FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis

Device Designation:

KFD0-CS-Ex*.54*
and
KFD0-CS-Ex*.56*

Project:

X7300

Pepperl+Fuchs GmbH
Mannheim
Germany

1. Report Summary

This report summarizes the results of the FMEDA carried out on the transformer-isolated repeaters for fire alarm and smoke alarm signals KFD0-CS-Ex*.54* and KFD0-CS-Ex*.56* with circuit diagram 251-5072B from 2009-Jan-27. It is not valid for obsolete devices with part no. #072221, #107496 and #107497.

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^{-1} for SIL1 safety functions or < 10^{-3} for SIL3 safety functions. For Systems operating in High Demand or Continuous Mode of Operation the PFH value has to be < 10^{-5} 1/h for SIL1 or < 10^{-7} 1/h for SIL3. However, as the modules under consideration are only part of an entire safety function they should not claim more than 10% of this range. For Low Demand Mode the PFD_{avg} should be lower than 10^{-2} for SIL1 or 10^{-4} for SIL3. For High Demand Mode, the PFH should be lower than 10^{-6} 1/h for SIL1 or 10^{-8} 1/h for SIL3.

Since the repeaters KFD0-CS-Ex*.54* and KFD0-CS-Ex*.56* are considered to be Type A devices with a hardware fault tolerance of “0”, the SFF shall be $\geq$ 90% for SIL3 according to table 2 of IEC 61508-2.

2. Overview of the safety characteristic values

The following table shows under which conditions the described modules fulfill these requirements.

Acc. to table 2: KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56* 1oo1 structure

Parameters acc. to IEC61508:2010	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Bidirectional Communication ensured
HFT	0
SIL (SC)	3
λ_{s}	0 FIT
λ_{dd}	60 FIT
λ_{du}	5.7 FIT
$\lambda_{\text{total (Safety function)}}$	66 FIT
$\lambda_{\text{no effect}}$	65 FIT
$\lambda_{\text{not part}}$	17.0 FIT
SFF[1]	91 %
PTC	100 %
MTBF[2]	770 years
PFH	$5.74 * 10^{-9}$ 1/h
PFD_{avg} for T_1 = 1 year	$2.51 * 10^{-5}$
PFD_{avg} for T_1 = 2 years	$5.03 * 10^{-5}$
PFD_{avg} for T_1 = 5 years	$1.26 * 10^{-4}$
Safety Response Time	50 µs (.54 version) / 250 µs (.56 version)

[1] "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the safety values / SFF.

[2] Acc. to SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.

Acc. to table 3: KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56* 1oo1 structure

Parameters acc. to IEC61508:2010	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Correct Analog Signal Transfer
HFT	0
SIL (SC)	1
λ_{s}	0 FIT
λ_{dd}	34.0 FIT
λ_{du}	34.2 FIT
$\lambda_{\text{total (Safety function)}}$	68 FIT
$\lambda_{\text{no effect}}$	58 FIT
$\lambda_{\text{not part}}$	22.2 FIT
SFF[1]	49 %
PTC	100 %
MTBF[2]	770 years
PFH	$3.4 * 10^{-8}$ 1/h
PFD_{avg} for T_1 = 1 year	$1.49 * 10^{-4}$
PFD_{avg} for T_1 = 2 years	$2.98 * 10^{-4}$
PFD_{avg} for T_1 = 5 years	$7.49 * 10^{-4}$
Safety Response Time	50 µs (.54 version) / 250 µs (.56 version)

[1] "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the safety values / SFF.

[2] Acc. to SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.

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]	Date of Review	Changes since last version
V 0 Rev. 1	DP.MKI	2015-May-27	Newly created
V 0 Rev. 2	DP.MKI	2015-Jun-15	Update including FMEDA Report
V 1 Rev. 0	DP.MKI	2015-Jun-23	From SIL 2 to SIL 3, corrected SFF
V 1 Rev. 1	DP.MKI	2015-Jul-23	Added a further table for the safety function without communication. Index A
V 1 Rev. 2	DP.MKI	2015-Aug-19	Added Edition 1 and Edition 2 values
V 2 Rev. 0	DP.MKI	2016-Jan-14	Corrected safety function description and safe state

3. Functional Description of the analysed Devices KFD0-CS-Ex*.54* / .56*

The devices are the transformer-isolated repeaters for fire alarm and smoke alarm signals. They provide 2-wire connection for fire alarm and smoke alarm devices.
For the **KFD0-CS-Ex*.54***, current input is 1 .. 20 mA. The safety relevant data is transferred on the same signal lines with AC signals up to 6 V. The fall time of the digital signal must be smaller than 50 µs and the current in the hazardous area must be bigger than 1 mA.
For the **KFD0-CS-Ex*.56***, current input is 0 .. 41 mA. The safety relevant data is transferred on the same signal lines with AC signals in the range of Esserbus / Esserbus plus levels. The rise and fall times of the digital signal must be smaller than 250 µs.

This isolated barrier is used for intrinsic safety applications. It provides a current output to power fire alarm and smoke alarm devices in a hazardous area and transfers the signal from that sensor to the safe area.

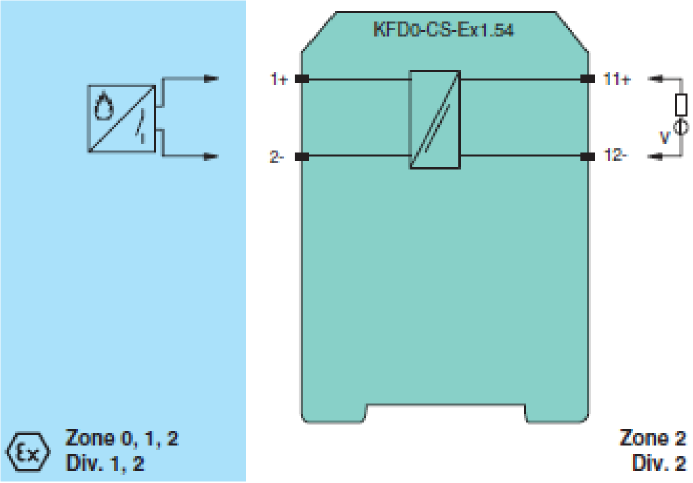

Fig. 1: Connection of the KFD0-CS-Ex1.54 representing all devices in this evaluation

Table 1: Connection Features

	KFD0-CS-Ex*.54*	**KFD0-CS-Ex*.56***
Input (left side)		
Terminals	KL+1 / KL-2	KL+1 / KL-2
Transmission range (AC)	0 .. 6 V	Esserbus / Esserbus plus
Input operating current	1 .. 20 mA	0 .. 41 mA
Output (right side)		
Terminals	KL11+ / KL12-	KL11+ / KL12-
Output operating current	1 .. 20 mA	0 .. 41 mA

Output supply voltage	4 V ≤ U_{in} ≤ 24 V:
	≥ U_{in} – (0.38V/mA * I) - 0.5 V
		for 3 V ≤ U_{in} ≤ 19 V:
		approx. U_{in} - (150 Ω x output current) - 1.0 V
		for 19 V < U_{in} ≤ 42 V:
		approx. 19 V - (150 Ω x output current) - 1.0 V

4. Definition of the failure categories

The FMEDA was done and is documented in EDM under FS-0082PF-26A and FS-0082PF-26A2. This isolator is used as part of a smart fire alarm system.

There are two possibilities for establishing a safety function using these devices. In one case (Case A), the bidirectional communication between the fire alarm system and the alarms must be ensured. In the other case (Case B), the analog signal transfer of the device must work correctly.

In order to judge the failure behaviour of the transformer-isolated repeaters for fire alarm and smoke alarm signals KFD0-CS-Ex*.54* and KFD0-CS-Ex*.56*, the following definitions for the failure of the product were considered:

Fail-safe state: None

Safety function:
Case A: Bidirectional communication ensured.
This includes sufficient supply for the field devices to be able to communicate.
Case B: Correct analog signal transfer according to data sheet. This requires:

- The device output is not increased by more than 0.5 mA or reduced by more than 1 V at maximum load current.
- Enough voltage is available to supply the field devices in the alarm state.
- The monitored input current is within the allowed current range (1 – 20 mA or 1 – 41 mA depending on device type).

Safe failure: As the output has no reserved safe state condition there are no safe failures.

Dangerous undetected failure:
Case A: causes the device output to increase by more than 0.5 mA or reduce by more than 1 V at maximum load current without breakdown in communication and without leaving the expected current range or field device supply voltage range.
Case B: causes the device output to increase by more than 0.5 mA or reduce by more than 1 V at maximum load current without leaving the expected current range or field device supply voltage range.

Dangerous detected failure:
Case A: Any failure which causes incoherence in the bidirectional communication or causes the supply to leave the expected current output range or supply voltage range.
Case B: Any failure which causes the fire alarm system to leave the expected current output range or supply voltage range.

Fail high / Fail low / Annunciation / Not considered failure:
Not used.

No effect failure (Residual, Don't care):
Failure of a component that is part of the safety function but has no effect on the safety function. The device output may increase by less than 0.5 mA or decrease by less than 1 V.

Not part:
None of the failure modes has an effect on the safety function. Nonetheless it is part of the circuit diagram and 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 ($\lambda_{\text{total (Safety function)}}$).

Safety Response Time:
The time that is needed to transfer an input signal of a device to its output according to the safety function.

5. Assumptions

The following assumptions were made during the Failure Modes, Effects and Diagnostic Analysis of the KFD0-CS-Ex*.54* and KFD0-CS-Ex*.56*.

- The device shall claim less than 10 % of the total failure budget for a SIL3 safety loop.
- For a SIL1 application operating in Low Demand Mode the total PFD_{avg} value of the SIF (Safety Instrumented Function) should be smaller than 10^{-1}, hence the maximum allowable PFD_{avg} value would then be 10^{-2}.
- For a SIL1 application operating in High Demand Mode of operation the total PFH value of the SIF should be smaller than 10^{-5} per hour, hence the maximum allowable PFH value would then be 10^{-6} 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.
- Failure rates based on the Siemens standard SN29500.
- Failure rates are constant, wear out mechanisms are not included.
- External power supply failures are not included.
- Since the circuit has a Hardware Fault Tolerance of zero and is considered to be a type A component, the SFF must be > 90 % for a SIL3 (sub)system according to table 2 of IEC 61508-2.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HDBK-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.

- It was assumed that the appearance of a safe error (e. g. output in safe state) would be repaired within 8 hours.
- 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 application program in the safety logic solver is constructed in such a way that all currents below 1 mA or above 40 mA (20 mA for KFD0-CS-Ex*.54*) are detected and lead to the safe state.
- Devices with part no. #072221, #107496, #107497 have the same name but are based on older designs. These devices are not evaluated within this assessment.

6. Results of the assessment according to EN/IEC 61508:2010

The following table shows how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 7.1.18 by exida.com.

These values are calculated for one channel of the device.

Table 2: KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56* 1oo1 structure

Parameters acc. to EN/IEC 61508:2010	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Bidirectional Communication ensured
HFT	0
SIL (SC)	3
λ_{s}	0 FIT
λ_{dd}	60 FIT
λ_{du}	5.7 FIT
$\lambda_{\text{total (Safety function)}}$	66 FIT
$\lambda_{\text{no effect}}$	65 FIT
$\lambda_{\text{not part}}$	17.0 FIT
SFF[1]	91 %
PTC	100 %
MTBF[2]	770 years
PFH	$5.74 * 10^{-9}$ 1/h
PFD_{avg} for T_1 = 1 year	$2.51 * 10^{-5}$
PFD_{avg} for T_1 = 2 years	$5.03 * 10^{-5}$
PFD_{avg} for T_1 = 5 years	$1.26 * 10^{-4}$
Safety Response Time	50 µs (.54 version) / 250 µs (.56 version)

[1] "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the safety values / SFF.

[2] acc. To SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.

Table 3: KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56* 1oo1 structure

Parameters acc. to EN/IEC 61508:2010	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Correct Analog Signal Transfer
HFT	0
SIL (SC)	1
λ_{s}	0 FIT
λ_{dd}	34.0 FIT
λ_{du}	34.2 FIT
$\lambda_{\text{total (Safety function)}}$	68 FIT
$\lambda_{\text{no effect}}$	58 FIT
$\lambda_{\text{not part}}$	22.2 FIT
SFF[1]	49 %
PTC	100 %
MTBF[2]	770 years
PFH	$3.4 * 10^{-8}$ 1/h
PFD_{avg} for T_1 = 1 year	$1.49 * 10^{-4}$
PFD_{avg} for T_1 = 2 years	$2.98 * 10^{-4}$
PFD_{avg} for T_1 = 5 years	$7.49 * 10^{-4}$
Safety Response Time	50 µs (.54 version) / 250 µs (.56 version)

[1] "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the safety values / SFF.

[2] Acc. to SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.

7. Possibilities to Reveal Dangerous Undetected Faults during the Proof Test

The Proof test shall reveal dangerous undetected (du) faults if any have occurred during the proof test interval and were not detected before.

Table 3 shows an importance analysis of the dangerous undetected faults and indicate in how far these faults are detected during proof testing. The proof test procedure is available from www.pepperl-fuchs.com. All failures are detected during the proof test (PTC = 100%) as all such faults are located in the direct signal path and the deviation between input and output can easily be found.

Table 3: Importance analysis of dangerous undetected failures of KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56*

Component	% of total λ_{DU} Bidirectional Communication ensured	% of total λ_{DU} Correct Analog Signal Transfer	Detection by
L4, L6	-	23,41 %	100% functional test
IC1	17,42 %	11,71 %	
L5	-	13,17 %	
P3	-	7,32 %	
C18	17,42 %	2,93 %	
NZ16	12,19 %	-	
NZ7	12,19 %	-	
IC2	10,45 %	8,78 %	
T1	10,45 %	7,90 %	
P17	8,71 %	-	
N10	8,71 %	-	
NZ10 – NZ13	-	6,44 %	
R6, R24, R7	1,78 %	-	

8. Periodic Proof Testing

The voltage repeater module can be proof tested by executing a proof test procedure according to a procedure available from www.pepperl-fuchs.com. The proof test recognizes dangerous concealed faults that would affect the safety function of the plant.

According to the results of the analysis, the KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56* have to be subjected to a proof test in intervals of not exceeding 1 year when assuming 10% of the failure budget.

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 can have an influence on the proof test time.

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

9. 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.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime. 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.

10. Results of the assessment according to EN 61508:2000

The following table shows how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 7.1.18 by exida.com.

These values are calculated for one channel of the device.

Table 3: KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56* 1oo1 structure

Parameters acc. to EN/IEC 61508:2000	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Bidirectional Communication ensured
HFT	0
SIL	3
λ_{s} [1]	65 FIT
λ_{dd}	60 FIT
λ_{du}	5.7 FIT
$\lambda_{total\ (Safety\ function)}$	131 FIT
SFF	95.6 %
PTC	100 %
MTBF[2]	770 years
PFH	$5.7 * 10^{-9}$ 1/h
PFD_{avg} for T_1 = 1 year	$2.51 * 10^{-5}$
PFD_{avg} for T_1 = 2 years	$5.03 * 10^{-5}$
PFD_{avg} for T_1 = 5 years	$1.26 * 10^{-4}$
Safety Response Time	50 µs (.54 version) / 250 µs (.56 version)

[1] Failures in parts that are part of the safety function but do not influence the safety function (“no effect”) are regarded as safe undetected.

[2] Acc. to SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.

Table 4: KFD0-CS-Ex*.54* / KFD0-CS-Ex*.56* 1oo1 structure

Parameters acc. to EN/IEC 61508:2000	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Correct Analog Signal Transfer
HFT	0
SIL	2
λ_s [1]	58 FIT
λ_{dd}	34.0 FIT
λ_{du}	34.2 FIT
λ_{total} (Safety function)	126 FIT
SFF	72 %
PTC	100 %
MTBF[2]	770 years
PFH	$3.4 * 10^{-8}$ 1/h
PFD_{avg} for T_1 = 1 year	$1.49 * 10^{-4}$
PFD_{avg} for T_1 = 2 years	$2.98 * 10^{-4}$
PFD_{avg} for T_1 = 5 years	$7.49 * 10^{-4}$
Safety Response Time	50 µs (.54 version) / 250 µs (.56 version)

[1] Failures in parts that are part of the safety function but do not influence the safety function are regarded as safe undetected.

[2] Acc. to SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.

11. 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
PTC	Proof Test Coverage
SIL (SC)	Safety Integrity Level (Systematic Capability)
MTBF	Mean Time between Failures
T_1	Proof time
AVG	Average
PLC	Programmable Logic Controller

12. Literature

Manufacturing Documents

251-5072B from 2009-Jan-29, Circuit diagram for KFD0-CS-Ex*.54* and KFD0-CS-Ex*.56*
255-5060B from 2009-Apr-06, Layout for KFD0-CS-Ex*.54* and KFD0-CS-Ex*.56*
Bill of material for KFD0-CS-Ex1.54 part no. 207802 dated 2015-Jan-27
FS-0082PF-27 V1R0 from 2016-Jan-14

Standards

IEC 61508-1:1998 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – General Part
IEC 61508-2:2000 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Requirements
IEC 61508-1:2010 (Edition 2) Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – General Part
IEC 61508-2:2010 (Edition 2) 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