# FMEDA – Report
# Failure Modes, Effects and Diagnostic Analysis according to EN/IEC 61508:2010 (Ed. 2)

Device Model Number:

## HiD2035
## and
## HiD2036

## Project:
## X7300 (Product Maintenance)

**Pepperl+Fuchs GmbH**
**Mannheim**
**Germany**

# 1. Report Summary

This report summarizes the results of the FMEDA carried out on the isolated barrier for fire detectors or I/P supply HiD2035 and HiD2036 with circuit diagram 351-0058 and 351-0059 both from 2002-Jun-21. The circuits are build identical. The two channels in device HiD2036 are fully independent.

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 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 $< 10^{-6}$ 1/h 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, 10% of the failure budget or lower than $1,0 \times 10^{-7}$1/h are necessary.

Since the barriers HiD2035 and HiD2036 are considered to be Type A devices with a hardware fault tolerance of “0”, the SFF shall be ≥ 60% according to table 2 of EN/IEC 61508-2.

## 2. Overview of safety characteristic values

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

**Acc. table 1: HiD2035 and HiD2036 1oo1 structure**

| **Parameters acc. to EN/IEC 61508:2010** | **Safety Characteristic Values** |
|---|---|
| Device type | A |
| Demand mode | Low Demand Mode or High Demand Mode |
| Safety Function | current driver |
| HF | 0 |
| SIL (SC) | 2 |
| $\lambda_{sd}+\lambda_{su}$[1] | 0 FIT |
| $\lambda_{dd}$ | 124 FIT |
| $\lambda_{du}$[1] | 71 FIT |
| $\lambda_{\text{total (Safety function)}}$ | 194 FIT |
| $\lambda_{\text{no effect}}$ | 189 FIT |
| $\lambda_{\text{not part}}$ | 0 FIT |
| SFF | 63 % |
| PTC | 100 % |
| MTBF[2] | 298 years |
| PFH | $7{,}06 \cdot 10^{-8}$ 1/h |
| $PFD_{avg}$ for $T_1$ = 1 year | $3{,}09 \cdot 10^{-4}$ |
| $PFD_{avg}$ for $T_1$ = 2 years | $6{,}18 \cdot 10^{-4}$ |
| $PFD_{avg}$ for $T_1$ = 5 years | $1{,}54 \cdot 10^{-3}$ |
| Reaction time | <100 ms |

[1] Not considered failures are used 50 % as dangerous undetected and 50 % as “No effect”. “No effect” failures are not influencing the safety functions and are therefore not included in the calculation of the SFF.

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

## 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] | Date of Review | Changes since last version |
|---|---|---|---|
| V 0 Rev. 0 | Kindermann (DP.MKI) | 2014-Mar-03 | Newly created |
| V 0 Rev. 1 | Fiebig (DP.DFI),<br>Kindermann (DP.MKI) | 2015-Jun-30 | Update after review |
| V 0 Rev. 2 | Fiebig (DP.DFI)<br>Kindermann (DP.MKI) | 2015-Jul-20 | Change values in accordance to EN/IEC 61508:2010 (Ed. 2) |
| V 0 Rev. 4 | Fiebig (DP.DFI)<br>Kindermann (DP.MKI) | 2015-Aug-18 | Correction after review |
| V 1 Rev. 0 | Kindermann (DP.MKI) | 2015-Aug-18 | Updated version for EDM |
| | | | |

# 3. Functional description of the Analysed Module HiD2035 and HiD2036

The device is a current driver / repeater module which provides fire detectors or I/P supply with 2-wire connection.

This isolated barrier is used for intrinsic safety applications. It is loop-powered and is primarily intended to interface with fire and smoke detectors or with similar switched resistor systems requiring a wide output current range (1.5 mA … 50 mA) to operate correctly. It is also used to drive a current to I/P converter.

Reverse polarity protection prevents damage to the isolator caused by faulty wiring.

The HiD2035 device provides one channel, the HiD2036 device provides two channels (fully independent) with the additionally terminals no. 1a, 1b, 10a, 9a shown in Figure 1.

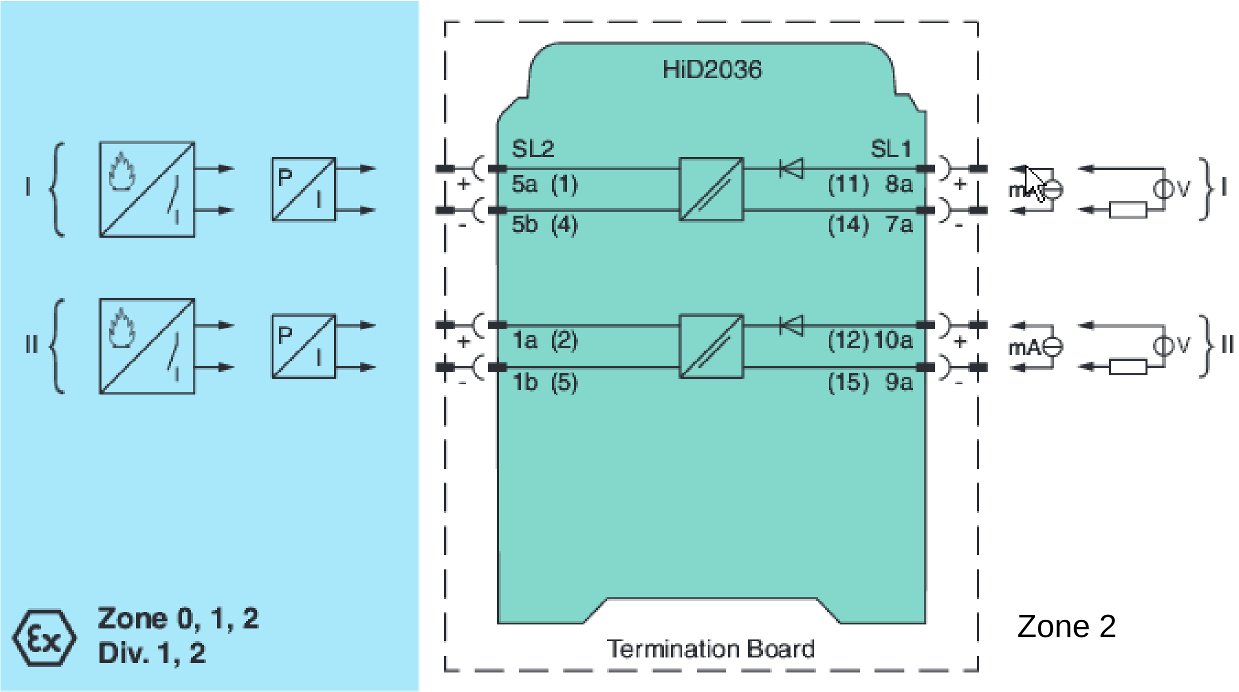

Fig. 1: Connection of the HiD2036

**Supply**

| | |
|---|---|
| Connection | via input terminals |
| Rated voltage | 6…30 V, loop powered, reverse voltage protection |

**Control circuit (right side):**

| | |
|---|---|
| Current consumption | <0.6 mA at 24 V and open circuit |
| Current | 1.5…50 mA, loop powered |
| Signal level | voltage drop 9.6 V at 20 mA and 500 ohm load (4 V at 4 mA) |

**Field circuit (left side):**

| | |
|---|---|
| Characteristics | for fire and smoke detectors<br>$U_{out}$ = ($U_{in}$ – 1.6) – (0.4 x $I_{out}$) 6 V < $U_{in}$ < 25 V<br>$U_{out}$ = (25 – 1.6) – (0.4 x $I_{out}$) 25 V < $U_{in}$ < 30 V |
| Load | 0…750 ohm for I/P applications |
| Ripple | ≤ 150 µA peak to peak for I/P applications |

# 4. Definition of the failure categories

The FMEDA was done and is documented in EDM under the number FS-0093PF-26 (HiD2036) and FS-0093PF-26_2 (HiD2035).
In order to judge the failure behaviour of the current repeater HiD2035 and HiD2036, 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 values of < 2 mA or > 16 mA. The logic solver must be able to detect both thresholds.

**Safe failure:**
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 failure:**
A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that:
a) leads to a measurement error of more than +/-1 mA (considering a range of 1,5…50 mA) and prevents a safety function from operating when required (demand mode) or 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 failure:**
A fail high failure (H) is defined as a failure that causes the output signal to go higher than 16 mA (up to the maximum value of 50 mA).

**Fail low failure:**
A fail low failure (L) is defined as a failure that causes the output signal to go lower than 2 mA (down to the minimum value of 0 mA).

**No Effect failure:**
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 +/- 1 mA (considering a range of 1,5...50 mA). The "No Effect" failure **is not used** for the SFF calculation.

**Annunciation failure:**
Not used in this FMEDA.

**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.

**Not considered:**
Not considered (!) means that this failure mode was not considered. When calculating the SFF this failure mode is divided into **50%** “**no effect**” failures and 50% dangerous undetected failures.

**Reaction 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 HiC2035 and HiD2036.

- 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 EN/IEC 61508-2 for SIL2 (sub)system.
- Failure rates are constant, wear out mechanisms are not included.
- 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 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.
- Do not use the two signal paths of one device in one safety function as components are used that influence both signal paths (supply).
- **The devices are not protected against power supply failures. It is within the responsibility of the user to ensure that low supply voltages are detected and adequate reaction on this fault is implemented.**

# 6. Results of the assessment according to EN/IEC 61508:2010

The following table shows how the above stated requirements are fulfilled. The evaluation was done using the FMEDA tool version 7.1.18 by exida.com.
These values are calculated for one channel of the device. (In device HiD2036 the channels are fully independent.)

**Table 1: HiD2035 and HiD2036 1oo1 structure**

| **Parameters acc. to EN/IEC 61508:2010** | **Safety Characteristic Values** |
|---|---|
| Device type | A |
| Demand mode | Low Demand Mode or High Demand Mode |
| Safety Function | current driver |
| HFT | 0 |
| SIL (SC) | 2 |
| $\lambda_{sd}+\lambda_{su}$[1] | 0 FIT |
| $\lambda_{dd}$ | 124 FIT |
| $\lambda_{du}$[1] | 71 FIT |
| $\lambda_{\text{total (Safety function)}}$ | 194 FIT |
| $\lambda_{\text{no effect}}$ | 189 FIT |
| $\lambda_{\text{not part}}$ | 0 FIT |
| SFF | 63 % |
| PTC | 100 % |
| MTBF[2] | 298 years |
| PFH | $7,06*10^{-8}$ 1/h |
| $PFD_{avg}$ for $T_1$ = 1 year | $3,09*10^{-4}$ |
| $PFD_{avg}$ for $T_1$ = 2 years | $6,18*10^{-4}$ |
| $PFD_{avg}$ for $T_1$ = 5 years | $1,54*10^{-3}$ |
| Reaction time | <100 ms |

[1] Not considered failures are used 50 % as dangerous undetected and 50 % as "No effect".
"No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the SFF.

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

## 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 dangerous undetected failures of HiD2035**

| Component | % of total $\lambda_{DU}$ | Detection through |
|---|---|---|
| P2 – 10 kOhm | 38,26% | 100% functional test |
| P1 – 50 kOhm | 19,13% | |
| P3 – 1 MOhm | 4,25% | |
| T2 – EP13 signal transformer | 3,83% | |
| IC4 – low power op-amp type OP90 | 3,40% | |
| TR4 – NPN BC846 | 2,98% | |
| D3, BAV70 | 2,27% | |
| TR2, TR3 – N-Mosfet type VN0808 | 2,13% | |

## 8. Periodic Proof Testing

The current repeater module can be proof tested by executing a proof test procedure according to a procedure available from 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 HiD2035 / HiD2036 has to be subjected to a proof test in intervals of max. 3 years 2 month 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.

# 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 EN/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.

# 10. Results of the assessment according to EN/IEC 61508:2000

Here, the safety characteristic values for use with edition 1 of EN/IEC 61508 are stated.

**Table 3: HiD2035 and HiD2036 in 1oo1 structure**

| Parameters acc. to EN/IEC 61508:2000 | Safety Characteristic Values |
|---|---|
| Device type | A |
| Demand mode | Low Demand Mode or High Demand Mode |
| Safety Function | current driver |
| HFT | 0 |
| SIL | 2 |
| $\lambda_{sd} + \lambda_{su}$[1] | 189 FIT |
| $\lambda_{dd}$ | 124 FIT |
| $\lambda_{du}$[1] | 71 FIT |
| $\lambda_{total\ (Safety\ function)}$ | 383 FIT |
| $\lambda_{not\ part}$ | 0 FIT |
| SFF | 81,6 % |
| PTC | 100 % |
| MTBF[2] | 298 years |
| PFH | $7{,}06 \cdot 10^{-8}$ 1/h |
| $PFD_{avg}$ for $T_1$ = 1 year | $3{,}09 \cdot 10^{-4}$ |
| $PFD_{avg}$ for $T_1$ = 2 years | $6{,}18 \cdot 10^{-4}$ |
| $PFD_{avg}$ for $T_1$ = 5 years | $1{,}54 \cdot 10^{-3}$ |
| Safety Response Time | < 100 ms |

[1] Not considered failures are considered 50 % as dangerous undetected and 50 % as "No effect". "No effect" failures are not influencing the safety functions and are therefore added to the $\lambda_s$. Failures in parts that are part of the safety function but do not influence the safety function are regarded as safe undetected.

[2] acc. to SN29500. This value includes failures which are not part of the safety function. MTTR = 8h. This value is calculated for one safety function of a device.

# 11. Abbreviations

| | |
|---|---|
| FMEDA | Failure Modes, Effects and Diagnostic Analysis |
| FIT | Failure in Time in $10^{-9}$ 1/h |
| 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 |
| SC | Systematic Capability |
| MTBF | Mean Time Between Failure |
| PTC | Proof Test Coverage |
| $T_1$ | Proof time |
| AVG | Average |
| PLC | Programmable Logic Controller |

# 12. Literature

**Manufacturing Documents**

351-0058 from 2002-Jun-21, Circuit diagram for HiD2035 and
351-0059 from 2002-Jun-21, Circuit diagram for HiD2036.
355-0059 from 2002-Jun-17, Layout for HiD2035/2036.
352-0068, Components List for HiD2035 dated 2002-Jun-21.
352-0069, Components List for HiD2036 dated 2002-Jun-21.
FS-0093PF-27 from 2015-Aug-18, Calculation Sheet

**Standards**

EN/IEC 61508-1:1998 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – General Part
EN/IEC 61508-2:2000 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Requirements
EN/IEC 61508-1:2010 (Edition 2) Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – General Part
EN/IEC 61508-2:2010 (Edition 2) 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