

**FMEDA – Report  
Failure Modes, Effects and Diagnostic Analysis**

Device Model Number:

**HiC2095  
and  
HiD2096**

**Project:  
DDE-0913**

**Pepperl+Fuchs GmbH  
Mannheim  
Germany**



	This document is subject to change without notice. All rights reserved.	scale: 1:1	date: 2014-Dec-09
 <b>PEPPERL+FUCHS</b> Mannheim	FMEDA – Report	respons.	DP.MKI
	HiC2095 and HiD2096	approved	
		norm	
			CERT-3466 sheet 1 of 10

Table of content:

1. Report Summary.....	3
2. Result of the assessment .....	3
3. Functional description of the Analysed Module HiC2095 and HiD2096.....	4
4. Definition of the failure categories.....	5
5. Assumptions .....	6
6. Results of the assessment.....	7
7. Possibilities to Reveal Dangerous Undetected Faults during the Proof Test.....	8
8. Periodic Proof Testing .....	8
9. Useful life time .....	9
10. Abbreviations .....	10
11. Literature .....	10

	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
 Mannheim	FMEDA – Report	respons.	DP.MKI	CERT-3466
	HiC2095 and HiD2096	approved		
			norm	

# 1. Report Summary

This report summarizes the results of the FMEA carried out on the Transformer-isolated barrier for vibration sensors HiC2095 and HiD2096 with circuit diagram 251-5068C from 16/06/2010.

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 for Low Demand Mode, i.e. they should be lower than  $10^{-3}$  for SIL2. For High Demand Mode, 15% of the failure budget or lower than  $1,5 \times 10^{-7} h^{-1}$  are necessary.

Since the barriers HiC2095 and HiD2096 are considered to be Type A devices with a hardware fault tolerance of "0", the SFF shall be  $\geq 60\%$  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: HiC2095 and HiD2096 1oo1 structure**

Parameters acc. to IEC61508	Variables
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Voltage Repeater
HFT	0
SIL	2
$\lambda_{sd} + \lambda_{su}^2$	312 FIT
$\lambda_{dd}$	0 FIT
$\lambda_{du}$	126 FIT
$\lambda_{total}$ (Safety function)	438 FIT
SFF	71.3 %
MTBF <sup>1</sup>	240 years
PFH	$1.26 \cdot 10^{-7} 1/h$
PFD <sub>avg</sub> for T <sub>proof</sub> = 1 year	$5.50 \cdot 10^{-4}$
PFD <sub>avg</sub> for T <sub>proof</sub> = 2 years	$1.10 \cdot 10^{-3}$
PFD <sub>avg</sub> for T <sub>proof</sub> = 5 years	$2.75 \cdot 10^{-3}$
Safety Response Time	12.5 $\mu$ s

<sup>1</sup> acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h

<sup>2</sup> failures in parts that are part of the safety function but do not influence the safety function are regarded as safe undetected.

 Mannheim	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
	FMEA – Report		respons.	DP.MKI
	HiC2095 and HiD2096		approved	CERT-3466
			norm	sheet 3 of 10

### 3. Functional description of the Analysed Module HiC2095 and HiD2096

The device is a voltage repeater module which provides vibration sensors or accelerometer with 2- or 3-wire connection.

This isolated barrier is used for intrinsic safety applications. It provides a floating output to power a vibration sensor or accelerometer in a hazardous area and transfers the voltage signal from that sensor to the safe area.

The device is designed to provide a voltage or current supply to the vibration sensor. Depending on DIP switch setting the barrier provides 3.7 mA, 5.3 mA, or 9.0 mA supply current for 2-wire sensors, or 18 V at 20 mA for 3-wire sensors.

The HiC device provides one channel, the HiD device provides two channels with the additionally terminals no. 1a, 3b, 3a, 1b, 10a, 9a shown in Figure 1.

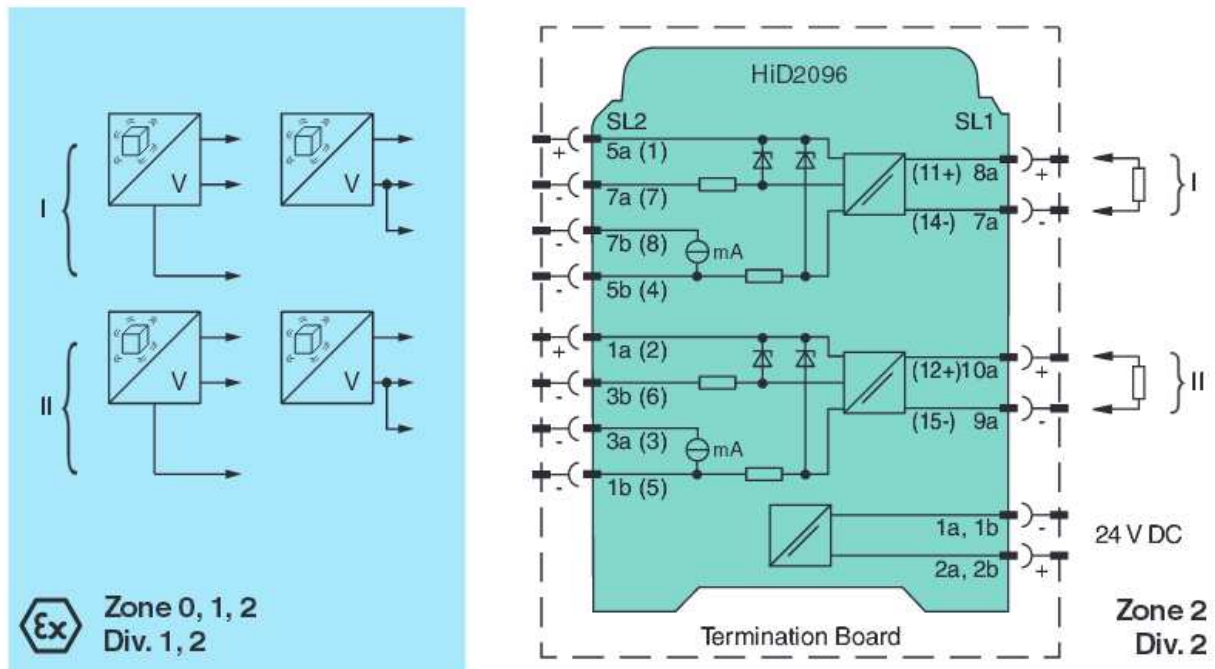



Fig. 1: Connection of the HiD2096

#### Input (left side):

Transmission range 0...-20V  
 Output operating current SL2: 5a, 5b: > 10 mA at -21 V or > 20 mA at -18 V  
 SL2: 5a, 7a: 3.7 ± 0.26 mA, 5.3 ± 0.34 mA or 9.0 ± 0.55 mA, dependent on switch settings  
 Input resistance 10 kΩ terminals 5a and 7a

#### Output (right side):

Voltage 0...-20 V  
 Output resistance 24 Ω typ., 27 Ω max.  
 Output load > 9 kΩ

 <b>PEPPERL+FUCHS</b> Mannheim	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09	
	FMEDA – Report		respons.	DP.MKI	
	HiC2095 and HiD2096		approved		CERT-3466
			norm		sheet 4 of 10

## 4. Definition of the failure categories

The FMEDA was done and is documented in EDM under the number FS-0075PF-26. In order to judge the failure behaviour of the resistance repeater HiC2095 and HiD2096, the following definitions for the failure of the product were considered:

### Fail-safe state:

For the user all signals above -1.1 V are invalid. Therefore the safe state was chosen as -0.5 V and higher or -20.5 V and lower.

### Safe failure:

A failure that causes the device to go to the defined fail-safe state without a demand from the process.

### Dangerous failure:

A failure that can cause the device to not respond to a demand from the process (i.e. being unable to go to the defined safe state) or deviates the output by more than 2% of the full measurement span.

### Fail high failure:

Not used.

### Fail low failure:

Not used.

### No effect failure (Residual, Don't care):

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:

Not used.

### Not part:


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 ( $\lambda_{\text{total (Safety function)}}$ ).

### Not considered:

The reaction on this failure mode could not be decided. When calculating the SFF this failure mode is divided into 50% safe failures and 50% dangerous undetected failures.

### Safety Response Time:


The time that is needed to transfer an input signal of a device to its output according to the safety function.

 <b>PEPPERL+FUCHS</b> Mannheim	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
	FMEDA – Report HiC2095 and HiD2096	respons.	DP.MKI	CERT-3466
		approved		
	norm		sheet 5 of 10	

## 5. Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the HiC2095 and HiD2096.

- 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<sub>avg</sub> value of the SIF (Safety Instrumented Function) should be smaller than  $10^{-2}$ , hence the maximum allowable PFD<sub>avg</sub> 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.
- 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-HDBK-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 °C. Humidity levels are assumed within manufacturer's rating. 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 application program in the safety logic solver is constructed in such a way that all voltages above -0.5V or below -20.5V are introducing the safe state of the safety function.
- In a two channel device, a failure leading to a safe state in one channel can result in a wrong potential on the other channel. Therefore the safety PLC must assume that the output is incorrect on that other channel.

		This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
 Mannheim	FMEDA – Report	respons.	DP.MKI	CERT-3466	
	HiC2095 and HiD2096	approved			
			norm		sheet 6 of 10

## 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. These values are calculated for one channel of the device.

**Table 1: HiC2095 and HiD2096 1oo1 structure**

Parameters acc. to IEC61508	Variables
Device type	A
Demand mode	Low Demand Mode or High Demand Mode
Safety Function	Voltage Repeater
HFT	0
SIL	2
$\lambda_{sd} + \lambda_{su}$	312 FIT
$\lambda_{dd}$	0 FIT
$\lambda_{du}$	126 FIT
$\lambda_{total}$ (Safety function)	438 FIT
$\lambda_{total}$ (Device)	476 FIT
SFF	71.3 %
MTBF <sup>1</sup>	240 years
PFH	$1.26 \cdot 10^{-7}$ 1/h
PFD <sub>avg</sub> for T <sub>proof</sub> = 1 year	$5.50 \cdot 10^{-4}$
PFD <sub>avg</sub> for T <sub>proof</sub> = 2 years	$1.10 \cdot 10^{-3}$
PFD <sub>avg</sub> for T <sub>proof</sub> = 5 years	$2.75 \cdot 10^{-3}$
Safety Response Time	12.5 $\mu$ s
<sup>1</sup> acc. To SN29500. This value includes failures which are not part of the safety function / MTTR = 8h <sup>2</sup> failures in parts that are part of the safety function but do not influence the safety function are regarded as safe undetected.	

$$\text{PFD}_{\text{avg}} (\text{T}_{\text{proof}} = 1 \text{ year}) = \lambda_{du} \cdot \frac{T_1}{2} + \lambda_{dd} \cdot T_{\text{Rep}} = 1.26 \cdot 10^{-7} \text{ 1/h} \cdot \frac{8760 \text{ h}}{2} + 0.0$$


$$= 5.50 \cdot 10^{-4}$$

$$\text{PFH} = 1.26 \cdot 10^{-7} \text{ 1/h}$$

$$\text{SFF} = 1 - \frac{\lambda_{du}}{\lambda_{total\_safety}} = 1 - \frac{126.0 \cdot 10^{-7}}{438 \cdot 10^{-7}} \approx \mathbf{71.3 \%}$$

$$\text{MTBF} = \text{MTTF} + \text{MTTR} = [(1 / \lambda_{total}) + 8 \text{ h}]$$

$$= 1 / (4.76 \cdot 10^{-7} \text{ h} \cdot 8760 \text{ h}) = \mathbf{240 \text{ years}}$$

 <b>PEPPERL+FUCHS</b> Mannheim	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
	FMEDA – Report		respons.	DP.MKI
	HiC2095 and HiD2096		approved	
			norm	
				CERT-3466
				sheet 7 of 10

## 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](http://www.pepperl-fuchs.com)

**Table 2: Importance analysis of dangerous undetected failures of HiC2095**

Component	% of total $\lambda_{DU}$	Detection through
RP3	23.89%	100% functional test
RP12	23.89%	
IC11	5.18%	
IC4	3.58%	
IC13	2.87%	
IC12	2.87%	
N101/N102/N103	2.39%	
IC14	2.39%	
NZ11, NZ12, NZ15, NZ16	2.23%	

## 8. Periodic Proof Testing


The voltage repeater module can be proof tested by executing a proof test procedure according to a procedure available from [www.pepperl-fuchs.com](http://www.pepperl-fuchs.com).

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

According to the results of the analysis, the HiC2095 / HiD2096 has to be subjected to a proof test in intervals of not exceeding 1 year when assuming 10% of the failure budget.

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.

 <b>PEPPERL+FUCHS</b> Mannheim	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
	FMEDA – Report		respons.	DP.MKI
	HiC2095 and HiD2096		approved	
			norm	
				CERT-3466
				sheet 8 of 10



## 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.

As noted in DIN EN 61508-2:2011 note NA4, appropriate measures taken by the manufacturer and operator can extend the useful lifetime. 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.

	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
 <b>PEPPERL+FUCHS</b> Mannheim	FMEDA – Report	respons.	DP.MKI	CERT-3466
	HiC2095 and HiD2096	approved		
			norm	

## 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
HFT	Hardware Fault Tolerance
SIL	Safety Integrity Level
MTBF	Mean Time between Failures
T <sub>proof</sub>	Proof time
AVG	Average
PLC	Programmable Logic Controller

## 11. Literature

### Manufacturing Documents


251-5068C from 16-Jun-2010, Circuit diagram for HiC2095 and HiD2096  
 05-5264D from 16-Jun-2011, Layout for HiC2095  
 Bill of material for HiC2095 part no. 200858 dated 13-Mar-2013  
 DDE-0913A from 20-Mar-2007, Development Order HiD2096 and HiC2095

### Assessment Documents

FS-0075PF-20 from 24-Nov-2014, FMEDA Report  
 FS-0075PF-26 from 01-Oct-2014, FMEDA  
 FS-0075PF-26\_2 from 29-Oct-2014, FMEDA  
 FS-0075PF-26\_3 from 28-Oct-2014, Fault Insertion  
 FS-0075PF-26\_4 from 24-Sep-2014, Derating Analysis

### 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

	This document is subject to change without notice. All rights reserved.		scale: 1:1	date: 2014-Dec-09
 Mannheim	FMEDA – Report	respons.	DP.MKI	CERT-3466
	HiC2095 and HiD2096	approved		
			norm	