

FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis

Device
SMART Current Drivers KFD2-SCD2-Ex*-Y1

Project
FS-0072EA

Pepperl+Fuchs GmbH
Mannheim
Germany



	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 PEPPERL+FUCHS Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	CERT-3668
	SMART Current Drivers	norm	

Table of Content

1	Report summary	3
2	Result of the assessment	4
3	Functional description of the analysed module KFD2-SCD2-Ex*.Y1	5
4	Safety Function and Safe State	6
5	Definition of the failure categories	6
6	Assumptions for the FMEDA	7
7	Safety relevant values for the modules	8
8	Periodic Proof Testing	9
9	Useful life time	10
10	Abbreviations	11
11	Literature	11

	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	CERT-3668
	SMART Current Drivers	norm	sheet 2 of 11


1 Report summary

This report summarizes the results of the FMEDA carried out on the SMART Current Drivers KFD2-SCD2-Ex*-Y1 with circuit diagram 251-0417D from 2002-11-14 including assembly instruction 257-5159 from 2009-07-22.

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 must be $\geq 60\%$ according to table 2 of IEC 61508-2.


	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment KFD2-SCD2-Ex*.Y1 SMART Current Drivers	respons.	DP.MKI
		approved	
		norm	
			CERT-3668 sheet 3 of 11

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) fulfills these requirements.

KFD2-SCD2-Ex*.Y1 1oo1 structure (acc. to table 1)

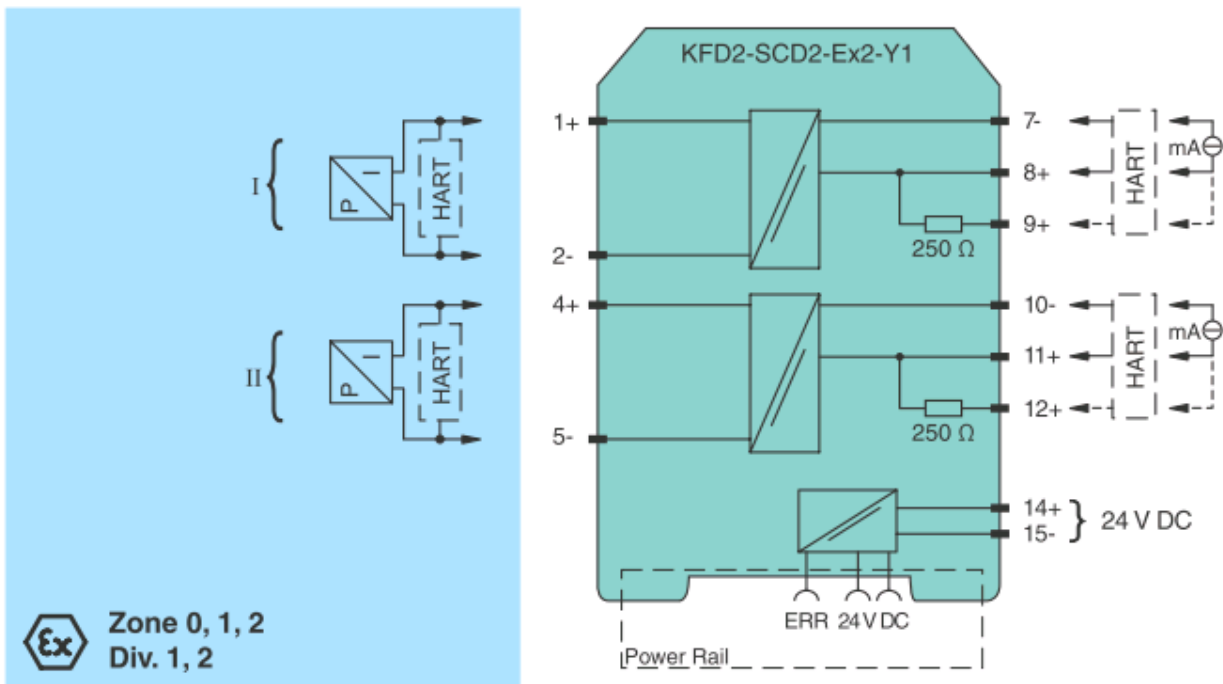
Parameters acc. to IEC61508	Values
Assessment Type and Documentation	FMEDA Report
Device type	A (only Hardware)
Mode of protection	Low demand mode or High demand mode
Safety function	An analog signal is transferred and converted with a maximum of 5% deviation of the full scale
HFT	0
SIL (hardware)	2
$\lambda_{sd} + \lambda_{su}$	388 FIT
λ_{dd}	0 FIT
λ_{du}	66.3 FIT
λ_{total} (Safety function)	454 FIT
$\lambda_{not\ part}$	149 FIT
SFF	85,3%
MTBF ¹	251 years
PFH	$6.63 * 10^{-8}$ 1/h
PFD _{avg} for T ₁ = 1 year	$2.90 * 10^{-4}$
PFD _{avg} for T ₁ = 3 years	$8.70 * 10^{-4}$
PFD _{avg} for T ₁ = 5 years	$1.45 * 10^{-3}$
Safety Response Time	20 ms
¹ acc. to SN29500. This value is valid for the safety function of the device / MTTR = 8h	

	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	CERT-3668
	SMART Current Drivers	norm	sheet 4 of 11

3 Functional description of the analysed module KFD2-SCD2-Ex*.Y1

This isolated barrier is used for intrinsic safety applications. It drives SMART I/P converters, electrical valves, and positioners in hazardous areas. The device supports a pass through for SMART communication signals that can be deactivated for periphery that does not support SMART communication by DIP switches.

Connection:



The connection to the periphery is done by standard removable terminals which are coded to prevent from misconnection when devices are removed for a proof test. The transfer function is such that a current or voltage signal is transferred from the PLC to the field via a galvanic isolation.

Supply:

- Terminals 14(+), 15(-)
- Rated voltage 20 ... 35 V DC

Input:

- Channel 1 Terminals 8(+), 7(-), optional 9(+) with additional resistance for HART communication
- Channel 2 (2 channel version only) Terminals 11(+), 10(-), optional 12(+) with additional resistance for HART communication
- Input Resistance > 100 kΩ, when wiring resistance in the field > 800 Ohms

	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI	CERT-3668
	KFD2-SCD2-Ex*.Y1	approved		
	SMART Current Drivers	norm		
				sheet 5 of 11

Output:

- Channel 1 Terminals 1(+), 2(-)
- Channel 2 (2 channel version only) Terminals 4(+), 5(-)
- Operating Voltage ≥ 14 V at 20 mA
- Operating load 0...700 Ω

4 Safety Function and Safe State

The safe state of each channel is reached when the output is below 4 mA.

5 Definition of the failure categories

The FMEDA was done and is documented in EDM under the number FS-0072EA-26
In order to judge the failure behaviour of the SMART Current Drivers KFD2-SCD2-Ex*.Y1, the following definitions for the failure of the product were considered:

Safe failure:

A failure that causes the device to go to the defined 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 5% of the full scale.

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.

Not part:

The component is not part of the safety function, but part of the circuit diagram and is listed for completeness. When calculating the SFF it's failure modes are not taken into account. They are also not part of the total failure rate of the safety function ($\lambda_{\text{total (Safety function)}}$).

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.

	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	CERT-3668
	SMART Current Drivers	norm	sheet 6 of 11

6 Assumptions for the FMEDA

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the SMART Current Drivers KFD2-SCD2-Ex*.Y1.

- Only one channel may be used in a safety function as both channels rely on the same components for their supply.
- The PLC must be set to detect if the output current leaves the allowed range of 4 .. 20 mA
- Failure rates are constant, wear out mechanisms are not included.
- Failure rates based on the Siemens standard SN29500.
- Propagation of failures is not relevant.
- 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.
- The appearance of a safe error (e. g. output in safe state) leads to a repair within 8 hours (e. g. replace defective periphery).
- 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).


	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	CERT-3668
	SMART Current Drivers	norm	sheet 7 of 11

7 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 V7.1.18, profile: SN29500 (40°C).by exida.com. It is valid for the for KFD2-SCD2-Ex*.Y1 SMART Current Drivers with circuit diagram 251-0417D from 2002-11-14 including assembly instruction 257-5159 from 2009-07-22. The difference to the original version KFD2-SCD2-Ex* of the devices is that a diagnostic function that switches the input to a high impedance state in case of short circuit on the output side is not available on this circuit. Failures in this diagnostic circuit were prevalently safe errors in the original version. Analysis showed that the effect of removing this part of the diagnosis does not have significant effects on the safety function. For ease of use and supported by repair statistics the values of the original device are still considered valid.

Table 1: KFD2-SCD2-Ex*.Y1 1oo1 structure

Parameters acc. to IEC61508	Values
Assessment Type and Documentation	FMEDA Report
Device type	A (only Hardware)
Mode of protection	Low demand mode or High demand mode
Safety function	An analog signal is transferred and converted with a maximum of 5% deviation of the full scale
HFT	0
SIL (hardware)	2
$\lambda_{sd} + \lambda_{su}$	388 FIT
λ_{dd}	0 FIT
λ_{du}	66.3 FIT
λ_{total} (Safety function)	454 FIT
$\lambda_{not\ part}$	149 FIT
SFF	85,3%
MTBF ¹	251 years
PFH	$6.63 * 10^{-8}$ 1/h
PFD _{avg} for T ₁ = 1 year	$2.90 * 10^{-4}$
PFD _{avg} for T ₁ = 3 years	$8.70 * 10^{-4}$
PFD _{avg} for T ₁ = 5 years	$1.45 * 10^{-3}$
Safety Response Time	20 ms
¹ acc. to SN29500. This value is valid for the safety function of the device / MTTR = 8h	

	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	
	SMART Current Drivers	norm	
			CERT-3668
			sheet 8 of 11

8 Periodic Proof Testing

The SMART Current Drivers KFD2-SCD2-Ex*.Y1 can be proof tested by checking the transfer characteristics at minimum input / maximum input / one value in between.


For proof tests at the inputs from a hazardous area, be sure to use adequate equipment.

The proof test recognizes dangerous concealed faults that would affect the safety function of the plant.

According to the results of the analysis, the SMART Current Drivers KFD2-SCD2-Ex*.Y1 have to be subjected to a proof test in intervals of 3 years 5 months maximum (if the safety function is SIL 2 and the failure budget is 10% maximum of the allowed PFD value).

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. Both of these influence the necessary proof test time.

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

	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	CERT-3668
	SMART Current Drivers	norm	sheet 9 of 11

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, 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.

The Current Drivers KFD2-SCD2-Ex*.Y1 do not use components with reduced life time in the safety path.

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

	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2014-Jul-24
 PEPPERL+FUCHS Mannheim	FMEDA – Hardware Assessment	respons.	DP.MKI
	KFD2-SCD2-Ex*.Y1	approved	
	SMART Current Drivers	norm	
			CERT-3668 sheet 10 of 11

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
HFT	Hardware Fault Tolerance
SIL	Safety Integrity Level
MTBF	Mean Time Between Failure
Tproof	Proof time
AVG	Average

11 Literature

Manufacturing Documents

Circuit Diagram 251-0417D from 2002-11-14 for KFD2-SCD2-Ex*.Y1 SMART Current Drivers

Assembly instruction 257-5159 from 2009-07-22 for KFD2-SCD2-Ex*.Y1 SMART Current Drivers

FMEDA excel sheets FS-0072EA-26 generated with FMEDA tool by exida.com

FMEDA and prior-use-assessment P+F 03-10-12 R014 V1 R1.0 dated March 2004

Standards


IEC 61508-1:2001 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – General Part

IEC 61508-2:2001 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

	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2014-Jul-24
 Mannheim	FMEDA – Hardware Assessment KFD2-SCD2-Ex*.Y1 SMART Current Drivers	respons.	DP.MKI	CERT-3668
		approved		
		norm		sheet 11 of 11