



**Binary output**



**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.: 9175612310 / 217688  
Publication Code: S-SM-9175-04-en-02/2014

### **Additionally to the Safety Manual the following documents must be observed:**

- × Operating Instructions for the ISpac Binary output 9175 Ex i (9175601310 / 160428)
- × Operating Instructions for the ISpac Binary output 9175 LFT Ex i (9175611310 / 200104)
- × Exida FMEDA Report No.: STAHL 07/10-01 R012
- × Exida FMEDA Report No.: STAHL 14/01-116 R028

We reserve the right to make technical changes without notice.

## 1.3 Area of application

This Safety Manual applies to the Binary output ISpac,  
types 9175/\*0-1\*-1\*  
type 9175/10-16-11 C1651

Hardware version: Rev. B  
Software version: not applicable, device does not include software

Binary output modules are used for intrinsically safe operation of magnetic valves, LED signal lights and horns in hazardous locations.

The modules are controlled by safety PLC. The ON-signal and OFF-signal must be within defined ranges.

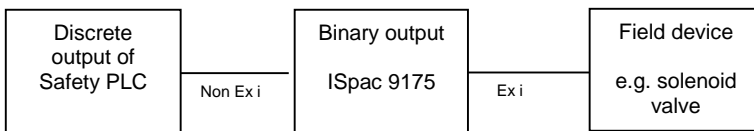
Line faults are detected and reported by a red LED and a separate line fault contact. The Line fault detection can be deactivated.

The LFT (Line Fault Transparent) versions 9175/10-1\*-12 are reporting detected line faults directly via the input to the control system.

The safety function of the ISpac 9175 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 a discrete signal of a safety PLC into an intrinsically safe discrete signal in order to switch a field device.



Safe state ISpac 9175: The fail-safe state is defined as the output being de-energized or the output current is less than 3 mA (for 9175/\*0-1\*-1\*) or the following values for type 9175/10-16-11 C1651:

Current value	Load resistance
250 $\mu$ A	10 k $\Omega$
1,65 mA	100 $\Omega$

### 1.5 Terms and Definitions

DCS	Diagnostic Coverage of safe failures (DCS = $\lambda_{sd} / (\lambda_{sd} + \lambda_{su})$ )
DCD	Diagnostic Coverage of dangerous failures (DCD = $\lambda_{sd} / (\lambda_{dd} + \lambda_{du})$ )
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 <sub>AVG</sub>	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 9175 Binary output Ex i (9175601310)
- Observe the operating instructions for the ISpac 9175 LFT Binary output Ex I (9175611310)

#### 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 or 3 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 (Report No.: STAHL 07/10-01 R012 and Report No.: STAHL 14/01-116 R028, download available from [www.stahl.de](http://www.stahl.de)). 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:

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

$$\text{SFF} = 1 - \lambda_{\text{DU}} / \lambda_{\text{total}}$$

The binary output ISpac 9175 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 <sub>Proof</sub> = 1 year	T <sub>Proof</sub> = 2 years	T <sub>Proof</sub> = 5 years
9175/10-1*-12	PFD <sub>AVG</sub> = 6.50E-05	PFD <sub>AVG</sub> =1.24E-04	PFD <sub>AVG</sub> =3.01E-04
9175/a=-1*-11 (single)	PFD <sub>AVG</sub> = 4.25E-05	PFD <sub>AVG</sub> =8.12E-05	PFD <sub>AVG</sub> =1.97E-04
9175/a=-1*-11 (parallel)	PFD <sub>AVG</sub> = 8.39E-05	PFD <sub>AVG</sub> =1.60E-04	PFD <sub>AVG</sub> =3.89E-04
9175/10-16-11 C1651	PFD <sub>AVG</sub> = 7.81E-05	PFD <sub>AVG</sub> =1.94E-04	PFD <sub>AVG</sub> =3.62E-04

This means that for a SIL 3 application, the PFD<sub>AVG</sub> for a one year Proof Test Interval considering profile 1 data is approximately equal to 7% of the range considering the single output and approx. equal to 8% of the range considering the parallel output.

The following values are based on the calculation according IEC EN 61508-1, edition 1.

#### Binary output type 9175/10-1\*-12 LFT

Failure category	Failure rates (in FIT)
Fail Safe Undetected ( $\lambda_{\text{SU}}$ )	210
Fail Dangerous Detected ( $\lambda_{\text{DD}}$ )	0
Fail Dangerous Undetected ( $\lambda_{\text{DU}}$ )	14
No part	132
No effect	335
SFF	93 %
SIL AC	SIL 3

**Binary output type 9175/a0-1\*-11**

Failure category	Failure rates (in FIT)
Fail Safe Undetected ( $\lambda_{SU}$ )	166
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	9
No part	212
No effect	243
SFF	94 %
SIL AC	SIL 3

**Binary Output type 9175/20-1\*-11 with parallel output connection**

Failure category	Failure rates (in FIT)
Fail Safe Undetected ( $\lambda_{SU}$ )	266
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	18
No part	417
No effect	429
SFF	93 %
SIL AC	SIL 3

**Binary Output type 9175/10-16-11 C1651**

Failure category	Failure rates (in FIT)
Fail Safe Detected ( $\lambda_{SD}$ )	0
Fail Safe Undetected ( $\lambda_{SU}$ )	155
Fail Dangerous Detected ( $\lambda_{DD}$ )	0
Fail Dangerous Undetected ( $\lambda_{DU}$ )	17
Fail Annunciation Detected ( $\lambda_{AD}$ )	0
Fail Annunciation Undetected ( $\lambda_{AD}$ )	9
No part	344
No effect	217
Total failure rate (safety function)	172
SFF	90 %
SIL AC	SIL 3

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire Safety Instrumented Function (SIF). For SIL 3 applications the sum of the  $PF_{D,AVG}$  values of all devices of a Safety Instrumented Function (SIF) needs to be  $1.00E-4 < SIF < 1.00E-03$ .

Useful Lifetime	10 years
Hardware structure	1001D
MTTR	24 hours
Ambient temperature	-20 °C ... +65 °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 Binary Output Type 9175.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- 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
- Short circuit and lead breakage are either activated or de-activated, please check the safety manual and operating manual of the field device.
- For safety applications only the described variants are considered
- The two channels on the two channel devices shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve higher SIL, as they contain common components.



## 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 Binary output ISpac 9175 according to the installation (read the cabinet installation guideline).





## 5 Parametrization

### Warning

#### Danger due to improper parameterization

- 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 a functional test.

### 5.1 Parameterization using the front DIP switches

	Line fault detection LF	
	Deactivated *	Activated
Channel 1	OFF ON 1  LF1	OFF ON 1  LF1
Channel 2	2  LF2	2  LF2

\*) Default factory setting



Please note that the activation of the line fault detection may cause that a solenoid valve cannot be released means it cannot trip. Please check the technical data of the solenoid valve accordingly. The current used for line fault detection is described in the table below.

## 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<sub>AVG</sub> - 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 kept 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 Binary output 9175 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 signal within the specified range (see technical data)
  - If the input is de-energized: LED "OUT" is off, LED "PWR" is on, output signal below 3 mA
- Restore the loop to full operation.
- Remove the bypass from the safety PLC or otherwise restore normal operation.

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

## **8 Repair work**

<b>Warning</b>
<b>Danger due to improper repair!</b> <ul style="list-style-type: none"><li>• The device must be repaired only by the manufacturer!</li></ul>



No changes to the device are permitted!



R. STAHL Schaltgeräte GmbH  
Am Bahnhof 30  
74638 Waldenburg (Württ.) – Germany  
[www.stahl.de](http://www.stahl.de)