA output or a complete temperature sensor assembly consisting of the Temperature Transmitters TT*200-*H with 4..20 mA output and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output will go to the pre-defined alarm state on detected failures of the thermocouple, the failure rate contribution for the thermocouple is:

Low stress environment (extension wire)	**High stress environment (extension wire)**
λ_{dd} = 900 FIT	λ_{dd} = 18000 FIT
λ_{du} = 50 FIT + 50 FIT = 100 FIT	λ_{du} = 1000 FIT + 1000 FIT = 2000 FIT

Low stress environment (close coupled)	**High stress environment (close coupled)**
λ_{dd} = 95 FIT	λ_{dd} = 1900 FIT
λ_{du} = 4 FIT + 1 FIT = 5 FIT	λ_{du} = 80 FIT + 20 FIT = 100 FIT

This results in a failure rate distribution and SFF to:

Table 24: TT*200-*H with TC (LS – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF [7]
0 FIT	0 FIT	1191 FIT	127 FIT	90%

Table 25: TSP* with TTH200-*H or TT*200-*H with TC (LS – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF [7]
0 FIT	0 FIT	386 FIT	32 FIT	92%

Table 26: TT*200-*H with TC (HS – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF [7]
0 FIT	0 FIT	18291 FIT	2027 FIT	90%

Table 27: TSP* with TTH200-*H or TT*200-*H with TC (HS – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF [7]
0 FIT	0 FIT	2191 FIT	127 FIT	94%

[7] The number listed assumes that the temperature sensing device and the transmitter together are considered to be an element according to IEC 61508:2010. However, it would also be possible to consider both parts as separate elements where each element has to fulfill the SFF by itself. See section 7.4.4.2.3 of IEC 61508-2.

5.1.2 TSP*** with TTH200-*H or TT*200-*H with RTD

The failure mode distribution for an RTD also depends on the application with the key variables being stress level, RTD wire length and RTD type (2/3 wire or 4 wire). The key stress variables are high vibration and frequent temperature cycling as these are known to cause cracks in the substrate leading to broken lead connection welds. Failure rate distributions are shown in Table 28 to Table 31. The Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output will detect open circuit, short circuit and a certain percentage of drift RTD failures and drive their output to the specified failure state.

Table 28 Typical failure rates for 4-Wire RTDs (with extension wire)

RTD Failure Mode Distribution	*Low Stress (LS)*	*High Stress (HS)*
Open Circuit (Burn-out)	410 FIT	8200 FIT
Short Circuit (Burn-out)	20 FIT	400 FIT
Drift (Temperature Measurement in error)	70 FIT [8]	1400 FIT [9]

Table 29 Typical failure rates for 4-Wire RTDs (close coupled)

RTD Failure Mode Distribution	*Low Stress (LS)*	*High Stress (HS)*
Open Circuit (Burn-out)	41,5 FIT	830 FIT
Short Circuit (Burn-out)	2,5 FIT	50 FIT
Drift (Temperature Measurement in error)	6 FIT [10]	120 FIT [11]

Table 30 Typical failure rates for 2/3-Wire RTDs (with extension wire)

RTD Failure Mode Distribution	*Low Stress (LS)*	*High Stress (HS)*
Open Circuit (Burn-out)	370,5 FIT	7410 FIT
Short Circuit (Burn-out)	9,5 FIT	190 FIT
Drift (Temperature Measurement in error)	95 FIT	1900 FIT

Table 31 Typical failure rates for 2/3-Wire RTDs (close coupled)

RTD Failure Mode Distribution	*Low Stress (LS)*	*High Stress (HS)*
Open Circuit (Burn-out)	37,92 FIT	758,4 FIT
Short Circuit (Burn-out)	1,44 FIT	28,8 FIT
Drift (Temperature Measurement in error)	8,64 FIT	172,8 FIT

[8] It is assumed that 65 FIT are detectable if the 4-wire RTD is correctly used.

[9] It is assumed that 1300 FIT are detectable if the 4-wire RTD is correctly used.

[10] It is assumed that 3.5 FIT are detectable if the 4-wire RTD is correctly used.

[11] It is assumed that 70 FIT are detectable if the 4-wire RTD is correctly used.

TSP*** with TTH200-*H and 4..20 mA output or a complete temperature sensor assembly consisting of the Temperature Transmitters TT*200-*H with 4..20 mA output and a temperature sensing device can be modeled by considering a series subsystem where a failure occurs if there is a failure in either component. For such a system, failure rates are added. Assuming that the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output will go to the pre-defined alarm state on a detected failure of the RTD, the failure rate contribution for the RTD is:

4-wire RTD with extension wire:

	Low stress environment	**High stress environment**
λ_{dd}:	410 FIT + 20 FIT + 65 FIT = 495 FIT	8200 FIT + 400 FIT + 1300 FIT = 9900 FIT
λ_{du}:	5 FIT	100 FIT

4-wire RTD close coupled:

	Low stress environment	**High stress environment**
λ_{dd}:	41.5 FIT + 2.5 FIT + 3.5 FIT = 47.5 FIT	830 FIT + 50 FIT + 70 FIT = 950 FIT
λ_{du}:	2,5 FIT	50 FIT

2/3-wire RTD with extension wire:

	Low stress environment	**High stress environment**
λ_{dd}:	370.5 FIT + 9.5 FIT = 380 FIT	7410 FIT + 190 FIT = 7600 FIT
λ_{du}:	95 FIT	1900 FIT

2/3-wire RTD close coupled:

	Low stress environment	**High stress environment**
λ_{dd}:	37.92 FIT + 1.44 FIT = 39,36 FIT	758.4 FIT + 28.8 FIT = 787.2 FIT
λ_{du}:	8.64 FIT	172.8 FIT

This results in a failure rate distribution and SFF to:

Table 32: TT*200-*H with 4-wire RTD (LS – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	786 FIT	32 FIT	96%

Table 33: TSP* with TTH200-*H or TT*200-*H with 4-wire RTD (LS – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	338.5 FIT	29.5 FIT	91%

Table 34: TT*200-*H with 4-wire RTD (HS – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	10191 FIT	127 FIT	98%

Table 35: TSP* with TTH200-*H or TT*200-*H with 4-wire RTD (HS – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	1241 FIT	77 FIT	94%

Table 36: TT*200-*H with 2/3-wire RTD (LS – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	671 FIT	122 FIT	84%

Table 37: TSP* with TTH200-*H or TT*200-*H with 2/3-wire RTD (LS – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	330 FIT	36 FIT	90%

Table 38: TT*200-*H with 2/3-wire RTD (HS – extension wire)

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	7891 FIT	1927 FIT	80%

Table 39: TSP* with TTH200-*H or TT*200-*H with 2/3-wire RTD (HS – close coupled)**

λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	**SFF** [12]
0 FIT	0 FIT	1078 FIT	200 FIT	84%

[12] The number listed assumes that the temperature sensing device and the transmitter together are considered to be an element according to IEC 61508:2010. However, it would also be possible to consider both parts as separate elements where each element has to fulfill the SFF by itself. See section 7.4.4.2.3 of IEC 61508-2.

5.2 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) Temperature Transmitters TT*200-*H with 4..20 mA output with *exida's* exSILentia tool. The worst-case failure rate data used in this calculation are displayed in section 4.3.1. A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours, a proof test coverage of 99% (see Appendix 1.1) and a maintenance capability of 100%. The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Table 40.

For SIL2 applications, the PFD_{AVG} value needs to be < 1.00E-02.

Table 40: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 1.33E-04	PFD_{AVG} = 2.48E-04	PFD_{AVG} = 5.92E-04

This means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval is approximately equal to 1.5% of the allowed range.

The resulting PFD_{AVG} graph for a Temperature Transmitter TT*200-*H with 4..20 mA output generated from the exSILentia tool for a proof test of 1 year is displayed in Figure 2

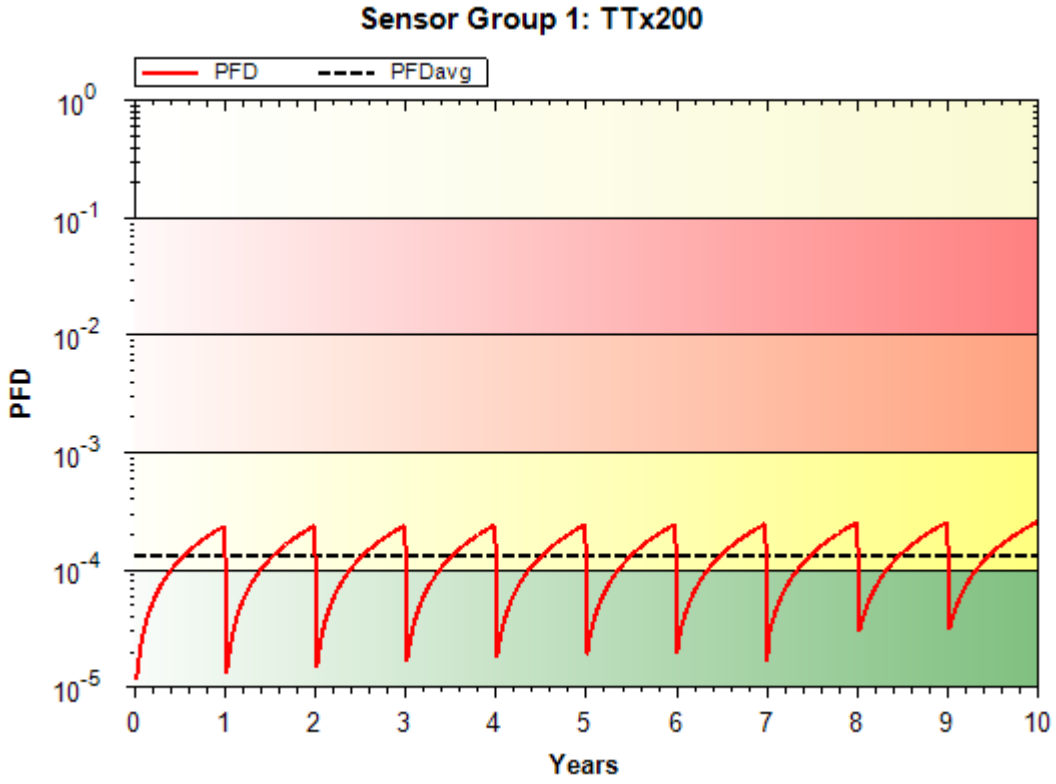


Figure 2: PFD_{AVG} value for a single TT*200-*H with proof test interval of 1 year

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

These results must be considered in combination with PFD_{AVG} values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

6 Terms and Definitions

DC	Diagnostic Coverage of dangerous failures (DC = λ_{dd} / (λ_{dd} + λ_{du}))
FIT	Failure In Time (1x10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
Low stress	Low stress applies to a low vibration environment or the use of a cushioned sensor. The operation is below 67% maximum rating according to specification.
High stress	High stress applies to a high vibration environment. The operation is above 67% maximum rating according to specification.
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of a dangerous failure per hour
RTD	Resistance Temperature Detector
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
TC	Thermocouple
Type B element	“Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

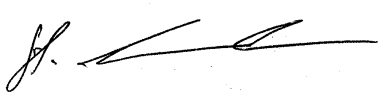
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

7.2 Releases

Version History:	V2R1:	Changed ABB site location to Minden; August 16, 2016
	V2R0:	FMEDA was updated to new HW rev1.13; August 8, 2016
	V1R0:	Review comments incorporated; December 21, 2012
	V0R1:	Initial version; November 21, 2012
Authors:	Stephan Aschenbrenner, Jürgen Hochhaus	
Review:	V0R1:	Rudolf P. Chalupa (*exida*); November 26, 2012
		Dietmar Overhoff (ABB); December 19, 2012
Release status:	Released to ABB Automation Products GmbH	

7.3 Release Signatures



Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner

Dipl.-Ing.(FH) Jürgen Hochhaus, Senior Safety Engineer

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 41.

Table 41 Suggested steps for a proof test

Step	Action
1	Bypass the safety PLC or take other appropriate action to avoid a false trip
2	Perform a multi-point calibration of the temperature transmitter covering the applicable temperature range
3	Apply an adequate input signal to reach the pre-defined alarm level and verify that the safe state is reached (The analog current output corresponds to the provided input signal).
4	Send a HART command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
5	Send a HART command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value. This tests for possible quiescent current related failures
6	Restore the loop to full operation
7	Remove the bypass from the safety PLC or otherwise restore normal operation

It is assumed that this test will detect 99% of possible “du” failures in the Temperature Transmitters TT*200-*H with 4..20 mA output and TSP*** with TTH200-*H and 4..20 mA output.

Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime[13] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular (for example, electrolyte capacitors can be very sensitive).

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components. Therefore it is obvious that the PFD_{AVG} calculation is only valid for components which have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation period and therefore the assumption of a constant failure rate during the useful lifetime is valid.

Table 42 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{AVG} calculation and what their estimated useful lifetime is.

Table 42: Useful lifetime of components contributing to λ_{du}

Type	Useful life
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Appr. 500 000 hours
Sensors	According to ABB specification

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

[13] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.