IS1+ I/O-Modules with “Plant-STOP”

Series 9469/35

9472/35

9475/32

9478/22

Contents

1 General Information

1.1 Manufacturer

R. STAHL Schaltgeräte GmbH
Am Bahnhof 30
74638 Waldenburg
Germany

Phone: +49 7942 943-0
Fax: +49 7942 943-4333
Internet: r-stahl.com
E-Mail: info@stahl.de

1.2 Information regarding the Safety manual

ID-No.: 168028 / 940060310010
Publication Code: 2019-05-15·SM00·III·en·00

Additionally to the Safety manual the following documents must be observed

- Operating instructions of the respective module:
  Universal Module HART 9469/35
  Digital Input Output Module 24 V 9472/35
  Digital Output Module 9475/32
  Digital Output Module Valve 9478/22

- Exida FMEDA Report of the respective module:
  Report No.: STAHL 15/05-054 R036 for 9469/35
  Report No.: STAHL 15/05-054 R037 for 9472/35
  Report No.: STAHL 13/04-027 R024 for 9475/32
  Report No.: STAHL 11/01-104 R021 for 9478/22

We reserve the right to make technical changes without notice.

1.3 Area of application

This Safety Manual applies to the Plant-STOP functionality of the following IS1+ I/O-modules:

IS1+ I/O-module	Hardware version	Firmware version
9469/35-08-12	Rev. A	not relevant for safety
9472/35-08-12	Rev. A	not relevant for safety
9475/32-04-12	Rev. B	not relevant for safety
9475/32-04-22	Rev. B	not relevant for safety
9475/32-04-72	Rev. B	not relevant for safety
9475/32-08-52	Rev. B	not relevant for safety
9475/32-08-62	Rev. B	not relevant for safety
9478/22-08-51	Rev. H	not relevant for safety

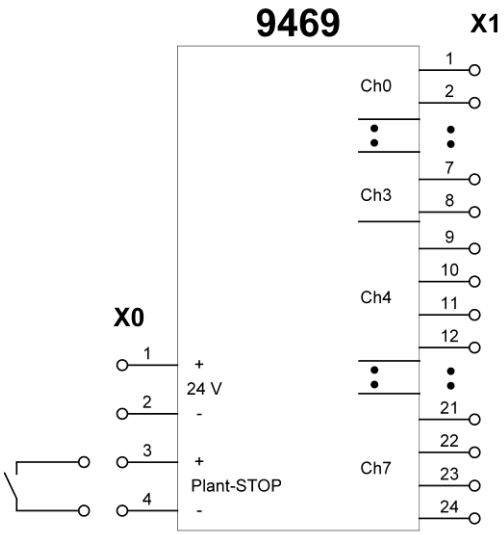
The Plant-STOP functionality is used for the safe switching off (= de-energize) of all the output signals of the respective module.
The safety function of the Plant-STOP can be used for example in safety process shutdown (PSD) applications in e.g. oil, gas or chemical industries. The Plant-STOP is suitable for low demand mode of operation.

1.4 Safety function

Depending on the respective I/O-module, the Plant-STOP functionality “all outputs OFF” is activated in three different operating modes:

1. Series 9469/35 and 9472/35 use a pluggable terminal X0 on front side of modules. Activation of Plant-STOP by disconnecting X0.1, X0.2 (via volt-free contact or switch).

Connecting diagram of the Plant-STOP 9469



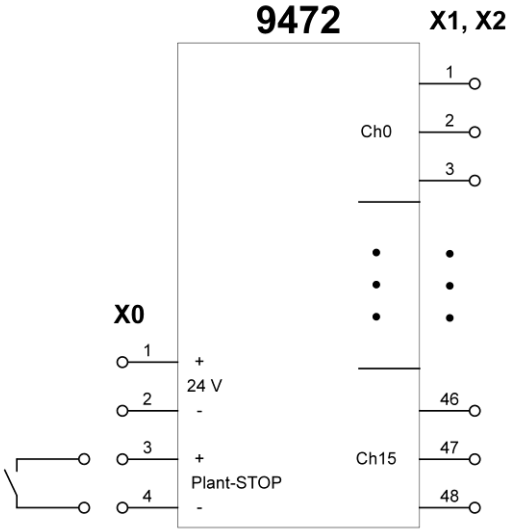
9469/35 Normal Operation

- Contact closed

9469/35 All outputs “OFF”

- Contact open

Connecting diagram of the Plant-STOP 9472



9472/35 Normal Operation

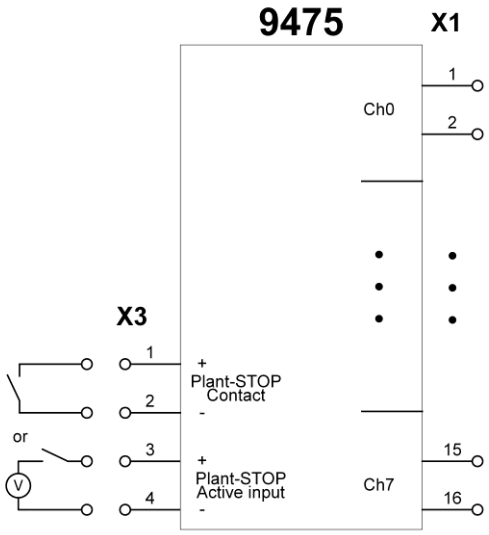
- Contact closed

9472/35 All outputs “OFF”

- Contact open

2. Series 9475/32 use a pluggable terminal X3 on backside of modules. Activation of Plant-STOP by either disconnecting X3.1, X3.2 (via volt-free contact or switch) or de-energizing X3.3, X3.4 (via active I.S. signal source).

Connecting diagram of the Plant-STOP 9475

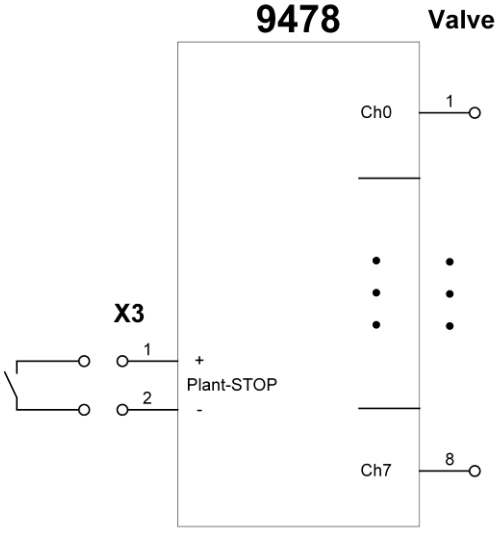


9475/32 Normal Operation
- Contact closed
- or active signal source is energized

9475/32 All outputs “OFF”
- Contact open
- or active signal source is de-energized

3. Series 9478/22 use a pluggable terminal X2 on backside of module. Activation of Plant-STOP by disconnecting X2.1, X2.2 (via volt-free contact or switch).

Connecting diagram of the Plant-STOP 9478



9478/22 Normal Operation
- Contact closed

9478/22 All outputs “OFF”
- Contact open

Safe state Plant-STOP: The fail-safe state is defined as all the outputs being de-energized.

1.5 Terms and Definitions

Automatic Diagnostics	Tests performed on line internally by the device or, if specified, externally by another device without manual intervention.
DC	Diagnostic Coverage of dangerous failures $(DC = \lambda_{DD}/(\lambda_{DD} + \lambda_{DU}))$
FIT	Failure In Time (1x 10^{-9} failure per hour)
FMEDA	Failure Modes, Effects and Diagnostic Analysis
HFT	Hardware Fault Tolerance A hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function.
High demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
Low demand mode	Mode, where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
MTBF	Mean Time Between Failures
$MTTF_d$	Mean Time To dangerous Failure
MTTR	Mean Time To Restoration
PFD_{AVG}	Average Probability of Failure on Demand
SIF	Safety Instrumented Function
SIL	Safety Integrity Level IEC 61508: discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. IEC 62061: discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest.
Type A element	"Non-complex" element (all failure modes are well defined); for details see 7.4.4.1.2 of IEC 61508-2
T[Proof]	Proof Test Interval

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 respective modules (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:

CAUTION
Risk due to operating the device!

- Ensure, that the mean time to restoration (MTTR) after a safe failure is ≤ 24 hours.
- Connect the Plant-STOP input of the module to a SIL compliant safety device.
- Ensure that only authorized personal has access to the set-up of the device.
- For 9469/35: ensure that a leakage signal ≤ 1.5 mA / 5.3 V (for 4-wire output)
- or ≤ 0.1 mA / 5.3 V (2-wire output) is uncritical for the safety application.
- For 9472/35: ensure that a output leakage signal ≤ 1.5 mA / 5.3 V is uncritical for the safety application
- For 9475/32: ensure that a output leakage current ≤ 200 µA is uncritical for the safety application
- For 9478/22: ensure that air is permanently supplied (either direct or by any air accumulator) and that clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for instrument air. Manual override shall not be used for safety application.

If you have questions:

- Contact the manufacturer.

3 Characteristics for the Functional Safety

Confirmation of meeting the requirements of IEC 61508 is done by FMEDA reports of Exida (see 1.2), download available from r-stahl.com. The failure rate of the Plant-STOP function is calculated by an FMEDA. The failure modes used in this analysis are from the Exida Electrical Component Reliability Handbook at a mean temperature of 40 °C and a MTTR of 24 hours. The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500.

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 Plant-STOP function 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.

For detailed information see Exida FMEDA Report of the respective module.

	T_{Proof}				
PFD_{AVG}	1 year	2 year	5 year	10 year	15 year
9469/35, 2-wire out	4.98 E-05	9.51 E-05	2.31 E-04	4.58 E-04	
9469/35, 4-wire out	3.39 E-05	6.47 E-05	1.57 E-04	3.11 E-04	
9472/35	5.42 E-05	1.04 E-04	2.52 E-04	4.98 E-04	
9475/32	2.29 E-04	3.34 E-04	6.62 E-04	1.20 E-03	1.74 E-03
9478/22	1.47 E-03	2.16 E-03	4.24 E-03	--	--

	Failure rates (in FIT)		
Failure category	9469/35, 2-wire out	9469/35, 4-wire out	9472/35
Fail Safe Undetected (λ_{SU})	17	19	47
Fail Safe Detected (λ_{SD})	0	0	0
Fail Dangerous Detected (λ_{DD})	0	0	0
Fail Dangerous Undetected (λ_{DU})	10	7	11
Total failure rate (safety function)	27	26	58
Safe failure fraction (SFF)	61%	73%	80%
SIL AC	SIL2	SIL2	SIL2

	Failure rates (in FIT)		
Failure category	9475/32 X3.1 - 3.2	9475/32 X3.3 - 3.4	9478/22
Fail Safe Undetected (λ_{SU})	58	83	146
Fail Safe Detected (λ_{SD})	0	0	0
Fail Dangerous Detected (λ_{DD})	34	34	30
Fail Dangerous Undetected (λ_{DU})	28	28	176
Total failure rate (safety function)	120	145	352
Safe failure fraction (SFF)	76%	80%	--
SIL AC	SIL2	SIL2	--

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-02.

3.2 Assumptions

Useful Lifetime	10 years
Hardware structure	1oo1D
MTTR	24 hours
Ambient temperature	-40 °C … + 75 °C (0 °C … + 60 °C for 9478) For average operation temperatures higher than 40 °C, the failure rates should be multiplied with an experience based factor of 1.5 (< 50 °C), 2.5 (< 60 °C), 5 (< 80 °C),
Storage temperature	-40 °C … + 80 °C (-20 °C … + 65 °C for 9478)
Transport temperature	-40 °C … + 80 °C (-20 °C … + 65 °C for 9478)

The following assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Plant-STOP function of all modules:

- Failure rates are constant, wear out mechanisms are not included.
- Propagation of failures is not relevant.
- The Plant-STOP 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 analyzed.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage (DC) provided by the automatic diagnostics.
- The Plant-STOP is operated in the low demand mode of operation.
- External power supply failure rates are not included.
- For safety applications only the described variants are considered.
- Only the Plant-STOP function of the modules was considered. The controller part is decoupled from the signal path and thereby not part of the safety function.
- Only one output is part of the considered safety function. The other outputs are assumed to be identical.

The following additional assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Plant-STOP function of **9469/35**

- Leakage signals ≤ 1.5 mA / 5.3 V (for 4-wire output) or ≤ 0.1 mA / 5.3 V (2-wire output) are assumed to be uncritical and thereby safe failures

The following additional assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Plant-STOP function of **9472/35**

- Leakage signals ≤ 1.5 mA / 5.3 V are assumed to be uncritical and thereby safe failures

The following additional assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Plant-STOP function of **9475/32**

- Leakage currents ≤ 200 µA are assumed to be uncritical and thereby safe failures

The following additional assumptions have been made during the Failure Modes, Effects and Diagnostic Analysis of the Plant-STOP function of **9478/22**

- Materials are compatible with process conditions and process fluids
- Air is permanently supplied (either direct or by any air accumulator)
- Breakage or plugging of air inlet and outlet line has not been included in the analysis
- Manual override must not be used for safety application
- Clean and dry operating air is used per ANSI/ISA-7.0.01-1996 Quality Standard for instrument air
- The module has a minimum distance of 5 mm from other ferromagnetic materials in order to avoid malfunctioning during operating conditions.

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 respective module.
- 9478/22 has a minimum distance of 5 mm from other ferromagnetic materials in order to avoid malfunctioning during operating conditions

5 Indications

The following LEDs are indicating the activated status of the Plant-STOP:

	Color	9469/35 9472/35	9475/32	9478/22
LED “ERR”	red	flashing	flashing	flashing
LED “24 V”	green/yellow	Yellow ON	n/a	n/a
LED ch.15	yellow	n/a	ON	n/a

The indication LEDs and the status information via the bus communication are not considered in FMEDA reports.

For detailed information about the status of all other LEDs, see respective Operating instruction.

6 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

For 9469/35, 9472/35 and 9475/32:

1. Bypass the safety function and take appropriate action to avoid a false trip
2. Force the module to go to the safe state by activating the Plant-STOP function and verify that the safe state is reached:
   a. Measure the output signal and compare values with chapter 2.1
   b. Compare the status of the LEDs with chapter 6
3. Restore the loop to full operation.
4. Remove the bypass from the safety PLC or otherwise restore normal operation.

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

For 9478/22:

1. Bypass the safety function and take appropriate action to avoid a false trip
2. Force the module to go to the safe state by activating the Plant-STOP function and verify that the safe state is reached.
   a. Compare the status of the LED with chapter 6
3. Inspect the device for any visible damage or contamination
4. Remove the bypass from the safety PLC or otherwise restore normal operation.

This test will detect approx. 90% of possible “du” failures.

7 Repair work

WARNING
Danger due to improper repair!

- The device must be repaired only by the manufacturer!

No changes to the device are permitted!