

Table of contents

1. SCOPE	1
1.1. DEVICE IDENTIFICATION	1
1.2. APPLICABLE DOCUMENTS	2
1.3. RESTRICTIONS	2
2. DEVICE DESCRIPTION	2
2.1. APPLICATION RANGE	2
2.2. OPERATING CONDITIONS	2
2.3. SAFETY FUNCTION	2
2.3.1. Safe state	2
2.3.2. Failure modes	3
2.4. SAFETY-RELATED CHARACTERISTIC DATA	3
3. INSTALLATION NOTES	3
3.1. ELECTRICAL CONNECTION	3
3.2. SETTINGS	4
3.2.1. Configuration	4
3.2.2. Delay	4
3.3. FUNCTION TEST	4
4. APPLICATION NOTES	5
4.1. BEHAVIOR IN CASE OF FAILURE	5
4.2. FAULT REACTION TIME	5
4.3. PERIODIC FUNCTIONAL TESTING	5
5. SIL DECLARATION OF CONFORMITY	5

1. Scope

The Safety manual at hand refers to devices RN 600* with the special requirements for safety technique in accordance with IEC 61508 (option position 25 B "SIL").

1.1. Device identification

The identification of a device is done by its nameplate. On the nameplate a 6-digit device name (RN 600*) is noted. The device name is followed by a 40-digit typecode for identifying several options. Devices with the option SIL are marked with "B" at position 25 of typecode.


UWT GmbH		D-87488 Betzigau Westendstr. 5	
SN	*****		
RN 6001	*****	****	B*****
Supply	24V DC 4W 22..230V AC 10VA	L	200mm
Output	max. 250V AC, 5A max. 30V DC, 4A	T (amb)	-40 ..+50°C
Enclosure	IP66, Type 4	T (process)	-40 ..+80°C
Conduit	1x M20x1.5	P (process)	-0.9.. 0.8bar
		Process con.	NPT 1½"
		Extension	stainless steel
		See instruction manual for proper operation	

Figure: exemplary nameplate with typecode for device identification

1.2. Applicable documents

The following documents have to be considered additional to this Safety manual:

- Series RN 3000 / 6000 Technical information / Instruction manual
- Series RN 3000 / 6000 Selection list
- FMEDA report
- If necessary Ex-documentations

1.3. Restrictions

The Safety manual is only valid for devices listed in section 1.1. Modifications to devices are only allowed to the manufacturer under compliance of the safety life cycle.

2. Device description

2.1. Application range

The device is designed to implement a safety function in a safety-related system.

The device can be used for overall safety functions in low demand mode as well as for overall safety functions in high demand mode / continuous mode.

2.2. Operating conditions

At transport, storage, installation, operation and maintenance of the device the requirements according *Series RN 3000 / 6000 Technical information / Instruction manual* have to be obtained.

Additional to operating conditions the EMC-limits for general industrial applications according EN 61326-3-1 (Electrical equipment for measurement, control and laboratory use - EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications) must not be exceeded.

2.3. Safety function

The safety function of the device is the detection of a limit level of bulk material in containers. Thereby the device can be configured as full detector (overfilling protection) or empty detector (running dry protection).

The output of the safety function depends on the configuration of the device as full detector or empty detector:

- **Full detector:**
detection of a filling level exceeding a defined limit value (covered rotating paddle)
- **Empty detector:**
detection of a filling level below a defined limit value (uncovered rotating paddle)

2.3.1. Safe state

The safe state is given, when the signal output presents an open electric circuit.

Under normal conditions this depends on the state of the rotating paddle:

	Safe state (open circuit at signal output)	Unsafe state (closed circuit at signal output)
Full detector	covered rotating paddle	uncovered rotating paddle
Empty detector	uncovered rotating paddle	covered rotating paddle

In case of failure the device is designed to switch permanent to safe state.

2.3.2. Failure modes

Aging of components can lead to random hardware defects of the device. This can result in a failure of the device. In the following table the possible failures are listed:

Failure modes	Signal output	Correct level indication
Safe, detected failure	open	yes
Safe, undetected failure	open	yes
Unsafe, detected failure	open	no
Unsafe, undetected failure	closed	no

2.4. Safety-related characteristic data

Assumptions for determining safety-related characteristic data:

- Failure rates according to SN 29500
- Single channel architecture (1001D)
- Mean time to repair (MTTR) = 24h

SIL: 2
HFT: 0
Type: B
MTBF: 81 years
Fault reaction time: <120s (see section 4.2)

		Full detector	Empty detector
λ_{SD}		0 FIT	323 FIT
λ_{SU}		268 FIT	269 FIT
λ_{DD}		519 FIT	196 FIT
λ_{DU}		72 FIT	71 FIT
SFF		91.6%	91.8%
PFH		$0.0717 \times 10^{-6}/h$	$0.0706 \times 10^{-6}/h$
PFD _{avg} depending on time interval for periodic function test	1 year	3.2×10^{-4}	3.2×10^{-4}
	2 years	6.3×10^{-4}	6.3×10^{-4}
	5 years	1.6×10^{-3}	1.6×10^{-3}
	10 years	3.2×10^{-3}	3.1×10^{-3}

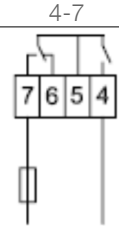
3. Installation notes

3.1. Electrical connection

➔ see Series RN 3000 / 6000 Technical information / Instruction manual

The instructions for electrical connection mentioned in the Technical information / Instruction manual have to be obtained.

The signal output of the safety function has to be connected like in connection example "maximum safety" (see *Series RN 3000 / 6000 Technical information / Instruction manual*).

Terminal block pair for the signal output of the safety function	
Schematic signal output	
Additional terminal blocks <u>not</u> to be used for safety function	5, 6, 8, 9, 10

NOTE: The signal output of the safety function (terminal block pair 4-7) is realized internally by a series connection of two redundant switching relays (terminal block pairs 4-5 and 5-7).

WARNING: The additional terminal blocks (5, 6, 8, 9, 10) are not part of the devices safety function. They can be used according to the instruction manual. The safety-related characteristic data are **not** valid for the additional terminal blocks.

3.2. Settings

3.2.1. Configuration

→ see Series RN 3000 / 6000 Technical information / Instruction manual

WARNING: When configured wrong, the safety function cannot be assured. A missing of the jumper FSH/FSL is diagnosed and turns the device into safe state.

3.2.2. Delay

→ see Series RN 3000 / 6000 Technical information / Instruction manual

WARNING: For the safety function the maximum delay times have to be considered.

3.3. Function test

To avoid systematic failures during installing as well as for periodic functional testing a function test has to be carried out. While the function test is performed, the overall safety function has to be ensured otherwise than by the device.

Procedure of function test:

- **Checking of the device configuration:**
 - Does the configuration (FSH/FSL) correspond to the overall safety function of the device?
- **Checking of the mechanics:**
 - Does the rotating paddle turn when uncovered?
 - Does the rotation speed of the rotating paddle correspond to the devices specification?
 - Does the switching lug tense when changing from uncovered to covered rotating paddle?
- **Checking of the signal output:**
 - Does the signal output in uncovered state correspond to the device configuration (FSH/FSL)?
 - Does the signal output in covered state correspond to the device configuration (FSH/FSL)?
 - Does the delay at the signal output (uncovered to covered rotating paddle / covered to uncovered rotating paddle) correspond the requirement of the overall safety function?

NOTE: The covered / uncovered state has to be induced by ramping-up the bulk material to the respective limit level or by a suitable simulation of this.
The checking of the signal output is done based on a continuity test at terminal block pair 4-5 as well as at terminal block pair 5-7 and has to be identical for both at terminal block pairs.

WARNING: In case of failed function test, the overall safety function has to be ensured otherwise than by the device until replacing.

4. Application notes

4.1. Behavior in case of failure

In case of failure the device turns to safe state.

Furthermore the failure is signalized by light up of the red LED.

Is the failure diagnosed, the safe state is hold even if the diagnosed failure disappears. To reset the failure the supply voltage has to be turned off.

4.2. Fault reaction time

The maximum fault reaction time from appearance until switching to the safe state for failures able to diagnose is 120s. The fault reaction time is independent from the configured delay of the signal output in normal condition (see *Series RN 3000 / 6000 Technical information / Instruction manual*).

4.3. Periodic functional testing

When the device is used to realize a overall safety function in low demand mode, a periodic function test has to be performed. The procedure of the periodic function test is a described in section 3.3.

The maximum time interval for the periodic function test has to be calculated depending on the tolerable failure probability for the device and its PFD_{avg} – value (see section 2.4) according to IEC 61511.

5. SIL Declaration of conformity

UWT GmbH
Westendstraße 5
87488 Betzigau
GERMANY

declares as manufacturer, that the level limit switches RN 600* with the option position 25 B „SIL“ (RN 600* ***** ***** **B***** *****) have been developed corresponding to the requirements of

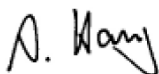
IEC 61508:2010
Functional Safety of
Electrical/Electronic/Programmable Electronic
Safety-related Systems

and are suitable for the use as safety function in safety related systems.

The safety-related characteristic data (see section 2.4) have to be considered.

The safety-related characteristic data were determined by an external, independent institute.

Betzigau, 11/2015



Dipl. Ing. (FH) A. Haug,
Head of Engineering



M.Sc. P. Drey,
Functional Safety Coordinator



Failure Modes, Effects and Diagnostic Analysis

Project:
Level Limit Switch Series RN 600x

Customer:
UWT GmbH
Betzigau
Germany

Contract No.: UWT 13/10-044
Report No.: UWT 13/10-044 R001
Version V1, Revision R0; November 2015

Stephan Aschenbrenner

Management summary

This report summarizes the results of the hardware assessment carried out on the Level Limit Switch Series RN 600x with software version V3.30 and hardware versions as listed in the circuit diagrams referenced in section 2.5.1.

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.

For safety applications only the described Level Limit Switch Series RN 600x with relay outputs was considered. All other possible variants or electronics are not covered by this report.

The failure modes used in this analysis are from the *exida* Electrical Component Reliability Handbook (see [N2]). The failure rates used in this analysis are the basic failure rates from the Siemens standard SN 29500 (see [N4]). This failure rate database is specified in the safety requirements specification from UWT GmbH for the Level Limit Switch Series RN 600x.

UWT GmbH and *exida* together did a quantitative analysis of the sensor specific parts of the Level Limit Switch Series RN 600x to calculate the mechanical failure rates using *exida's* experienced-based data compilation for the different mechanical components ([N3], Profile 3). The worst-case results of this quantitative analysis are part for the calculations described in sections 4.3.2 to 4.3.3.

The Level Limit Switch Series RN 600x can be considered to be a Type B¹ element with a hardware fault tolerance of 0.

The following table shows how the above stated requirements are fulfilled for "Limit detection (MIN/MAX)".

¹ Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2.

Table 1 Summary for RN 600x (full detector – MAX) – IEC 61508 failure rates

Failure category	SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	0
Fail Safe Undetected (λ_{SU})	268
Fail Dangerous Detected (λ_{DD}) ²	519
Fail Dangerous Undetected (λ_{DU})	72
Total failure rate of the safety function (λ_{Total})	859
Safe failure fraction (SFF)³	91%
DC	87%
SIL AC⁴	SIL 2

Table 2 Summary for RN 600x (empty detector – MIN) – IEC 61508 failure rates

Failure category	SN 29500 [FIT]
Fail Safe Detected (λ_{SD})	323
Fail Safe Undetected (λ_{SU})	269
Fail Dangerous Detected (λ_{DD}) ²	196
Fail Dangerous Undetected (λ_{DU})	71
Total failure rate of the safety function (λ_{Total})	859
Safe failure fraction (SFF)³	91%
DC	73%
SIL AC⁴	SIL 2

The failure rates are valid for the useful life of the Level Limit Switch Series RN 600x (see Appendix A).

² The Dangerous Detected (λ_{DD}) values are based on a worst-case diagnostic test rate and a reaction time of 120 seconds. The ratio of the diagnostic test rate to the demand rate shall equal or exceed 100.

³ The complete sensor subsystem will need to be evaluated to determine the overall Safe Failure Fraction. The number listed is for reference only.

⁴ SIL AC (architectural constraints) means that the calculated values are within the range for hardware architectural constraints for the corresponding SIL but does not imply all related IEC 61508 requirements are fulfilled. In addition it must be shown that the device has a suitable systematic capability for the required SIL and that the entire safety function can fulfill the required PFD / PFH values.