Failure Modes, Effects and Diagnostic Analysis

Project:
Loop Powered Digital Output 9176

Company:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 14/04-121
Report No.: STAHL 14/04-121 R030
Version V1, Revision R0; September 2014
Jan Hettenbach

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 of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the Digital output 9176. All covered configurations are listed in Table 1 and all related drawings are 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.

The failure rates used in this analysis are from the *exida* Electrical Component Reliability Handbook for Profile 1. The operating stress conditions [1] are typical for an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC.

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.

The Digital output 9176 can be considered to be a Type A [2] element with a hardware fault tolerance of 0. The failure rates for the covered configurations according to IEC 61508:2010 are listed in Table 2.

Table 1: Covered configurations of Digital output 9176

Types Hardware revision: C	**Configuration**	**Operating conditions**
9176/10-12-00	1 channel	10 V, 60 mA, 150 Ω
9176/20-12-00	2 channels	10 V, 60 mA, 150 Ω
9176/10-14-00	1 channel	17,5 V, 45 mA, 130 Ω
9176/20-14-00	2 channels	17,5 V, 45 mA, 130 Ω
9176/10-15-00	1 channel	25 V, 29 mA, 320 Ω
9176/20-15-00	2 channels	25 V, 29 mA, 320 Ω
9176/10-16-00	1 channel	25 V, 35 mA, 250 Ω
9176/20-16-00	2 channels	25 V, 35 mA, 250 Ω
9176/10-17-00	1 channel	25 V, 40 mA, 460 Ω
9176/20-17-00	2 channels	25 V, 40 mA, 460 Ω

[1] The results of the profile are similar to SN29500 operating conditions for 40°C. For a higher average temperature of 60°C, the failure rates must be multiplied with an experience based factor of 2.5.

[2] 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 2: Failure rates of one channel of Digital output 9176

	exida Profile 1
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**364**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Undetected (λ_{DU}) [3]	**0**

No effect	0
No part	5

Total failure rate (safety function)	**364**

Safe failure fraction (SFF) [4]	**100%**
SIL AC [5]	**SIL3**

[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] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[5] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

Table of Contents

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the Digital output 9176.

The FMEDA builds the basis for an evaluation whether a sensor subsystem, including the described Digital output 9176 meets the average Probability of Failure on Demand (PFD_{AVG}) 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

R. STAHL Schaltgeräte GmbH	Manufacturer of the Digital output 9176 and carried out the FMEDA.
exida	Reviewed the FMEDAs and issued this report.

R. STAHL Schaltgeräte GmbH contracted *exida* in March 2014 with review of the FMEDAs and the preparation of this 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]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0

2.4 Reference documents

2.4.1 Documentation provided by the customer

[D1]	91 766 03 20 0_01.pdf	Schematic diagram of 14.11.2013
[D2]	STL_91 766 03 20 0_01_V1R0.xlsx	Parts list of Digital output 9176, Rev. C
[D3]	9176611310 de en.pdf	Operating instructions Digital output 9176, Rev. C
[D4]	SafetyConcept 9176 V0R1.docx	Safety concept description of 27.02.2014
[D5]	FMEDA V7 9176 V2R2.efm	FMEDA of Digital output 9176 V2R2 of 18.02.2014

2.4.2 Documentation generated by *exida*

[R1]	FMEDA review checklist 9176.xls of 01.06.2014

2.5 *exida* tools used

[T1]	SILcal V7	FMEDA Tool

3 Product Description

The Digital output 9176 can be considered as a Type A [6] element according to IEC 61508, having a hardware fault tolerance of 0.

The Digital output 9176 is a loop powered digital output module. It has no internal power supply and can be used for solenoid valve control or signaling devices like sounder or indicator. The high input signal is the power source for the output signal. The Digital output 9176 has up to two channels. Each channel is electrically insulated from the other channel.

Input and output signals of each channel are electrically insulated and can be installed in zone 2 / Div 2. Output signals fulfill category Ex ia.

Figure 1 shows the connection diagram of the Digital output 9176.

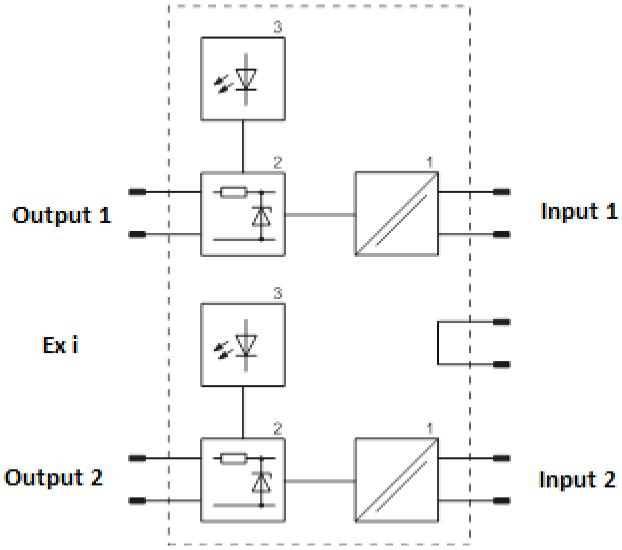

Figure 1: Connection of Digital output 9176 with two independent channels

[6] Type A element: "Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by R. STAHL Schaltgeräte GmbH and reviewed by *exida*. The results are documented in [D5].

4.1 Description of the failure categories

In order to judge the failure behavior of the Digital output 9176, 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.

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 output signals 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 outputs 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 or external diagnostics (DU).

Fail Dangerous Detected

Failure that is dangerous but is detected by internal or external diagnostics (DD).

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.

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 rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbook [N2] which was derived using over ten billion unit operational hours of field failure data from multiple sources and failure data from various databases. 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 *exida* Profile 1. 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 such as *exida* SILStat^{TM} 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 Digital output 9176.

- 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.
- 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 configurations of the Digital output 9176 are considered.
- Only one channel of the Digital output 9176 is part of the FMEDA, both channels in dual channel configuration are independent of each other.

4.3 Results of the assessment

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

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

$MTBF = MTTF + MTTR = (1 / (\lambda_{total} + \lambda_{no\ part} + \lambda_{AU})) + 24\ h$

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 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 assessment supports the 1_H approach.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$SFF = (\Sigma\lambda_S\ avg + \Sigma\lambda_{DD}\ avg) / (\Sigma\lambda_S\ avg + \Sigma\lambda_{DD}\ avg + \Sigma\lambda_{DU}\ avg\ )$

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD}) / (\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU}\ )$

Where:

$\lambda_{S\ =}$ Fail Safe

$\lambda_{DD\ =}$ Fail Dangerous Detected

$\lambda_{DU=}$ Fail Dangerous Undetected

As the Digital output 9176 is only one part of an element, the architectural constraints should be determined for the entire sensor element.

4.3.1 Results of Digital output 9176

The FMEDA carried out on the Digital output 9176 and the assumptions described in section 4.2.3 and 4.3 is leading to the following failure rates:

Table 3: Failure rates of Digital output 9176

	***exida* Profile 1**
Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**364**
Fail Dangerous Detected (λ_{DD})	**0**
Fail Dangerous Undetected (λ_{DU}) [7]	**0**

No effect	0
No part	5

Total failure rate (safety function)	**364**

Safe failure fraction (SFF) [8]	**100%**
SIL AC [9]	**SIL3**

[7] 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.

[8] The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

[9] SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. The SIL AC (architectural constraints) needs to be evaluated on subsystem level

5 Terms and Definitions

FIT	Failure In Time (1x10-9 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
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).
PLC	Programmable Logic Controller
Type A element	“Non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

6 Status of the Document

6.1 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.

6.2 Releases

Version History:	V1R0:	Editorial Changes after review; September 26, 2014
	V0R1:	Initial draft; July 21, 2014
Author:	Jan Hettenbach	
Review:	Andreas Bagusch (R. STAHL Schaltgeräte GmbH); July 28, 2014	
	Stephan Aschenbrenner (*exida*); September 25, 2014	
Release Status:	V1R0 Released to R. STAHL Schaltgeräte GmbH	

6.3 Release Signatures

Hettenbach

Dipl. -Ing. (Univ.) Jan Hettenbach

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

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 following steps, as described in Table 4. It is assumed that this test will detect 99% of possible dangerous failures.

Table 4: Steps for proof test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip.
2.	Apply an input signal with a defined amplitude at the Digital output 9176.
3.	Check, if the output current of the Digital output 9176 is within the specification.
4.	Remove the bypass from the monitoring system or 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[10] 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 Digital output 9176 has no components with reduced life time which are contributing to the dangerous undetected failure rate.

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

[10] 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 C: *exida* Environmental Profiles

Table 5 *exida* Environmental Profiles

***exida* Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted	General Field Mounted	Subsea	Offshore	N/A
		no self-heating	self-heating			
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3	C3	N/A	C3	N/A
		also applicable for D1	also applicable for D1		also applicable for D1	
Average Ambient Temperature	30C	25C	25C	5C	25C	25C
Average Internal Temperature	60C	30C	45C	5C	45C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5C	25C	25C	0C	25C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5C	40C	40C	2C	40C	N/A
Exposed to Elements/Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[11]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[12]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[13]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[14]	G2	G3	G3	G3	G3	Compatible Material
Surge[15]						
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[16]						
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)[17]	6kV	6kV	6kV	6kV	6kV	N/A

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

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

[13] Vibration rating per IEC 60770-1

[14] Chemical Corrosion rating per ISA 71.04

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

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

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