



# **Safety Manual**

## **SmartRadar FlexLine**



---

## Table of Contents

---

<b>CHAPTER 1 Introduction</b>	<b>1-1</b>
<b>1.1 About this Manual</b>	<b>1-1</b>
1.1.1 Purpose	1-1
1.1.2 Content	1-1
1.1.3 Related Documents	1-1
<b>1.2 Basic Skills and Knowledge</b>	<b>1-1</b>
<b>1.3 Safety Standards</b>	<b>1-2</b>
1.3.1 Safety Instrumented Systems, Functions and Integrity Levels	1-2
1.3.2 What standard to use	1-2
<b>CHAPTER 2 Functions, Architecture and Compliance</b>	<b>2-1</b>
<b>2.1 Functions</b>	<b>2-1</b>
<b>2.2 Architecture</b>	<b>2-1</b>
<b>2.3 Compliance</b>	<b>2-2</b>
<b>2.4 Safety-related Data</b>	<b>2-2</b>
<b>2.5 Safety Design</b>	<b>2-3</b>
<b>2.6 Principle of Operation</b>	<b>2-3</b>
<b>2.7 Fault Detection and Reaction</b>	<b>2-5</b>
<b>CHAPTER 3 Implementation</b>	<b>3-1</b>
<b>3.1 General</b>	<b>3-1</b>
<b>3.2 Assumptions and Constraints</b>	<b>3-1</b>
<b>3.3 New Installation or Upgrade</b>	<b>3-1</b>
3.3.1 New Installation	3-1
3.3.2 Upgrade	3-1
<b>3.4 Configuration</b>	<b>3-2</b>
3.4.1 Hardware Configuration	3-2
3.4.2 Software Configuration	3-4
<b>3.5 Verification of the Safety Instrumented Function(s)</b>	<b>3-5</b>
<b>CHAPTER 4 Maintenance Requirements</b>	<b>4-1</b>
<b>4.1 Purpose</b>	<b>4-1</b>
<b>4.2 Proof Testing</b>	<b>4-1</b>

---

## Table of Contents

---

## CHAPTER 1 INTRODUCTION

---

### 1.1 About this Manual

#### 1.1.1 Purpose

The Safety Manual provides information about the SmartRadar FlexLine that is relevant for integration of this radar-based level gauge into a Safety Instrumented System (SIS). This manual is aimed at technical personnel responsible for such integration.

#### 1.1.2 Content

Chapter Title	Contents Description
Introduction	This chapter.
Functions, Architecture and Compliance	Specification of the Safety Instrumented Functions (SIF) that are applied and the architecture(s) these SIFs need to operate. Furthermore relevant certification and compliance information is given.
Implementation	Description of - or reference to - details how to achieve and implement the applicable SIFs.
Maintenance Requirements	Description of - or reference to - details how to maintain the required Safety Integrity Levels of the implemented SIFs.

#### 1.1.3 Related Documents

- IEC 61508 (2010),
- IEC 61511 (2004),
- SmartRadar FlexLine Service Manual; Part No.: 4417.762,
- SmartRadar FlexLine safety instructions;  
Doc. No.: GB478-1990000-4x,
- Installation Guide Radar gauge Antennas; Part No.: 4416.642,

### 1.2 Basic Skills and Knowledge

Before you start to work on the SmartRadar FlexLine it is assumed that you are certified to do work on safety related systems and devices, and that you have appropriate knowledge of:

- The concepts and functioning of the SmartRadar FlexLine,
- The applicable process and equipment under control within the SIS,
- This Safety Manual,
- Site procedures,
- Applicable safety standards (e.g. IEC 61508 and IEC 61511).

### 1.3 Safety Standards

#### 1.3.1 Safety Instrumented Systems, Functions and Integrity Levels

Processes and Equipment Under Control (PUC/EUC) in the process industry require a high level of safety. Safety Instrumented Systems (SIS) are used to perform Safety Instrumented Functions (SIF). Instrumentation that is used for SIFs, must meet minimum standards and performance levels. Standards like IEC 61508 and IEC 61511 have been developed for this purpose. One of the performance criteria that these standards apply is the Safety Integrity Level (SIL).

IEC 61508 details the design requirements for achieving the required SIL. The safety integrity requirements for each individual safety function may differ. The safety function and SIL requirements are derived from hazard analyses and risk assessments. The higher the level of adapted safety integrity, the lower the likelihood of dangerous failure of the SIS. These standards also address the safety-related sensors and final elements regardless of the technology used.

The SmartRadar FlexLine can be used for a specific SIF that demands SIL 1 or SIL 2. If used in a redundant arrangement, the SmartRadar FlexLine can be applied in loops that require SIL 3.

#### 1.3.2 What standard to use

IEC 61508 has been developed as a generic standard. A framework of standards, incl. IEC 61511, for specific industry sectors were based on this one. The information in the table below is meant as a guideline.

Standard	Typical application within the process industry
IEC 61508  Functional safety of electrical / electronic / programmable electronic (E/E/PE) safety-related systems	If you are a manufacturer, it is strongly recommended that you apply the IEC 61508.  This generic standard is intended to provide guidance on how to develop E/E/PE safety-related devices as used in Safety Instrumented Systems (SIS). The IEC 61508 serves as a basis for the development of sector standards (e.g. for the machinery sector, the process sector, the nuclear sector, etc.). It can serve as stand-alone standard for those sectors where a sector specific standard does not exist.
IEC 61511  Functional safety - Safety instrumented systems for the process industry sector	If you are an owner/user, it is strongly recommended that you apply the IEC 61511.  This standard addresses the application of SISs for the process industries. It requires a process hazard and risk assessment to be carried out, to enable the specification for SISs to be derived. In this standard a SIS includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s). The standard is intended to lead to a high level of consistency in underlying principles, terminology and information within the process industries. This should have both safety and economic benefits.

## CHAPTER 2 FUNCTIONS, ARCHITECTURE AND COMPLIANCE

### 2.1 Functions

Beside its standard functions the SmartRadar FlexLine can also be used for Safety Instrumented Functions (SIF) for storage tanks in the oil and gas industry. These functions are:

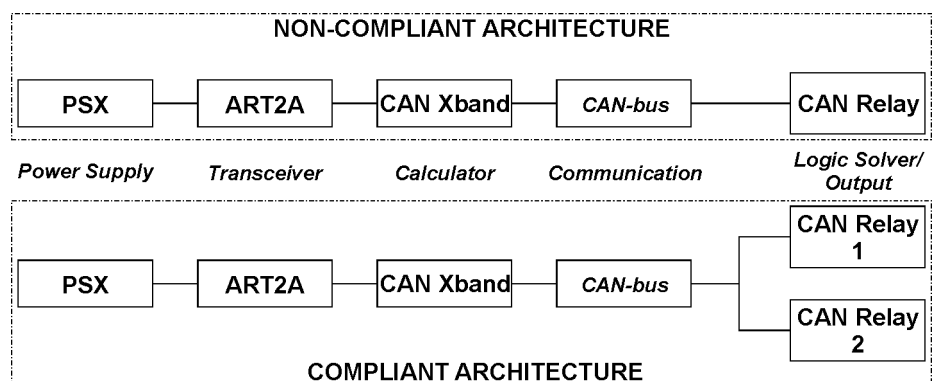
- the SIL compliant “overflow protection”,
- the SIL compliant “underfill protection”.

To establish that the safety parameters for these functions of the SmartRadar FlexLine are in the range of SIL 2, it is necessary to:



- use the correct architecture; see chapter 2.2 "Architecture",
- apply the function correctly; for further details see,
  - chapter 3 "Implementation",
  - chapter 4 "Maintenance Requirements".

### 2.2 Architecture

The major requirement to establish the SIFs in the range of SIL 2 is that the SmartRadar FlexLine has the correct architecture. The block diagrams below show the different architectures of the SmartRadar FlexLine. For safety related output, the SmartRadar FlexLine uses an architecture with redundant CAN Relays.



### 2.3 Compliance

Organization	Relevant details
	In case the SmartRadar FlexLine has the correct architecture it is considered to be a Type B system in the meaning of IEC 61508. If implemented and maintained correctly, the safety parameters for the “overflow protection” are in the range of SIL 2.
	Details of the assessment done by TUV Rheinland are recorded in: Report-No. 986/EL 717.00/10.

### 2.4 Safety-related Data

The table below specifies the applicable data relating to IEC 61508:

Entity / parameter	Value	Remarks
Safety Integrity Level	SIL 2	
Classification of the device	Type B	
Architectural approach	2oo4D	2 out of 4 diagnostics.
Hardware fault tolerance	0	This value applies to the integral hardware configuration. For the CAN-Relay board a value of 1 applies.
Safe Failure Fraction (SFF)	SFF = 97%	This value applies to the integral hardware configuration. Details on hardware element level are specified in: chapter 3.4.1 "Hardware Configuration".
Total failure rate	$\lambda_{DU} = 112.8 \text{ FIT}$	
Probability of Failure per Hour	PFH = $6.8 \cdot 10^{-8} \text{ 1/h}$	corresponds to 6.8% of the overall SIL 2 budget
Probability of Failure on Demand	PFD = $3.0 \cdot 10^{-3}$	corresponds to 30% of the overall SIL 2 budget; this value is valid for the stated Proof Test Interval T.
External power supply	85 - 240 VAC, 3A	AC supply is required to achieve the specified SFF.
Proof Test Interval	T = 10 a	Once every 10 years.

TABLE 2-1 Safety-related data



## 2.5 Safety Design

FIGURE 2-1 shows a schematic diagram of the SIL compliant design including the Safe Failure Fraction (SFF) per hardware element.

The SIL compliant design uses two CAN-RELAY boards for safety related output. In this way it differs from a standard SmartRadar FlexLine.

A CAN-RELAY board has four relays; in this configuration only relays R3 and R4 of each CAN-RELAY board are used. Use of relays R4 increases availability.

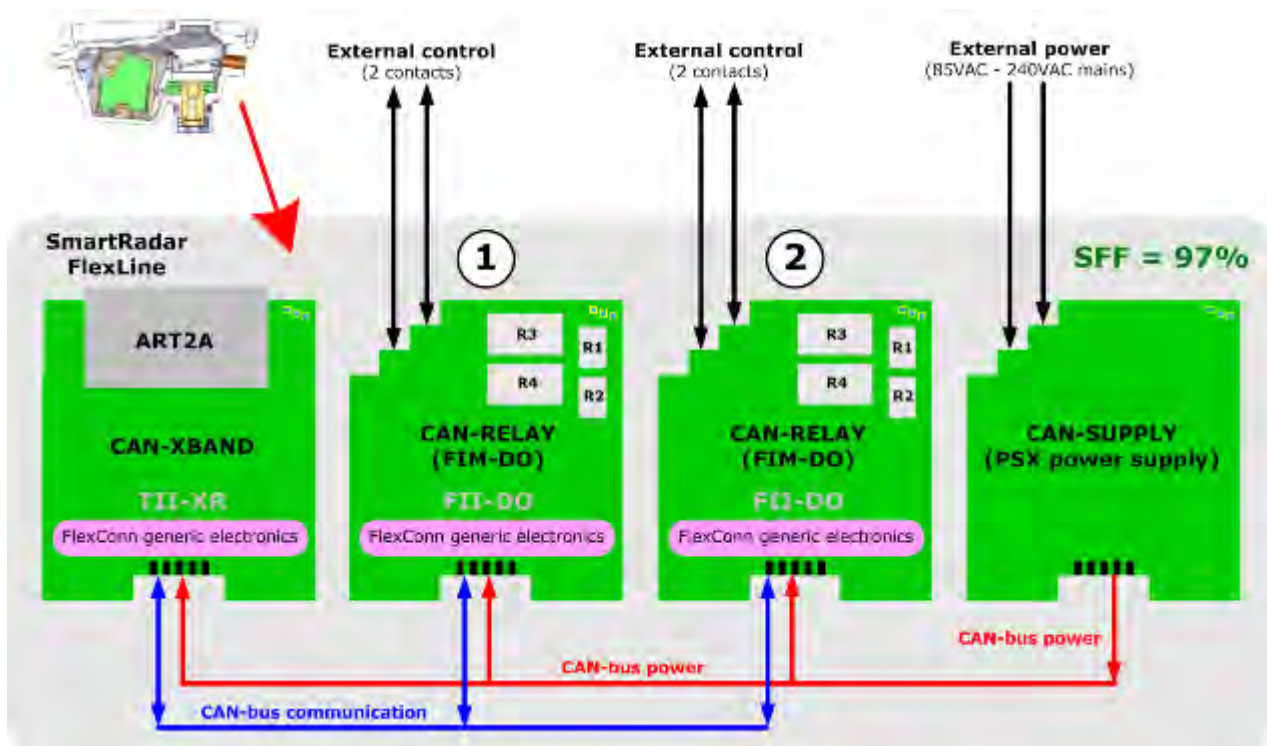


FIGURE 2-1

Safety design and hardware element SFF details

## 2.6 Principle of Operation

The ART2A board functions as a transceiver to measure the actual product level. Signals that are sent out will be reflected by the product surface. The ART2A communicates the reflected signal directly to the CAN-XBAND board. This board performs the required calculations and communicates the result to both CAN-RELAY boards over a CAN-bus.

The CAN-RELAY boards are each others counterpart. The processors of the two boards in this design:

- each scan and analyze various parameters for status and health,
- exchange and compare diagnostic data.

The result of the analysis by each CAN-RELAY board is called the overfill protection status and is communicated back to the CAN-XBAND board. This board will process the data and merge it to a comprehensive status level that is suitable for use in the control room.

When configured for SIL compliant “overflow protection” or “underfill protection” the SmartRadar FlexLine will switch an output when it detects a predetermined (potentially) unsafe status. For more detailed information, see chapter 2.7 "Fault Detection and Reaction".

FIGURE 2-2 shows an example of how the SmartRadar FlexLine can be applied. In this example the output is connected to a field device - such as a pump or valve - to mitigate the unsafe situation. The output can also be connected to a logic solver, such as a safety PLC.

In this example mitigation can imply stopping a pump and/or closing a valve. In this way the SmartRadar FlexLine performs the safety related function, although the connected field device can also be controlled by a non-safety related user application.

The basic arrangement of the output relays of the SmartRadar FlexLine as shown in FIGURE 2-2 is always the same. In a normal (healthy) operating situation the contacts of the CAN-RELAYS are closed.

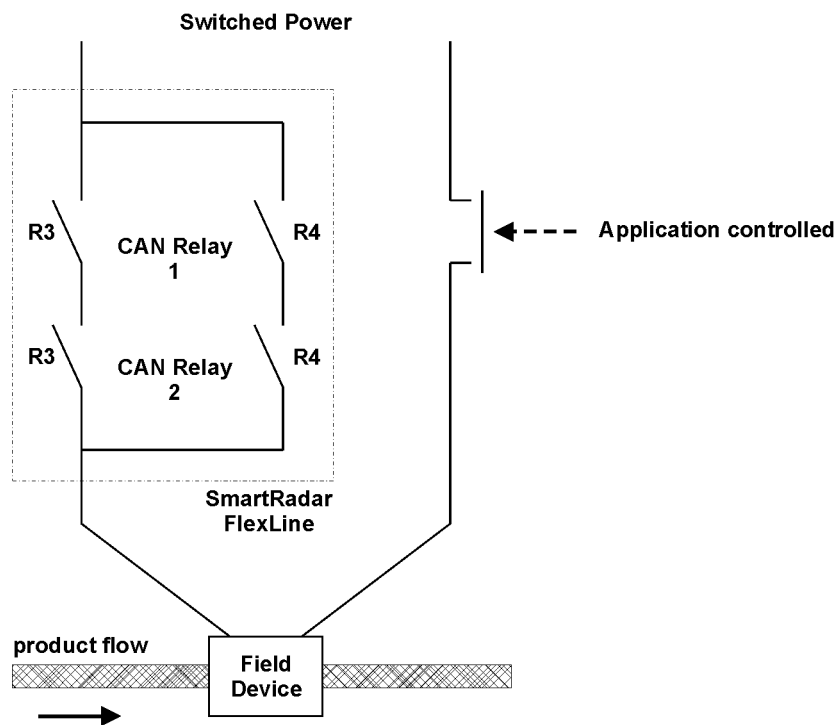


FIGURE 2-2

Basic output arrangement

The redundant arrangement of the output relays offers a distinct advantage. In case a single relay contact fails SIL compliant fault detection is still maintained. In addition any relay contact failure is detected and forms an integral part of the diagnostics of the device.

## 2.7 Fault Detection and Reaction

The SmartRadar FlexLine is configured for one of the safety related functions by applying the appropriate software settings (for details refer to chapter 3.4.2 "Software Configuration"). The principle of operation and fault detection for both functions is the same.

At a fixed interval of 1 second the SmartRadar FlexLine executes several scans, and analyzes the data at the same rate. The result of this safety analysis is used to update the overfill/underfill protection status. Scans are executed by each CAN-RELAY board and the CAN-XBAND board.

The safety analysis is done by each CAN-RELAY board independently. At the same time these boards exchange and compare diagnostic data.

As part of the protection function the CAN-XBAND board scans the protection status from both CAN-RELAYs. It analyzes this data, and merges and maps it to the product level status.

TABLE 2-2 specifies the scans that the SmartRadar FlexLine executes.

Scan type *	Executing board	Source
Product level (innage)	each CAN-RELAY	CAN-XBAND
Board diagnostics	each CAN-RELAY	other CAN-RELAY
Relay 3 function diagnostics	each CAN-RELAY	other CAN-RELAY
Relay 4 function diagnostics	each CAN-RELAY	other CAN-RELAY
Overfill protection status	X-BAND	both CAN-RELAYs

\*)for scans the following applies: two (2) retries will be performed in case no healthy status is detected.

TABLE 2-2

SmartRadar FlexLine scans

During the safety analysis a CAN-RELAY performs several checks and processes this data. Part of the required data is taken from the scans (see TABLE 2-2), while other data comes from the board itself.

The purpose of the safety analysis is to intervene when the product level becomes unsafe and/or board diagnostics indicate an unhealthy status. The product level is considered to be unsafe when it comes outside (above or under) a predetermined value. Board diagnostics health is derived from a number of parameters that are processed during the overfill safety analysis. These parameters will be described in further detail. In case the resulting overfill/underfill protection status demands intervention, the CAN-RELAY boards will take action on the relays R3 and R4 outputs accordingly. As stated before, in a normal operating situation the contacts of the CAN-RELAYs are closed.

## Functions, Architecture and Compliance

Failures that originate from one of the CAN-RELAY boards do not necessarily lead to an immediate safety shutdown as these boards make up the redundant part of the architecture. If this applies only a second failure related to the CAN-RELAY boards will cause a safety shutdown. The user can configure a safety shutdown timer to meet with local repair requirements.

TABLE 2-3 shows the applicable parameters and CAN-RELAY board actions.

**SD = Shut Down**

**O = Overfill alarm**

**N = No**

**NO = Normal Operation**

**W = Gauge alarm (warning)**

**Y = Yes**

**H = Healthy**

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
<b>Own board status</b>														
<b>Level</b> (incl. TII-XR comms + TV Health + status check)	0	X	X	X	X				1	1	1	1	1	1
<b>Voltage</b>	X	0	X	X	X				1	1	1	1	1	1
<b>Diag board</b>	X	X	0	X	X				1	1	1	1	1	1
<b>Diag R3</b>	X	X	X	X	X				0	0	0	1	1	1
<b>Diag R4</b>	X	X	X	X	X				1	1	1	0	0	0
<b>Counter part communication</b>	X	X	X	0	X				1	1	1	1	1	1
<b>Other board status</b>														
<b>Diag board</b> (incl. Voltage)	X	X	X	X	0				1	1	1	1	1	1
<b>Diag R3</b>	X	X	X	X	X				0	1	1	0	1	1
<b>Diag R4</b>	X	X	X	X	X				1	0	1	1	0	1
<b>Board action</b>														
<b>Output R3</b>	0	0	0	0	0				0	0	0	0	1	1
<b>Output R4</b>	0	0	0	0	0				1	0	1	0	0	1
<b>Application status</b>	SD	SD	SD	SD	SD				NO	SD	NO	SD	NO	NO
<b>Overfill Protection Status</b>	O	W	W	W	W				W	W	W	W	W	W
<b>Start safety timer</b>	N	N	N	N	N				Y	N	Y	N	Y	Y

for communication the following applies: two (2) retries will be performed in case no healthy status is detected.

TABLE 2-3

CAN-RELAY board actions for "overfill protection"

The CAN-XBAND board merges and maps the overflow/underfill protection status from the CAN-RELAY boards to the product level status.

TABLE 2-4 shows the relations between CAN-RELAY board status and the product level status of the GPU protocol <sup>1</sup>.

CAN-RELAY-1	CAN-RELAY-2	CAN-X-BAND
Overflow Protection status	Overflow Protection status	level status GPU protocol
O	O	F
O	H	F
O	W	F
W	O	F
W	H	?
W	W	?
H	O	F
H	H	-
H	W	?
no comms	X	F
X	no comms	F

TABLE 2-4 Relation between CAN-RELAY board status and level status of the GPU protocol

1. The GPU protocol is an Enraf proprietary field bus protocol.



## CHAPTER 3 IMPLEMENTATION

---

### 3.1 General

This chapter provides the information that is relevant for correct implementation of the safety-related function(s) of the SmartRadar FlexLine.

### 3.2 Assumptions and Constraints

The user must install, implement and use the SmartRadar FlexLine according to the conditions that are specified in this manual. The SIL compliant “overflow/underfill protection” or will operate as intended when:

- the compliant architecture is applied,
- the correct configuration is installed and commissioned.

Any radar-based level gauge of the type SmartRadar FlexLine that does not comply with these features cannot be used for this purpose.

### 3.3 New Installation or Upgrade

#### 3.3.1 New Installation

In case you have purchased a SmartRadar FlexLine radar-based level gauge with the option for SIL compliant “overflow/underfill protection”, this function is included by design. This means that the required architecture, hardware and software is present in the device. Correct implementation of the function is obtained by setting the required configuration during commissioning.

#### 3.3.2 Upgrade

In case you own a SmartRadar FlexLine radar-based level gauge, the SIL compliant “overflow/underfill protection” can be included by upgrading the device. By ordering the option for SIL compliant “overflow/underfill protection” you will receive the required features. Implementation of the upgrade needs to be done by a Service Engineer.

Implementation of the upgrade implies:

- two FII-DO modules with SIL compliant functionality are placed; when an FII-DO module is already installed, the user application determines if that module can be used or has to be replaced,
- TII-XR firmware is upgraded,
- “commissioning” is done according to the instructions in the SmartRadar FlexLine Service Manual.

### 3.4 Configuration

Hardware and software features contribute to the SIL compliant “overflow/underfill protection”. TABLE 3-1 specifies the boards the SmartRadar FlexLine must consist of and the relevant firmware (N/A means: not applicable). Further details are described in the next paragraphs.

Board type	Revision	Firmware	Version
ART2A	3 and 4	N/A	N/A
CAN-XBAND	10	TII-XR (FlexConn)	≥ A1030
		TII-XR (DSP)	≥ A1030
CAN-SUPPLY (PSX)	2	N/A	N/A
CAN-RELAY (FIM-DO) *	7	FII-DO	≥ A1005

\*) two CAN-RELAY boards are used for safety related output.

TABLE 3-1 Required boards and firmware

#### 3.4.1 Hardware Configuration

This paragraph describes aspects of the design and integration of the applicable hardware. The required hardware configuration of the SmartRadar FlexLine is achieved by:

- correct use of the specified hardware elements (see TABLE 3-1),
- execution of the hardware settings.

The specified hardware elements are necessary to achieve the SIL compliant “overflow/underfill protection”. These elements are arranged in a specific design (see FIGURE 2-1).

To achieve the 2oo4D approach the relays on the CAN-RELAY boards need to be wired correctly.

FIGURE 3-1 shows a schematic diagram of the SIL compliant application, including the internal wiring principles when two CAN-RELAY boards are used. Also an application controlled output is shown. Furthermore power supply from the CAN-SUPPLY is indicated in this diagram, as well as communication lines between relevant elements.

FIGURE 3-2 shows wiring details for the CAN-RELAY boards.



## Implementation

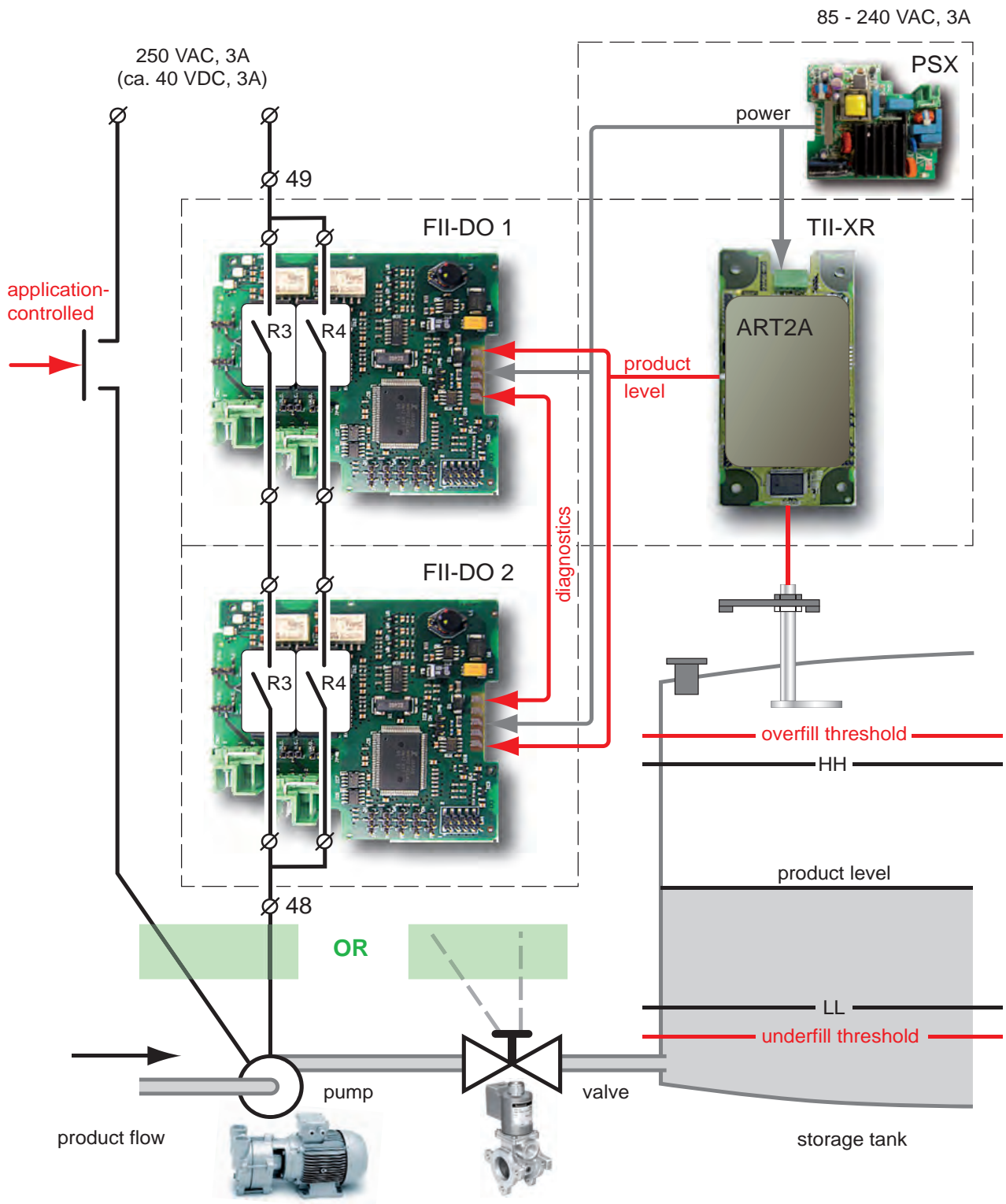


FIGURE 3-1

Overfill protection application using 2 CAN-RELAY boards

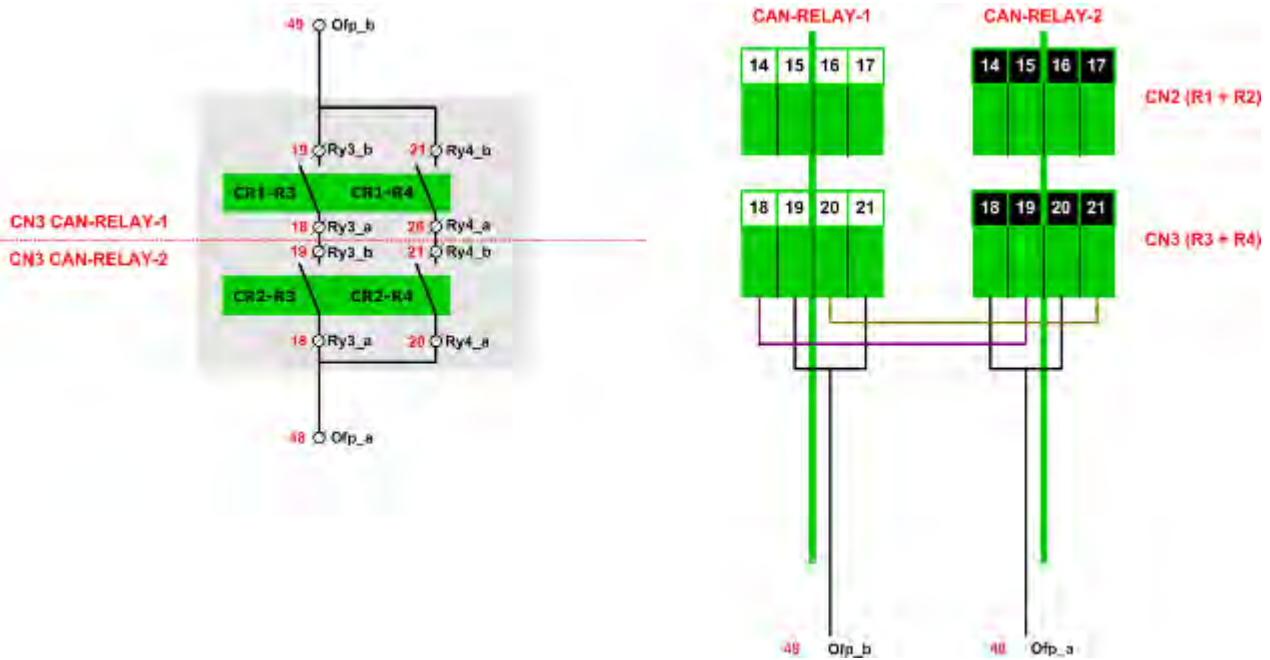


FIGURE 3-2 CAN-RELAY boards - wiring details

The required hardware settings as listed below must be executed for each CAN-RELAY board:

- jumper JP30 must be set to N.O. (= normally open),
- jumper JP40 must be set to N.O. (= normally open).

### 3.4.2 Software Configuration

This paragraph describes the steps to achieve the correct software configuration. The required software configuration of the SmartRadar FlexLine is achieved by:

- execution of the software settings (commissioning),
- verification of the function (see chapter 3.5).

To guarantee correct functioning of the “overflow/underfill protection” both CAN-RELAY boards must be configured identically, except for the Board Instance settings.

TABLE 3-2 provides a basic overview of the applicable entities and their settings. For full details please refer to the “Commissioning” section of the SmartRadar FlexLine Service Manual.

## Implementation

HW element	Entity	Setting
CAN-RELAY board	[Board Instance] *	unique setting *
	[Counterpart Board Instance]	setting of counterpart *
	[Relay Mode]	<Normally Energized>
	[Alarm Mode]	<Local Threshold>
	[Monitor Mode]	<PV Monitoring>
	[Threshold]	refer to "Commissioning"
	[Hysteresis]	refer to "Commissioning"
	[Threshold Mode] For overfill protection - For underfill protection -	<Treat as HA> for R3 and R4 <Treat as LA> for R3 and R4
CAN-XBAND	[Overfill Protection Function]	<Enabled>
	[First Relay Board Instance]	setting of first CAN-RELAY
	[Second Relay Board Instance]	setting of second CAN-RELAY
	Ignore the "Maximum Safe Fill" mechanism.	
	[Maximum safe fill level] OR [Compensations and features] of the 9th switch	above [Threshold] values of the CAN-RELAYS  <FALSE>

\*) the redundant CAN-RELAY boards share the same board ID; Board Instance settings must be unique to enable internal CAN-bus addressing.

TABLE 3-2

Software settings overview

### 3.5 Verification of the Safety Instrumented Function(s)

To verify the correct functioning of the "overfill/underfill protection" function carry out the task described in chapter 4.2 "Proof Testing".

---

## Implementation

---

## CHAPTER 4 MAINTENANCE REQUIREMENTS

---

### 4.1 Purpose

This chapter provides the information that is relevant for correct maintenance of the safety-related function(s) of the SmartRadar FlexLine.

### 4.2 Proof Testing

To make sure that the “overflow/underfill protection” remains SIL compliant a proof test has to be performed once in every 5 year.



Attention!

- By activating the command [\[Start Proof test\]](#) entity, the FII-DO simulates an overflow or underfill. The remainder of the SIF should work as expected (e.g. close a valve, stop a pump, generate an alarm) this should be validated.


*NOTE: This test must only be performed in a healthy situation when the product level in the tank is below the overflow threshold or above the underfill threshold.*

During the proof test - when the level is simulated above or below the threshold - the "Overflow protection status" will indicate "0" in order to enable checking the "Proof test" results in the control room as well.

Each FII-DO of the overflow protection application implements the proof test functionality, so the proof test has to be performed *successively for both modules*.

- By activating the command [\[Stop Proof test\]](#) entity, the FII-DO returns to normal overflow analysis mode again.

*NOTE: The FII-DO module of the SmartRadar FlexLine overflow protection safety application implements an automatic termination of the "Proof test" function in case the user forgets the command [\[Stop Proof test\]](#).*



Engauge  
SmartView

- ❖ Set the [\[Proof test termination time out\]](#) entity to the most desired value in minutes:
  - <0> (auto termination off)
  - <5> (default)
  - <10>
  - <20>
  - <30>

---

## Maintenance Requirements

---



**Honeywell Enraf**

Delftechpark 39

2628 XJ Delft

The Netherlands

Tel: +31 (0)15-2701 100

Email: [hfs-tac-support@honeywell.com](mailto:hfs-tac-support@honeywell.com)

[www.honeywellenraf.com](http://www.honeywellenraf.com)

**Honeywell Enraf**

4417807 - Revision 1  
May 2014

© 2014 Honeywell International Inc.