Failure Modes, Effects and Diagnostic Analysis

Project:
Limit Switch Box

Customer:
EUROTEC Antriebszubehör GmbH
Kressbronn
Germany

Contract No.: EUROTEC 10/01-84
Report No.: EUROTEC 10/01-84 R001
Version V1, Revision R0; June 2010

Stephan Aschenbrenner
Management summary

This report summarizes the results of the hardware assessment carried out on the Limit Switch Box in the version listed in the mechanical drawings referenced in section 2.4.1. The types EA, EV, EP Series 2008 and EBAS, EBAL, EBPS, EBPL belong to the considered Limit Switch Box.

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) can be calculated for a subsystem. For full assessment purposes all requirements of IEC 61508 must be considered.

For safety applications only the described types of the Limit Switch Box have been considered. All other possible variants and configurations are not covered by this report and need to be calculated separately. The individual sensors or switches which come with the Limit Switch Box have not been part of this analysis and must be considered separately.

EUROTEC Antriebszubehör GmbH and exida together did a quantitative analysis of the Limit Switch Box to calculate the failure rates using exida’s component database (see [N2]) for the different components. The failure rates used in this analysis are from the exida Electrical & Mechanical Component Reliability Handbook for Profile 4 ¹.

The Limit Switch Box is classified as a Type A² subsystem with a hardware fault tolerance of 0. For Type A subsystems with a hardware fault tolerance of 0 the SFF has to be > 60% for SIL 2 subsystems according to table 2 of IEC 61508-2.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.2.

It is important to realize that the “no effect” failures are included in the “safe” failure category according to IEC 61508:2000. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The following table shows how the above stated requirements are fulfilled for the considered Limit Switch Box.

¹ For details see Appendix 3.
² Type A subsystem: “Non-complex” subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
### Table 1: Limit Switch Box – failure rates per IEC 61508 ³

<table>
<thead>
<tr>
<th>Failure category</th>
<th>Failure rates (in FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fail Safe Detected</strong> ($\lambda_{SD}$)</td>
<td></td>
</tr>
<tr>
<td>Fail safe detected</td>
<td>0</td>
</tr>
<tr>
<td><strong>Fail Safe Undetected</strong> ($\lambda_{SU}$)</td>
<td>91</td>
</tr>
<tr>
<td>Fail safe undetected</td>
<td>0</td>
</tr>
<tr>
<td>No effect</td>
<td>91</td>
</tr>
<tr>
<td><strong>Fail Dangerous Detected</strong> ($\lambda_{DD}$)</td>
<td></td>
</tr>
<tr>
<td>Fail detected (detected by internal diagnostics)</td>
<td>0</td>
</tr>
<tr>
<td>Annunciation detected</td>
<td>0</td>
</tr>
<tr>
<td><strong>Fail Dangerous Undetected</strong> ($\lambda_{DU}$)</td>
<td>36</td>
</tr>
<tr>
<td>Fail dangerous undetected</td>
<td>36</td>
</tr>
<tr>
<td>No part</td>
<td>0</td>
</tr>
</tbody>
</table>

| Total failure rate (safety function)   | 127 FIT                |
| SFF ⁴                                  | 71%                    |
| DCₐ                                      | 0%                     |
| MTBF                                    | 899 years              |

| SIL AC ⁵                                | SIL2                   |

A user of the considered Limit Switch Box 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 4.4.1 along with all assumptions.

The failure rates are valid for the useful life of the considered Limit Switch Box (see Appendix 2) when operating as defined in the considered scenarios.

---

³ The individual sensors or switches which are fitted into the Limit Switch Box have not been part of this analysis and must be considered separately.

⁴ The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁵ 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.
Table of Contents

Management summary .................................................................................................... 2
1 Purpose and Scope .................................................................................................... 5
2 Project management .................................................................................................. 6
  2.1 *exida* .................................................................................................................. 6
  2.2 Roles of the parties involved .................................................................................. 6
  2.3 Standards / Literature used ................................................................................... 6
  2.4 Reference documents ............................................................................................ 6
    2.4.1 Documentation provided by the customer ..................................................... 6
    2.4.2 Documentation generated by *exida* ............................................................. 6
3 Description of the analyzed subsystem .................................................................... 7
4 Failure Modes, Effects, and Diagnostic Analysis ...................................................... 8
  4.1 Description of the failure categories ...................................................................... 8
  4.2 Methodology – FMEDA, Failure rates .................................................................... 8
    4.2.1 FMEDA .......................................................................................................... 8
    4.2.2 Failure rates .................................................................................................... 9
  4.3 Assumptions .......................................................................................................... 9
  4.4 Results ................................................................................................................... 10
    4.4.1 Limit Switch Box ............................................................................................ 11
5 Using the FMEDA results ...................................................................................... 12
  5.1 Example PFD<sub>AVG</sub> calculation .................................................................... 12
  5.2 Example SFF calculation ..................................................................................... 12
6 Terms and Definitions ............................................................................................. 13
7 Status of the document ............................................................................................ 14
  7.1 Liability ................................................................................................................ 14
  7.2 Releases ............................................................................................................... 14
  7.3 Release Signatures ............................................................................................... 14
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test .. 15
  Appendix 1.1: Proof tests to detect dangerous undetected faults............................. 15
Appendix 2: Impact of lifetime of critical components on the failure rate ................. 16
Appendix 3: Description of the considered profiles .................................................... 17
  Appendix 3.2: *exida* mechanical database .............................................................. 17
Appendix 4: Ordering code for the Limit Switch Box .................................................. 18
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 according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand (PFD_{AVG}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

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

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per 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 according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

**This assessment shall be done according to option 1.**

This document shall describe the results of the mechanical assessment carried out on the Limit Switch Box in the version listed in the mechanical drawings referenced in section 2.4.1. The types EA, EV, EP Series 2008 and EBAS, EBAL, EBPS, EBPL belong to the considered Limit Switch Box.

The information in this report can be used to evaluate whether a final element subsystem, including the described Limit Switch Box meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirement per IEC 61508.
2 Project management

2.1 exida

exida is one of the world’s leading 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 partnership company with offices around the world. exida 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 maintains a comprehensive failure rate and failure mode database on process equipment.

2.2 Roles of the parties involved

EUROTEC Antriebszubehör GmbH  Manufacturer of the Limit Switch Box.
exida  Performed the mechanical assessment according to option 1 (see section 1).

EUROTEC Antriebszubehör GmbH contracted exida in March 2010 with the FMEDA of the above mentioned device.

2.3 Standards / Literature used

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


2.4 Reference documents

2.4.1 Documentation provided by the customer

| D1 | EAE.pdf | Datasheet "Compact limit switch box EAE" |
| D2 | EVE.pdf | Datasheet "Compact limit switch box EVE" |
| D3 | EPE.pdf | Datasheet "Compact limit switch box EPE" |
| D4 | Z_EVP_19112008_a.pdf | Mechanical drawing "Endschalterbox Vestamid" Z_EVP_19112008_a of 19.11.08 |
| D5 | Stückliste-EVP2S01-28-IA.pdf | Parts list |
| D6 | Bestellschlüssel für Boxen.pdf | Ordering code for the Limit Switch Box |
| D7 | SIL-Handbuch-EUROTEC_V2.doc | Safety Manual of 11.03.10 |

2.4.2 Documentation generated by exida

| R1 | FMEDA_V7_Limit_Switch_box_V0R1.efm of 04.03.10 |
3 Description of the analyzed subsystem

The Limit Switch Box is considered to be a Type A subsystem with a hardware fault tolerance of 0. An overview of the different types is given in the following figures.

Figure 1: EAE  
Figure 2: EVE  
Figure 3: EPE  
Figure 4: EBAS  
Figure 5: EBAL  
Figure 6: EBPS  
Figure 7: EBPL

The individual sensors or switches which come with the Limit Switch Box have not been part of this analysis and must be considered separately. For the FMEDA it is assumed that the output of the Limit Switch Box is used as SIF input (not as a diagnostic of SIF).
4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with EUROTEC Antriebszubehör GmbH and is documented in [R1].

4.1 Description of the failure categories

In order to judge the failure behavior of the Limit Switch Box, the following definitions for the failure of the products were considered.

- **Fail-Safe State**: The fail-safe state is defined as the output providing a limit switch signal at the desired position.

- **Fail Safe**: Failure that causes the system to go to the defined fail-safe state without a demand from the process.

- **Fail Dangerous**: Failure that has the potential to not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

- **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. For the calculation of the SFF it is treated like a safe undetected 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. When calculating the SFF this failure mode is not taken into account. It is also not part of the total failure rate.

The “no effect” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508:2000 the “no effect” 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.

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) 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 is from a proprietary mechanical component failure rate database derived using field failure data from multiple sources and failure data from various databases. 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 exida Profile 4. 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. 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, physical abuse, or problems due to intermittent instrument air quality.

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”. Corrosion, erosion, etc. are considered age related (late life) or systematic failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

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 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the Limit Switch Box.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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.
- Materials are compatible with process conditions.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- The Limit Switch Box is installed per the manufacturer’s instructions.
- The stress levels are average for an industrial outdoor environment and can be compared to exida Profile 4 with temperature limits within the manufacturer’s rating. Other environmental characteristics are assumed to be within the manufacturer’s ratings.
- Only the described types are used for safety applications.
- All devices are operated in the low demand mode of operation.
4.4 Results

*exida* did the FMEDAs together with EUROTEC Antriebszubehör GmbH.

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

- $\lambda_{total}$ consists of the sum of all component failure rates of the Limit Switch Box. This means:
  
  $$
  \lambda_{total} = \lambda_{safe} + \lambda_{dangerous}
  $$

  
  $$
  SFF = 1 - \frac{\lambda_{dangerous}}{\lambda_{total}}
  $$

  
  $$
  MTBF = MTTF + MTTR = \left(1 / (\lambda_{total} + \lambda_{no\,part})\right) + 24\,h
  $$

  
  The individual sensors or switches which come with the Limit Switch Box need to be added to $\lambda_{safe}$ and $\lambda_{dangerous}$.
4.4.1 Limit Switch Box

The FMEDA carried out the Limit Switch Box leads under the assumptions described in section 4.3 and 4.4 and the definitions given in section 4.1 to the following failure rates:

<table>
<thead>
<tr>
<th>Failure category</th>
<th>Failure rates (in FIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Safe Detected ($\lambda_{SD}$)</td>
<td>0</td>
</tr>
<tr>
<td>Fail safe detected</td>
<td>0</td>
</tr>
<tr>
<td>Fail Safe Undetected ($\lambda_{SU}$)</td>
<td>91</td>
</tr>
<tr>
<td>Fail safe undetected</td>
<td>0</td>
</tr>
<tr>
<td>No effect</td>
<td>91</td>
</tr>
<tr>
<td>Fail Dangerous Detected ($\lambda_{DD}$)</td>
<td>0</td>
</tr>
<tr>
<td>Fail detected (detected by internal diagnostics)</td>
<td>0</td>
</tr>
<tr>
<td>Annunciation detected</td>
<td>0</td>
</tr>
<tr>
<td>Fail Dangerous Undetected ($\lambda_{DU}$)</td>
<td>36</td>
</tr>
<tr>
<td>Fail dangerous undetected</td>
<td>36</td>
</tr>
<tr>
<td>No part</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total failure rate (safety function)</strong></td>
<td><strong>127 FIT</strong></td>
</tr>
<tr>
<td><strong>SFF</strong></td>
<td><strong>71%</strong></td>
</tr>
<tr>
<td><strong>DC_D</strong></td>
<td><strong>0%</strong></td>
</tr>
<tr>
<td><strong>MTBF</strong></td>
<td><strong>899 years</strong></td>
</tr>
<tr>
<td><strong>SIL AC</strong></td>
<td><strong>SIL2</strong></td>
</tr>
</tbody>
</table>

6 The individual sensors or switches which are fitted into the Limit Switch Box have not been part of this analysis and must be considered separately.

7 The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

8 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. 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. The results must be considered in combination with PFD$_{AVG}$ values of other devices of a Safety Instrumented Function in order to determine suitability for a specific Safety Integrity Level.

5.1 Example PFD$_{AVG}$ calculation

An average Probability of Failure on Demand (PFD$_{AVG}$) calculation is performed for a single (1oo1) Limit Switch Box. The failure rate data used in this calculation are displayed in section 4.4.1. The resulting PFD$_{AVG}$ (for a variety of proof test intervals) values are displayed in Table 2. A mission time of 10 years and a MTTR of 24 hours have been considered. It is assumed that proof testing is performed with a proof test coverage of 90%, see Appendix 1.1.

For SIL2 applications, the PFD$_{AVG}$ value needs to be < 1.00E-02. This means that for a SIL2 application, the PFD$_{AVG}$ for a 1-year Proof Test Interval is equal to 3% of the allowed range.

Table 2: Limit Switch Box – PFD$_{AVG}$ values

<table>
<thead>
<tr>
<th>T[Proof] = 1 year</th>
<th>T[Proof] = 2 years</th>
<th>T[Proof] = 5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Switch Box</td>
<td>PFD$_{AVG}$ = 3.00E-04</td>
<td>PFD$_{AVG}$ = 4.42E-04</td>
</tr>
</tbody>
</table>

Figure 8 shows PFD$_{AVG}$ as a function of the proof test interval.

![Figure 8: PFD$_{AVG}$(t)](image)

5.2 Example SFF calculation

The SFF for the Limit Switch Box together with an individual sensor or switch can be calculated as follows:

\[
\text{SFF} = 1 - \left( \frac{\lambda_{DU (Box)} + \lambda_{DU (Sensor)}}{\lambda_{Box (Gesamt)} + \lambda_{Sensor (Gesamt)}} \right)
\]

Assuming that a used micro switch has a dangerous undetected failure rate of 30 FIT and a total failure rate of 150 FIT the SFF results in:

\[
\text{SFF} = 1 - \left( \frac{36 \text{ FIT} + 30 \text{ FIT}}{127 \text{ FIT} + 150 \text{ FIT}} \right) = 76\%
\]
### 6 Terms and Definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIT</td>
<td>Failure In Time (1x10^-9 failures per hour)</td>
</tr>
<tr>
<td>FMEDA</td>
<td>Failure Modes, Effects, and Diagnostic Analysis</td>
</tr>
<tr>
<td>HFT</td>
<td>Hardware Fault Tolerance</td>
</tr>
<tr>
<td>Low demand mode</td>
<td>Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Restoration</td>
</tr>
<tr>
<td>PFD_AVG</td>
<td>Average Probability of Failure on Demand</td>
</tr>
<tr>
<td>SFF</td>
<td>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.</td>
</tr>
<tr>
<td>SIF</td>
<td>Safety Instrumented Function</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>Type A subsystem</td>
<td>“Non-complex” subsystem (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.</td>
</tr>
<tr>
<td>T[Proof]</td>
<td>Proof Test Interval</td>
</tr>
</tbody>
</table>
7 Status of the document

7.1 Liability

exida prepares 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:
- V1R0: Review comments incorporated; June 23, 2010
- V0R1: Initial version; April 20, 2010

Authors: Stephan Aschenbrenner

Review:
- V0R1: Rachel Amkreutz (exida); June 21, 2010
  Melissa Berge (EUROTEC); April 21, 2010

Release status: Released to EUROTEC Antriebszubehör GmbH

7.3 Release Signatures

[Signatures]

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

Rachel Amkreutz, Safety Engineer
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

Appendix 1.1: Proof tests to detect dangerous undetected faults

A suggested proof test consists of the following steps, as described in Table 3.

Table 3 Steps for Proof Test

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Take appropriate action to avoid a false trip</td>
</tr>
<tr>
<td>2</td>
<td>Inspect the device for any visible damage, corrosion or contamination.</td>
</tr>
<tr>
<td>3</td>
<td>Force the Limit Switch Box to detect a desired position and verify that the desired position is correctly indicated.</td>
</tr>
<tr>
<td>4</td>
<td>Force the Limit Switch Box to detect a desired position at the opposite side and verify that the desired position is correctly indicated.</td>
</tr>
<tr>
<td>5</td>
<td>Restore the loop to full operation</td>
</tr>
<tr>
<td>6</td>
<td>Restore normal operation</td>
</tr>
</tbody>
</table>

It is assumed that the test will detect approximately 90% of possible “du” failures.
Appendix 2: Impact of lifetime of critical components on the failure rate

According to section 7.4.7.4 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 4.3) 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 meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. 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 4 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and therefore to the $PFD_{AVG}$ calculation and what their estimated useful lifetime is.

**Table 4: Useful lifetime of components with reduced useful lifetime contributing to $\lambda_{du}$**

<table>
<thead>
<tr>
<th>Type</th>
<th>Useful life</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanical parts</td>
<td>Approximately 10 years</td>
</tr>
</tbody>
</table>

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

---

*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.*
Appendix 3: Description of the considered profiles

Appendix 3.2: *exida* mechanical database

<table>
<thead>
<tr>
<th>Profile</th>
<th>Profile according to IEC60654-1</th>
<th>Ambient Temperature [°C]</th>
<th>Temperature Cycle [°C / 365 days]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Average (external)</td>
<td>Mean (inside box)</td>
</tr>
<tr>
<td>1</td>
<td>B2</td>
<td>30</td>
<td>60</td>
</tr>
<tr>
<td>2</td>
<td>C3</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>3</td>
<td>C3</td>
<td>25</td>
<td>45</td>
</tr>
<tr>
<td>4</td>
<td>D1</td>
<td>25</td>
<td>30</td>
</tr>
</tbody>
</table>

**PROFILE 1:**
Cabinet mounted equipment typically has significant temperature rise due to power dissipation but is subjected to only minimal daily temperature swings.

**PROFILE 2:**
Mechanical field products have minimal self heating and are subjected to daily temperature swings.

**PROFILE 3:**
Mechanical field products may have moderate self heating and are subjected to daily temperature swings.

**PROFILE 4:**
Unprotected mechanical field products with minimal self heating, are subject to daily temperature swings and rain or condensation.
Appendix 4: Ordering code for the Limit Switch Box

- Housing material:
  - A: Aluminum
  - P: Polystyrene
  - V: Stainless steel

- Mounting bracket:
  - P: PA (30% fiber glass)
  - E: Stainless steel

- Switch quantity:
  - 1: 1 switch
  - 2: 2 switches
  - 3: 3 switches
  - 4: 4 switches

- Switch type:
  - M: Mechanical
  - I: Inductive proximity
  - S: Slot type
  - D: Double sensor

- Hole spacing actuator:
  - 00: 50x25x20
  - 01: 80x30x20
  - 02: 80x30x30
  - 03: 130x30x30
  - 04: 130x30x50
  - 06: 80x30x40
  - 07: 130x30x40
  - 08: 50x25x30

- Housing color:
  - Black
  - Grey
  - Royal blue
  - Anthracite
  - White
  - Ruby red
  - Orange
  - Green
  - Navy blue
  - Red
  - Yellow
  - Turquoise

- Accessories:
  - 3D: 3D visual indication
  - MA: Solenoid valve connection (1 coil)
  - 2MA: Solenoid valve connection (2 coils)
  - DAE: Venting screw in the cover against condensation
  - M12: M12 plug connector
  - 2K: 2 x cable glands M20 frontal in parallel
  - OC: Visual indicator OPEN-CLOSED below the box

- Switch model:
  - See table