Type 9160 / 9163

Transmitter supply unit / Isolating repeater

STAHL

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 ... 7
4 Installation ... 8
5 Parametrization ... 8
5.1 Parameterization using the front DIP switches ... 8
6 Indications ... 9
7 Proof Test ... 9
8 Repair work ... 10

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.: 9160616310 / 217690
Publication Code: S-SM-9160-06-en-09/2015

Additionally to the Safety Manual the following documents must be observed:
X Operating Instructions for the ISpac Transmitter supply unit 9160 Ex i (221787 / 9160617310)
X Operating instruction for the ISpac Isolating repeater 9163 Ex i (221792 / 9163611310)
X Exida FMEDA Report No.: STAHL 10/02-01 R027

We reserve the right to make technical changes without notice.

1.3 Area of application

This Safety Manual applies to the Transmitter supply unit ISpac,
series 9160 and Isolating repeater series 9163
Hardware version 9160: Rev. F
Hardware version 9163: Rev. B
Software version: not applicable, device does not include software

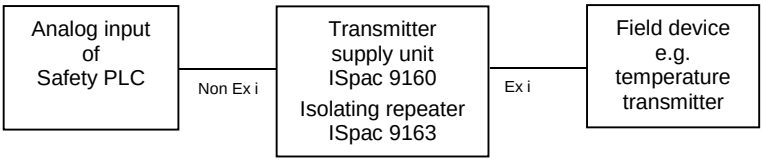
The transmitter supply units are used for the operation of 2-wire and 3-wire transmitters or to connect to intrinsically safe current sources.
The 2-wire and 3-wire transmitters are supplied with power by the transmitter power supply unit. The devices transfer bidirectionally a superimposed HART communications signal. Line fault detection (LFD) can be selected or disabled via a DIP switch.

The isolating repeater is used to transmit intrinsically safe analog signals (current or voltage) from the field to a process control system or a PLC. These field devices can be 3- or 4-conductor transmitters with an intrinsically safe signal 0/4 ... 20 mA. The device transmits a superimposed HART communication signal bidirectionally. One version of the isolating repeater converts intrinsically safe standard voltage signals into a non-intrinsically safe signal 0/4 ... 20 mA.

The safety function of the ISpac 9160 and 9163 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 analog input signal of a transmitter a non-intrinsically safe signal for a safety PLC.



Transmitter supply unit / Isolating repeater:
The 4...20 mA signal is received from a transmitter installed in the field. The signal is transferred to the output. The analog 4…20 mA signal is connected to an analog input of a Safety PLC or ESD system. The maximum allowed signal deviation is 2% of the measurement range.

Safe state: The fail-safe state is defined as the output being in the Fail Low or Fail High mode of operation. The Fail Low state is defined as an output signal to be below 3,6 mA. The Fail High state is defined as an output signal higher than 21 mA.

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
PFH	Probability of Failure per Hour
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 9160 Transmitter supply unit Ex i (221787 / 9160617310) / ISpac Isolating repeater Ex i (221792 / 9163611310)

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 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 10/02-01 R027; 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:
$\lambda_{total} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$
$SFF = 1 - \lambda_{DU} / \lambda_{total}$

The Transmitter supply unit ISpac 9160 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.

	T_{Proof} = 1 year	T_{Proof} = 2 years	T_{Proof} = 5 years
9160 / 9163 - standard types	PFD_{AVG}= 2.29E-04	PFD_{AVG}=3.38E-04	PFD_{AVG}=6.64E-04
9160 / 9163 - signal compare output	PFD_{AVG}= 5.96E-05	PFD_{AVG}=8.76E-05	PFD_{AVG}=1.72E-04

9160 / 9163 – standard types

Failure category	**Failure rates (in FIT)**
Fail Safe Undetected (λ_{SU})	0
Fail Safe Detected (λ_{SD})	0
Fail Dangerous Detected (λ_{DD})	163
Fail Dangerous Undetected (λ_{DU})	28
No effect	177
Annunciation undetected	2
No part	333
Total failure rate	191
SFF	85 %
SIL	SIL 2
PFH	2.8E-08 1/h

9160 / 9163 - compare output (only 9160/13-1x-13 and 9163/13-1x-13)

Failure category	**Failure rates (in FIT)**
Fail Safe Undetected (λ_{SU})	0
Fail Safe Detected (λ_{SD})	0
Fail Dangerous Detected (λ_{DD})	185
Fail Dangerous Undetected (λ_{DU})	8

No effect	173
Annunciation undetected	243
No part	339
Total failure rate	193
SFF	95 %
SIL	SIL 3
PFH	8.0E-09 1/h

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.

Useful Lifetime	> 10 years
Hardware structure	1001D
MTTR	24 hours
Ambient temperature	-40 °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 Transmitter supply unit Type 9160 /isolating repeater 9163.
.

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- External power supply failure rates are not included.
- The time to restoration after a safe failure is 24 hours.
- 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.
- For safety applications only the described versions are considered.
- The different versions are separated into two main versions which can be configured by a few resistors. The considered main versions which cover all subtypes (see table 1 and table 2)
- Only the signal transmission function of the Transmitter Supply Unit 9160 types is part of the FMEDA. The failure rates of the transmitter supply function are not included. It is assumed that a connected transmitter checks the supply voltage which is provided by the Transmitter Supply Unit 9160 and stops operation in case of insufficient supply instead of generating wrong output signals.
- The device is installed per manufacturer's instructions.

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 Transmitter supply unit ISpac 9160 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		
Channel 2		

*) Default factory setting

The versions 9160/13-11-10 and 9160/23-11-10 do not support line fault detection and signalization. Therefore these versions do not offer DIP switches.

Please note: The line fault detection is applied for the input and output circuits. The version 9160/19-..-.. offers one input – two output structure. The line fault detection monitors the common input channel and the according output channel. An open output (without load) leads to fault indication. Please connect a load of 250 Ohm to the unused output.

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	

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

Proof test 1

- Bypass the PLC or take another appropriate action to avoid a false trip.
- Force the Transmitter supply unit 9160 / Isolating repeater 9163 to go to the high alarm and verify that the analog output reaches that value.
    - This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
- Force the Transmitter supply unit 9160 / Isolating repeater 9163 to go to the low alarm and verify that the analog output reaches that value.
    - This tests for possible quiescent current related failures.
- Restore the loop to full operation.
- Remove the bypass from the safety PLC or otherwise restore normal operation**.**

This test will detect approx. 50% of possible “du” failures in the transmitter supply unit 9160.

Proof test 2

- Bypass the PLC or take another appropriate action to avoid a false trip.
- Perform Proof test 1.
- Perform a two-point calibration of the connected transmitter.
    - This requires that the transmitter has already been tested without the transmitter supply unit 9160 and does not contain any dangerous undetected faults anymore.
- 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 in the transmitter supply unit 9160.

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
www.stahl.de

ID-Nr. 9160616310 / 217690 S-SM-9160-06-en-09/2015