




FMEDA – Report

Failure Modes, Effects and Diagnostic Analysis

Device Model Number:
EU/AH420


Project:
E-Card
for
Transmitter Power Supply

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: 2010-Oct-12
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.HSU	FS-0012PF-20A
	EU/AH420	approved		
			norm	

template: FTM-0027_1

1. Management Summary.....	4
2. Description of the Analysed Module EU/AH420.....	5
3. Failure Modes, Effect and Diagnostic Analysis	6
3.1 Description of the Failure Categories.....	6
3.2 Assumptions	7
3.3 FMEDA results for the EU/AH420 According to 1oo1d structure.....	8
4. Periodic Proof Testing.....	9
5. 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: 2010-Oct-12
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons. DP.HSU	FS-0012PF-20A
	EU/AH420	approved	
			norm


template: FTM-0027_1

Reviewers:

Role
Development Team Leader (PA-PG-IF)
Functional Safety Manager

Input Documents

EDM	Document name	Remarks
01-7901 / 01-7898	Schematic	
FS-0012PF-26	Electronic FMEDA	

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2010-Oct-12
 Mannheim	FMEDA – Report	respons. DP.HSU	FS-0012PF-20A
	EU/AH420	approved	
		norm	sheet 3 of 10

template: FTM-0027_1

1. Management Summary

This report summarizes the results of the FMEDA carried out on the Transmitter power supply EU/AH420

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. 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 15% of this range, i.e. they should be lower than $1.5 * 10^{-3}$ for SIL2 in Low demand mode respectively lower than $1.5 * 10^{-7} h^{-1}$ for SIL2 in High demand mode.

The Transmitter power supply EU/AH420 is considered to be a Type A component with a hardware fault tolerance of "0"

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

Acc. table 1: EU/AH420, E-Card 1oo1d structure

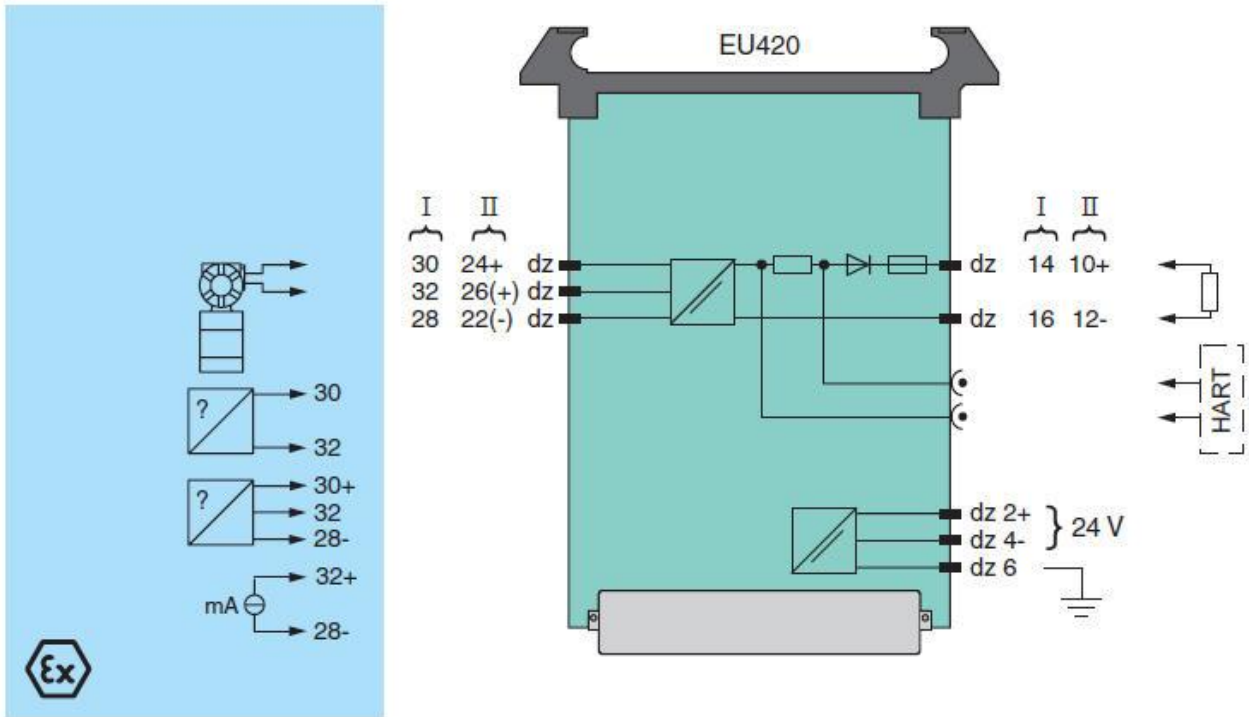
Parameters acc. to IEC61508	Variables
Device type	A
Demand mode	Low demand mode or High demand mode
Safety Function ¹	Current output
HFT	0
SIL	2
$I_{sd} + I_{su}$	289.5 FIT
I_{dd}	173 FIT
I_{du}	115FIT
I_{total} (Safety function)	578 FIT
SFF	80%
MTBF ²	197 years
PFH ³	$1.15 * 10^{-7} 1/h$
PFD _{avg} for $T_1 = 1 \text{ year}$ ³	$5.05 * 10^{-4}$
T _{proof} _{max}	2.5 years
¹ The device can be used as 2-wire analog input, current output device (4...20mA). ² acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h ³ For PFD _{avg} and PFH 15% of the range is allowed (PFD $<1.5 * 10^{-3}$ and PFH $<1.5 * 10^{-7} 1/h$)	

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2010-Oct-12
 Mannheim	FMEDA – Report	respons.	DP.HSU
	EU/AH420	approved	
		norm	sheet 4 of 10

2. Description of the Analysed Module EU/AH420

The device supplies 2-wire transmitter in the hazardous area.

Connection:



Power supply: 24V DC terminals dz2 (+), dz4 (-), dz6 (PE)
 20 ... 30 V DC (<4.5 W / 2 channels)
 20 ... 26.4 V AC (< 3 VA/channel)

Input I: terminals dz30+, dz32- (+), dz28 (-)

Input II: terminals dz24+, dz26- (+), dz22 (-)

Output I: terminals dz14+, dz16-

Output II: terminals dz10+, dz12-

Input resistance: 150 Ω , dynamic 250 Ω (HART)

Load: $\leq 750 \Omega$, for HART/FSK < 500 Ω

Current output: 4...20mA

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2010-Oct-12
 Mannheim	FMEDA – Report	respons. DP.HSU	FS-0012PF-20A
	EU/AH420	approved	
			norm


3. Failure Modes, Effect and Diagnostic Analysis

The FMEDA was done and is documented in EDM under the number [FS-0012PF-26]

3.1 Description of the Failure Categories

In order to judge the failure behaviour of the transmitter power supply EU/AH420, 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 or the output signal to go to the minimum output current (< 4mA) or the output signal to go to the maximum output current (> 20mA)
- Safe state: A safe failure is defined as a failure that causes the module / (sub) system to go to the defined fail-safe state without a demand from the process.
- Dangerous: A dangerous failure is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined safe state) or deviates the output current by more than 5% full scale (+/- 0.8mA).
- 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: 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 (I_{total} (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: 2010-Oct-12
 Mannheim	FMEDA – Report	respons.	DP.HSU	FS-0012PF-20A
	EU/AH420	approved		
			norm	

3.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the transmitter power supply EU/AH420.

- Failure rates are constant, wear out mechanisms are not included.
- Failure rates based on the Siemens standard SN29500.
- Propagation of failures is not relevant.
- All components failure modes are known.
- The repair time after a safe failure is 8 hours.
- The average temperature over a long period of time is 40°C.
- The stress levels are average for an industrial environment.
- All modules are operated in the Low demand mode or High demand mode of operation.
- The subsystem shall be considered of type “A” (non complex component as described in 7.4.3.2.1.of IEC 61508).
- The transmitter power supply has a hardware fault tolerance of “0”
- 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).
- Both channels on a module may not be used to carry out the same safety function.
- The application program in the safety logic solver is configured to detect under-range and over-range failures, therefore these failures have been classified as dangerous detected failures.

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2010-Oct-12
 Mannheim	FMEDA – Report	respons.	DP.HSU	FS-0012PF-20A
	EU/AH420	approved		
			norm	

3.3 FMEDA results for the EU/AH420 According to 1oo1d structure

Table 1: EU/AH420 According to 1oo1d structure

Parameters acc. to IEC61508	Variables
Device type	A
Demand mode	Low demand mode or High demand mode
Safety Function ¹	Current output
HFT	0
SIL	2
$I_{sd} + I_{su}$	289.5 FIT
I_{dd}	173 FIT
I_{du}	115FIT
I_{total} (Safety function)	578 FIT
SFF	80%
MTBF ²	197 years
PFH ³	$1.15 \cdot 10^{-7}$ 1/h
PFD _{avg} for $T_1 = 1$ year ³	$5.05 \cdot 10^{-4}$
T _{proof_max}	2.5 years

¹ The device can be used as 2-wire analog input, current output device (4...20mA).
² acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h
³ For PFD_{avg} and PFH 15% of the range is allowed (PFD < $1.5 \cdot 10^{-3}$ and PFH < $1.5 \cdot 10^{-7}$ 1/h)

$$SFF = 1 - \frac{I_{du}}{I_{total}} = 1 - \frac{1.15 \cdot 10^{-7}}{5.78 \cdot 10^{-7}} \approx 80 \%$$

T1 = 1 year (8760h)
 MTTR = 8h


$$PFD_{avg}(T1) = \lambda_{du} \cdot \frac{T1}{2} + \lambda_{dd} \cdot MTTR = 1.15 \cdot 10^{-7} \cdot \frac{8760}{2} + 1.73 \cdot 10^{-7} \cdot 8$$

$$PFD_{avg}(T1=8760h) = 5.05 \cdot 10^{-4}$$

$$PFH = \frac{PFD_{avg}(T1)}{T1} \cdot 2$$

$$PFH = 1.15 \cdot 10^{-7} \text{ 1/h}$$

T_{proof_max}(SIL2) ≈ 2.5 years

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!	scale: 1:1	date: 2010-Oct-12
 Mannheim	FMEDA – Report	respons.	DP.HSU
	EU/AH420	approved	
		norm	
		FS-0012PF-20A	
		sheet 8 of 10	


4. Periodic Proof Testing

The transmitter power supply EU/AH420 can be checked at regular intervals. It is recommended that proof tests are carried out once in 2.5 years.

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

In practice the input and output field devices have a more frequent proof test interval (every 6 or 12 months) than the EU/AH420 module. If the end-user tests the complete safety loop because of the field devices, then the EU/AH420 is automatically included in these tests (rudimentary test). No additional periodic tests are required for the EU/AH420, if the proof test considered all safety related functions of the device.

If the proof test of the field devices does not include the EU/AH420, then the device needs to be tested as a minimum once in 2.5 years. This can be done by executing a proof test procedure according to safety application of the EU/AH420.

CONFIDENTIAL acc. to ISO 16016	Only valid as long as released in EDM or with a valid production documentation!		scale: 1:1	date: 2010-Oct-12
 Mannheim	FMEDA – Report	respons.	DP.HSU	FS-0012PF-20A
	EU/AH420	approved		
			norm	

template: FTM-0027_1

5. 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: 2010-Oct-12
 PEPPERL+FUCHS Mannheim	FMEDA – Report	respons.	DP.HSU	FS-0012PF-20A
	EU/AH420	approved		
			norm	

template: FTM-0027_1