FMEDA – Report
Failure Modes, Effects and Diagnostic Analysis and ‘Proven-in-use’-assessment

Device Model Number:
KF-CRG2-**1.D**

Transmitter supply isolator

Pepperl+Fuchs GmbH
Mannheim
Germany

Reviewers:

Role
Project Leader (PL)
Product Management
Functional Safety Manager

History of this document:

Revision of this document	**Changes since last version**
Index 0 From 2008-Apr-08	Newly created
Index A From 2016-Oct-19	Adapted format. Updated to EN/IEC 61508:2010. Included results from re-assessment
Index B From 2017-Jan-11	Updated chapter ‘Useful Lifetime’

1. Report Summary

This report summarizes the results of the hardware assessment with proven in use and field experience aspects consideration according to EN/IEC 61508 and EN/IEC 61511.

For field experience, EN/IEC 61508 lists techniques and measures to exclude systematic failures and evaluates their effectiveness (EN/IEC 61508-2 Table B.6). Field experience can be used as a measure to avoid systematic failures. A claim to use field experience for such an evaluation is made within this document.
Failure rates used in this analysis are basic failure rates from the Siemens Standard SN29500.

According to table 2 of EN/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 Mode of operation, the PFH value has to be < 10^{-6} h^{-1} for SIL2. However, as the devices under consideration are only part of an entire safety function they should not claim more than 10% of this range, i.e. they should claim an average PFD of less than 10^{-3} for SIL2 in Low Demand Mode respectively a PFH of less than 10^{-7} h^{-1} for SIL2 in High Demand Mode.

The Transmitter Supply Isolators KF**-CRG2-**1.D are considered to be Type B components with a hardware fault tolerance of “0”. Type B components with a SFF of 60% to < 90% must have a hardware fault tolerance of 1 according to table 3 of EN/IEC 61508-2 for SIL 2 (sub-) systems. According to the requirements of EN/IEC 61511-1 section 11.4.4 (proven in use), a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of 60% to < 90%.

2. Result of the Assessment

The following table shows the safety characteristic values for the Transmitter Supply Isolators KF**-CRG2-**1.D as calculated within the FMEDA (under the assumptions described in subsequent chapters):

Table 1: Transmitter Supply Isolators KF-CRG2-**1.D, usage in 1oo1D structure**

Failure Category	KFD2 Relay Output	KFU8 Relay Output	KFD2 Analog Output	KFU8 Analog Output
Device type	B			
Mode of operation	Low Demand or High Demand			
SIL	2			
HFT	0			
Safety Function	Relay Output		Analog Output	
λ_s [1]	165 FIT	213 FIT	137 FIT	177 FIT
λ_{dd} [1]	70 FIT	79 FIT	74 FIT	83 FIT
λ_{du} [1]	114 FIT	108 FIT	90 FIT	81 FIT
$\lambda_{no\ effect}$ [1]	164 FIT	194 FIT	151 FIT	178 FIT
$\lambda_{not\ part}$ [1]	35.8 FIT	34.4 FIT	35.0 FIT	34.8 FIT
$\lambda_{total\ (Safety\ function)}$	348 FIT	399 FIT	300 FIT	341 FIT
$\lambda_{total\ (Signal\ path)}$	548 FIT	628 FIT	486 FIT	554 FIT
SFF [2]	67 %	72 %	70 %	76 %
PTC	99 %	99 %	99 %	99 %
MTBF [3]	207 years	181 years	234 years	206 years
PFH [1]	1.13×10^{-7} 1/h [4]	1.08×10^{-7} 1/h [4]	9.0×10^{-8} 1/h	8.1×10^{-8} 1/h
PFD_{avg} (T_1 = 1 year)	4.96×10^{-4} 1/h	4.75×10^{-4} 1/h	3.94×10^{-4} 1/h	3.56×10^{-4} 1/h
PFD_{avg} (T_1 = 2 years)	9.92×10^{-4} 1/h	9.50×10^{-4} 1/h	7.88×10^{-4} 1/h	7.12×10^{-4} 1/h
PFD_{avg} (T_1 = 5 years)	2.48×10^{-3} 1/h [4]	2.37×10^{-3} 1/h [4]	1.97×10^{-3} 1/h [3]	1.78×10^{-3} 1/h [3]

NOTE 1: Failure rates were adapted to most recent data base values. Edition 1 evaluation still valid for existing installations.
NOTE 2: For calculation of values according to EN/IEC 61508:2010, the 'no effect' values are excluded from SFF calculation.
NOTE 3: acc. To SN29500. This value is only valid for the signal path and includes failures which are not part of the safety function.
NOTE 4: For using this proof test interval for a safety application, usage of more than 10% of the failure budget for the safety loop is necessary.

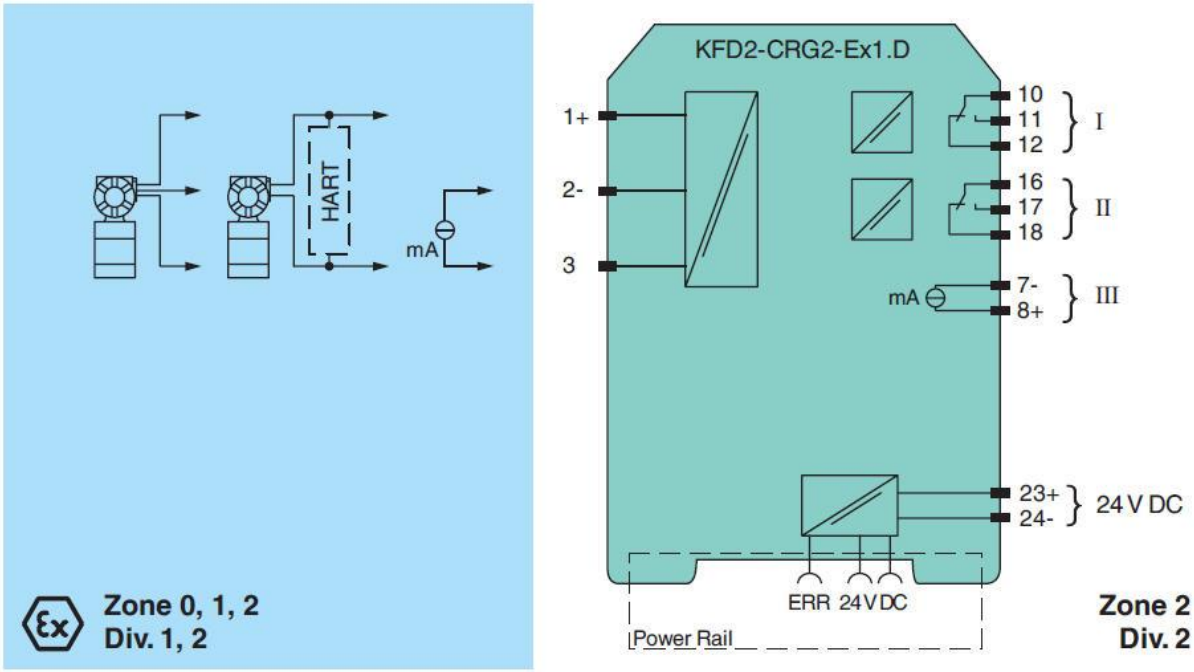
The safety characteristic values given within this table are valid for a permissible fault reaction time of 1 second.

3. Functional Description of the analysed Devices

3.1 KFD2-CRG2-**1.D

The device is a 1 channel isolated barrier with an active 4mA…20mA current source output and two relay contact outputs: The device supplies 2-wire and 3-wire transmitters in a hazardous area, and can also be used with active current sources.

Connection:



Supply: (Power rail or terminals 23+, 24-) rated voltage 20…30V DC

Input: (Terminals 1, 2 and 3) the input signal is 4…20mA

Output I: (terminals 10, 11 and 12) relay output
contact loading 250V AC / 2 A / cos Φ ≥ 0.7; 40 DC / 2A

Output II: (terminals 16, 17 and 18) relay output
contact loading 250V AC / 2 A / cos Φ ≥ 0.7; 40 DC / 2A

Output III: (terminals 7 and 8)
Current range 4…20mA

3.2 KFU8-CRG2-**1.D

In the KFU8 devices, a different power supply is used: (Terminals 23+, 24-) rated voltage 20…90 V DC or 48 .. 253 V AC. No connection to power rail is given.

4. Definition of the failure Categories

In order to judge the failure behaviour of the device KF**-CRG2-**1.D the following definitions for the failure of the product were considered:

Relay Output:

Safe state:	The safe state is defined as the outputs being de-energized (output relay contact is not conducting).
Safe failure:	Causes the device / (sub)system to go to the defined safe state without a demand from the process.
Dangerous failure:	Causes the device to not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state). The output remains energized.
No effect:	Failure of a component that is part of the safety function but has no effect on the safety function. These failures are excluded from the SFF calculation.
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. It is not part of the total failure rate ($\lambda_{total\ (Safety\ function)}$) used for calculating the safe failure fraction SFF of the safety function, but is used for calculating the MTBF of the device.

Current Output:

Safe state:	The safe state is defined as the output going to "fail low" or "fail high" state.
Safe failure:	Causes the device / (sub)system to go to the defined safe state without a demand from the process.
Dangerous failure:	Causes the device to 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 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. These failures are excluded from the SFF calculation.
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. It is not part of the total failure rate ($\lambda_{total\ (Safety\ function)}$) used for calculating the safe failure fraction SFF of the safety function, but is used for calculating the MTBF of the device.

5. Assumptions for the FMEDA

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Transmitter Supply Isolators KF**-CRG2-**1.D.

- Failure rates based on the values of the Siemens database SN 29500.
- Process related parameters are protected by password.
- Failure rates are constant, wear out mechanisms are not included.
- All components failure modes are known (except µC).
- Propagation of failures is not relevant.
- The current output is configured to NE43 mode.
- The alarm current is set to “fail low” or “fail high”.
- Features that add a delay to the output response are not considered in the given reaction times. It is within the responsibility of the user to respect these times within safety calculations.
- Check the device configuration to ensure the expected output behaviour. Failures during parameterization are not considered for the FMEDA.
- The repair time after a safe failure is 8 hours.
- The test time of the logic solver to react on a dangerous detected failure is 1 hour.
- External power supply failure rates are not included.
- All devices are operated in the Low Demand or High Demand Mode of operation.
- Short circuit (SC) and lead breakage (LB) detection are activated on the device.
- The application program in the safety logic solver evaluates the signals coming from the device and reacts as the safety function requires. This includes detecting when current output values leave the specified range.
- Two outputs on a device may not be used to increase the output safety values.
- If the current output is used in safety relevant applications, the HOLD function must be deactivated.
- For the relay output, regard the lifetime limitations of the output relays as stated within the data sheet.

According to EN/IEC 61511-1 section 11.4.4 for all type A subsystems (e.g. sensor, final elements and non-PE logic solvers) except PE logic solvers the minimum fault tolerance may be reduced by one. In this case the HFT can be reduced from 1 to 0 for a SIL 2 apparatus. For the full argumentation please refer to Exida Report No. P+F 02/11-01 R012.

The ‘proven-in-use’ assessment is based on evaluation of sales figures and questionnaires to the addresses of main clients regarding their applications. The assumption is based on experience with over 13.000 units in over 8 years (> 800 * 10^6 operating hours). The failure behaviour of the returned units does not indicate any systematic failures. Therefore the aspects for ‘proven in use’ are fulfilled.

6. Periodic Proof Testing

The Transmitter Supply Isolators KF**-CRG2-**1.D 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 Transmitter Supply Isolators used only in Relay applications have to be subjected to a proof test in intervals of 2.5 years, the Transmitter Supply Isolators used only in current output applications have to be subjected to proof test in intervals of less than or equal to 2.5 years.

7. Useful lifetime

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 lifetime, the result of the probabilistic calculation is meaningless as the probability of failure significantly increases with time. The useful lifetime 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 lifetime is valid.

However, according to IEC 61508-2, a useful lifetime, based on experience, should be assumed. Experience has shown that the useful lifetime often lies within a range period of about 8 ... 12 years.

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and plant operator can extend the useful lifetime.

Our experience has shown that the useful lifetime of a Pepperl+Fuchs product can be higher if the devices are not driven under harsh environmental conditions. This can be established by using the devices in a controlled environment with small temperature changes and ambient temperatures well within the limits of the device specification (see data sheet and accompanying documentation for limitations).

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

The useful lifetime for a relay output is also limited by the maximum switching cycles under load conditions. Please refer to the data sheet for further information.

Unsere Erfahrung hat gezeigt, dass die Gebrauchsdauer höher sein kann wenn das Gerät nicht unter

8. Bibliography

Manufacturing Documents

01-4294 from 02.04.01, Circuit diagram for KF..-CRG/CRGN-(Ex)1.. I/O boards.
01-7367A from 21. Aug. 2007, Circuit diagram for KF..-CRG2…D.. I/O boards.
01-4384C from 14.04.00, Circuit diagram for KFD2 / KFU8 power supplies.
01-7317 and 01-7308A, Circuit diagrams for KFD2 / KFU8 power supplies.
05-4511A from 02. Jun 2006, Layout for KFD2 power supply for an input of 20..30 VDC for the CRG2 devices.
05-4501B from 30. Jun 2006, Layout for KFU8 power supply for an input of 20..90 VDC / 48..253VAC for the CRG2 devices.
05-4568B from 04. Mar 2008, Layout CRG2 I/O board.
Bill of material for KFD2-CRG-Ex1.D part no. 051097 dated 2011-May-25.
Bill of material for KFD2-CRG2-Ex1.D part no. 191877 dated 2011-May-25.
Bill of material for KFU8-CRG-Ex1.D part no. 051099 dated 2011-May-25.
Bill of material for KFU8-CRG2-Ex1.D part no. 191879 dated 2011-May-25.
18-30076C from 2003-Jul-02, Software release information version CRG2V10 for the CRG device.
368-3023A from 2006-Dec-1, Software release information version 3.02 for the CRG2 device.
CRG2 sales statistics, e-mail dated 2010-Nov-25.
CRG2 repair statistics, excel sheet dated 2010-Oct-07.
General repair statistics process automation dated 2014-Jan-29

Standards

IEC 61508:2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
Harmonized as EN 61508:2010
IEC 61511-1 2003-01+Corr.2004, Functional safety: Safety Instrumented Systems for the process industry sector; Part 1: Framework, definitions, system, hardware and software requirements
Harmonized as EN 61511-1:2005
SN 29500 Failure rates of components
FMD-91, RAC 1991 Failure Mode / Mechanism Distributions
FMD-97, RAC 1997 Failure Mode / Mechanism Distributions