Failure Modes, Effects and Diagnostic Analysis

Project:
9203 Solenoid / Alarm Driver

Customer:
PR electronics A/S
Rønde
Denmark

Contract No.: PR Q23/09-138
Report No.: PR electronics 06/03-19 R023
Version V3, Revision R3; April, 2024

Armin Schulze, Stephan Aschenbrenner

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

Management summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the 9203 Solenoid / Alarm Driver with hardware version 9203SMD1A-2045 and 9203SMD2A-2041.

A Failure Modes, Effects, and Diagnostic Analysis is one of the steps taken to achieve functional safety assessment of a device per IEC 61508 or ISO 13849. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the devices.

The FMEDA that is described in this report concerns only the hardware of the 9203 Solenoid / Alarm Driver. For full assessment purposes all requirements of IEC 61508 or ISO 13849 must be considered.

Table 1: Overview of the considered Product variants

Description	Variant description
9203B2A (Ex) / 9203A2A	High current type (single channel).

This analysis also covers the low current product variant of the 9203 Solenoid / Alarm Driver. From the perspective of the functional safety, the high current variant is the more critical device, even if the failure rates are very similar.

For safety applications only the described variants with the described hardware and software versions of the 9203 Solenoid / Alarm Driver have been considered. Any other variants and configurations are not covered by this report.

The 9203 Solenoid / Alarm Driver can be considered as a Type B [1] element with a hardware fault tolerance (HFT) of 0.

The failure modes and failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook [N2] for Profile 1. They meet the *exida* criteria for Route 2_H (see Appendix 4). Therefore, the 9203 Solenoid / Alarm Driver can be classified as a 2_H device when the listed failure rates are used. The analysis resulted in a DC (Diagnostic Coverage) of over 60%.

The failure rates are valid for the useful life of the 9203 Solenoid / Alarm Driver (see Appendix 2) when operating as defined in the considered scenarios.

When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 for low demand mode applications or SIL 2 / SIL 3 at HFT=1 for high and low demand mode applications.

The two channels on the dual channel devices shall not be used in 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 regard is taken of the possibility of common failures.

[1] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2:2010.

Table 2: Summary for the 9203 Solenoid / Alarm Driver (high current type) – IEC 61508 failure rates

	exida Profile 1 [2]
Failure category	**Failure rates (in FIT)**
Safe Detected (λ_{SD})	0
Safe Undetected (λ_{SU})	214
Dangerous Detected (λ_{DD})	106
Dangerous Undetected (λ_{DU})	56
Total failure rate (safety function)	376
DC	65%

Table 3: Safety metrics according to ISO 13849-1

$MTTF_D$ (years)	706 (High)
DC_{avg}	65% (Low)
Average frequency of a dangerous failure per hour (PFH) [3]	5.60E-08 1/h
Performance Level (PL) [4]	d

[2] For details see Appendix 3.

[3] The PFH valuen is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

[4] The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the $MTTF_D$, DC_{avg} and PFH value of the device itself.

Table of Contents

Management summary 2

1 Purpose and Scope 5

2 Project management 6
- 2.1 *exida* 6
- 2.2 Roles of the parties involved 6
- 2.3 Standards / Literature used 6
- 2.4 *exida* tools used 6
- 2.5 Reference documents 7
  - 2.5.1 Documentation provided by the customer 7
  - 2.5.2 Documentation generated by *exida* 7

3 Product Description 8

4 Failure Modes, Effects, and Diagnostic Analysis 9
- 4.1 Failure categories description 9
- 4.2 Methodology – FMEDA, Failure rates 10
  - 4.2.1 FMEDA 10
  - 4.2.2 Failure rates 10
  - 4.2.3 Assumptions 11
- 4.3 FMEDA Results 11
  - 4.3.1 9203 Solenoid / Alarm Driver (high current type) 12
- 4.4 Architectural Constraints 13

5 Using the FMEDA results 14
- 5.1 Example PFD_{AVG} / PFH calculation 15

6 Terms and Definitions 16

7 Status of the document 17
- 7.1 Liability 17
- 7.2 Releases 18
- 7.3 Release Signatures 18

Appendix 1: Possibilities to reveal dangerous undetected faults during the proof test 19
- Appendix 1.1: Possible proof tests to detect dangerous undetected faults 19

Appendix 2: Impact of lifetime of critical components on the failure rate 20

Appendix 3: *exida* Environmental Profiles 21

Appendix 4: *exida* Route 2H Criteria 22

1 Purpose and Scope

This document shall describe the results of the hardware assessment carried out on the 9203 Solenoid / Alarm Driver with hardware version 9203SMD1A-2045 and 9203SMD2A-2041.

The FMEDA builds the basis for an evaluation whether a sensor / logic / final-element subsystem, including the product, meets the average Probability of Failure on Demand (PFD_{AVG}) / Probability of dangerous Failure per hour (PFH) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 or ISO 13849.

It **does not** consider any calculations necessary for proving intrinsic safety or an evaluation of the correct device behavior in general. This FMEDA **does not** replace a full assessment according to IEC 61508 or ISO 13849.

2 Project management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety, availability, and cybersecurity with over 500 person years of cumulative experience in functional safety, alarm management, and cybersecurity.

Founded by several of the world's top reliability and safety experts from manufacturers, operators and assessment organizations, *exida* is a global corporation with offices around the world. *exida* offers training, coaching, project oriented consulting services, safety engineering tools, detailed product assurance and ANSI accredited functional safety and cybersecurity certification. *exida* maintains a comprehensive failure rate and failure mode database on electronic and mechanical equipment and a comprehensive database on solutions to meet safety standards such as IEC 61508 or ISO 13849.

2.2 Roles of the parties involved

PR electronics A/S	Manufacturer of the 9203 Solenoid / Alarm Driver. PR electronics A/S performed the original FMEDA of the devices under consideration.
exida	Reviewed the original FMEDA from PR electronics A/S and transferred it to the latest SILcal X format.

PR electronics A/S contracted *exida* in September 2023 with the update of the hardware assessment of the above mentioned device.

2.3 Standards / 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
[N2]	ISO 13849-1:2023	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
[N3]	Component Reliability Database Handbook, 5th Edition, 2021 Vol. 1 – Electrical Components	*exida* LLC, Component Reliability Database Handbook, 5th Edition, 2021 Vol. 1 – Electrical Components ISBN 978-1-934977-09-5

2.4 *exida* tools used

[T1]	SILcal V6 and SILcal X	FMEDA Tools
[T2]	exSILentia V4.13.0	SIL Verification Tool

2.5 Reference documents

2.5.1 Documentation provided by the customer

[D1]	9203SMD1A_2045.xlsx	BOM and version history of 15.12.2023
[D2]	9203SMD2A_2041.xlsx	BOM and version history of 15.12.2023
[D3]	9203-1-09-PDF.pdf	Schematic of 26.04.2022
[D4]	9203 Derating Analysis.xls	Derating analysis V6R1
[D5]	9203 FMEDA high current.xls	FMEDA results file generated by customer for high current type of 15.12.2023
[D6]	9203bv003_106_uk.pdf	Safety Manual V5R0

The list above only means that the referenced documents were provided as basis for the FMEDA, but it does not mean that *exida* checked the correctness and completeness of these documents.

2.5.2 Documentation generated by *exida*

[R1]	9203 FMEDA high current_CRD_5th_Ed_FIT_values - with AD.xls of 12.02.2024	FMEDA results file based on [D5] with failure rate data used from the *exida* CRD [N3]

3 Product Description

The 9203B1A/B and 9203B2A Solenoid / Alarm Driver series (see block diagram **Figure 1**) feature an intrinsically safe output with limited current and voltage, thus making direct connection to loads in the Ex-area possible.

Typical applications are the control of alarms or solenoids / valves. The loads can be controlled when the corresponding input pins of X10 are short circuit, switched from external voltage > +12 VDC and < +31.2 VDC, or switched by an PNP from external supply, or switched to ground by NPN transistor. If the input pins are left open, the outputs are de-energized.

There are two main types of the 9203 Solenoid / Alarm Driver; the 9203B1A/B (Ex) / 9203A1A/B (Standard) low current type (single or dual channel) with 93/100/110mA outgoing current, and the 9203B2A (Ex) / 9203A2A (Standard) high current type (single channel) with 115/125/135mA outgoing current. The different currents are found on the three connector poles of each channel output connector X40/X50. The outgoing voltage is limited to 28 VDC.

From the perspective of functional safety, the high current type is the more critical device and therefore, this analysis only covers the high current type. The results from this analysis can be also applied to the low current type.

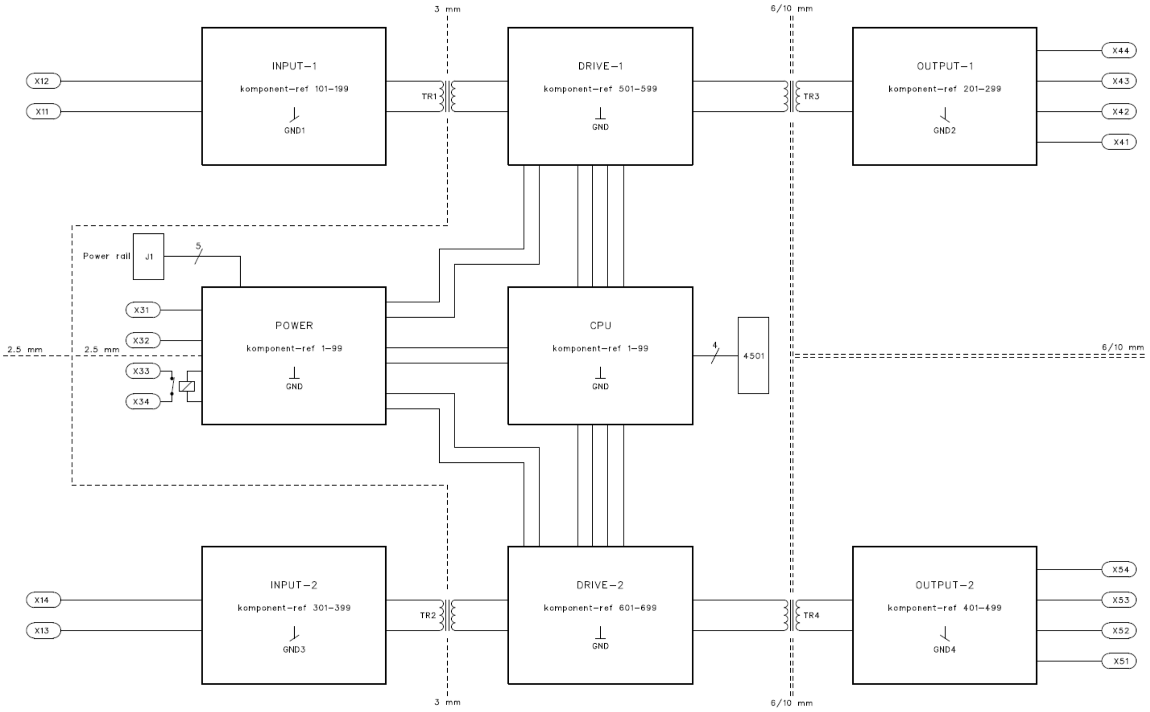

Figure 1: Block diagram of the 9203 Solenoid / Alarm Driver series

4 Failure Modes, Effects, and Diagnostic Analysis

The original Failure Modes, Effects, and Diagnostic Analysis was done by **PR electronics A/S** and is documented in [D5]. *exida* updated the failure rates from that report to the *exida* CRD (see [N3]) and created the FMEDA documented in [R1]. The analysis presented in this chapter is based on [R1].

When the effect of a certain component failure mode could not be analyzed theoretically, the failure modes were introduced on component level and the effects of these failure modes were examined on system level. This resulted in failures that can be classified according to the following failure categories.

4.1 Failure categories description

In order to judge the failure behavior of the 9203 Solenoid / Alarm Driver, 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 Safe
Failure that causes the subsystem to go to the defined fail-safe state without a demand from the process.

Fail Dangerous
A dangerous failure (D) is defined as a failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state)

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 and causes the output signal to go to the fail-safe state.

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. For the calculation of the SFF it is treated like a safe undetected failure.

Annunciation
Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit). Annunciation failures are divided into annunciation detected (AD) and annunciation undetected (AU) failures.

No Part
Component that plays no part in implementing the safety function but is part of the circuit diagram and is listed for completeness. It is also not part of the total failure rate.

In this analysis, the annunciation detected faults (AD) are added to the dangerous detected faults (DD), because they offer a sufficient diagnostic accuracy to be treated as a safety diagnostic mechanism.

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 modes and failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook [N3] for environmental profile 1 (see Appendix 3). The rates were chosen in a way that is appropriate for safety integrity level verification calculations and the intended applications. 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 or ISO 13849 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.

Early life failures (infant mortality) are not included in the failure rate prediction as it is assumed that some level of commission testing is done. End of life failures are not included in the failure rate prediction as useful life is specified.

Failures caused by external events 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 the failure rate applicability to any particular environment.

Accurate plant specific data may be used to check validity of the failure rate data. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.2.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the 9203 Solenoid / Alarm Driver.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer’s instructions.
- Failures during parameterization are not considered.
- 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.
- The Mean Time To Restoration (MTTR) after a safe failure is 24 hours.
- External power supply failure rates are not included.
- Only the described versions are used for safety applications.
- Only one input and one output are part of the considered safety function.
- The worst-case internal fault detection time is 1 minute. Therefore, a demand for the safety function in high demand mode is only possible every 6000 seconds [5], which corresponds to 100 minutes.

4.3 FMEDA Results

For the calculations the following has to be noted:

$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$

IEC 61508:

$DC = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$

ISO 13849-1:

$MTTF_D$ [years] $= 1 / ((\lambda_{DD} + \lambda_{DU}) * 24 * 365)$

$PFH = \lambda_{DU}$

$DC_{avg} = \lambda_{DD} / (\lambda_{DD} + \lambda_{DU})$

[5] See IEC 61508-2:2010, paragraph 7.4.4.1.4 and ISO 13849-1:2023, paragraph 6.1.3.2.4

4.3.1 9203 Solenoid / Alarm Driver (high current type)

The FMEDA carried out on the 9203 Solenoid / Alarm Driver in the high current product variant under the assumptions described in section 4.2.3 and the definitions given in section 4.1 and 4.2 leads to the following failure rates. These failure rates are also valid for the low current product variant, as described in the Management summary and the Product Description:

	***exida* Profile 1** [6]
Failure category	**Failure rates (in FIT)**
Safe Detected (λ_{SD})	**0**
Safe Undetected (λ_{SU})	**214**
Dangerous Detected (λ_{DD})	**106**
Dangerous Detected (λ_{dd})	54
Annunciation Detected (λ_{AD})	52
Dangerous Undetected (λ_{DU})	**56**

Annunciation Undetected (λ_{AU})	44
No effect ($\lambda_{\#}$)	174
No part (λ_{-})	156

Total failure rate (safety function)	**376**

DC	**65%**

Safety metrics according to ISO 13849-1

MTTF$_D$ (years)	**706 (High)**

DC$_{avg}$	**65% (None)**
Average frequency of a dangerous failure per hour (PFH) [7]	**5.60E-08 1/h**
Performance Level (PL) [8]	**d**

These failure rates are valid for the useful lifetime of the product (see Appendix 2).

[6] For details see Appendix 3.

[7] The PFH value is only valid if the demand rate for the Safety Function is at least 100 times lower than the worst-case internal fault detection time.

[8] The complete Safety Function according to ISO 13849-1 needs to be evaluated to determine the overall achieved Performance Level. The Performance Level listed here only considers the MTTF$_D$, DC$_{avg}$ and PFH value of the device itself.

4.4 Architectural Constraints

The architectural constraint type for the 9203 Solenoid / Alarm Driver is B. The hardware fault tolerance of the device is 0.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508-2 or the 2_H approach according to 7.4.4.3 of IEC 61508-2.

The 1_H approach involves calculating the Safe Failure Fraction (SFF) for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508-2.

This FMEDA analysis uses the 2_H approach with the 2_H qualified failure rates from the *exida* component reliability database [N3] (see also Appendix 4). To apply the 2_H approach on a Type B device, the diagnostic coverage has to be at least 60%.

The analysis shows that the 9203 Solenoid / Alarm Driver has a diagnostic coverage of 65% and therefore meets hardware architectural constraints for up to SIL 2 as a single device.

When 2_H data is used for all of the devices in an element, then the element meets the hardware architectural constraints up to SIL 2 at HFT=0 for low demand mode applications or SIL 2 / SIL 3 at HFT=1 for high and low demand mode applications.

As the 9203 Solenoid / Alarm Driver is only one part of an element, the architectural constraints should be determined for the entire sensor element.

The SIS designer is responsible for meeting other requirements of applicable standards for any given SIL.

5 Using the FMEDA results

Using the failure rate data given in section 4.3.1 and the failure rate data for the associated element devices, an average Probability of Failure on Demand (PFD_{AVG}) calculation can be performed for the entire Safety Instrumented Function (SIF).

Probability of Failure on Demand (PFD_{AVG}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

To perform an average Probability of Failure on Demand (PFD_{AVG}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{AVG} by making many assumptions about the application and operational policies of a site. Therefore, use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{AVG}) calculation is best accomplished with *exida's* exSILentia tool.

The failure rates for all the devices of the Safety Instrumented Function and the corresponding proof test coverages are required to perform the PFD_{AVG} calculation. The proof test coverage of the suggested proof test for the 9203 Solenoid / Alarm Driver is listed in Appendix 1.1. This has to be combined with the dangerous failure rates after proof test for other devices to establish the proof test coverage for the entire Safety Instrumented Function.

When performing testing at regular intervals, the 9203 Solenoid / Alarm Driver contribute less to the overall PFD_{AVG} of the safety instrumented function.
The following section gives a simplified example on how to apply the results of the FMEDA.

5.1 Example PFD_{AVG} / PFH calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1) 9203 Solenoid / Alarm Driver with *exida's* exSILentia tool. The failure rate data used in this calculation are given in section 4.3.1.

A mission time of 10 years has been assumed, a Mean Time To Restoration of 24 hours and a maintenance capability of 100%. Table 4 lists the results for different proof test intervals considering an average proof test coverage of 95% (see Appendix 1.1).

Table 4: 9203 Solenoid / Alarm Driver – PFD_{AVG} / PFH values

Device variant	PFH [1/h]	T[Proof]	
		1 year	4 years
High Current	5.60E-8	PFD_{AVG} = 4.04E-4	PFD_{AVG} = 1.08E-3

For SIL2 the overall PFD_{AVG} shall be better than 1.00E-02 and the PFH shall be better than 1.00E-06 1/h.

As the 9203 Solenoid / Alarm Driver is contributing to the entire safety function, it 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 a PFD_{AVG} value of 1.00E-03 or a PFH value of 1.00E-07 1/h, respectively.

With a proof test interval of one year, the calculated PFD_{AVG} / PFH values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1:2010 and do fulfill the assumption to not claim more than 10% of the allowed range, i.e. to be better than or equal to 1.00E-03 or 1.00E-07 1/h, respectively.

The resulting PFD(t) / PFD_{AVG} graph for the high current variant is generated with exSILentia for a proof test interval of one year and is displayed in Figure 2.

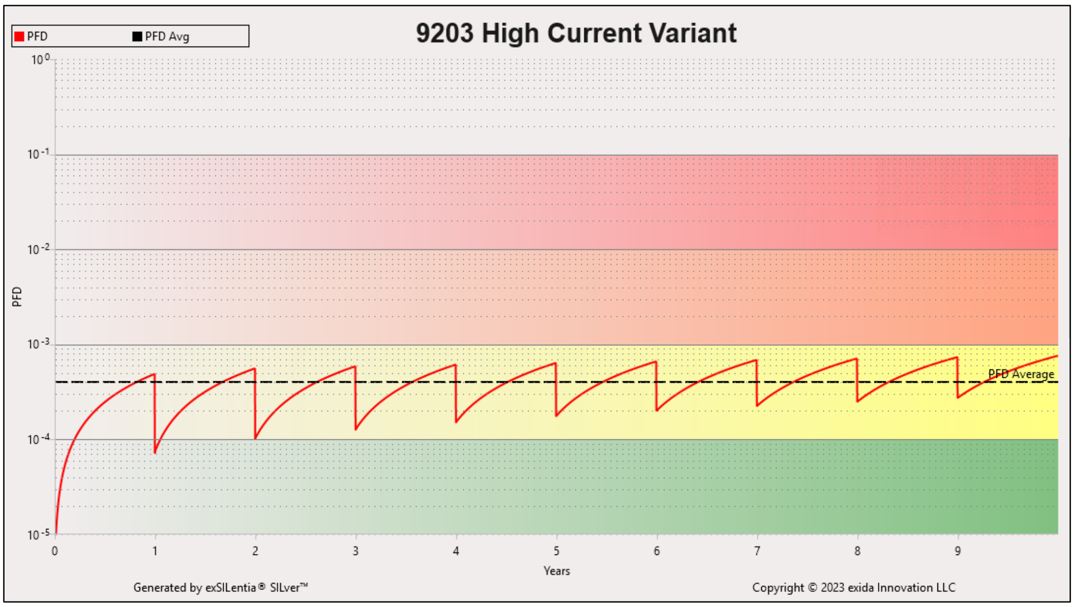

Figure 2: PFD(t) / PFDAVG for high current variant

6 Terms and Definitions

Internal Diagnostics	Tests performed internally by the device or, if specified, externally by another device without manual intervention.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
DC / DC_{avg}	Diagnostic Coverage of dangerous failures (in %)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
HFT	Hardware Fault Tolerance A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function.
High demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
$MTTF_D$	Mean Time To dangerous Failure
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
PL	Performance Level ISO 13849-1: Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level IEC 61508: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. IEC 62061: discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest.
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 B element	“Complex” element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2
T[Proof]	Proof Test Interval

7 Status of the document

7.1 Liability

exida prepares 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:	V3R3:	Corrected after review by customer; April 09, 2024
	V3R2:	Added Soft Errors to the FMEDA; February 16, 2024
	V3R1:	Included also the AD failures to calculate the DD failure rate; February 2nd, 2024
	V3R0:	Updated to IEC 61508:2010; Includes metrics according to ISO 13849-1; January 22, 2024
	V2R0:	Non-Ex versions added; July 8, 2014
	V1R2:	Purpose and Scope section modified; September 27, 2010
	V1R1:	Description of proof test modified; March 9, 2010
	V1R0:	Review comments incorporated; January 15, 2010
	V0R1:	Initial version; November 26, 2009

Authors: Stephan Aschenbrenner, Alexander Dimov, Philipp Hanzik, Armin Schulze

Review:	V3R1:	Stephan Aschenbrenner (*exida*); February 2nd, 2024
	V3R0:	Armin Schulze (*exida*); January 19, 2024
	V0R1:	Hans Jørgen Eriksen (PR electronics A/S); November 30, 2009 Rachel Amkreutz (*exida*); January 12, 2010

Release status: Released to PR electronics A/S.

7.3 Release Signatures

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

Armin Schulze

Dipl.-Ing. (Univ.) Armin Schulze, Safety Engineer

Appendix 1: 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.

Tables 5/6 show an importance analysis of the dangerous undetected faults and indicates how these faults can be detected during proof testing.

Appendix 1 shall be considered when writing the safety manual as it contains important safety related information.

Appendix 1.1: Possible proof tests to detect dangerous undetected faults

A possible proof test is described in section 10 of the safety manual [D6] for the 9203 Solenoid / Alarm Driver.

This test will detect approximately 95% of possible “DU” failures in the device.

Appendix 2: 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 determined and used to replace equipment before the end of useful life.

Although a constant failure rate is assumed by the *exida* FMEDA prediction method (see section 4.2) this only applies provided that the useful lifetime [9] of components is not exceeded. Beyond their useful lifetime, the result of the probabilistic calculation method is likely optimistic, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore, it is obvious that the probability 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.

It is the responsibility of the end user to maintain and operate the 9203 Solenoid / Alarm Driver per manufacturer’s instructions.

Note 3 in IEC 61508-2 states that experience has shown that the useful lifetime often lies within a range of 8 to 12 years. It can, however, be significantly less if elements are operated near to their specification limits.

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

[9] 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.

Appendix 3: *exida* Environmental Profiles

exida Profile	1	2	3	4	5	6
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30°C	25°C	25°C	5°C	25°C	25°C
Average Internal Temperature	60°C	30°C	45°C	5°C	45°C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5°C	25°C	25°C	0°C	25°C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5°C	40°C	40°C	2°C	40°C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[10]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[11]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[12]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[13]	G2	G3	G3	G3	G3	Compatible Material
Surge[14]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[15]						
80MHz to 1.4 GHz	10V /m	10V /m	10V /m	10V /m	10V /m	N/A
1.4 GHz to 2.0 GHz	3V/m	3V/m	3V/m	3V/m	3V/m	
2.0Ghz to 2.7 GHz	1V/m	1V/m	1V/m	1V/m	1V/m	
ESD (Air)[16]	6kV	6kV	6kV	6kV	6kV	N/A

[10] Humidity rating per IEC 60068-2-3

[11] Shock rating per IEC 60068-2-27

[12] Vibration rating per IEC 60068-2-6

[13] Chemical Corrosion rating per ISA 71.04

[14] Surge rating per IEC 61000-4-5

[15] EMI Susceptibility rating per IEC 6100-4-3

[16] ESD (Air) rating per IEC 61000-4-2

Appendix 4: *exida* Route 2H Criteria

IEC 61508:2010 2nd edition describes the Route 2_H alternative to Route 1_H architectural constraints.

The standard states:
"based on data collected in accordance with published standards (e.g., IEC 60300-3-2: or ISO 14224); and, be evaluated according to

- the amount of field feedback; and
- the exercise of **expert judgment**; and when needed
- the undertake of specific tests,

in order to estimate the average and the uncertainty level (e.g., the 90% confidence interval or the probability distribution) of each reliability parameter (e.g., failure rate) used in the calculations."

exida has interpreted this to mean not just a simple 90% confidence level in the uncertainty analysis, but a high confidence level in the entire data collection process. As IEC 61508:2010 2nd edition does not give detailed criteria for Route 2_H, *exida* has established the following:

1. field unit operational hours of 100,000,000 per each component; and
2. a device and all of its components have been installed in the field for one year or more; and
3. operational hours are counted only when the data collection process has been audited for correctness and completeness; and
4. failure definitions, especially "random" versus "systematic" are checked by *exida*; and
5. every component used in an FMEDA meets the above criteria.

This set of requirements is chosen to assure high integrity failure data suitable for safety integrity verification.