Series 9147

Vibration Transducer Supply Unit

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: r-stahl.com

1.2 Information regarding the Safety Manual

ID-No.: 914760310070
Publication code: S-SM-9147-01-en-06/2019

Additionally to the Safety Manual the following documents must be observed:
X Operating Instructions for Vibration Transducer Supply Unit 9147 (213097 / 914760310010)
X Exida FMEDA Report No.: STAHL 13/06-082 R025

We reserve the right to make technical changes without notice.

1.3 Area of application

This Safety Manual applies to the Vibration Transducer Supply Unit ISpac, types: 9147/*0-99-10. Hardware revision C

Software version: not applicable, device does not include software

The Vibration Transducer Supply Unit is used for the intrinsically safe operation of vibration transducers or acceleration sensors. It's possible to operate 2-wire acceleration sensor current-feed or voltage-feeds 3-wire eddy current transducers.
The device supplies the sensors and transmits its signal galvanic separated to the output.

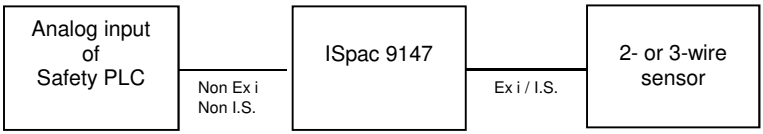
The modules are controlled by safety PLC.

The safety function of the ISpac 9147 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

Binary/discrete output application:

Converts a discrete signal of a safety PLC into an intrinsically safe discrete signal in order to switch a field device.



Fail safe state: The fail-safe-state is defined as the output reaching the user defined threshold value.

1.5 Terms and Definitions

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.
PFD_{AVG}	Average Probability of Failure on Demand
SFF	Safe Failure Fraction, summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s) and final element(s).
PLC	Programmable Logic Solver
T[proof]	Proof Test Interval
Type A element	”non-complex” element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2.

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 9147 module (see 1.2)

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 compliant output 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 13/06-082 R025, download available at r-stahl.com). The failure rate of the module is calculated by 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 device 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.
The PFD_{AVG} value needs to be < 1.00E-02.

	T_{PROOF} = 1 year	T_{PROOF} = 2 years	T_{PROOF} = 5 years
9147 – 2 wire	PFD_{AVG} = 7.95-04	PFD_{AVG} = 1.17E-03	PFD_{AVG} = 2.29E-03
9147 – 3 wire	PFD_{AVG} = 6.70-04	PFD_{AVG} = 9.86E-04	PFD_{AVG} = 1.93E-03

Failure rates

Vibration Transducer Supply Unit 9147 with 2-wire input

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	0
Fail Dangerous Detected (λ_{DD})	188
Fail Dangerous Detected (λ_{DD})	0
Fail High (H)	23
Fail Low (L)	165
Fail Annunciation Undetected (λ_{AU})	0
Fail Dangerous Undetected (λ_{DU})	95
Fail Annunciation Undetected (λ_{AU})	11
No part	33
No effect	215
Total failure rate (safety function)	283
SFF	66 %
SIL AC	SIL 2
PFH	9.5E-08 1/h

Vibration Transducer Supply Unit 9147 with 3-wire input

Failure category	**Failure rates (in FIT)**
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	0
Fail Dangerous Detected (λ_{DD})	184
Fail Dangerous Detected (λ_{DD})	0
Fail High (H)	23
Fail Low (L)	161
Fail Annunciation Undetected (λ_{AU})	0
Fail Dangerous Undetected (λ_{DU})	80
Fail Annunciation Undetected (λ_{AU})	11
No part	32
No effect	217
Total failure rate (safety function)	264
SFF	69 %
SIL AC	SIL 2
PFH	8.0E-08 1/h

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

Fail-safe state: The fail-safe-state is defined as the output reaching the user defined threshold value.

Fail High: Failure that causes the voltage output signal to go to the maximum output voltage (< -20.5 V)

Fail Low: Failure that causes the voltage output signal to go to the minimum output voltage (> -0.5 V)

Useful Lifetime	10 years
Hardware structure	1001
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 ... + 80 °C
Transport temperature	-40 °C ... + 80 °C

3.2 Assumptions

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The device is installed per manufacturer's instructions.
- 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.
- External power supply failure rates are not included.
- The mean time to restoration (MTTR) after a safe failure is 24 hours.
- For safety applications only the described versions of the series 9147 are considered.
- Only one channel of the device is part of the FMEDA assessment and can be used for safety application. The second channel must not be used for the same safety application, because of possible common cause failures in the common power supply.
- Failure with less than 2% of full span are uncritical and within the specification of the device.
- The connected control logic considers signal levels outside the range of – 0.5 V and – 20.5 V as a failure.

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 according to the installation (read the cabinet installation guideline).

5 Parametrization

The device need to be parameterized according to the applied sensor or transducer. A rotary switch on the front side of the device is used for the set-up.
Open the transparent lid of the device. The rotary switch is located in the middle of the front side. The rotary switch can be operated best by a fitting screw driver. Set the screw driver carefully into the groove of the rotary switch and turn it into the required position according to the table below. There is one rotary switch per channel.

Sensor	3-wire *)	2-wire		
		2,6 mA	4,3 mA	7,9 mA
Position of rotary switch				

*) Default set-up

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	None, as long as this is expected behaviour.
		OFF	Device does not receive power within the specified range.	Yes	Restore the connection to the power supply

The indication LEDs are not considered in FMEDA reports.

7 Proof Test

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.

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 safety PLC or take another appropriate action to avoid a false trip.
- Apply an input signal with a defined frequency and amplitude at the input of the device.
- Measure if the output signal of the device is within the frequency and amplitude specification.
- Apply a signal amplitude > - 0.5 V and < 20.5 V
- Check if the connected safety PLC switches into safe state.
- Remove the bypass from the safety PLC or otherwise restore normal operation.

It is assumed that this test will detect 99% of possible dangerous failures.

The device has to be replaced if the test uncovers a malfunction. Please inform the manufacturer about a detected malfunction that happened within the defined useful life time / mission time.

8 Repair work

Warning
Danger due to improper repair! • Repair work on the devices must be performed only by R. STAHL Schaltgeräte GmbH.

Do not modify or alter the device!

9 Returning the device

Only return or package the devices after consulting R. STAHL!
Contact the responsible representative from R. STAHL. R. STAHL's customer service is available to handle returns if repair or service is required.

- Contact customer service personally. or
- Go to the r-stahl.com website.
- Under "Support" > "RMA", select "RMA -REQUEST".
- Fill out the form and send it. You will automatically receive an RMA form via email. Please print this file.
- Send the device along with the RMA form in the packaging to R. STAHL Schaltgeräte GmbH.

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

ID-Nr. 914760310070 S-SM-9147-01-en-06/2019