![exida Proven in Use logo]

# FMEDA and Proven-in-use Assessment

Project:
Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881

Customer:

## Pepperl+Fuchs GmbH
Mannheim
Germany

Contract No.: P+F 04/05-08
Report No.: P+F 04/05-08 R021
Version V1, Revision R1.0, November 2004
Stephan Aschenbrenner

## 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 Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881.

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 Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

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, i.e. they should be better than or equal to 1,00E-03.

The Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881 are considered to be Type A[1] components with a hardware fault tolerance of 0.

For Type A components the SFF has to be between 60% and 90% for SIL 2 (sub-) systems with a hardware fault tolerance of 0 according to table 2 of IEC 61508-2.

As the above described devices are supposed to be proven-in-use devices, an assessment of the hardware with additional proven-in-use demonstration for the devices was carried out. The proven-in-use investigation was based on field return data collected and analyzed by Pepperl+Fuchs GmbH.

According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 5.3 the devices are suitable to be used, as a single device, for SIL 2 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

It is important to realize that the "no effect" failures are included in the "safe" failure category according to IEC 61508. Note that these failures on its own will not affect system reliability or safety, and should not be included in spurious trip calculations.


**Table 1: Summary for HiD2871/2872, HiD2875/2876 – Failure rates**

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF |
|---|---|---|
| 167 FIT | 24 FIT | 87,35% |

**Table 2: Summary for HiD2871/2872, HiD2875/2876 – $PFD_{AVG}$ values**

| T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|---|---|---|
| $PFD_{AVG}$ = 1,06E-04 | $PFD_{AVG}$ = 2,11E-04 | $PFD_{AVG}$ = 5,28E-04 |

---

[1] Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

**Table 3: Summary for HiD2881 – Failure rates**

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF |
|---|---|---|
| 200 FIT | 42 FIT | 82,68% |

**Table 4: Summary for HiD2881 – PFD$_{AVG}$ values**

| T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|---|---|---|
| PFD$_{AVG}$ = 1,83E-04 | PFD$_{AVG}$ = 3,67E-04 | PFD$_{AVG}$ = 9,16E-04 |

The boxes marked in green ( ▮ ) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 2 according to 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.

**The functional assessment has shown that the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881 have a PFD$_{AVG}$ within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and a Safe Failure Fraction (SFF) of more than 82%. Based on the verification of "proven-in-use" according to IEC 61508 and its direct relationship to "prior-use" of IEC 61511-1 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 the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in section 5.1 to 5.2 along with all assumptions.

The failure rates are valid for the useful life of the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881, which is estimated to be between 8 and 12 years (see Appendix 3).

The modules HiD2871/2872, HiD2875/2876 and HiD2881, when configured in loop powered mode can be used for SIL 3 safety applications. The following tables show how the above stated requirements are fulfilled.

**Table 5: Summary for HiD2871/2872, HiD2875/2876 – Loop powered mode[2]**

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF | PFD$_{AVG}$ |
|---|---|---|---|
| 191 FIT | 0 FIT[3] | 100% | 0,00E+00 |

**Table 6: Summary for HiD2881 – Loop powered mode[4]**

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF | PFD$_{AVG}$ |
|---|---|---|---|
| 242 FIT | 0 FIT[3] | 100% | 0,00E+00 |

The calculations are based on the assumption that the loop powered modules are mounted in an environment that is IP 54 compliant (e.g. housing, control cabinet or control room).

---

[2] This requires the following switch setting: SWA/B 2 and SWA/B 3 open; SWA/B 1 closed. Input terminals to be used are 8B1 / 7B1 and 9B1 / 10B1.

[3] In order to deal with the excluded faults in the quantitative analysis it might be reasonable to consider a dangerous failure rate of 0.1 FIT, leading to a SFF of 99,97% and a PFD$_{AVG}$ of 4,38E-06 for a proof time of 10 years.

[4] This requires the following switch setting: SW5 and SW6 open; SW1, SW2 and SW3 closed. Input terminals to be used are 8B1 / 7B1.

**Table of Contents**

# 1 Purpose and Scope

Generally three options exist when doing an assessment of sensors, interfaces and/or final elements.

*Option 1: Hardware assessment according to IEC 61508*

Option 1 is a hardware assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand ($PFD_{AVG}$).

This option for pre-existing hardware devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and does not consist of an assessment of the software development process

*Option 2: Hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511*

Option 2 is an assessment by *exida.com* according to the relevant functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The hardware assessment consists of a FMEDA to determine the fault behavior and the failure rates of the device, which are then used to calculate the Safe Failure Fraction (SFF) and the average Probability of Failure on Demand ($PFD_{AVG}$). In addition this option consists of an assessment of the proven-in-use documentation of the device and its software including the modification process.

This option for pre-existing programmable electronic devices shall provide the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and justify the reduced fault tolerance requirements of IEC 61511 for sensors, final elements and other PE field devices.

*Option 3: Full assessment according to IEC 61508*

Option 3 is a full assessment by *exida.com* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like DIN V VDE 0801, IEC 61508 or EN 954-1. The full assessment extends option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option is most suitable for newly developed software based field devices and programmable controllers to demonstrate full compliance with IEC 61508 to the end-user.


**This assessment shall be done according to option 2.**

This document shall describe the results of the FMEDAs carried out on the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881.

It shall be assessed whether these devices meet the average Probability of Failure on Demand ($PFD_{AVG}$) requirements and the architectural constraints for SIL 2 sub-systems according to IEC 61508 / IEC 61511. It **does not** consider any calculations necessary for proving intrinsic safety.

## 2 Project management

### 2.1 *exida.com*

*exida.com* is one of the world's leading knowledge companies specializing in automation system safety and availability with over 100 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations like TUV and manufacturers, *exida.com* is a partnership with offices around the world. *exida.com* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detail product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida.com* maintains a comprehensive failure rate and failure mode database on process equipment.

### 2.2 Roles of the parties involved

| | |
|---|---|
| Pepperl+Fuchs | Manufacturer of the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881. |
| *exida.com* | Performed the hardware and proven-in-use assessment according to option 2 (see section 1). |

Pepperl+Fuchs GmbH contracted *exida.com* in June 2004 with the FMEDA and $PFD_{AVG}$ calculation of the above mentioned devices.

### 2.3 Standards / Literature used

The services delivered by *exida.com* were performed based on the following standards / literature.

| N1 | IEC 61508-2:2000 | Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems |
|---|---|---|
| N2 | IEC 61511-1 First Edition 2003-01 | Functional safety: Safety Instrumented Systems for the process industry sector; Part 1: Framework, definitions, system, hardware and software requirements |
| N3 | ISBN: 0471133019 John Wiley & Sons | Electronic Components: Selection and Application Guidelines by Victor Meeldijk |
| N4 | FMD-91, RAC 1991 | Failure Mode / Mechanism Distributions |
| N5 | FMD-97, RAC 1997 | Failure Mode / Mechanism Distributions |
| N6 | SN 29500 | Failure rates of components |

## 2.4  Reference documents

### 2.4.1  Documentation provided by the customer

| | | |
|---|---|---|
| [D1] | 351-0073 of 21.06.02 | Electrical schematic HiD 2872 |
| [D2] | 351-0077 of 21.06.02 | Electrical schematic HiD 2876 |
| [D3] | 351-0080 of 21.06.02 | Electrical schematic HiD 2881 |
| [D4] | Version 0 of 05.06.02 | P02.05 Produktpflege.pps |
| [D5] | Version 0 of 05.04.02 | P08.01 Abwicklung von Produktrücklieferungen-0.ppt |
| [D6] | 12.02.02 | P0205010202 NCDRWorkflow.ppt |
| [D7] | Email of 07.09.04 | Statistics of field-feed-back tracking; sold and returned devices |
| [D8] | Repair-data.doc | Revision history and description of failure behavior of returned devices |
| [D9] | Email of 09.09.04 | Description of application examples |
| [D10] | Email of 05.11.04 | Description of clearance and creepage distances |
| [D11] | Email of 05.11.04 | Description of jumper and switch setting for loop powered mode |

### 2.4.2  Documentation generated by *exida.com*

| | |
|---|---|
| [R1] | FMEDA V5 HiD2871-72-75-76 V0 R1.0.xls of 03.08.04 |
| [R2] | FMEDA V5 HiD2881 V0 R1.0.xls of 03.08.04 |
| [R3] | Auswertung - exida.xls of 09.09.04 (Field data evaluation of operating hours, sold devices and returned devices) |
| [R4] | Repair-data exida.doc of 10.09.04 (Evaluation of the description of failure behavior of returned devices) |

# 3 Description of the analyzed modules

## 3.1 HiD2871/2872

Solenoid Drivers HiD2871/2872 energize intrinsically safe solenoid valves, alarm sounders, displays or LED indicators in a Hazardous Area from a loop powered Safe Area control signal, or controlled by a Safe Area switch contact or transistor.

An alternative low current output is available for driving a single LED without installing an external current limiting resistor.

Each channel can be loop-powered, ensuring high integrity operation and permitting current monitoring for detection of line fault. Status of each channel is signalled by an LED.

The Solenoid Drivers HiD2871/2872 are considered to be Type A components with a hardware fault tolerance of 0.

The Solenoid Driver HiD2871 is a single channel module. The Solenoid Driver HiD2872 consists of two channels as shown in Figure 1. The two channels are completely independent of each other.
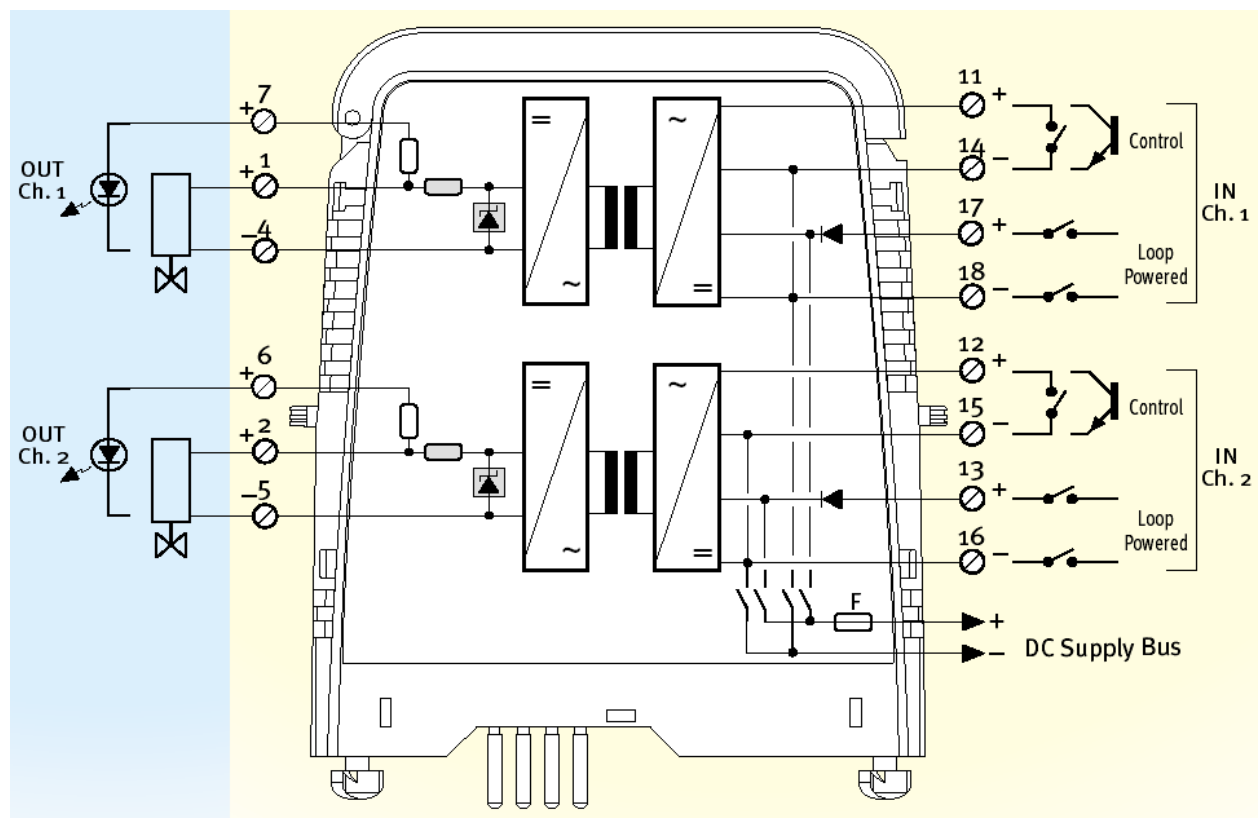


**Figure 1: Block diagram of HiD2872**

## 3.2 HiD2875/2876

Solenoid Drivers HiD2875/2876 energize intrinsically safe solenoid valves, alarm sounders, displays or LED indicators in a Hazardous Area from a loop powered Safe Area control signal, or controlled by a Safe Area switch contact or transistor.

An alternative low current output is available for driving a single LED without installing an external current limiting resistor.

Each channel can be loop-powered, ensuring high integrity operation and permitting current monitoring for detection of line fault. Status of each channel is signalled by an LED.

They are similar to HiD2871/2872 but with different I.S. characteristics.

The Solenoid Drivers HiD2875/2876 are considered to be Type A components with a hardware fault tolerance of 0.

The Solenoid Driver HiD2875 is a single channel module. The Solenoid Driver HiD2876 consists of two channels as shown in Figure 2. The two channels are completely independent of each other.
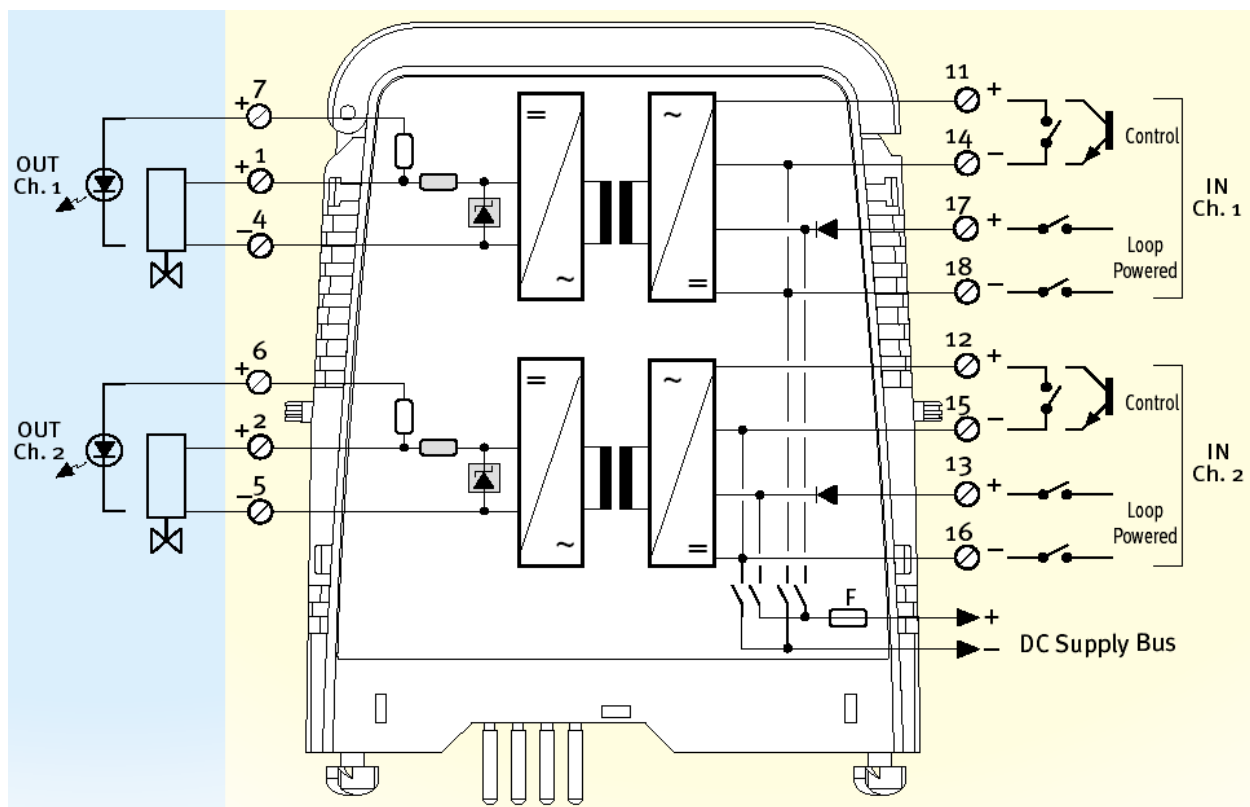


**Figure 2: Block diagram of HiD2876**

---

### 3.3 HiD2881

The Solenoid Driver HiD2881 energizes intrinsically safe solenoid valves in a Hazardous Area controlled by a Safe Area contact, transistor or logic level.

A further programming mode allows the unit to be totally control loop powered ensuring high integrity operation.

Line faults (open and short) can be detected and signalled by a LED, a fault bus output signal and an isolated transistor which is energized in case of fault.

The Solenoid Driver HiD2881 is considered to be a Type A component with a hardware fault tolerance of 0.

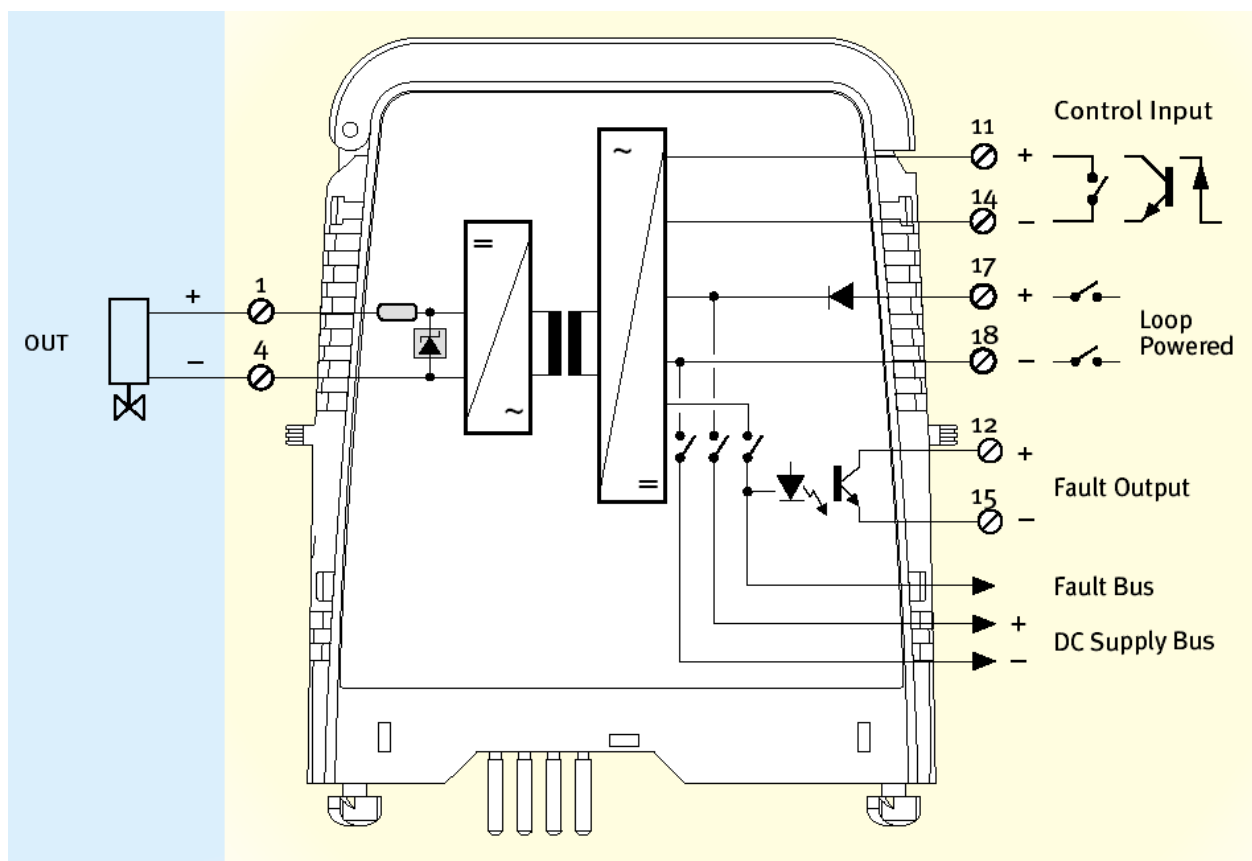Figure 3 shows a block diagram of the Solenoid Driver HiD2881.



**Figure 3: Block diagram of HiD2881**

# 4  Failure Modes, Effects, and Diagnostics Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done together with Pepperl+Fuchs GmbH and is documented in [R1] and [R2].

## 4.1  Description of the failure categories

In order to judge the failure behavior of the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881, the following definitions for the failure of the product were considered.

| | |
|---|---|
| Fail-Safe State | The fail-safe state is defined as the output being de-energized. |
| Fail Dangerous | 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 power more than 10% of the actual value. |
| Fail No Effect | Failure of a component that is part of the safety function but that has no effect on the safety function or deviates the output power not more than 10% of the actual value. For the calculation of the SFF it is treated like a safe undetected failure. |
| Not considered | Not considered (!) means that this failure mode was not considered. When calculating the SFF this failure mode is divided into 50% safe failures and 50% dangerous failures. |
| Not part | Failures of a component which 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. |

The "no effect" failures are provided for those who wish to do reliability modeling more detailed than required by IEC 61508. In IEC 61508 the "no effect" failures are defined as safe undetected failures even though they will not cause the safety function to go to a safe state. Therefore they need to be considered in the Safe Failure Fraction calculation.

## 4.2 Methodology – FMEDA, Failure rates

### 4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

### 4.2.2 Failure rates

The failure rate data used by *exida.com* in this FMEDA are the basic failure rates from the Siemens SN 29500 failure rate database. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match operating stress conditions typical of an industrial field environment similar to IEC 645-1, class C. It is expected that the actual number of field failures will be less than the number predicted by these failure rates.

The user of these numbers is responsible for determining their applicability to any particular environment. Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system that indicates higher failure rates, the higher numbers shall be used. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

### 4.2.3 Assumptions

The following assumptions have been made during the FMEDA:

- Failure rates are constant, wear out mechanisms are not included.

- Propagation of failures is not relevant.

- The repair time after a safe failure is 8 hours.

- 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:

  o 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 40ºC. Humidity levels are assumed within manufacturer's rating.

- All modules are operated in the low demand mode of operation.

- External power supply failure rates are not included.

- The separate fault output of the HiD2881 module which signals if the field wiring is broken or shorted, is not considered in the FMEDA and the calculations.

## 4.2.4  Critical Points of Failure

The analysis has shown that no components of the loop powered modules can be found where potentially dangerous failures exist. All component failures have either no effect on the safety function or can only lead to the defined fail-safe state. The only possible fault which could have an impact on the safety function is a short-circuit on the printed circuit board of the two channel modules HiD2872 and HiD2876.

This possible fault, however, can be excluded according to draft IEC 60947-5-3 A.1.2 if:

- The loop powered modules are mounted in a housing of minimum IP 54

- The base material used is according to IEC 60249, the design and use of the printed board is according to IEC 60326 T3 and the creepage distances and clearances are designed according to IEC 60664-1 (1992) with pollution degree 2 / installation category III, **or**

- The printed side(s) are coated with an insulation material in accordance with IEC 60664-3 (1992)

Clearances and creepage distances according to IEC 60661-1 with pollution degree 2 / installation category III for a nominal voltage of 24 VDC are given in Table 7.

**Table 7: Clearances and creepage distances according to IEC 60661-1**

|  | Clearances (table 2) | Creepage distances (table 4) |
|---|---|---|
| Printed wiring material | 0,2 mm | 0,04 mm |

According to Pepperl+Fuchs the base material used is according to IEC 60249 and the minimum creepage and clearance distances are 0,3 mm. This is sufficient according to Table 7.

The printed circuit boards are insulated with lacquer.

# 5 Results of the assessment

*exida.com* did the FMEDAs together with Pepperl+Fuchs.

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:

$\lambda_{total}$ consists of the sum of all component failure rates. This means:

$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{no\ effect}$

$SFF = 1 - \lambda_{dangerous} / \lambda_{total}$

For the FMEDAs failure modes and distributions were used based on information gained from [N3] to [N5].

For the calculation of the $PFD_{AVG}$ the following Markov model for a 1oo1 system was used. As after a complete proof test all states are going back to the OK state no proof test rate is shown in the Markov models but included in the calculation.

The proof test time was changed using the Microsoft® Excel 2000 based FMEDA tool of *exida.com* as a simulation tool. The results are documented in the following sections.



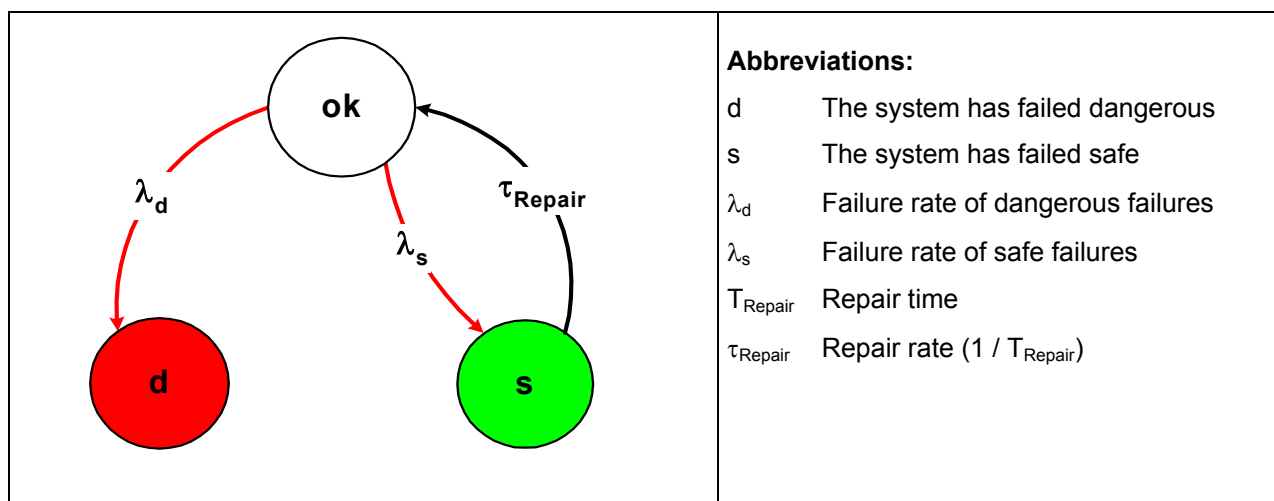| | **Abbreviations:** |
|---|---|
| d | The system has failed dangerous |
| s | The system has failed safe |
| $\lambda_d$ | Failure rate of dangerous failures |
| $\lambda_s$ | Failure rate of safe failures |
| $T_{Repair}$ | Repair time |
| $\tau_{Repair}$ | Repair rate (1 / $T_{Repair}$) |

**Figure 4: Markov model for a 1oo1 structure**

## 5.1 HiD2871/2872 and HiD2875/2876

The FMEDA carried out on HiD2872 leads under the assumptions described in section 4.2.3 to the following failure rates:

$\lambda_{safe}$ = 6,26E-08 1/h

$\lambda_{dangerous}$ = 2,36E-09 1/h

$\lambda_{no\ effect}$ = 8,24E-08 1/h

$\lambda_{not\ considered}$ = 4,36E-08 1/h

$\lambda_{total}$ = 1,91E-07 1/h

$\lambda_{not\ part}$ = 1,16E-08 1/h

MTBF = MTTF + MTTR = 1 / ($\lambda_{total}$ + $\lambda_{not\ part}$) + 8 h = 564 years

Under the assumptions described in section 4.2.4 the following tables show the failure rates according to IEC 61508:

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF |
|---|---|---|
| 167 FIT | 24 FIT | 87,35% |

The PFD$_{AVG}$ was calculated for three different proof test times using the Markov model as described in Figure 4.

| T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|---|---|---|
| PFD$_{AVG}$ = 1,06E-04 | PFD$_{AVG}$ = 2,11E-04 | PFD$_{AVG}$ = 5,28E-04 |

The boxes marked in green (▬) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 2 according to 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. Figure 5 shows the time dependent curve of PFD$_{AVG}$.



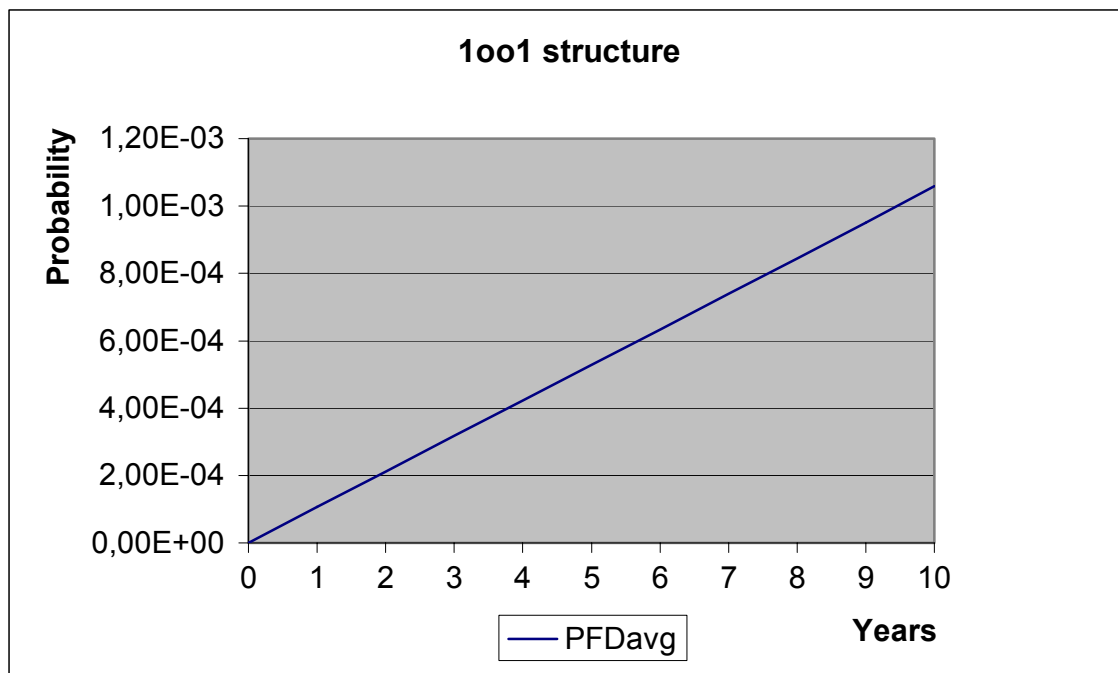**Figure 5: PFD$_{AVG}$(t) of HiD2872**

## 5.2 HiD2881

The FMEDA carried out on HiD2881 leads under the assumptions described in section 4.2.3 to the following failure rates:

$\lambda_{safe}$ = 7,07E-08 1/h

$\lambda_{dangerous}$ = 1,03E-08 1/h

$\lambda_{no\ effect}$ = 9,76E-08 1/h

$\lambda_{not\ considered}$ = 6,31E-08 1/h

$\lambda_{total}$ = 2,42E-07 1/h

$\lambda_{not\ part}$ = 6,12E-08 1/h

MTBF = MTTF + MTTR = 1 / ($\lambda_{total}$ + $\lambda_{not\ part}$) + 8 h = 377 years

Under the assumptions described in section 4.2.4 the following tables show the failure rates according to IEC 61508:

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF |
|---|---|---|
| 200 FIT | 42 FIT | 82,68% |

The PFD$_{AVG}$ was calculated for three different proof test times using the Markov model as described in Figure 4.

| T[Proof] = 1 year | T[Proof] = 2 years | T[Proof] = 5 years |
|---|---|---|
| PFD$_{AVG}$ = 1,83E-04 | PFD$_{AVG}$ = 3,67E-04 | PFD$_{AVG}$ = 9,16E-04 |

The boxes marked in green (▮) mean that the calculated PFD$_{AVG}$ values are within the allowed range for SIL 2 according to 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. Figure 6 shows the time dependent curve of PFD$_{AVG}$.



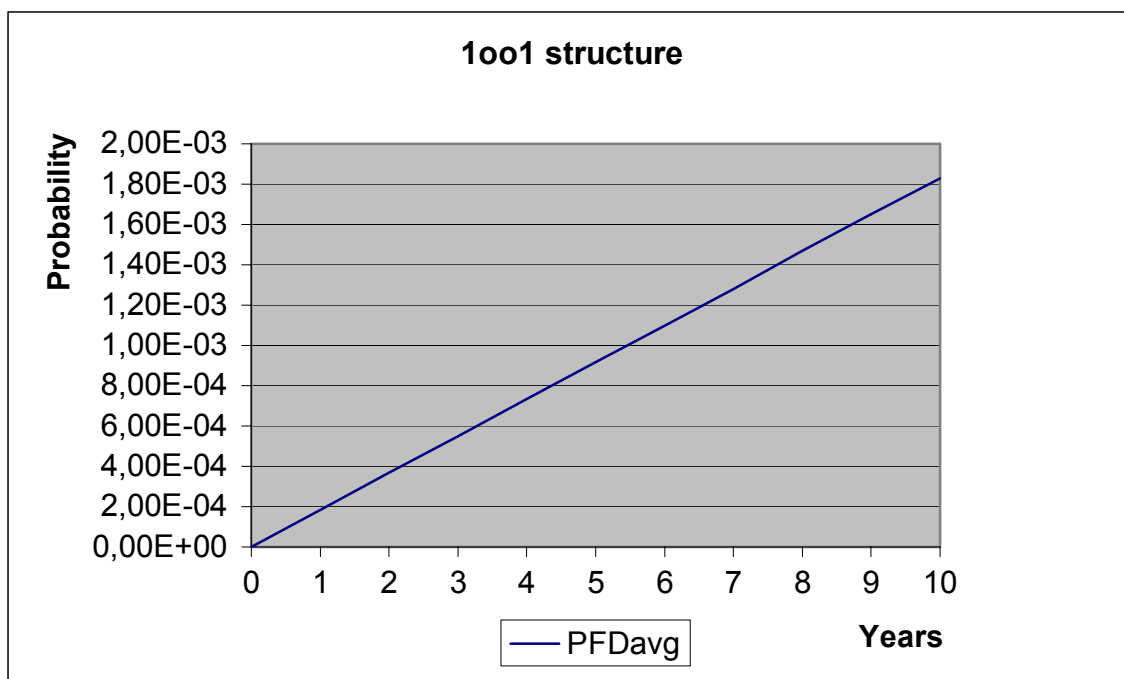**Figure 6: PFD$_{AVG}$(t) of HiD2881**

## 5.3 Loop powered modules

Because the loop powered modules are directly driven from the digital output of a safety PLC there is no additional power supply which can keep the output energized in case of an internal fault. Thus all internal faults have either no effect on the safety function or lead to a safe state.

The modules HiD2871/2872, HiD2875/2876 and HiD2881, when configured in loop powered mode can be used for SIL 3 safety applications. The following tables show how the above stated requirements are fulfilled.

**Table 8: Summary for HiD2871/2872, HiD2875/2876 – Loop powered mode[5]**

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF | PFD$_{AVG}$ |
|---|---|---|---|
| 191 FIT | 0 FIT[6] | 100% | 0,00E+00 |

**Table 9: Summary for HiD2881 – Loop powered mode[7]**

| $\lambda_{safe}$ | $\lambda_{dangerous}$ | SFF | PFD$_{AVG}$ |
|---|---|---|---|
| 242 FIT | 0 FIT[3] | 100% | 0,00E+00 |

The calculations are based on the assumption that the loop powered modules are mounted in an environment that is IP 54 compliant (e.g. housing, control cabinet or control room).

---

[5] This requires the following switch setting: SWA/B 2 and SWA/B 3 open; SWA/B 1 closed. Input terminals to be used are 8B1 / 7B1 and 9B1 / 10B1.

[6] In order to deal with the excluded faults in the quantitative analysis it might be reasonable to consider a dangerous failure rate of 0.1 FIT, leading to a SFF of 99,97% and a PFD$_{AVG}$ of 4,38E-06 for a proof time of 10 years.

[7] This requires the following switch setting: SW5 and SW6 open; SW1, SW2 and SW3 closed. Input terminals to be used are 8B1 / 7B1.

# 6 Proven-in-use Assessment

## 6.1 Definition of the term "Proven-in-use" according to IEC 61508

**Reference**: IEC 61508-7; B.5.4

**Aim:** To use field experience from different applications to prove that the safety-related system will work according to its specification.

**Description:** Use of components or subsystems, which have been shown by experience to have no, or only unimportant, faults when used, essentially unchanged, over a sufficient period of time in numerous different applications.

For proven by use to apply, the following requirements must have been fulfilled:

- unchanged specification;
- 10 systems in different applications;
- $10^5$ operating hours and at least 1 year of service history.

The proof is given through documentation of the vendor and/or operating company. This documentation must contain at least the:

- exact designation of the system and its component, including version control for hardware;
- users and time of application;
- operating hours;
- procedures for the selection of the systems and applications procured to the proof;
- procedures for fault detection and fault registration as well as fault removal.

## 6.2 "Prior-use" requirements according to IEC 61511-1

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 specified in Table 6 of this standard may be reduced by one if the devices under consideration comply with all of the following:

- the hardware of the device is selected on the basis of prior use (see 11.5.3)
- the device allows adjustment of process-related parameters only, e.g., measuring range, upscale or downscale failure direction, etc.;
- the adjustment of the process-related parameters of the device is protected, e.g., jumper, password;
- the function has a SIL requirement less than 4.

**Table 6 of IEC 61511-1 First Edition 2003-01**
**(Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers):**

| SIL | Minimum Hardware Fault Tolerance | |
|---|---|---|
| | Does not meet 11.4.4 requirements | Meets 11.4.4 requirements |
| 1 | 0 | 0 |
| 2 | 1 | 0 |
| 3 | 2 | 1 |
| 4 | Special requirements apply - See IEC 61508 | |

This means that if the requirements of section 11.4.4 of IEC 61511-1 First Edition 2003-01 are fulfilled a hardware fault tolerance of 0 is sufficient for SIL 2 (sub-) systems with a SFF of 60% to < 90%[8].

This is identical to the requirements on Type A (sub)-systems. The Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881 have been developed without considering IEC 61508, however, and so IEC 61511-1 First Edition 2003-01 section 11.4.4 is used as a basis for arguing that proven-in-use shows the unlikelihood of systematic failures.

The assessment of the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881 has shown that the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 are fulfilled based on the following argumentation:

| Requirement | Argumentation[9] |
|---|---|
| See Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01 | 1. The devices are considered to be suitable for use in safety instrumented systems as they are used for more than 6 years in a wide range of applications. They are considered to be of low complexity and the probability that they will fail[10] is <0,3% over the last three years. |
| | 2. Pepperl+Fuchs GmbH is ISO 9001 certified with appropriate quality management and configuration management system. See [D4] to [D6]. The assessed sub-systems are clearly identified and specified.<br>The field feedback tracking database of Pepperl+Fuchs GmbH together with the explanations given in [D7] to [D9] demonstrated the performance of the sub-systems in similar operating profiles and physical environments and the operating experience.<br>The following operating experience exist:<br>HiD2872:  More than 34.500.000 operating hours<br>This is considered to be sufficient taking into account the low complexity of the sub-systems and the use in SIL 2 safety functions only). |
| | 3. 11.5.2 is under the responsibility of the user / manufacturer –> no argumentation. 11.5.3 see bullet items before. |
| | 4. The separate fault output of the HiD2881 module which signals if the field wiring is broken or shorted does not jeopardize the safety function. |
| | 5. Under the responsibility of the user / manufacturer – concerning suitability based on previous use in similar applications and physical environments see [D9]. |

---

[8] IEC 61511-1 First Edition 2003-01 explicitly says "…provided that the dominant failure mode is to the safe state or dangerous failures are detected…".

[9] The numbering is based on the requirements detailed in appendix 1.

[10] The probability of failure is the percentage of all returned devices with relevant repair reasons to all sold devices.

| Requirement | Argumentation[9] |
|---|---|
| Adjustment of process-related parameters only | 3 DIP-switches for each channel ( 6 DIP-switches in total ) with the purpose to configure three function<br><br>- Loop powered<br>- Loop powered with control |
| Adjustment of process-related parameters is protected | N/A as the DIP-switch setting is not critical. The worst-case setting of the DIP switches was considered during the FMEDA. |
| SIL < 4 | The device shall be assessed for its suitability in SIL 2 safety functions only. |

This means that the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881 with a SFF of 60% - < 90% and a HFT = 0 can considered to be proven-in-use according to IEC 61511-1 First Edition 2003-01.

# 7 Terms and Definitions

| | |
|---|---|
| FIT | Failure In Time ($1 \times 10^{-9}$ failures per hour) |
| FMEDA | Failure Mode Effect and Diagnostic Analysis |
| HFT | Hardware Fault Tolerance |
| Low demand mode | Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency. |
| $PFD_{AVG}$ | Average Probability of Failure on Demand |
| SFF | Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action. |
| SIF | Safety Instrumented Function |
| SIL | Safety Integrity Level |
| Type A component | "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2. |
| T[Proof] | Proof Test Interval |

# 8 Status of the document

## 8.1 Liability

*exida.com* prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida.com* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

## 8.2 Releases

Version:              V1
Revision:             R1.0
Version History:  V0, R1.0:   Initial version, August 25, 2004
                           V0, R1.1:   Proven-in-use section completed; September 10, 2004
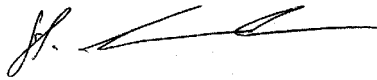                           V1, R1.0:   Review comments integrated; November 15, 2004
Authors:             Stephan Aschenbrenner
Review:              V0, R1.0:   Rachel Amkreutz (exida.com), October 11, 2004
Release status:   Released to Pepperl+Fuchs

## 8.3 Release Signatures

Dipl.-Ing. (Univ.) Stephan Aschenbrenner, Partner

Dipl.-Ing. (Univ.) Rainer Faller, Principal Partner

# Appendix 1: Prior use Proof according to IEC 61511-1 First Edition 2003-01

## Appendix 1.1    Section 11.5.3 of IEC 61511-1 First Edition 2003-01

**(Requirements for the selection of components and subsystems based on prior use)**

1. An assessment shall provide appropriate evidence that the components and sub-systems are suitable for use in the safety instrumented system.

2. The evidence of suitability shall include the following:

   - consideration of the manufacturer's quality, management and configuration management systems;

   - adequate identification and specification of the components or sub-systems;

   - demonstration of the performance of the components or sub-systems in similar operating profiles and physical environments;

   - the volume of the operating experience.

## Appendix 1.2    Section 11.5.4 of IEC 61511-1 First Edition 2003-01

**(Requirements for selection of FPL programmable components and subsystems (for example, field devices) based on prior use)**

3. The requirements of 11.5.2 and 11.5.3 apply.

4. Unused features of the components and sub-systems shall be identified in the evidence of suitability, and it shall be established that they are unlikely to jeopardize the required safety instrumented functions.

5. For the specific configuration and operational profile of the hardware and software, the evidence of suitability shall consider:

   - characteristics of input and output signals;

   - modes of use;

   - functions and configurations used;

   - previous use in similar applications and physical environments.

## Appendix 1.3    Section 11.5.2 of IEC 61511-1 First Edition 2003-01

**(General Requirements)**

6. Components and sub-systems selected for use as part of a safety instrumented system for SIL 1 to SIL 3 applications shall either be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate, or else they shall be in accordance with sub-clauses 11.4 and 11.5.3 to 11.5.6, as appropriate.

7. Components and sub-systems selected for use as part of a safety instrumented system for SIL 4 applications shall be in accordance with IEC 61508-2 and IEC 61508-3, as appropriate.

8. The suitability of the selected components and sub-systems shall be demonstrated, through consideration of:

   - manufacturer hardware and embedded software documentation;

   - if applicable, appropriate application language and tool selection (see clause 12.4.4).

9. The components and sub-systems shall be consistent with the SIS safety requirements specifications.

## Appendix 2: Possibilities to reveal dangerous undetected faults during the proof test

According to section 7.4.3.2.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by diagnostic tests.

This means that it is necessary to specify how dangerous undetected faults which have been noted during the FMEDA can be detected during proof testing.

Table 10 and Table 11 show a sensitivity analysis of the dangerous undetected faults and indicates how these faults can be detected during proof testing.

Appendix 2 and 3 should be considered when writing the safety manual as they contain important safety related information.

**Table 10: Sensitivity Analysis of "du" failures of HiD2872**

| Component | % of total $\lambda_{du}$ | Detection through |
|---|---|---|
| TR1A | 50,85% | 100% functional test with monitoring of the output signal |
| DZ1A | 6,36% | 100% functional test with monitoring of the output signal |
| DZ2A | 6,36% | 100% functional test with monitoring of the output signal |
| DZ3A | 6,36% | 100% functional test with monitoring of the output signal |
| DZ4A | 6,36% | 100% functional test with monitoring of the output signal |
| R3A | 5,93% | 100% functional test with monitoring of the output signal |
| R25A | 5,93% | 100% functional test with monitoring of the output signal |
| R29A | 5,93% | 100% functional test with monitoring of the output signal |
| R30A | 5,93% | 100% functional test with monitoring of the output signal |

**Table 11: Sensitivity Analysis of "du" failures of HiD2881**

| Component | % of total $\lambda_{du}$ | Detection through |
|---|---|---|
| OT1 | 36,41% | 100% functional test with monitoring of the output signal |
| TR4 | 19,42% | 100% functional test with monitoring of the output signal |
| TR5 | 16,02% | 100% functional test with monitoring of the output signal |
| TR7 | 16,02% | 100% functional test with monitoring of the output signal |
| D7 | 5,83% | 100% functional test with monitoring of the output signal |
| DZ1 | 1,46% | 100% functional test with monitoring of the output signal |
| DZ2 | 1,46% | 100% functional test with monitoring of the output signal |
| DZ3 | 1,46% | 100% functional test with monitoring of the output signal |
| DZ4 | 1,46% | 100% functional test with monitoring of the output signal |
| VR1 | 0,49% | 100% functional test with monitoring of the output signal |

## Appendix 3: Impact of lifetime of critical components on the failure rate

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.3) this only applies provided that the useful lifetime of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method 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, electrolyte capacitors can be very sensitive).

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 the $PFD_{AVG}$ calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime 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.

The circuits of the Solenoid Drivers HiD2871/2872, HiD2875/2876 and HiD2881 do not contain any electrolytic capacitors that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

However, according to section 7.4.7.4 of IEC 61508-2, a useful lifetime, based on experience, should be assumed. According to section 7.4.7.4 note 3 of IEC 61508-2 experience has shown that the useful lifetime often lies within a range of 8 to 12 years.