Series 9170

Switching repeater

Safety manual

Content

1 General information ... 3
1.1 Manufacturer ... 3
1.2 Information regarding the Safety Manual ... 3
1.3 Area of application ... 3
1.4 Safety function ... 4
1.5 Terms and Definitions ... 4
1.6 Conformity to Standards ... 5
2 General safety information ... 5
2.1 Safety Instructions for Assembly and Operating Personnel ... 5
3 Characteristics for the Functional Safety ... 6
3.1 Functional Safety Data ... 6
3.2 Assumptions ... 8
4 Installation ... 9
5 Parametrization ... 9
5.1 Parameterization using the front DIP switches ... 9
6 Indications ... 10
7 Proof Test ... 10
8 Repair work ... 11

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: www.stahl.de

1.2 Information regarding the Safety Manual

ID-No.: 9170616310 / 217689
Publication Code: S-SM-9170-07-en-06/2022

Additionally to the Safety Manual the following documents must be observed:
X Operating Instructions for the ISpac Switching repeater 9170/*1 Ex i (9170612310 / 200089)
X Exida FMEDA Report No.: STAHL 09/03-52 R019 for 9170/*1

We reserve the right to make technical changes without notice.

1.3 Area of application

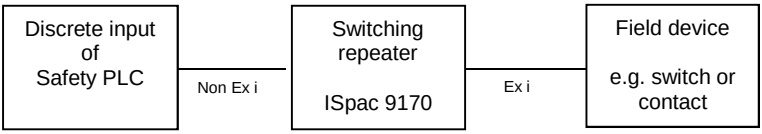
This Safety Manual applies to the Switching repeater ISpac, types 9170/*1-1*-**.

Hardware version: Rev. C, D, E
Software version: not applicable, device does not include software

Switching repeaters transfer intrinsically safe discrete signals of a field device such as NAMUR sensors/proximitors or mechanical contacts) via a galvanic isolation to an non-intrinsically safe output. The field device controls either a normally open relay contact, a switchover relay contact or an electronic output (depends on the individual version).
The state of the output is changing when the input state changes.
The normal output state can be reversed via DIP switches. Line fault detection (LFD) can be selected or disabled via a DIP switch.
The LFT (Line Fault Transparent) versions 9170/**-14-12 are reporting detected line faults directly via the input to the control system.
The safety function of the ISpac 9170 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

Converts an intrinsically safe discrete signal of field device like a switch into a non-intrinsically safe signal for a safety PLC.



Safe state ISpac 9170: The fail-safe state is defined as the output being de-energized.

1.5 Terms and Definitions

DC_S	Diagnostic Coverage of safe failures ($DC_S = \lambda_{sd} / (\lambda_{sd} + \lambda_{su})$)
DC_D	Diagnostic Coverage of dangerous failures ($DC_D = \lambda_{sd} / (\lambda_{dd} + \lambda_{du})$)
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.
MTBF	Mean Time between Failures
MTTR	Mean Time To Repair
PFD	Probability of Failure on Demand
PFD_{AVG}	Average Probability of Failure on Demand
SIL	Safety Integrity Level
SFF	Safe Failure Fraction
T[proof]	Proof Test Intervall
XooY	X out of Y redundancy

1.6 Conformity to Standards

X IEC 61508:
"Functional safety of electrical/electronic/programmable electronic safety-related systems"
X IEC 61511:
"Functional safety - Safety instrumented systems for the process industry sector "
X IEC 61326-1:
"Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 1: General requirements"
X NAMUR NE 21

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 9170/*1 Switching repeater Ex i (9170612310)

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.
- Enable the Line Fault Detection Mode by means of the DIP switches.
- Connect the input of the module to a SIL compliant input 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 (9170/*1 Report No.: STAHL 09/03-52 R019 , download available from r-stahl.com). The failure rate of the module is calculated by a 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 Switching repeater ISpac 9170 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 > 90% for SIL 3 subsystems according to IEC 61508-2, table 2.

	T_{Proof} = 1 year	T_{Proof} = 2 years	T_{Proof} = 5 years
9170/a1-c2/3-ef	PFD_{AVG}= 3.44E-04	PFD_{AVG}=6.56E-04	PFD_{AVG}=1.59E-03
9170/a1-c4-ef	PFD_{AVG}= 1.00E-04	PFD_{AVG}=1.91E-04	PFD_{AVG}=4.65E-04
9170/a1-c0/1-ef	PFD_{AVG}= 1.34E-04	PFD_{AVG}=2.55E-04	PFD_{AVG}=6.19E-04

Switching repeater type 9170/a1-c2-ef

Failure category	**Failure rates (in FIT)**
Fail Safe Undetected (λ_{SU})	120
Fail Safe Detected (λ_{SD})	8
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	72
Total failure rate (safety function)	201
SFF	64 %
SIL AC	SIL 2
PFH	7.2E-8 1/h

Switching repeater type 9170/a1-c2-2f, 9170/a1-c3-2f

Failure category	Failure rates (in FIT)
Fail Safe Undetected (λ_{SU})	167
Fail Safe Detected (λ_{SD})	8
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	72
Total failure rate (safety function)	248
SFF	70 %
SIL AC	SIL 2
PFH	7.2E-8 1/h

Switching repeater type 9170/a1-c4-ef

Failure category	Failure rates (in FIT)
Fail Safe Undetected (λ_{SU})	106
Fail Safe Detected (λ_{SD})	7
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	21
Total failure rate (safety function)	135
SFF	84 %
SIL AC	SIL 2
PFH	2.1E-8 1/h

Switching repeater type 9170/a1-cd-ef

Failure category	Failure rates (in FIT)
Fail Safe Undetected (λ_{SU})	92
Fail Safe Detected (λ_{SD})	8
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	28
Total failure rate (safety function)	129
SFF	78 %
SIL AC	SIL 2
PFH	2.8E-8 1/h

Switching repeater type 9170/a1-cd-2f

Failure category	Failure rates (in FIT)
Fail Safe Undetected (λ_{SU})	139
Fail Safe Detected (λ_{SD})	8
Fail Dangerous Detected (λ_{DD})	1
Fail Dangerous Undetected (λ_{DU})	28
Total failure rate (safety function)	176
SFF	84 %
SIL AC	SIL 2
PFH	2.8E-8 1/h

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

Useful Lifetime	10 years
Hardware structure	1001D
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 ... + 70 °C
Transport temperature	-40 °C ... + 70 °C

3.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Switching repeater Type 9170.

- 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.
- Complete practical fault insertion tests can demonstrate that the diagnostic coverage (DC) corresponds to the assumed DC in the FMEDAs.
- 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.
- All modules are operated in the low demand mode of operation.
- Line fault detection function is activated.

- The power relay outputs (d=2 and 3) are protected by a fuse which initiates at 60% of the rated current to avoid contact welding.
- The resistive relay outputs (d=0 and 1) are only connected to resistive load and to maximum 100 mA.
- Only one input and one output are part of the considered safety function.
- The time of a connected safety PLC to react on a dangerous detected failure and to bring the process to the safe state is identical to MTTR.
- For safety applications only the described outputs are considered.

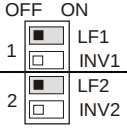
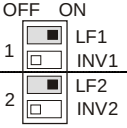
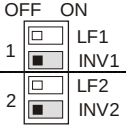
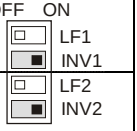
4 Installation

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 Switching repeater ISpac 9170 according to the installation (read the cabinet installation guideline).

5 Parametrization

Warning
Danger due to improper parameterization • Activate the line fault detection as described in chapter 5.1. • Set-up the device according to the below mentioned parameters. • Any other alternative is not permitted. • After the set-up you need to check that the module applies the set-up. This need to be done by an functional test.

5.1 Parameterization using the front DIP switches

	Line fault detection (LF)		**Output inverted (INV)**	
	deactivated *)	**activated**	**OFF *)**	**ON**
Channel 1				
Channel 2				

*) Default factory setting

Mandatory set-up for safety applications

	Please note that the activation of the output inversion (INV) may cause a false indication of the field device status. The misinterpretation leads to dangerous situations as the safety PLC is not able to detect a unsafe status of the plant.

6 Indications

The following LEDs are indicating the status of the device:

LED marking	Colour	Status	Meaning	Action required	Type of action
PWR	Green	ON	Device receives power within the specified range.	No	
		OFF	Device receives power within the specified range.	Yes	Restore the connection to the power supply
LF	Red	ON	Line fault detected	Yes	Check the field for line break or short circuit
		OFF	No line fault	No	
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.

7 Proof Test

Warning
Routine proof tests are mandatory to keep alive the functional safety of the device. They are required to detect failures, which are not detectable in safe operation of the device. • The time interval has to be chosen in accordance with the required PFD_{AVG} - Level.

Warning
Danger due to errors or malfunctions If errors or malfunctions were recognized during the test, the system has to be set out of service immediately and the safety of the process has to be keep ahead by other measures. Errors or malfunctions within the device shall be reported to the manufacturer R. STAHL

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.

After expiration of the Proof test interval (T_{proof}), 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 PLC or take another appropriate action to avoid a false trip.

- Force the Switching repeater 9170 to go to the safe state and verify that the safe state is reached.
  - If the input is energized: LED “OUT” is on, LED “PWR” is on, output contact is closed (inversion not activated)
  - If the input is de-energized: LED “OUT” is off, LED “PWR” is on, output contact is open (inversion is not activated)

- Restore the loop to full operation.

- Remove the bypass from the safety PLC or otherwise restore normal operation.

Detailed description of the operating states can be found in the operating guide, chapter 8.

This test will detect approx. 99% of possible “du” failures.

8 Repair work

Warning
Danger due to improper repair! • The device must be repaired only by the manufacturer!

No changes to the device are permitted!

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

ID-Nr. 9170616310 / 217689 S-SM-9170-07-en-06/2022