Type 9182

Temperature Transmitter
9182/.0-5.-.3

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: www.stahl.de

1.2 Information regarding the Safety Manual

ID-No.: 171444 / 9182612310
Publication Code: S-SM-9182-04-en-06/2015

Additionally to the Safety manual the following documents must be observed:

X Operating Instructions for the ISpac Temperature Transmitter 9182 Ex i (9182601310)
X Operating Instructions for the ISpac Temperature Transmitter 9182 Non-Ex i (918260330)
X Operating Instructions for the ISpac Wizard software 9199/20-01 (read me file).

We reserve the right to make technical changes without notice.

1.3 Area of application

This Safety manual applies to the ISpac Temperature Transmitter types 9182/*0-5*-*3.

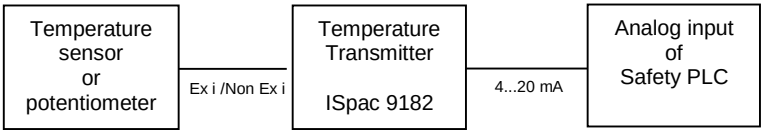
Hardware version: Rev. B, C
Software version: V01-09
Configuration Software ISpac Wizard: 3.02.01 or higher.

Temperature Transmitters are used for intrinsically safe (types 9182/*0-5*-13) or non-intrinsically safe operation (types 9182/*0-5*-63) of temperature sensors or potentiometers with requirements according to IEC 61508 up to SIL 2.

Nearly all sensors, such as Pt100, Pt500 or thermocouples and potentiometers, may be connected. Parameters can be set via PC software ISpac Wizard.
The safety function of the ISpac 9182 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

Transmission of an analog signal of a temperature sensor into a linear 4…20 mA signal.



The value of a selected temperature sensor is measured and transmitted into a linear 4…20 mA signal. The active analog 4…20 mA signal is feed into an analog input of a safety PLC.

Safe state ISpac 9182:

Fail High	Output signal > 21 mA
Fail Low	Output signal < 3,6 mA

The Safety PLC is able to detect if a line fault has occurred. It is recommended to set the line fault detection values of the safety PLC to the Namur NE43 values:

Fail high	Output signal ≥ 21 mA
Fail Low	Output signal ≤ 3,6 mA

1.5 Terms and Definitions

DCS	Diagnostic Coverage of safe failures (DCS = λ_{sd} / (λ_{sd} + λ_{su}))
DCD	Diagnostic Coverage of dangerous failures (DCD = λ_{sd} / (λ_{dd} + λ_{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
PVD_{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 Temperature Transmitter ISpac 9182 Ex i (9182601310)
- Observe the Operating Instructions for the Temperature Transmitter Non-Ex i ISpac 9182 (91826033 0)

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.
- Feed the 4…20 mA output signal to a SIL 2 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 assessment report of EXIDA (Report No.: STAHL 07/07-23 R016, download available from 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:

$\lambda_{total} = \lambda_{safe} + \lambda_{dangerous} + \lambda_{residual} + \lambda_{annunciation}$

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

The Temperature Transmitter ISpac 9182 is considered to be a Type B subsystem with a hardware fault tolerance of 0. For Type B subsystems with a hardware fault tolerance of 0 the SFF shall be > 90% for SIL 2 subsystems according to IEC 61508-2, table 3.
As the Temperature Transmitter type 9182/10-5*-*3 is supposed to be a proven-in-use device, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. The proven-in-use investigation was based on field return data collected and analyzed by R. STAHL Schaltgeräte GmbH.
According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the exida proven-in-use assessment described in section 6, the Temperature Transmitter type 9182/10-5*-*3 with a SFF of < 90% might also be used for a SIL 2 safety function.

T_{Proof} = 1 year	T_{Proof} = 2 years	T_{Proof} = 5 years
PFD_{AVG}= 7.59E-04	PFD_{AVG}=1.44E-03	PFD_{AVG}=3.48E-03

This means that for a SIL 2 application, the PFD_{AVG} for a one year Proof Test Interval considering profile 1data is approximately equal to 7,6% of range.

Failure category	Failure rates (in FIT)
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	173
Fail Dangerous Detected (λ_{DD})	384
Fail Dangerous Undetected (λ_{DU})	157
No part	234
Total failure rate (safety function)	714
SFF	78 %
DC_D	71%
MTBF	120 years

It is the responsibility of the Safety Instrumented Function designer to do calculations for the entire Safety Instrumented Function (SIF). For SIL 2 applications the sum of the PFD_{AVG} values of all devices of a Safety Instrumented Function (SIF) needs to be 1.00E-3 < SIF < 1.00E-02. The proven-in-use information is used for a prior in use justification per IEC 61511-1.

Useful Lifetime	10 years
Hardware structure	1001D
MTTR	24 hours
Safety accuracy	2% of the measurement span
Fault detection delay time	max. 60 seconds
Ambient temperature	-20 °C ... +65 °C (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.
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 Temperature Transmitter Type 9182/*0-5*-*3.

- 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.
- Sufficient tests are performed prior to shipment to veriy 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.
- The worst-case internal fault detection time is 60 seconds.
- All modules are operated in the low demand mode of operation
- The time of a connected safety PLC to react on a dangerous detected failure and to bring the process to safe state is identical to MTTR.
- The output signal is fed to a SIL 2 compliant input board of a safety PLC.
- Only the current output 4..20 mA is used for safety applications.
- Lead breakage is activated.
- The application program in the safety logic solver is configured to detect under-range and over-range failures and does not automatically trip on these failures; therefore these failures have been classified as dangerous detected failures.
- 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 Temperature Transmitter ISpac 9182.

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 an functional test.

5.1 Parameterization using ISpac Wizard software

The following described set-ups are done by means of the software ISpac Wizard. Please read the instruction carefully before operating the software.

Parameter	**Set-up selections for safety function**	**Remark**
Output - channel 1 Output signal type	4-20 mA (life zero)	Enables line fault detection by the safety PLC.
Output - channel 1 Fault behavior	Output fault value Fault value: 2,4 mA	Please check the set-up of the safety PLC.

All other set-ups can be done in the software can be selected according to the specific application.

Parameter	Set-up selections
Input	According to the sensor applied: - Mode - Sensor type - Circuit type - Wire resistance - CJC type - Fixed CJC temperature
Signal processing	According to the measurement range
Limit value	Not available

5.2 DIP switch setting

The front panel of the device includes a DIP switch. It includes a switch for the line fault detection (LF) and a switch (ADJ) which enables functions like line balancing/2-wire calibration (more details in the operating instructions).

Warning
Danger due to incorrect parameterization of line fault detection • The line fault protection setting (LF) is required to be switched on. • Disabling the line fault detection by DIP switch overrides the fault behaviour settings done with the ISpac Wizard software.

6 Functional tests

Warning
Danger due to mismatch between parameterization and device behavior • The functional tests are mandatory in order to verify the correct function of the device.

The following tests steps are recommended to verify a proper parameterization.

- Generate a line break condition by disconnecting the sensor and verify that the output signal is < 2.4 mA. (see setting of output fault value, chapter 5.1)
- Generate a short circuit condition by short circuiting the sensor input at the device and verify that the output signal is < 2.4 mA. (see setting of output fault value, chapter 5.1)
- Generate signals by means of a sensor generator or calibrator and verify that the 4…20 mA signal output value (e.g. 0%, 25%, 50%, 75%, 100% of the measurement range) corresponds to the expected values considering the specified accuracy.

7 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
		Flashing	Measured sensor signal out of range, analog output saturated	Yes	Change the parameterization. The set-up of the transmitter does not fit to the application.
		OFF	No line fault	No	

8 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

The execution of the proof tests, test conditions and results of the testing has to be documented.

After expiration of the Proof test interval (T_{proof}) (see chapter 3.1), 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.
- Generate a line break condition by disconnecting the sensor and verify that the output signal is < 2.4 mA. (see setting of output fault value, chapter 5.1)
- Generate a short circuit condition by short circuiting the sensor input at the device and verify that the output signal is < 2,4 mA. (see setting of output fault value, chapter 5.1)
- Generate several signals within the allowed range of the sensor and check if it corresponds to the analog output signal.
- Restore normal operation**.**

The proof test coverage is considered to be 99%.

9 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
www.stahl.de