



## **Failure Modes, Effects and Diagnostic Analysis**

Project:

Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877

Company:

**Pepperl+Fuchs GmbH**  
Mannheim  
Germany

Contract No.: P+F 11/07-044

Report No.: P+F 11/07-044 R034

Version V1, Revision R4; April 2017

Stephan Aschenbrenner, Jürgen Hochhaus

## Management Summary

This report summarizes the results of the hardware assessment carried out on the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 in the versions listed in the drawings referenced in section 2.4.1.

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.

For safety applications only the described variants were considered. All other possible variants are not covered by this report.

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

The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment 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 (daily fluctuation of > 15°C) must be assumed.

These failure rates are valid for the useful lifetime of the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877, see Appendix B.

The failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.3.

A user of the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 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 sections 4.3.1 and 4.3.2 along with all assumptions.

The Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 are classified as Type A<sup>1</sup> elements according to IEC 61508, having a hardware fault tolerance of 0.

They can be used for low demand mode applications as well as for high demand mode applications.

The failure rates according to IEC 61508:2010 2<sup>nd</sup> edition for the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 are listed in the following tables. As HiC2873Y1 is restricted to bus powered operation, only Table 1 applies for this variant.

The two channels on the redundant boards HiD2872 and HiD2876 shall not be used for the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either channel used in a single safety function. The two channels may be used in separate safety functions if due regard is taken of the possibility of common failures.

---

<sup>1</sup>. Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

**Table 1: Summary for bus powered operation <sup>2</sup> – IEC 61508 failure rates**

Failure category	Failure rates (in FIT)
Fail Safe Detected ( $\lambda_{SD}$ )	0
Fail Safe Undetected ( $\lambda_{SU}$ )	97
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	30
No effect	131
No part	131
<b>Total failure rate (safety function)</b>	<b>127</b>
<b>SFF <sup>3</sup></b>	<b>76%</b>
<b>SIL AC <sup>4</sup></b>	<b>SIL2</b>
<b>PFH</b>	<b>2.96E-08 1/h</b>

<sup>2</sup> The DIP switch settings selecting the mode of operation are described in the data sheet.

<sup>3</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>4</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

**Table 2: Summary for loop powered operation <sup>5</sup> – IEC 61508 failure rates**

Failure category	Failure rates (in FIT)
Fail Safe Detected ( $\lambda_{SD}$ )	0
Fail Safe Undetected ( $\lambda_{SU}$ )	127
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	0
No effect	131
No part	131
<b>Total failure rate (safety function)</b>	<b>127</b>
<b>SFF <sup>6</sup></b>	<b>100%</b>
<b>SIL AC <sup>7</sup></b>	<b>SIL3</b>
<b>PFH</b>	<b>0.00E-00 1/h</b>

<sup>5</sup> The DIP switch settings selecting the mode of operation are described in the data sheet.

<sup>6</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>7</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

## Table of Contents

Management Summary .....	2
1 Purpose and Scope.....	6
2 Project Management.....	7
2.1 <i>exida</i> .....	7
2.2 Roles of the parties involved .....	7
2.3 Standards and Literature used.....	7
2.4 Reference documents.....	8
2.4.1 Documentation provided .....	8
2.4.2 Documentation generated by exida.....	8
3 Product Description.....	9
4 Failure Modes, Effects, and Diagnostic Analysis.....	11
4.1 Description of the failure categories .....	11
4.2 Methodology – FMEDA, Failure Rates .....	12
4.2.1 FMEDA .....	12
4.2.2 Failure Rates.....	12
4.2.3 Assumptions .....	13
4.3 Results.....	13
4.3.1 Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 .....	14
4.3.2 Loop powered modules.....	15
5 Using the FMEDA Results .....	16
5.1 Example PFD <sub>AVG</sub> calculation .....	16
6 Terms and Definitions .....	17
7 Status of the Document.....	18
7.1 Liability.....	18
7.2 Releases.....	18
7.3 Release Signatures.....	18
Appendix A: Possibilities to reveal dangerous undetected faults during the proof test ..	19
Appendix A.1: Possible proof tests to detect dangerous undetected faults .....	19
Appendix B: Impact of lifetime of critical components on the failure rate .....	20

## 1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the Empty with hardware version as listed in the drawings referenced in section 2.4.1.

The FMEDA builds the basis for an evaluation whether an element including the described Empty meets the average Probability of Failure on Demand ( $PFD_{AVG}$ ) / Probability of dangerous Failure per Hour (PFH) requirements and if applicable the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511. It does not consider any calculations necessary for proving intrinsic safety.

## 2 Project Management

### 2.1 *exida*

*exida* is one of the world's leading product certification and knowledge companies specializing in automation system safety and availability with over 300 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented consulting services, internet based safety engineering tools, detailed product assurance and certification analysis and a collection of on-line safety and reliability resources. *exida* maintains a comprehensive failure rate and failure mode database on process equipment.

### 2.2 Roles of the parties involved

Pepperl+Fuchs GmbH                      Manufacturer of the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877.

*exida*    Carried out the FMEDAs and issued this report.

Pepperl+Fuchs GmbH contracted *exida* in July 2011 with the FMEDA of the above mentioned devices and in October 2016 with the extension of the report.

### 2.3 Standards and Literature used

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

[N1]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems; 2nd edition
[N2]	SN 29500-1:06.1996 SN 29500-1 H1:11.1999 SN 29500-2:11.1999 SN 29500-3:07.1997 SN 29500-4:04.1999 SN 29500-5:06.1996 SN 29500-6:06.1996 SN 29500-7:07.1997 SN 29500-9:04.1992 SN 29500-10:05.1982 SN 29500-11:08.1990 SN 29500-12:03.1994 SN 29500-13:03.1994 SN 29500-14:03.1994	Failure rates of components

[N3]	Electrical & Mechanical Component Reliability Handbook, 2nd Edition, 2008	<i>exida</i> L.L.C, Electrical & Mechanical Component Reliability Handbook, Second Edition, 2008, ISBN 978-0-9727234-6-6
[N4]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic conditions

## 2.4 Reference documents

### 2.4.1 Documentation provided

[D1]	Functional description 3640005.pdf	FUNCTIONAL DESCRIPTION of HiD2872, HiD2876, HiC2873, HiC2877; 364-0005 Rev. P0 of 03.06.08
[D2]	Prelim-data-sheet-HiC2873.pdf	Preliminary datasheet "HiC2873" 210496_ENG_1387495.xml
[D3]	Prelim-data-sheet-HiC2877.pdf	Preliminary datasheet "HiC2877" 210523_ENG_1387496.xml
[D4]	Prelim-data-sheet-HiD2872.pdf	Preliminary datasheet "HiD2872" 204846_eng_1419168.xml
[D5]	Prelim-data-sheet-HiD2876.pdf	Preliminary datasheet "HiD2876" 204847_eng_1419225.xml
[D6]	275177_eng.pdf	Datasheet "HiC2873Y1" 275177_eng.pdf
[D7]	3510552c.pdf	Circuit diagram 351-0552C "HiD2872/2876 HiC2873/2877" of 12.01.10
[D8]	3521294c.pdf	Component list 352-1294C "HiD2872" of 12.01.10
[D9]	Comp list 3521374b.pdf	Component list 352-1374B "HiC2873" of 12.01.10
[D10]	tdoct3721b_eng.pdf	Safety Manual HiD2872, HiC2873(Y1), HiD2876, HiC2877, Version 2017-01
[D11]	fs0091ea-25b.pdf	Impact Analysis for changes for special version HiC2873Y1, of 01.09.2016
[D12]	RE Results of FMEDA review for Hix287x.msg of 25.07.11	
[D13]	Schematic-with-comments.pdf	
[D14]	FMEDA Hix287x Safe To De-Energize Output.xls of 21.07.11	
[D15]	FMEDA Hix287x Safe To De-Energize Output - Review exida-CG.xls of 22.07.11	
[D16]	AW2 Results of FMEDA review for Hix287x.msg of 17.08.11	
[D17]	Antwort bezüglich der Abstandsberechnung.msg of 28.09.11	

### 2.4.2 Documentation generated by *exida*

[R1]	FMEDA Hix287x Safe To De-Energize Output - Review exida.xls of 22.07.11
------	---



### 3 Product Description

The Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 are classified as Type A elements according to IEC 61508, having a hardware fault tolerance of 0.

The isolated barriers are used for intrinsic safety applications. They supply power to solenoids, LEDs and audible alarms located in a hazardous area. They are controlled with a loop-powered control signal, switch contact, transistor, or logic signal.

HiD2872 and HiD2876 are 2-channel devices whereas HiC2873, HiC2873Y1 and HiC2877 are 1-channel devices. The two channels are completely independent of each other.

For HiD2876 and HiC2877 at full load, 11.2 V at 40 mA (with 55 mA current limit) is available for the hazardous area application.

For HiD2872, HiC2873 and HiC2873Y1 at full load, 12 V at 40 mA (with 55 mA current limit) is available for the hazardous area application.

Line fault detection of the field circuit is indicated by a red LED and an output on the fault bus.

The HiD2872 and HiD2876 devices mount on a HiD Termination Board.

The HiC2873, HiC2873Y1 and HiC2877 devices mount on a HiC Termination Board.

The terminal set-up for the different variants is as follows:

HiC2873: For bus powered mode, the input is attached between terminals 12+ and 15- while the supply is attached via power rail. For loop powered mode, the input is attached between terminals 11+ and 14-.

HiD2872 / HiD2876: For bus powered mode, the input is attached between terminals 17+ and 18- (or 13+ and 16- for the second channel) while the supply is attached via power rail. For loop powered mode, the input is attached between terminals 11+ and 14- (or 12+ und 15- for the second channel).

HiC2873Y1: This device only allows bus powered mode. The input is attached between terminals 11+ and 14- while the supply is attached via power rail.

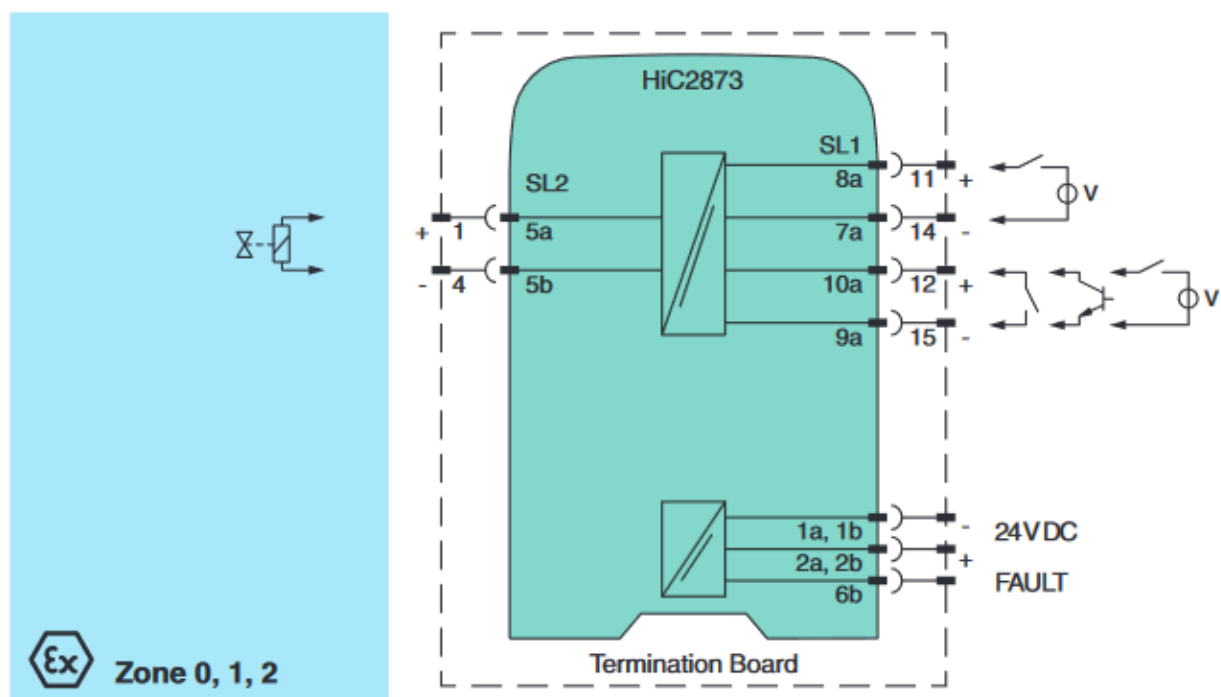


Figure 1: Block diagram of HiC2873 representative for HiC2873 and HiC2877

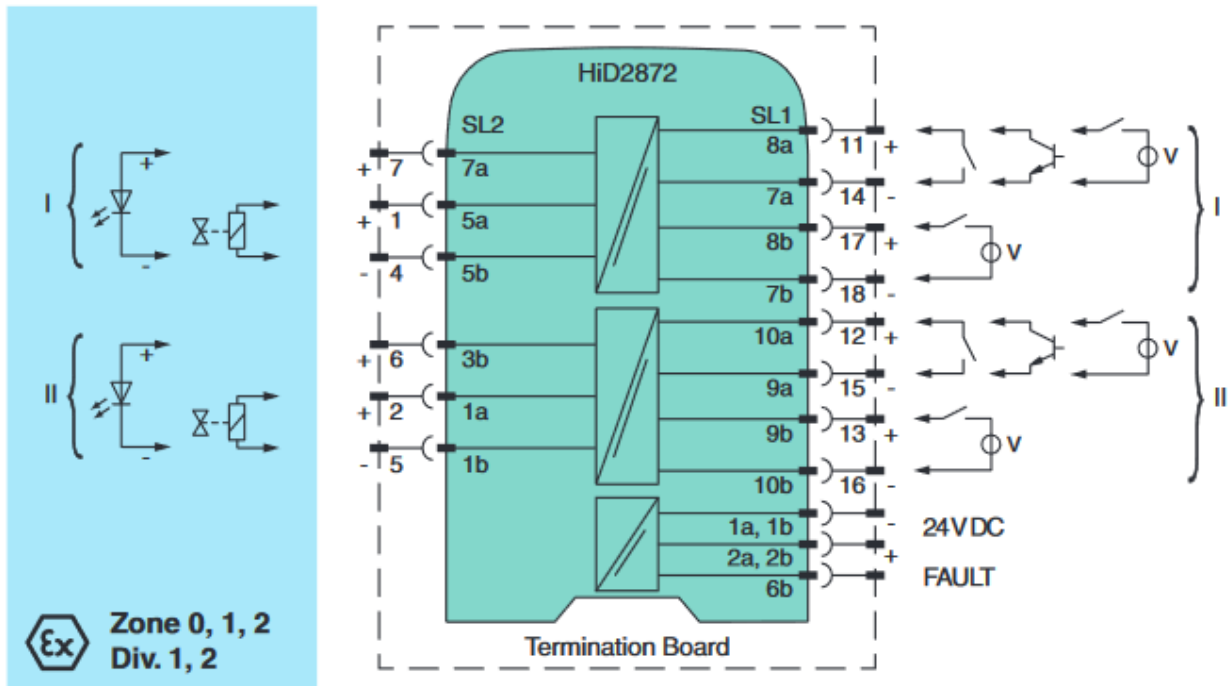


Figure 2: Block diagram of HiD2872 representative for HiD2872 and HiD2876

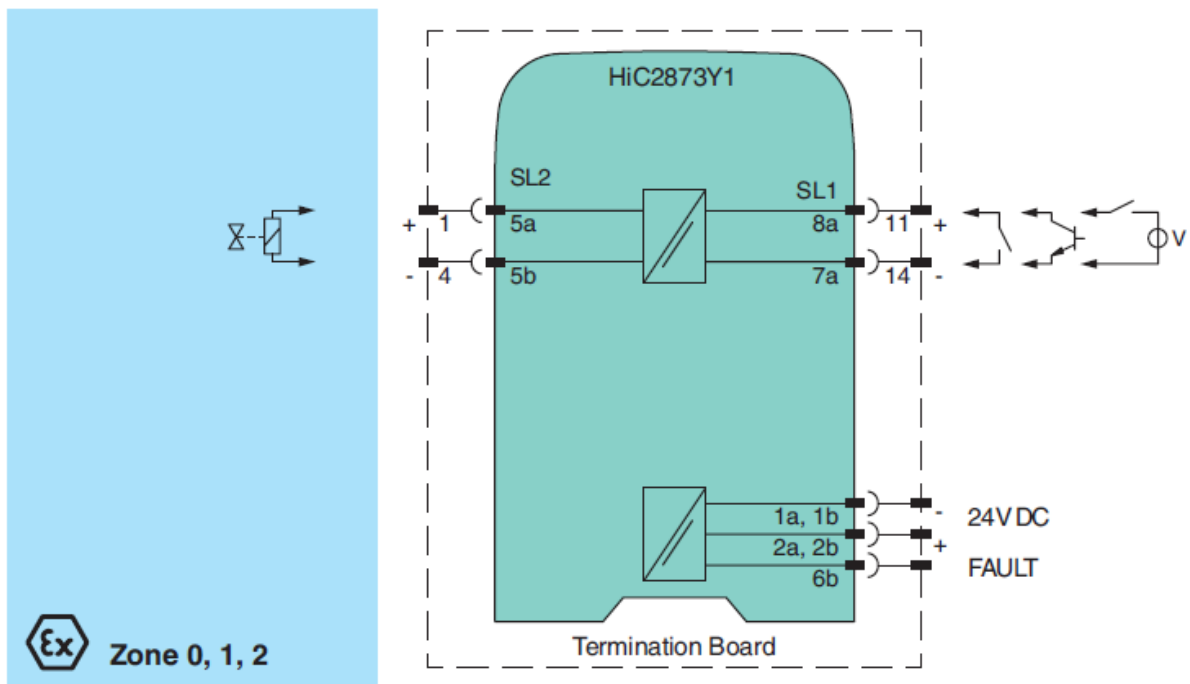


Figure 3: Block diagram of HiC2873Y1

## 4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by *exida*. The results are documented in [D15] and [D16].

### 4.1 Description of the failure categories

In order to judge the failure behavior of the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877, the following definitions for the failure of the device were considered.

Fail-Safe State	The fail-safe state is defined as the output being de-energized (output current less than the specified LFD current of about 0.4mA average).
Fail Safe	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.
Fail Dangerous	A dangerous failure (D) is defined as a failure that plays a part in implementing the safety function that: a) 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 Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by internal diagnostics.
No effect	Failure mode of a component that plays a part in implementing the safety function but is neither a safe failure nor a dangerous failure.
No 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.

## 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 under consideration.

An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extensions 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 rates used in this analysis are the basic failure rates from the Siemens standard SN 29500. 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. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events however should be considered as random failures. Examples of such failures are loss of power or physical abuse.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”.

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 Failure Modes, Effects, and Diagnostic Analysis of the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- Sufficient tests are performed prior to shipment to verify the absence of vendor and/or manufacturing defects that prevent proper operation of specified functionality to product specifications or cause operation different from the design analyzed.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDAs.
- Only one input and one output are part of the considered safety function.
- The two channels on the redundant boards HiD2872 and HiD2876 are not used for the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components.
- External power supply failure rates are not included.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- For safety applications only the described variants are considered.
- The listed SN29500 failure rates are valid for operating stress conditions typical of an industrial field environment 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 (daily fluctuation of > 15°C) must be assumed. Other environmental characteristics are assumed to be within the manufacturer's ratings.
- The separate fault output which signals if the field wiring is broken or shorted is not considered in the FMEDA and the calculations.

### 4.3 Results

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 contributing to the safety function. This means:

$$\lambda_{total} = \lambda_S + \lambda_{DD} + \lambda_{DU}$$

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

### 4.3.1 Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877

The FMEDA carried out on the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates:

**Table 3: Summary for bus powered operation <sup>8</sup> – IEC 61508 failure rates**

Failure category	Failure rates (in FIT)
Fail Safe Detected ( $\lambda_{SD}$ )	0
Fail Safe Undetected ( $\lambda_{SU}$ )	97
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	30
No effect	131
No part	131
<b>Total failure rate (safety function)</b>	<b>127</b>
<b>SFF <sup>9</sup></b>	<b>76%</b>
<b>SIL AC <sup>10</sup></b>	<b>SIL2</b>
<b>PFH</b>	<b>2.96E-08 1/h</b>

<sup>8</sup> The DIP switch settings selecting the mode of operation are described in the data sheet.

<sup>9</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>10</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

### 4.3.2 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 (see also [D17]). Thus all internal faults have either no effect on the safety function or lead to a safe state.

**Table 4: Summary for loop powered operation <sup>11</sup> – IEC 61508 failure rates**

Failure category	Failure rates (in FIT)
<b>Fail Safe Detected (<math>\lambda_{SD}</math>)</b>	<b>0</b>
<b>Fail Safe Undetected (<math>\lambda_{SU}</math>)</b>	<b>127</b>
<b>Fail Dangerous Detected (<math>\lambda_{DD}</math>)</b>	<b>0</b>
<b>Fail Dangerous Undetected (<math>\lambda_{DU}</math>)</b>	<b>0</b>
No effect	131
No part	131
<b>Total failure rate (safety function)</b>	<b>127</b>
<b>SFF <sup>12</sup></b>	<b>100%</b>
<b>SIL AC <sup>13</sup></b>	<b>SIL3</b>
<b>PFH</b>	<b>0.00E-00 1/h</b>

<sup>11</sup> The DIP switch settings selecting the mode of operation are described in the data sheet.

<sup>12</sup> The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

<sup>13</sup> SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL. The SIL AC needs to be evaluated on subsystem level. For full assessment purposes all requirements of IEC 61508 must be considered.

## 5 Using the FMEDA Results

The following section describes how to apply the results of the FMEDA. It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire SIF. *exida* recommends the accurate Markov based exSILentia tool for this purpose.

The following results must be considered in combination with  $PFD_{AVG}$  values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

### 5.1 Example $PFD_{AVG}$ calculation

An average Probability of Failure on Demand ( $PFD_{AVG}$ ) calculation is performed for a single (1oo1D) Solenoid Driver HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 for bus powered operation considering a proof test coverage of 99% (see Appendix A.1) and a mission time of 10 years. The failure rate data used in this calculation is displayed in section 4.3.1. The resulting  $PFD_{AVG}$  values for a variety of proof test intervals are displayed in Table 5.

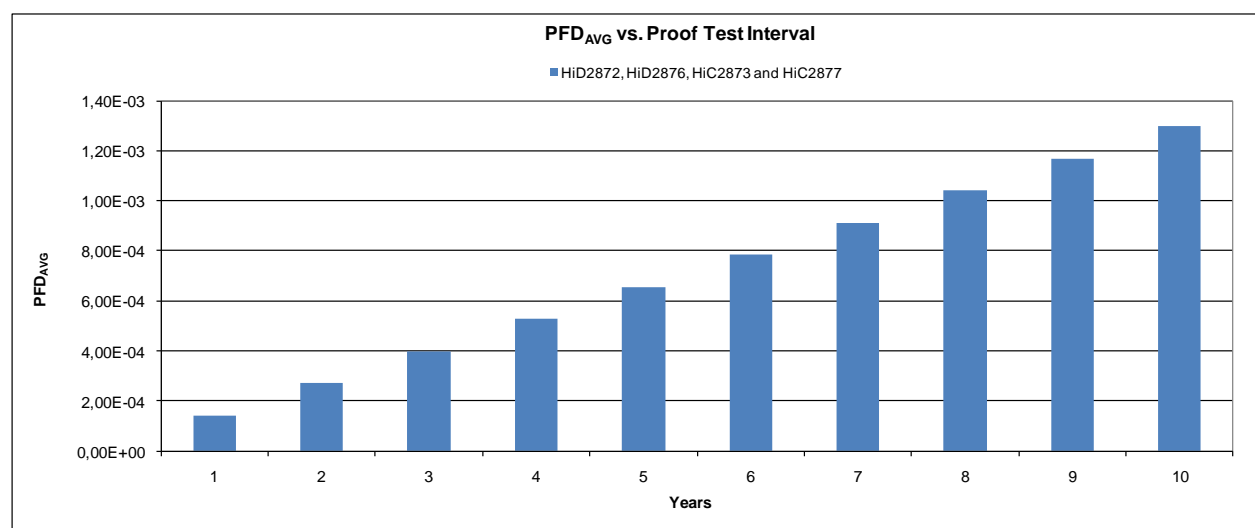
For SIL 2 applications, the  $PFD_{AVG}$  value needs to be  $< 1.00E-02$ .

**Table 5:  $PFD_{AVG}$  values**

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
$PFD_{AVG} = 1.41E-04$	$PFD_{AVG} = 2.70E-04$	$PFD_{AVG} = 6.55E-04$

As the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 are a part of an entire safety function they should only consume a certain percentage of the allowed range. Assuming 10% of this range as a reasonable budget they should be better than or equal to  $1.00E-03$ . The calculated  $PFD_{AVG}$  values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and do fulfill the assumption to not claim more than 10% of this range, i.e. to be better than or equal to  $1.00E-03$ .

Figure 4 shows the time dependent curve of  $PFD_{AVG}$ .



**Figure 4:  $PFD_{AVG}(t)$**



## 6 Terms and Definitions

FIT	Failure In Time (1x10 <sup>-9</sup> failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
LFD	Line Fault Detection
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency.
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.
MTTR	Mean Time To Restoration
PFD <sub>AVG</sub>	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
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

## 7 Status of the Document

### 7.1 Liability

*exida* prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* 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.

Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

### 7.2 Releases

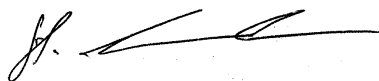
Version History: V1R4: Correction terminal set-up, latest version of safety manual referenced; April 20, 2017  
V1R3: Addition of special version HiC2873Y1; October 10, 2016  
V1R2: Editorial changes; November 4, 2011  
V1R1: Editorial changes; October 26, 2011  
V1R0: Review comments incorporated, October 16, 2011  
V0R1: Initial version; August 22, 2011

Author: Stephan Aschenbrenner, Jürgen Hochhaus

Review: V1R1: Michael Kindermann (P+F); November 4, 2011  
V1R0: Michael Kindermann (P+F); October 19, 2011  
V0R1: Rachel Amkreutz (*exida*); September 16, 2011  
Michael Kindermann (P+F); September 12 and 28, 2011

Release Status: Released to Pepperl+Fuchs GmbH

### 7.3 Release Signatures



---

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



---

Dipl.-Ing.(FH) Jürgen Hochhaus, Senior Safety Engineer

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

According to section 7.4.5.2 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.

Appendix A shall be considered when writing the safety manual as it contains important safety related information.

### Appendix A.1: Possible proof tests to detect dangerous undetected faults

A suggested proof test consists of the steps as described in Table 6. It is assumed that this test will detect 99% of possible dangerous failures.

**Table 6: Steps for proof test**

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Force the Solenoid Drivers HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 to go to the safe state and verify that the safe state is reached.
3.	For the two-channel devices HiD2872 and HiD2876, force 1 channel to go to the safe state and verify that the safe state is achieved. Verify that the other channel is not affected. Repeat this step for the second channel.
4.	Inspect the device for any visible damage.
5.	Remove the bypass and otherwise restore normal operation.

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

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

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<sup>14</sup> 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. Therefore it is obvious that the  $PFD_{AVG}$  calculation is only valid for components which 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 HiD2872, HiD2876, HiC2873, HiC2873Y1 and HiC2877 do not contain any electrolytic capacitors or other components with reduced useful lifetime that are contributing to the dangerous undetected failure rate. Therefore there is no limiting factor with regard to the useful lifetime of the system.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

---

<sup>14</sup> Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.