


FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis

Device:
KFD2-VM-Ex1.35.L


Project:
1-channel isolated barrier
for
De-energized to safe

Pepperl+Fuchs GmbH
Mannheim
Germany

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Apr-27
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.MKI
	KFD2-VM-Ex1.35.L	approved	
		norm	
			FS-0065PF-20A sheet 1 of 10

Index


1.	FMEDA Documentation	3
2.	Device Safety Parameters	5
3.	Functional Description	6
4.	Failure Modes, Effect and Diagnostic Analysis	7
4.1	Description of the Failure Categories	7
4.2	Assumptions	8
5.	Proof Testing	9
6.	Useful life time	10

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2011-Apr-27
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.MKI	FS-0065PF-20A
	KFD2-VM-Ex1.35.L	approved		
			norm	

template: FTM-0027_1

1. Document Revision History

Revision of this document	Changes
V 1 Rev. 0	Newly created
V 1 Rev. 1	Added revision history table. Added remarks regarding switch operation.
V 2 Rev. 0	Put into EDM

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Apr-27
 Mannheim	FMEDA – Report	respons.	DP.MKI
	KFD2-VM-Ex1.35.L	approved	
		norm	
			FS-0065PF-20A sheet 3 of 10

template: FTM-0027_1

2. FMEDA Documentation


Manufacturer information:
 Pepperl + Fuchs GmbH
 68301 Mannheim / Germany

Input Documents:

EDM	Document name	Remarks
-	Bill of materials part #103076 (main device and sub-assemblies)	-
51-0628A	Schematic Complete device KFD2-VM-Ex1.35.L	-
01-3247B	Schematic transformer part U2	-
FS-0042EA-26	Electronic FMEDA	-
103076_ENG	Device data sheet dated 2010-07-08	-

Used standards:

EN/IEC 61508-1:1998 - Functional safety of electrical / electronic / programmable electronic safety-related systems – General requirements
 EN/IEC 61508-2:2000 - Functional safety of electrical / electronic / programmable electronic safety-related systems – Requirements for electrical / electronic / programmable electronic safety-related systems
 SN29500-1:2004 – SN29500-14:1994: - Failure rates of components

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2011-Apr-27
 Mannheim	FMEDA – Report	respons.	DP.MKI	FS-0065PF-20A
	KFD2-VM-Ex1.35.L	approved		
			norm	

template: FTM-0027_1

3. Device Safety Parameters

This report summarizes the results of the FMEDA carried out on the 1-channel isolated barrier KFD2-VM-Ex1.35.L.

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 has to be $<10^{-2}$ for SIL2 safety functions. For Systems operating in High demand or continuous mode of operation the PFH value has to be $<10^{-6} h^{-1}$ for SIL2. 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 SIL2 in Low demand mode respectively lower than $10^{-7} h^{-1}$ for SIL2 in High demand mode.

The isolated barrier KFD2-VM-Ex1.35.L is considered to be a Type A device with a hardware fault tolerance (HFT) of "0".

The following tables show under which conditions the described modules fulfill these requirements.

Table 2.1: Device used in 1oo1 structure

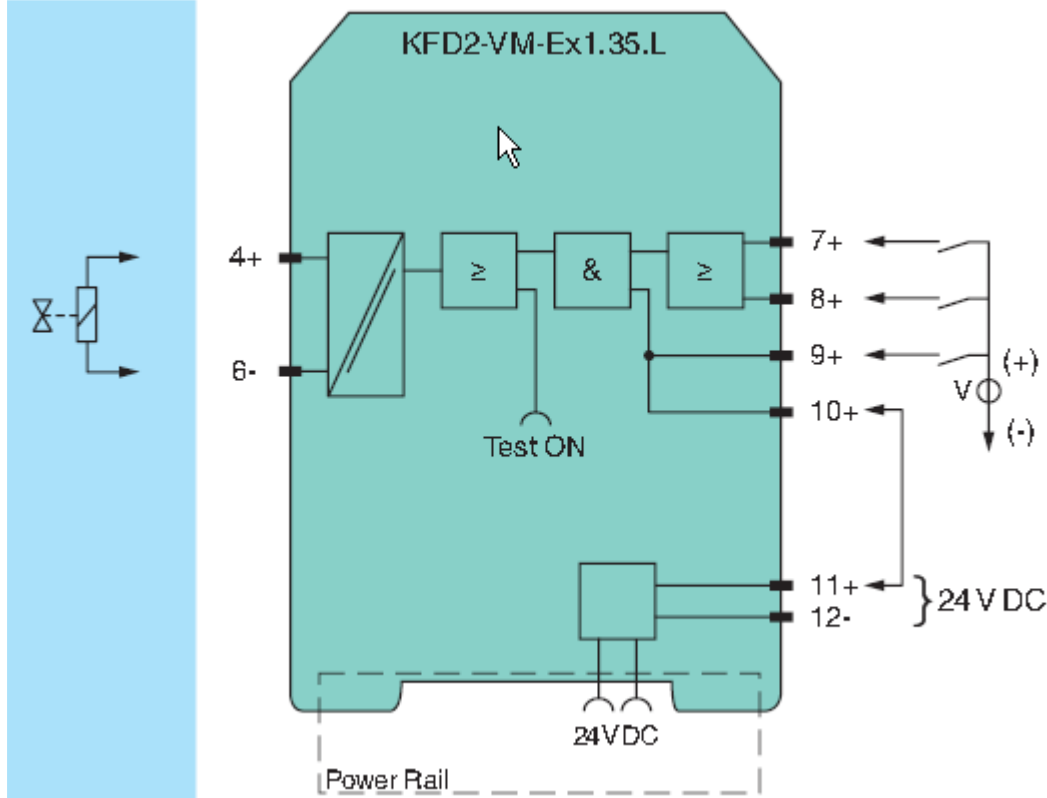
Parameters acc. to IEC61508	Variables
Assessment type and documentation	FMEDA
Device type	A
Demand mode	Low demand mode or High demand mode
Safety Function	De-energize to safe
HFT	0
SIL	2
$\lambda_{sd} + \lambda_{su}$	72.8 FIT
λ_{dd}	0 FIT
λ_{du}	12.9 FIT
λ_{total} (Safety function)	199 FIT
SFF	93.5%
MTBF ¹	543 years
PFH	$1.29 \cdot 10^{-8} 1/h$
PFD _{avg} for T ₁ = 1 year	$5.65 \cdot 10^{-5}$
T _{proof_max} ²	17.5 years
Reaction time	< 70 msec
¹ acc. To SN29500. This value includes failures which are not part of the safety function. MTTR = 8h ² For SIL2 applications no proof test has to be carried out, the calculated proof time is higher than the useful lifetime (T _{proof_max} for SIL2 is >17 years).	

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Apr-27
 Mannheim	FMEDA – Report	respons.	DP.MKI
	KFD2-VM-Ex1.35.L	approved	
		norm	
			FS-0065PF-20A sheet 5 of 10

4. Functional Description

The device is powered externally using a 24 V DC power supply. It has three logic inputs and one electronic output. Additionally a test socket is available for manual activation of the output. SIL 2 is reached when the device is used as de-energized to safe. For this the safe state is reached when the output is de-energized. The test socket must not be operated within the process as the output is energized by this, activating the unsafe state.

Connection:



Inputs 7+ / 8+: The input signals are combined with a logical 'or'. 0-Signal is nominal 0 V .. 5 V DC, 1-Signal is nominal 15 V .. 30 V.

Input 9+: The input signals 7+ and 8+ are only leading to an activated output if input 9+ is active. 0-Signal is nominal 0 V .. 5 V DC, 1-Signal is nominal 15 V .. 30 V DC.

Output 4+ / 6-: The device contains a binary output. A logical 1-Signal at the output is given with min. values for the on state 17 mA / 15.3 V

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Apr-27
 Mannheim	FMEDA – Report	respons.	DP.MKI
	KFD2-VM-Ex1.35.L	approved	
		norm	
			FS-0065PF-20A sheet 6 of 10

template: FTM-0027_1


5. Failure Modes, Effect and Diagnostic Analysis

The FMEDA was done and is documented in EDM under the number [FS-0065PF-26].

4.1 Description of the Failure Categories

In order to judge the failure behaviour of the relay module KFD2-VM-Ex1.35.L, the following definitions for the failure of the product were considered:

- Safe:** Failure that plays a part in implementing the safety function that: a) results in the spurious operation of the safety function to put the EUC (equipment under control) into a safe state or maintain a safe state; or, b) increases the probability of the spurious operation of the safety function to put the EUC (equipment under control) into a safe state or maintain a safe state.
- Dangerous:** Failure that energizes the output while de-energized state is required (the input states are not considered to energize the output).
- No Effect:** 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.
- Not part:** Component is not part of the safety function, but part of the circuit diagram and is listed for completeness. It is used for the MTBF of the complete device, not for any values related to the safety functions.


CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2011-Apr-27
 Mannheim	FMEDA – Report	respons.	DP.MKI	FS-0065PF-20A
	KFD2-VM-Ex1.35.L	approved		
			norm	

template: FTM-0027_1

4.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the KFD2-VM-Ex1.35.L.

- The user needs to ensure that the test input is protected against misuse while operation. The test input is energizing the output, leading to the unsafe state.
- Failure rates are constant, wear out mechanisms are not included.
- Failure rates based on the Siemens standard SN29500.
- The device shall claim less than 10 % of the total failure budget for a SIL2 safety loop.
- The device is considered of type “A” with a hardware fault tolerance (HFT) of 0 (non complex component as described in 7.4.3.2.1.of IEC 61508).
- Since the circuit has a Hardware Fault Tolerance of 0 and it is a type A component, the SFF must be > 60 % according to table 2 of IEC 61508-2 for a SIL2 (sub)system.
- 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 °C. Humidity levels are assumed within manufacturer's rating.
- 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 must be assumed.
- All components failure modes are known.
- All devices in the loop are operated in the Low demand mode or High demand mode of operation.
- 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 repair time subsequent to a safe failure (output de-energized while assumed to be energized) is 8 hours.

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2011-Apr-27
 Mannheim	FMEDA – Report	respons.	DP.MKI	FS-0065PF-20A
	KFD2-VM-Ex1.35.L	approved		
			norm	

template: FTM-0027_1

6. Proof Testing

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


Proof testing is easily done by a test regarding the function of the device.

According to the results of the analysis (P+F calculation tool), the devices have to be subject of a proof test in intervals of 17 years.

Usually no proof test has to be carried out, because the calculated proof test interval (17 years) is higher than the useful lifetime. Where a proof test is regarded necessary testing is done by simply testing the logical function. Precautions have to be taken that the de-energized or energized output is not leading to any unwanted reaction in the process.

Table 5.1: Proof testing

Input Pin 7	Input Pin 8	Input Pin 9	Reaction
1-Signal	1-Signal	0-Signal	Output de-energized
0-Signal	0-Signal	1-Signal	Output de-energized
1-Signal	0-Signal	1-Signal	Output energized

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Apr-27
 Mannheim	FMEDA – Report	respons.	DP.MKI
	KFD2-VM-Ex1.35.L	approved	
		norm	
			FS-0065PF-20A sheet 9 of 10

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.

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2011-Apr-27
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.MKI	FS-0065PF-20A
	KFD2-VM-Ex1.35.L	approved		
			norm	

template: FTM-0027_1