FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis

Device Model Number:

KFD0-RO-(Ex)2

Project:

Relay module

Pepperl+Fuchs GmbH
Mannheim
Germany

Table of content:

Reviewers:

Role
Project Leader (PL)
Product Management
Functional Safety Manager

History of this document:

Revision of this document	Reviewed by / [Reviewer abbreviation within the detailed comment list]	Changes since last version
Index 0 From 2008-Apr-08	Sülük Hasan	Newly created
Index A From 2012-Apr-05	Kindermann Michael DP.MKI	Changed format to fit to recent reports, added non-ex version
Index A From 2012-Jun-04	Kindermann Michael DP.MKI	New calculation under FS-0014PF-27
Index A From 2012-Jun-25	Kindermann Michael DP.MKI	Formal corrections SIL 3 description in chapter 1, formatting chapter 1, proof testing

1. Report Summary

This report summarizes the results of the FMEDA carried out on the relay modules KFD0-RO-(Ex)2 with circuit diagram 51-0364A dated 6/5/97.

Failure rates used in this analysis are basic failure rates from the Siemens Standard SN29500.

According to table 2 of IEC 61508-1, the average PFD for systems operating in Low Demand Mode for type A devices has to be <10^{-2} for SIL 2 safety functions and <10^{-3} for SIL 3 safety functions. For Systems operating in High Demand or Continuous Mode of Operation the PFH value has to be <10^{-6} h^{-1} for SIL 2 and <10^{-7} h^{-1} for SIL 3.

However, as the modules under consideration are only part of an entire safety function they should not claim more than 10% of this range, i.e. they should be lower than 10^{-3} for SIL 2 and 10^{-4} for SIL 3 in Low Demand Mode respectively lower than 10^{-7} h^{-1} for SIL 2 and 10^{-8} h^{-1} for SIL 3 in High Demand Mode.

Since the relay modules KFD0-RO-(Ex)2 are considered to be Type A devices with a hardware fault tolerance of "0", the SFF shall be >60% for SIL 2 and >90% for SIL 3 according to table 2 of IEC 61508-2.

Acc. Table 1: Overall parameters for KFD0-RO-(Ex)2

Parameters acc. to IEC61508	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	DTS[1]
MTBF[2]	351 years

[1] DTS: de-energize to safe

[2] acc. To SN29500. This value is valid for the complete device with two channels and includes failures which are not part of the safety function.

For one channel used in the safety function, the following safety characteristic values apply.

Acc. Table 2: KFD0-RO-(Ex)2 1oo1 structure

Parameters acc. to IEC61508:2000	Variables
SIL	2
HFT	0
$\lambda_{sd}+\lambda_{su}$	85.2 FIT
λ_{dd}	0 FIT
λ_{du}	40 FIT
$\lambda_{total\ (Safety\ function)}$ [1]	160.4 FIT
$\lambda_{total\ (Device)}$	162.6 FIT
SFF	75.0 %
PFH	$4.0*10^{-8}$ 1/h
PFD_{avg} for T_{proof} = 1 year	$1.75*10^{-4}$
PFD_{avg} for T_{proof} = 2 years	$3.50*10^{-4}$
PFD_{avg} for T_{proof} = 5 years	$8.76*10^{-4}$

[1] For this value failures of safety relevant components that have no effect on the safety function are counted.

For two channels used in the safety function, the inputs are combined by a wire bridge or steered by two channels of the ESD system. The relay outputs are switched in series. The following safety characteristic values apply.

Acc. Table 3: KFD0-RO-(Ex)2 1oo2 structure

Parameters acc. To IEC61508:2000	Variables
SIL	3
HFT	1[2]
$\lambda_{sd}+\lambda_{su}$	170.4 FIT
λ_{dd}	0 FIT
λ_{du}	4.4 FIT
$\lambda_{total\ (Safety\ function)}$ [1]	320.8 FIT
$\lambda_{total\ (Device)}$	325.2 FIT
SFF	98.6 %
PFH	$4.42*10^{-9}$ 1/h
PFD_{avg} for T_{proof} = 1 year	$1.94*10^{-5}$
PFD_{avg} for T_{proof} = 2 years	$3.87*10^{-5}$
PFD_{avg} for T_{proof} = 5 years	$9.68*10^{-5}$

[1] For this value failures of safety relevant components that have no effect on the safety function are counted.

[2] The redundance of the circuit parts has already been regarded in the probabilistic calculations. The failure probabilities, SFF, PFD and PFH need to be regarded as complete values for one single SIL 3 safety path with HFT = 0.

2. Functional description of the device KFD0-RO-(Ex)2

The devices have a logic input of 15 V DC .. 30 V DC and a relay output.

The device KFD0-RO-Ex2 is an isolated barrier used for intrinsic safety applications. It switches circuits inside the hazardous area. The device KFD0-RO-2 is used as a signal conditioner, transferring a voltage signal to a relay output. A fuse and an electronic current-limiting circuit protect the inputs.

Both outputs are galvanically isolated to the inputs. The inputs are not polarized and share a common reference potential.

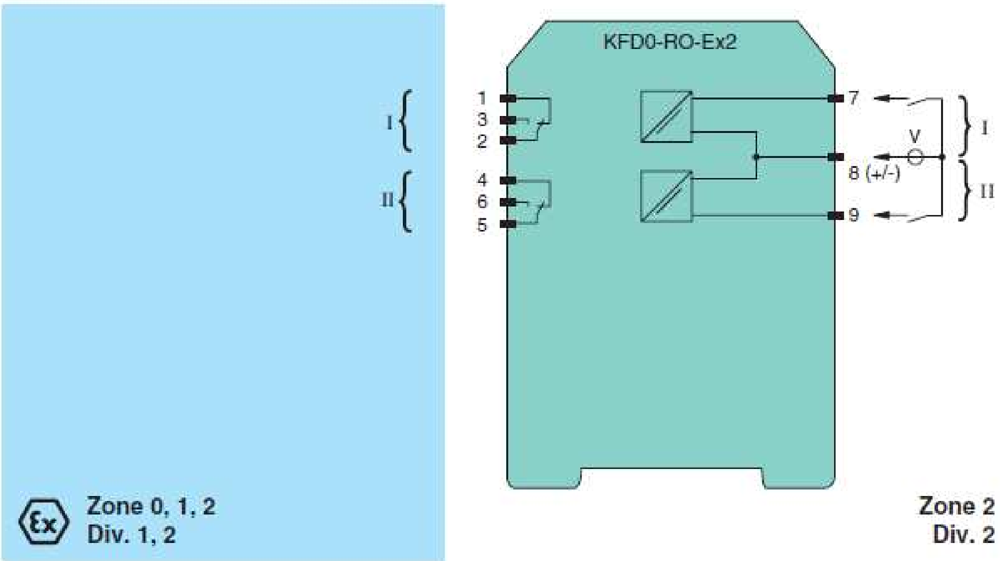

Fig. 1: Connection of the KFD0-RO-(Ex)2

3. Definition of the failure categories

The FMEDA was done and is documented in EDM under the number FS-0014PF-26.

In order to judge the failure behaviour of the isolated barrier KFD0-RO-(Ex)2, the following definitions for the failure of the product were considered:

Fail-safe state:

Defined as the output being de-energized or when no supply is on the device.

Safe failure:

A failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.

Dangerous failure:

When the device does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state).

Fail high / Fail low failure: not used in this evaluation.

No Effect failure:

A failure of a component that is part of the safety function but has no effect on the safety function. For the calculation of the SFF it is treated like a safe undetected failure.

Annunciation failure:

This failure does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). For calculation of the SFF it is treated like a safe undetected failure.

Not part:

Not part means that this component is not part of the safety function, but 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 ($\lambda_{\text{total (Safety function)}}$).

4. Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the KFD0-RO-(Ex)2 system.

- Failure rates are constant, wear out mechanisms are not included.
- The device shall claim less than 10 % of the total failure budget for a SIL2 safety loop.
- For a SIL2 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (Safety Instrumented Function) should be smaller than 10^{-2}, hence the maximum allowable PFD_{avg} value would then be 10^{-3}.
- For a SIL2 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10^{-6} per hour, hence the maximum allowable PFH value would then be 10^{-7} per hour.
- For a SIL3 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (Safety Instrumented Function) should be smaller than 10^{-3}, hence the maximum allowable PFD_{avg} value would then be 10^{-4}.
- For a SIL3 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10^{-7} per hour, hence the maximum allowable PFH value would then be 10^{-8} per hour.
- Since the circuit has a Hardware Fault Tolerance of zero and is considered to be a type A component, the SFF must be > 60 % according to table 2 of IEC 61508-2 for SIL2 (sub)system.
- Since the circuit has a Hardware Fault Tolerance of zero and is considered to be a type A component, the SFF must be > 90 % according to table 2 of IEC 61508-2 for SIL3 (sub)system.
- Failure rates based on the Siemens standard SN29500.
- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 8 hours (e. g. remove sensor burnout).
- During the absence of the device for repairing, measures have to be taken to ensure the safety function (for example: substitution by an equivalent device).
- 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 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 ºC. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 ºC, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.
- For lifetime estimation also refer to the data sheet containing information on the maximum mechanical / electrical switching cycles for the relays.
- All modules are operated in the Low demand mode or High demand mode of operation.

5. Results of the Assessment

The following tables show how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 6 by exida.com.

Table 1: Overall parameters for KFD0-RO-(Ex)2

Parameters acc. to IEC61508	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	DTS[1]
MTBF[2]	351 years

[1] DTS: de-energize to safe

[2] acc. To SN29500. This value is valid for the complete device with two channels and includes failures which are not part of the safety function.

For one channel used in the safety function, the following safety characteristic values apply.

Table 2: KFD0-RO-(Ex)2 1oo1 structure

Parameters acc. to IEC61508:2000	**Variables**
SIL	2
HFT	0
$\lambda_{sd}+\lambda_{su}$	85.2 FIT
λ_{dd}	0 FIT
λ_{du}	40 FIT
$\lambda_{total\ (Safety\ function)}$[1]	160.4 FIT
$\lambda_{total\ (Device)}$	162.6 FIT
SFF	75.0 %
PFH	$4.0 \cdot 10^{-8}$ 1/h
PFD_{avg} for T_{proof} = 1 year	$1.75 \cdot 10^{-4}$
PFD_{avg} for T_{proof} = 2 years	$3.50 \cdot 10^{-4}$
PFD_{avg} for T_{proof} = 5 years	$8.76 \cdot 10^{-4}$

[1] For this value failures of safety relevant components that have no effect on the safety function are counted.

For two channels used in the safety function, the inputs are combined by a wire bridge or steered by two channels of the ESD system. The relay outputs are switched in series. The following safety characteristic values apply.

Table 3: KFD0-RO-(Ex)2 1oo2 structure

Parameters acc. to IEC61508:2000	**Variables**
SIL	3
HFT	1[2]
$\lambda_{sd}+\lambda_{su}$	170.4 FIT
λ_{dd}	0 FIT
λ_{du}	4.4 FIT
$\lambda_{total\ (Safety\ function)}$ [1]	320.8 FIT
$\lambda_{total\ (Device)}$	325.2 FIT
SFF	98.6 %
PFH	$4.42*10^{-9}$ 1/h
PFD_{avg} for T_{proof} = 1 year	$1.94*10^{-5}$
PFD_{avg} for T_{proof} = 2 years	$3.87*10^{-5}$
PFD_{avg} for T_{proof} = 5 years	$9.68*10^{-5}$

[1] For this value failures of safety relevant components that have no effect on the safety function are counted.
[2] The redundance of the circuit parts has already been regarded in the probabilistic calculations. The failure probabilities, SFF, PFD and PFH need to be regarded as complete values for one single SIL 3 safety path with HFT = 0.

6. Possibilities to Reveal Dangerous Undetected Faults During the Proof Test

The Proof test shall reveal the dangerous undetected (du) faults, which have been noticed during the FMEDA.

Dangerous failures are limited to the correct function of the relays. The proof test recognizes dangerous concealed faults that would affect the safety function of the plant.

The proof test procedure is available from www.pepperl-fuchs.com.

According to the results of the analysis, the KFD0-RO-(Ex)2 has to be subjected to a proof test in intervals of 5 years. It is possible that the device is used under other circumstances than specified within the assumptions for the FMEDA assessment. The calculations for the safety loop can also reveal that the device may claim a different amount of the PFD value (standard is 10%). Both effects have an influence on the proof test time.

It is the responsibility of the operator to select a suitable proof test time.

7. Useful life time

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

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 failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful life time 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 life time is valid.

However, according to IEC 61508-2, a useful life time, based on experience, should be assumed. Experience has shown that the useful life time often lies within a range period of about 8 ... 12 years.

Our experience has shown that the useful life time of a Pepperl+Fuchs product can be higher

- if there are no components with reduced life time in the safety path (like electrolytic capacitors, relays, flash memory, opto coupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

Please note that the useful life time refers to the (constant) failure rate of the device. The effective life time can be higher.

Please also be aware that the lifetime can be limited by the maximum mechanical / electrical switching cycles for the relays. For further information see the data sheet or the safety manual.

8. Abbreviations

FMEDA	Failure Modes, Effects and Diagnostic Analysis
PFD	Probability of dangerous failure on demand
PFH	Probability of dangerous failure per hour
SFF	Safe Failure Fraction
HFT	Hardware Fault Tolerance
SIL	Safety Integrity Level
MTBF	Mean Time Between Failure
T_{proof}	Proof time
AVG	Average
DTS	De-energize to safe

9. Literature

Manufacturing Documents:

51-0364A dated 6/5/97, Circuit diagram for KFD0-RO-Ex2 isolated barriers.

Bill of material for KFD0-RO-Ex2 part no. 038975 dated 15-Apr-2006.

FS-0014PF-26 V1R0 from 15.4.2006, electronic FMEDA

FS-0014PF-27 dated 2012-May-10

Standards:

IEC 61508-2:2000 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Requirements

SN 29500 parts 1 – 13, Failure rates of components

FMD-91, RAC 1991 Failure Mode / Mechanism Distributions

FMD-97, RAC 1997 Failure Mode / Mechanism Distributions

Appendix: Safety Characteristic Values for IEC 61508:2010

For use with edition 2 of the standard, all failures that have no effect on the safety function are excluded from the evaluation. Therefore the following values apply.

Table 4: KFD0-RO-(Ex)2 1oo1 structure

Parameters acc. to IEC61508:2010	Variables
SIL	2
HFT	0
$\lambda_{sd}+\lambda_{su}$	85.2 FIT
λ_{dd}	0 FIT
λ_{du}	40 FIT
$\lambda_{total\ (Safety\ function)}$	125.2 FIT
$\lambda_{total\ (Device)}$ [1]	162.6 FIT
SFF	68.0 %
PFH	$4.0 \cdot 10^{-8}$ 1/h
PFD_{avg} for T_{proof} = 1 year	$1.75 \cdot 10^{-4}$
PFD_{avg} for T_{proof} = 2 years	$3.50 \cdot 10^{-4}$
PFD_{avg} for T_{proof} = 5 years	$8.76 \cdot 10^{-4}$

[1] This value is valid for the complete device with two channels and includes failures which are not part of the safety function.

For two channels used in the safety function, the inputs are combined by a wire bridge or steered by two channels of the ESD system. The relay outputs are switched in series. The following safety characteristic values apply.

Table 5: KFD0-RO-(Ex)2 1oo2 structure

Parameters acc. To IEC61508:2010	**Variables**
SIL	3
HFT	1[2]
$\lambda_{sd}+\lambda_{su}$	170.4 FIT
λ_{dd}	0 FIT
λ_{du}	4.4 FIT
$\lambda_{total\ (Safety\ function)}$	174.4 FIT
$\lambda_{total\ (Device)}$ [1]	325.2 FIT
SFF	97.4 %
PFH	$4.42 \cdot 10^{-9}$ 1/h
PFD_{avg} for T_{proof} = 1 year	$1.94 \cdot 10^{-5}$
PFD_{avg} for T_{proof} = 2 years	$3.87 \cdot 10^{-5}$
PFD_{avg} for T_{proof} = 5 years	$9.68 \cdot 10^{-5}$

[1] This value is valid for the complete device with two channels and includes failures which are not part of the safety function.

[2] The redundance of the circuit parts has already been regarded in the probabilistic calculations. The failure probabilities, SFF, PFD and PFH need to be regarded as complete values for one single SIL 3 safety path with HFT = 0.