Series 9172

Relay module

STAHL

Safety manual

Content

1 General information

1.1 Manufacturer

R. STAHL Schaltgeräte GmbH
Am Bahnhof 30
D-74638 Waldenburg

Phone: +49 7942 943-0
Fax: +49 7942 943-4333
Internet: r-stahl.com

1.2 Information regarding the Safety Manual

ID-No.: 9172617310
Publication code: S-SM-9172-01-en-06/2019

Additionally to the Safety Manual the following documents must be observed:
X Operating Instructions for Relay module 9172 (160372 / 9172601310)
X Exida FMEDA Report No.: STAHL 13/11-017 R031

We reserve the right to make technical changes without notice.

1.3 Area of application

This Safety Manual applies to the Relay Module ISpac, types:
9172/*0-11-00. Hardware revision B
9172/*1-11-00. Hardware revision C
9172/*2-11-00. Hardware revision B
9172/*1-11-50. Hardware revision A

Software version: not applicable, device does not include software

The ISpac relay modules series 9172 are used for isolation of two different circuits. The input circuit controls the switching of a relay. Depending on the version either the control circuits or the signal circuits or both circuits are intrinsically safe.
The versions 9172/*1-11-50 feature input and output circuits without explosion protection. The devices could be used for binary output or binary input applications.

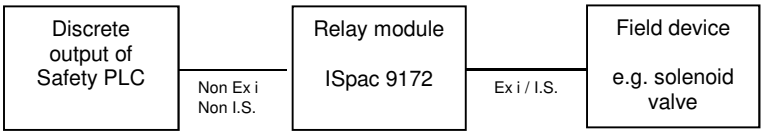
The modules are controlled by safety PLC. The ON-signal and OFF-signal must be within defined ranges. (Please refer to the technical data). The modules are loop-powered and do not offer a line fault detection.

The safety function of the ISpac 9172 modules can be used for example in safety process shut down applications in e.g. oil, gas or chemical industries. The modules are suitable for low demand mode of operation.

1.4 Safety function

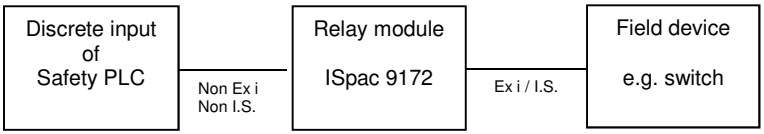
Binary/discrete output application:

Converts a discrete signal of a safety PLC into an intrinsically safe discrete signal in order to switch a field device.

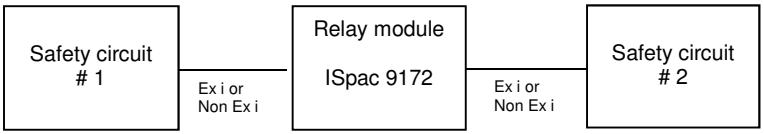


Safe state ISpac 9172: The fail-safe state is defined as the output being de-energized

Binary/discrete input application:
Converts a discrete signal of field device into a non-intrinsically safe discrete signal in order to switch the discrete input of a safety PLC.



Coupling of two circuits:
The discrete signal of circuit #1 controls the contacts of the relay module which are included in circuit #2.



1.5 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 not greater than twice the proof test frequency.
PFD	Probability of Failure on Demand
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 Solver
T[proof]	Proof Test Interval
Type A element	”non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

2 General safety information

2.1 Safety Instructions for Assembly and Operating Personnel

The Safety Manual contains basic safety instructions which are to be observed during installation, operation, parameterization and maintenance. Non-observance can lead to persons, plant and the environment being endangered.

Warning
Risk due to unauthorized work being performed on the device! • There is a risk of injury and damage to equipment. • Mounting, installation, commissioning and servicing work must only be performed by personnel who is both authorized and suitably trained for this purpose.

When installing the device:

- Observe the national installation and assembly regulations (e.g. EN 60079-14)
- Observe the operating instructions for the ISpac 9172 Relay module (see 1.2)

Before Commissioning:

- Ensure, that the set-up has been made in accordance to the safety manual (see chapter 3.1).
- Ensure proper set-up of the device by a functional test of the device before you start to operate it in the safety circuit.

When operating the device:

- Ensure, that the mean time to restoration (MTTR) after a safe failure is < 24 hours.
- Connect the input of the module to a SIL 2 compliant output board of a safety PLC.
- Ensure that only authorized personal has access to the set-up of the device.

If you have questions:

- Contact the manufacturer.

3 Characteristics for the Functional Safety

Confirmation of meeting the requirements of IEC 61508 is done by an FMEDA report of EXIDA (Report No.: STAHL 13/11-017 R031, download available at r-stahl.com). The failure rate of the module is calculated by FMEDA. The failure rates of the components are taken from Exida Electrical and Mechanical Component Reliability Handbook profile 1 at a mean temperature of 40 °C and a MTTR of 24 hours.

3.1 Functional Safety Data

For the calculation of the Safe Failure Fraction (SFF) the following has to be noted:
$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$
$SFF = 1 - \lambda_{DU} / \lambda_{total}$

The Relay Module ISpac 9172 is considered to be a Type A subsystem with a hardware fault tolerance of 0. For Type A subsystems with a hardware fault tolerance of 0 the SFF shall be > 60% for SIL 2 subsystems according to IEC 61508-2, table 2.
The PFD_{AVG} value needs to be < 1.00E-02.

T_{PROOF} = 1 year	T_{PROOF} = 2 years	T_{PROOF} = 5 years
PFD_{AVG} = 1.17E-04	PFD_{AVG} = 2.23E-04	PFD_{AVG} = 5.42E-04

Failure rates of Relay module series 9172

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	41
Fail Dangerous Detected (λ_{DD})	0
Fail Dangerous Undetected (λ_{DU})	25
Fail Annunciaion Undetected (λ_{AU})	0
No part	2
No effect	20
Total failure rate (safety function)	66
SFF	62 %
SIL AC	SIL 2

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire Safety Instrumented Function (SIF).

Fail-safe state: The fail-safe-state is defined as the output being de-energized.

Useful Lifetime	10 years or 100.000 switching cycles
Hardware structure	1001
MTTR	24 hours
Ambient temperature	-20 °C ... +70 °C (For a temperature of more than 40°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.
Storage temperature	-40 °C ... + 80 °C
Transport temperature	-40 °C ... + 80 °C

3.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis:

- 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 analysed.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- For safety applications only the described configurations of the Relay Modules 9172 are considered.
- For safety applications only the described variants are considered.
- Only one channel of the Relay Module 9172 is part of the FMEDA, both channels in dual channel configuration are independent of each other.
- It is assumed that the relay output is protected against current overload by using a fuse or other limiting devices.

4 Installation

Warning
Danger due to improper Installation • Install the device according to the national installation and assembly regulations (e.g. EN 60079-14) • Observe the operating instructions of the Relay Module ISpac 9172 according to the installation (read the cabinet installation guideline).

5 Parametrization

The module does not need to be parametrized.

6 Indications

The following LEDs are indicating the status of the device:

LED marking	Colour	Status	Meaning	Action required	Type of action
OUT	Amber	ON	Output in status "ON" (energized)	No	None, as long as this is expected behaviour.
		OFF	Output in status "OFF" (de-energized)	No	None, as long as this is expected behaviour.

The indication LEDs are not considered in FMEDA reports.

7 Proof Test

It is under the responsibility of the operator to define the type of proof test and the interval time period. The execution of the proof tests, test conditions and results of the testing has to be recorded.

It shall be tested, if:

- the functionality and safety shut down of the loop is working (during the test the safe interaction of all components of the safety system shall be tested. If it's not possible to drive the process up till the safety system intervenes, because of process-related reasons, the system has to be forced to intervention by suitable simulation).
- the LEDs are working and no faulty conditions are displayed.

Possible Proof Test to test the functionality and safety shut down of the loop

- Bypass the safety PLC or take another appropriate action to avoid a false trip.
- Force the Relay Module 9172 to switch to the safe state and verify that the safe state is reached.
    - If the input is energized: LED "OUT" is on, the relay contacts are in the energized state.

      Types 9172/.0 and 9172/.2:
      Contact between terminal 1 and 2: Closed
      Contact between terminal 2 and 3: Open
      Contact between terminal 4 and 6: Open
      Contact between terminal 5 and 6: Closed

      Types 9172/.1:
      Contact between terminal 10 and 11: Closed
      Contact between terminal 11 and 12: Open
      Contact between terminal 13 and 15: Open
      Contact between terminal 14 and 15: Closed

- If the input is de-energized (safe state): LED “OUT” is off, the relay contacts are in the de-energized state.

  Types 9172/.0 and 9172/.2:
  Contact between terminal 1 and 2: Open
  Contact between terminal 2 and 3: Closed
  Contact between terminal 4 and 6: Closed
  Contact between terminal 5 and 6: Open

  Types 9172/.1:
  Contact between terminal 10 and 11: Open
  Contact between terminal 11 and 12: Closed
  Contact between terminal 13 and 15: Closed
  Contact between terminal 14 and 15: Open

- Restore the loop to full operation.
- Remove the bypass from the safety PLC or otherwise restore normal operation.

It is assumed that this test will detect 99% of possible dangerous failures.

The device has to be replaced if the test uncovers a malfunction. Please inform the manufacturer about a detected malfunction that happened within the defined useful life time / mission time.

8 Repair work

Warning
Danger due to improper repair! • Repair work on the devices must be performed only by R. STAHL Schaltgeräte GmbH.

Do not modify or alter the device!

9 Returning the device

Only return or package the devices after consulting R. STAHL!
Contact the responsible representative from R. STAHL. R. STAHL's customer service is available to handle returns if repair or service is required.

- Contact customer service personally. or
- Go to the r-stahl.com website.
- Under "Support" > "RMA", select "RMA -REQUEST".
- Fill out the form and send it. You will automatically receive an RMA form via email. Please print this file.
- Send the device along with the RMA form in the packaging to R. STAHL Schaltgeräte GmbH.

R. STAHL Schaltgeräte GmbH
Am Bahnhof 30
74638 Waldenburg (Württ.) – Germany
r-stahl.com

ID-Nr. 9172617310 S-SM-9172-01-en-06/2019