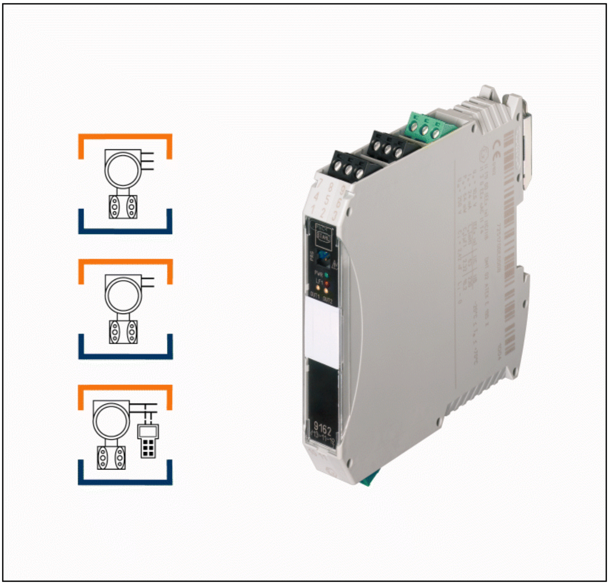
Type 9162



Transmitter Supply Unit with Limit Values 9162/13-11-14 9162/13-11-64

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.:	916260310130
Publication Code:	S-SM-9162-03-en-12/2015

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

X Operating Instructions for the ISpac Transmitter Supply Unit with Limit Values 9162 (916260310140 / SAP 240194)
X Operating Instructions for the ISpac Wizard software 9199/20-02.
X FMEDA Report – STAHL 13/12-013 R029

We reserve the right to make technical changes without notice.

1.3 Area of application

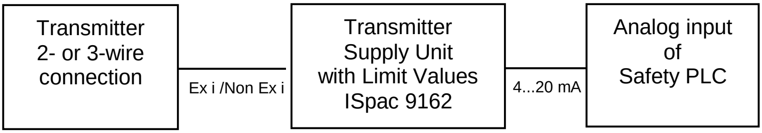
This Safety manual applies to the ISpac Transmitter Supply Unit with Limit Values,
type 9162/13-11-14,
type 9162/13-11-64.

Hardware version:	Rev. C
Software version:	V01-06
Configuration Software ISpac Wizard:	3.04 or higher.

Transmitter Supply Unit with Limit Values is used for intrinsically safe (types 9162/13-11-14) or non-intrinsically safe operation (types 9162/13-11-64) of 4...20 mA transmitter with requirements according to IEC 61508 up to SIL 2 AC.
The transmitter may be operated as 2-wire and 3-wire device. Parameters are set via PC software ISpac Wizard. The PC is connected to the device by means of RS 232 interface.
The safety function of the ISpac 9162 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

Application 1) Transmission of an analog signal 4…20 mA signal of transmitter installed in the field into a linear 4…20 mA signal.



The 4...20 mA signal is received from a transmitter installed in the field. The signal is transferred to the output. The active analog 4…20 mA signal is fed into an analog input of a Safety PLC or ESD system. The maximum allowed signal deviation is 2% of the measurement range.

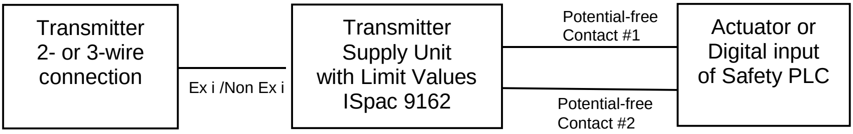
Safe state ISpac 9162:

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

The Safety PLC or ESD system is able to detect if a line fault has occurred. It is recommended to set the line fault detection values of the Safety PLC or ESD system to the following values:

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

Application 2) Trip amplifier (limit values)



The 4...20 mA signal is received from a transmitter installed in the field. The signal is transferred to the output and continuously compared with two preselected limit values. Depending on the set-up a potential-free contact will open if the measured value is above or below the limit value. The maximum allowed signal deviation is 2% of the measurement range.

The limit value contacts can be used independently. The limit value contacts can be used in series.

Fail safe state: Limit value contact open.

The two applications shall not be used in the same safety function, e.g. to increase the hardware fault tolerance to achieve a higher SIL, as they contain common components. The FMEDA applies to either function used in a single safety function. The applications may be used in separate safety functions if the probability of common failures is taken into account.

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 Restoration
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 IEC 61326-3-2: “Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - Industrial applications with specified electromagnetic environment” *)
X NAMUR NE 21 *)

*) 20 ms power supply buffering by means of external power supply device.

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 9162 Transmitter Supply Unit with Limit Values

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:

- Allow for a start-up time of 20 minutes after switch-on of power supply.
- 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.
- Connect the limit value output to actuators of your safety loop or to a safety PLC.
- Online parameterization (during operation) is not permitted.
- Ensure that only authorized personal has access to the set-up of the device.
- Ensure that HART is not intend for safety critical operation

If you have questions: Contact the manufacturer.

3. Characteristics for Functional Safety

Confirmation of meeting the requirements of IEC 61508 is done by an assessment report of EXIDA (Report No.: STAHL 13/12-013 R029 Version V1, Revision R1). The numbers for fulfilling the hardware safety integrity requirements of the module are calculated by an 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

An average Probability of Failure on Demand (PFD_{AVG}) calculation is performed considering a proof test coverage of 99% and a mission time of 10 years.

For SIL 2 applications, the PFD_{AVG} value needs to be < 1.00E-02.

Configuration	**T_{Proof} = 1 year**	**T_{Proof} = 2 years**	**T_{Proof} = 5 years**
4…20 mA current output	PFD_{AVG}= 1.30E-04	PFD_{AVG}= 2,43E-04	PFD_{AVG}= 5,81E-04
Limit value output	PFD_{AVG}= 2.23E-04	PFD_{AVG}= 4.19E-04	PFD_{AVG}= 1.01E-03
Limit value output in series	PFD_{AVG}= 1.29E-04	PFD_{AVG}= 2.38E-04	PFD_{AVG}= 5.67E-04

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 isolator ISpac 9162 is considered to be a Type B subsystem with a Hardware Fault Tolerance (HFT) 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.

9162/13-11*4 with 4...20 mA current output:

Failure category	**Value**
Fail Safe Detected (λ_{SD})	0 FIT
Fail Safe Undetected (λ_{SU})	0 FIT
Fail Dangerous Detected (λ_{DD})	416 FIT
Fail Dangerous Undetected (λ_{DU})	27 FIT
Total failure rate (safety function)	443 FIT
SFF	93 %
SIL AC	SIL 2

9162/13-11-*4 with limit value output:

Failure category	**Value**
Fail Safe Detected (λ_{SD})	0 FIT
Fail Safe Undetected (λ_{SU})	0 FIT
Fail Dangerous Detected (λ_{DD})	436 FIT
Fail Dangerous Undetected (λ_{DU})	46 FIT
Total failure rate (safety function)	482 FIT
SFF	90 %
SIL AC	SIL 2

9162/13-11*4 with two limit value outputs in series:

Failure category	**Value**
Fail Safe Detected (λ_{SD})	0 FIT
Fail Safe Undetected (λ_{SU})	0 FIT
Fail Dangerous Detected (λ_{DD})	447 FIT
Fail Dangerous Undetected (λ_{DU})	26 FIT
Total failure rate (safety function)	473 FIT
SFF	94%
SIL AC	SIL 2

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

Usefull Lifetime	10 years Please ensure that the max. current of 100 mA at the limit value contact is not exceeded.
Hardware structure	1oo1D
MTTR	24 hours
Safety accuracy	2% of the measurement span
Worst case fault detection time	20 minutes
Ambient temperature	-40 °C ... +65 °C*)
Storage temperature	-40 °C … + 80 °C
Transport temperature	-40 °C … + 70 °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.

3.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Transmitter Supply Unit with Limit Values type 9162/13-11-*4.

- 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 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.
- EN 61326-3-2 and NE 21 require a power supply buffer time of 20 ms. In order to achieve this buffer time use an external power supply device which supports a minimum buffer time of 20 ms.
- The Mean Time to Restoration (MTTR) after a safe failure is 24 hours.
- For safety applications only the described configurations of the Transmitter Supply Unit with Limit Values 9162 are considered.
- Safety critical failures are defined as a deviation of more than 2% FS (Full Scale) for current output or deviation of relay output switching threshold.
- For soft errors, a failure rate of 1.2 FIT/kBit was assumed.
- The worst-case internal fault detection time is 20 minutes.
- 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 application program in the safety logic solver is configured according to Namur NE 43 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 short circuit and lead breakage detection are activated (permanently activated in the described versions, manual deactivation not possible)
- The end-user performs proof tests regularly. The cycle time is defined in the chapter 3.1 (T_{proof}). The proof test is in the responsibility of the end-user.

Safety relevant interfaces:

- 1 x Analog input (4...20 mA)
- 1 x Analog output (4...20 mA)
- 2 x Digital outputs (limit value)

Not safety relevant interfaces:

- 1 x HART (superimposed on 4...20 mA)
- 1 x pac-Bus type 9194 (power supply and line fault detection)
- 1 x Power supply
- 1 x Configuration interface RS 232

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 device ISpac 9162.

5. Parameterization

Warning
Danger due to improper parameterization • Set-up of the device in operation is not permitted. • 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 needs to be done by a functional test.

5.1 Parameterization using ISpac Wizard software

Please note that a proper definition of the SIF is the prerequisite for the set-up of the device 9162.

It is not allowed to set-up the device while it is in use.

Tab	Option	Set-up selections	Allowed for safety function
Limit value	Behavior of contact	Inactive	Yes
		Opens, if value > limit value	Yes
		Opens, if value < limit value	Yes
	Limit value	Limit value at which the corresponding relay should switch	Yes 3.8…20.5 mA
	Hysteresis	The range of hysteresis within the respective limit value relay should switch	Yes 0.24…2.4 mA
	Reset lockout	Inactive	Yes
		Active	Yes

5.2 DIP switch setting

The front panel of the device includes a DIP switch. It includes a switch (RL) which enables the reset lockout function (more details in the operating instructions).

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 test steps are recommended to verify a proper parameterization.

- Generate a line break condition by disconnecting the sensor. Verify that the output signal is 0 mA (< 3,6 mA) and the limit value contacts trip to open.
- Generate a short circuit condition by short circuiting the sensor input at the device. Verify that the output signal is 25 mA (> 21 mA) and the limit value contacts trip to open.
- 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.
- Generate a signal which verifies the correct setting of the limit value. Please take the hysteresis into consideration.

7. Timing

Please allow the device for 2 seconds start-up time before you use it in a safety loop.
The setting time of the signal is 2.4 seconds. The fault detection delay time is 20 minutes.

8. Indications

The following LEDs are indicating the status of the device:

LED marking	Colour	Status	Meaning	Action required	Type of action
PWR	Green	ON	Supplied power within specified range.	No	
		OFF LF: OFF	Supplied power outside specified range	Yes	Restore the connection to the power supply
		OFF LF: Flash	Malfunction detected by internal check routine	Yes	Set the device out of service. Make sure that the safety function is in the safe state. Exchange the device and report the failure to R. STAHL.
LF	Red	ON	Line fault detected	Yes	Check the field for line break or short circuit
		Flashing PWR: OFF	Malfunction detected by internal check routine	Yes	Set the device out of service. Make sure that the safety function is in the safe state. Exchange the device and report the failure to R. STAHL.
		OFF	No line fault	No	
A or B	Amber	ON	Limit value criteria achieved – relay switched, contact closed	No	
		OFF	Limit value criteria not achieved – relay deenergized, contact open	No	

9. 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 kept 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 have 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 0 mA (< 3.6 mA).
- Generate a short circuit condition by short circuiting the sensor input at the device and verify that the output signal is > 21 mA.
- Generate several signals within the allowed range of the sensor and check if they correspond to the analog output signal. The deviation between input and output signal needs to be lower than 2%.
- Generate a signal which verifies the correct setting of the limit value. Please take the hysteresis into consideration.
- Restore normal operation.

10. Repair work

Please report any malfunction of the devices back to the manufacturer. Please contact the local R. STAHL representation. In order to ensure that our database includes all necessary information we request you to fill in the return for repair form of R. STAHL.

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

Modifications of the device are not permitted!

If a fault has been detected by internal check-routines the device will change into the safe state. A power-on will reset the device and start diagnostic cycle.

11. Firmware update / Calibration

Warning
Danger due to improper function! • Firmware updates or calibrations are not permitted.

R. STAHL Schaltgeräte GmbH
Am Bahnhof 30
74638 Waldenburg (Württ.) – Germany
www.stahl.de