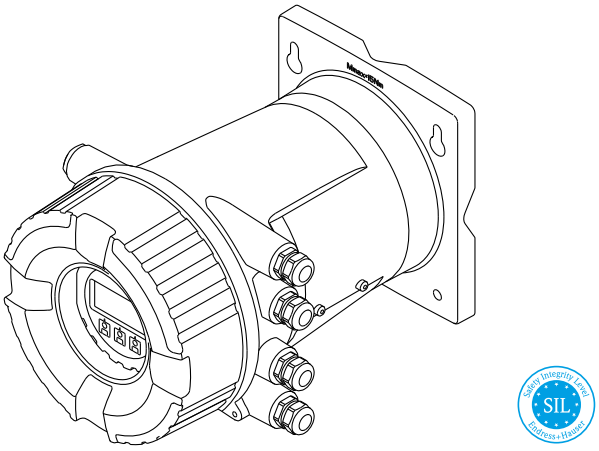
SD01929G/00/DE/04.20
71498585
2020-10-07

Sonderdokumentation
Tankside Monitor NRF81

Handbuch zur Funktionalen Sicherheit



Tankside Monitor mit Stromausgang 4 … 20 mA und Schaltausgang

Endress+Hauser
People for Process Automation

Inhaltsverzeichnis

Konformitätserklärung

SIL_00323_02.20

Endress+Hauser
People for Process Automation

Declaration of Conformity

Functional Safety according to IEC 61508
Based on NE 130 Form B.1

Endress+Hauser SE+Co. KG, Hauptstraße 1, 79689 Maulburg

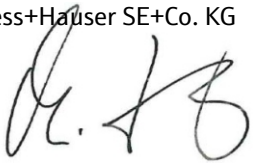
being the manufacturer, declares that the product

Tankside Monitor NRF81

is suitable for the use in safety-instrumented systems according to IEC 61508. The instructions of the corresponding functional safety manual must be followed.

This declaration of compliance is exclusively valid for the customer listed in the cover letter of the respective Endress+Hauser sales center and for the listed products and accessories in delivery status.

Maulburg, 31-July-2020
Endress+Hauser SE+Co. KG



i. V.
Manfred Hammer
Dept. Man. Technology
Quality Management / FSM
Research & Development

A0044234

SIL_00323_02.20

Endress+Hauser
People for Process Automation

General			
Device designation and permissible types	Tankside Monitor NRF8x - *********+LA		
	x = 1		
Safety-related output signal [a] [b]	[a] 4...20 mA	[b] relay contact	
Fault signal [a] [b]	[a] ≤ 3.6 mA ; ≥ 21 mA	[b] open contact	
Process variable/function	Current in measurement		
Safety function(s)	MIN, MAX, Range		
Device type acc. to IEC 61508-2	☐ Type A	☒ Type B	
Operating mode	☒ Low Demand Mode	☒ High Demand Mode	☐ Continuous Mode
Valid hardware version	As of manufacturing date after Nov.28,2016		
Valid software version	As of 01.02.zz (zz: any double number)		
Safety manual	SD01929G		
Type of evaluation (check only one box)	☒	Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3	
	☐	Evaluation of "proven in use" performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, 3	
	☐	Evaluation of HW/SW field data to verify „prior use" acc. to IEC 61511	
	☐	Evaluation by FMEDA acc. to IEC 61508-2 for devices w/o software	
Evaluation through – report/certificate no.	TÜV Rheinland Industrie Service GmbH-report no. 968/FSP 1809.00/19 and Worksheet		
Test documents	Development documents	Test reports	Data sheets

SIL - Integrity			
Systematic safety integrity		☐ SIL 2 capable	☒ SIL 3 capable
Hardware safety integrity	Single channel use (HFT = 0)	☒ SIL 2 capable	☐ SIL 3 capable
	Multi channel use (HFT 1)	☐ SIL 2 capable	☒ SIL 3 capable

FMEDA			
Safety function	MIN	MAX	Range
λ_{DU} [1),2)]	157 FIT	157 FIT	157 FIT
λ_{DD} [1),2)]	4990 FIT	4990 FIT	4990 FIT
λ_{SU} [1),2)]	2255 FIT	2255 FIT	2255 FIT
λ_{SD} [1),2)]	0 FIT	0 FIT	0 FIT
SFF	97 %	97 %	97 %
PFD_{avg} (T_1 = 1 year) [2)] (single channel architecture)	7.27×10^{-4}	7.27×10^{-4}	7.27×10^{-4}
PFD_{avg} (T_1 = 2 years) [2)] (single channel architecture)	1.41×10^{-3}	1.41×10^{-3}	1.41×10^{-3}
PFH	1.57×10^{-7} 1/h	1.57×10^{-7} 1/h	1.57×10^{-7} 1/h
PTC [3)]	Depending on the proof test, see safety manual	Depending on the proof test, see safety manual	Depending on the proof test, see safety manual
λ_{total} [1,2)]	7402 FIT	7402 FIT	7402 FIT
Diagnostic test interval [4)]	60 min	60 min	60 min
Fault reaction time [5)]	1 min	1 min	1 min

Comments
–

Declaration	
☒	Our internal company quality management system ensures information on safety-related systematic faults which become evident in the future

[1)] FIT = Failure In Time, number of failures per 10^9 h
[2)] Valid for average ambient temperature up to +40 °C (+104 °F)
For continuous operation at ambient temperature close to +60 °C (+140 °F), a factor of 2.1 should be applied
[3)] PTC = Proof Test Coverage
[4)] All diagnostic functions are performed at least once within the diagnostic test interval
[5)] Maximum time between error recognition and error response

A0044235

Weitere sicherheitstechnische Kenngrößen

Kenngröße gemäß IEC 61508	Wert
MTBF [1]	36 Jahre
Systemreaktionszeit nach DIN EN 61508-2	Im Betriebs-Mode "Experten-Parametrierung": Frei parametrierbar

1) Gemäß Siemens SN29500. Dieser Wert berücksichtigt funktionsrelevante Ausfallarten der Elektronikkomponenten.

Gebrauchsdauer elektrischer Bauteile

Die zugrunde gelegten Ausfallraten elektrischer Bauteile gelten innerhalb der Gebrauchsdauer gemäß IEC 61508-2:2010 Abschnitt 7.4.9.5 Hinweis 3. Nach DIN EN 61508-2:2011 Abschnitt 7.4.9.5 Nationale Fußnote N3 sind durch entsprechende Maßnahmen des Herstellers und des Betreibers längere Gebrauchsdauern zu erreichen.

Zertifikat

Certificate

No.: 968/FSP 1809.00/19

Product tested	Tank Side Monitor	**Certificate holder**	Endress+Hauser SE + Co. KG Hauptstraße 1 79689 Maulburg Germany
Type designation	NRF81		
Codes and standards	IEC 61508 Parts 1-7:2010		
Intended application	The device complies with the requirements of Hardware Safety Integrity SIL 2 and Systematic Capability SC 3 acc. to IEC 61508 and can be used in applications up to SIL 2 (HFT=0) resp. SIL 3 (HFT=1) for following safety function: "Safe current in measurement (min, max, range) within the measuring range, accuracy of ±1% and with safe analogue and/or digital outputs".		
Specific requirements	The instructions of the associated Operating Manual and Safety Manual shall be considered.		

Valid until 2024-02-26

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1809.00/19 dated 2019-01-29.
This certificate is valid only for products which are identical with the product tested.

Köln, 2019-02-26

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln
Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Gebhard Bouwer

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

A0040360

Hinweise zum Dokument

Dokumentfunktion

Das Dokument ist Teil der Betriebsanleitung und dient als Nachschlagwerk für anwendungsspezifische Parameter und Hinweise.

- Allgemeine Informationen über Funktionale Sicherheit: SIL
- Die allgemeinen Informationen zu SIL sind verfügbar:
  Im Download-Bereich der Endress+Hauser Internetseite: www.de.endress.com/SIL

Umgang mit dem Dokument

Informationen zum Dokumentaufbau

Zur Anordnung der Parameter mit Kurzbeschreibung gemäß Menü **Betrieb**, Menü **Setup**, Menü **Diagnose**: Betriebsanleitung zum Gerät

Verwendete Symbole

Warnhinweissymbole

Symbol	Bedeutung
GEFAHR	**GEFAHR!** Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu Tod oder schwerer Körperverletzung führen wird.
WARNUNG	**WARNUNG!** Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu Tod oder schwerer Körperverletzung führen kann.
VORSICHT	**VORSICHT!** Dieser Hinweis macht auf eine gefährliche Situation aufmerksam, die, wenn sie nicht vermieden wird, zu leichter oder mittelschwerer Körperverletzung führen kann.
HINWEIS	**HINWEIS!** Dieser Hinweis enthält Informationen zu Vorgehensweisen und weiterführenden Sachverhalten, die keine Körperverletzung nach sich ziehen.

Symbole für Informationstypen

Symbol	Bedeutung
A0011193	**Tipp** Kennzeichnet zusätzliche Informationen.
	Verweis auf Dokumentation
	Verweis auf Seite
	Verweis auf Abbildung
1., 2., 3...	Handlungsschritte

Symbole in Grafiken

Symbol	Bedeutung
1, 2, 3,...	Positionsnummern
1., 2., 3...	Handlungsschritte
A, B, C, ...	Ansichten

Mitgeltende Dokumentation

Dokumentation	Bemerkung
Technische Information: TI01251G/00	Die Dokumentation steht über das Internet zur Verfügung: → www.endress.com
Betriebsanleitung BA01465G/00	Die Dokumentation steht über das Internet zur Verfügung: → www.endress.com
Kurzanleitung : KA01209G/00	▪ Die Dokumentation liegt dem Gerät bei. ▪ Die Dokumentation steht über das Internet zur Verfügung: → www.endress.com
Sicherheitshinweise abhängig von der gewählten Option in Bestellmerkmal "Zulassung".	Bei zertifizierten Geräteausführungen werden zusätzliche Sicherheitshinweise (XA, ZE) mitgeliefert. Dem Typenschild kann entnommen werden, welche Sicherheitshinweise für die jeweilige Gerätevariante relevant sind.

Dieses Sicherheitshandbuch gilt ergänzend zur Betriebsanleitung, Technischen Information und zu den ATEX-Sicherheitshinweisen. Die mitgeltende Gerätedokumentation ist bei Installation, Inbetriebnahme und Betrieb zu beachten. Die für die Schutzfunktion abweichenden Anforderungen sind in diesem Sicherheitshandbuch beschrieben.

Zulässige Gerätetypen

Die in diesem Handbuch enthaltenen Angaben zur Funktionalen Sicherheit sind für die unten angegebenen Geräteausprägungen und ab der genannten Soft- und Hardwareversion gültig. Sofern nicht anderweitig angegeben, sind alle nachfolgenden Versionen ebenfalls für Sicherheitsfunktionen einsetzbar. Bei Geräteänderungen wird ein zu IEC 61508 konformer Modifikationsprozess angewendet.

Gültige Geräteausprägungen für sicherheitsbezogenen Einsatz:

Bestellmerkmal	Benennung	Option
010	Zulassung	alle
020	Anschlusstyp	alle
030	Energieversorgung; Anzeige	alle
040	Primärer Ausgang	siehe nächste Tabelle
050	Sekundär I/O Analog	siehe nächste Tabelle
060	Sekundär I/O Digital Ex d/XP	siehe nächste Tabelle
070	Gehäuse	alle, außer Y9
090	Elektrischer Anschluss	alle
150	Genauigkeit, Eichzulassung	alle
500	Bediensprachen; Anzeige	alle
540	Anwendungspaket	alle
570	Dienstleistung	alle
580	Test; Zeugnis	alle
590	Weitere Zulassung	LA [1)] SIL
610	Zubehör montiert	alle
620	Zubehör beigelegt	alle
850	Firmware Version	Ist hier keine Ausprägung gewählt, wird die aktuelle SIL-fähige SW geliefert. Alternativ kann folgende SW-Version gewählt werden: 01.02.zz oder 01.03.zz
895	Kennzeichnung	alle

1) Eine zusätzliche Auswahl weiterer Ausprägungen ist möglich.

Bestellmerkmal	040	050	060
Option	E1	A1 oder B1	*
	H1	A1 oder B1	*
	E1	*	A1, A2, A3, B2 oder B3
	H1	*	A1, A2, A3, B2 oder B3
	*	A2	*
	*	B2	*
	*	C2	*
	*	A1	A1, A2, A3, B2 oder B3
	*	B1	A1, A2, A3, B2 oder B3

* Alle Optionen sind möglich. (Diese Auswahl beeinflusst nicht die SIL-Fähigkeit.)

- Gültige Firmware-Version: ab 01.02.zz (→ Gerätetypenschild)
- Gültige Hardware-Version (Elektronik): ab Herstellungsdatum 23.11.2016 (→ Gerätetypenschild)

SIL-Kennzeichnung auf dem Typenschild

SIL-zertifizierte Geräte sind mit folgendem Symbol auf dem Typenschild gekennzeichnet: SIL

Sicherheitsfunktion

Definition der Sicherheitsfunktion

Die Sicherheitsfunktion des Messgeräts ist:

Stromeingangsüberwachung

Die Sicherheitsfunktion beinhaltet die Messung des Stroms eines angeschlossenen Geräts.

Sicherheitsbezogenes Signal

Digital

Das sicherheitsbezogene Signal des Geräts ist der geschlossene Relaiskontakt des digitalen Ausgangs. Alle Sicherheitsmaßnahmen beziehen sich ausschließlich auf dieses Signal.

Der analoge Eingangsstrom (Sicherheitsfunktion) wird korrekt in einen digitalen Ausgangswert umgewandelt. Innerhalb des Gültigkeitsbereiches ist der Relaiskontakt geschlossen, außerhalb offen.

Das sicherheitsbezogene Ausgangssignal wird einer nachgeschalteten Logikeinheit wie z.B. einer speicherprogrammierbaren Steuerung oder einem Grenzsignalgeber zugeführt und dort überwacht auf:
- Überschreiten und/oder Unterschreiten eines vorgegebenen Grenzstandes.
- Eintreten einer Störung, z. B. Kontakt offen (Unterbrechung der Signalleitung).

Im Fehlerfall ist sicher zu stellen, dass die zu überwachende Anlage in einem sicheren Zustand bleibt oder in einen sicheren Zustand gebracht werden kann.

Analog

Das sicherheitsbezogene Signal des Geräts ist das analoge Ausgangssignal 4 … 20 mA. Alle Sicherheitsmaßnahmen beziehen sich ausschließlich auf dieses Signal.

Zusätzlich kann das Gerät informativ die Kommunikation über HART ausgeben und beinhaltet alle HART-Merkmale mit zusätzlichen Geräteinformationen.

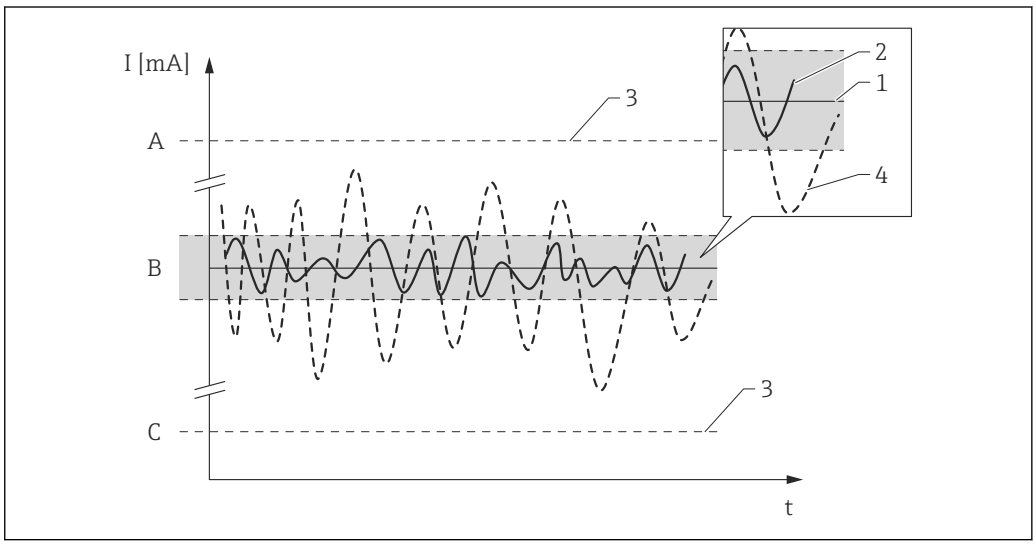
Das sicherheitsbezogene Ausgangssignal wird einer nachgeschalteten Logikeinheit wie z.B. einer speicherprogrammierbaren Steuerung oder einem Grenzsignalgeber zugeführt und dort überwacht auf:
- Überschreiten und/oder Unterschreiten eines vorgegebenen Grenzstandes.
- Eintreten einer Störung, z. B. Fehlerstrom (≤3,6 mA, ≥21,0 mA), Unterbrechung oder Kurzschluss der Signalleitung).

Im Fehlerfall ist sicher zu stellen, dass die zu überwachende Anlage in einem sicheren Zustand bleibt oder in einen sicheren Zustand gebracht werden kann.

Einschränkung für die Anwendung im sicherheitsbezogenen Betrieb

- Angaben zum sicherheitsbezogenen Signal (→ 10).
- Die Spezifikationen aus den Betriebsanleitungen dürfen nicht überschritten werden (→ 8).
- Zusätzlich gilt für den sicherheitsbezogenen Einsatz folgende Einschränkung:
  - Starke, impulsartige EMV-Störungen auf der Leitung können zu kurzzeitigen (<1 s) Abweichungen ≥±2 % des Ausgangssignals führen. Deshalb sollte in der nachgeschalteten Logikeinheit eine Filterung mit einer Zeitkonstante ≥1 s durchgeführt werden.
  - Das Fehlerband ist gerätespezifisch und wird ab Werk gemäß FMEDA (Failure Modes, Effects and Diagnostic Analysis) definiert. Es sind alle in der Technischen Information beschriebenen Einflussfaktoren bereits enthalten (z.B. Nichtlinearität, Nichtwiederholbarkeit, Hysterese, Nullpunktabweichung, Temperaturdrift, EMV-Einfluss).
    Die sicherheitstechnischen Fehler sind gemäß IEC / EN 61508 in unterschiedliche Kategorien eingeteilt (siehe folgende Tabelle). Die Tabelle zeigt die Auswirkungen auf das sicherheitsbezogene analoge Ausgangssignal und die Messunsicherheit.

Sicherheitstechnische Fehler	Erklärung	Auswirkung auf das sicherheitsbezogene Ausgangssignal	Auswirkung auf die Messunsicherheit (Position, siehe Abb. → 11)
Kein Gerätefehler	Safe: Keine Fehler vorhanden	Keine	1 Liegt innerhalb der Spezifikation (siehe TI, BA, ...)
λ_{SD}	Safe detected: Sicherer und erkennbarer Fehler	Führt zu einem Fehlerverhalten am Ausgangssignal (siehe, → 12)	3 Hat keinen Einfluss
λ_{SU}	Safe undetected: Sicherer aber nicht erkennbarer Fehler	Bewegt sich innerhalb des festgelegten Fehlerbandes	2 Kann außerhalb der Spezifikation liegen
λ_{DD}	Dangerous detected: Gefährlicher aber erkennbarer Fehler (Diagnose im Gerät)	Führt zu einem Fehlverhalten am Ausgangssignal (siehe, → 12)	3 Hat keinen Einfluss
λ_{DU}	Dangerous undetected: Gefährlicher und nicht erkennbarer Fehler	Kann außerhalb des festgelegten Fehlerbandes liegen	4 Kann außerhalb des festgelegten Fehlerbandes liegen



A HI-Alarm ≥21 mA
B Fehlerband ±2 %
C LO-Alarm ≤3,6 mA

Gefährliche unerkannte Fehler in dieser Betrachtung

Als gefährlich unerkannter Fehler wird ein falsches Ausgangssignal betrachtet, das vom realen Messwert um mehr als 2 % abweicht, wobei das Ausgangssignal weiterhin im Bereich von 4 ... 20 mA liegt bzw. der Relaiskontakt weiterhin geschlossen ist.

Einsatz in Schutzeinrichtungen

Geräteverhalten im Betrieb

Digital

Geräteverhalten beim Einschalten

Nach dem Einschalten durchläuft das Gerät eine Diagnosephase von ca. 30 Sekunden. Während dieser Zeit ist der Relaiskontakt geöffnet. Während der Diagnosephase ist keine Kommunikation über die Serviceschnittstelle (CDI) oder über Protokolle (HART, V1, Modbus) möglich.

Geräteverhalten bei Anforderung der Sicherheitsfunktion

Das Gerät gibt einen dem zu überwachenden Grenzwert entsprechenden digitalen Ausgangswert an. Innerhalb des Gültigkeitsbereiches ist der Relaiskontakt geschlossen, außerhalb offen. Dies muss von einer angeschlossenen Logikeinheit entsprechend überwacht und weiterverarbeitet werden.

Geräteverhalten bei Alarmen und Warnungen

Das Relaisverhalten bei Alarmen und Warnungen ist immer ein offener Kontakt. Dies muss von einer angeschlossenen Logikeinheit entsprechend überwacht und weiterverarbeitet werden.

Alarm- und Warnmeldungen

Die ausgegebenen Alarm- und Warnmeldungen in Form von Fehlercodes und zugehörigen Klartextmeldungen sind zusätzliche Informationen.

Folgende Tabelle zeigt den Zusammenhang zwischen Fehlercode und ausgegebenem Relaiskontakt:

Fehlercode [1]	Relaiskontakt (Meldungstyp)	Anmerkung
Fxxx	offen	xxx = dreistellige Zahl
Mxxx	entsprechend dem Messbetrieb	xxx = dreistellige Zahl
Cxxx	entsprechend dem Messbetrieb	xxx = dreistellige Zahl
Sxxx	entsprechend dem Messbetrieb	xxx = dreistellige Zahl

1) Die Fehlercodes sind in der Betriebsanleitung aufgelistet.

Analog

Geräteverhalten beim Einschalten

Nach dem Einschalten durchläuft das Gerät eine Diagnosephase von ca. 30 Sekunden. Während dieser Zeit befindet sich der Stromausgang auf Fehlerstrom ≤3,6 mA.

Während der Diagnosephase ist keine Kommunikation über die Serviceschnittstelle (CDI) oder über Protokolle (HART, V1, Modbus) möglich.

Geräteverhalten bei Anforderung der Sicherheitsfunktion

Das Gerät gibt einen dem zu überwachenden Grenzwert entsprechenden Stromwert aus, der in einer angeschlossenen Logikeinheit überwacht und weiterverarbeitet werden muss.

Geräteverhalten bei Alarmen und Warnungen

Der Ausgangsstrom bei Alarm kann auf einen Wert von ≤3,6 mA oder ≥21,0 mA eingestellt werden.

In einigen Fällen, z.B. Ausfall der Versorgung, einem Leitungsbruch, sowie Störungen im Stromausgang selbst, bei denen der Fehlerstrom ≥21,0 mA nicht gestellt werden kann, liegen unabhängig vom eingestellten Fehlerstrom Ausgangsströme ≤3,6 mA an.

In einigen anderen Fällen, z.B. Kurzschluss der Zuleitung, liegen unabhängig vom eingestellten Fehlerstrom Ausgangsströme ≥21,0 mA an.

Zur Alarmüberwachung muss die nachgeschaltete Logikeinheit Fehlerströme des oberen Ausfallsignalpegels (≥21,0 mA) und des unteren Ausfallsignalpegels (≤3,6 mA) erkennen können.

Alarm- und Warnmeldungen

Die ausgegebenen Alarm- und Warnmeldungen in Form von Fehlercodes und zugehörigen Klartextmeldungen sind zusätzliche Informationen.

Folgende Tabelle zeigt den Zusammenhang zwischen Fehlercode und ausgegebenem Strom:

Fehlercode [1]	Stromausgang (Meldungstyp)	Anmerkung
Fxxx	≥ 21,0 mA oder ≤ 3,6 mA	xxx = dreistellige Zahl
Mxxx	entsprechend dem Messbetrieb	xxx = dreistellige Zahl
Cxxx	entsprechend dem Messbetrieb	xxx = dreistellige Zahl
Sxxx	entsprechend dem Messbetrieb	xxx = dreistellige Zahl

1) Die Fehlercodes sind in der Betriebsanleitung aufgelistet.

Ausnahmen:

Fehlercode [1]	Stromausgang (Meldungstyp)	Anmerkung
C484	≥ 21,0 mA oder ≤ 3,6 mA	Simulation Fehlermodus

1) Die Fehlercodes sind in der Betriebsanleitung aufgelistet.

Geräteparametrierung für sicherheitsbezogene Anwendungen

Es wird empfohlen vor der Parametrierung ein Werksreset durchzuführen.

Navigieren zu: Setup → Erweitertes Setup → Administration

Gerät zurücksetzen = **Auf Werkseinstellung**

Alle Parameter werden auf definierte Werte zurückgesetzt.

Abgleich der Messstelle

Der Abgleich der Messstelle ist in der Betriebsanleitung beschrieben (→ 🖹 8).

Festlegen, welche Art von Konfiguration a) oder b) genutzt werden soll. Beide Konfigurationen können parallel betrieben werden.

a) Analog Eingang (Quelle) (1) -> Sicherheitsbezogenes Signal: Analog Ausgang (2)
b) Analog Eingang (Quelle) (1) -> Sicherheitsbezogenes Signal: Digital Ausgang (3)

Analog Eingang (Quelle) (1)

Es ist zu beachten, dass die richtige Quelle parametriert wird (Analog I/O B1-3 oder Analog I/O C1-3).

Navigieren zu: Setup → Erweitertes Setup → Ein/Ausgang → Analog I/O

Einstellung
- **Betriebsart** = **4..20mA Eingang** oder **HART Master+4..20mA Eingang**
- **AI 0% Wert** muss richtig eingestellt werden.
- **AI 100% Wert** muss richtig eingestellt werden.

Analog Ausgang (2)

Es ist zu beachten, dass der richtige Ausgang parametriert wird (Analog I/O B1-3 oder Analog I/O C1-3).

Navigieren zu: Setup → Erweitertes Setup → Ein/Ausgang → Analog I/O

Einstellung
- **Betriebsart** = **4..20mA Ausgang** oder **HART Slave+4..20mA Ausgang**
- **Quelle Analog** = **AIO B1-3 Wert mA** bzw. **AIO C1-3 Wert mA** (je nach Quelle)
- **0 % Wert**
- **100 % Wert**
- **Genutzt für SIL** = **Aktiviert**

Digital Ausgang (3)

Zuerst ist ein Alarmblock (Alarm 1, Alarm 2, Alarm 3 oder Alarm 4) für die Grenzwerteinstellungen zu wählen.

Navigieren zu: Setup → Erweitertes Setup → Applikation → Alarm 1 → Alarm X

Einstellung
- **Alarm Modus** = **An**
- **Quelle Alarm Wert** = **AIO B1-3 Wert mA** oder **AIO C1-3 Wert mA** (je nach Quelle)
- **HH Alarm Wert**, **H Alarm Wert**, **L Alarm Wert** und **LL Alarm Wert** müssen entsprechend der Anwendung so eingestellt werden, dass der gültige Bereich innerhalb der HH, H und L, LL Grenzen liegt.

Es ist zu beachten, dass der richtige Ausgang parametriert wird (Digital A1-2, Digital A3-4, Digital B1-2, Digital B3-4, Digital C1-2, Digital C3-4, Digital D1-2, Digital D3-4).

Navigieren zu: Setup → Erweitertes Setup → Ein/Ausgang → Digital Xy-z

Einstellung
- **Betriebsart** = **Ausgang passiv**
- **Quelle Digitaleingang** = ausgewählter Alarmblock (**Alarm 1 Alle**, **Alarm 2 Alle**, **Alarm 3 Alle** oder **Alarm 4 Alle**)
- **Genutzt für SIL** = **Aktiviert** muss eingestellt werden, um diesen Digital-Ausgang als SIL-Ausgang zu nutzen.

Methode der Parametrierung

Beim Einsatz der Geräte in PLT-Schutzeinrichtungen muss die Geräteparametrierung zwei Anforderungen erfüllen:
- Bestätigungskonzept:
  Nachgewiesenes unabhängiges Überprüfen eingegebener sicherheitsrelevanter Parameter.
- Verriegelungskonzept:
  Verriegelung des Geräts nach erfolgter Parametrierung (IEC 61511-1: 2016 Abschnitt 11.6.3).

Zur Aktivierung des SIL-Betriebs muss eine Bediensequenz durchlaufen werden, wobei die Bedienung über das Gerätedisplay oder ein beliebiges Asset Management Tool erfolgen kann (z. B. FieldCare) für das eine Integration zur Verfügung steht.

"Expertenmodus"

Hier ist eine größere Zahl an sicherheitsrelevanten Parametern frei einstellbar.

Eine detaillierte Beschreibung der Einstellungsschritte erfolgt im nachfolgenden Kapitel.

Nur bei SIL-Geräten (Bestellmerkmal 590 "Weitere Zulassungen", Option LA "SIL") ist die SIL-Inbetriebnahmesequenz am Display und in externen Bedientools sichtbar. Daher kann auch nur bei solchen Geräten die SIL-Verriegelung aktiviert werden.

Verriegelung im "Expertenmodus"

Zur Inbetriebnahme des Geräts folgende Schritte in der angegebenen Reihenfolge durchführen und dokumentieren → 🖹 23:

1. Parametrierung durchführen, siehe auch → 🖹 13: Die Vorgehensweise zur Parametrierung sowie die Bedeutung der einzelnen Parameter sind in der Betriebsanleitung beschrieben → 🖹 8. Die Parametereinstellungen der folgenden Tabelle müssen beachtet werden → 🖹 16.
2. SIL-Bestätigungssequenz starten.
   Navigieren zu: Setup → Erweitertes Setup → SIL/WHG-Bestätigung
   Schreibschutz setzen = entsprechenden Verriegelungscode eingeben (SIL: 7452). Mit "Weiter" bestätigen.
3. **Inbetriebnahme** = **Expertenmodus** mit "Weiter" bestätigen. Das Gerät überprüft die Parametereinstellungen entsprechend der nachfolgenden Tabelle → 🖹 16 und führt gegebenenfalls eine Zwangsumschaltung von Parametern durch.
   Nach abgeschlossener Überprüfung wird **SIL-Vorbereitung** = **Fertig** angezeigt. Die Inbetriebnahmesequenz kann fortgeführt werden.
   Mit "Weiter" bestätigen.

4. Funktionstest durchführen: Für MIN- und MAX-Überwachung muss mindestens ein Stromeingangswert oberhalb (MAX-Überwachung) oder unterhalb (MIN-Überwachung) des Schaltpunkts angefahren werden.
   Für Bereichsüberwachung sollten 5 Stromeingangswerte angefahren werden, die den kompletten Messbereich abdecken. Dabei jeweils die richtige Reaktion des sicherheitsbezogenen Signals (Stromausgang/Relais) prüfen.
5. Den erfolgreichen Funktionstest bestätigen:
   Funktionstest bestätigen = **Ja**.
6. **Schreibschutz setzen** = Verriegelungscode erneut eingeben (SIL: 7452). Nach der SIL-Verriegelung ist der Status der Verriegelung zu überprüfen.
   Navigieren zu: Setup → Erweitertes Setup
   Status Verriegelung = **SIL-verriegelt** muss mit einem "✔" bestätigt sein.
7. Optional kann zusätzlich die Hardware-Verriegelung (über den mit "WP" gekennzeichneten Dip-Schalter an der Hauptelektronik) aktiviert werden.

Weitere Parametereinstellungen

Folgende Parameter beeinflussen die Sicherheitsfunktion, können aber entsprechend der Anwendung frei eingestellt werden:

Empfehlung: Eingestellte Werte notieren!

Parameter	Parametername
Stromeingangsmessung: Setup → Erweitertes Setup → Ein/Ausgang → Analog I/O	0 % Wert
	100 % Wert

Die folgenden Parameter beeinflussen die Sicherheitsfunktion und sind nicht im Expertenmodus frei einstellbar, sondern werden zu Beginn der SIL-Bestätigung vom Gerät automatisch auf die genannten, sicherheitsgerichteten Werte zwangsumgestellt:

Parameter	Voreingestellter Wert
Setup → Erweitertes Setup → Ein/Ausgang → Digital A1-2 → Kontakt Typ	Öffner
Setup → Erweitertes Setup → Applikation → Alarm 1 → Alarm X → Fehlerwert	Alle Alarme
Setup → Erweitertes Setup → Applikation → Alarm 1 → Alarm X → Alarm Modus	An
Diagnose → Simulation → Simulation Stromausgang 2	Aus
Experte → Ein/Ausgang → Analog I/O → Fehlerverhalten bei Ereignis	Jeglicher Fehler
Experte → Ein/Ausgang → Analog I/O → Ausgang ausserhalb Messbereich	Alarm
Experte → Ein/Ausgang → Digital A1-2 → Fehlerverhalten bei Ereignis	Jeglicher Fehler
Experte → Ein/Ausgang → Digital A1-2 → Ausgangs Simulation	Deaktivieren

Nicht genannte Parameter beeinflussen die Sicherheitsfunktion nicht und können auf beliebige, sinnvolle Werte eingestellt werden. Die Sichtbarkeit der genannten Parameter im Bedienmenü hängt teilweise von der Benutzerrolle, von bestellten SW-Optionen und von Einstellungen anderer Parameter ab.

Entriegeln eines SIL-Geräts

Ein SIL-verriegeltes Gerät ist gegen unberechtigte Bedienung durch einen Verriegelungscode und optional zusätzlich durch einen Hardware-Schreibschutzschalter geschützt. Zur Veränderung der Parametrierung muss das Gerät entriegelt werden.

⚠ VORSICHT

Durch die Entriegelung des Geräts werden Diagnosen deaktiviert und das Gerät kann unter Umständen im entriegelten Zustand die Sicherheitsfunktion nicht ausführen.

- ▶ Deshalb muss durch unabhängige Maßnahmen sichergestellt werden, dass während der Zeit der Entriegelung keine Gefährdung bestehen kann.

Zur Entriegelung folgendermaßen vorgehen:

1. Position des Hardware-Schreibschutzschalter (mit "WP" gekennzeichneter Dip-Schalter an der Hauptelektronik) prüfen und diesen Schalter auf "OFF" stellen.
2. Die Sequenz "Setup → Erweitertes Setup → SIL/WHG deaktivieren" auswählen und beim Parameter **Schreibschutz rücksetzen** den entsprechenden Entriegelungscode eingeben (SIL: 7452).
   - ↳ Die erfolgreiche Entriegelung wird durch die Meldung "Sequenzende" signalisiert.

Wiederholungsprüfung

Sicherheitsfunktionen in angemessenen Zeitabständen auf ihre Funktionsfähigkeit und Sicherheit überprüfen! Die Zeitabstände sind vom Betreiber festzulegen.

Hierzu können die entsprechenden Werte und Abbildungen im Kapitel "Weitere sicherheitstechnische Kenngrößen" herangezogen werden → 📄 5. Die Prüfung ist so durchzuführen, dass die einwandfreie Funktion der Schutzeinrichtung im Zusammenwirken aller Komponenten nachgewiesen wird.

Der anzusetzende Wert von PFD_{avg} hängt bei einer einkanaligen Architektur nach folgender Formel vom Diagnose-Deckungsgrad der Wiederholungsprüfung (PTC = Proof Test Coverage) und der vorgesehenen Lebensdauer (LT = Lifetime) ab:

$$PFD_{avg} = \frac{1}{2} \bullet PTC \bullet \lambda_{DU} \bullet T_I + \lambda_{DD} \bullet MTTR + \frac{1}{2} \bullet (1 - PTC) \bullet \lambda_{DU} \bullet LT$$

A0024244

Für die im Folgenden beschriebene Wiederholungsprüfung ist der Diagnose-Deckungsgrad angegeben, der zur Berechnung verwendet werden kann. Der Diagnose-Deckungsgrad ist abhängig vom Prüfablauf.

Für die genutzte Sicherheitsfunktion muss ein Prüfablauf für die Wiederholungsprüfung durchgeführt werden.

Sicherheitsfunktion (Stromeingangsmessung)		PTC
	Prüfablauf A – Einspeisung realer Ströme	99 %

Zusätzlich ist zu prüfen und sicherzustellen, dass alle Deckeldichtungen und Kabeleinführungen ihre Dichtfunktion korrekt erfüllen.

⚠ VORSICHT

Gewährleistung der Prozesssicherheit.

- Während der Wiederholungsprüfung müssen zur Gewährleistung der Prozesssicherheit alternative überwachende Maßnahmen ergriffen werden.

Ist eines der Prüfkriterien des folgenden Prüfablaufs nicht erfüllt, darf das Gerät nicht mehr als Teil einer Schutzeinrichtung eingesetzt werden. Die Wiederholungsprüfung dient zur Aufdeckung zufälliger Geräteausfälle (λ_{du}). Der Einfluss systematischer Fehler auf die Sicherheitsfunktion wird durch diese Prüfung nicht abgedeckt und ist gesondert zu betrachten. Systematische Fehler können beispielsweise durch Stoffeigenschaften, Betriebsbedingungen, Ansatzbildung oder Korrosion verursacht werden.

Prüfablauf A (Einspeisung realer Ströme)

Vorbereitung

1. Grenzstandüberwachung und Bereichsüberwachung können auch bei aktiviertem SIL-Mode durchgeführt werden.
2. Wenn das sicherheitsbezogene Signal "Analog" genutzt wird, geeignetes Messgerät (empfohlene Genauigkeit besser ±0,1 mA) in den installierten Stromkreis dazwischenschalten.
3. Wenn das sicherheitsbezogene Signal "Digital" genutzt wird, geeignetes Messgerät (Durchgangsprüfer / Widerstandmessung) (empfohlene Genauigkeit besser ±0,1 Ω) an Digitalausgang anschließen.
4. Feststellen der Sicherheitsschaltung (Grenzstand- bzw. Bereichsüberwachung).

Ablauf bei Grenzstandüberwachung (Strom)

1. Einen Strom direkt unterhalb (MAX-Überwachung) bzw. direkt oberhalb (MIN-Überwachung) des zu überwachenden Stromgrenzwerts einspeisen (z.B. durch Simulation am angeschlossenen Gerät).
2. Den Ausgangsstrom (mA) ablesen, protokollieren und auf Richtigkeit bewerten.
3. Den Schaltzustand des Relais (Ω) ablesen, protokollieren und auf Richtigkeit bewerten.
4. Einen Strom direkt oberhalb (MAX-Überwachung) bzw. direkt unterhalb (MIN-Überwachung) des zu überwachenden Stromgrenzwerts eingeben.
5. Den Ausgangsstrom (mA) ablesen, protokollieren und auf Richtigkeit bewerten.
6. Den Schaltzustand des Relais (Ω) ablesen, protokollieren und auf Richtigkeit bewerten.

Die Prüfung gilt als bestanden, wenn der Strom und der Schaltzustand des Relais die Sicherheitsfunktion nicht bei den Schritten 2 und 3, sondern nur bei den Schritten 5 und 6 auslösen.

Ablauf bei Bereichsüberwachung (Strom)

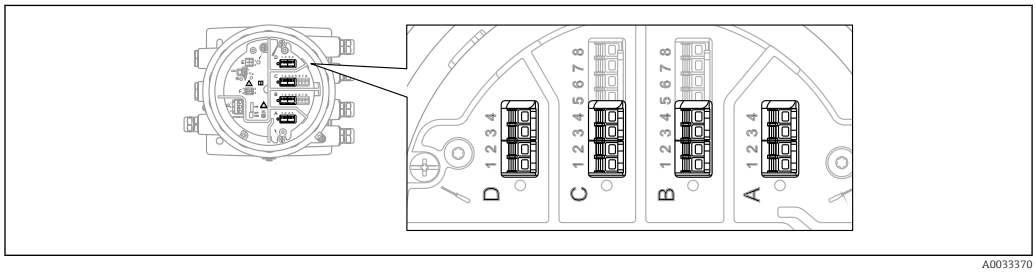
1. Fünf Stromwerte innerhalb des zu überwachenden Bereichs einspeisen (z.B. durch Simulation am angeschlossenen Gerät).
2. Den Ausgangsstrom (mA) und den Schaltzustand des Relais (Ω) bei jedem Stromwert ablesen, protokollieren und auf Richtigkeit bewerten.

Die Prüfung gilt als bestanden, wenn die Stromwerte und der Schaltzustand des Relais bei Schritt 2 innerhalb der erforderlichen Genauigkeitsgrenzen liegen.

Relais-Selbstüberprüfung

Die Relais-Selbstüberprüfung muss nur durchgeführt werden, wenn das sicherheitsbezogene Signal "Digital" genutzt wird.

Beispiel für die Anschlussbezeichnung: Wenn das für die Sicherheitsfunktion genutzte IO Modul Digital im Slot D installiert ist und die Kontakte 3 und 4 genutzt werden, ist für die Bezeichnung Digital Xy-z Digital D3-4 einzusetzen.



A0033370

1. SIL-Betrieb deaktivieren. Navigieren zu: Setup → Erweitertes Setup → SIL/WHG deaktivieren und beim Parameter **Schreibschutz rücksetzen** den entsprechenden Entriegelungscode eingeben (SIL: 7452).
2. Geräte-Selbsttest wie folgt durchführen. Navigieren zu: Setup → Erweitertes Setup
3. Einstellen: **Ein/Ausgang** = **Digital Xy-z**
4. Prüfen, ob **Kontakt Typ** = **Öffner** (SIL Werkseinstellung).

5. Einstellen: **Ausgangs Simulation** = **Simulation Inaktiv**.
6. Prüfen, ob der Kontakt geschlossen ist (Widerstand <1 Ω) zwischen den Kontakten Xy und Xz.
7. Einstellen: **Ausgangs Simulation** = **Fehler 1**.
8. Prüfen, ob der Kontakt offen ist (Widerstand >1 MΩ) zwischen den Kontakten Xy und Xz.
9. Einstellen: **Ausgangs Simulation** = **Simulation Inaktiv**.
10. Prüfen, ob der Kontakt geschlossen ist (Widerstand <1 Ω) zwischen den Kontakten Xy und Xz.
11. Einstellen: **Ausgangs Simulation** = **Fehler 2**.
12. Prüfen, ob der Kontakt offen ist (Widerstand >1 MΩ) zwischen den Kontakten Xy und Xz.
13. Einstellen: **Ausgangs Simulation** = **Simulation Aktiv**.
14. Prüfen, ob der Kontakt offen ist (Widerstand >1 MΩ) zwischen den Kontakten Xy und Xz.
15. Einstellen: **Ausgangs Simulation** = **Deaktivieren**.
16. SIL-Betrieb wieder aktivieren gemäß “Geräteparametrierung für sicherheitsbezogene Anwendungen“ → 🖹 13, nur die Punkte 3, 4, 6, 7, 8. (Alle anderen Vorgaben dieses Kapitels wurden im Rahmen der (Erst-)Inbetriebnahme/Parametrierung bzw. im Rahmen dieser Wiederholungsprüfung durchführt.)

Die Prüfung gilt als bestanden, wenn die Relais-Durchgangswerte bei den Schritten 6-15 innerhalb der geforderten Genauigkeit liegen.

Ende Prüfablauf A

- Bei Abweichung des erwarteten Stromwertes/Relais-Durchgangswerte zu einem bestimmten Füllstand von > ±2 % ist die Wiederholungsprüfung nicht bestanden. Zur Störungsbehebung, siehe Betriebsanleitung → 🖹 8. Durch diese Prüfung werden 99 % der gefährlichen unerkannten Ausfälle aufgedeckt (Diagnose-Deckungsgrad der Wiederholungsprüfung, PTC = 0,99).
- Bei der Auswahl der Menügruppe "Experte" wird am Display ein Freigabecode abgefragt. Wenn unter Setup → Erweitertes Setup → Administration → Freigabecode definieren ein Freigabecode definiert wurde, dann muss dieser hier eingegeben werden. Falls kein Freigabecode definiert wurde, kann die Abfrage durch Drücken der "E"-Taste quittiert werden.

Lebenszyklus

Anforderungen an das Personal

Das Personal für Installation, Inbetriebnahme, Diagnose, Reparatur und Wartung muss folgende Bedingungen erfüllen:
- Ausgebildetes Fachpersonal: Verfügt über Qualifikation, die dieser Funktion und Tätigkeit entspricht
- Vom Anlagenbetreiber autorisiert
- Mit den nationalen Vorschriften vertraut
- Vor Arbeitsbeginn: Anweisungen in Anleitung und Zusatzdokumentation sowie Zertifikate (je nach Anwendung) lesen und verstehen
- Anweisungen und Rahmenbedingungen befolgen

Das Bedienpersonal muss folgende Bedingungen erfüllen:
- Entsprechend den Aufgabenanforderungen vom Anlagenbetreiber eingewiesen und autorisiert
- Anweisungen in dieser Anleitung befolgen

Installation

Die Installation des Geräts ist in der entsprechenden Betriebsanleitung beschrieben (→ 🖹 8).

Inbetriebnahme

Die Inbetriebnahme des Geräts ist in der entsprechenden Betriebsanleitung beschrieben (→ 🖹 8).

Bedienung

Die Bedienung des Geräts ist in der entsprechenden Betriebsanleitung beschrieben (→ 🖹 8).

Wartung

Hinweise zur Wartung und zur Nachkalibrierung sind in der zugehörigen Betriebsanleitung beschrieben (→ 🖹 8).

Während der Parametrierung, Wiederholungsprüfung und der Wartungsarbeiten am Gerät müssen zur Gewährleistung der Prozesssicherheit alternative überwachende Maßnahmen ergriffen werden.

Reparatur

Reparatur bedeutet Wiederherstellung der Funktionsfähigkeit durch den Austausch von defekten Komponenten. Hierfür müssen Komponenten gleichen Typs verwendet werden. Wir empfehlen die Reparatur zu dokumentieren. Hierzu gehört die Angabe der Geräte-Seriennummer, Reparaturdatum, Art der Reparatur und ausführende Person.

Ein Austausch folgender Komponenten darf durch Fachpersonal des Kunden vorgenommen werden, wenn Original-Ersatzteile verwendet und die jeweiligen Einbauanleitungen beachtet werden:

Komponente	Geräteprüfung nach Reparatur
I/O Modul Mainboard Baugruppe Abdeckung, beschriftet	▪ Sichtkontrolle, ob alle Teile vorhanden und ordnungsgemäß montiert sind. ▪ Wiederholungsprüfung Prüfablauf A
Deckel Alu, Schauglas Deckelsicherung O-Ring, Gehäuse	▪ Sichtkontrolle, ob alle Teile vorhanden und ordnungsgemäß montiert sind. ▪ Kontrolle der Messung bei einem beliebigen Füllstand.
Elektronische Box, vollständig	▪ Sichtkontrolle, ob alle Teile vorhanden und ordnungsgemäß montiert sind. ▪ Wiederholungsprüfung Prüfablauf A
Gehäusefilter	Sichtkontrolle, ob alle Teile vorhanden und ordnungsgemäß montiert sind
SD-Karte mit Halter	Sichtkontrolle, ob alle Teile vorhanden und ordnungsgemäß montiert sind.
Display Set, Displayhalter, Fixierring	Sichtkontrolle, ob alle Teile vorhanden und ordnungsgemäß montiert sind.
Klemmenset, Federklemme, Klemmenset, Schraubklemme,	Sichtkontrolle, ob alle Teile vorhanden und ordnungsgemäß montiert sind.

Einbauanleitungen, siehe Downloadbereich unter www.endress.com.

Die ausgetauschte Komponente muss zwecks Fehleranalyse an Endress+Hauser eingesendet werden, falls das Gerät in einer Schutzeinrichtung betrieben wurde und ein Gerätefehler nicht ausgeschlossen werden kann. In diesem Fall ist bei der Rücksendung des defekten Gerätes die „Erklärung zur Kontamination und Reinigung“ mit dem entsprechenden Hinweis „Einsatz als SIL-Gerät in Schutzeinrichtung“ beizulegen. Hierfür das Kapitel „Rücksendung“ in der Betriebsanleitung (→ 🖹 8) beachten.

Modifikation

Modifikationen sind Änderungen an bereits ausgelieferten oder installierten SIL-fähigen Geräten.

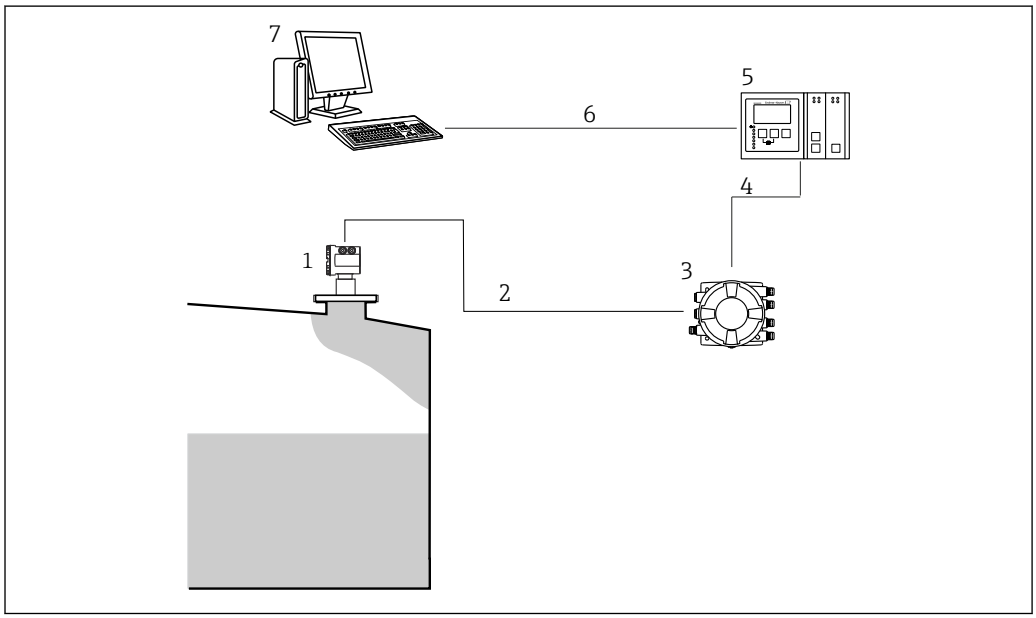
- ▶ Üblicherweise werden Modifikationen von SIL-fähigen Geräten im Endress+Hauser Herstellerwerk durchgeführt.
- ▶ Modifikationen an SIL-fähigen Geräten beim Anwender vor Ort sind nach Freigabe durch das Endress+Hauser Herstellerwerk möglich. In diesem Fall müssen die Modifikationen durch einen Endress+Hauser Servicetechniker durchgeführt und dokumentiert werden.
- ▶ Modifikationen von SIL-fähigen Geräten durch den Anwender sind nicht erlaubt.

Anhang

Aufbau des Messsystems

Systemkomponenten

In der folgenden Abbildung sind die Geräte des Messsystems beispielhaft dargestellt:



1 *Level radar*
2 *4-20 mA HART*
3 *Tankside Monitor*
4 *Feldbus (z.B. Modbus, V1)*
5 *Tankvision Tank Scanner NXA820*
6 *Ethernet*
7 *Computer mit Fieldcare*

Beschreibung der Anwendung als Schutzeinrichtung

Der Tankside Monitor ist ein Feldgerät für die Integration von Tanksensoren in Bestandsführungssysteme. Er ermöglicht den Zugriff auf alle angeschlossenen Tanksensoren. Alle gemessenen und berechneten Werte können auf der integrierten Anzeige ausgegeben werden. Zudem können sie über ein Feld-Kommunikationsprotokoll in ein Lagerhaltungssystem übertragen werden.

In Schutzeinrichtungen kann das Gerät in dieser Anordnung für MIN-Sicherheit, MAX-Sicherheit und Bereichsüberwachung eingesetzt werden.

Der sichere Betrieb des Geräts setzt eine ordnungsgemäße Installation voraus.

Wiederholungsprüfung

Anlagenspezifische Daten	
Firma	
Messstellen/TAG Nr.	
Anlage	
Gerätetyp/Bestellcode	
Seriennummer Gerät	
Name	
Datum	
Freigabecode (falls individuell pro Gerät)	
Verwendeter Verriegelungscode	SIL ❑ 7452
Unterschrift	

Gerätespezifische Inbetriebnahmeparameter	
Rohrdurchmesser (Flüssigkeitsmessung; Schwallrohr/Bypass)	
Abgleich Leer	
Abgleich Voll	

Proof Test Protokoll		
Prüfschritt	Sollwert	Istwert
1. Stromwert 1		
2. Stromwert 2		
3. ggf. Stromwert 3		
4. ggf. Stromwert 4		
5. ggf. Stromwert 5		
Durchgangswert		

Hinweis bei redundanter Verschaltung mehrerer Sensoren

Dieser Abschnitt gibt zusätzlich Hinweise bei der Verwendung homogen redundanter Sensoren z.B. in Auswahlschaltung 1oo2 oder 2oo3.

Die in der Tabelle unten angegebene Common Cause Faktoren ß und $ß_D$ sind Mindestwerte für das Gerät. Diese sind bei der Auslegung des Teilsystems Sensorik zu verwenden.

Mindestwert ß bei homogen redundantem Einsatz	5%
Mindestwert $ß_D$ bei homogen redundantem Einsatz	2%

Das Gerät erfüllt die Anforderungen für SIL 3 in homogen redundantem Einsatz.

Bei der Wiederholprüfung ist folgendes zu beachten: Wird an einem der redundant betriebenen Geräte ein Fehler entdeckt, sind die anderen Geräte dahingehend zu überprüfen, ob der gleiche Fehler vorliegt.

Weiterführende Informationen

Allgemeine Informationen über Funktionale Sicherheit (SIL) sind erhältlich unter:

www.de.endress.com/SIL (deutsch) bzw. www.endress.com/SIL (englisch) und in der Kompetenzbroschüre CP01008Z/11 "Funktionale Sicherheit in der Prozess-Instrumentierung zur Risikoreduzierung".

www.addresses.endress.com

Endress+Hauser

People for Process Automation