Inhalt

1. Geltungsbereich

Das vorliegende Sicherheitshandbuch bezieht sich auf die Geräte RN 600* mit den besonderen Anforderungen der Sicherheitstechnik nach IEC 61508 (Option Position 25 B „SIL“).

1.1. Geräteidentifizierung

Die Identifizierung eines Geräts erfolgt über das Typenschild. Auf dem Typenschild ist eine 6-stellige Gerätebezeichnung (RN 600*) vermerkt.
Im Anschluss an die Gerätebezeichnung folgt ein 40-stelliger Typencode zur Identifizierung von Optionen. Geräte mit der Option SIL zeigen im Typencode an der Position 25 „B“.

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

Abbildung: Beispielhaftes Typenschild mit Typencode zur Geräteidentifizierung

1.2. Mitgeltende Unterlagen

Folgende Unterlagen sind zusätzlich zu diesem Sicherheitshandbuch zu beachten:

- Serie RN 3000 / 6000 Geräteinformation / Betriebsanleitung
- Serie RN 3000 / 6000 Auswahlliste
- FMEDA Report
- ggf. Ex-Unterlagen

1.3. Einschränkungen

Das Sicherheitshandbuch ist für die unter Kap. 1.1 aufgeführten Geräte gültig. Modifikationen an Geräten sind nur vom Hersteller unter Einhaltung des Sicherheitslebenszyklus möglich.

2. Gerätebeschreibung

2.1. Einsatzbereich

Das Gerät ist zur Realisierung einer Sicherheitsfunktion in sicherheitstechnischen Systemen konzipiert.
Das Gerät ist für Schutzfunktionen mit niedriger Anforderungsrate sowie für Schutzfunktionen mit kontinuierlicher Anforderungsrate tauglich.

2.2. Einsatzbedingungen

Bei Transport, Lagerung, Installation, Betrieb und Wartung des Geräts müssen die Anforderungen entsprechend *Serie RN 3000 / 6000 Geräteinformation / Betriebsanleitung* eingehalten werden.

Zusätzlich sind unter den Einsatzbedingungen die EMV-Grenzwerte für Allgemeine industrielle Anwendungen gemäß EN 61326-3-1 (Elektrische Mess-, Steuer-, Regel- und Laborgeräte - EMV-Anforderungen - Teil 3-1: Störfestigkeitsanforderungen für sicherheitsbezogene Systeme und für Geräte, die für sicherheitsbezogene Funktionen vorgesehen sind (Funktionale Sicherheit) - Allgemeine industrielle Anwendungen) nicht zu überschreiten.

2.3. Sicherheitsfunktion

Die Sicherheitsfunktion des Geräts ist die Grenzstandsüberwachung von Schüttgütern in Behältern. Dabei kann das Gerät entweder als Vollmelder (Überfüllschutz) oder als Leermelder (Leerlaufschutz) konfiguriert werden.
Der Ausgang der Sicherheitsfunktion ist abhängig von der Konfiguration des Geräts als Vollmelder oder Leermelder:

- **Vollmelder:**
  Detektion eines Überschreiten eines Füllstands von einem festgelegten Grenzwert (bedeckter Drehflügel)
- **Leermelder:**
  Detektion eines Unterschreiten eines Füllstands von einem festgelegten Grenzwert (unbedeckter Drehflügel)

2.3.1. Sicherer Zustand

Der sichere Zustand ist gegeben, wenn am Ausgang ein geöffneter Stromkreis vorliegt.
Im Normalbetrieb hängt dies vom Zustand des Drehflügels ab:

	Sicherer Zustand (Geöffneter Ausgangsschaltkreis)	Unsicherer Zustand (Geschlossener Ausgangsschaltkreis)
Vollmelder	bedeckter Drehflügel	unbedeckter Drehflügel
Leermelder	unbedeckter Drehflügel	bedeckter Drehflügel

Im Fehlerfall ist das Gerät so konzipiert, dass es permanent in den sicheren Zustand schaltet.

2.3.2. Ausfallmöglichkeiten

Alterungserscheinungen von Bauteilen können zu zufälligen Hardwaredefekten des Geräts führen. Diese können einen Ausfall des Geräts zur Folge haben. Im Folgenden werden die möglichen Ausfälle aufgelistet:

Ausfallmöglichkeit	Ausgangs-Stromkreis	Korrekte Füllstandsanzeige
Sicherer, detektierter Ausfall	offen	ja
Sicherer, nicht detektierter Ausfall	offen	ja
Unsicherer, detektierter Ausfall	offen	nein
Unsicherer, nicht detektierter Ausfall	geschlossen	nein

2.4. Sicherheitstechnische Kenndaten

Annahmen zur Ermittlung der Sicherheitstechnischen Kenndaten:

- Ausfallraten aus SN 29500
- Einkanalige Architektur (1001D)
- Reparaturzeit (MTTR) = 24h

SIL: 2
HFT: 0
Typ: B
MTBF: 81 Jahre
Fehlerreaktionszeit: <120s (siehe Abschnitt 4.2)

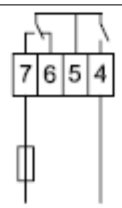
		Vollmelder	Leermelder
λ_{SD}		0 FIT	323 FIT
λ_{SU}		268 FIT	269 FIT
λ_{DD}		519 FIT	196 FIT
λ_{DU}		72 FIT	71 FIT
SFF		91,6%	91,8%
PFH		$0{,}0717 \times 10^{-6}$/h	$0{,}0706 \times 10^{-6}$/h
PFD_{avg} abhängig von Intervallzeit der wiederkehrenden Funktionsprüfung	1 Jahr	$3{,}3 \times 10^{-4}$	$3{,}2 \times 10^{-4}$
	2 Jahre	$6{,}4 \times 10^{-4}$	$6{,}3 \times 10^{-4}$
	5 Jahre	$1{,}6 \times 10^{-3}$	$1{,}6 \times 10^{-3}$
	10 Jahre	$3{,}2 \times 10^{-3}$	$3{,}1 \times 10^{-3}$

3. Installationshinweise

3.1. Elektrischer Anschluss

➔ Siehe Serie RN 3000 / 6000 Geräteinformation / Betriebsanleitung

Die Anweisungen zum Elektrischen Anschluss der Geräteinformation / Betriebsanleitung des eingesetzten Geräts sind zu beachten.
Der Signalausgang der Sicherheitsfunktion ist nach dem Anschlussbeispiel „Maximumsicherheit“ anzuschließen (siehe *Serie RN 3000 / 6000 Geräteinformation / Betriebsanleitung*).

Anschlussklemmenpaar für Signalausgang der Sicherheitsfunktion	4-7
Schaltbild Signalausgang	
Zusätzliche Anschlussklemmen, nicht für Sicherheitsfunktion zu verwenden	5, 6, 8, 9, 10

HINWEIS: Der Signalausgang der Sicherheitsfunktion (Anschlussklemmenpaar 4-7) wird intern durch eine Reihenschaltung zweier redundant schaltender Relais (Anschlussklemmenpaare 4-5 und 5-7) realisiert.

ACHTUNG: Die zusätzlichen Anschlussklemmen (5, 6, 8, 8, 10) sind nicht Teil der Sicherheitsfunktion des Geräts. Sie können gemäß der Betriebsanleitung als Signalausgang verwendet werden. Die sicherheitstechnischen Kenndaten gelten **nicht** für diese zusätzlichen Anschlussklemmen.

3.2. Einstellungen

3.2.1. Konfiguration

➔ Siehe Serie RN 3000 / 6000 Geräteinformation / Betriebsanleitung

ACHTUNG: Bei falscher Konfiguration wird die Sicherheitsfunktion nicht gewährleistet. Das Fehlen des Jumpers FSH/FSL wird diagnostiziert und schaltet das Gerät in den sicheren Zustand.

3.2.2. Verzögerung

➔ Siehe Serie RN 3000 / 6000 Geräteinformation / Betriebsanleitung

ACHTUNG: Für die Sicherheitsfunktion sind die maximalen Verzögerungswerte zu berücksichtigen.

3.3. Funktionstest

Zur Vermeidung systematischer Fehler bei der Installation sowie zur wiederkehrenden Funktionsprüfung ist ein Funktionstest durchzuführen. Während des Funktionstests ist für eine anderweitige Realisierung der Schutzfunktion als durch das Gerät zu sorgen.

Ablauf des Funktionstests:

- Überprüfung der Konfiguration des Geräts:
  - Entspricht die Konfiguration (FSH/FSL) des Geräts der Schutzfunktion?
- Überprüfung der Mechanik:
  - Dreht sich der Drehflügel im unbedeckten Zustand?
  - Entspricht die Drehgeschwindigkeit des Drehflügels der Spezifikation des Geräts?
  - Spannt sich die Schaltlasche beim Übergang vom unbedeckten in den bedeckten Zustand?
- Überprüfung des Signalausgangs:
  - Ist der Signalausgang bei unbedecktem Drehflügel entsprechend der Konfiguration (FSH/FSL) des Geräts?
  - Ist der Signalausgang bei bedecktem Drehflügel entsprechend der Konfiguration (FSH/FSL) des Geräts?
  - Entspricht die Verzögerung am Signalausgang (unbedeckter -> bedeckter Drehflügel / bedeckter -> unbedeckter Drehflügel) den Anforderungen der Schutzfunktion?

HINWEIS: Der bedeckte / unbedeckte Zustand ist durch Anfahren des jeweiligen Grenzstands mit Schüttgut oder durch eine geeignete Simulation dessen herzustellen.
Die Überprüfung des Signalausgangs ist anhand einer Durchgangsprüfung an dem Anschlussklemmenpaar 4-5 sowie dem Anschlussklemmenpaar 5-7 durchzuführen, und muss für beide Anschlussklemmenpaare identisch sein.

ACHTUNG: Bei nicht bestandenem Funktionstest ist bis zum Ersatz des Geräts für eine anderweitige Realisierung der Schutzfunktion Sorge zu tragen.

4. Anwendungshinweise

4.1. Verhalten im Fehlerfall

Im Fehlerfall schaltet das Gerät in den sicheren Zustand.
Zusätzlich wird der Fehlerfall durch Aufleuchten der roten LED signalisiert.
Wird ein Fehler diagnostiziert, wird der sichere Zustand beibehalten, auch wenn der diagnostizierte Fehler wieder verschwindet. Zum Zurücksetzen des Fehlers ist eine Unterbrechung der Spannungsversorgung notwendig.

4.2. Fehlerreaktionszeit

Die maximale Fehlerreaktionszeit vom Auftreten eines Fehlers bis zum Schalten in den sicheren Zustand für diagnostizierbare Fehler beträgt 120s.
Die Fehlerreaktionszeit ist unabhängig von der eingestellten Verzögerung des Signalausgangs im normalen Betrieb (siehe *Serie RN 3000 / 6000 Geräteinformation / Betriebsanleitung*).

4.3. Wiederkehrenden Funktionsprüfung

Wird das Gerät für die Realisierung von Schutzfunktionen mit niedriger Anforderungsrate eingesetzt, ist an dem Gerät eine wiederkehrende Funktionsprüfung durchzuführen. Zum Ablauf der wiederkehrenden Funktionsprüfung siehe Abschnitt 3.3.

Die maximale Intervallzeit der wiederkehrenden Funktionsprüfung ist in Abhängigkeit von der tolerierbaren Fehlerwahrscheinlichkeit für das Gerät und dem PFD_{avg} –Wert (siehe Abschnitt 2.4) entsprechend IEC 61511 festzulegen.

5. SIL Konformitätserklärung

UWT GmbH
Westendstraße 5
87488 Betzigau
GERMANY

erklärt als Hersteller, dass die Grenzstandsmelder RN 600* mit der Option Position 25 B „SIL“
(RN 600* ********** ********** ****B***** **********) gemäß den Anforderungen der

IEC 61508:2010
Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

entwickelt worden sind, und zum Einsatz in Sicherheitsfunktionen sicherheitstechnischer Systeme geeignet sind.
Die sicherheitstechnischen Kenndaten (siehe Abschnitt 2.4) sind zu berücksichtigen.
Die sicherheitstechnischen Kenndaten wurden von einem unabhängigen, externen Institut ermittelt.

Betzigau, 11/2015

Dipl. Ing (FH) A. Haug,
Technischer Leiter

M.Sc. P. Drey,
Koordinator Funktionale Sicherheit

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 B[1] 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 AC [4]	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 AC [4]	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.