Special Documentation
Overfill Prevention System SOP600

Functional Safety Manual

Endress+Hauser
People for Process Automation

Table of contents

Declaration of Conformity

SIL-Konformitätserklärung
SIL Declaration of Conformity

Endress+Hauser
People for Process Automation

Company	**Endress+Hauser** **Process Solutions AG , Christoph Merian-Ring 12, CH-4153 Reinach** erklärt als Hersteller in alleiniger Verantwortung, dass das Produkt declares as manufacturer under sole responsibility, that the product
Product	**Overfill Prevention System** SOP600
Regulations	für den Einsatz in Schutzeinrichtungen entsprechend der IEC 61511:2003 unter den unten genannten Bedingungen geeignet ist. is suitable for the use in safety-instrumented systems according to IEC 61511:2003 under the below mentioned conditions
Safety Functions	MOPS- Manual Overfill Prevention System AOPS – Automatic Overfill Prevention System Mode: Low demand SIL: 3
Certification includes:	Management of functional safety Safety requirements specification Hardware requirements Reliability requirements Logic requirements User documentation Factory Acceptance Testing

Reinach, 2016-10-31
Endress+Hauser Process Solutions AG

Dr. Rolf Birkhofer
Managing Director

Felix Kraft
Department Manager Controlling

1/1

Safety-related characteristic values

Characteristics as per IEC 61511		
Features of MOPS		
Mission time:	1 year	1 year
Proof test interval:	1 year	1 year
MTTR:	72 hour	72 hour
Common cause:	5 %	5 %
Sensor:	FTL8x and FTL825	Liquiphant M/S, FEL57 and FTL325P
PFD_{avg}:	2.23E-04	8.04E-04
% SIL2:	2.2 %	8.0 %
% SIL3:	22 %	Not permitted
Features of AOPS [1)]		
Mission time:	1 year	1 year
Proof test interval:	1 year	1 year
MTTR:	72 hour	72 hour
Common cause:	5 %	5 %
Sensor:	FTL8x and FTL825	Liquiphant M/S, FEL57 and FTL325P
PFD_{AVG}:	3.29E-05	6.13E-04
% SIL2:	0.3 %	6.13 %
% SIL3:	3 %	Not permitted

1) The PFD_{avg} value for the AOPS is calculated without the actuators. The PFD_{avg} value of the AOPS is calculated without actuators. It is the responsibility of the end user to recalculate the PFDavg of the complete safety functions including actuators to demonstrate compliance with the applicable SIL level according to IEC 61511 or to request full certification based on the end user's final configuration.

Useful lifetime of electric components

The useful lifetimes of the individual components apply, see the **Supplementary device documentation** section. → 🖹 9

Certificate

The Type Approval Certificate is a safety certificate that has been issued by Risknowlogy for the Overfill Prevention System (OPS) developed by Endress+Hauser Process Solutions AG.

The Type Approval Certificate has been issued for the standard OPS system developed by Endress+Hauser Process Solutions AG. The standard OPS prevents the overfilling of up to 16 tanks in a tank farm. This OPS offers superior safety compliance (up to SIL3 according to IEC 61511) particularly for the oil, gas and chemical industry.

An additional System Approval Certificate for customized versions of the standard OPS can also be issued on completion of a Safety Site Acceptance Test (SSAT).

RISKNOWLOGY®

Certificate of Compliance

Safety Instrumented System

Holder:	Endress+Hauser Process Solutions AG
Safety Instrumented System:	OPS
Basis of Certification:	IEC 61511:2003
Certification Include(s):	☑ Management of functional safety ☑ Safety requirements specification ☑ Hardware requirements ☑ Reliability requirements ☑ Logic requirements ☑ User documentation ☑ Factory Acceptance Testing
Functional Safety Data:	
Safety functions	MOPS - Manual Overfill Prevention System AOPS - Automatic Overfill Prevention System
Mode	Low demand
SIL	3

Certification Results:

Risknowlogy certifies that the above Safety Instrumented System meets the requirements of the Basis of Certification for the selected assessment(s). The Risknowlogy report 211.259.5 and safety manual are an integral part of this certificate.

Certificate Number:	211.259.6
Issue Date:	2016-04-04
Expiry Date:	After modification of Safety Instrumented System

Certifier:

Document information

Document function

The document is part of the Operating Instructions and serves as a reference for application-specific parameters and notes.

- General information about functional safety: SIL
- General information about SIL is available in the Download Area of the Endress+Hauser website: www.de.endress.com/SIL

Using this document

This document describes the safety-related components and the safety-related operation of the system, and is used in conjunction with the documents listed in the **Supplementary device documentation** section. → 9

Symbols used

Safety symbols

Symbol	Meaning
DANGER	**DANGER!** This symbol alerts you to a dangerous situation. Failure to avoid this situation will result in serious or fatal injury.
WARNING	**WARNING!** This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in serious or fatal injury.
CAUTION	**CAUTION!** This symbol alerts you to a dangerous situation. Failure to avoid this situation can result in minor or medium injury.
NOTICE	**NOTE!** This symbol contains information on procedures and other facts which do not result in personal injury.

Symbols for certain types of information

Symbol	Meaning
	**Permitted** Procedures, processes or actions that are permitted.
	**Preferred** Procedures, processes or actions that are preferred.
	**Forbidden** Procedures, processes or actions that are forbidden.
	**Tip** Indicates additional information.
	Reference to documentation
	Reference to page
	Reference to graphic
	Visual inspection

Software symbols

Symbol	Function	Meaning
	Login	Opens the dialog box for user login/logout
	Lamp Test	Opens the **Lamp/Horn-Test** screen
	Proof Test	Opens the **Proof-Test** screen
	Settings	Opens the **Settings** screen
	Alarms	Opens the **Alarm** screen
	Logout	Logout (the DEFAULT user is logged in automatically)
	Password	Opens the **Standard Panel Password Input** dialog box
	History	Opens the **History** screen (only users with **Operator** and **Administrator** roles)
	Module Status	Opens the **Safety I/O Module Status** screen
	Reset	Resets the safety relays (same function as door button)
	Ack. All	Acknowledge all the warnings and alarms (same function as door button)
	Ack.	Acknowledge a single warning or alarm that has been selected
	Arrow keys	Scroll up or down
	Keys with double arrows	Scroll up or down a page
	Close	Closes the window
	Yes	Notification that the check was successful
	No	Notification that the check was not successful
	Next	Opens the next screen
	Print	Opens a new screen with a white background
	Start	Opens the **Step 1** screen and starts the proof test (High-High Level transmitter)
	Cancel	Cancels the operation
	Repeat	Repeats the operation

Symbol	Function	Meaning
	Tank Sett.	Opens the **Tank Settings** screen
	Date/Time	Opens the **Date/Time** dialog box
	Test Time	Opens the **Proof-Test Time** dialog box
	License Key	Opens the **License Key** dialog box
	Remote	Opens the **Remote Modem** dialog box
	Events	Opens the **Log File** screen
	System Info	Opens the **System Info** screen
	Apply	Applies the changes made to the settings
	Enable	Enables the remote maintenance modem (after confirming with **Apply**)
	Disable	Disables the remote maintenance modem (after confirming with **Disable**)
	Overview	Opens the **Overview** screen
	Proof-Test	Opens the **Proof-Test** screen
	Lamp-Test	Opens the **Lamp-Test** screen
	Enable	Manually enable the corresponding component

Text emphasis

Emphasis	Meaning	Example
Bold	Keys, buttons, program icons, tabs, menus, commands	**Start → Programs → Endress+Hauser** In the **File** menu, select the **Print** option.
Angle brackets	Variables	<DVD drive>

Acronyms used

Acronyms	Meaning
AOPS	Automatic Overfill Prevention System
CST	Coordinated System Time
DC	Diagnostic Coverage
DI	Digital Inputs
DO	Digital Outputs
FAT	Factory Acceptance Test
FIFO	First In First Out
H	High Limit - Warning
HH	High-High Limit - Alarm
HMI	Human Machine Interface
MOPS	Manual Overfill Prevention System

Acronyms	Meaning
OPS	Overfill Prevention System
PLC	Programmable logic controller (PLC)
PTC	Proof Test Coverage
Remote I/O	Remote Input/Output and Control Interface
SAT	Site Acceptance Test
SFAT	Safety Factory Acceptance Test (factory acceptance test for safety functions)
SSAT	Safety Site Acceptance Test
UPS	Uninterruptible power supply
Safety signature	The PLC safety program is protected by a safety signature. If modifications are made to the safety program, the safety signature is reset (deleted). A new safety signature is generated automatically once the modifications are completed. Modifications can only be made by Endress+Hauser.
Safety lock	The PLC program is protected by a safety lock and a password. Modifications to the PLC program can only be made by Endress+Hauser.
Stack lights	Visual indicators for the user that signal the machine status or process events. Alarm light and warning light, flashing or steady on.

Registered trademarks

FactoryTalk®, RSLinx®, Studio 5000™ and all other Rockwell Software® products are registered trademarks of Rockwell Automation.

Microsoft®, Windows XP®, Windows 7®, Internet Explorer® and the Microsoft logo are registered trademarks of the Microsoft Corporation.

All other brand and product names are trademarks or registered trademarks of the respective companies and organizations.

Supplementary device documentation

Additional information and technical documents:

- for Endress+Hauser devices at: www.endress.com
- for third-party components on the DVD supplied

Documentation	Comment
Endress+Hauser	
BA01587S/04/EN	Operating Instructions for Overfill Prevention System SOP600
BA01038F/00/EN	Operating Instructions for Nivotester FailSafe FTL825
BA01037F/00/EN	Operating Instructions for Liquiphant FailSafe FTL8x
SD00350F/00/EN	Functional Safety Manual (SIL): Nivotester FailSafe FTL825/Liquiphant FailSafe FTL8x
KA00167F/00/A6	Brief Operating Instructions for Nivotester FTL 325
KA00147F/00/A6	Brief Operating Instructions for Liquiphant FTL5/7x
KA00143F/00/A6	Brief Operating Instructions for Liquiphant FTL5x
KA172F/00/A6	Brief Operating Instructions for Liquiphant FTL7x
SD111F/00/EN	Functional Safety Manual (SIL): Liquiphant FTL5x/7x/Nivotester FTL325P
Wiring drawing	Project-specific
Rockwell	
1768-um002_-en-p.pdf	User Manual for Compact GuardLogix Controllers 1768-L4xS

Documentation	Comment
1734-um013_-en-p.pdf	User Manual for POINT Guard I/O Safety Modules 1734-xxxS
440r-in042-mu-p.pdf	Installation Instructions for Guardmaster Safety Relay SI 440R-S12R2
Pfannenberg	
085501929.pdf	Operating Instructions for alarm siren DS5-SIL
085501930.pdf	Operating Instructions for alarm strobe Quadro F12-SIL
HIMA	
H4116-E.pdf	Operating Instructions for safety relay H4116

Permitted devices types

The details pertaining to functional safety in this manual relate to this system and are valid as of the specified software and hardware version. Unless otherwise specified, all the versions can also be used for safety functions. A modification process according to IEC 61511 is applied for any system modifications.

SIL label on the nameplate

SIL certified devices are marked with the following symbol on the nameplate: (SIL)

Safety function

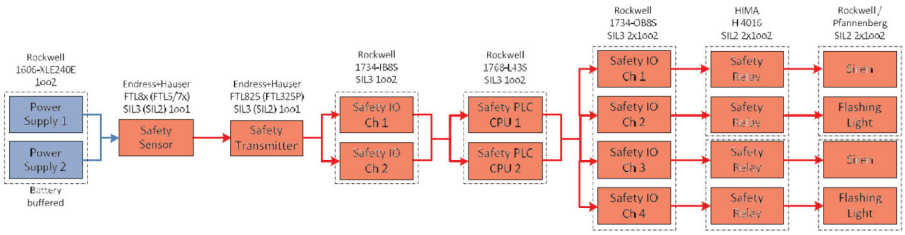
Definition of the safety function

The Overfill Prevention System is type-certified up to SIL 3 according to IEC 61511.

Safety function 1: Manual Overfill Prevention System (MOPS)

The level in the tank is measured. If a defined upper level is reached, control room signalization (strobe light and siren) and field signalization (strobe light and siren) are activated. The operator must take the appropriate safety measures.

This safety function is an **energize-to-trip** safety function and depends on the correct action on the part of the operator in the field.

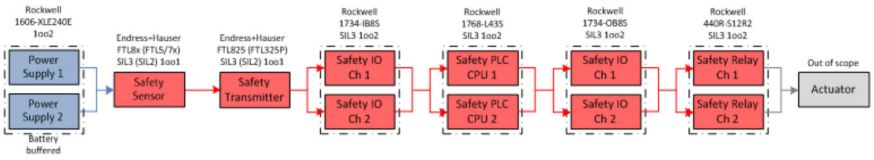


The components provided for this safety function are shown in red.

Safety function 2: Automatic Overfill Prevention System (AOPS)

The level in the tank is measured. If a defined upper level is reached, the safety relay is de-energized.

This safety function is a **de-energise-to-trip** safety function and depends on the correct action on the part of the connected actuator (e.g. valve and/or pump). The actuator is not included in the system delivery and is also not taken into account for SIL type certification.



The components provided for this safety function are shown in red.

Since this is a Safety Integrated System, only appropriately trained and authorized persons may make modifications to the system. All modifications to the hardware or software configuration must be agreed beforehand with Endress+Hauser Process Solutions AG.

You can contact service@solutions.endress.com or sales@solutions.endress.com for more support.

Restrictions for use in safety-related applications

The safety shutdown system connected to the safety relay and the actuator are not part of this system. They are plant-specific and are therefore the responsibility of the plant owner/operator.

Use in protective systems

System behavior during operation

System behavior during power-up

After power-up, the system goes through a boot sequence for the individual components.

The system behaves as follows during this time:

Safety relay (AOPS)	Terminals at relay	Open	Closed
Safety contact 1	13 <> 14	x	
Safety contact 2	23 <> 24	x	

Signalization		Color	On	Off	Flashing
Control room alarm stack light	Siren module	Black	x		
	Strobe module	Red			x
	Steady light module	Red	x		
Control room warning stack light	Buzzer module	Black	1)	1)	1)
	Lamp module	Amber	1)	1)	1)
	Steady light module	Green	1)	1)	1)
Field signalization (optional for AOPS)	Alarm strobe	Red			x
	Alarm siren	Red	x		

1) Depends on status of boot sequence

Once the system has fully booted (including the PLC and touch panel), the alarms can be acknowledged with the **Acknowledge all** door button and the safety components can then be reset with the **Reset safety device** door button. If no more alarms and warnings are active after this procedure, the system status is normal.

The system behaves as follows in the normal system state:

Safety relay (AOPS)	Terminals at relay	Open	Closed
Safety contact 1	13 <> 14		x
Safety contact 2	23 <> 24		x

Signalization		Color	On	Off	Flashing
Control room alarm stack light	Siren module	Black		x	
	Strobe module	Red		x	
	Steady light module	Red		x	
Control room warning stack light	Buzzer module	Black		x	
	Lamp module	Amber		x	
	Steady light module	Green	x		
Field signalization (optional for AOPS)	Alarm strobe	Red		x	
	Alarm siren	Red		x	

System behavior in safety function demand mode

As soon as the level limit being monitored is reached, the failsafe contacts on the safety relay (AOPS) open, and safety field signalization is activated (MOPS).

The system behaves as follows in the demand mode:

Safety relay (AOPS)	Terminals at relay	Open	Closed
Safety contact 1	13 <> 14	x	
Safety contact 2	23 <> 24	x	

Signalization		Color	On	Off	Flashing
Control room alarm stack light	Siren module	Black	x		
	Strobe module	Red			x
	Steady light module	Red		x	
Control room warning stack light	Buzzer module	Black		x	
	Lamp module	Amber		x	
	Steady light module	Green		x	
Field signalization (optional for AOPS)	Alarm strobe	Red			x
	Alarm siren	Red	x		

System behavior in event of alarms or warnings

The system behaves as follows in the event of an alarm:

Safety relay (AOPS)	Terminals at relay	Open	Closed
Safety contact 1	13 <> 14	x	
Safety contact 2	23 <> 24	x	

Signalization		Color	On	Off	Flashing
Control room alarm stack light	Siren module	Black	x		
	Strobe module	Red			x
	Steady light module	Red		x	
Control room warning stack light	Buzzer module	Black		x	
	Lamp module	Amber		x	
	Steady light module	Green		x	

Signalization		Color	On	Off	Flashing
Field signalization (optional for AOPS)	Alarm strobe	Red			x
	Alarm siren	Red	x		

The system behaves as follows in the event of a warning:

Safety relay (AOPS)	Terminals at relay	Open	Closed
Safety contact 1	13 <> 14		x
Safety contact 2	23 <> 24		x

Signalization		Color	On	Off	Flashing
Control room alarm stack light	Siren module	Black		x	
	Strobe module	Red		x	
	Steady light module	Red		x	
Control room warning stack light	Buzzer module	Black	x		
	Lamp module	Amber			x
	Steady light module	Green		x	
Field signalization (optional for AOPS)	Alarm strobe	Red		x	
	Alarm siren	Red		x	

Alarm and warning messages

Details of the alarm and warning messages are provided in:

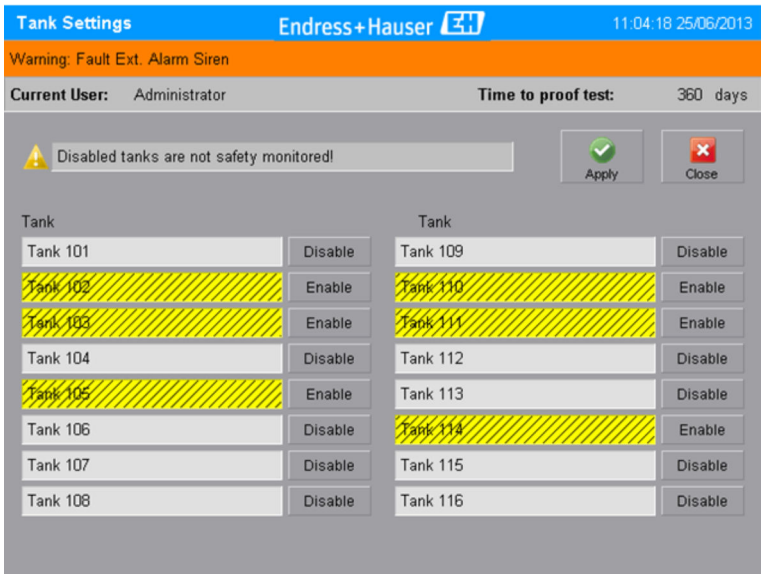
the **Diagnostics and troubleshooting** section of **Operating Instructions BA01587S/04/EN**

System configuration for safety-related applications

Configuration methods

Tank Settings:

The **Tank Settings** screen is used to enable and disable level monitoring and to assign the tank a name. The tank names can contain a maximum of 15 characters. If a tank is disabled, this means it is no longer monitored for safety alarms, failures or overly high levels of product. Disabled tanks are indicated by a specific color in the **Overview** screen. In addition, disabled tanks are also listed in the log file. All changes made on this screen only take effect once the **Apply** button is pressed. Disabled tanks are flagged as such **D (= Disabled)** in the proof test.



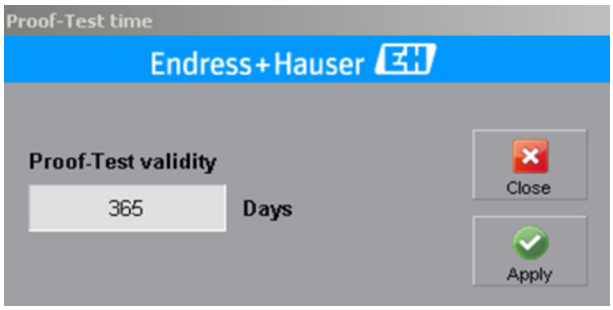
1 *Tank Settings screen*

WARNING

If a tank is disabled,
it is no longer monitored for safety alarms, failures and overly high levels of product.
► Disabled tanks may not be filled without additional safety measures.

Proof-Test Time:

The time between the required proof tests can be defined in this dialog box. In addition, the status bar also displays the time remaining until the next proof test. The time between two proof tests can range between 1 and 365 days. 365 days is the default setting. If the time for proof tests is exceeded, the **Warning: Proof-Test validity time expired** message is displayed. The timer starts counting down the days from the last successful proof test. Changing the time between two proof tests does not affect the current time remaining until the next test. All changes to the time to next test made here only take effect after the next successfully completed proof test. Perform a new proof test if the new time has to be activated immediately.



2 *Proof-Test time dialog box*

The customer is responsible for setting the time span between the individual proof tests (according to in-house standards or based on a risk analysis). The proof test must be performed at least once a year (every 365 days).

Proof-testing

In the proof test, all the safety-related components are checked automatically and a report is created.

It is advisable to perform the proof test at least once a year (every 365 days). However, the proof test can also be performed several times a year if necessary.

If one of the test criteria from the test sequences described below is not fulfilled, the device may no longer be used as part of a safety system. The purpose of proof-testing is to detect any device failures. The impact of systematic errors on the safety function is not covered by this test and must be assessed separately. Systematic errors can be caused, for example, by the properties of the process materials, operating conditions, deposit build-up or corrosion.

The components used must also undergo a periodic visual inspection (mechanical damage of components including cabling, leak-tightness). More information is provided in the **Safety documentation** for the components. → 9

More information on the **Proof-Test** screen:

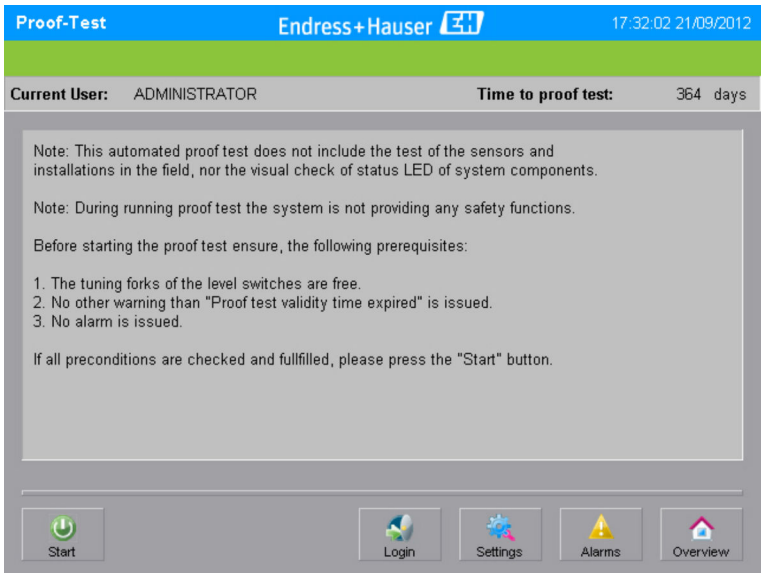
Operating Instructions BA01587S/04/EN

Structure of the proof test

The proof test comprises the start screen and 4 individual steps. Once the 4th step is finished, the **Report** screen opens and the proof test report is created.

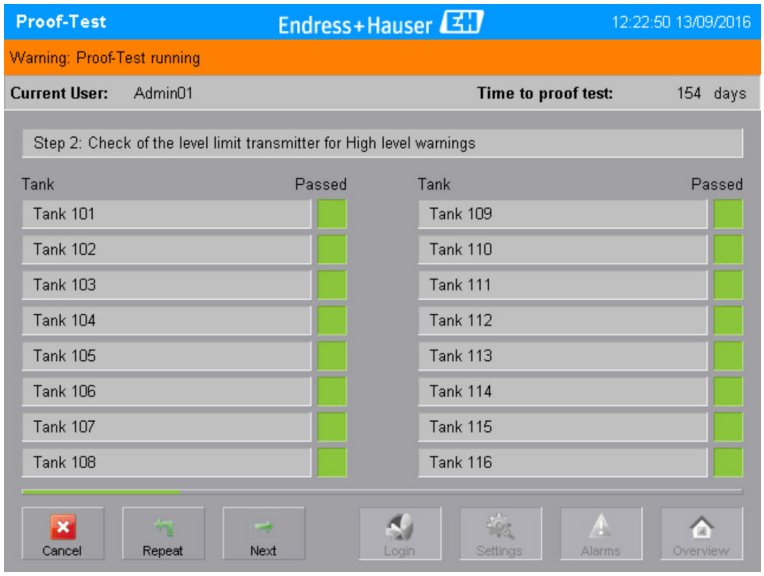
1. Check the High-High Level transmitters and the sensors of the enabled tanks. Check the safety relays of the enabled tanks.
2. Check the High Level transmitters and the sensors of the enabled tanks.
3. Check the general system status (power supply, PLC state, field signalization).
4. Check the visual and acoustic signals (interactive).

Proof test step 1



The first step is started via the start screen for the proof test (Proof-Test screen). Read all the information and instructions carefully. Press **Start**. The timer starts and runs for a maximum period of 10 minutes.

The proof test must be completed within this time. Otherwise the test is canceled. A progress bar indicates how much time has passed.

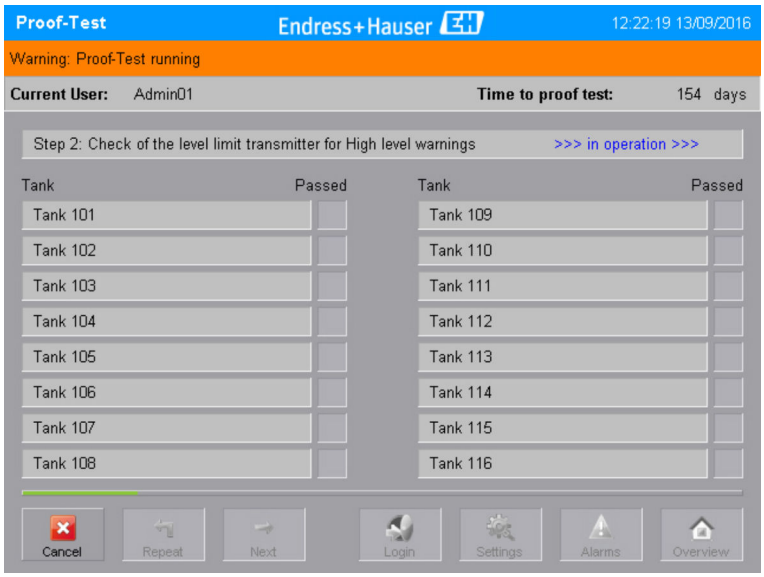


Step 1 of the proof test is performed according to **Test sequence B** in the **Functional Safety Manual SD00350F/00/EN for Nivotester FTL825** or according to the **Test phase** in the **Brief Operating Instructions KA00167F/00/A6 for Nivotester FTL325P**.

Functional Safety Manual SD00350F/00/EN

Brief Operating Instructions KA00167F/00/A6

Proof test step 2

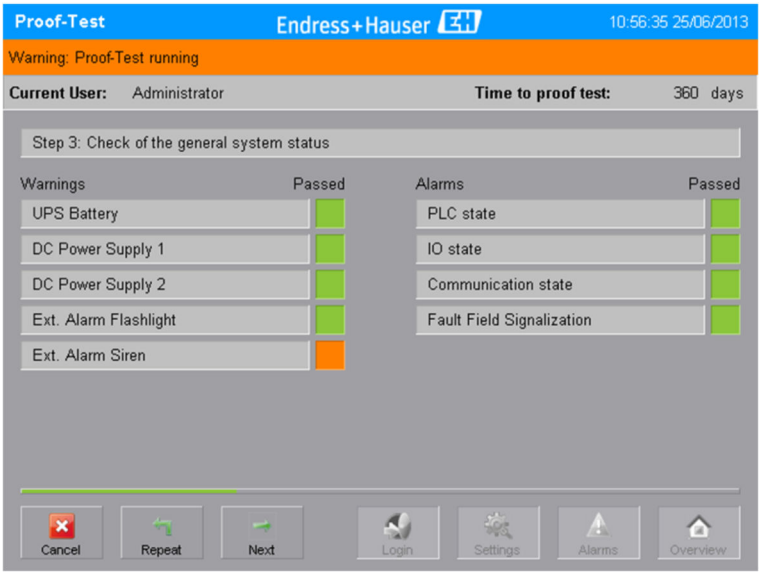


Step 2 of the proof test is performed according to **Test sequence B** in the **Functional Safety Manual SD00350F/00/EN for Nivotester FTL825** or according to the **Test phase** in the **Brief Operating Instructions KA00167F/00/A6 for Nivotester FTL325P**.

Functional Safety Manual SD00350F/00/EN

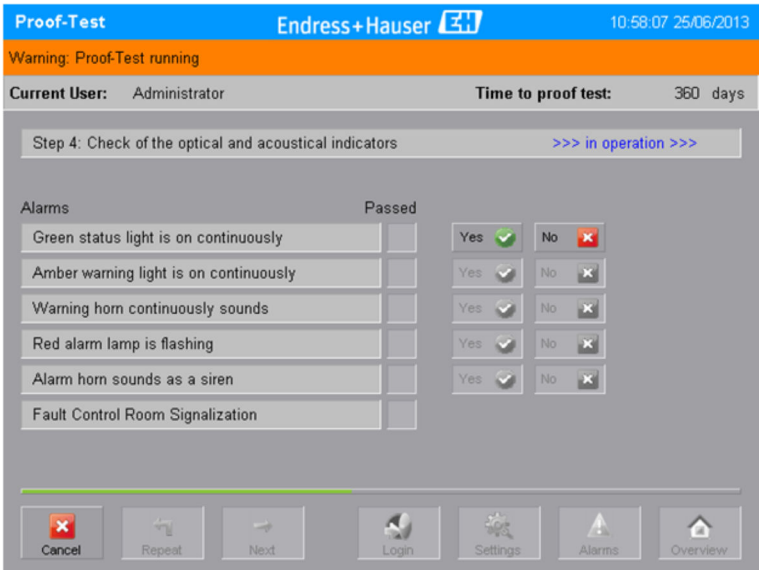
Brief Operating Instructions KA00167F/00/A6

Proof test step 3



Step 3 of the proof test checks the general system status of the elements listed in the screenshot above:

Proof test step 4



Each test performed in step 4 must be confirmed by clicking **Yes** or **No** as soon as the individual visual and acoustic checks are completed.

Proof test report

Once the 4th step of the proof test is completed and the **Next** button is pressed, the **Proof-Test Report** screen opens and creates a test report that is saved in a log file of the PLC. This test report can be printed out if a USB printer is connected to the system.

Successful completion of the proof test with and without warnings

The proof test can be completed successfully even if a warning was displayed during the test. If a warning is detected during the proof test, it is displayed immediately once the proof test is completed. If a proof test has been completely successfully (without any alarms), the remaining time to the next proof test is reset to the preset value.

Proof test completed with alarms

If an alarm occurs during the proof test, the proof test fails and the alarms are displayed immediately once the proof test is completed. If the proof test has not been passed, the remaining time until the next test is not reset.

Alarm

An alarm is displayed if the proof test was not passed. This alarm activates the alarm strobe and the alarm siren on the control cabinet and the external alarm strobe and the external alarm siren in the field and writes an entry in the log file.

Description of alarm:	Cause:	Troubleshooting:
Proof-Test failed	An alarm was detected during the proof test.	Check the test report to determine which component caused the alarm. Information on how to rectify faults in faulty components is provided in these Operating Instructions.

Life cycle

Requirements for the personnel

Since this is a Safety Integrated System, any persons making modifications to the system must have appropriate training and authorization. All modifications to the hardware or software must be agreed beforehand with your Endress+Hauser sales center at www.addresses.endress.com.

Installation

Information about installing the system:

Operating Instructions BA01587S/04/EN

Commissioning

Information about installing the system:

Operating Instructions BA01587S/04/EN

Before the system is used as a safety function, it is essential to perform a successful proof test once the system has been successfully installed (incl. installation check).

Operation

Information about installing the system:

Operating Instructions BA01587S/04/EN

Logging on at the touch panel

You must log on as an administrator to be able to change safety-related settings in the HMI screens of the touch panel.

Information about installing the system:

Operating Instructions BA01587S/04/EN

Maintenance

In addition to the (functional) proof test, which must be performed periodically, the components must also be visually inspected periodically. Endress+Hauser also offers its customers Maintenance Agreements and Software Level Agreements for this.

Repairs

All device repairs may only be performed by Endress+Hauser. The safety functions can no longer be guaranteed if repairs are made by persons other than Endress+Hauser staff.

Exception:

Customers may themselves exchange the following components of the measuring system provided that original E+H spare parts are used, the customer's technician responsible for replacing the component has been appropriately trained for this task by Endress+Hauser and the relevant installation instructions have been observed.

The customer may replace the following safety-related components with original E+H components of the same type:
- Liquiphant FTL5x/FTL7x/FTL8x
- Nivotester FTL825/FTL325P
- Safety digital input module 1734-IB8S (only **out of the box** parts (never previously used))
- Safety digital output module 1734-OB8S (only **out of the box** parts (never previously used))
- Safety relay SI 440R-S12R2 or H4116
- Alarm siren DS5-SIL
- Alarm strobe Quadro F12-SIL

In the case of the following safety-related components, customers may replace the spare parts listed below with corresponding original E+H spare parts:

Nivotester FTL825/safety relay H4116:
Fuses with holder (bayonet lock)

Liquiphant FTL5x/FTL7x/FTL8x:
- Cover
- Cover seal
- Cable gland
- Electronic insert FEL85 (FTL8x)
- Electronic insert FEL57 (FTL5x/FTL7x)

WARNING

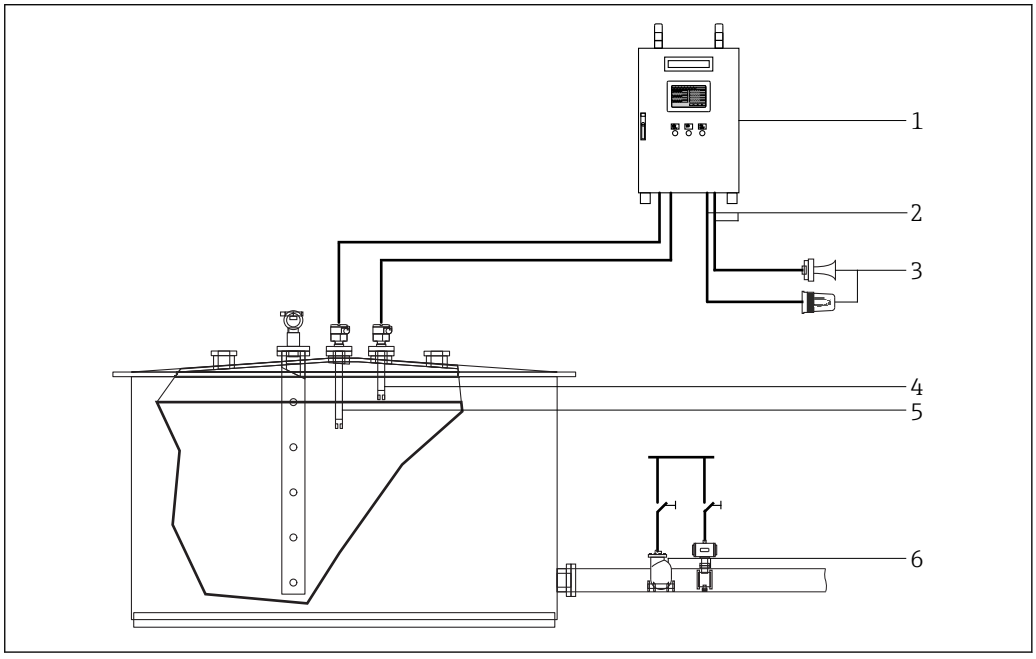
If the replacement component is defective or incorrectly installed,
the safety function can no longer be guaranteed.
▶ A proof test must be performed once the component has been replaced.

- The replaced components must be sent to Endress+Hauser for fault analysis.
- Corresponding original parts can be purchased from Endress+Hauser

Appendix

Structure of the measuring system

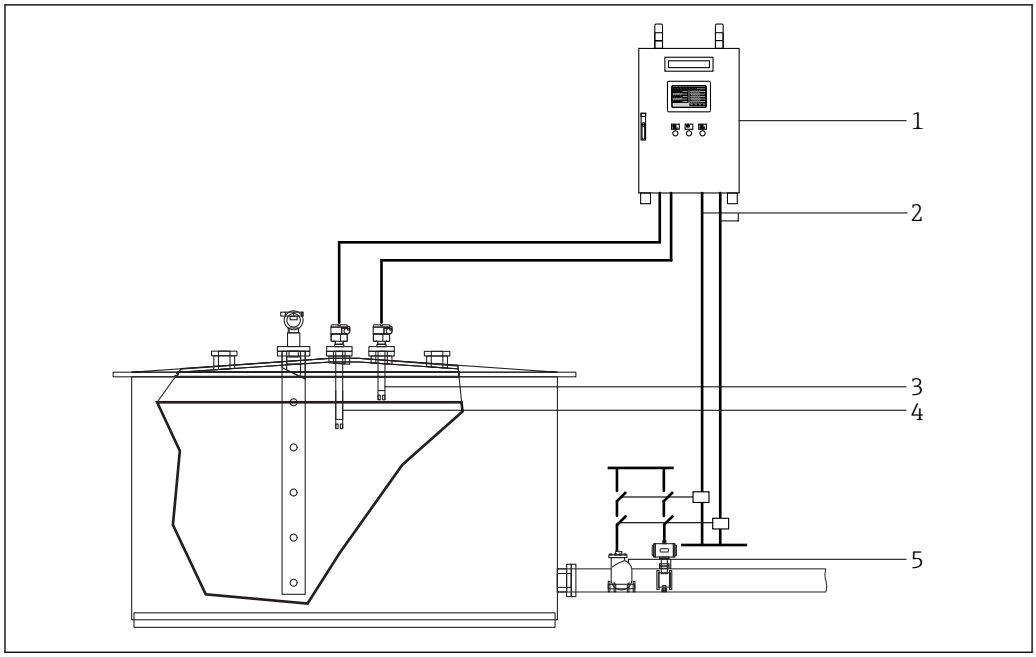
Manual Overfill Prevention System (MOPS)



3 *Manual Overfill Prevention System (MOPS) - overview*

1 *Cabinet for Overfill Prevention System*
2 *Safety relay output*
3 *Field signaling*
4 *Sensor, High-High alarm*
5 *Sensor, High warning*
6 *Actuator to be disabled manually*

Automatic Overfill Prevention System (AOPS)

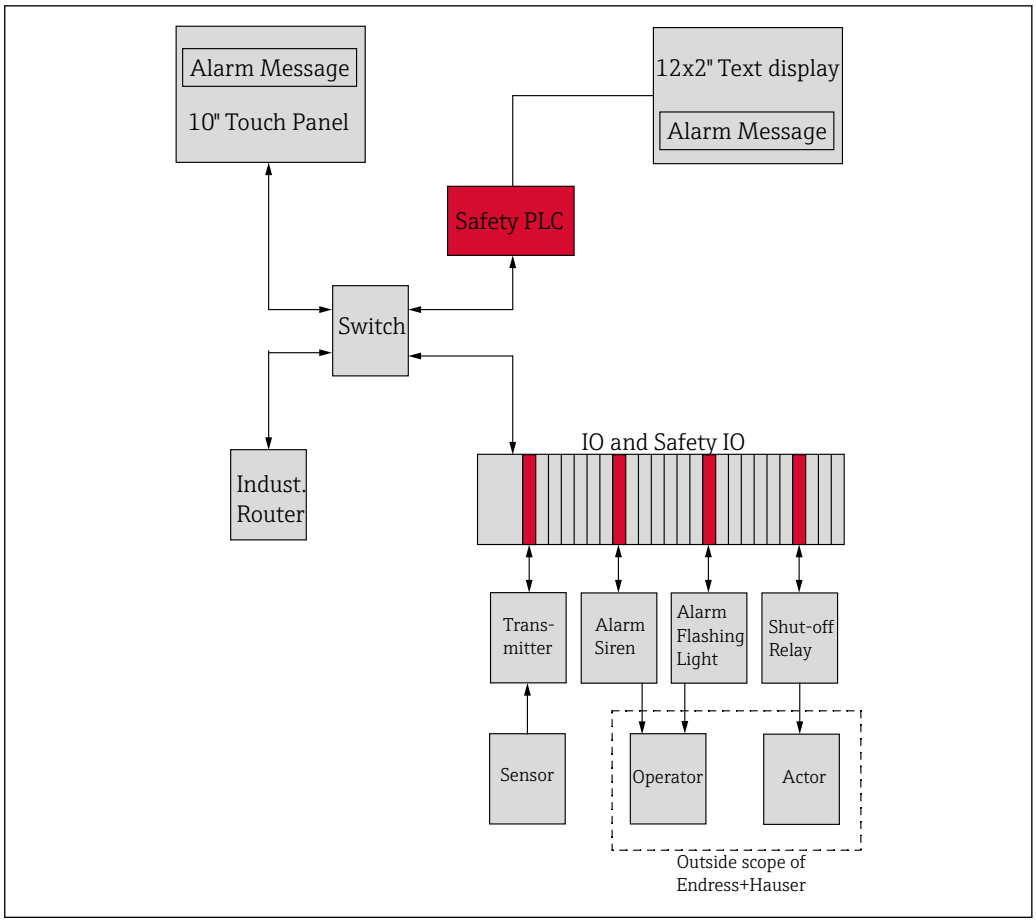


4 *Automated Overfill Prevention System (AOPS) - overview*

1 Cabinet for Overfill Prevention System
2 Safety relay output
4 Sensor, High-High alarm
5 Sensor, High warning
6 Automatically disabled actuator

System components

The overview of the control system is divided into non-safety-related components (gray) and safety-related components (red).



Safety PLC	Rockwell 1768-L43S
Safety I/O	Rockwell 1734-IB8S / 1734-OB8S
Transmitter for point level switch	Endress+Hauser Nivotester FTL825 (SIL3) or FTL325P (SIL2)
Safety point level switch	Endress+Hauser Liquiphant FTL81 (SIL3) or FTL5/7x (SIL2)
Safety relay	Rockwell GuardMaster 440R-S12R2 (optional for MOPS)
Safety relay	HIMA H4116 (for field signalization)
Alarm strobe	Pfannenberg Quadro F12-SIL (optional for AOPS)
Alarm siren	Pfannenberg DS5-SIL (optional for AOPS)

Description of use as a protective system

Safety PLC

The safety PLC communicates with the safety I/O modules and the touch panel.

The safety PLC comprises:
- Power supply (not illustrated below)
- Ethernet module (bottom left in the graphic)
- Safety CPU (bottom right in the graphic)

Name	Manufacturer	Version (indicated under Properties in the PLC module)
1768-L43S PLC	Rockwell	20.013 (20.13)

For all the status indicators listed below, the green light must be switched on and the key switch must be in the RUN position in order to confirm that all the safety conditions are met.

For more information, please refer to the Rockwell User Manual 1768-um002_-en-p.pdf

Status indicator		Description
PWR	Green	The controller is providing power to 1768 modules in the system.
	Red	The power supply is not producing valid 24V power to the 1768 modules.
	Off	The power supply is turned off, lacks adequate input power, or has failed.
I/O PWR	Off	Either the controller or the power supply is not operating properly.
	Green	The controller is operating properly.
	Flashing red/ green or solid red	An end cap or 1769 I/O module is not properly attached.
RUN	Off	The controller is in Program or Test mode.
	Green	The controller is in RUN mode.
I/O	Off	There are no devices in the I/O configuration of the controller or the controller does not contain a project.
	Green	The controller is communicating with all of the devices in its I/O configuration.
	Flashing green	One or more devices in the controller's I/O configuration are not responding.
	Flashing red	The controller is not communicating with any of the devices in its I/O configuration.
OK	Off	No power is applied. If the MEM SAVE indicator is green, the user program and configuration data are being saved to the non-volatile memory.
	Flashing red	The controller requires a firmware update or a firmware update is in progress. A recoverable major fault occurred in the controller. A non-recoverable major fault occurred in the controller.
	Red	The controller detected a non-recoverable major fault and cleared the project from memory.
	Green	Controller is OK.
	Flashing green	The controller is storing or loading a project to or from the non-volatile memory.

Status indicator		Description
SAFETY RUN	Off	The user safety task or safety outputs are disabled. The controller is in the PROG mode, Test mode or the safety task is faulty.
	Green	The user safety task and safety outputs are enabled. The safety task is executing. The safety task signature is present.
	Flashing green	The user safety task and safety outputs are enabled. The safety task is executing. The safety task signature is not present.
SAFETY TASK	Off	No partnership established.
	Green	Safety controller status is "OK". The coordinated system time (CST) is synchronized and safety I/O connections are established.
	Flashing green	Safety controller status is "OK". The coordinated system time (CST) is not synchronized.
	Red	The safety partnership was lost.
	Flashing red	The safety task is inoperable.
SAFETY LOCK	Off	The safety task is not locked.
	Green	The safety task is locked.
SAFETY OK	Off	No power is applied.
	Green	The safety partner is OK.
	Flashing green	The safety partner is storing or loading a project to or from non-volatile memory.
	Red	The safety partner detected a non-recoverable major fault and cleared the project from its memory.
	Flashing red	The internal safety partner requires a firmware update, or a firmware update is in progress. A recoverable major fault occurred in the safety partner. A non-recoverable major fault occurred in the safety partner.

Errors in the PLC and in communication trigger an alarm event. The alarm activates the alarm signalization lamp (strobe light and siren) in the control room and the field signalization system (strobe light and siren) and writes an entry in the log file.

Information on diagnostics and troubleshooting:

Operating Instructions BA01587S/04/EN

The safety PLC is supplied with a unique safety signature and is locked (status indicator **SAFETY LOCK** is on). The safety signature is displayed on the **System Info** HMI screen. If the safety signature is changed or if the safety PLC is not locked, Endress+Hauser is no longer responsible for the safety functionality of the Overfill Prevention System (OPS).

WARNING

If a PLC or communication error occurs, or if the CPU switches to the Stop mode owing to a critical error,
the system does not alert the user to potential overfilling.
- ▶ Stop product being filled into the tank.

Safety I/O modules

The Rockwell Point I/O safety modules 1734-IB8S are connected to the Nivotester FTL825 or FTL 325P. The safety output modules 1734-OB8S are connected to the Rockwell GuardLogix 440R safety relay.

Name	Manufacturer	Version (indicated under Properties in the PLC module)
1734-IB8S Series B Point I/O Safety DI module	Rockwell	2.002 (2.2)
1734-OB8S Series B Point I/O Safety DO module	Rockwell	2.002 (2.2)

The table below lists the status indicators on the Rockwell I/O module, series 1734-IB8S or 1734-OB8S respectively. For all the status indicators listed below, the green light must be switched on; it confirms that all the safety conditions are met. The yellow lights 0–7 on the I/O modules indicate whether the individual input or output is switched on. In the normal system state, the inputs/outputs must be active for each of the connected tanks.

For more information, please refer to the Rockwell User Manual 1734-um013_-en-p.pdf provided on the DVD supplied.

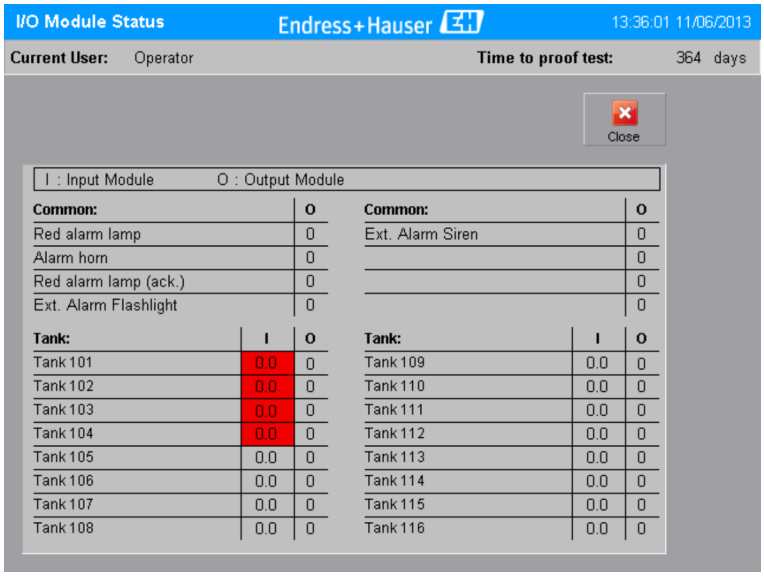
Indicator		Description
MS	Off	No power is applied to the module.
	Green	The module is operating normally
	Red	The module has detected an unrecoverable fault.
	Flashing green	Device is in **Idle** or Standby state.
	Flashing red	The module has detected a recoverable fault. User-initiated firmware update is in progress.
	Flashing red/ green	Module is not configured. The module is performing its power cycle diagnostic tests.
NS	Off	The module is not online with the network or there is no power.
	Flashing green	Module online with no connections in established state. The module identified the communication rate of the network but no connections are established.
	Green	Module online with connections in established state. The module is operating normally.
	Flashing red	One or more I/O connections is in timed-out state. User-initiated firmware update is in progress.
	Red	Critical link failure. The module detected an error that prevents it from communicating on the network, such as a duplicate node address.
PWR	Off	No field power applied.
	Green	Normal condition, field power supplied and within specification.
	Yellow	Field power out of specification.
0...7	Off	Safety input or output is off, or module is being configured.
	Yellow	Safety input or output is on.
	Red	A fault in the external wiring or input circuit has been detected.
	Flashing red	A fault in the partner input circuit of a dual-input configuration has been detected.

Errors in the I/O modules trigger an alarm event. The alarm activates the alarm stack light (strobe light and siren) in the control room and the field signalization system (strobe light and siren) and writes an entry in the log file.

For information on diagnostics and troubleshooting, see: **Operating Instructions BA01587S/04/EN**

WARNING

If an error occurs in the I/O module,
the system does not alert the user to potential overfilling.
- ▶ Stop product being filled into the tank.



Red background: error in corresponding module

Gray background: corresponding module is OK

Safety level sensor and transmitter

Liquiphant FTL8x and Nivotester FTL825 (1oo1 SIL3)

The High-High Level safety measuring system comprises a point level switch of the Liquiphant FTL8x FailSafe series and a transmitter of the Nivotester FTL825 FailSafe series. A level-dependent 4 to 20 mA signal is generated in the Liquiphant FTL8x sensor . The signal is read and monitored by the Nivotester FTL825 in order to determine whether the level exceeds or drops below a specific limit value.

Liquiphant FailSafe FTL80/81/85

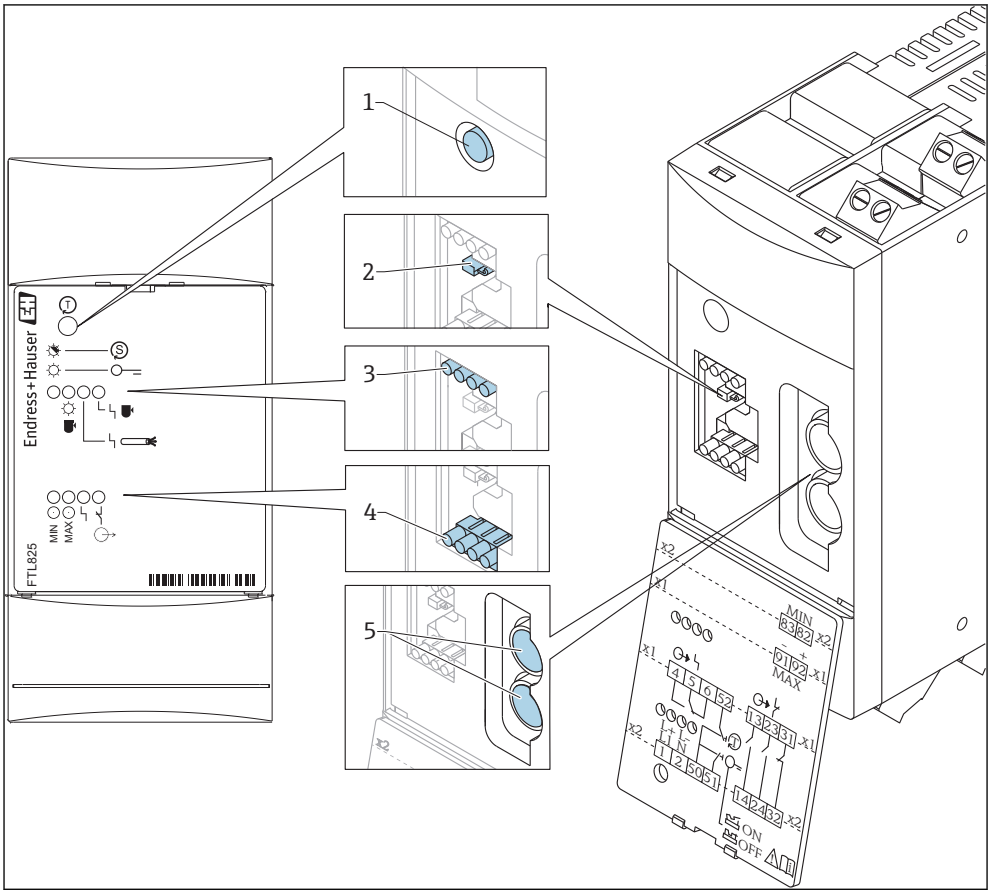
The Liquiphant FailSafe works as a safety-related point level switch and detects whether the tuning fork is covered or free. It outputs a current signal in accordance with NAMUR NE43 (4 to 20 mA).

Nivotester FailSafe FTL825

The Nivotester FailSafe acts as switching unit to monitor the input current and a dynamic signal (LIVE signal) that is transmitted by the Liquiphant FailSafe FTL8x. The two safety contacts are opened on demand or if errors are detected. In addition to the safety contacts opening, a signalling contact is also closed. A separate fault-signaling contact switches if a device error occurs. The sensor tuning fork vibrates at its intrinsic resonance frequency. The vibration frequency decreases as the density increases. This change in frequency causes the current signal to change. The purpose of the measuring system is to prevent the level of the product rising above a maximum level, i.e. it prevents overfilling. During normal operation, the fork is not covered by the liquid and the measuring system signals the status **OK**. If the tuning fork is covered by the liquid, the Nivotester switches to the fail-safe position and holds the demand mode.

Name	Manufacturer	Firmware from version	Electronics from version
Liquiphant FTL8x	Endress+Hauser	01.00.00	1.00
Nivotester FTL825	Endress+Hauser	01.00.00	1.00

Display and operating elements on the Nivotester FTL825

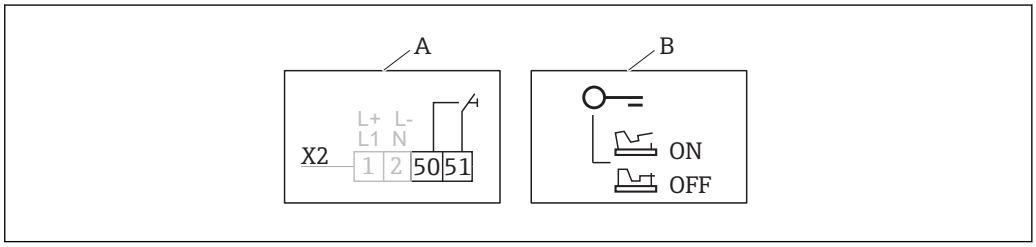


5 Operating and display element Nivotester FTL825

Operating elements
- 1: Test button (T)
- 2: Lock switch

Indicator element: light emitting diodes (LEDs)
- 3: LEDs (from left)
  - LIVE signal (flashing yellow) and lock switch (lit yellow)
  - Sensor covered (yellow)
  - Wiring error (red)
  - Liquiphant error (red)
- 4: LEDs (from left)
  - MIN detection mode (green)
  - MAX detection mode (green)
  - Nivotester error (red)
  - Safety contact closed (yellow)

Fuses
5: Two replaceable fuses for the two safety contacts (3.15 A; T; 250 V; design 5x20)



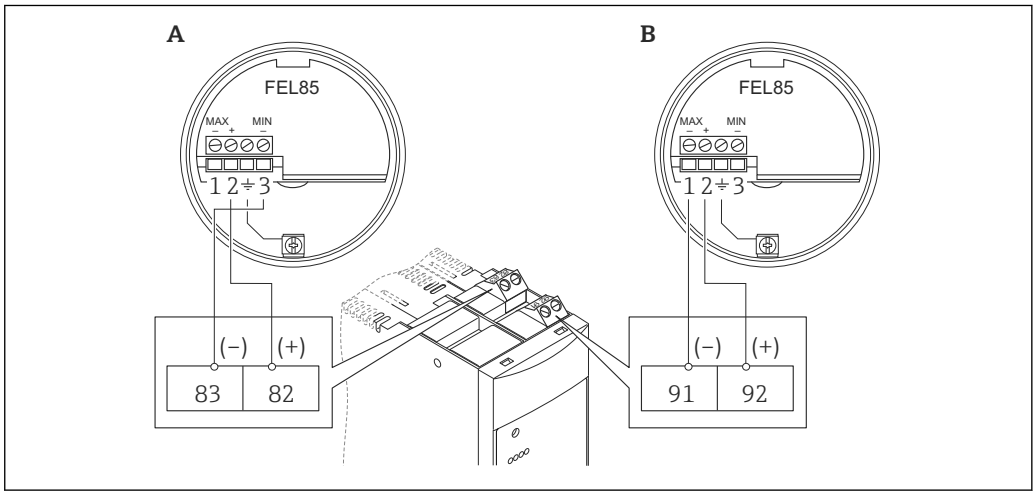
A Button to acknowledge a demand in the locked state
B Configuration with lock switch (ON/OFF)

Lock switch **B** must be in the **OFF** position.

Safe operating mode

The **MAX** operating mode (overfill prevention) is the safety mode used. The output switches in a safety-oriented manner when the probe is covered (demand).

On the Nivotester FTL825, the Liquiphant FTL8x is connected to terminals 91 and 92.



A MIN fail-safe mode
B MAX fail-safe mode

Terminal on the Liquiphant FailSafe			Terminal on the Nivotester FailSafe FTL825			
1	2	3	83	82	91	92
-	+	Open	Open	Open	-	+

MAX operating mode:

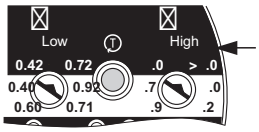
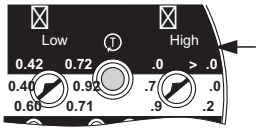
Measuring point status	Message	Current output (nominal value)
Fork free	Status **OK**, incl. LIVE signal [1)]	13.5 mA
Tuning fork covered	In demand mode	6.0 mA
Error	Alarm	< 3.6 mA
Short circuit	Alarm	> 21.0 mA

1) For more information please refer to the Functional Safety Manual SD00350FEN_0213

Density of the medium

The measuring system must be used correctly for the specific application and the properties of the medium and environmental conditions must be taken into consideration. Comply with all instructions concerning critical process situations and installation conditions, see **Operating Instructions BA01037F/00/EN** and **BA01038F/00/EN**

The black background indicates the configurable density range in the **MAX** operating mode. In most cases, it is necessary to set the density range 0.7 / >2.0 (second line) in the Liquiphant FTL8x.

Liquid type	Low density p_{High} g/cm³ (SGU)	High density p_{High} g/cm³ (SGU)	"MAX" operating mode (black background)
e.g. liquefied gas	0.4 (0.4)	2.0 (2.0)	
Other liquids	0.7 (0.7)	>2.0 (>2.0)	

⚠ WARNING

If the rotary switches are not parallel to one another,
a valid density range has not been selected and the red error LED flashes in alternation with the green LED.

- ▶ The rotary switches must be set so that they are parallel to one another.

This can be accomplished in two different ways:
- Press the test button on the Liquiphant FTL8x.
- Disconnect the measuring system from the supply voltage (approx. 1 second or longer).

If the red LED continues flashing after the restart (i.e. after more than 4 s), this could be due to the following:
- The tuning fork is locked in the **MIN** operating mode.
- The density range combination is not valid.

For more information, please refer to:

Functional Safety Manual SD00350F/00/EN

Viscosity of the medium (MAX)

The viscosity of the medium may not exceed 10 000 mPa·s. The Liquiphant FailSafe only signals the change in status from **covered** to **free** once a sufficient volume of the viscose medium has drained off. Therefore, a medium with a higher viscosity can cause the switching times to be exceeded.

For more information, please refer to:

Functional Safety Manual SD00350F/00/EN

Liquiphant FTL5/7x and Nivotester FTL325P (1oo1 SIL2)

The High-High Level safety measuring system comprises a point level switch of the Liquiphant FTL5/7x series with a FEL57-series electronic insert and a transmitter of the Nivotester FTL325P series. A signal that depends on the level is generated in the Liquiphant sensor. This signal is forwarded to the Nivotester switching unit, causing the fail-safe contact to change its state.

Liquiphant FTL5/7x (with FEL57 electronic insert)

The sensor tuning fork vibrates at its intrinsic resonance frequency. This frequency decreases when the tuning fork is covered by liquid. The PFM output signal changes from a high to a low frequency when the sensor is covered, causing the fail-safe contact of the Nivotester to change its state.

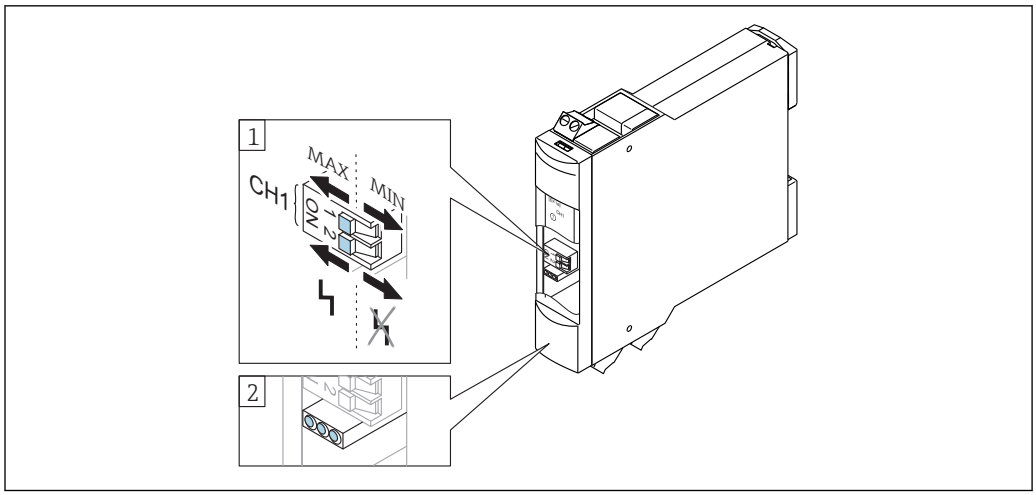
Nivotester FTL325P

The intrinsically safe signal input of the point level switch of the Nivotester FTL 325P series is galvanically isolated from the mains power supply and from the output. The Nivotester powers the measuring sensors of the Liquiphant FTL5/7x series via a 2-wire DC measuring circuit and receives a frequency that indicates whether the limit value has been reached or not. Current pulses (PFM signals) of the transmitter are superimposed on the power supply. These pulses have a pulse width of approx. 200 µs and an amperage of approx. 10 mA. The Nivotester evaluates the frequency and switches the output relay for the level alarm. The relay switch status is indicated by a yellow LED on the front of the Nivotester.

The purpose of the measuring system is to prevent the level of the product rising above a maximum level, i.e. it prevents overfilling. During normal operation, the fork does not come into contact with the liquid and the measuring system signals the status **OK**. If the tuning fork is covered by the liquid, the Nivotester switches to the fail-safe position and holds the demand mode.

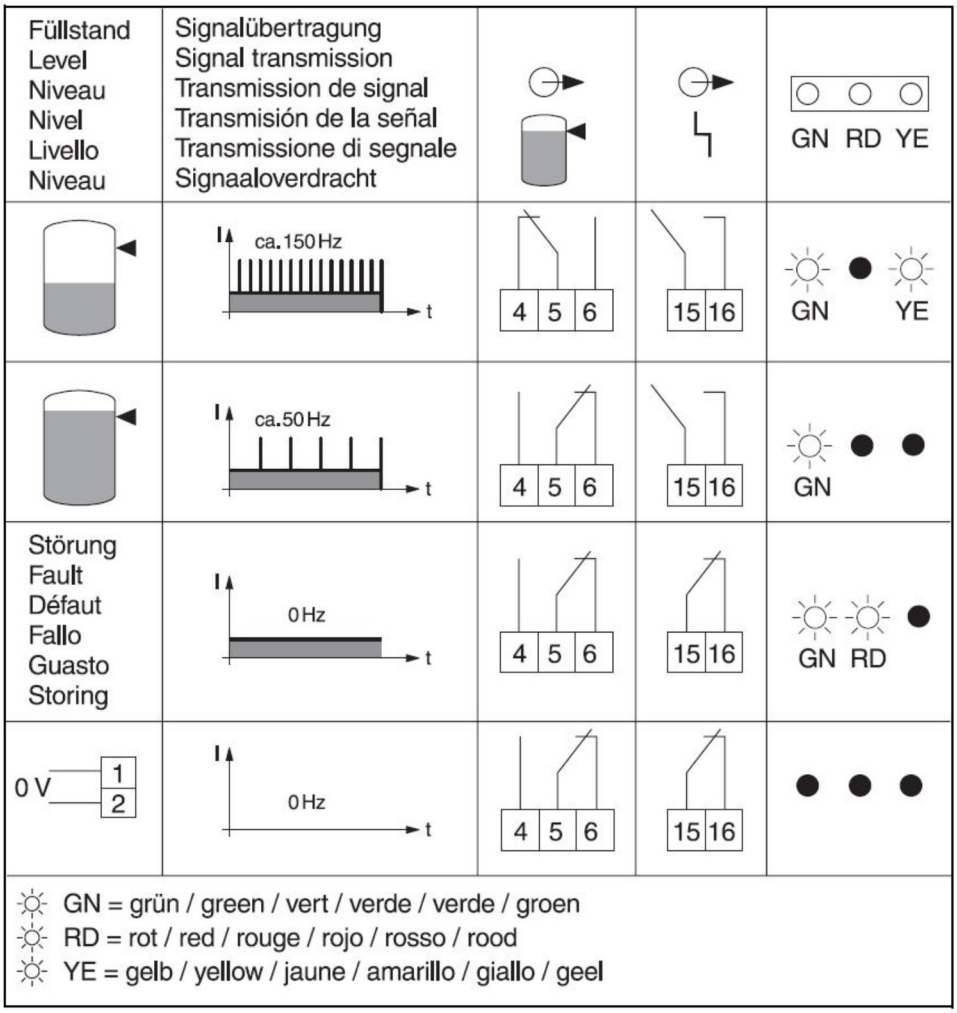
Display and operating elements on the Nivotester FTL325P

The switches must be set to **MAX** and **Fault On**.



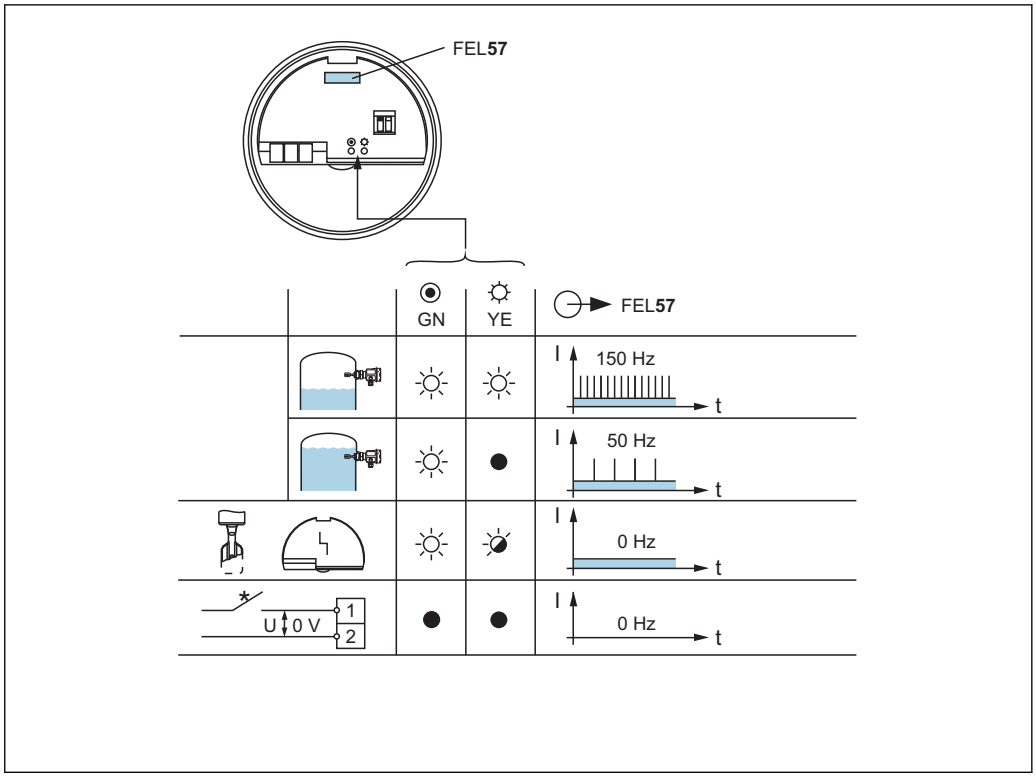
6 Operating and display element, 1-channel Nivotester FTL325P

1 DIL switch: MAX/MIN position (1), fault on/off position (2)
2 Light emitting diodes (LEDs)

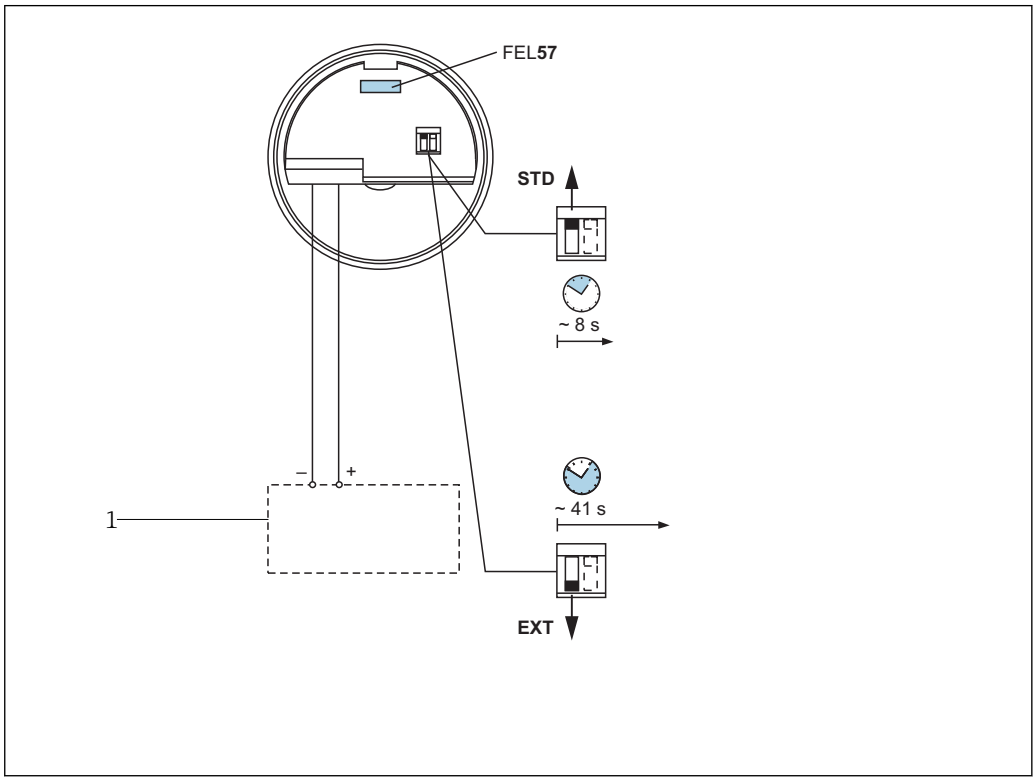


7 MAX / Fault On

Display and operating elements on the Liquiphant FTL5/7x (FEL 57)

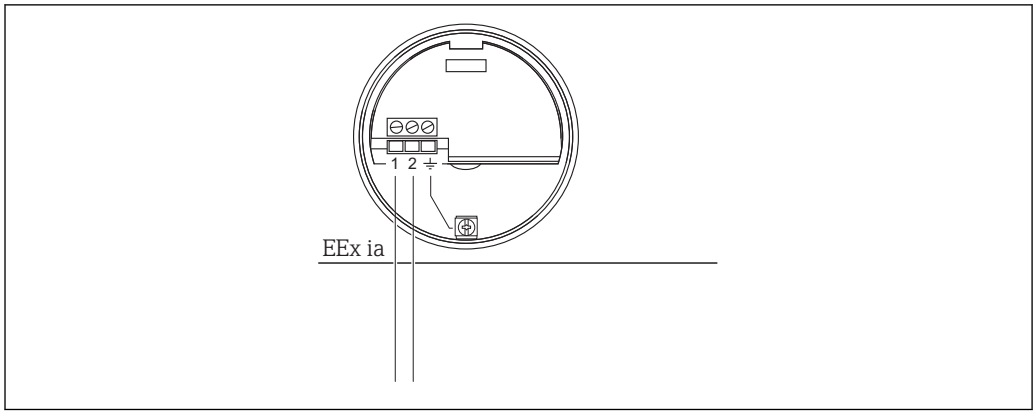


The switch must be set to **EXT** (with a corrosion test); otherwise the automatic proof test will fail.



1 Switching unit

Installation

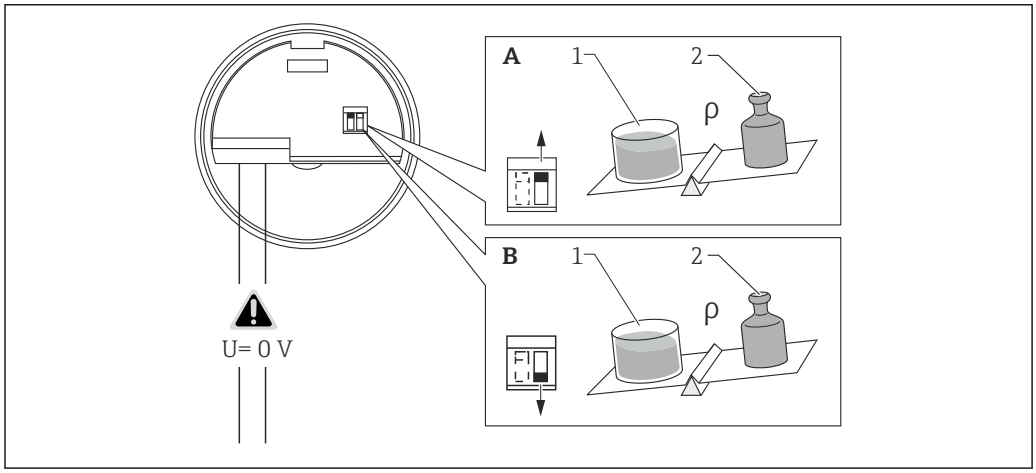


Density of the medium

WARNING

If an incorrect density range is set for the medium,
the safety function can no longer be guaranteed.
► The density range must be set to match the medium.

In most cases, the following applies: set the switch to >0.7 for liquids with a density ρ greater than 0.7 (kg/l or g/cm³).



A Default > 0.7
A-1 1l
A-2 min. 0.7 kg
B e.g. propane > 0.5
B-1 1 l
B-2 0.5 to 0.7 kg

Viscosity of the medium

Liquids with a maximum viscosity of 10 000 mm²/s.

Safety relays and actuators

The safety relays are relays of the Rockwell Guardmaster SI 440R-S12R2 series.

- A safety relay is used as a tank safety relay (mandatory for AOPS)
- The tank safety relay (one per tank) is always disabled (floating safety contacts open) if a tank alarm occurs
- Safety relays are enabled via the safety outputs of the PLC
- Safety relays have two floating contacts. The customer can connect two main contactors for a pump or a valve (actuators) to these contacts
- Safety relay contacts are protected by a fuse terminal (fine-wire fuse 5x20 mm, 230 V_{AC} 2 AT)
- In accordance with a requirement of EN 50205 for safety relays, main contactors must have **forcibly guided contacts**) and a corresponding SIL certificate
- Auxiliary contacts of the main contactor must be connected in series in the reset circuit of the safety relay (S43) (must be bridged if no actuator feedback contact is used)
- This system does not include actuators

LED indicators:

PWR/FAULT	Status and diagnosis
IN	Status of safety inputs
OUT	Status of safety outputs

Configuration of a new safety relay:
The safety relays must be set to MM (Manual Monitored Reset):
– Start configuration/overwrite:
  With the device switched off, set the rotary switch to the **0** position; the device is switched on; the **PWR** LED flashes red after the power-up test
– Configure:
  Turn the rotary switch to the desired position, **LED IN** 1 indicates the position, the position is set when the **PWR LED** is a steady green
– Lock the configuration by switching off the device and switching it back on again (power cycle)
– The configuration must be confirmed before operation

Power limitation of the safety relay contacts 13-14/23-24:

UL	C 300
AC-15	1.5 A / 250 V_{AC}
DC-13	2 A / 24 V_{DC} 0.1 Hz

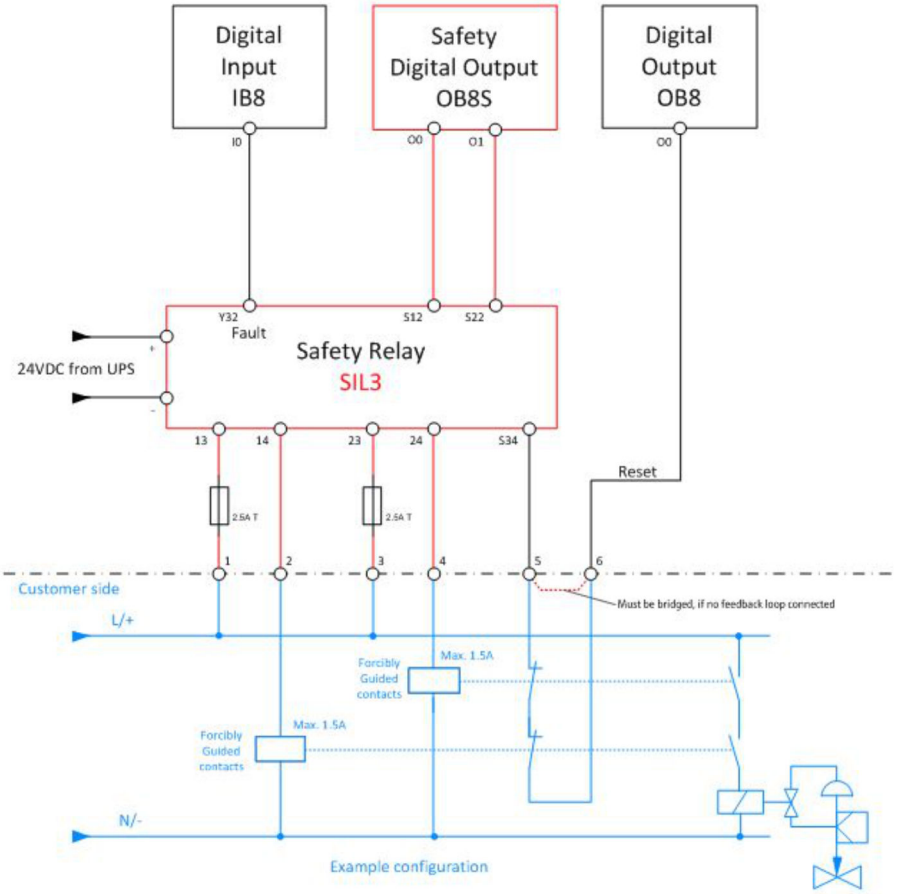
Reset input S34 of the safety relay:

The safety relay must be reset as soon as the event that triggered the alarm has been rectified and the alarm has been acknowledged.

The prerequisites for a reset are as follows:
- The two main contacts must be open (13/14 and 23/24)
- The safety inputs are set (**IN LED** is lit green)
- The reset signal at S34 is active between 250 to 3 000 ms

Reset procedure:

- ▶ Press the **Reset Safety Devices** cabinet button or the button on the **Alarm** HMI screen.
  - ↳ The alarms are reset in the PLC application.
    The safety outputs of the PLC are enabled (only if the alarm trigger is no longer active).
    The safety relay inputs S12 and S22 detect a 24 V DC signal (IN LED is lit green).
    The PLC default output **Reset** is active.
    The safety relay input S34 detects a 24 V DC signal (250 to 3000 ms).
    The safety relay outputs 13-14 and 23-24 are active (OUT LED is lit green).
    The electronic safety output Y32 is inactive.



Safety relay errors are classified as alarms. The alarm activates the alarm stack light (strobe light and siren) in the control room and the field signalization system (strobe light and siren) and writes an entry in the log file.

Information on diagnostics and troubleshooting:

Operating Instructions BA01587S/04/EN

Safety relay and field signalization (optional for AOPS)

Alarm strobe Quadro F12-SIL and alarm siren DS5-SIL by Pfannenberg.

Safety relay H4116 by HIMA.

If an alarm occurs, this is signalled in the field by the alarm strobe and alarm siren. The alarm strobe and alarm siren are each controlled by a safety relay, and field signalizations are active if the relay is disabled.

In this case, the user must take the appropriate safety measures. Once the alarm has been acknowledged via the touch panel or door button, the strobe and the siren are switched off again.

Information on diagnostics and troubleshooting:

Operating Instructions BA01587S/04/EN

⚠ WARNING

In the event of an active alarm Fault Field Signalization,
the safety function of the MOPS is no longer guaranteed and the system does not alert the user to potential overfilling.
- ▶ Filling processes must be stopped immediately.

NOTICE

In the event of an active warning Fault Ext. Alarm Flash Light or Fault Ext Alarm Siren,
the safety function of the MOPS is only guaranteed to a limited extent.
- ▶ Troubleshooting must be performed immediately and the fault rectified.
- ▶ During this time, it is strongly recommended to increase testing or to stop filling processes.

8 Alarm strobe

9 Alarm siren

Other

Operator

- Users must be familiar with the **Fundamental Safety Instructions** in the documents listed.
- In the case of a MOPS, ensure that an operator is always in the immediate vicinity of the system so that visual or acoustic alarm signals are noticed immediately.
- Operators must be appropriately instructed on what action to take in the event of an alarm (e.g. manually stop the pump filling the tank, close the filling valve etc.).
- Operators with administrator rights are responsible for the settings in the password-protected HMI screens.

Further information

General information on functional safety (SIL) is available at:
- www.endress.com/SIL and
- Competence brochure CP01008Z/11/EN Functional safety in process instrumentation for risk reduction

Revision history

Product version	Operating Instructions	Modifications	Comments
1.02.xx	SD01599S/04/EN/01.16	Initial version	-

www.addresses.endress.com

Endress+Hauser

People for Process Automation