Failure Modes, Effects and Diagnostic Analysis

Project:
Solenoid Drivers
KFD2-SL2-(Ex)1.LK.vvcc
KFD2-SL2-(Ex)*(B).vvcc

Customer:
Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 06/09-23
Report No.: P+F 06/09-23 R029
Version V2, Revision R3, July 2008
Otto Walch,
Philipp Neumeier
Management summary

This report summarizes the results of the FMEDA carried out on the solenoid drivers KFD2-SL2-(Ex)*.**.vvcc. These types are without relays at the output and are equipped with or without fault detection for short circuit and lead breakage.

Table 1: Version overview of the KFD2-SL2-(Ex)*.** modules

<table>
<thead>
<tr>
<th>Type</th>
<th>Channels</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KFD2-SL2-(Ex)1.B</td>
<td>1</td>
<td>without loop monitoring (fault detection for short circuit and lead breakage)</td>
</tr>
<tr>
<td>KFD2-SL2-(Ex)1</td>
<td>1</td>
<td>with loop monitoring (fault detection for short circuit and lead breakage)</td>
</tr>
<tr>
<td>KFD2-SL2-(Ex)1.LK</td>
<td>1</td>
<td>with loop monitoring and fault signal output (fault detection for short circuit and lead breakage)</td>
</tr>
<tr>
<td>KFD2-SL2-(Ex)2.B</td>
<td>2</td>
<td>without loop monitoring (fault detection for short circuit and lead breakage)</td>
</tr>
<tr>
<td>KFD2-SL2-(Ex)2</td>
<td>2</td>
<td>with loop monitoring (fault detection for short circuit and lead breakage)</td>
</tr>
</tbody>
</table>

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.

The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be \( \geq 10^{-3} \) to \( < 10^{-2} \) for SIL 2 safety functions. However, as the module under consideration is only one part of an entire safety function it should not claim more than 10% of this range, i.e. they should be better than or equal to \( 10^{-3} \) for SIL 2.

The module under evaluation can be considered to be Type A\(^3\) component.

For Type A components the SFF has to be between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

The listed SN29500 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 40°C (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.

---

1 The term “vvcc” is a placeholder for multiple voltage/current combinations.
2 These additional features are not part of the safety function and therefore not considered in the calculations.
3 Type A component: “Non-complex” component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.
The following tables show which modules (considering one input and one output being part of the safety function) fulfill this requirement.

Table 2: Summary of solenoid drivers with regard to SIL 2 requirements

<table>
<thead>
<tr>
<th>Name</th>
<th>$T[\text{Proof}] = 1$ year</th>
<th>$T[\text{Proof}] = 2$ years</th>
<th>$T[\text{Proof}] = 5$ years</th>
<th>SFF</th>
<th>PFH</th>
</tr>
</thead>
<tbody>
<tr>
<td>KFD2-SL2-(Ex)1.LK</td>
<td>PFD$_{AVG} = 4.49E-05$</td>
<td>PFD$_{AVG} = 8.98E-05$</td>
<td>PFD$_{AVG} = 2.24E-04$</td>
<td>98 %</td>
<td>10.3 FIT</td>
</tr>
<tr>
<td>KFD2-SL2-(Ex)*(.B)</td>
<td>PFD$_{AVG} = 4.25E-05$</td>
<td>PFD$_{AVG} = 8.50E-05$</td>
<td>PFD$_{AVG} = 2.12E-04$</td>
<td>98 %</td>
<td>9.7 FIT</td>
</tr>
</tbody>
</table>

The boxes marked in green (■) mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to be better than $10^{-3}$.

A user of the Pepperl+Fuchs solenoid drivers can utilize the failure rates given in section 5.1 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).

The two channels on the KFD2-SL2-(Ex)2(.B) modules should not be used for one safety function as they contain common components.
Table of Contents

Management summary ........................................................................................................... 2
1 Purpose and Scope ........................................................................................................... 5
2 Project management ........................................................................................................ 6
  2.1 Roles of the parties involved ..................................................................................... 6
  2.2 Standards / Literature used ....................................................................................... 6
  2.3 Reference documents ............................................................................................... 6
    2.3.1 Documentation provided by the customer ......................................................... 6
    2.3.2 Documentation generated by exida ................................................................... 7
3 Description of the analyzed modules .............................................................................. 8
  3.1 KFD2-SL2-(Ex)1.LK .................................................................................................. 8
  3.2 KFD2-SL2-(Ex)*(.B) ............................................................................................... 9
4 Failure Modes, Effects, and Diagnostics Analysis ....................................................... 10
  4.1 Description of the failure categories ........................................................................ 10
  4.2 Methodology – FMEDA, Failure rates ..................................................................... 11
    4.2.1 FMEDA ........................................................................................................... 11
    4.2.2 Failure rates ..................................................................................................... 11
    4.2.3 Assumptions ..................................................................................................... 12
5 Results of the assessment ............................................................................................... 13
  5.1 KFD2-SL2-(Ex)1.LK ............................................................................................... 14
  5.2 KFD2-SL2-(Ex)*(.B) ............................................................................................... 15
6 Terms and Definitions ..................................................................................................... 16
7 Status of the document ................................................................................................... 17
  7.1 Releases ................................................................................................................... 17
  7.2 Release Signatures ................................................................................................... 17
Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test .. 18
Appendix 2: Impact of lifetime of critical components on the failure rate ................. 20
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 EN 954-1. 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\textsubscript{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 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 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 hardware assessment according to IEC 61508 carried out on the solenoid drivers KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B) equipped with or without fault detection for short circuit and lead breakage.

The information in this report can be used to evaluate whether the solenoid drivers KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B) meet the average Probability of Failure on Demand (PFD\textsubscript{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. It does not consider any calculations necessary for proving intrinsic safety.
2 Project management

2.1 Roles of the parties involved
Pepperl+Fuchs Manufacturer of the solenoid drivers.
exida Did the FMEDAs together with the determination of the Safe Failure Fraction (SFF) and calculated the Probability of Failure on Demand (PFD) using Markov models.

Pepperl+Fuchs GmbH contracted exida in September 2006 and June 2008 with the FMEDA of the above mentioned module.

2.2 Standards / Literature used
The services delivered by exida were performed based on the following standards / literature.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[N2]</td>
<td>SN 29500</td>
</tr>
<tr>
<td>[N5]</td>
<td>FMD-97, RAC 1997</td>
</tr>
</tbody>
</table>

2.3 Reference documents

2.3.1 Documentation provided by the customer

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[D1]</td>
<td>01-7066 C of 05.09.05</td>
</tr>
<tr>
<td>[D2]</td>
<td>017937a.pdf</td>
</tr>
<tr>
<td>[D3]</td>
<td>BOM_200542_SL2_EX1_LK.pdf</td>
</tr>
<tr>
<td>[D4]</td>
<td>Changes_Impact_EX1LK_R0V1.pdf</td>
</tr>
<tr>
<td>[D5]</td>
<td>AW KFD2-SL2-(Ex)1.LK SiL Assessment DDE-0870 SP EX2-Version.msg</td>
</tr>
<tr>
<td>[D6]</td>
<td>Auszug FMEDA KFD2-SL2-(EX)1-LK V0 R1_kom.xls</td>
</tr>
</tbody>
</table>
### 2.3.2 Documentation generated by exida

<table>
<thead>
<tr>
<th>[D7]</th>
<th>Block_SL2_Ex2.doc</th>
<th>Block diagrams KFD2-SL2-(Ex)2*</th>
</tr>
</thead>
<tbody>
<tr>
<td>[D8]</td>
<td>Block_SL2_Ex1_LK.doc</td>
<td>Block diagram KFD2-SL2-(Ex)1.LK</td>
</tr>
</tbody>
</table>

| [R1] | FMEDA KFD2-SL2-EX2 V2 R4.0 of October 01, 2007 |
3 Description of the analyzed modules

The KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B) solenoid drivers supply and switch the intrinsically safe field devices (valves) in hazardous areas.

The devices have a logic input that is isolated from the power supply.

The field devices are controlled by means of these logic inputs.

Voltage signals in a range of DC 16 V .... 30 V are accepted as 1-signals. The 0-signal must be within a range of DC 0 V... 5 V.

3.1 KFD2-SL2-(Ex)1.LK

The solenoid driver KFD2-SL2-(Ex)1.LK has an additional fault signal output.

Figure 1: Block diagram of KFD2-SL2-(Ex)1.LK
3.2 KFD2-SL2-(Ex)*(.B)

Figure 2: Block diagram of KFD2-SL2-(Ex)2(.B)
4 Failure Modes, Effects, and Diagnostics Analysis

4.1 Description of the failure categories

In order to judge the failure behavior of the solenoid drivers KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B), the following definitions for the failure of the product were considered.

Fail-Safe State The fail-safe state is defined as the output being de-energized.

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

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 and signalized via the fault relay (These failures may be converted to the selected fail-safe state).

Residual 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 “Residual” failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. The “Residual” 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 Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the 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, etc.) 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 from the Siemens SN 29500 failure rate database. 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 60654-1, 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.
4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the solenoid driver KFD2-SL2-(Ex)1.LK and KFD2-SL2-(Ex)*(.B).

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- Complete practical fault insertion tests can demonstrate that the diagnostic coverage (DC) corresponds to the assumed DC in the FMEDAs.
- 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 time to restoration after a safe failure is 8 hours.
- External power supply failure rates are not included.
- The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40°C (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. Humidity levels are assumed within manufacturer's rating.
- Only the described versions are used for safety applications.
5 Results of the assessment

*exida* did the FMEDAs together with Pepperl+Fuchs.

The two channels on the KFD2-SL2-(Ex)*(,B) modules should not be used for one safety function as they contain common components.

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

\[ \lambda_{\text{total}} = \lambda_{\text{safe}} + \lambda_{\text{dangerous}} + \lambda_{\text{residual}} \]

\[ \text{SFF} = 1 - \frac{\lambda_{\text{dangerous}}}{\lambda_{\text{total}}} \]

For the calculation of the PFD$_{\text{AVG}}$ the following Markov model for a 1oo1 system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

The proof test time was changed using the FMEDA tool of *exida* as a simulation tool. The results are documented in the following sections.

Abbreviations:

- d One channel has failed dangerous
- s One channel has failed safe
- \( \lambda_d \) Failure rate of dangerous failures
- \( \lambda_s \) Failure rate of safe failures
- \( T_{\text{Repair}} \) Repair Time

Figure 3: Markov model
5.1 KFD2-SL2-(Ex)1.LK

The FMEDA carried out on the KFD2-SL2-(Ex)1.LK module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

\[
\begin{align*}
\lambda_{\text{total}} &= 7.14 \times 10^{-7} \text{ 1/h} \\
\lambda_{\text{safe}} &= 3.38 \times 10^{-7} \text{ 1/h} \\
\lambda_{\text{dangerous}} &= 1.03 \times 10^{-8} \text{ 1/h} \\
\lambda_{\text{residual}} &= 3.66 \times 10^{-7} \text{ 1/h} \\
\lambda_{\text{no part}} &= 3.38 \times 10^{-8} \text{ 1/h} \\
\text{SFF} &= 98 \% \\
\text{PFH} &= 10.3 \text{ FIT}
\end{align*}
\]

The PFD was calculated for three different proof times using the Markov model as described in Figure 3.

<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>PFD(_{AVG}) = 4.49E-05</td>
<td>PFD(_{AVG}) = 8.98E-05</td>
<td>PFD(_{AVG}) = 2.24E-04</td>
</tr>
</tbody>
</table>

The boxes marked in green (■) mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to be better than \(10^{-3}\).

Figure 5 shows the time dependent curve of PFD\(_{AVG}\).

Figure 5: PFD\(_{AVG}(t)\)
5.2 KFD2-SL2-(Ex)*(.B)

The FMEDA carried out on the KFD2-SL2-(Ex)*(.B) module leads under the assumptions described in section 4.2.3 and 5 to the following failure rates and SFF:

- $\lambda_{total} = 6.52E-07 \text{ 1/h}$
- $\lambda_{safe} = 3.20E-07 \text{ 1/h}$
- $\lambda_{dangerous} = 9.70E-09 \text{ 1/h}$
- $\lambda_{residual} = 3.22E-07 \text{ 1/h}$
- $\lambda_{no\ part} = 2.90E-08 \text{ 1/h}$
- SFF = 98%
- PFH = 9.7 FIT

The PFD was calculated for three different proof times using the Markov model as described in Figure 3.

<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>PFD$_{AVG}$ = 4.25E-05</td>
<td>PFD$_{AVG}$ = 8.50E-05</td>
<td>PFD$_{AVG}$ = 2.12E-04</td>
</tr>
</tbody>
</table>

The boxes marked in green (■) mean that the calculated PFD values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to be better than $10^{-3}$.

Figure 5 shows the time dependent curve of PFD$_{AVG}$.
### 6 Terms and Definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMEDA</td>
<td>Failure Mode Effect and Diagnostic Analysis</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of Failure on Demand</td>
</tr>
<tr>
<td>PFD\text{AVG}</td>
<td>Average Probability of Failure on Demand</td>
</tr>
<tr>
<td>PFH</td>
<td>Probability of a dangerous Failure per Hour</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>SIS</td>
<td>Safety Instrumented System</td>
</tr>
<tr>
<td>Type A component</td>
<td>“Non-complex” component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.</td>
</tr>
</tbody>
</table>

- $\lambda_{\text{dangerous}}$: Failure rate $\lambda$ of all dangerous failures
- $\lambda_{\text{safe}}$: Failure rate $\lambda$ of all safe failures
- $\lambda_{\text{total}}$: Total failure rate $\lambda$ (overall failure rate of all components)
7 Status of the document

7.1 Releases

Version History:  
V1R1  External comments incorporated; October 10, 2007  
V2R0  Philipp Neumeier: Added KFD2-SL2-(Ex)1.LK, July 3, 2008  
V2R1  Pepperl+Fuchs review comments incorporated, July 4, 2008  
V2R2  Pepperl+Fuchs review comments incorporated, July 7, 2008  

Authors:  
Otto Walch, Philipp Neumeier  

Review:  
V0R1  Stephan Aschenbrenner (exida); October 1, 2007  
V1R0  Harald Eschelbach (Pepperl + Fuchs); October 2, 2007  
V2R0  Harald Eschelbach (Pepperl + Fuchs); July 3, 2008  
V2R1  Harald Eschelbach (Pepperl + Fuchs); July 7, 2008  

Release status: Released to Pepperl+Fuchs.

7.2 Release Signatures

Dipl.-Ing. (FH) Otto Walch, Manager Hazardous Locations

Dipl.-Ing. (FH) Philipp Neumeier, Safety Engineer

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

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.

Table 3 and Table 4 shows an importance analysis of the ten most critical dangerous undetected faults and indicate how these faults can be detected during proof testing.

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

Table 3: Importance Analysis for Solenoid driver KFD2-SL2-(Ex)*(.B)

<table>
<thead>
<tr>
<th>Component</th>
<th>% of total $\lambda_{du}$</th>
<th>Detection through</th>
</tr>
</thead>
<tbody>
<tr>
<td>P12</td>
<td>17.01%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>P7</td>
<td>17.01%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>P10</td>
<td>17.01%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>P5</td>
<td>17.01%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>C30</td>
<td>10.31%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>N14</td>
<td>8.76%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>C18</td>
<td>5.15%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>R57</td>
<td>1.86%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>R23</td>
<td>1.86%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>N5</td>
<td>1.55%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
</tbody>
</table>

Table 4: Importance Analysis for Solenoid driver KFD2-SL2-(Ex)1.LK

<table>
<thead>
<tr>
<th>Component</th>
<th>% of total $\lambda_{du}$</th>
<th>Detection through</th>
</tr>
</thead>
<tbody>
<tr>
<td>P7</td>
<td>24.39%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>P12</td>
<td>16.10%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>P5</td>
<td>16.10%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>Component</td>
<td>Failure Rate</td>
<td>Test Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>------------------</td>
</tr>
<tr>
<td>P10</td>
<td>16.10%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>C30</td>
<td>9.76%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>N14</td>
<td>8.29%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>C18</td>
<td>4.88%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>N5</td>
<td>1.46%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>R57</td>
<td>1.17%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
<tr>
<td>R23</td>
<td>1.17%</td>
<td>100% functional test with monitoring of the output signal</td>
</tr>
</tbody>
</table>
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 4.2.3) this only applies provided that the useful lifetime\(^4\) 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, electrolytic 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\(_{\text{AVG}}\) 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.

The circuit of the Solenoid drivers KFD2-SL2-(Ex)\(^1\)1.LK and KFD2-SL2-(Ex)\(^4\)\((.B)\) do not contain any components with reduced useful lifetime that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

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

---

\(^4\) 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.