



FMEDA – Report Failure Modes, Effects and Diagnostic Analysis

Project Voltage Repeater KFD2-VR4-Ex1.26

**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-Aug-8
 PEPPERL+FUCHS Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	sheet 1 of 11

Table of Content

1	Report summary	3
2	Result of the assessment	4
3	Functional description of the analysed module KFD2-VR4-Ex1.26	5
4	Definition of the failure categories	6
5	Assumptions for the FMEDA	7
6	Safety relevant values for the modules	8
7	Possibilities to Reveal Dangerous Undetected Faults During the Proof Test	9
8	Periodic Proof Testing	9
9	Useful life time	10
10	Abbreviations	11
11	Literature	11

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	


1 Report summary

This report summarizes the results of the FMEDA carried out on the Voltage Repeater KFD2-VR4-Ex1.26 with circuit diagram 251-5067D from 16-Jan-2009 and layout 05-5189D from 05-Feb-2009.

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 $<10^{-6} h^{-1}$. 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} in Low demand mode respectively lower than $10^{-7} h^{-1}$ in High demand mode.

Since the module is considered to be a Type A device with a hardware fault tolerance of zero, the SFF shall be $\geq 60\%$ according to table 2 of IEC 61508-2.


CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	

2 Result of the assessment

The following table shows under which conditions the described module (considering one input and one output being part of the safety function, always with activated line fault detection) fulfils these requirements.

Acc. to table 1: KFD2-VR4-Ex1.26 1oo1 structure

Parameters acc. to IEC61508	Variables
Assessment Type and Documentation	FMEDA Report
Device type	A (only Hardware)
Mode of protection	Low demand mode or High demand mode
HFT	0
SIL (hardware)	2
$\lambda_{sd} + \lambda_{su}$ ¹	385 FIT
λ_{dd}	0 FIT
λ_{du}	73.5 FIT
λ_{total} (Safety function)	458.5 FIT
$\lambda_{not\ part}$	7.3 FIT
SFF	83.9%
MTBF ²	245 years
PFH	$7.4 * 10^{-8}$ 1/h
PFD _{avg} for T ₁ = 1 year	$3.22 * 10^{-4}$
PFD _{avg} for T ₁ = 3 year	$9.66 * 10^{-4}$
PFD _{avg} for T ₁ = 5 year	$1.61 * 10^{-3}$
T _{proof_max}	3.1 years
Safety Response Time	12.5 μ s
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	

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	

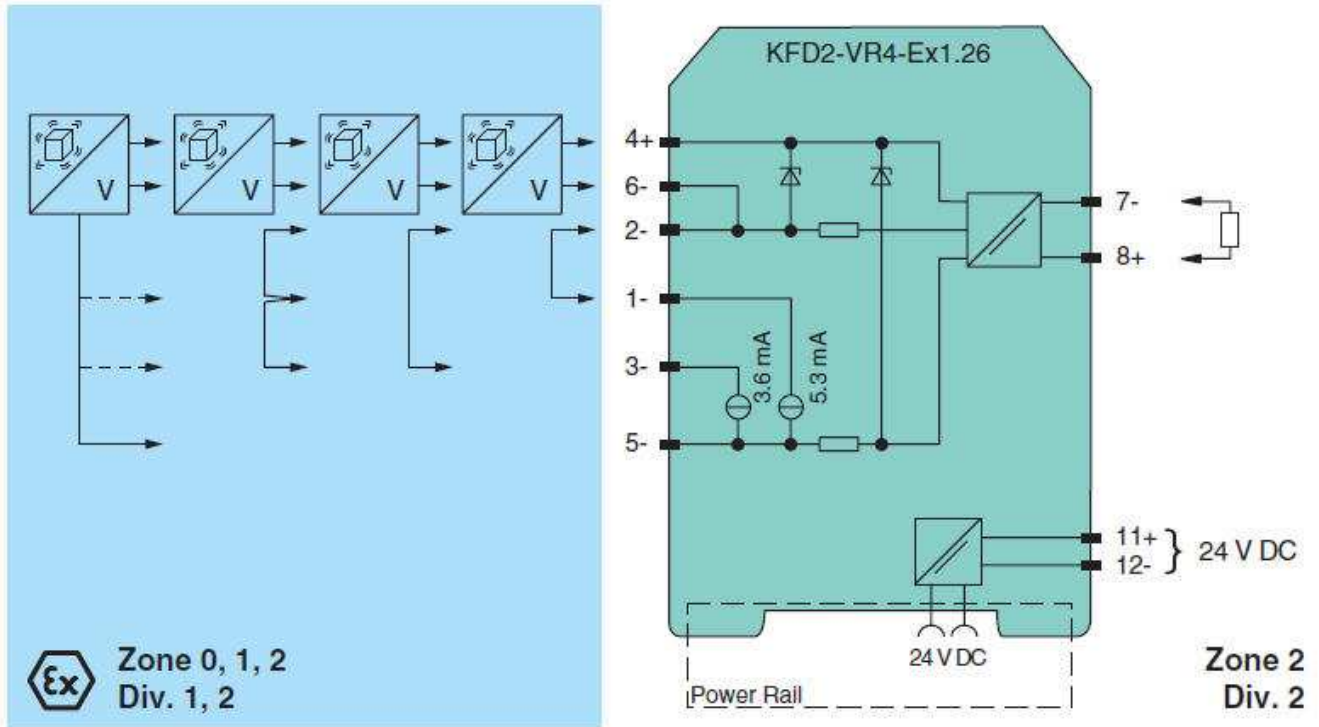
3 Functional description of the analysed module KFD2-VR4-Ex1.26

Ex1.26

This isolated barrier is used for intrinsic safety applications. It provides a floating output to power a vibration sensor (i. e. Bently Nevada) or accelerometers in a hazardous area and transfers the voltage signal from that sensor to the safe area.

Depending on connection the barrier provides 3.6 mA, 5.3 mA, or 8.9 mA supply current for 2-wire sensors, or 18 V at 20 mA for 3-wire sensors.

Connection:



Supply: Connection Power Rail or terminals 11+, 12-; Rated voltage 20 ... 35 V DC

Input: Connection terminals 4 (common), 1, 3 and 5 (supply -), 2 and 6 (signal -)
Input resistance 10 k Ω terminals 4 (common), 6-/2-

Output rated operating current:

terminals 4 (common), 5-: > 10 mA at -21 V or > 20 mA at -18 V

terminals 4 (common), 1-: > 5.3 mA \pm 0.1 mA at -10 V

terminals 4 (common), 3-: > 3.6 mA \pm 0.7 mA at -10 V

Output: Connection terminals 7-, 8+; Load \geq 2 k Ω ; Voltage 0 ... -20 V; Output res. \approx 10 Ω

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	

4 Definition of the failure categories

The FMEDA was done and is documented in EDM under the number FS-0040PF-26B. In order to judge the failure behaviour of the Voltage Repeater KFD2-VR4-Ex1.26, 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 (Voltage increase or reduction or Wrong common Signal).

Safe failure:

A failure that causes the device to go to the defined fail-safe state without a demand from the process.

Dangerous failure:

A failure that can cause the device to not respond to a demand from the process (i.e. being unable to go to the defined safe state) or deviates the output by more than 2% of the full measurement span.

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. For the 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 ($\lambda_{\text{total (Safety function)}}$).

Safety Response Time:


The time that is needed to transfer a signal step on the input of the device to its output according to the safety function.

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	

5 Assumptions for the FMEDA

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Voltage Repeater KFD2-VR4-Ex1.26.

- 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 PFDavg value of the SIF (Safety Instrumented Function) should be smaller than 10^{-2} , hence the maximum allowable PFDavg 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.
- 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 a SIL2 (sub)system.
- Failure rates based on the Siemens standard SN29500.
- Propagation of failures is not relevant.
- 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).
- 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.
- 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).
- There is no signalisation of dangerous failures available at the output of the device Therefore any fault detection by external safety devices is not assumed.


CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	

6 Safety relevant values for the modules

The following table shows how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 6 by exida.com. It is valid for the Voltage Repeater KFD2-VR4-Ex1.26 with circuit diagram 251-5067D from 16-Jan-2009 and layout 05-5189D from 05-Feb-2009.

Table 1: KFD2- VR4-Ex1.26 – Failure rates

Parameters acc. to IEC61508	Variables
Assessment Type and Documentation	FMEDA Report
Device type	A (only Hardware)
Mode of protection	Low demand mode or High demand mode
HFT	0
SIL (hardware)	2
$\lambda_{sd} + \lambda_{su}$ ¹	385 FIT
λ_{dd}	0 FIT
λ_{du}	73.5 FIT
λ_{total} (Safety function)	458.5 FIT
$\lambda_{not\ part}$	7.3 FIT
SFF	83.9%
MTBF ²	245 years
PFH	$7.4 * 10^{-8}$ 1/h
PFD _{avg} for T ₁ = 1 year	$3.22 * 10^{-4}$
PFD _{avg} for T ₁ = 3 year	$9.66 * 10^{-4}$
PFD _{avg} for T ₁ = 5 year	$1.61 * 10^{-3}$
T _{proof} _{max}	3.1. years
Safety Response Time	12.5 μ s
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.	

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	

7 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.

Table 2 shows an importance analysis of the dangerous undetected faults and indicate how these faults can be detected during proof testing.

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

Importance Analysis of “du” failures of KFD2- VR4-Ex1.26

Table 2: KFD2- VR4-Ex1.26

Component	% of total λ_{DU}	Detection through
RP1	40.84%	100% functional test with monitoring of the output
RP2	12.25%	
IC3	6.54%	
T2	5.45%	
RP3	4.08%	
P3	3.40%	
P1	3.40%	
IC2	3.27%	
C26	2.18%	
C1	2.18%	

8 Periodic Proof Testing


The Voltage Repeater KFD2-VR4-Ex1.26 can be proof tested by executing a proof test 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 Voltage Repeater KFD2-VR4-Ex1.26 has to be subjected to a proof test in intervals of at least 3 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 can have an influence on the proof test time.

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

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	

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.

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-Aug-8
 PEPPERL+FUCHS Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI	FS-0040PF-20B
	KFD2-VR4-Ex1.26	approved		
		norm		

10 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
RTD	Resistance Temperature Detection
HFT	Hardware Fault Tolerance
SIL	Safety Integrity Level
MTBF	Mean Time Between Failure
Tproof	Proof time
AVG	Average


11 Literature

Manufacturing Documents

251-5067D from 16-Jan-2009, Circuit diagram for KFD2-VR4-Ex1.26 I/O devices.
 05-5189D from 05-Feb-2009, Layout for KFD2-VR4-Ex1.26.
 Bill of material for KFD2-VR4-Ex1.26 part no. 196533 from 2011-Jul-08.

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
 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

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2011-Aug-8
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-VR4-Ex1.26	approved	FS-0040PF-20B
		norm	