PEPPERL+FUCHS

FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis

Device Model Number:

KFD2-PT2-Ex1-*
Potentiometer Converter

Pepperl+Fuchs GmbH
Mannheim
Germany

Reviewers:

Role
Development Engineer (PA-PG-IF)
Functional Safety Manager

Input Documents

EDM	Document name	Remarks
251-0423A	Schematic	
FS-0058PF-26	Electronic FMEDA	

1. Management Summary

This report summarizes the results of the FMEDA carried out on the Potentiometer converter KFD2-PT2-Ex1-*

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

The Potentiometer converter KFD2-PT2-Ex1-* 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: KFD2-PT2-Ex1-* Potentiometer converter 1oo1 structure

Parameters acc. to IEC61508	**Variables**
Device type	A
Demand mode	Low demand mode or High demand mode
Safety Function	Potentiometer converter
HFT	0
SIL	2
l_{s}	0 FIT
l_{dd}	0 FIT
l_{du}	86.1 FIT
$l_{\text{fail high}}$[1]	6.35 FIT
$l_{\text{fail low}}$[1]	86.5 FIT
$l_{\text{no effect}}$	218 FIT
$l_{\text{total (Safety function)}}$	397 FIT
SFF	78.31%
MTBF[2]	265 years
PFH	$8.62*10^{-8}$ 1/h
PFD_{avg} for T_1 = 1 year	$3.77*10^{-4}$
$\text{Tproof}_{\text{max}}$	2.5 years

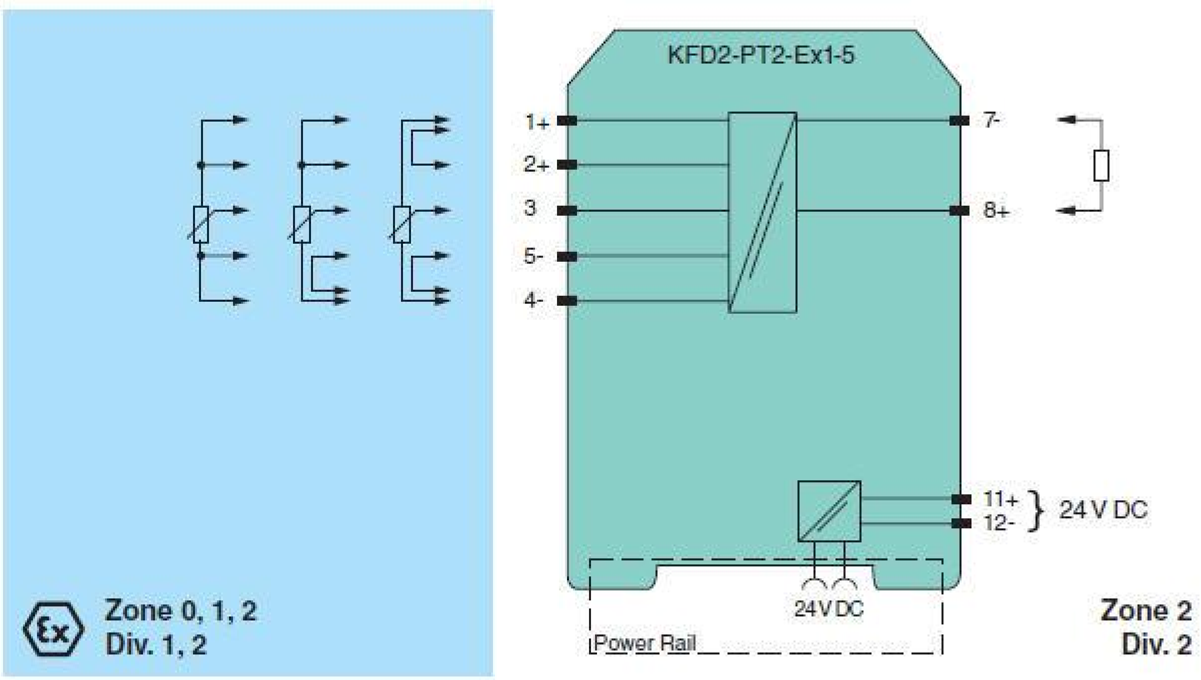
[1] “Fail high” and “fail low” failures are considered as dangerous detected failures.

[2] acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h

2. Description of the Analysed Module KFD2-PT2-Ex1-*

This isolated barrier is used for intrinsic safety applications. It provides the source voltage to a potentiometer and transfers its wiper position from hazardous areas to safe areas. It then converts the signal to a 4 mA ... 20 mA current output.
The unit can be used in a 3-, 4-, or 5-wire configuration depending on the required measurement accuracy.
Terminals 2 and 5 are used as the sense line for the potentiometer lead resistance compensation in a 5-wire configuration.
The barrier’s potentiometer can be used to compensate for lead resistance up to 5 % of the hazardous area potentiometer value.

Connection:



Power supply: terminals: 24V DC (Power rail) or 11(+), 12(-)

Input: terminals 4(-), 5(-); 3(+), 2(+), 1(+)
Types of measurement: 3-,4-,5-wire technology

Output: terminals 7(+), 8(-)
Current output: 4…20mA, Load ≤1kΩ

3. Failure Modes, Effect and Diagnostic Analysis

The FMEDA was done and is documented in EDM under the number [FS-0058PF-26]

3.1 Description of the Failure Categories

In order to judge the failure bahaviour of the potentiometer comverter KFD2-PT2-Ex1-*, the following definitions for the failure of the product were considered:

Fail safe state: The fail-safe state is defined as the output reaching the user defined threshold value.

Safe state: A safe failure (S) is defined as a 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 (or part thereof) 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 (or part thereof) into a safe state or maintain a safe state.

Dangerous: causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or,
b) decreases the probability that the safety function operates correctly when required.

Fail high: A fail high failure (H) is defined as a failure that causes the output signal to go to the maximum output current (> 21mA) or output voltage (> 5V or > 10V).

Fail low: A fail low failure (L) is defined as a failure that causes the output signal to go to the minimum output current (< 3.6mA) or output voltage (< 1V or < 2V).

No Effect: Failure mode of a component that plays a part in implementing the safety function but has no direct effect on the safety function and deviates the output by not more than 2% of full span.

Not part: Component that plays no part in implementing the safety function but is 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. ($l_{\text{total (Safety function)}}$).

3.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Potentiometer converter KFD2-PT2-Ex1-*.

- 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 voltage repeater 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).
- 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.

3.3 FMEDA results for the KFD2-PT2-Ex1-*

Table 1: KFD2-PT2-Ex1-* potentiometer converter 1oo1 structure

Parameters acc. to IEC61508	**Variables**
Device type	A
Demand mode	Low demand mode or High demand mode
Safety Function	Potentiometer converter
HFT	0
SIL	2
l_{s}	0 FIT
l_{dd}	0 FIT
l_{du}	86.1 FIT
$l_{\text{fail high}}$[1]	6.35 FIT
$l_{\text{fail low}}$[1]	86.5 FIT
$l_{\text{no effect}}$	218 FIT
$l_{\text{total (Safety function)}}$	397 FIT
SFF	78.31%
MTBF[2]	265 years
PFH	$8.62*10^{-8}$ 1/h
PFD_{avg} for T_1 = 1 year	$3.77*10^{-4}$
$\text{Tproof}_{\text{max}}$	2.5 years
[1] "Fail high" and "fail low" failures are considered as dangerous detected failures. [2] acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h	

$$\boxed{\textbf{SFF} = 1 - \frac{l\,du}{l\,total} = 1 - \frac{0.861*10^{-7}}{3.97*10^{-7}} \approx \textbf{78.31 \%}}$$

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

$$\text{PFDavg(T1)} = \lambda_{\text{du}} * \frac{T1}{2} + \text{MTTR} * (\lambda_{\text{dd}} + \lambda_{\text{fail high}} + \lambda_{\text{fail low}})$$

$$= 0.861*10^{-7} * \frac{8760}{2} + 8 *(0*10^{-9} + 6.35*10^{-9} + 0.865*10^{-7})$$

$$\boxed{\textbf{PFDavg(T1=8760h) = 3.77 *10}^{\mathbf{-4}}}$$

$$\text{PFH} = \frac{PFDavg(T1)}{T1} *2$$

$$\boxed{\textbf{PFH = 8.62 * 10}^{\mathbf{-8}}\textbf{ 1/h}}$$

$\text{Tproof}_{\text{max}}$(SIL2) $\approx$ 2.5 years

$$\boxed{\textbf{MTBF} = \frac{1}{l\,total} = \frac{1}{4.31*10^{-7}} \textbf{=2.32*10}^{\mathbf{6}} \textbf{ à 265years}}$$

4. Periodic Proof Testing

The voltage repeater KFD2-PT2-Ex1-* can be checked at regular intervals.
It is recommended that proof tests are carrier 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 KFD2-PT2-Ex1-* module, If the end-user tests the complete safety loop because of the field devices, then the KFD2-PT2-Ex1-* is automatically included in these tests (rudimentary test). No additional periodic tests are required for the KFD2-PT2-Ex1-*, if the proof test considered all safety related functions of the device.

If the proof test of the field devices does not include the KFD2-PT2-Ex1-*, 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 KFD2-PT2-Ex1-*.

.

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.