Failure Modes, Effects and Diagnostic Analysis

Project:
Digital Output Module Valve DOMV 9478/22-08-51

Company:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 11/01-104
Report No.: STAHL 11/01-104 R021
Version V1, Revision R1; March 2011
Stephan Aschenbrenner

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 Digital Output Module Valve DOMV 9478/22-08-51 in the version 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 variant was 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 and from *exida's* experienced-based data compilation for the different mechanical components as used in the FMEDAs carried out in 2004 and 2008.

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 40ºC. 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 Digital Output Module Valve DOMV 9478/22-08-51, 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 Digital Output Module Valve DOMV 9478/22-08-51 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 4.3.1 along with all assumptions.

The Digital Output Module Valve DOMV 9478/22-08-51 is classified as a Type A[1] element according to IEC 61508, having a hardware fault tolerance of 0. The failure rates according to IEC 61508:2010 for the Digital Output Module Valve DOMV 9478/22-08-51 are listed in the following table.

The failure rates according to IEC 61508:2000 are listed in Appendix C.

[1] 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: Digital Output Module Valve DOMV 9478/22-08-51 according to IEC 61508:2010

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**146**
Fail Dangerous Detected (λ_{DD})	**30**
Fail Dangerous Undetected (λ_{DU})	**176**

Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	54
No effect	443
No part	133

Total failure rate (safety function)	**352**
SFF [2]	**---**

SIL AC [3]	**---**

[2] The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction.

[3] The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

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 and Literature used 6
2.4 Reference documents 7
2.4.1 Documentation provided 7
2.4.2 Documentation generated by *exida* 7
3 Product Description 8
4 Failure Modes, Effects, and Diagnostic Analysis 10
4.1 Description of the failure categories 10
4.2 Methodology – FMEDA, Failure Rates 11
4.2.1 FMEDA 11
4.2.2 Failure Rates 11
4.2.3 Assumptions 12
4.3 Results 12
4.3.1 Digital Output Module Valve DOMV 9478/22-08-51 13
5 Using the FMEDA Results 14
5.1 Air quality failures 14
5.2 Air supply failures 14
5.3 Example PFD_{AVG} calculation 14
6 Terms and Definitions 16
7 Status of the Document 17
7.1 Liability 17
7.2 Releases 17
7.3 Release Signatures 17
Appendix A: Possibilities to reveal dangerous undetected faults during the proof test .. 17
Appendix A.1: Possible proof tests to detect dangerous undetected faults 18
Appendix B: Impact of lifetime of critical components on the failure rate 19
Appendix C: Failure rates according to IEC 61508-2:2000 20

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* according to the relevant functional safety standard(s) like IEC 61508 or ISO 13849-1. 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}). When appropriate, fault injection testing will be used to confirm the effectiveness of any self-diagnostics.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. This option does not include an assessment of the development process.

Option 2: Hardware assessment with proven-in-use consideration per IEC 61508 / IEC 61511

Option 2 extends Option 1 with an assessment of the proven-in-use documentation of the device including the modification process.

This option for pre-existing programmable electronic devices provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511. When combined with plant specific proven-in-use records, it may help with prior-use justification per 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* according to the relevant application standard(s) like IEC 61511 or EN 298 and the necessary functional safety standard(s) like IEC 61508 or ISO 13849-1. The full assessment extends Option 1 by an assessment of all fault avoidance and fault control measures during hardware and software development.

This option provides the safety instrumentation engineer with the required failure data as per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

This assessment shall be done according to option 1.

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 Module Valve DOMV 9478/22-08-51. From this, failure rates, Safe Failure Fraction (SFF) and example PFD_{AVG} values are calculated.

The information in this report can be used to evaluate whether a final element subsystem, including the Digital Output Module Valve DOMV 9478/22-08-51 meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508. 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 partnership 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 Module Valve DOMV 9478/22-08-51.
exida	Carried out the FMEDAs and issued this report according to Option 1 (see Section 1).

R. STAHL Schaltgeräte GmbH contracted *exida* in January 2011 to carry out the FMEDA and to issue the report.

2.3 Standards and Literature used

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

[N1]	IEC 61508-2:2000	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems; 1st edition
[N2]	IEC 61508-2:2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems; 2nd edition
[N3]	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
[N4]	ISBN: 0471133019 John Wiley & Sons	Electronic Components: Selection and Application Guidelines by Victor Meeldijk
[N5]	FMD-91, RAC 1991	Failure Mode / Mechanism Distributions
[N6]	FMD-97, RAC 1997	Failure Mode / Mechanism Distributions

[N7]	NPRD-95, RAC	Non-electronic Parts – Reliability Data 1995
[N8]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition

2.4 Reference documents

2.4.1 Documentation provided

[D1]	9478_22_DigitalOutputModuleVentil_AK00_III_en.pdf	Datasheet "Digital Output Module Valve - Series 9478; 2011-01-31 AK00 III en
[D2]	94 756 02 20 0 Index 02	Circuit diagram “Digital Output Module Typ 9475”
[D3]	DS6524-Standard-EU-EN.pdf	Data sheet 6524-*-***
[D4]	DS6144-standard-EU-EN.pdf	Data sheet 6144-*-***
[D5]	6524BG01_00077728.pdf	Diagram 6524 BG01 Version D02 of 23.03.06
[D6]	6524BG03_00077730.pdf	Diagram “3/2-Wege-Ventil WWC – INT“ 6524 BG03 Version B01 of 22.06.06
[D7]	Stückliste 6524.pdf	Parts list 6524 material no. 144 933
[D8]	Vergleich 6144 6104 2_2008-04-07.doc	Comparison between type 6104-*-*** and type 6144-*-***
[D9]	9000089865_6144BG01.pdf	Mechanical drawing “Lamellenventil” 9000089865 version F of 13.08.07
[D10]	9000089216_6144_Flipper_Lamelle.pdf	Mechanical drawing “Lamelle kpl.” 9000089216 version O of 24.04.08
[D11]	Verwendung der FMEDA Angaben.pdf of 16.02.11	

2.4.2 Documentation generated by *exida*

[R1]	FMEDA DOM 9475 2Abschaltweg.xls of 06.05.04
[R2]	FMEDA V6 6524 NC with 6144 V1R0.xls of 28.09.08
[R3]	Summary_9478.xlsx of 09.03.11

3 Product Description

The Digital Output Module Valve DOMV 9478/22-08-51 is classified as a Type A element according to IEC 61508, having a hardware fault tolerance of 0.

It is used to control up to 8 pneumatic valves. The System OFF signal is provided by an external safety PLC (see Figure 2) which de-activates all outputs.

The safety function is only provided by the System OFF Ex i input. This report does not cover the use of the data communication (e.g. PROFIBUS) for the safety function.

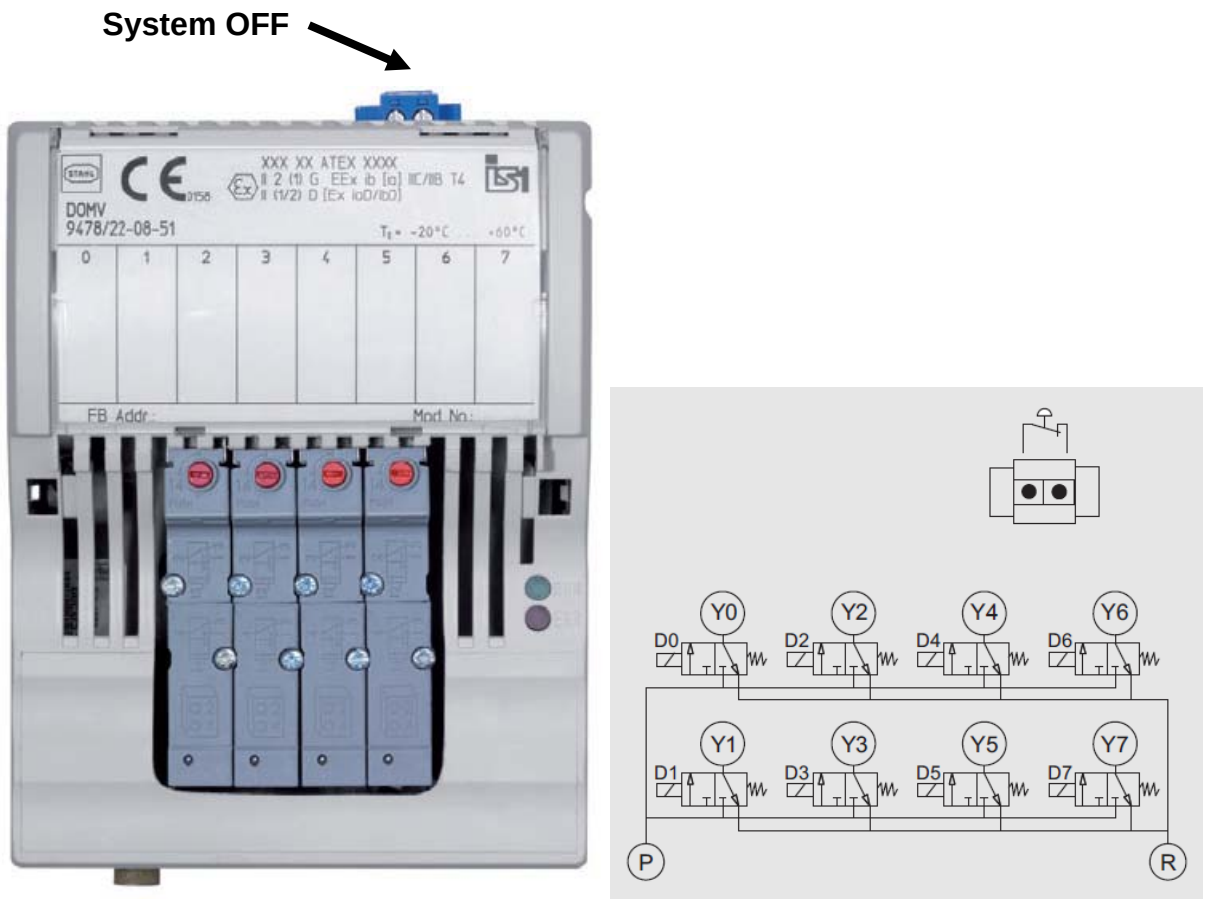

Figure 1: DOMV 9478/22-08-51

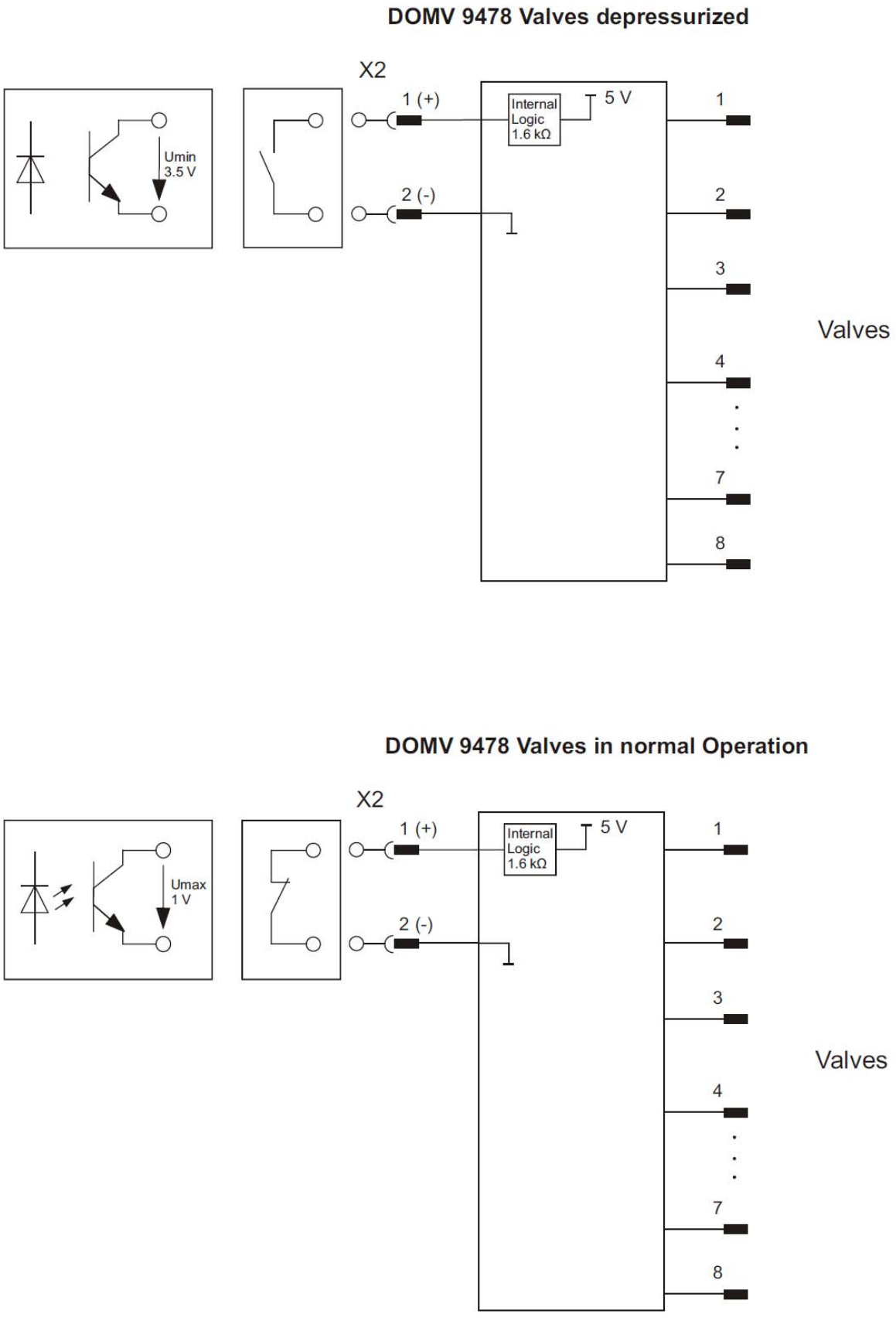

Figure 2: Connection between safety PLC and DOMV 9478/22-08-51

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed by *exida*. The results are documented in [R1] to [R2].

4.1 Description of the failure categories

In order to judge the failure behavior of the Digital Output Module Valve DOMV 9478/22-08-51, the following definitions for the failure of the device were considered.

Fail-Safe State	The fail-safe state is defined as the output being closed without electrically operated.
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.
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 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 and from *exida's* experienced-based data compilation for the different mechanical components. 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 Digital Output Module Valve DOMV 9478/22-08-51.

- 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.
- All devices are operated in the low demand mode of operation.
- Only one output is part of the considered safety function.
- Materials are compatible with process conditions and process fluids.
- Air is permanently supplied (either directly or by an air accumulator).
- 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 variant is considered.
- Breakage or plugging of air inlet and outlet lines has not been included in the analysis.
- The stress levels are average for an industrial outdoor environment and can be compared to IEC 60654-1, Class Dx (outdoor location) with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within the manufacturer's ratings.
- Manual override must not be used for safety applications.
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for Instrument Air.
- The device has a minimum distance of 5 mm from other ferromagnetic materials in order to avoid malfunctioning during operating conditions.

4.3 Results

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

λ_{total} consists of the sum of all component failure rates. This means:

$\lambda_{total} = \lambda_S + \lambda_{no\ effect} + \lambda_{DD} + \lambda_{DU}$

$SFF = 1 - \lambda_{DU} / \lambda_{total}$ (according to IEC 61508-2:2000)

$SFF = 1 - \lambda_{DU} / (\lambda_{total} - \lambda_{no\ effect})$ (according to IEC 61508-2:2010)

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

4.3.1 Digital Output Module Valve DOMV 9478/22-08-51

The FMEDA carried out on the Digital Output Module Valve DOMV 9478/22-08-51 leads under the assumptions described in section 4.2.3 and 4.3 to the following failure rates:

Table 2: Digital Output Module Valve DOMV 9478/22-08-51 according to IEC 61508:2010

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**146**
Fail Dangerous Detected (λ_{DD})	**30**
Fail Dangerous Undetected (λ_{DU})	**176**

Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	54
No effect	443
No part	133

Total failure rate (safety function)	**352**
SFF [4]	**---**

SIL AC [5]	**---**

[4] The complete final element subsystem will need to be evaluated to determine the overall Safe Failure Fraction.

[5] The SIL AC (architectural constraints) needs to be evaluated on subsystem level. See also previous footnote.

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 Air quality failures

The product failure rates that are displayed in this section are failure rates that reflect the situation where the device is used with clean filtered air. Additionally, contamination from poor control air quality may affect the function or air flow in the device. For applications where these assumptions do not apply, the user must estimate the failure rates due to contaminated air and add this failure rate to the product failure rates.

5.2 Air supply failures

Failure of the air supply shall be included in the average Probability of Failure on Demand (PFD_{AVG}) of the Safety Instrumented Function. If an accumulator system is used to protect against air supply failure, the accumulator subsystem needs to be reviewed and the dangerous failure rates of the accumulator subsystem shall be added to the actuator failure rates.

5.3 Example PFD_{AVG} calculation

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed for a single (1oo1D) Digital Output Module Valve DOMV 9478/22-08-51 considering a proof test coverage of 90% (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 3.

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

Table 3: PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 5 years
PFD_{AVG} = 1.47E-03	PFD_{AVG} = 2.16E-03	PFD_{AVG} = 4.24E-03

For the Digital Output Module Valve DOMV 9478/22-08-51 this means that for a SIL2 application, the PFD_{AVG} for a 1-year Proof Test Interval is approximately equal to 15% of the range.

Figure 3 shows the time dependent curve of PFD_{AVG}.

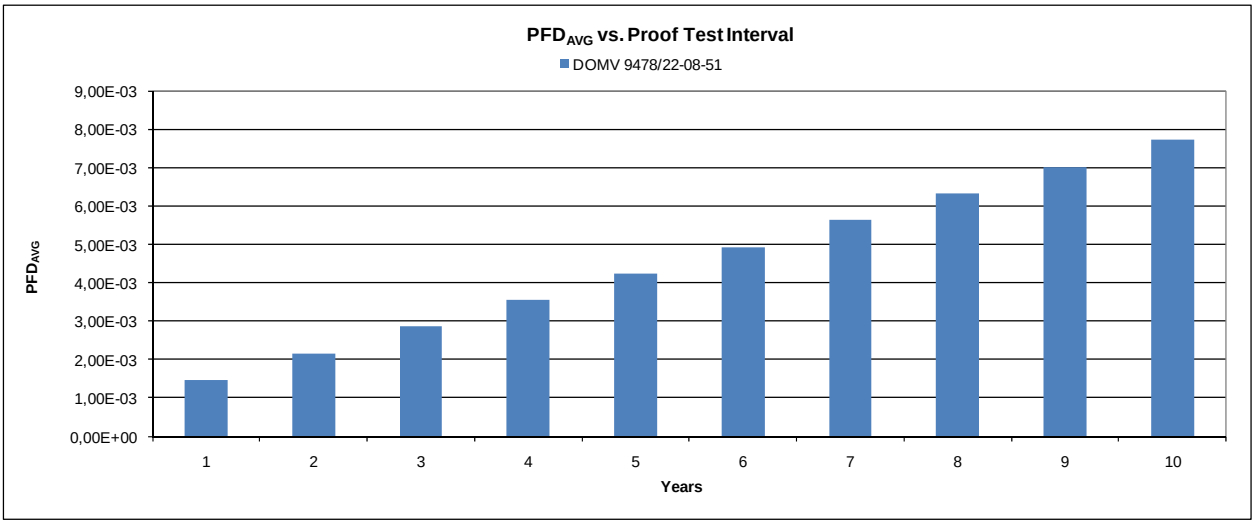

Figure 3: $PFD_{AVG}(t)$

6 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 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).
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:	V1R1:	Editorial changes; March 25, 2011
	V1R0:	Review comments incorporated; March 24, 2011
	V0R1:	Initial draft; March 11, 2011
Author:	Stephan Aschenbrenner	
Review:	V1R0:	Andre Fritsch (R. STAHL); March 25, 2011
	V0R1:	Andreas Bagusch (R. STAHL); March 15, 2011
		Rachel Amkreutz (*exida*); March 23 2011
Release Status:	Released to R. STAHL Schaltgeräte GmbH	

7.3 Release Signatures

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

Rachel Amkreutz, 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 a full stroke of the solenoid valve, as described in Table 4. It is assumed that this test will detect 90% 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.	Force the Digital Output Module Valve DOMV 9478/22-08-51 to go to the safe state and verify that the safe state is reached.
3.	Inspect the device for any visible damage or contamination.
4.	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[6] 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.

Based on general field failure data it is well known that all solenoids have a useful life period between 3 and 10 years. It is the responsibility of the end user to establish a preventative maintenance process to replace all solenoids before the end of the useful life.

Major factors influencing useful life are the air quality, ambient temperature and the air circulation around the solenoid.

If the solenoid valves are used with clean air in an ambient with air circulation (draft air) and an ambient temperature average of 40ºC, then a lifetime of 10 years is expected.

It is the responsibility of the end user to maintain and operate the valves per manufacturer's instructions. Furthermore, regular inspection should show that all components are clean and free from damage.

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

[6] 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: Failure rates according to IEC 61508-2:2000

Table 5: Digital Output Module Valve DOMV 9478/22-08-51

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	**0**
Fail Safe Undetected (λ_{SU})	**589**
Fail Safe Undetected (λ_{SU})	146
No effect	443
Fail Dangerous Detected (λ_{DD})	**30**
Fail Dangerous Undetected (λ_{DU})	**176**

Fail Annunciation Detected (λ_{AD})	0
Fail Annunciation Undetected (λ_{AU})	54
No part	133

Total failure rate (safety function)	**795**
SFF [7]	**77%**

SIL AC [8]	**2**

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

[8]. 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