

# FMEDA Hardware - Assessment

## KF\*\*-CRG2-\*\*1.D

### 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: 2011-Jan-17              |
|  <b>PEPPERL+FUCHS</b><br>Mannheim | FMEDA – Hardware Assessment   | respons. | DP.HSU     | FS-0013PF-20C<br>sheet 1 of 10 |
|  | KF**-CRG2-**1.D   | approved |            |                                |
|  |   | norm     |            |                                |

|  |           |
|--|-----------|
| <b>1. MANAGEMENT SUMMARY .....</b>                   | <b>3</b>  |
| <b>2. DESCRIPTION OF THE FAILURE CATEGORIES.....</b> | <b>5</b>  |
| <b>3. ASSUMPTION.....</b>                            | <b>7</b>  |
| <b>4. RESULTS OF THE KF**-CRG2-**1.D.....</b>        | <b>8</b>  |
| 4.1. RESULTS RELAY OUTPUT.....                       | 8         |
| 4.2. RESULTS CURRENT OUTPUT.....                     | 9         |
| <b>5. USEFUL LIFE TIME.....</b>                      | <b>10</b> |

|  |   |            |                   |
|--|---|------------|-------------------|
| CONFIDENTIAL acc. to ISO 16016   | Only valid as long as released in EDM or with a valid production documentation! | scale: 1:1 | date: 2011-Jan-17 |
|  <b>PEPPERL+FUCHS</b><br>Mannheim | FMEDA – Hardware Assessment   | respons.   | DP.HSU            |
|  | KF**-CRG2-**1.D   | approved   | FS-0013PF-20C     |
|  |   | norm       |                   |

# 1. Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the Transmitter Supply Isolators KF\*\*-CRG2-\*\*.1D. The impact analysis is done in the document 30-0624. Additionally the “proven in use” aspect was repeated as a basis for this document.

For field experience IEC 61508 lists techniques and measures to observe systematic failures and their effectiveness (IEC 61508-2 Table B.6). Field experience can be used as a measure to avoid systematic failures.

According to our sales figures we sold over 13 000 units during 2.5 years (approx.  $142 \cdot 10^6$  operating hours). The failure behaviour of the returned units does not indicate any systematic failures.

Therefore the proven in use aspect is fulfilled.

Table 1 shows an overview and explains the differences between the various versions.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safety Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

**Table 1: Version overview**

| Type            | Supply voltage            | Inputs                  | Outputs                         |
|-----------------|---------------------------|-------------------------|---------------------------------|
| KFD2-CRG2-1.D   | 24 VDC                    | AI 0/4..20mA            | 1 AO 4..20mA<br>2 relay outputs |
| KFD2-CRG2-Ex1.D | 24 VDC                    | AI 0/4..20mA Eex ia IIC | 1 AO 4..20mA<br>2 relay outputs |
|                 |                           |                         |                                 |
| KFD2-CRG2-1.D   | 20..90 VDC<br>48..253 VAC | AI 0/4..20mA            | 1 AO 4..20mA<br>2 relay outputs |
| KFD2-CRG2-Ex1.D | 20..90 VDC<br>48..253 VAC | AI 0/4..20mA Eex ia IIC | 1 AO 4..20mA<br>2 relay outputs |

The two relay outputs on each module shall not be used to increase the hardware fault tolerance, needed to achieve a higher SIL for a certain safety function, as they contain common components.

|   |   |            |                   |
|---|---|------------|-------------------|
| CONFIDENTIAL acc. to ISO 16016  | Only valid as long as released in EDM or with a valid production documentation! | scale: 1:1 | date: 2011-Jan-17 |
| <br>Mannheim | FMEDA – Hardware Assessment   | respons.   | DP.HSU            |
|   | KF**-CRG2-**.1D   | approved   | FS-0013PF-20C     |
|   |   | norm       |                   |

Failure rates used in this analysis are basic failure rates from the Siemens standard SN 29500.

According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be  $\geq 10^{-3}$  to  $< 10^{-2}$  for SIL 2 safety functions. However, as the modules under consideration are only one part of an entire safety function, they should not claim more than 10% of this range. For a SIL 2 application the total  $PFD_{AVG}$  value of the SIF must be smaller than  $1,00E-02$ , hence the maximum allowable  $PFD_{AVG}$  value for the Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* would then be  $1,00E-03$ .

The Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* 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 IEC 61508-2 for SIL 2 (sub-) systems.

As the Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. Therefore according to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4, a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems being Type B components and having a SFF of 60% to  $< 90\%$ .

**Acc. Table 3: Summary for the Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* (relay output)**

| T[Proof] = 1 year      | T[Proof] = 2 years     | T[Proof] = 5 years     | SFF   | DC <sub>S</sub> | DC <sub>D</sub> |
|------------------------|------------------------|------------------------|-------|-----------------|-----------------|
| $PFD_{AVG} = 3.94E-04$ | $PFD_{AVG} = 7.88E-04$ | $PFD_{AVG} = 1.97E-03$ | > 83% | 3%              | 50%             |

$$\lambda_{sd} = 9,00E-09 \text{ 1/h} = 9 \text{ FIT}$$

$$\lambda_{su} = 3,47E-07 \text{ 1/h} = 347 \text{ FIT}$$

$$\lambda_{dd} = 8,90E-08 \text{ 1/h} = 89 \text{ FIT}$$

$$\lambda_{du} = 9,00E-08 \text{ 1/h} = 90 \text{ FIT}$$

**Acc. Table 4: Summary for the Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* (current output)**

| T[Proof] = 1 year      | T[Proof] = 2 years     | T[Proof] = 5 years     | SFF   | DC <sub>S</sub> | DC <sub>D</sub> |
|------------------------|------------------------|------------------------|-------|-----------------|-----------------|
| $PFD_{AVG} = 4.14E-04$ | $PFD_{AVG} = 8.29E-04$ | $PFD_{AVG} = 2.07E-03$ | > 81% | 0%              | 71%             |

$$\lambda_{sd} = 0,00E-00 \text{ 1/h} = 0 \text{ FIT}$$

$$\lambda_{su} = 1,73E-07 \text{ 1/h} = 173 \text{ FIT}$$

$$\lambda_{dd} = 2,43E-07 \text{ 1/h} = 89 \text{ FIT}$$

$$\lambda_{du} = 9,47E-08 \text{ 1/h} = 95 \text{ FIT}$$

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1, but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to the table 2 of IEC 61508-1 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ .

|   |   |          |            |                   |
|---|---|----------|------------|-------------------|
| CONFIDENTIAL acc. to ISO 16016  | Only valid as long as released in EDM or with a valid production documentation! |          | scale: 1:1 | date: 2011-Jan-17 |
| <br>Mannheim | FMEDA – Hardware Assessment   | respons. | DP.HSU     | FS-0013PF-20C     |
|   | KF**-CRG2-**1.D   | approved |            |                   |
|   |   | norm     |            |                   |

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40°C. 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.

The hardware assessment according to IEC 61508 has shown that the Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* have a PFD<sub>AVG</sub> within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and a Safe Failure Fraction (SFF) of > 83%. Based on the verification of "prior use" they can be used as a single device for SIL2 Safety Functions in terms of IEC 61511-1 First Edition 2003-01.

A user of Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* can utilize these failure rates in a probabilistic model of a safety instrumental function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

## 2. Description of the Failure Categories

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

### Relay output:

**Fail safe state:** The fail-safe state is defined as the output being de-energized (output relay contact is not conducting).

**Safe state:** A safe failure (S) 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 (D) is defined as a failure that does 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. 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 ( $\lambda_{total}$  (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: 2011-Jan-17 |
| <br>Mannheim | FMEDA – Hardware Assessment   | respons. | DP.HSU     | FS-0013PF-20C     |
|   | KF**-CRG2-**.1D   | approved |            |                   |
|   |   | norm     |            |                   |

**Current output:**

- Fail safe state: The fail-safe state is defined as the output going to "fail low" or "fail high".
  
- Safe state: A safe failure (S) 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 (D) is defined as a failure that 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 5% full scale (+/- 0.8mA)
  
- 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).
  
- 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).
  
- 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 ( $\lambda_{total}$  (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: 2011-Jan-17                  |
|  <b>PEPPERL+FUCHS</b><br>Mannheim | FMEDA – Hardware Assessment   | respons. | DP.HSU     | FS-0013PF-20C<br><br>sheet 6 of 10 |
|  | KF**-CRG2-**1.D   | approved |            |                                    |
|  |   | norm     |            |                                    |

### 3. Assumption

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

- Short Circuit (SC) detection and Lead Breakage (LB) detection are activated.
- Process related parameters are protected by password.
- Failure rates are constant, wear out mechanisms are not included.
- All components failure modes are known.
- Propagation of failures is not relevant.
- The current output is configured for 4..20 mA.
- The alarm current is set to "Fail low" or "fail high".
- Failures during parameterization are not considered.
- 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 modules are operated in the low demand mode of operation.
- The application program in the safety logic solver is constructed in such a way that fail low and fail high failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Both channels on a module may not be used to carry out the same safety function.

### Assessment

According to IEC 61511-1 First Edition 2003-01 section 11.4.4 for all 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.

|  |   |          |            |                   |
|--|---|----------|------------|-------------------|
| CONFIDENTIAL acc. to ISO 16016   | Only valid as long as released in EDM or with a valid production documentation! |          | scale: 1:1 | date: 2011-Jan-17 |
|  <b>PEPPERL+FUCHS</b><br>Mannheim | FMEDA – Hardware Assessment   | respons. | DP.HSU     | FS-0013PF-20C     |
|  | KF**-CRG2-**1.D   | approved |            |                   |
|  |   | norm     |            |                   |

## 4. Results of the KF\*\*-CRG2-\*\*1.D

### 4.1. Results Relay Output

The FMEDA carried out on the Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* (relay output) leads under the assumptions described to the following failure rates and SFF:

$$\lambda_{sd} = 9,00E-09 \text{ 1/h}$$

$$\lambda_{su} = \lambda_{su} + \lambda_{don't \text{ care}} + \lambda_{annunciation} = 1,67E-07 \text{ 1/h} + 1,77E-07 \text{ 1/h} + 3,36E-09 \text{ 1/h} = 3,47E-07 \text{ 1/h}$$

$$\lambda_{dd} = 8,90E-08 \text{ 1/h}$$

$$\lambda_{du} = 9,00E-08 \text{ 1/h}$$

$$\lambda_{total} = 5,35E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 3,88E-08 \text{ 1/h}$$

$$SFF = 83,18\%$$

The  $PFD_{AVG}$  was calculated for three different proof times.

**Table 3: Relay output**

| T[Proof] = 1 year      | T[Proof] = 2 years     | T[Proof] = 5 years     |
|------------------------|------------------------|------------------------|
| $PFD_{AVG} = 3.94E-04$ | $PFD_{AVG} = 7.88E-04$ | $PFD_{AVG} = 1.97E-03$ |

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1, but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to the table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ .

|   |   |            |                   |
|---|---|------------|-------------------|
| CONFIDENTIAL acc. to ISO 16016  | Only valid as long as released in EDM or with a valid production documentation! | scale: 1:1 | date: 2011-Jan-17 |
| <br>Mannheim | FMEDA – Hardware Assessment   | respons.   | DP.HSU            |
|   | KF**-CRG2-**1.D   | approved   | FS-0013PF-20C     |
|   |   | norm       |                   |

## 4.2. Results Current Output

The FMEDA carried out on the Transmitter Supply Isolators KF\*\*-CRG2-\*\*\* (current output) leads under the assumptions described to the following failure rates and SFF:

$$\lambda_{sd} = 9,00E-09 \text{ 1/h}$$

$$\lambda_{su} = 5,63E-08 \text{ 1/h}$$

$$\lambda_{dd} = 6,55E-08 \text{ 1/h}$$

$$\lambda_{du} = 9,47E-08 \text{ 1/h}$$

$$\lambda_{high} = 2,29E-07 \text{ 1/h}$$

$$\lambda_{low} = 1,10E-07 \text{ 1/h}$$

$$\lambda_{annunciation} = 3,36E-09 \text{ 1/h}$$

$$\lambda_{no \text{ effect}} = 1,70E-07 \text{ 1/h}$$

$$\lambda_{total} = 5,11E-07 \text{ 1/h}$$

$$\lambda_{not \text{ part}} = 5,44E-08 \text{ 1/h}$$

$$MTBF = MTTF + MTTR = 1 / (\lambda_{total} + \lambda_{not \text{ part}}) + 8 \text{ h} = 202 \text{ years}$$

$$SFF = 81,47\%$$

The  $PFD_{AVG}$  was calculated for three different proof times.

**Table 4: Current output**

| T[Proof] = 1 year      | T[Proof] = 2 years     | T[Proof] = 5 years     |
|------------------------|------------------------|------------------------|
| $PFD_{AVG} = 4.14E-04$ | $PFD_{AVG} = 8.29E-04$ | $PFD_{AVG} = 2.07E-03$ |

The boxes marked in yellow (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1, but do not fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ . The boxes marked in green (  ) mean that the calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to the table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA-84.01-1996 and do fulfill the requirement to not claim more than 10% of this range, i.e. to be better than or equal to  $1,00E-03$ .

|   |   |            |                   |
|---|---|------------|-------------------|
| CONFIDENTIAL acc. to ISO 16016  | Only valid as long as released in EDM or with a valid production documentation! | scale: 1:1 | date: 2011-Jan-17 |
| <br>Mannheim | FMEDA – Hardware Assessment   | respons.   | DP.HSU            |
|   | KF**-CRG2-**1.D   | approved   | FS-0013PF-20C     |
|   |   | norm       |                   |

## 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.

The useful lifetime is also limited by the maximum switching cycles under load conditions. 100 000 cycles @ 2A contact load

|  |   |          |            |                                     |
|--|---|----------|------------|-------------------------------------|
| CONFIDENTIAL acc. to ISO 16016   | Only valid as long as released in EDM or with a valid production documentation! |          | scale: 1:1 | date: 2011-Jan-17                   |
|  <b>PEPPERL+FUCHS</b><br>Mannheim | FMEDA – Hardware Assessment   | respons. | DP.HSU     | FS-0013PF-20C<br><br>sheet 10 of 10 |
|  | KF**-CRG2-**-1.D  | approved |            |                                     |
|  |   | norm     |            |                                     |