FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis

Device Model Number:
KCD2-RR-Ex1(.SP)
and
HiC2077

Project:
Resistance Repeater

Pepperl+Fuchs GmbH
Mannheim
Germany

Table of content:

Reviewers:

Role
Project Leader (PL)
Product Management
Functional Safety Manager

History of this document:

Revision of this document	Reviewed by / [Reviewer abbreviation within the detailed comment list]	Changes since last version
Index 0	Kindermann DP.MKI	Newly created
Index A	Kindermann DP.MKI	Adapted to new format, see FS-0040PF-20B. Added .SP version

1. Report Summary

This report summarizes the results of the FMEDA carried out on the Resistance Repeater KCD2-RR-Ex1 and HiC2077 with circuit diagram 251-5066C from 17/12/08.

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 for type A devices 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.

Since the Resistance Repeaters KCD2-RR-Ex1 and HiC2077 are considered to be Type A devices with a hardware fault tolerance of "0", the SFF shall be ≥ 60% according to table 2 of IEC 61508-2.

2. Result of the assessment

The following table shows under which conditions the described modules fulfill these requirements.

Acc. table 1: KCD2-RR-Ex1(.SP) and HiC2077 1oo1 structure

Parameters acc. to IEC61508	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function[1]	Resistance Repeater
HFT	0
SIL	2
$\lambda_{sd} + \lambda_{su}$	77.0 FIT
λ_{dd}	39.9 FIT
λ_{du}	96.7 FIT
$\lambda_{total\ (Safety\ function)}$	625 FIT
SFF	83.3 %
MTBF[2]	182.6 years
PFH	$9.67*10^{-8}$ 1/h
PFD_{avg} for T_{proof} = 1 year	$4.24*10^{-4}$
PFD_{avg} for T_{proof} = 2 years	$8.48*10^{-4}$
PFD_{avg} for T_{proof} = 5 years	$2.12*10^{-3}$
Reaction time	See data sheet

[1] The device can be used as resistance repeater in a safety loop
[2] acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h

3. Functional description of the Analysed Module KCD2-RR-Ex1

The device is a resistance repeater module with a RTD / 2-, 3-, or 4-wire resistance input.

This isolated barrier is used for intrinsic safety applications. It transfers RTD resistance values from hazardous areas to safe areas.

A 2-, 3-, or 4-wire mode is available depending on the required accuracy.
The monitor registers the same load as if it were connected directly to the resistance in a hazardous area.

The KCD2-RR-Ex1 are available with screw terminals or spring terminals. The type code of the versions with spring terminals has the extension ".SP".

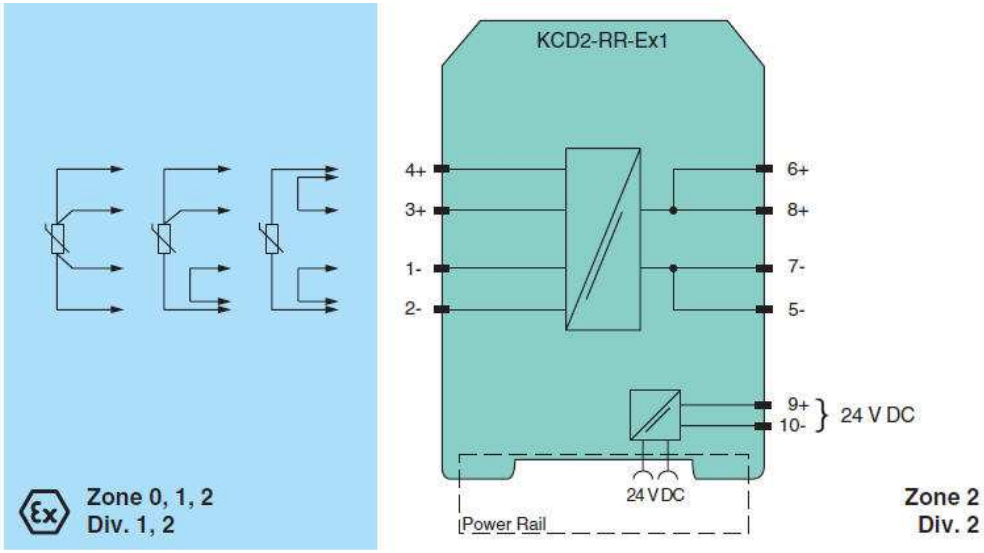

Fig. 1: Connection of the KCD2-RR-Ex1(.SP)

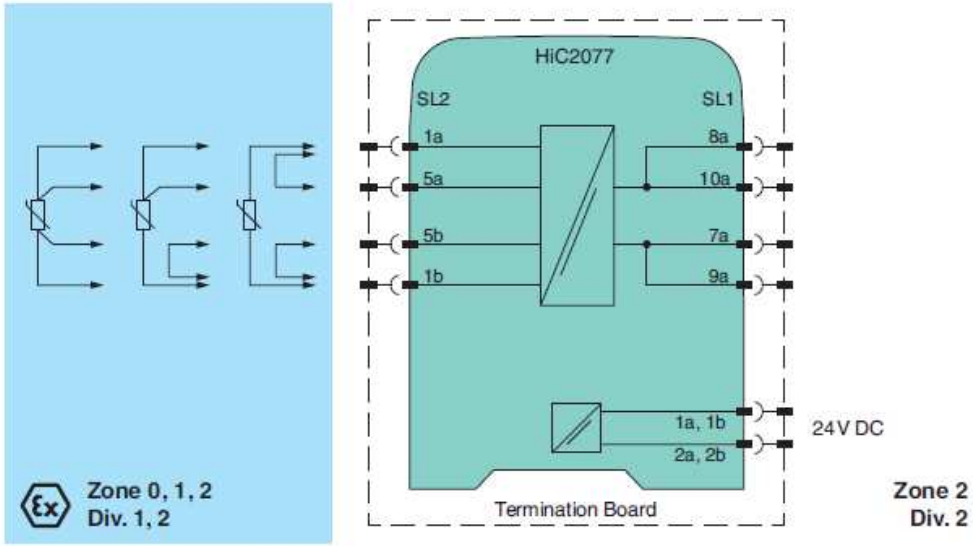

Fig. 2: Connection of the HiC2077

Input (left side): transmission range 0 …10mA
Available voltage 9V

Output (right side): current 0 … 10mA
Available voltage: 0 … 7V

4. Definition of the failure categories

The FMEDA was done and is documented in EDM under the number FS-0062PF-26.

In order to judge the failure behaviour of the resistance repeater KCD2-RR-Ex1 and HiC2077, the following definitions for the failure of the product were considered:

Fail-safe state:
Defined as the output being de-energized (> 100 kΩ is indicated) or when no supply is on the device.

Safe failure:
A failure that causes the module / (sub)system to go to the defined fail-safe state without a demand from the process.

Dangerous failure:
When the device does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 2% full span.

Fail high failure:
A resistance >400 Ω is signaled, but the device does not go to the fail-safe state. They are treated as dangerous undetected. This is due to the fact that with Pt500 and Pt1000 in the application this failure can not be evaluated.

Fail low failure:
A failure that causes the output signal to go to an output resistance < 10 Ω. For the SFF calculations these failures are counted as dangerous detected.

No Effect failure:
Failure of a component that is part of the safety function but has no effect on the safety function, or deviates the output current by not more than 2% full span. For the calculation of the SFF it is treated like a safe undetected failure.

Annunciation failure:
This failure does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). For calculation of the SFF, 5% are counted as dangerous undetected, the rest is counted as safe undetected.

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 an input signal of a device to its output according to the safety function.

5. Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the KCD2-RR-Ex1 and HiC2077.

- 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 PFD_{avg} value of the SIF (Safety Instrumented Function) should be smaller than 10^{-2}, hence the maximum allowable PFD_{avg} 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 SIL2 (sub)system.
- Failure rates based on the Siemens standard SN29500.
- 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).
- 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 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 ºC. Humidity levels are assumed within manufacturer's rating. For a higher average temperature of 60 ºC, 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 modules are operated in the Low demand mode or High demand mode of operation.
- The application program in the safety logic solver is constructed in such a way that fail low failures are detected regardless of the effect, safe or dangerous on the safety function.

6. Results of the assessment

The following table shows how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 6 by exida.com.

Table 1: KCD2-RR-Ex1 and HiC2077 1oo1 structure

Parameters acc. to IEC61508	**Variables**
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function[1]	Resistance Repeater
HFT	0
SIL	2
$\lambda_{sd+}\lambda_{su}$	77.0 FIT
λ_{dd}	39.9 FIT
λ_{du}	96.7 FIT
$\lambda_{total\ (Safety\ function)}$	625 FIT
SFF	83.3 %
MTBF[2]	182.6 years
PFH	$9.67*10^{-8}$ 1/h
PFD_{avg} for T_1 = 1 year	$4.24*10^{-4}$
PFD_{avg} for T_{proof} = 2 years	$8.48*10^{-4}$
PFD_{avg} for T_{proof} = 5 years	$2.12*10^{-3}$
Reaction time	See data sheet

[1] The device can be used as resistance repeater in a safety loop
[2] acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h

$$\mathbf{PFD_{avg}\ (T_{proof\ =\ 1\ year})} = \lambda_{du} * \frac{T1}{2} + \lambda_{dd} * T_{Rep} = 9.67 * 10^{-8}\,1/h * \frac{8760h}{2} + 39.9 * 10^{-9}\,1/h * 8\,h$$
$$= 4.24 * 10^{-4}$$

PFH = $9.67 * 10^{-8}$ 1/h

$$\mathbf{SFF} = 1 - \frac{\lambda_{du}}{\lambda_{total\_safety}} = 1 - \frac{96.7*10^{-7}}{578*10^{-7}} \approx \mathbf{83.3\ \%}$$

MTBF = MTTF + MTTR = [(1 / λ_{total}) + 8 h]
= 1/ ($6.25 * 10^{-7}$ h * 8760 h) = **182.6 years**

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

Table 2: Importance Analysis of "du" failures of KCD2-RR-Ex1

Component	% of total λ_{DU}	Detection through
P5, P7, P9, P10, P11, P13	21.34%	100% functional test
P6, P8, P12,P14	14.23%	
T2, T3	14.23%	
C66, C69, C70	4.27%	
C58, C59, C60, C61, C74, C75	4.27%	
IC1	3.56%	
C12, C15, C18, C41, C42	3.56%	
P2, P3	2.85%	
C62, C63, C64, C65	2.85%	
R70, R71, R13, R57, R24, R33, R28	1.99%	

8. Periodic Proof Testing

The resistance repeater module can be proof tested by executing a proof test procedure according to the Safety Manual.

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

According to the results of the analysis, the KCD2-RR-Ex1 has to be subjected to a proof test in intervals of at least 2 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.

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.

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
T_{proof}	Proof time
AVG	Average

11. Literature

Manufacturing Documents

251-5066C from 17-Dec-2008, Circuit diagram for KCD2-RR-Ex1 I/O devices.
255-5050F from 11-Jun-2009, Layout for KCD2-RR-Ex1.
Bill of material for KCD2-RR-Ex1 part no. 190247 dated 30-Jun-2011.
DDE-0738A from 07-Dec-2005, Requirement Profile KCD2-RR-Ex1.
FS-0062PF-026 V2R5 from 13-Jul-2011, electronic FMEDA / Fault Insertion Tests

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