Failure Modes, Effects and Diagnostic Analysis

Project:
8732C Magnetic Flow Transmitter

Customer:

Rosemount Inc.
Chanhassen, MN
USA

Contract No.: Ros 03/07-26
Report No.: Ros 03/07-26 R001
Version V1, Revision R1.0, October 2003

William M. Goble – John C. Grebe

Management summary

This report summarizes the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 8732C Magnetic Flow Transmitter. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates and Safe Failure Fraction are determined. The FMEDA that is described in this report concerns only the hardware of the 8732C Magnetic Flow Transmitter, electronic and mechanical. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The 8732C Magnetic Flow Transmitter is a four wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. Table 1 gives an overview of the different versions that belong to the considered 8732C Magnetic Flow Transmitter.

Table 1: Version overview

A	DC Power Option
B	AC Power Option

The 8732C Magnetic Flow Transmitter is classified as a Type B[1] device according to IEC 61508, having a hardware fault tolerance of 0. The analysis shows that the device has a safe failure fraction between 60 and 90% (assuming that the logic solver is programmed to detect over-scale and under-scale currents) and therefore may be used up to SIL 1 as a single device.

The failure rates for the 8732C Magnetic Flow Transmitter – DC power option are as follows:

λ^{H} = 6 * 10^{-9} failures per hour

λ^{L} = 566 * 10^{-9} failures per hour

λ^{DU} = 318 * 10^{-9} failures per hour

The failure rates for the 8732C Magnetic Flow Transmitter - AC power option are as follows:

λ^{H} = 6 * 10^{-9} failures per hour

λ^{L} = 582 * 10^{-9} failures per hour

λ^{DU} = 328 * 10^{-9} failures per hour

Tables 2 and 3 list the failure rates for 8732C Magnetic Flow Transmitter according to IEC 61508, assuming that the logic solver can detect both over-scale and under-scale currents.

Table 2: Failure rates according to IEC 61508 - 8732C Magnetic Flow Transmitter DC Power Option

Failure Categories	λ_{sd}	λ_{su}^{*}	λ_{dd}	λ_{du}	SFF
Low trip	566 FIT	287 FIT	6 FIT	318 FIT	73.0%
High trip	6 FIT	287 FIT	566 FIT	318 FIT	73.0%

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Table 3: Failure rates according to IEC 61508- 8732C Magnetic Flow Transmitter AC Power Option

Failure Categories	λ_{sd}	λ_{su}*	λ_{dd}	λ_{du}	SFF
Low trip	582 FIT	274 FIT	6 FIT	328 FIT	72.4%
High trip	6 FIT	274 FIT	582 FIT	328 FIT	72.4%

(*Note that the SU category includes failures that do not cause a spurious trip)

These failure rates are valid for the useful lifetime of the product, which is > 10 years.

A user of the 8732C Magnetic Flow Transmitter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 4.5 along with all assumptions.

Table of Contents

1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

Option 1: Hardware assessment according to IEC 61508

Option 1 is a hardware assessment by exida.com according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment contains a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not contain any software assessment.

Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511

Option 2 is an assessment by exida.com according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment contains a FMEDA to determine the fault behavior and the different failure rates resulting in the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). The option contains in addition an assessment of the proven-in-use demonstration of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

Option 3: Full assessment according to IEC 61508

Option 3 is a full assessment by exida.com according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.

This assessment shall be done according to option 1.

This document shall describe the results of the Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 8732C Magnetic Flow Transmitter. From these failure rates, the Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

2 Project management

2.1 *exida.com*

exida.com is one of the world's leading knowledge companies specializing in automation system safety and availability with over 100 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

Rosemount Inc. Manufacturer of the 8732C Magnetic Flow Transmitter

exida.com Project leader of the FMEDA

Rosemount Inc. contracted *exida.com* in October 2003 with the FMEDA and PFD_{AVG} calculation of the above-mentioned device.

2.3 Standards / Literature used

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

[N1]	IEC 61508-2: 1999	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	FMD-91 & FMD-97, RAC 1991, 1997	Failure Mode / Mechanism Distributions, Reliability Analysis Center. Statistical compilation of failure mode distributions for a wide range of components
[N3]	NPRD-95, RAC 1995	Nonelectronic Parts Reliability Data, Reliability Analysis Center. Statistical compilation of failure rate data, incl. mechanical and electrical sensors
[N4]	SN 29500	Failure rates of components
[N5]	US MIL-STD-1629	Failure Mode and Effects Analysis, National Technical Information Service, Springfield, VA. MIL 1629.
[N6]	Telcordia (Bellcore) Failure rate database and models	Statistical compilation of failure rate data over a wide range of applications along with models for estimating failure rates as a function of the application.
[N7]	Safety Equipment Reliability Handbook, 2003	exida.com L.L.C, Safety Equipment Reliability Handbook, 2003, ISBN 0-9727234-0-4
[N8]	Goble, W.M. 1998	Control Systems Safety Evaluation and Reliability, ISA, ISBN #1-55617-636-8. Reference on FMEDA methods

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	08732-0203, Sept 1, 2000	Schematic Internal Mag. Middle Board
[D2]	08732-0205 Feb 18, 2003	Schematic Drawing 8732 Upper Board
[D3]	08732-0200 July 7, 1997	Schematic Drawing 8732C Lower Board
[D4]	08732-0209 Oct 21, 2002	Schematic Drawing 8732C LOI
[D5]	08712-0740 Feb 6 2002	Schematic 8712 Plus

2.4.2 Documentation generated by *exida.com*

[R1]	FMEDA spreadsheet.xls	Failure rate calculations, 8732C Magnetic Flow Transmitter, October 13, 2003
[R2]	Ros 03-07-26 R001 V110.doc	FMEDA report, 8732C Magnetic Flow Transmitter, October 15, 2003

3 Product Description

The 8732C Magnetic Flow Transmitter is a four wire, 4 – 20 mA smart device. For safety instrumented systems usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. All other possible output variants are not covered by this report. The different devices can be equipped with or without display. Table 4 gives an overview of the different versions that belong to the considered 8732C Magnetic Flow Transmitter.

Table 4: Version overview

A	DC Power Option
B	AC Power Option

The 8732C Magnetic Flow Transmitter is classified as a Type B[2] device according to IEC 61508, having a hardware fault tolerance of 0.

The transmitter uses HART communications and uses a scalable frequency pulse output. The 8732C has an environmentally sealed compartment, making it ideal for harsh environment installations where moisture and contaminant infiltration is possible. Separate 0-ring seals provide isolation for the transmitter electronics, wiring compartment, and flow tube adapter.

[2] Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on documentation received from Rosemount Inc. and is documented in [R1] and [R2]. When the effect of a certain 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.

4.1 Description of the failure categories

In order to judge the failure behavior of the 8732C Magnetic Flow Transmitter, the following definitions for the failure of the product were considered.

Fail-Safe State	State where the process reaches a safe situation.
Fail Safe	Failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process. Safe failures are divided into safe detected (SD) and safe undetected (SU) failures.
Fail Dangerous	Failure that deviates the measured input state or the actual output by more than 2% of span and that leaves the output within active scale (including frozen output).
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics (These failures may be converted to the selected fail-safe state).
Fail High	Failure that causes the output signal to go to the maximum output current (> 21,5 mA, output saturate high)
Fail Low	Failure that causes the output signal to go to the minimum output current (< 3,6 mA, output saturate low)
Fail No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Undetected	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) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in [N1] which are only safe and dangerous, both detected and undetected. The reason for this is that, depending on the application, a Fail High or a Fail Low can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as either safe or dangerous.

The Annunciation Undetected failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. In IEC 61508 [N1] the No Effect and Annunciation Undetected failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

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.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an 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.com* in this FMEDA is from a proprietary component failure rate database derived using the Telcordia (N6) failure rate database/models, the SN29500 (N4) failure rate database and other sources. 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 similar to IEC 645-1, Class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

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 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.

4.3 Assumption

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 8732C Magnetic Flow Transmitter.

- Only a single component failure will fail the entire product
- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- The HART protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.

- The stress levels are average for an industrial environment and can be compared to the Ground Fixed classification of MIL-HNBK-217F. Alternatively, the assumed environment is similar to:
    - IEC 645-1, Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40ºC. Humidity levels are assumed within manufacturer's rating.
- External power supply failure rates are not included.

4.4 Behavior of the safety logic solver

Depending on the application, the following scenarios are possible:

- Low Trip: the safety function will go to the predefined fail-safe state when the process value below a predefined low set value. A current < 3.6mA (Fail Low) is below the specified trip-point.
- High Trip: the safety function will go to the predefined fail-safe state when the process value exceeds a predefined high set value. A current > 21.5mA (Fail High) is above the specified trip-point.

The Fail Low and Fail High failures can either be detected or undetected by a connected logic solver. The PLC Detection Behavior in Table 5 represents the under-range and over-range detection capability of the connected logic solver.

Table 5 Application example

Application	**PLC Detection Behavior**	l_{low}	l_{high}
Low trip	< 4mA	$= \lambda_{sd}$	$= \lambda_{du}$
Low trip	> 20mA	$= \lambda_{su}$	$= \lambda_{dd}$
Low trip	< 4mA and > 20mA	$= \lambda_{sd}$	$= \lambda_{dd}$
Low trip	-	$= \lambda_{su}$	$= \lambda_{du}$
High trip	< 4mA	$= \lambda_{dd}$	$= \lambda_{su}$
High trip	> 20mA	$= \lambda_{du}$	$= \lambda_{sd}$
High trip	< 4mA and > 20mA	$= \lambda_{dd}$	$= \lambda_{sd}$
High trip	-	$= \lambda_{du}$	$= \lambda_{su}$

In this analysis it is assumed that the logic solver is able to detect under-range and over-range currents, therefore the yellow highlighted behavior is assumed.

4.5 Results

Using reliability data extracted from the exida.com component reliability database the following failure rates resulted from the 8732C Magnetic Flow Transmitter FMEDA.

Table 6 Failure rates 8732C Magnetic Flow Transmitter – DC power option

Failure category				Failure rate (in FITs)
Fail High (detected by the logic solver)				6
Fail Low (detected by the logic solver)				566
	Fail detected (int. diag.)	480		
	Fail low (inherently)	86		
Fail Dangerous Undetected				318
No Effect				271
Annunciation Undetected				16

Table 7 Failure rates 8732C Magnetic Flow Transmitter – AC power option

Failure category				Failure rate (in FITs)
Fail High (detected by the logic solver)				6
Fail Low (detected by the logic solver)				582
	Fail detected (int. diag.)	514		
	Fail low (inherently)	68		
Fail Dangerous Undetected				328
No Effect				258
Annunciation Undetected				16

It is assumed that upon the detection of a failure the output will be sent downscale, all detected failure categories are sub-categories of the fail low failure category.

According to IEC 61508 [N1], the Safe Failure Fraction (SFF) of the 8732C Magnetic Flow Transmitter should be calculated. The SFF is the fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. As both the Fail High and Fail Low failure categories are assumed to be detected by the logic solver (regardless of the fact if their effect is safe or dangerous), the Safe Failure Fraction can be calculated independently of the 8732C Magnetic Flow Transmitter application.

This is reflected in the following formulas for SFF:

$SFF = 1 – \lambda_{du} / \lambda_{total}$

Note that according to IEC61508 definition the No Effect and Annunciation Undetected failures are classified as safe and therefore need to be considered in the Safe Failure Fraction calculation and are included in the total failure rate.

Table 8 Safe Failure Fraction of 8732C Magnetic Flow Transmitter

8732C Magnetic Flow Transmitter	SFF
8732C Magnetic Flow Transmitter – DC Power Option	73.0%
8732C Magnetic Flow Transmitter – AC power Option	72.4%

The architectural constraint type for 8732C Magnetic Flow Transmitter is B. The SFF and required SIL determine the level of hardware fault tolerance that is required per requirements of IEC 61508 [N1] or IEC 61511. The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL as well.

5 Using the FMEDA results

5.1.1 Converting failure rates to IEC 61508 format

The failure rates that are derived from the FMEDA for the 8732C Magnetic Flow Transmitter are in a format different from the IEC 61508 format. This section will explain how the failure rates can be converted into the IEC 61508 format.

First of all, depending on the application, the high and low failure rates of the 8732C Magnetic Flow Transmitter must be classified as either safe or dangerous. Assume an application where a safety action needs to be performed if the flow in a pipe drops below a certain level. The transmitter will therefore be configured with a low trip level. A low failure of the flowmeter will cause the transmitter output to go through the low trip level. Consequently the transmitter will indicate that the safety action needs to be performed. Therefore a low failure can be classified as a safe failure for this application. A high failure on the other hand will cause the flowmeter output to move away from the trip level and therefore not cause a trip. The failure will prevent the transmitter from indicating that the safety action needs to be performed and is therefore classified as a dangerous failure for this application.

Assuming that the logic solver can detect both over-range and under-range, a low failure can be classified as a safe detected failure and a high failure can be classified as a dangerous detected failure. For this application the following would then be the case:

8732C Magnetic Flow Transmitter – DC power option

$\lambda^{H} = \lambda^{DD} =$ 6 * 10^{-9} failures per hour

$\lambda^{L} = \lambda^{SD} =$ 566 * 10^{-9} failures per hour

$\lambda^{DU} =$ 318 * 10^{-9} failures per hour

8732C Magnetic Flow Transmitter – AC power option

$\lambda^{H} = \lambda^{DD} =$ 6 * 10^{-9} failures per hour

$\lambda^{L} = \lambda^{SD} =$ 582 * 10^{-9} failures per hour

$\lambda^{DU} =$ 328 * 10^{-9} failures per hour

In a similar way, the high and low failure rates can be classified as respectively safe detected and dangerous detected in case the application has a high trip level. The failure rates as displayed above are the same failure rates as stored in the exida.com equipment database that is part of the online SIL verification tool, SILver.

Furthermore the No Effect failures and Annuncation Undetected failure are classified as Safe Undetected failures according to IEC 61508. Note that these failures will not affect system reliability or safety, and should not be included in spurious trip calculations.

Note that the dangerous undetected failures will of course remain dangerous undetected.

5.1.2 PFD_{AVG} calculation 8732C Magnetic Flow Transmitter

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 8732C Magnetic Flow Transmitter (with DC power option). The failure rate data used in this calculation is displayed in Section 4.5.

The resulting PFD_{AVG} values for a variety of proof test intervals are displayed in Figure 1. As shown in the figure the PFD_{AVG} value for a single 8732C Magnetic Flow Transmitter DC power option with a proof test interval of 1 year equals 1.39E-03.

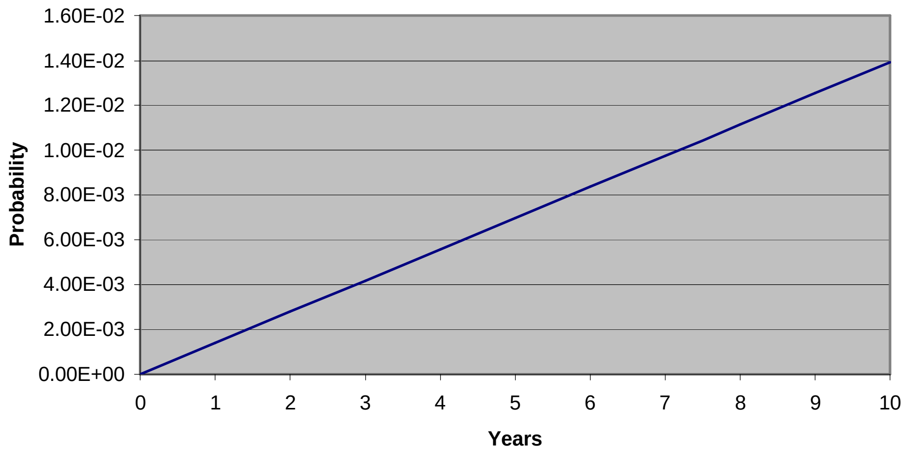

Figure 1: PFD_{AVG}(t) 8732C Magnetic Flow Transmitter – DC power option

For SIL 1 applications, the PFD_{AVG} value needs to be = 10^{-2} and < 10^{-1}. This means that for a SIL 1 application, the PFD_{AVG} for a 1-year Proof Test Interval of the 8732C Magnetic Flow Transmitter is equal to 1.4% of the range. 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

FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HART	Highway Addressable Remote Transducer
HFT	Hardware Fault Tolerance
PFD_{AVG}	Average Probability of Failure on Demand
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
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	"Non-Complex" component (using discrete elements); for details see 7.4.3.1.3 of IEC 61508-2
Type B component	"Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2

7 Status of the document

7.1 Liability

exida.com prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* 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.

7.2 Releases

Version:	V1	
Revision:	R1.0	
Version History:	V0, R1.0:	Initial version; October 13, 2003
	V1, R1.0:	Changes after review – corrected errors; October 15, 2003
Authors:	William Goble – John Grebe	
Review:	V0, R1.0	Rachel Amkreutz
Release status:	released	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Appendix A: Lifetime of critical components

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.3) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore 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).

Therefore it is obvious that the PFD_{AVG} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 4 shows the estimated useful lifetime of the limiting component type.

Table 4: Useful lifetime of electrolytic capacitors contributing to λ_{du}

Type	Useful life at 40°C
Capacitor (electrolytic) - Aluminium electrolytic, solid electrolyte	Appr. 90 000 Hours[3]

As the capacitors are the limiting factors with regard to the useful lifetime of the system, the useful lifetime should be limited to 10 years.

[3] The operating temperature has a direct impact on this time. Therefore already a small deviation from the ambient operating temperature reduces the useful lifetime dramatically. Capacitor life at lower temperatures follows "The Doubling 10°C Rule" where life is doubled for each 10°C reduction in operating temperature.