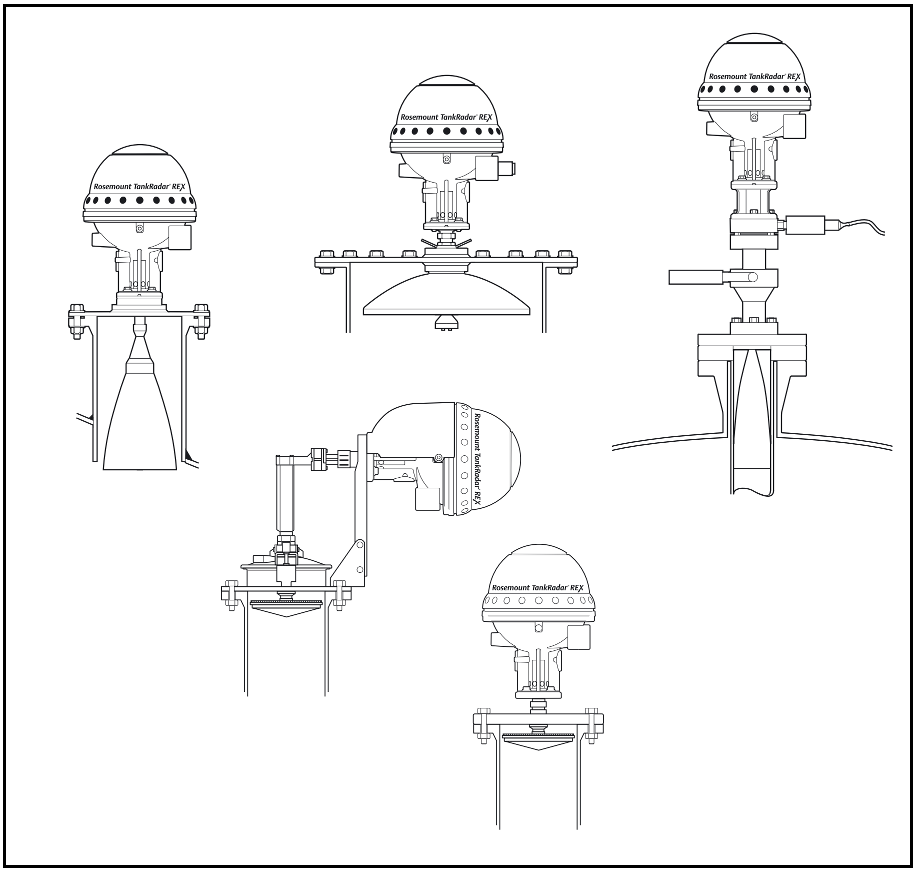
Safety Manual
308020EN, Edition 1
June 2007

Rosemount TankRadar Rex

Safety Manual For Use In Safety Instrumented Systems



Product Discontinued

ROSEMOUNT®
Tank Gauging

EMERSON™
Process Management

www.rosemount-tg.com

Safety Manual

Rosemount TankRadar Rex

First edition

ROSEMOUNT®
Tank Gauging

EMERSON™
Process Management

Spare Parts

Any substitution of non-recognized spare parts may jeopardize safety. Repair, e.g. substitution of components etc, may also jeopardize safety and is under no circumstances allowed.

Rosemount Tank Radar AB will not take any responsibility for faults, accidents, etc caused by non-recognized spare parts or any repair which is not made by Rosemount Tank Radar AB.

WARNING
Do not open the Integrated Junction Box JBi when the circuit is alive.

Contents

1. Scope and Purpose of the Safety Manual

The purpose of the safety manual is to document all the information, relating to TankRadar Rex 3900 Series, which is required to enable the integration of TankRadar Rex into a safety-related system, in compliance with the requirements of IEC 61508.

2. Reference Documents

- IEC 61508
- IEC 61511
- Rosemount TankRadar Rex Installation Manual, Ref. no. 308014EN
- Rosemount TankRadar Rex Service Manual, Ref. no. 308012EN
- Rosemount TankRadar Rex Special Safety Instruction, Ref. no. 308016E
- TankMaster WinSetup User’s Guide, Ref. no. 303027EN
- Rosemount TankRadar REX Technical Description, Ref. no. 703010EN.

3. Scope of the Product

3.1 Purpose of the Product

The Rosemount TankRadar Rex 3900 Series is designed for high performance level gauging in various types of storage tanks. Temperature sensors, remote display unit, water level sensors, pressure sensors, and other devices can be connected. Two relays are available for alarm indication and overfill and dry run protection.

3.2 Assumptions and Restrictions

Install the TankRadar Rex according to the instructions in this document. The *Rosemount TankRadar Rex Installation Manual* and the *Rosemount TankRadar Rex Special Safety Instruction* provide further instructions for a safe installation.

Note that the TankRadar Rex is not safety-rated during maintenance work, configuration changes, or other activity that affects the Safety Function. Alternative means should be used to ensure process safety during such activities.

False echoes within the radar beam from flat obstructions with a sharp edge may lead to a situation where the TankRadar Rex can no longer be used for safety related functions with the listed failure rates, Safe Failure Fraction and PFD_{AVG}. However, reduced proof test intervals can help to detect such unwanted causes.

Operating conditions are available in the *TankRadar Rex Technical Description*, ref no. 703010EN.

3.3 Functional Specification of the Safety Functions

The Safety Function is based on the relay output (one or two relays) used as the primary safety variable for overfill and dry run protection. The relay function is configured to activate the alarm mode at a preset product Level or product Ullage (Ullage is the space between the top of the tank and the product surface).

TankRadar Rex is equipped with two cable outputs for intrinsically safe and non-intrinsically safe connections, respectively. Wires are clearly marked with numbers and designation of wires is shown on a printed plate at the cable outputs. The transmitter can also be equipped with an Integrated Junction Box (JBi).

W11 is for the relays, the TRL/2 Bus, and the non-intrinsically safe power supply.

W12 is for the intrinsically safe connection of Data Acquisition Unit (DAU), Remote Display Unit RDU40, analog inputs, and temperature sensors.

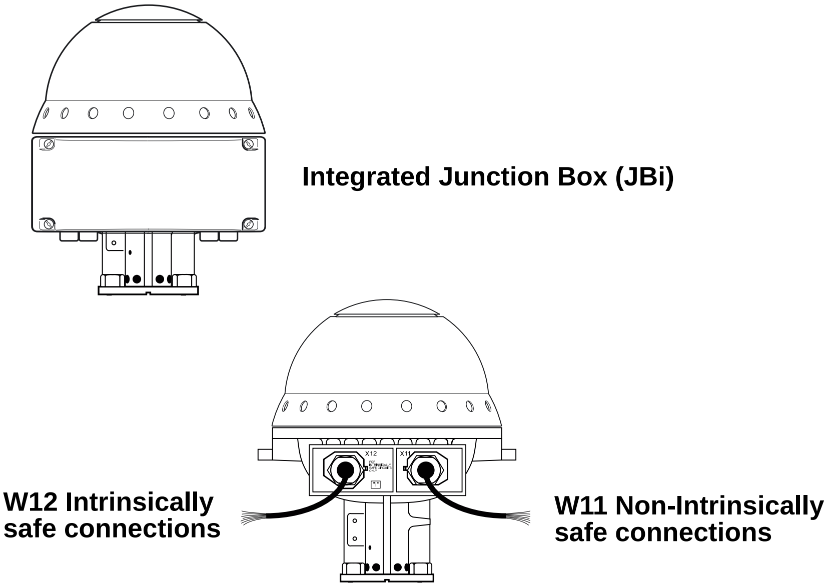

Integrated Junction Box (JBi)
X12
X11
W12 Intrinsically safe connections
W11 Non-Intrinsically safe connections

Figure 1. Electrical connections on the TankRadar REX.

Connect to the relay ports on the W11 side, or to the X11 terminal if the TankRadar REX with Integrated Junction Box JBi is used:

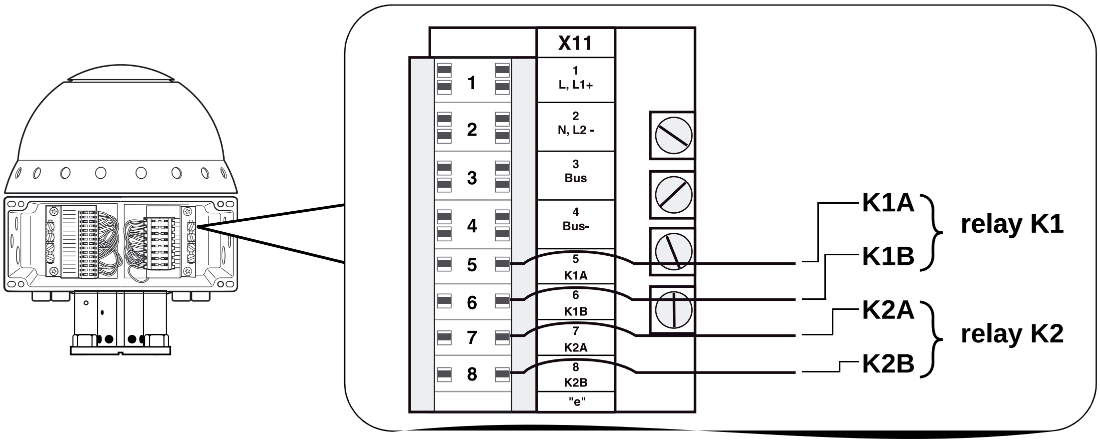


Figure 2. Connecting to the relay ports via Integrated Junction Box (JBi).

Note! *Depending on system configuration one or two relays are available.*

3.3.1 Safety Function Using One Relay

The Safety Function is based on the relay output (relay K1 or relay K2) used as the primary safety variable for overfill and dry run protection. The Safety Function requires that the relay output is configured as **Normally Open**. Normally Open refers to the contact position when the relay is de-energized. This is also referred to as the Alarm state. The terminology for Normally Open can be summarized as described in Table 1 below:

Normally Open	
Open	**Closed**
De-energized	Energized
Not active	Active
Alarm (reset)	Normal

Table 1. Relay terminology for relays configured as Normally Open.

See the *TankRadar REX Installation Manual* for information on how to configure the Relay Output Card (ROC) for operation in Normally Open mode.

3.3.2 Safety Function Using Two Relays in Series

This Safety Function is based on the two relay outputs coupled in series used as the primary safety variable for overfill and dry run protection. The Safety Function requires that the two relay outputs are configured as follows: one relay **Normally Open** and the other relay **Normally Closed**.

The default setting is Normally Open for both relays K1 and K2. See the *TankRadar REX Installation Manual* for information on how to configure the Relay Output Card (ROC) for operation in Normally Open or Normally Closed mode.

The relays are configured in such manner that when the set point (e.g. overfill) is reached one of the relays will "pull" while the second relay will "release". Below the set point (normal operation) the relays will be in the positions as shown in Figure 3:

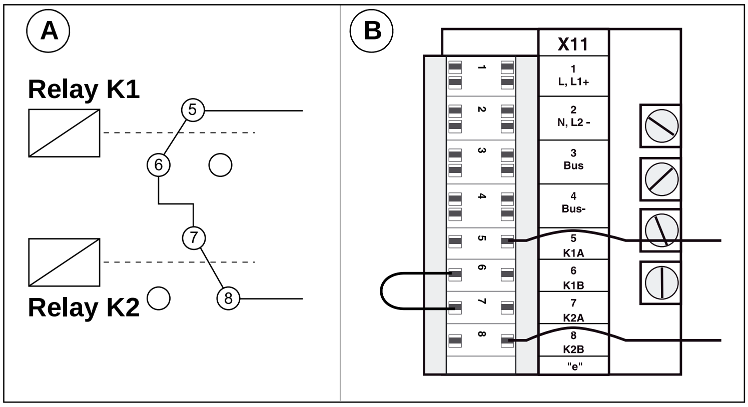


Figure 3. A. Relay positions under normal operation.
B. Wiring diagram for Safety Function using two relays coupled in series.

The system state is given by the states of the two relays according to Table 2:

System state	Relay K1 (Normally Open)	Relay K2 (Normally Closed)
Normal	Energized	De-energized
Alarm	De-energized	Energized
Alarm	Energized	Energized
Alarm	De-energized	De-energized

Table 2. System state versus relay state with Safety Function using two relays coupled in series.

3.4 Parameters Related to Safety Functions

TankRadar Rex is classified as a Type B device having a hardware fault tolerance of 0. The TankRadar Rex is available with one or two relays. With two relays coupled in series a higher Safe Failure Fraction (SFF) value is achieved.

3.4.1 Parameters Related to Safety Function Using One Relay

When using one relay, either of the relays K1 or K2 can be used. A Failure Modes, Effects and Diagnostics Analysis (FMEDA) was conducted resulting in failure rates according to Table 3:

Failure Category	**Failure Rates (in FIT)**	
	Relay K1	**Relay K2**
Fail Safe Detected	0	0
Fail Safe Undetected	1262	1261
Fail Dangerous Detected	775	775
Fail Dangerous Undetected	492	493

Table 3. Failure rates of TankRadar Rex according to IEC61508 using one relay.

Based on the FMEDA the Safe Failure Fraction (SFF) was calculated, see Table 4:

Characteristics	**Value**	
	Relay K1	**Relay K2**
Safe Failure Fraction (SFF)	80.55%	80.49%
PFD_{avg} (proof test interval=1 year)	$2.15x10^{-3}$	$2.16x10^{-3}$
Diagnostic test interval	1 minute	1 minute

Table 4. Safety characteristics of TankRadar Rex.

The analysis shows that TankRadar Rex has SFF between 60% and 90%. According to Table 3 of IEC 61508, Type B components with 60% <SFF< 90% may be used up to SIL 2 as a single device only when the hardware fault tolerance is 1. By fulfilling the criteria of IEC 61511 First Edition 2003-01 section 11.4.4, the hardware fault tolerance of a device may be reduced by 1.

A third-party assessment conducted by *exida.com* of the TankRadar Rex has shown that the requirements of the IEC 61511 First Edition 2003-01 section 11.4.4 are fulfilled and that the TankRadar Rex is supposed to be a Proven-in-use device.

In conclusion, based on the third part FMEDA and Proven-in-use assesment (by *exida.com*), the TankRadar Rex with a hardware fault tolerance of 0 and a SFF of 60 % to < 90% is considered to be suitable for use in SIL 2 safety functions.

However, the decision on the usage of Proven-in-use devices is always with the end-user.

According to IEC 61508 the average Probability of Failure on Demand (PFD_{avg}) shall be between 10^{-2} and 10^{-3} for SIL2 applications. According to a generally accepted stand of view, a stand-alone sensor may contribute with up to 35% of the PFD_{avg} for a complete SIL rated system (sensor, logic solver & final element). For TankRadar Rex the PFD_{avg} for a proof test interval of one year is $2.15*10^{-3}$ (relay K1) and $2.16*10^{-3}$ (relay K2). This means that the TankRadar Rex gauge fulfills the required PFD_{avg} value for SIL2, both according to Table 2 of IEC 61508-1, and the requirement not to claim more than 35% of the range.

Assumptions

- For safety instrumented systems it is assumed that the relay output is used as the primary safety variable. The assumed configuration of the relay output is “Normally Open”
- Failure rates are constant within the useful lifetime of components
- Safety function does not rely on analog output, analog input, communication protocol, and temperature measurement functions
- Failure of one part will cause failure of entire unit
- Propagation of failures is not relevant

- The instrument utilizes Fixed Program Language (FPL)
- The estimated useful lifetime of electrolytic capacitors is > 20 years. As the capacitors are the limiting factor with regard to useful lifetime of the system, the useful lifetime of the product is considered to be 20 years.
- The average ambient temperature during the operating time is 40 °C

3.4.2 Parameters Related to Safety Function Using Two Relays

A Failure Modes, Effects and Diagnostics Analysis (FMEDA) was conducted resulting in failure rates according to Table 5:

Failure Category	Failure Rates (in FIT)
Fail Safe Detected	0
Fail Safe Undetected	1344
Fail Dangerous Detected	810
Fail Dangerous Undetected	336

Table 5. Failure rates of TankRadar Rex according to IEC61508 using two relays coupled in series.

Based on the FMEDA the Safe Failure Fraction (SFF) was calculated, see Table 6:

Characteristics	Value
Safe Failure Fraction (SFF)	86.51%
PFD_{avg} (proof test interval=1 year)	$1.47x10^{-3}$
Diagnostic test interval	1 minute

Table 6. Safety characteristics of TankRadar Rex using two relays coupled in series.

The analysis shows that TankRadar Rex has SFF between 60% and 90%. According to Table 3 of IEC 61508, Type B components with 60% <SFF< 90% may be used up to SIL 2 as a single device only when the hardware fault tolerance is 1. By fulfilling the criteria of IEC 61511 First Edition 2003-01 section 11.4.4, the hardware fault tolerance of a device may be reduced by 1.

A third-party assessment conducted by *exida.com* of the TankRadar Rex has shown that the requirements of the IEC 61511 First Edition 2003-01 section 11.4.4 are fulfilled and that the TankRadar Rex is supposed to be a Proven-in-use device.

In conclusion, based on the third part FMEDA and Proven-in-use assesment (by *exida.com*), the TankRadar Rex with a hardware fault tolerance of 0 and a SFF of 60 % to < 90% is considered to be suitable for use in SIL 2 safety functions.

However, the decision on the usage of Proven-in-use devices is always with the end-user.

According to IEC 61508 the average Probability of Failure on Demand (PFD_{avg}) shall be between 10^{-2} and 10^{-3} for SIL2 applications. According to a generally accepted stand of view, a stand-alone sensor may contribute with up to 35% of the PFD_{avg} for a complete SIL rated system (sensor, logic solver & final element). For TankRadar Rex the PFD_{avg} for a proof test interval of one year is $1.47*10^{-3}$. This means that the TankRadar Rex gauge fulfills the required PFD_{avg} value for SIL2, both according to Table 2 of IEC 61508-1, and the requirement not to claim more than 35% of the range.

Assumptions

- For safety instrumented systems it is assumed that the two relay outputs, coupled in series, are used as the primary safety variable. The assumed configuration of the relay outputs is: one relay “Normally Closed” and the other relay “Normally Open”.
- Safety function does not rely on analog output, analog input, communication protocol, and temperature measurement functions
- Failure rates are constant within the useful lifetime of components
- Failure of one part will cause failure of entire unit
- Propagation of failures is not relevant
- The instrument utilizes Fixed Program Language (FPL)
- The estimated useful lifetime of electrolytic capacitors is > 20 years. As the capacitors are the limiting factor with regard to useful lifetime of the system, the useful lifetime of the product is considered to be 20 years
- The average ambient temperature during the operating time is 40 °C

3.5 Hardware and software configuration

Valid software and hardware versions:

- Software version 1.G4 and higher
- Serial numbers > 42315

Unless specified at the time when purchasing the TankRadar Rex, please contact Emerson Process Management/Rosemount Tank Gauging to verify that the gauge can be considered within the scope of the assessment by *exida.com*.

4. Installation and Configuration

Please refer to the following documentation for instructions on how to install and configure the TankRadar Rex gauge:

- REX Installation Manual, Ref. no. 308014E
- TankMaster WinSetup User’s Guide, Ref. no. 303027E
- REX Service Manual, Ref. no. 308012E

Make sure that the TankRadar Rex is properly installed and configured according to the instructions. Before configuration of the relay outputs can be done, use the *WinSetup* configuration tool to adjust the gauge. Verify correct level values as given by the tank geometry, by comparing hand dip values with measurement values from the REX gauge as described in section 5.2.

Note that the TankRadar Rex gauge is not safety-rated during maintenance work, configuration changes, or other activity that affects the Safety Function. Alternative means should be used to ensure process safety during such activities.

4.1 Configuration with One Relay

In the following description configuration of relay K1 is used as an example. The same procedure applies for relay K2.

The relay K1 is configured by using the *REX Relay Output 1* configuration window, see Figure 4 (*REX Relay Output 2* window applies for relay K2).

Besides entering the alarm limits and relay states for either overfill or dry run applications, the following parameters have to be checked for compliance:

Parameter	Configuration in Relay Output window
Control mode	Auto
Disable Invalid Variable Alarm (check box)	Unmarked
Source	Level/Ullage

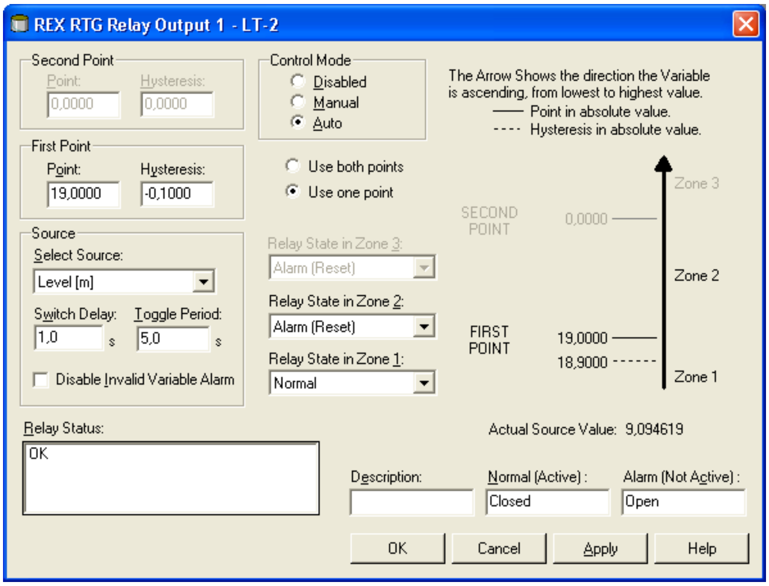
Table 7. Parameter settings for the relay output.

To configure the Safety Function with one relay output on a TankRadar Rex gauge do the following:

1 Start the *TankMaster WinSetup* program.

2 In the WinSetup workspace, click the right mouse button on the device icon that represents the desired REX gauge, and select **Properties**.
Response: the *REX RTG Properties* window appears.

3 Select the **Configuration** tab and click the **Relay Output 1** button to open the *REX Relay Output* window:



REX RTG Relay Output 1 - LT-2

Second Point
Point: 0,0000
Hysteresis: 0,0000

First Point
Point: 19,0000
Hysteresis: -0,1000

Source
Select Source: Level [m]
Switch Delay: 1,0 s
Toggle Period: 5,0 s
□ Disable Invalid Variable Alarm

Control Mode
○ Disabled
○ Manual
● Auto

○ Use both points
● Use one point

Relay State in Zone 3: Alarm (Reset)
Relay State in Zone 2: Alarm (Reset)
Relay State in Zone 1: Normal

The Arrow Shows the direction the Variable is ascending, from lowest to highest value.
—— Point in absolute value.
---- Hysteresis in absolute value.

Actual Source Value: 9,094619

Relay Status: OK

Description:
Normal (Active): Closed
Alarm (Not Active): Open

Figure 4. Configuration of relay output in TankMaster WinSetup.

The overfill and dry run protection safety function requires that you choose Level or Ullage as relay output source. Choose the desired option from the **Select Source** drop-down list.

Level is the distance between the product surface and the lower reference point.

Ullage is the distance between the upper reference point and the product surface, see *Figure 5*. There are two options for the upper reference point (see the *WinSetup User's Guide*):

- RTG Reference Point (at the flange of the REX gauge)
- Tank Reference Point (at the top of a hand dip nozzle)

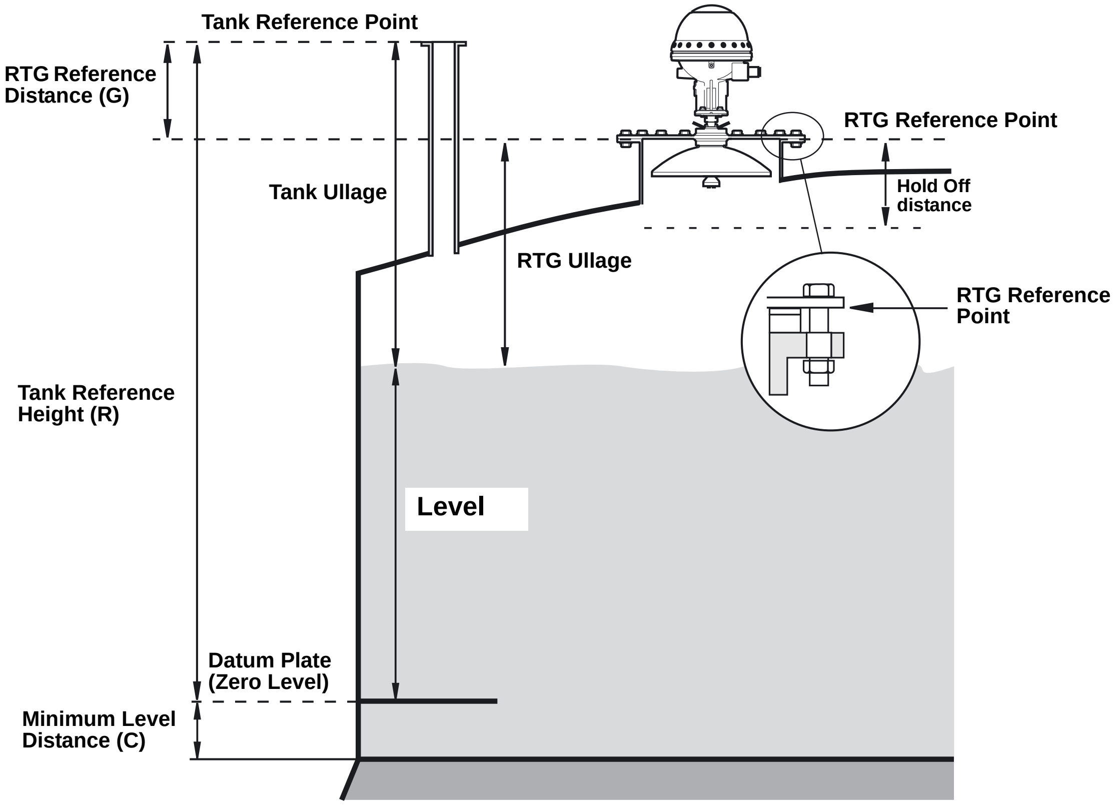


Figure 5. Tank geometry

4 Set **First Point** to a value that corresponds to the desired **Alarm Limit**.

Note that the set point has to be below the **Hold Off** distance, see *Figure 5*.

5 Set **Relay State in Zone 1** to **Normal**.
Set **Relay State in Zone 2** to **Alarm**.

6 Make sure that the other parameters are set according to Table 7, “Parameter settings for the relay output.,” on page 14.

4.2 Configuration When Using Two Relays In Series

When two relays are used they must be connected as illustrated in Figure 3.

Each relay is configured separately using the *REX Relay Output 1* and the *REX Relay Output 2* configuration windows, see Figure 6 and Figure 7. Besides entering the alarm limits (First Point) and relay states for either overfill or dry run applications, the following parameters have to be checked for compliance:

Parameter	**Configuration in Relay Output window**
Control mode	Auto
Disable Invalid Variable Alarm (check box)	Unmarked
Source	Level/Ullage

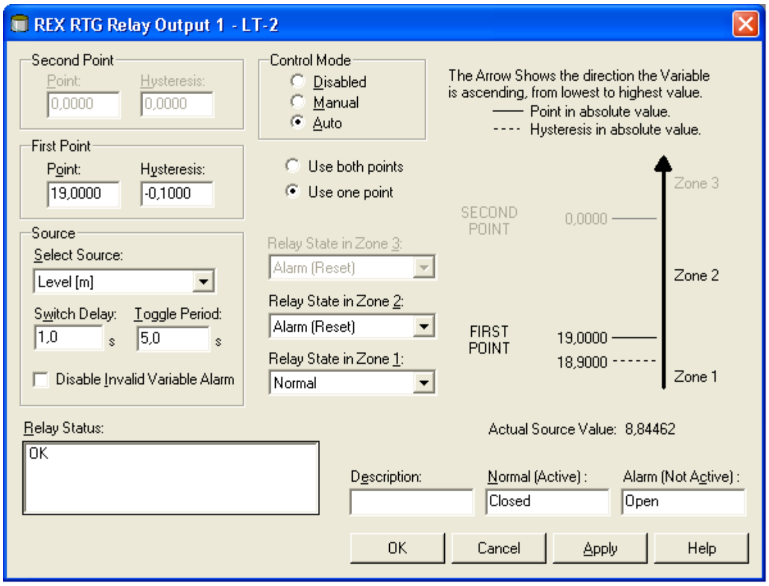
Table 8. Parameter settings for relay output.

To configure the Safety Function with two relay outputs on a TankRadar Rex gauge do the following:

1 Start the *TankMaster WinSetup* program.

2 In the WinSetup workspace, click the right mouse button on the device icon that represents the desired REX gauge, and select **Properties**.

3 Select the **Configuration** tab and click the **Relay Output 1** button:



REX RTG Relay Output 1 - LT-2

Second Point
Point: 0,0000
Hysteresis: 0,0000

First Point
Point: 19,0000
Hysteresis: -0,1000

Source
Select Source: Level [m]
Switch Delay: 1,0 s
Toggle Period: 5,0 s
□ Disable Invalid Variable Alarm

Control Mode
○ Disabled
○ Manual
● Auto

○ Use both points
● Use one point

Relay State in Zone 3: Alarm (Reset)
Relay State in Zone 2: Alarm (Reset)
Relay State in Zone 1: Normal

The Arrow Shows the direction the Variable is ascending, from lowest to highest value.
—— Point in absolute value.
- - - - Hysteresis in absolute value.

Relay Status: OK

Actual Source Value: 8,84462

Description:
Normal (Active): Closed
Alarm (Not Active): Open

Figure 6. Configuration of Relay Output 1.

The overfill and dry run protection safety function requires that you choose Level or Ullage as relay output source. Choose the desired option from the **Select Source** drop-down list.

Level is the distance between the product surface and the lower reference point.

Ullage is the distance between the upper reference point and the product surface, see *Figure 5*. There are two options for the upper reference point (see the *WinSetup User's Guide*):

- RTG Reference Point (at the flange of the REX gauge)
- Tank Reference Point (at the top of a hand dip nozzle)

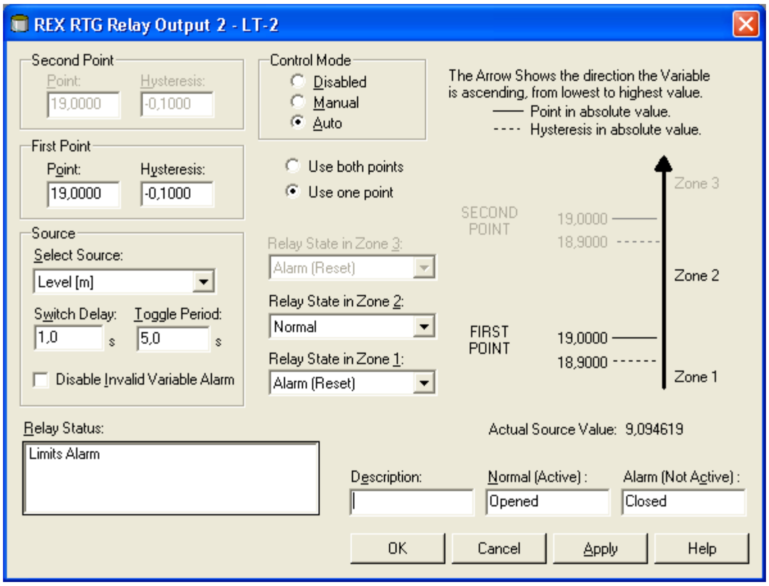
4 Set **First Point** to a value that corresponds to the desired **Alarm Limit**. Note that the same Alarm Limit must be used for relay 2.

5 Set **Relay State in Zone 1** to **Normal**.
Set **Relay State in Zone 2** to **Alarm**.

6 Make sure that the other parameters are set according to Table 8, “Parameter settings for relay output.,” on page 17.

7 When relay 1 is configured, continue with the relay 2. In the WinSetup workspace, click the right mouse button on the REX gauge icon, and select **Properties**.

8 Select the **Configuration** tab and click the **Relay Output 2** button:



REX RTG Relay Output 2 - LT-2

Second Point
Point: 19,0000 Hysteresis: -0,1000

First Point
Point: 19,0000 Hysteresis: -0,1000

Source
Select Source: Level [m]
Switch Delay: 1,0 s Toggle Period: 5,0 s
☐ Disable Invalid Variable Alarm

Control Mode
○ Disabled
○ Manual
● Auto

○ Use both points
● Use one point

Relay State in Zone 3: Alarm (Reset)
Relay State in Zone 2: Normal
Relay State in Zone 1: Alarm (Reset)

The Arrow Shows the direction the Variable is ascending, from lowest to highest value.
—— Point in absolute value.
---- Hysteresis in absolute value.

Relay Status: Limits Alarm

Actual Source Value: 9,094619

Description:
Normal (Active) : Opened
Alarm (Not Active) : Closed

Figure 7. Configuration of relay output 2.

Choose Level (or Ullage) as relay output source from the **Select Source** drop-down list.

9 Set **First Point** to a value that corresponds to the desired **Alarm Limit**. Note that the same set point must be used for relay 1 and relay 2.

Set **Relay State in Zone 1** to **Alarm**.
Set **Relay State in Zone 2** to **Normal**. Note the difference compared to the settings for relay 1.

10 Make sure that the other parameters are set according to Table 8, “Parameter settings for relay output.,” on page 15.

4.3 Verification of the Safety Function

Prior to putting the system in operation it has to be tested to verify proper operation.

1. Verify the relay function, see section 5.3.

2. Verify the system response, see section 5.1.

3. Write protect the gauge. See section 4.4 for more information on write protection.

4.4 Write Protection

The Write Protection switch has to be used for locking the database in order to prevent unauthorized changes of the configuration. To write protect the TankRadar Rex gauge, either an internal or an external switch can be used (see the *Rosemount TankRadar Rex Service Manual* for further information). The internal switch is located on a circuit board in the transmitter head:

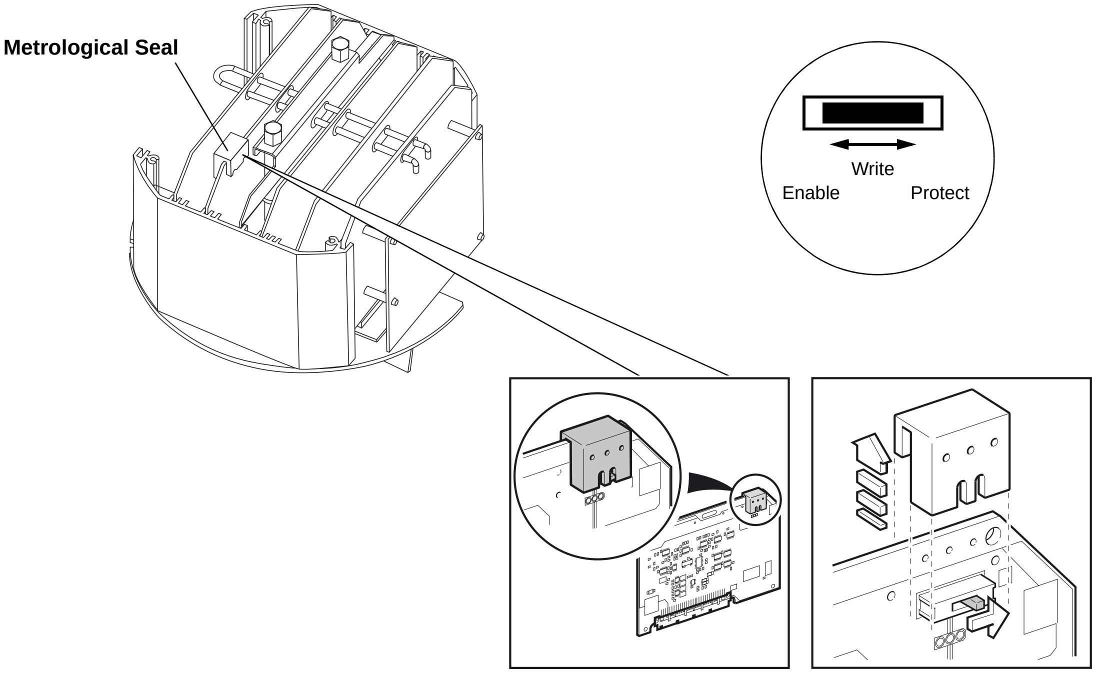


Figure 8. A write protection switch is available in the transmitter head of the TankRadar Rex gauge.

The TankRadar Rex can also be equipped with an optional external metrological seal, see Figure 9. In this case the gauge housing does not need to be opened to enable the write protection.

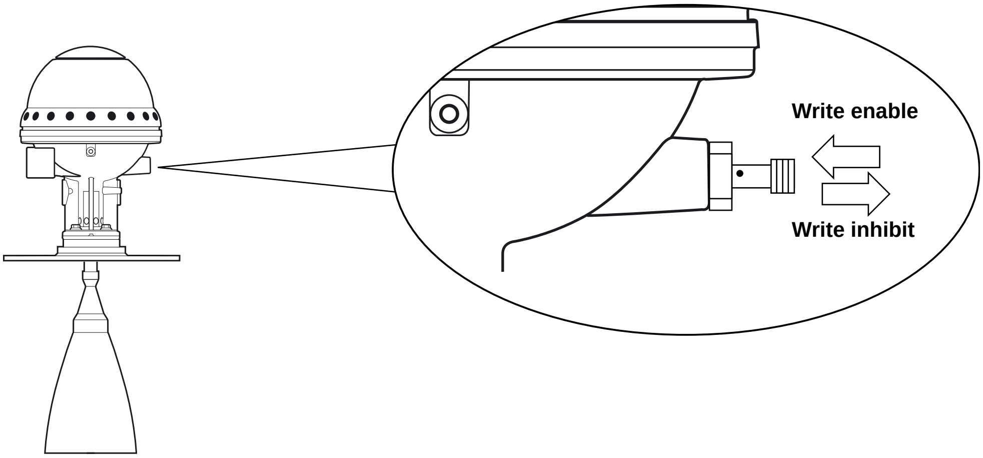


Figure 9. An optional external metrological seal can be used for the TankRadar Rex gauge.

5. Proof Tests

The TankRadar REX gauge must be checked at regular intervals. It is recommended that proof tests are carried out once a year.

The level measuring function can be verified via *TankMaster WinOpi* and *WinSetup*.

For verification of the relay function see section 5.3.

Note that the TankRadar Rex gauge is not safety-rated during maintenance work, configuration changes, or other activity that affects the Safety Function. Alternative means should be used to ensure process safety during such activities.

One or more of the proof tests described below are recommended.

5.1 Triggering the Relay

This proof test will detect approximately 99% of the DU (dangerous undetected) failures not detected by the diagnostics in TankRadar Rex.

The test includes the following:

- Inspection of the Tank Spectrum
- Testing of the relay response

Use the **Tank Scan** function in the *TankMaster WinSetup* program to ensure that no disturbing echoes are present. See *WinSetup User's Guide* for more information on the Tank Scan function. If there is an amplitude peak in the tank spectrum which can not be traced back to the product surface, compare the spectrum with the tank drawing or by visible inspection of the tank. Note if there are any objects like beams, heating coils, etc. which correspond to the found echoes. If the disturbing echoes affect measurement performance, appropriate action has to be taken. Please contact Emerson Process Management/Rosemount Tank Gauging for advice.

The overfill and dry run protection function should be checked by testing the system response when the product level reaches the relay set point (see “Configuration with One Relay” on page 14).

If the overfill and dry run function can not be tested by filling or emptying the tank, a suitable method (i.e. a simulation of the level or triggering the measuring system by a physical measuring effect) may be used.

It is important that the test takes into consideration the overfill and dry run protection in conjunction with all system components.

5.2 Hand Dipping

This proof test will detect approximately 84% of the DU (dangerous undetected) failures not detected by the diagnostics in TankRadar Rex:

- Make a hand dip of the level in the tank using a calibrated dip tape traceable to national standard
- Compare the manual reference level measurement to the level value presented in WinSetup configuration tool

5.3 Verification of the Relay Function

This proof test will detect approximately 64% of the DU (dangerous undetected) failures not detected by the diagnostics in TankRadar Rex.

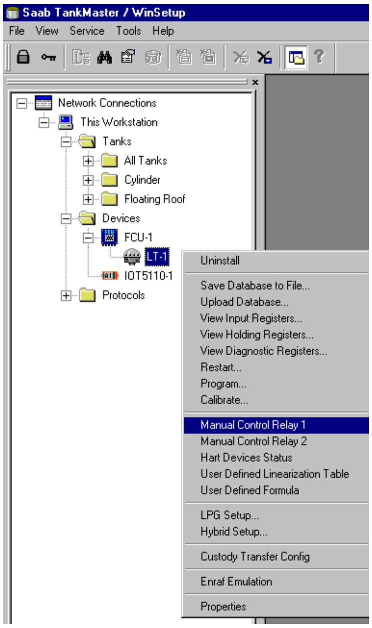
Prior to this test, the write protection must be disabled (see “Write Protection” on page 20).

When the relay function is verified, make sure that the “auto” Control Mode is chosen before enabling the write protection.

The relay function must be checked at regular intervals. It can be tested manually by using the built-in control function in *TankMaster WinSetup*.

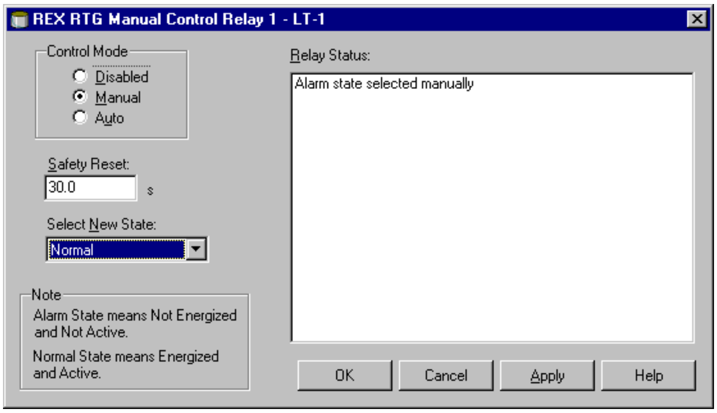
To manually switch between different relay states do the following:

1 Select a Rex gauge in the *TankMaster WinSetup Workspace* window:



Manual Control Relay

2 Click the right mouse button and choose the **Manual Control Relay** option, or from the WinSetup **Service** menu choose **Devices/Manual Control Relay**:


REX RTG Manual Control Relay 1 - LT-1

Control Mode
○ Disabled
● Manual
○ Auto

Safety Reset: 30.0 s

Select New State: Normal

Note
Alarm State means Not Energized and Not Active.
Normal State means Energized and Active.

Relay Status:
Alarm state selected manually

3 Make sure that an appropriate Safety Reset value is set. This value specifies the time-out period for the relay to reset if a communication failure occurs.

4 Choose Manual in the **Control Mode** pane.

5 Choose a new relay state from the **Select New State** list. You should test switching between Normal and Alarm to verify that the relay responds in a proper way.

6 Set the **Control Mode** to **Auto** when the verification is finished.

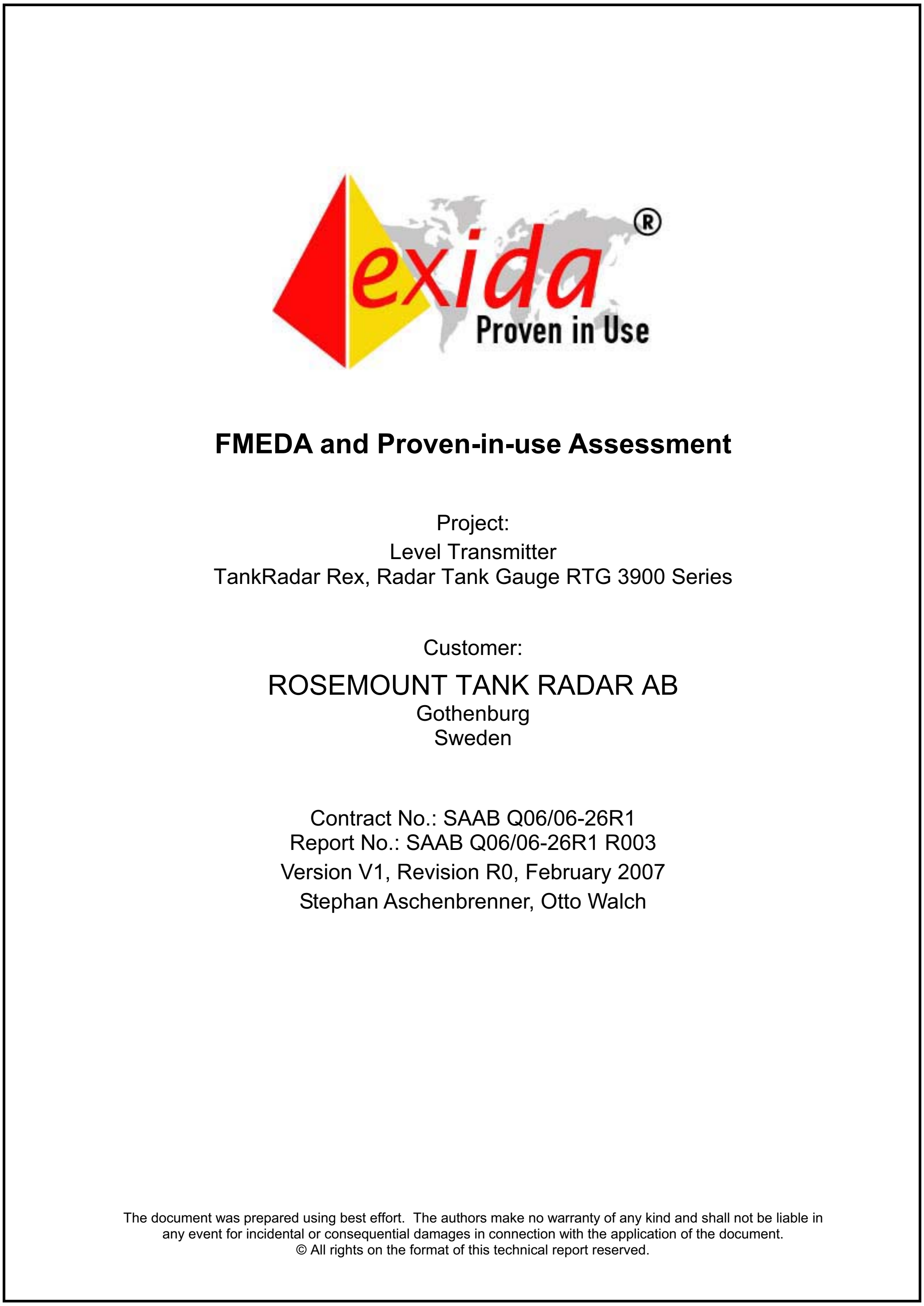
5.4 Repair

All failures detected by the transmitter diagnostics or by the Proof Test must be reported.

6. Terms and Definitions

FIT	Failure in Time (1 FIT = 1failure/10^9 h)
FMEDA	Failure Modes, Effects and Diagnostics Analysis
HFT	Hardware Fault Tolerance
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
Type B component	Complex component (using microcontrollers or programable logic)

Appendix FMEDA and Proven-in-use Assessment



exida Proven in Use

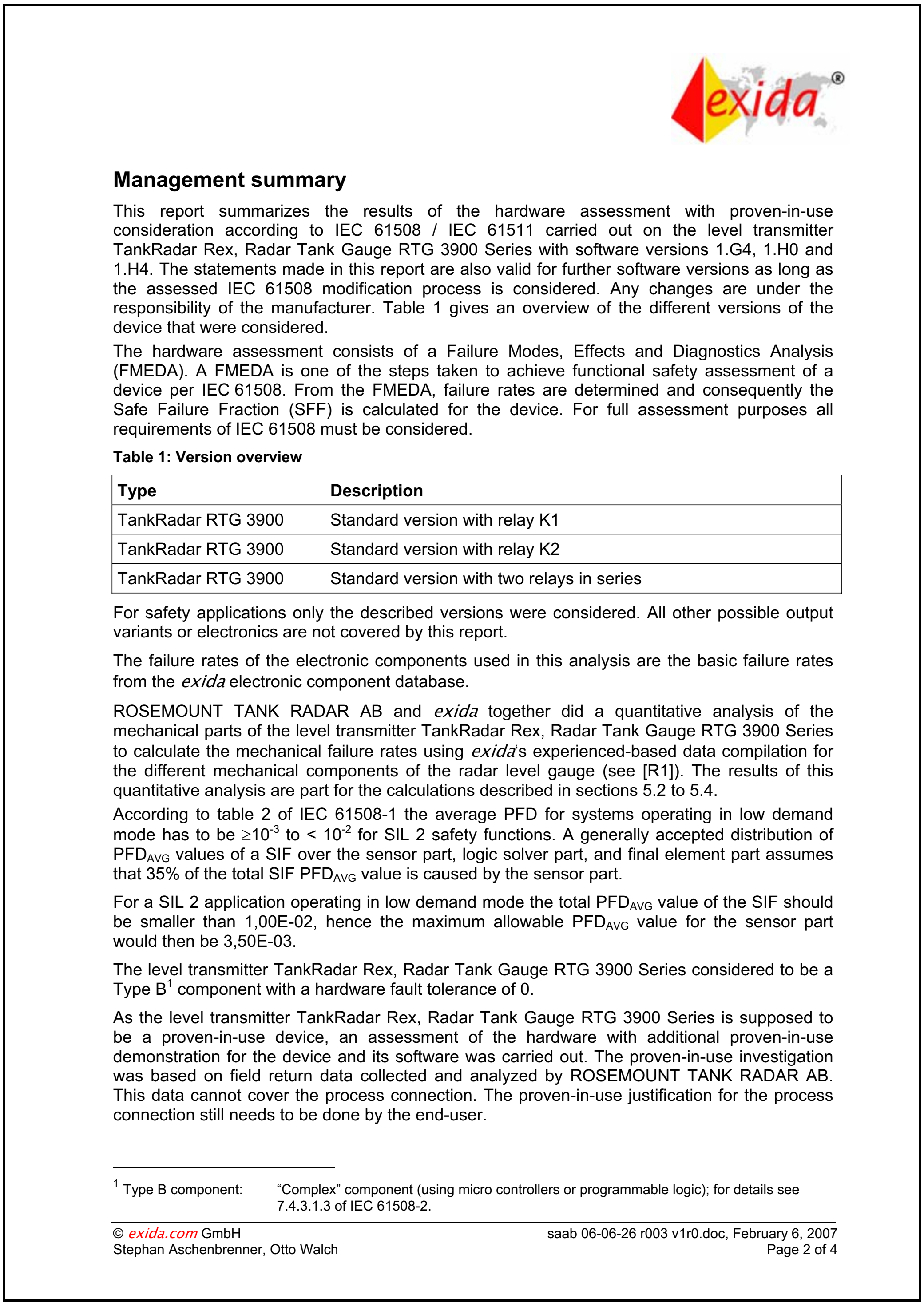
FMEDA and Proven-in-use Assessment

Project:
Level Transmitter
TankRadar Rex, Radar Tank Gauge RTG 3900 Series

Customer:
ROSEMOUNT TANK RADAR AB
Gothenburg
Sweden

Contract No.: SAAB Q06/06-26R1
Report No.: SAAB Q06/06-26R1 R003
Version V1, Revision R0, February 2007
Stephan Aschenbrenner, Otto Walch

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.



Management summary

This report summarizes the results of the hardware assessment with proven-in-use consideration according to IEC 61508 / IEC 61511 carried out on the level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series with software versions 1.G4, 1.H0 and 1.H4. The statements made in this report are also valid for further software versions as long as the assessed IEC 61508 modification process is considered. Any changes are under the responsibility of the manufacturer. Table 1 gives an overview of the different versions of the device that were considered.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

Table 1: Version overview

Type	**Description**
TankRadar RTG 3900	Standard version with relay K1
TankRadar RTG 3900	Standard version with relay K2
TankRadar RTG 3900	Standard version with two relays in series

For safety applications only the described versions were considered. All other possible output variants or electronics are not covered by this report.

The failure rates of the electronic components used in this analysis are the basic failure rates from the *exida* electronic component database.

ROSEMOUNT TANK RADAR AB and *exida* together did a quantitative analysis of the mechanical parts of the level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series to calculate the mechanical failure rates using *exida*'s experienced-based data compilation for the different mechanical components of the radar level gauge (see [R1]). The results of this quantitative analysis are part for the calculations described in sections 5.2 to 5.4.

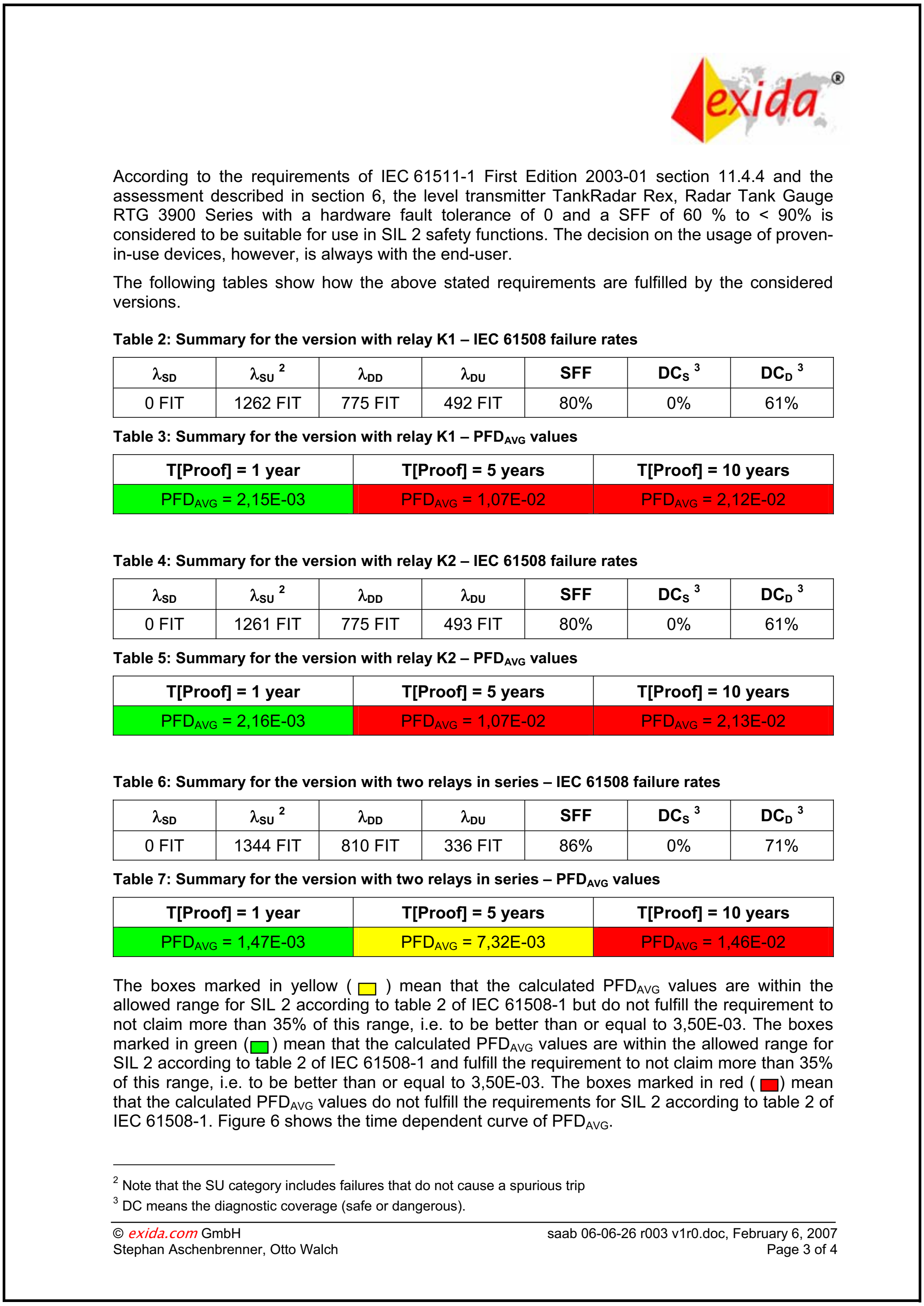
According to table 2 of IEC 61508-1 the average PFD for systems operating in low demand mode has to be $\geq 10^{-3}$ to $< 10^{-2}$ for SIL 2 safety functions. A generally accepted distribution of PFD_{AVG} values of a SIF over the sensor part, logic solver part, and final element part assumes that 35% of the total SIF PFD_{AVG} value is caused by the sensor part.

For a SIL 2 application operating in low demand mode the total PFD_{AVG} value of the SIF should be smaller than 1,00E-02, hence the maximum allowable PFD_{AVG} value for the sensor part would then be 3,50E-03.

The level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series considered to be a Type B[1] component with a hardware fault tolerance of 0.

As the level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series is supposed to be a proven-in-use device, an assessment of the hardware with additional proven-in-use demonstration for the device and its software was carried out. The proven-in-use investigation was based on field return data collected and analyzed by ROSEMOUNT TANK RADAR AB. This data cannot cover the process connection. The proven-in-use justification for the process connection still needs to be done by the end-user.

[1] Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.



According to the requirements of IEC 61511-1 First Edition 2003-01 section 11.4.4 and the assessment described in section 6, the level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series with a hardware fault tolerance of 0 and a SFF of 60 % to < 90% is considered to be suitable for use in SIL 2 safety functions. The decision on the usage of proven-in-use devices, however, is always with the end-user.

The following tables show how the above stated requirements are fulfilled by the considered versions.

Table 2: Summary for the version with relay K1 – IEC 61508 failure rates

λ_{SD}	λ_{SU} [2]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [3]	**DC_D** [3]
0 FIT	1262 FIT	775 FIT	492 FIT	80%	0%	61%

Table 3: Summary for the version with relay K1 – PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 2,15E-03	PFD_{AVG} = 1,07E-02	PFD_{AVG} = 2,12E-02

Table 4: Summary for the version with relay K2 – IEC 61508 failure rates

λ_{SD}	λ_{SU} [2]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [3]	**DC_D** [3]
0 FIT	1261 FIT	775 FIT	493 FIT	80%	0%	61%

Table 5: Summary for the version with relay K2 – PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 2,16E-03	PFD_{AVG} = 1,07E-02	PFD_{AVG} = 2,13E-02

Table 6: Summary for the version with two relays in series – IEC 61508 failure rates

λ_{SD}	λ_{SU} [2]	λ_{DD}	λ_{DU}	**SFF**	**DC_S** [3]	**DC_D** [3]
0 FIT	1344 FIT	810 FIT	336 FIT	86%	0%	71%

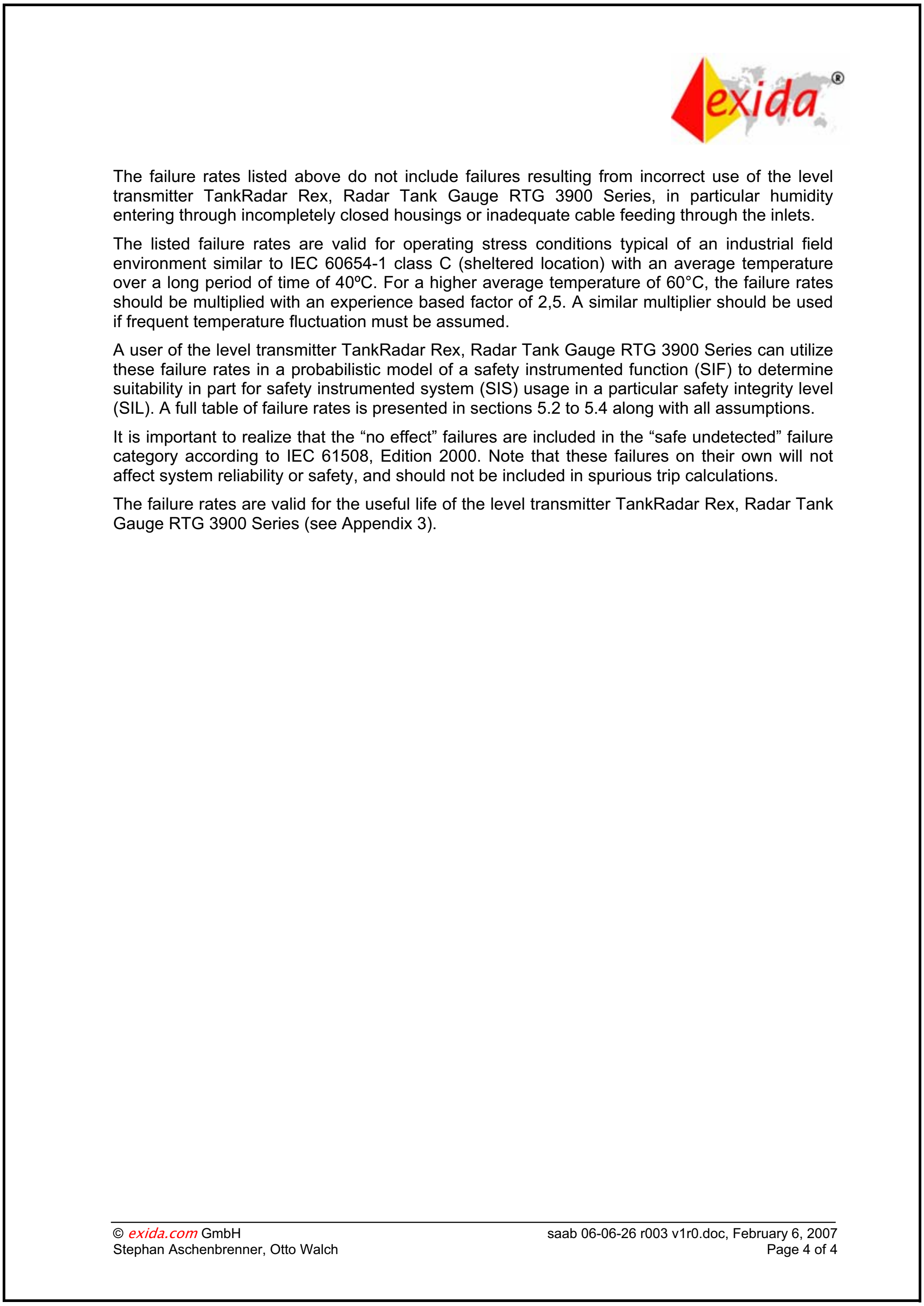
Table 7: Summary for the version with two relays in series – PFD_{AVG} values

T[Proof] = 1 year	**T[Proof] = 5 years**	**T[Proof] = 10 years**
PFD_{AVG} = 1,47E-03	PFD_{AVG} = 7,32E-03	PFD_{AVG} = 1,46E-02

The boxes marked in yellow (🟨) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. The boxes marked in green (🟩) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and fulfill the requirement to not claim more than 35% of this range, i.e. to be better than or equal to 3,50E-03. The boxes marked in red (🟥) mean that the calculated PFD_{AVG} values do not fulfill the requirements for SIL 2 according to table 2 of IEC 61508-1. Figure 6 shows the time dependent curve of PFD_{AVG}.

[2] Note that the SU category includes failures that do not cause a spurious trip

[3] DC means the diagnostic coverage (safe or dangerous).



The failure rates listed above do not include failures resulting from incorrect use of the level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the inlets.

The listed failure rates are valid for operating stress conditions typical of an industrial field environment similar to IEC 60654-1 class C (sheltered location) with an average temperature over a long period of time of 40ºC. For a higher average temperature of 60°C, the failure rates should be multiplied with an experience based factor of 2,5. A similar multiplier should be used if frequent temperature fluctuation must be assumed.

A user of the level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL). A full table of failure rates is presented in sections 5.2 to 5.4 along with all assumptions.

It is important to realize that the “no effect” failures are included in the “safe undetected” failure category according to IEC 61508, Edition 2000. Note that these failures on their own will not affect system reliability or safety, and should not be included in spurious trip calculations.

The failure rates are valid for the useful life of the level transmitter TankRadar Rex, Radar Tank Gauge RTG 3900 Series (see Appendix 3).

Safety Manual
308020EN, Edition 1
June 2007

Rosemount Tank Gauging local representative:

Emerson Process Management

Rosemount Tank Gauging
Box 130 45
SE-402 51 Göteborg
SWEDEN
Tel (International): +46 31 337 00 00
Fax (International): +46 31 25 30 22
E-mail: sales.srt@emersonprocess.com
www.rosemount-tg.com

Ref. no: 308020E, Edition 1. June 2007.