Failure Modes, Effects and Diagnostic Analysis

Project:
Relay Module Ex i/ Ex e Type 9177/12-11-01

Customer:
R. STAHL Schaltgeräte GmbH
Waldenburg
Germany

Contract No.: STAHL 21/09-070
Report No.: STAHL 21/09-070 R037
Version V1, Revision R0; September 2023

Jan Hettenbach

Management summary

This report summarizes the results of the hardware safety assessment carried out on the Relay Module Ex i/ Ex e Type 9177/12-11-01 to be used for galvanically separated switching.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). An FMEDA is one of the steps taken to achieve functional safety assessment of a device or subsystem per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) and other safety metrics are calculated for the device or subsystem. For full assessment purposes all requirements of the applicable standards must be considered.

The Relay Module can switch signals as well as loads.

Table 1: Overall results for the Relay Module Ex i/ Ex e

	SN29500, 60°C	
Failure category	**control signal switching [1]**	**power switching [2]**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**129**	**157**
Fail Dangerous Detected (λ_{DD})	**0**	**0**
Fail Dangerous Undetected (λ_{DU})	**1**	**37**
No effect	253	269
No part	0	0
Total failure rate (safety function)	**130**	**194**
Safe Failure Fraction (SFF) [3]	**99%**	**81%**
SIL AC [4]	**SIL3**	**SIL2**
Results according to ISO 13849-1		
$MTBF_d$ (a)	**>100**	**>100**

[1]. Results valid for signal switching of relay (resistive load and <50mA and <32V), which are within stress region II according to SN29500-7:2005, Table 2a (<0.1A and 1V min. voltage).

[2]. Results valid for power load switching (stress region IV according to SN29500-7:2005, Table 2a). The used relay is in stress region IV when operating outside the range of signal switching.

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

[4] 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 Relay Module Ex i/ Ex e Type 9177/12-11-01.

The FMEDA builds the basis for an evaluation whether the Relay Module Ex i/ Ex e meets the Probability of dangerous Failure per Hour (PFH) requirements per IEC 61508. This FMEDA **does not** replace a full assessment according to 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 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.

2.2 Roles of the parties involved

R. STAHL Schaltgeräte GmbH	Manufacturer of the Relay Module Ex i/ Ex e. Performed the hardware assessment (FMEDA).
exida	Reviewed the FMEDA

R. STAHL Schaltgeräte GmbH contracted *exida* in January 2022 with the review of the FMEDA 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]	Electrical & Mechanical Component Reliability Handbook, 4th Edition, 2017	*exida* L.L.C, Electrical & Mechanical Component Reliability Handbook, Fourth Edition, 2017
[N3]	SN 29500-1:01.2004 SN 29500-1 H1:11.2016 SN 29500-2:09.2010 SN 29500-3:06.2009 SN 29500-4:03.2004 SN 29500-5:06.2004 SN 29500-7:11.2005 SN 29500-9:11.2005 SN 29500-10:12.2005 SN 29500-11:04.2015 SN 29500-12:02.2008 SN 29500-15:11.2016 SN 29500-16:08.2010	Siemens standard with failure rates for components
[N4]	ISO 13849-1:2015	Safety of machinery — Safety-related parts of control systems

2.4 Tools used

[T1]	SILcal V9.00.093 Build 4316	*exida* FMEDA Tool

2.5 Reference documents

2.5.1 Documentation provided by R. STAHL Schaltgeräte GmbH

[D1]	9177 0 000 005 0_00.pdf	Electrical circuit of the Relay Module Ex i/ Ex e, Version 0 of 14.10.2019
[D2]	9177 0 000 050_00.pdf	Description of the Relay Module Ex i/ Ex e of 28.02.2023
[D3]	9177_FMEDA_V1R0.efmx	FMEDA created by R. STAHL Schaltgeräte GmbH for the Relay Module Ex i/ Ex e (load and signal switching version), reviewed by *exida*

The FMEDA files were reviewed under considering the other provided documents, but it does not mean that *exida* checked the correctness and completeness of all documents.

2.5.2 Documentation generated by *exida*

[R1]	Relay Module Ex i/ Ex e FMEDA review checklist

3 Product Description

3.1 General

The safety function of the Relay Module Ex i/ Ex e is for the output to follow 1:1 the binary input signal. When, for example, a 0-Signal (Off-Signal) is on Input / coil-circuit applied, the Output / contactor-circuit shows also 0-Signal. The output is, in this example, so in the state “not conducting“, "high impedance" or rather "opened".

The safe state of the relay output is "opened" / "0-Signal".

The relay module can be used for galvanic isolated switching of electrical circuits with up to 253V AC or 125V DC and/ or a maximum current up to 2A. See operating instructions for details about pairs of switching voltage, switching current and switching power.
The relay module can also be used for control signal switching with up to 32V and 50mA resistive loads. If inductive and capacitive loads are to be switched, then the relay module must be protected against large switching power, e.g. by means of a free-wheeling circuit or an inrush current limiter.

The coil-circuit is to be connected to a direct voltage source with nominal 24 V DC.
The Relay Module Ex i/ Ex e can be considered as Type A element with HFT = 0.

Figure 1: Relay Module Ex i/ Ex e Type 9177/12-11-01

The relay module is a single-channel device, which means it has one coil-circuit and one contactor-circuit. The device has no adjustment elements.

The following failure categories are defined:

- Safe fault: Relay output "opened" / "0-Signal", while input signal is "HIGH" / "1-Signal"
- Dangerous fault: Relay output "closed" / "1-Signal", while input signal is "LOW" / "0-Signal"
- No effect: fault having no effect on the safety function.

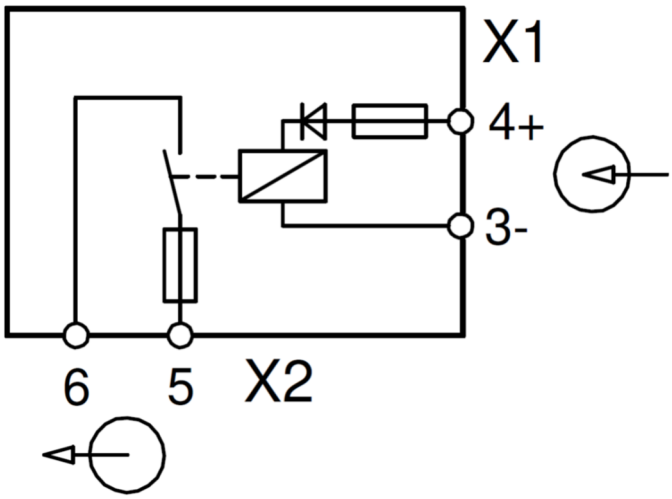


Figure 2: Principle circuit diagram of Relay Module Ex i/ Ex e

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was done by R. STAHL Schaltgeräte GmbH and is documented in [D3]. The FMEDA was reviewed by *exida*. This resulted in failures that can be classified according to the failure categories listed in Chapter 4.1.

4.1 Description of the failure categories

In order to judge the failure behavior of the Relay Module Ex i/ Ex e Type 9177/12-11-01, the following definitions for the failure of the product were considered.

Fail-Safe State	The fail-safe state is defined as relay output is open.
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.
Safe Undetected	Failure that is safe and that is not being diagnosed by internal or external diagnostics (SU).
Safe Detected	Failure that is safe but is detected by internal diagnostics (SD).
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.
Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by internal or external diagnostics (DU).
Dangerous Detected	Failure that is dangerous but is detected by internal 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 in consideration.

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

4.2.2 Failure rates

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N2]) which was derived from multiple sources and failure data from various databases. The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N3]). 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.

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.

The assumption is also made that the equipment is maintained per the requirements of IEC61508 or IEC61511 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. 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.

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™ 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 Relay Module Ex i/ Ex e.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- 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 FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- The device is locked against unintended operation/modification.
- In low demand mode of operation, the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for the safety function.
- In high demand mode, the maximum useful lifetime and additional limitations during operation of the relay shall be considered according to user manual.
- The device is powered by the input signal (loop-powered).
- The Mean Time To Restoration (MTTR) is considered to be 24 hours.
- The Relay Module Ex i/ Ex e is installed and used according to manufacturer's instructions.
- The listed failure rates are valid for operating stress conditions typical of an industrial field environment with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 60°C. For higher average temperatures, the failure rates should be multiplied with an experience-based factor according to SN29500-7 Table 5.
- Only the described variant is used for safety applications.
- Switching voltage, switching current and switching power at the relay output are within the manufacturer´s instructions.
- The binary input signal range is above 18V DC (for HIGH signal) and lower than 3V DC (for LOW signal). The voltage range in between is only valid during switching transition and no valid range for static signals.
- The frequency of operation is limited to 6 switching cycles per minute to avoid overload of the relay contacts.

4.3 Results

The FMEDA carried out on the Relay Module Ex i/ Ex e leads under the assumptions described in section 4.2.3 and the definitions given in section 4.1 to the following failure rates according to IEC 61508.

Table 2: Overall results for the Relay Module Ex i/ Ex e

	SN29500, 60°C	
Failure category	**control signal switching [5]**	**power switching [6]**
Fail Safe Detected (λ_{SD})	**0**	**0**
Fail Safe Undetected (λ_{SU})	**129**	**157**
Fail Dangerous Detected (λ_{DD})	**0**	**0**
Fail Dangerous Undetected (λ_{DU})	**1**	**37**
No effect	253	269
No part	0	0
Total failure rate (safety function)	**130**	**194**
Safe Failure Fraction (SFF) [7]	**99%**	**81%**
SIL AC [8]	**SIL3**	**SIL2**
Results according to ISO 13849-1		
$MTBF_d$ (a)	**>100**	**>100**

[5]. Results valid for signal switching of relay (resistive load and <50mA and <32V), which are within stress region II according to SN29500-7:2005, Table 2a (<0.1A and 1V min. voltage).

[6]. Results valid for power load switching (stress region IV according to SN29500-7:2005, Table 2a). The used relay is in stress region IV when operating outside the range of signal switching.

[7] The complete sensor 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.

5 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
DC	Diagnostic Coverage of dangerous failures (DC = λ_{DD} / (λ_{DD} + λ_{DU}))
EUC	Equipment Under Control
FIT	Failure In Time (1x10^{-9} failures per hour)
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
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.
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.
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.
MTTR	Mean Time To Restoration
$MTBF_d$	Mean Time Between dangerous Failures
PFH	Probability of dangerous Failure per Hour (average frequency of a dangerous failure per hour)
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.
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 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.

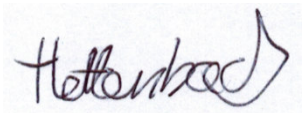
Due to future potential changes in the standards, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical product at some future time. As a leader in the functional safety market 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.

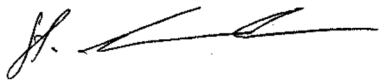
Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years and the exact results are critical to the SIL verification you may wish to contact the product vendor to verify the current validity of the results.

6.2 Releases

Version History:	V1R0	Editorial Changes; September 8, 2023
	V0R3	Editorial changes, update of results tables; August 30, 2023
	V0R2	Update after review, June 28, 2023
	V0R1	Initial draft; April 20, 2023
Authors:		Jan Hettenbach, Oleksandr Sakada
Review:	V0R3	Joachim Greiner, R. STAHL Schaltgeräte GmbH
		Stephan Aschenbrenner (*exida*)
Release status:		Released to R. STAHL Schaltgeräte GmbH

6.3 Release Signatures





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

Appendix 1: Lifetime of Critical Components

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[9] 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.

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.

Table 3 shows which components with reduced useful lifetime are contributing to the dangerous undetected failure rate and what their estimated useful lifetime is.

Table 3: Useful lifetime of components with reduced useful lifetime contributing to λ_{DU}

Type	Useful life
Relay	10^5 electrical operations at rated resistive load can be assumed

Assuming one demand per year for low demand mode applications and additional switching cycles during installation and proof testing, the relay do not have a real impact on the useful lifetime.

For high demand mode applications, the relay can be a limiting factor and must be considered in the useful lifetime assumption.

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 site experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant 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.