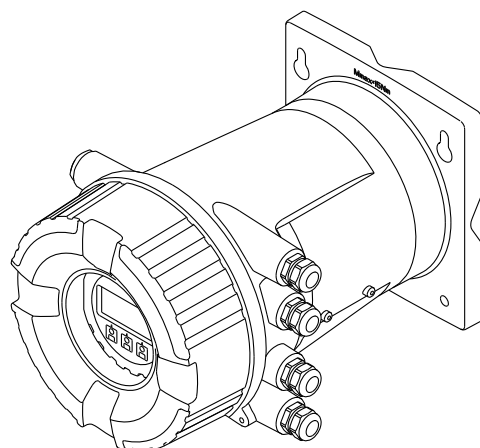


個別説明書

Tankside Monitor NRF81

機能安全マニュアル



4~20mA 電流出力およびスイッチ出力機能を持つタンクサイドモニタ

目次

適合宣言	3
その他の安全関連特性値	4
電気部品の耐用年数	5
資料情報	6
資料の機能	6
本書の使用法	6
使用されるシンボル	6
機器の補足資料	7
有効な機器タイプ	8
銘板の SIL ラベル	9
安全機能	9
安全機能の定義	9
安全関連信号	9
安全関連アプリケーションの制約事項	9
安全計装システムでの使用	11
安全機能	11
安全関連アプリケーションのパラメータ設定	12
ブルーフトテスト	16
ライフサイクル	21
作業員の要件	21
設置	21
設定	21
操作	21
メンテナンス	21
修理	22
変更	22
付録	23
計測システムの構成	23
ブルーフトテスト	24
詳細情報	24

適合宣言

SIL_00264_01.18

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, 2-August-2018
Endress+Hauser SE+Co. KG

i. V.



Manfred Hammer
Dept. Man. R&D Quality Management/FSM
Research & Development

1/2

A0037372

SIL_00264_01.18



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	<input type="checkbox"/> Type A	<input checked="" type="checkbox"/> Type B	
Operating mode	<input checked="" type="checkbox"/> Low Demand Mode	<input checked="" type="checkbox"/> High Demand Mode	<input type="checkbox"/> Continuous Mode
Valid hardware version	As of manufacturing date after Nov.28,2016		
Valid software version	01.02.zz or 01.03.zz (zz: any double number)		
Safety manual	SD01929G		
Type of evaluation (check only <u>one</u> box)	<input checked="" type="checkbox"/>	Complete HW/SW evaluation parallel to development incl. FMEDA and change request acc. to IEC 61508-2, 3	
	<input type="checkbox"/>	Evaluation of "proven in use" performance for HW/SW incl. FMEDA and change request acc. to IEC 61508-2, 3	
	<input type="checkbox"/>	Evaluation of HW/SW field data to verify „prior use“ acc. to IEC 61511	
	<input type="checkbox"/>	Evaluation by FMEDA acc. to IEC 61508-2 for devices w/o software	
Evaluation through – report/certificate no.	Tank Side Monitor NRF81 Assessment report SIL2 (27.03.2017)		
Test documents	Development documents	Test reports	Data sheets
SIL - Integrity			
Systematic safety integrity		<input checked="" type="checkbox"/> SIL 2 capable	<input type="checkbox"/> SIL 3 capable
Hardware safety integrity	Single channel use (HFT = 0)	<input checked="" type="checkbox"/> SIL 2 capable	<input type="checkbox"/> SIL 3 capable
	Multi channel use (HFT ≥ 1)	<input checked="" type="checkbox"/> SIL 2 capable	<input type="checkbox"/> SIL 3 capable
FMEDA			
Safety function	MIN	MAX	Range
$\lambda_{DU}^{1),2)}$	146 FIT	146 FIT	146 FIT
$\lambda_{OP}^{1),2)}$	5101 FIT	5101 FIT	5101 FIT
$\lambda_{SU}^{1),2)}$	2254 FIT	2254 FIT	2254 FIT
$\lambda_{SD}^{1),2)}$	0 FIT	0 FIT	0 FIT
SFF	98 %	98 %	98 %
$PFD_{avg} (T_1 = 1 \text{ year})^{2)}$ (single channel architecture)	6.81×10^{-4}	6.81×10^{-4}	6.81×10^{-4}
$PFD_{avg} (T_1 = 2 \text{ years})^{2)}$ (single channel architecture)	1.32×10^{-3}	1.32×10^{-3}	1.32×10^{-3}
PFH	$1.46 \times 10^{-7} \text{ 1/h}$	$1.46 \times 10^{-7} \text{ 1/h}$	$1.46 \times 10^{-7} \text{ 1/h}$
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
$\lambda_{total}^{1),2)}$	7501 FIT	7501 FIT	7501 FIT
Diagnostic test interval ⁴⁾	60 min	60 min	60 min
Fault reaction time ⁵⁾	1 min	1 min	1 min
Comments			
-			
Declaration			
<input checked="" type="checkbox"/>	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 10⁹ 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

その他の安全関連特性値

IEC 61508 準拠特性	値
MTBF ¹⁾	35 年
DIN EN 61508-2 に準拠するシステム応答時間	「エキスパートモード」時： ユーザーが設定可能

1) Siemens SN29500 に準拠。この値は電子部品の機能に関連する故障タイプを考慮しています。


電気部品の耐用年数

電気部品の規定の故障率は IEC 61508-2:2010 7.4.9.5 項、備考 3 に準拠した耐用年数が適用されます。製造者および事業者が DIN EN 61508-2:2011 7.4.9.5 項、脚注 N3 に従い、適切な対策を講じた場合、この耐用期間が延長される場合があります。

資料情報


資料の機能

本資料は取扱説明書の一部であり、アプリケーション固有のパラメータや注意事項が記載されています。

-  機能安全に関する全般的な情報：SIL
- SILに関する全般的な情報は以下から取得できます。
Endress+Hauser ウェブサイトのダウンロードエリア：www.jp.endress.com/SIL





本書の使用法

本書の構成情報





 **操作** メニュー、**設定** メニュー、**診断** メニュー に従った簡単な説明付きのパラメータの配置については、機器の取扱説明書を参照してください。

使用されるシンボル

安全シンボル

シンボル	意味
 危険	危険 危険な状況を警告するシンボルです。この表示を無視して誤った取り扱いをすると、死亡したり、大けがをしたりするほか、爆発・火災を引き起こす恐れがあります。
 警告	警告 危険な状況を警告するシンボルです。この表示を無視して誤った取り扱いをすると、死亡、大けが、爆発、火災の恐れがあります。
 注意	注意 危険な状況を警告するシンボルです。この表示を無視して誤った取り扱いをすると、けが、物的損害の恐れがあります。
 注記	注意！ 人身傷害につながらない、手順やその他の事象に関する情報を示すシンボルです。

特定情報に関するシンボル


シンボル	意味
 ヒント A0011193 追加情報を示します。	
	資料参照
	ページ参照
	図参照
1, 2, 3...	一連のステップ

図中のシンボル

シンボル	意味
1, 2, 3,...	項目番号
1, 2, 3...	一連のステップ
A, B, C, ...	図

機器の補足資料

関連資料	コメント
技術仕様書 TI01251G	これらの資料はインターネットから入手できます。 → www.jp.endress.com
取扱説明書 BA01465G	これらの資料はインターネットから入手できます。 → www.jp.endress.com
簡易取扱説明書： KA01209G	<ul style="list-style-type: none"> ■ これらの資料は機器に付属します。 ■ これらの資料はインターネットから入手できます。 → www.jp.endress.com
安全注意事項は、選択した「認定」オプションに応じて異なります。	認定取得機器バージョンには、追加の安全注意事項 (XA、ZE) が付属します。該当する安全注意事項については、銘板を確認してください。

 取扱説明書、技術仕様書および ATEX 安全注意事項に加え、この補足安全マニュアルが適用されます。機器の設置、設定および操作時には、この補足機器資料に記載された内容を順守してください。この安全マニュアルには、保護機能に関する固有の要件が記載されています。

有効な機器タイプ

このマニュアルの機能安全に関する詳細は、下記の機器の仕様に対応しており、これは規定バージョン以降のソフトウェア/ハードウェアにおいて有効です。明記されている場合を除き、規定バージョン以降でも安全計装システムで使用できます。機器を変更した場合、IEC 61508 に基づく変更プロセスが適用されます。

安全関連アプリケーションの有効機器バージョン：

オーダーコード	名称	オプション
010	認定	すべて
020	コネクタタイプ	すべて
030	電源 (表示部)	すべて
040	プライマリ出力	次表を参照
050	セカンダリ I/O アナログ	次表を参照
060	セカンダリ I/O デジタル Ex d/XP	次表を参照
070	ハウジング	Y9 以外すべて
090	電気接続	すべて
150	精度、保税認定	すべて
500	操作言語 (表示部)	すべて
540	アプリケーションパッケージ	すべて
570	サービス	すべて
580	試験、証明	すべて
590	追加認証	LA ¹⁾ SIL
610	取付アクセサリ	すべて
620	同梱アクセサリ	すべて
850	ファームウェアのバージョン	ここでバージョンを選択しなかった場合、最新の SIL 対応 SW が提供されます。あるいは、次の SW バージョンも選択できます：01.02.zz または 01.03.zz
895	マーキング	すべて

1) 他のバージョンの追加選択が可能です。

オーダーコード	040	050	060
オプション	E1	A1 または B1	*
	H1	A1 または B1	*
	E1	*	A1, A2, A3, B2 または B3
	H1	*	A1, A2, A3, B2 または B3
	*	A2	*
	*	B2	*
	*	C2	*
	*	A1	A1, A2, A3, B2 または B3
	*	B1	A1, A2, A3, B2 または B3

* すべてのオプションを選択可能 (本セクションは SIL 機能に影響しません)。

- 有効ファームウェアバージョン：01.02.zz 以降または 01.03.zz (→ 機器の銘板)
- ハードウェアバージョン (電子部品)：製造日が 2016 年 11 月 23 日以降 (→ 機器の銘板)

銘板の SIL ラベル



SIL 認定機器の銘板には、次のシンボルマークが付加されています：Ⓢ

安全機能

安全機能の定義

計測システムの安全機能：

電流入力監視

安全機能は接続機器の電流測定で有効です。

安全関連信号

デジタル

機器の安全関連信号は、デジタル出力のリレー接点閉です。すべての安全対策では、この信号のみが参照されます。

アナログ入力電流 (安全機能) はデジタル出力値に正しく変換されます。リレー接点は有効範囲内では閉、有効範囲外では開です。

安全関連出力信号は外部接続機器のロジックユニット (プログラマブルロジックコントローラやリミット信号伝送器など) に供給され、以下が監視されます。

- 規定のレベルリミットのオーバーシュート/アンダーシュート
- エラーの発生 (例：接点开 (信号線遮断))



エラー発生時には制御機器の安全性を確保/維持する必要があります。

アナログ

機器の安全関連信号はアナログ出力信号 4~20 mA です。すべての安全対策では、この信号のみが参照されます。

また、機器は情報取得のために HART 経由で通信し、すべての HART 機能および追加の機器情報を取得します。

安全関連出力信号は外部接続機器のロジックユニット (プログラマブルロジックコントローラやリミット信号伝送器など) に供給され、以下が監視されます。

- 規定のレベルリミットのオーバーシュート/アンダーシュート
- エラーの発生 (例：エラー電流 ($\leq 3.6 \text{ mA}$ 、 $\geq 21.0 \text{ mA}$)、信号線の遮断または短絡)。

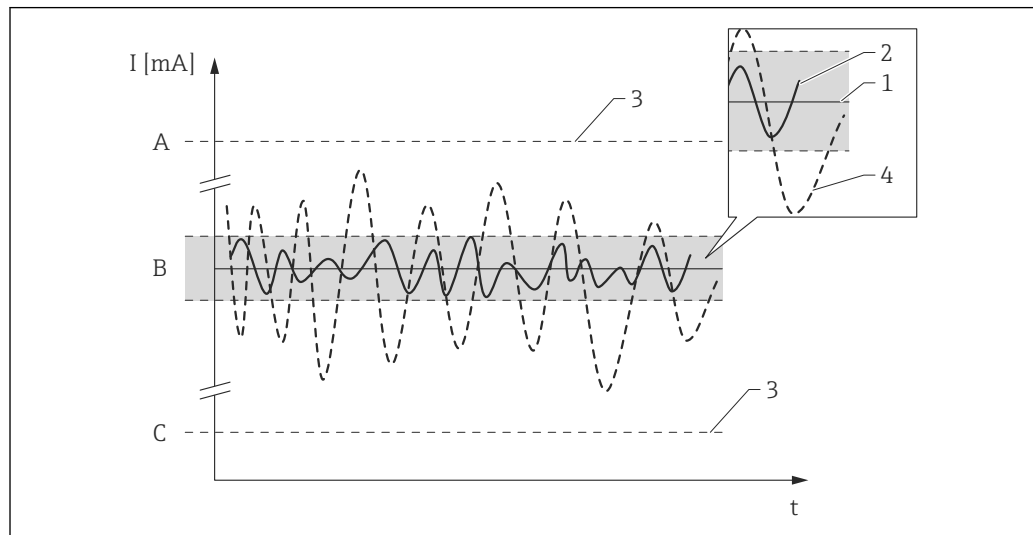


エラー発生時には制御機器の安全性を確保/維持する必要があります。

安全関連アプリケーションの
制約事項

- 安全関連信号の情報を参照してください (→ 9)。
 - 取扱説明書の仕様を超えないようにしてください (→ 7)。
 - 安全関連アプリケーションには、以下の制約事項も適用されます。
 - 信号線におけるパルスなどの強力な電磁干渉により、出力信号の過渡 ($< 1 \text{ s}$) 偏差 ($\geq \pm 2 \%$) が生じる可能性があります。このため、外部接続機器のロジックユニットで時定数 $\geq 1 \text{ s}$ によるフィルタリングを行う必要があります。
 - 誤差範囲は機器固有であり、納入時に FMEDA (Failure Modes, Effects and Diagnostic Analysis) に基づいて定義されます。これには、技術仕様書に記載されるすべての影響要因が含まれます (例：非線形性、非再現性、ヒステリシス、ゼロ点ドリフト、温度ドリフト、電磁干渉)。
- IEC/EN 61508 に従い、安全関連エラーは各種カテゴリに分類されます (下表を参照)。表は安全関連のアナログ出力信号および測定の不確実性による影響を示します。

安全関連エラー	説明	安全関連出力信号の影響	測定の不確かさの影響 (位置。図 → 10 を参照)
機器エラーなし	安全： エラーなし	なし	1 仕様範囲内 (TI、BA などを参照)
λ_{SD}	安全検知： 検知可能な安全側故障	出力信号によりフェール セーフモードの開始信号 を送信 (→ 11)	3 影響なし
λ_{SU}	安全未検知： 検知できない安全側故障	規定の誤差範囲内	2 仕様を超えている可 能性あり
λ_{DD}	危険検知： 検知可能な危険側故障 (機器内の診断)	出力信号によりフェール セーフモードの開始信号 を送信 (→ 11)	3 影響なし
λ_{DU}	危険未検知： 検知できない危険側故障	規定誤差範囲を超えてい る可能性あり	4 規定誤差範囲を超え ている可能性あり



A0025264

- A 上限アラーム $\geq 21 \text{ mA}$
- B 誤差範囲 $\pm 2 \%$
- C 下限アラーム $\leq 3.6 \text{ mA}$

検知できない危険側故障

検知できない危険側故障は、実際値から 2 % 以上ずれている出力信号であり、出力信号状態は依然として 4~20 mA の範囲内であるか、またはリレー接点は閉じたままです。

安全計装システムでの使用

安全機能

デジタル

電源投入時の機器動作

電源投入後、機器は約 30 秒間の診断フェーズを実行します。この間、リレー接点は開です。診断フェーズでは、サービスインターフェイス (CDI) および各種プロトコル (HART、V1、Modbus) を介して通信できません。

安全機能要求モードでの機器動作

機器は監視対象の制限値に対応するデジタル出力値を表示します。リレー接点は有効範囲内では閉、有効範囲外では開です。接続するロジックユニットにより、これを適切に監視および処理する必要があります。

アラームおよび警告発生時の機器動作

アラームおよび警告発生時のリレー接点は常時開です。接続するロジックユニットにより、これを適切に監視および処理する必要があります。

アラームおよび警告メッセージ

アラームおよび警告メッセージにより、エラーコードとテキストメッセージの形式で機器の状態がわかります。

以下の表は、エラーコードとリレー接点出力の対応関係を示します。

エラーコード ¹⁾	リレー接点 (メッセージタイプ)	備考
Fxxx	開	xxx = 3 桁の数字
Mxxx	測定モードに対応	xxx = 3 桁の数字
Cxxx	測定モードに対応	xxx = 3 桁の数字
Sxxx	測定モードに対応	xxx = 3 桁の数字

1) エラーコードは取扱説明書に記載されています。

アナログ

電源投入時の機器動作

電源投入後、機器は約 30 秒間の診断フェーズを実行します。この間、電流出力はエラー電流 ($\leq 3.6 \text{ mA}$) に設定されます。

診断フェーズでは、サービスインターフェイス (CDI) および各種プロトコル (HART、V1、Modbus) を介して通信できません。

安全機能要求モードでの機器動作

機器は監視対象の制限値に対応する電流値を出力します。接続するロジックユニットで、この値を適切に監視および処理する必要があります。

アラームおよび警告発生時の機器動作

アラーム発生時の出力電流は $\leq 3.6 \text{ mA}$ または $\geq 21.0 \text{ mA}$ に設定できます。

エラー電流 $\geq 21.0 \text{ mA}$ を設定できない一部のアラーム (電源の故障、ケーブル開回路、電流出力時の障害など) では、設定されたエラー電流に関係なく、出力電流 $\leq 3.6 \text{ mA}$ が生成されます。

また、設定されたエラー電流に関係なく、出力電流 $\geq 21.0 \text{ mA}$ が生成される場合もあります (ケーブル短絡など)。

アラーム監視では、外部接続機器のロジックユニットは上限レベルのエラー電流信号 ($\geq 21.0 \text{ mA}$) および下限レベルのエラー電流信号 ($\leq 3.6 \text{ mA}$) を監視できなければなりません。

アラームおよび警告メッセージ

アラームおよび警告メッセージにより、エラーコードとテキストメッセージの形式で機器の状態がわかります。

以下の表は、エラーコードと電流出力の対応関係を示します。

エラーコード ¹⁾	電流出力 (メッセージタイプ)	備考
Fxxx	≥ 21.0 mA または ≤ 3.6 mA	xxx = 3桁の数字
Mxxx	測定モードに対応	xxx = 3桁の数字
Cxxx	測定モードに対応	xxx = 3桁の数字
Sxxx	測定モードに対応	xxx = 3桁の数字

1) エラーコードは取扱説明書に記載されています。

例外：

エラーコード ¹⁾	電流出力 (メッセージタイプ)	備考
C484	≥ 21.0 mA または ≤ 3.6 mA	シミュレーションフェールセーフモード

1) エラーコードは取扱説明書に記載されています。

安全関連アプリケーションの パラメータ設定

パラメータを設定する前に初期設定にリセットすることをお勧めします。

次の項目に移動します。設定 → 高度な設定 → 管理

機器リセット = 工場出荷設定に

これにより、すべてのパラメータが初期設定値にリセットされます。

測定点の計算

測定点の計算については、取扱説明書に記載されています (→ 図 7)。

使用する設定タイプ (a または b) を指定します。両方の設定を同時に使用できます。

- a) アナログ入力 (ソース) (1) → 安全関連信号 : アナログ出力 (2)
- b) アナログ入力 (ソース) (1) → 安全関連信号 : デジタル出力 (3)

アナログ入力 (ソース) (1)

適切なソースを設定してください (アナログ I/O B1-3 またはアナログ I/O C1-3)。

次の項目に移動します。設定 → 高度な設定 → インพุット/アウトプット → Analog I/O

設定

- 動作モード = 4-20mA 入力または HART master+4-20mA 入力
- アナログ入力 0%値を正しく設定する必要があります。
- アナログ入力 100%値を正しく設定する必要があります。

アナログ出力 (2)

適切な出力を設定してください (アナログ I/O B1-3 またはアナログ I/O C1-3)。

次の項目に移動します。設定 → 高度な設定 → インพุット/アウトプット → Analog I/O

設定

- 動作モード = 4-20mA 出力または HART スレーブ+4-20mA 出力
- 電流入力ソース = AIO B1-3 値 mA または AIO C1-3 値 mA (ソースに応じて異なります)
- 0% 値
- 100% 値
- SIL = 有効 に設定します。

デジタル出力 (3)

最初に制限値設定のアラームブロックを選択します (アラーム 1、アラーム 2、アラーム 3 またはアラーム 4)。

次の項目に移動します。設定 → 高度な設定 → アプリケーション → Alarm 1 → アラーム X

設定

- **アラームモード = オン**
- **アラーム値ソース = AIO B1-3 値 mA または AIO C1-3 値 mA** (ソースに応じて異なります)
- **HH アラーム値、H アラーム値、L アラーム値および LL アラーム値**は、有効範囲が上上限、上限、下限、下下限の範囲内になるようにアプリケーションに合わせて設定する必要があります。

適切な出力を設定してください (デジタル A1-2、デジタル A3-4、デジタル B1-2、デジタル B3-4、デジタル C1-2、デジタル C3-4、デジタル D1-2、デジタル D3-4)。

次の項目に移動します。設定 → 高度な設定 → インプット/アウトプット → デジタル Xy-z

設定

- **動作モード = 出力パッシブ**
- **デジタル入力ソース = 選択したアラームブロック (アラーム 1、アラーム 2、アラーム 3 またはアラーム 4)**
- **SIL = 有効** に設定して、このデジタル出力を SIL 出力として使用する必要があります。

設定方法

安全計装システムで機器を使用する場合、機器設定では以下の 2 つの要件に従う必要があります。


- **確認コンセプト** :
自主的な試験により、入力した安全関連パラメータを検証します。
- **ロックコンセプト** :
パラメータ設定後の機器のロック (IEC 61511-1:2016 セクション 11.6.3)

SIL モードを有効にするには、機器の操作シーケンスを実行する必要があります。この間、機器表示部または統合可能なアセットマネジメントツール (FieldCare など) から機器を操作できません。


「エキスパートモード」





多数の安全関連パラメータを自由に設定できます。

設定手順の詳細については、次のセクションで説明します。

 **SIL 設定**シーケンスを表示部および外部操作ツールに表示できるのは、SIL 機器 (仕様コード 590 「追加認定」、オプション LA 「SIL」) のみです。したがって、SIL ロックはこれらの該当機器でのみ実行できます。

「エキスパートモード」でのロック


機器を設定するには、以下に示す手順を実行および文書化してください →  24。

1. パラメータ設定を実行します (→  12 も参照)。パラメータ設定手順と個々のパラメータの意味については、取扱説明書に記載されています →  7。次の表のパラメータ設定を順守する必要があります →  15。
2. SIL 確認シーケンスを開始します。
次の項目に移動します。設定 → 高度な設定 → SIL/WHG 確認
書き込み保護設定 = 該当するロックコード (SIL : 7452) を入力します。「次へ」を押して確定します。
3. 「次へ」を押して、**設定 = エキスパートモード**を確定します。パラメータ設定が該当する表 →  15 に準拠していることが機器で確認され、必要に応じてパラメータのスイッチングが強制的に実行されます。
確認が完了すると、**SIL 準備 = 完了**が表示されます。引き続き、設定シーケンスを実行できます。
「次へ」を押して確定します。
4. 機能テストの実行 : 最小および最大監視では、スイッチ点の上 (最大監視) または下 (最小監視) の電流入力値を少なくとも 1 つは使用する必要があります。
範囲監視では、測定範囲全体に及ぶ 5 つの電流入力値を使用する必要があります。これを行う場合、安全関連信号 (電流出力/リレー) がそれぞれ正しく応答することを確認してください。
5. 機能テストが正常に完了したことを確認します。
機能テストの確認 = はい

6. **書き込み保護設定**にロックコードを再び入力します (SIL : 7452)。SIL ロック実行後のロックステータスを確認します。
次の項目に移動します。設定 → 高度な設定
「✓」を選択して、**ロック状態 = SIL ロック**を確定します。
7. オプションとして、ハードウェアロックも実行できます (主要電子回路部にある「WP」のマークが付加されたディップスイッチを使用します)。

その他のパラメータ設定


以下のパラメータは安全機能に影響を与えます。ただし、アプリケーションに応じて自由に設定することができます。

 設定値を書き留めておくことをお勧めします。

パラメータ	パラメータ名
電流入力測定：設定 → 高度な設定 → インプット/アウトプット → Analog I/O	0 % 値
	100 % 値

以下のパラメータは安全機能に影響を与えるため、エキスパートモードでは自由に設定することはできません。これらの値は、機器により SIL 確認の開始時に指定された安全指向の値に自動的に設定されます。

パラメータ	プリセット値
設定 → 高度な設定 → インプット/アウトプット → デジタル A1-2 → 接点タイプ	通常閉
設定 → 高度な設定 → アプリケーション → Alarm 1 → アラーム X → エラー値	全アラーム
設定 → 高度な設定 → アプリケーション → Alarm 1 → アラーム X → アラームモード	オン
診断 → シミュレーション → 電流出力 2 のシミュレーション	オフ
エキスパート → インプット/アウトプット → Analog I/O → エラーイベント	アラーム
エキスパート → インプット/アウトプット → Analog I/O → 出力範囲外	アラーム
エキスパート → インプット/アウトプット → デジタル A1-2 → エラーイベント	アラーム
エキスパート → インプット/アウトプット → デジタル A1-2 → 出力シミュレーション	無効

 記載されていないパラメータは安全機能に影響を与えないため、必要に応じて値を設定することができます。記載されているパラメータの操作メニューでの表示については、ユーザーの役割、ご注文の SW オプションおよび他のパラメータの設定に応じて異なる場合があります。

SIL 機器のロック解除

機器で SIL ロックが有効な場合、ロックコードおよび追加オプション（ハードウェア書込保護スイッチ）により、機器は不正な操作から保護されます。パラメータ設定を変更するには、機器のロックを解除する必要があります。

注意

機器のロックを解除すると診断機能が無効になり、機器は安全機能を実行できなくなります。

▶ したがって、機器のロック解除中は機器が危険にさらされないように独自の対策を取る必要があります。

機器のロックを解除するには、以下の手順を実行します。

1. ハードウェア書込保護スイッチ（主要電子回路部にある「WP」のマークが付加されたディスプレイスイッチ）の位置を確認し、このスイッチを「OFF」に設定します。
2. シーケンスとして「設定 → 高度な設定 → SIL/WHG 無効」を選択し、**書き込み保護のリセット**パラメータに対応するロック解除コード（SIL：7452）を入力します。
 - ↳ シーケンスの終了メッセージにより、機器のロック解除が正常に実行されたことが示されます。

ブルーテスト

適切な間隔で安全機能の動作と安全性を確認してください。ユーザーは間隔を決定する必要があります。

これには「その他の安全関連特性値」セクションの値とグラフィックを使用できます。テストでは、保護システムがすべてのコンポーネントに対応して適切に動作することを検証する必要があります。

i シングルチャンネルアーキテクチャでは、使用する PFD_{avg} 値はブルーテストの診断カバー率 (PTC = Proof Test Coverage) および目的の耐用年数 (LT = LifeTime) に応じて異なります。これは以下の計算式で規定されます。

$$PFD_{avg} = \frac{1}{2} \cdot PTC \cdot \lambda_{DU} \cdot T_1 + \lambda_{DD} \cdot MITR + \frac{1}{2} \cdot (1 - PTC) \cdot \lambda_{DU} \cdot LT$$

A0024244

以下に説明するブルーテストでは、ブルーテストカバー率が規定されており、これを計算に使用することが可能です。ブルーテストカバー率はテストシーケンスに応じて異なります。

使用する安全機能のために、ブルーテストのテストシーケンスを実行する必要があります。

安全機能 (電流入力測定)		PTC
	テストシーケンス A - 実際の電流供給	99 %

すべてのカバーシールおよび外部配線が適切にシールされていることも確認する必要があります。

▲ 注意

プロセスの安全性を確保してください。

▶ プロセスの安全性を確保するため、ブルーテスト時には代替手段により監視してください。

i いずれかのテスト基準が満たされていない場合、機器を保護システムの一部として使用できなくなる可能性があります。ブルーテストの目的はランダム機器故障を検知することです (λ_{du})。安全機能の故障原因の特定は、このテストの対象ではないため、個別に確認する必要があります。故障原因は、プロセスの材質特性、動作条件、堆積物、腐食などです。

テストシーケンス C (シミュレーションおよび 1 点レベル検知)

準備

1. SIL モードを無効化します。次の項目に移動します。設定 → 高度な設定 → SIL/WHG 無効を選択し、「書き込み保護のリセット」パラメータに適切なロック解除コード (SIL : 7452) を入力します。
2. 安全関連の「アナログ」信号を使用する場合は、適切な計測機器 (推奨精度 : ± 0.1 mA 以上) を設置回路に接続します。
3. 安全関連の「デジタル」信号を使用する場合は、適切な計測機器 (抵抗試験器/抵抗測定) (推奨精度 : ± 0.1 Ω 以上) をデジタル出力に接続します。
4. フェールセーフモードを設定します (レベルリミットまたは範囲監視)。

レベルリミット監視の手順

1. 次の項目に移動します。エキスパート → センサ → センサ診断
2. **自己チェック開始** パラメータ = はい オプションに設定します。自己チェックが完了すると、**自己チェックの結果** パラメータ = Ok オプションが表示されます。自己チェックは OK です。
3. 測定範囲内の任意のレベル (例 : 現在のレベル) で機器に表示された実際の測定値を読み取るか、または実際の出力電流を特定し、それを現在のレベルによって定義された設定値と比較します。測定に必要な精度の範囲内で値が一致する場合、機器はこのテスト部分に合格となります。
4. 次の項目に移動します。診断 → シミュレーション
5. **シミュレーション距離** パラメータ = オン オプションに設定します。監視対象の上限値 (最大監視) または下限値 (最小監視) の超過直前のレベルをシミュレートします (**シミュレーション距離** パラメータ = 対応する値)。
6. 出力電流 (mA) を読み取り、記録して精度を評価します。
7. リレーの抵抗値 (Ω) を読み取り、記録して精度を評価します。
8. 上限値 (最大監視) または下限値 (最小監視) の超過直後のレベルをシミュレートします。
9. 出力電流 (mA) を読み取り、記録して精度を評価します。
10. リレーの抵抗値 (Ω) を読み取り、記録して精度を評価します。

手順 5 ではなく、手順 8 でのみ電流値およびリレーの抵抗値 (Ω) により安全機能が実行された場合、機器はテストに合格となります。

範囲監視の手順

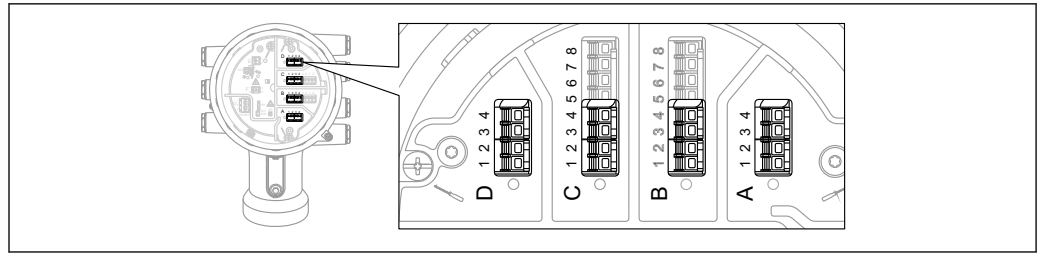
1. 次の項目に移動します。エキスパート → センサ → センサ診断
2. **自己チェック開始** パラメータ = はい オプションに設定します。自己チェックが完了すると、**自己チェックの結果** パラメータ = Ok オプションが表示されます。自己チェックは OK です。
3. 測定範囲内の任意のレベル (例 : 現在のレベル) で機器に表示された実際の測定値を読み取るか、または実際の出力電流を特定し、それを現在のレベルによって定義された設定値と比較します。測定に必要な精度の範囲内で値が一致する場合、機器はこのテスト部分に合格となります。
4. 5 つのレベルを監視対象の範囲内にシミュレートします。レベルリミット監視の手順 (レベル) の手順 4 および 5 を参照してください。
5. すべてのレベル値に対して、出力電流 (mA) およびリレーの抵抗値 (Ω) を読み取り、記録して精度を評価します。

手順 5 の電流値およびリレーの抵抗値 (Ω) が必要な精度範囲内の場合、テストが正常に完了したことを示します。

リレーの自己監視

リレーの自己監視は、「デジタル」安全関連信号を使用する場合にのみ実行する必要があります。

端子名称に関する注記 : たとえば、安全機能に使用するデジタル IO モジュールをスロット D に取り付けて接点 3 と 4 を使用する場合は、下記の手順説明内の「デジタル Xy-z」を「デジタル D3-4」に読み換えてください。



A0032388

1. SILモードを無効化します。次の項目に移動します。設定 → 高度な設定 → SIL/WHG 無効を選択し、**書き込み保護のリセット** パラメータに適切なロック解除コード (SIL : 7452) を入力します。
2. 次のように機器の自己チェックを行います。次の項目に移動します。設定 → 高度な設定 → インพุット/アウトプット → デジタル C1-2
3. **接点タイプ** パラメータ = **通常閉** オプション (SIL の初期設定) であることを確認します。
4. **出力シミュレーション** パラメータ = **OFF シミュレーション** オプションに設定します。
5. 接点 Xy と Xz の間の接点が閉 (抵抗 < 1 Ω) であることを確認します。
6. **出力シミュレーション** パラメータ = **フォルト 1** オプションに設定します。
7. 接点 Xy と Xz の間の接点が開 (抵抗 > 1 MΩ) であることを確認します。
8. **出力シミュレーション** パラメータ = **OFF シミュレーション** オプションに設定します。
9. 接点 Xy と Xz の間の接点が閉 (抵抗 < 1) であることを確認します。
10. **出力シミュレーション** パラメータ = **フォルト 2** オプションに設定します。
11. 接点 Xy と Xz の間の接点が開 (抵抗 > 1 MΩ) であることを確認します。
12. **出力シミュレーション** パラメータ = **OFF シミュレーション** オプションに設定します。
13. 接点 Xy と Xz の間の接点が開 (抵抗 > 1 MΩ) であることを確認します。
14. **出力シミュレーション** パラメータ = **無効** オプションに設定します。
15. 「安全関連アプリケーション用の機器設定」 → 12 に従って SIL モードを再度アクティブにします (項目 3、4、6、7、8 のみ) (本セクションの他の要件は、(初回) 試運転/設定またはこのプルーフテストとの関連で実行済み)。

手順 5~14 のリレーの抵抗値 (Ω) が必要な精度レベル範囲内の場合、テストが正常に完了したことを示します。

テストシーケンス C の終了

- i** 規定レベルで期待される電流値/リレーの抵抗値 (Ω) と比較して ±2 % を超える偏差が存在する場合、機器のプルーフテストは失敗です。トラブルシューティングについては、取扱説明書を参照してください → 7。このテストにより、検知できない危険側故障が 90 % 検出されます (プルーフテストカバー率、PTC = 0.90)。
- 「エキスパート」メニューグループを選択すると、表示部にアクセスコードの入力を求めるプロンプトが表示されます。アクセスコードを設定 → 高度な設定 → 管理 → アクセスコード設定 (0093) で定義した場合、そのコードをここに入力する必要があります。アクセスコードを定義していない場合は、プロンプトで「E」キーを押すと承認されます。

テストシーケンス A (実際の電流供給)

準備

1. SIL モードが有効な場合、レベルリミット値および範囲の監視もできます。
2. 安全関連の「アナログ」信号を使用する場合は、適切な計測機器（推奨精度： $\pm 0.1 \text{ mA}$ 以上）を設置回路に接続します。
3. 安全関連の「デジタル」信号を使用する場合は、適切な計測機器（抵抗試験器/抵抗測定）（推奨精度： $\pm 0.1 \Omega$ 以上）をデジタル出力に接続します。
4. 安全設定を決定します（レベルリミットまたは範囲の監視）。

レベルリミット監視の手順（電流）

1. (接続機器でのシミュレーションなどにより) 監視対象の上限値（最大監視）または下限値（最小監視）の超過直前の電流を入力します。
2. 出力電流 (mA) を読み取り、記録して精度を評価します。
3. リレーの抵抗値 (Ω) を読み取り、記録して精度を評価します。
4. 監視対象の上限値（最大監視）または下限値（最小監視）の超過直後の電流を入力します。
5. 出力電流 (mA) を読み取り、記録して精度を評価します。
6. リレーの抵抗値 (Ω) を読み取り、記録して精度を評価します。

手順 2、3 ではなく、手順 5、6 でのみ電流値およびリレーの抵抗値 (Ω) により安全機能が実行された場合、テストが正常に完了したことを示します。

範囲監視の手順（電流）

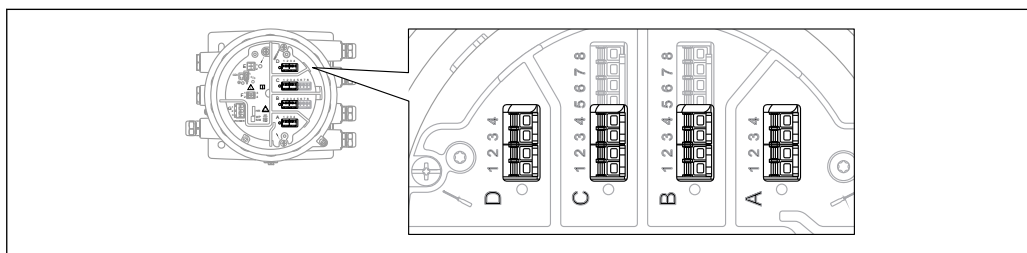
1. (接続機器でのシミュレーションなどにより) 監視対象範囲内の 5 つの電流値を入力します。
2. すべての電流値に対して、出力電流 (mA) およびリレーの抵抗値 (Ω) を読み取り、記録して精度を評価します。

手順 2 の電流値およびリレーの抵抗値 (Ω) が必要な精度範囲内の場合、テストが正常に完了したことを示します。

リレーの自己監視

リレーの自己監視は、「デジタル」安全関連信号を使用する場合にのみ実行する必要があります。

端子名称に関する注記：たとえば、安全機能に使用するデジタル IO モジュールをスロット D に取り付けて接点 3 と 4 を使用する場合は、下記の手順説明内の「デジタル Xy-z」を「デジタル D3-4」に読み換えてください。




A0033370

1. SIL モードを無効化します。次の項目に移動します。設定 → 高度な設定 → SIL/WHG 無効書き込み保護のリセットパラメータに対応したロック解除コード (SIL : 7452) を入力します。
2. 次のように機器の自己チェックを行います。次の項目に移動します。設定 → 高度な設定
3. インプット/アウトプット = デジタル Xy-z に設定します。
4. 接点タイプ = 通常閉 (SIL の初期設定) であることを確認します。
5. 出力シミュレーション = OFF シミュレーション に設定します。
6. 接点 Xy と Xz の間の接点が閉 (抵抗 $< 1 \Omega$) であることを確認します。
7. 出力シミュレーション = フォルト 1 に設定します。
8. 接点 Xy と Xz の間の接点が開 (抵抗 $> 1 \text{ M}\Omega$) であることを確認します。


9. 出力シミュレーション = OFF シミュレーション に設定します。
10. 接点 Xy と Xz の間の接点が開 (抵抗 <math>< 1 \Omega</math>)であることを確認します。
11. 出力シミュレーション = フォルト 2 に設定します。
12. 接点 Xy と Xz の間の接点が開 (抵抗 > $1 M\Omega$)であることを確認します。
13. 出力シミュレーション = ON シミュレーション に設定します。
14. 接点 Xy と Xz の間の接点が開 (抵抗 > $1 M\Omega$)であることを確認します。
15. 出力シミュレーション = 無効 に設定します。
16. 「安全関連アプリケーション用の機器設定」→ 12 に従って SIL モードを再度アクティブにします (項目 3、4、6、7、8 のみ) (本セクションの他の要件は、(初回) 試運転/設定またはこのプルーフテストとの関連で実行済み)。

手順 5~14 のリレーの抵抗値 (Ω) が必要な精度レベル範囲内の場合、テストが正常に完了したことを示します。


テストシーケンス A の終了

-  規定レベルで期待される電流値/リレーの抵抗値 (Ω) と比較して $\pm 2\%$ を超える偏差が存在する場合、機器のプルーフテストは失敗です。トラブルシューティングについては、取扱説明書を参照してください→ 7。このテストにより、検知できない危険側故障が 99% 検出されます (プルーフテストカバー率、PTC = 0.99)。
- 「エキスパート」メニューグループを選択すると、表示部にアクセスコードの入力を求めるプロンプトが表示されます。アクセスコードを 設定 → 高度な設定 → 管理 → アクセスコード設定 で定義した場合、そのコードをここに入力する必要があります。アクセスコードを定義していない場合は、プロンプトで「E」キーを押すと承認されます。

ライフサイクル

作業員の要件	<p>設置、設定、診断、修理およびメンテナンスを実施する作業員は、以下の要件を満たす必要があります。</p> <ul style="list-style-type: none">▪ 訓練を受けて、当該任務および作業に関する資格を取得した専門作業員であること▪ 施設責任者の許可を得ていること▪ 各地域/各国の法規を熟知していること▪ 専門作業員は作業を開始する前に、説明書、補足資料および証明書（用途に応じて）の説明を熟読して理解しておく必要があります。▪ 指示に従い、基本条件を遵守すること <p>オペレータは、以下の要件を満たす必要があります。</p> <ul style="list-style-type: none">▪ 施設責任者からその作業に必要な訓練および許可を得ていること▪ 本資料の説明に従うこと
設置	機器の設置については、機器の取扱説明書に記載されています（→ 図 7）。
設定	機器の設定については、機器の取扱説明書に記載されています（→ 図 7）。
操作	機器の操作については、機器の取扱説明書に記載されています（→ 図 7）。
メンテナンス	<p>メンテナンスと再校正については、機器の取扱説明書を参照してください（→ 図 7）。</p> <p> プロセスの安全性を確保するため、機器の設定、プルーフテストおよびメンテナンス作業時に代替手段により監視する必要があります。</p>

修理

 修理では、故障したコンポーネントを交換して機能の完全性を復元します。修理には、同じタイプのコンポーネントを使用する必要があります。修理作業を文書化することをお勧めします。これには、機器のシリアル番号、修理を実施した日付、修理のタイプ、修理担当者の氏名などを記載します。

以下のコンポーネントについては、お客様の技術スタッフが交換できます。ただし、純正のスペアパーツを使用し、適切な設置手順に従う必要があります。

コンポーネント	修理後の機器確認
I/O モジュール メインボード ラベルが付加された前面アセンブリ	<ul style="list-style-type: none"> ■ 外観検査により、すべてのパーツが適切に取り付けられていることを確認します。 ■ プルーフテスト、テストシーケンス A
ガラス窓付きカバー（アルミニウム製） カバークランプ Oリング、ハウジング	<ul style="list-style-type: none"> ■ 外観検査により、すべてのパーツが適切に取り付けられていることを確認します。 ■ 任意のレベルで測定値を確認します。
電子部品（全体）	<ul style="list-style-type: none"> ■ 外観検査により、すべてのパーツが適切に取り付けられていることを確認します。 ■ プルーフテスト、テストシーケンス A
ハウジングフィルタ	外観検査により、すべてのパーツが適切に取り付けられていることを確認します。
ホルダー付き SD カード	外観検査により、すべてのパーツが適切に取り付けられていることを確認します。
ディスプレイセット ディスプレイホルダー、固定リング	外観検査により、すべてのパーツが適切に取り付けられていることを確認します。
端子セット（プッシュイン） 端子セット（ネジ込み式）	外観検査により、すべてのパーツが適切に取り付けられていることを確認します。

設置手順については、www.jp.endress.com のダウンロードエリアを参照してください。

機器を保護システムで稼働しており、機器エラーを無視できない場合は、故障分析のため、交換した機器を Endress+Hauser に送付してください。この場合、故障した機器を返送するときに、「保護システムで SIL 機器として使用」という注釈を付加した「Declaration of Hazardous Material and Decontamination」（洗浄証明書）を必ず同梱してください。詳細については、取扱説明書を参照してください（→ 7）。

変更

変更とは、機器に導入済みの SIL 機能の変更を意味します。

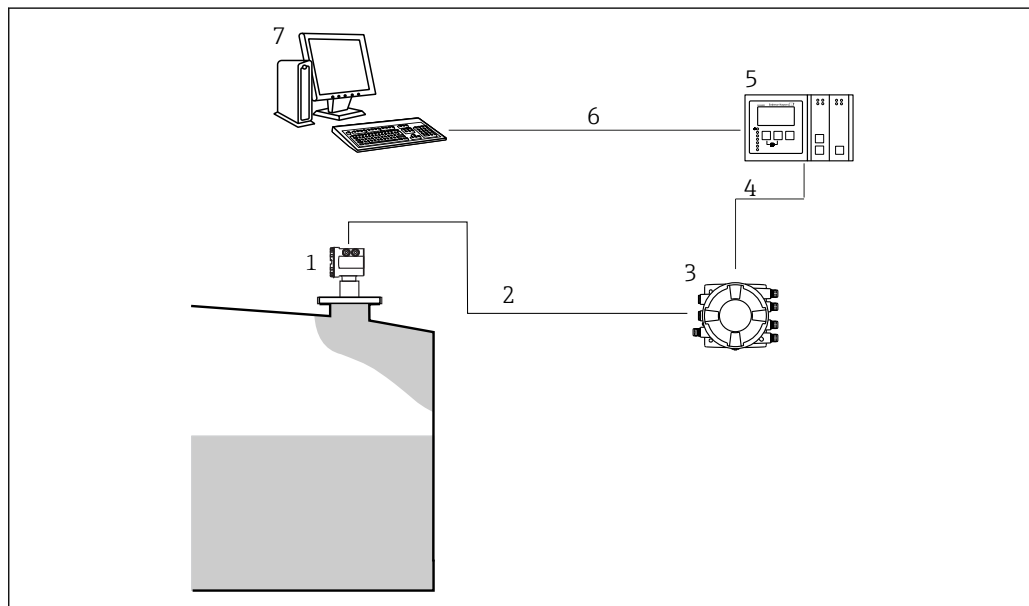
- ▶ 機器の SIL 機能の変更は、通常、Endress+Hauser プロダクションセンター（PC）で行います。
- ▶ Endress+Hauser プロダクションセンター（PC）から認可を受けた場合、機器の SIL 機能をユーザーのプラントで変更することも可能です。この場合、Endress+Hauser のサービス技術者が変更を実施し、文書化する必要があります。
- ▶ ユーザーによる機器の SIL 機能の変更は禁止されています。

付録

計測システムの構成

システムコンポーネント

以下の図に、計測システムを構成する機器を示します（例）。




A0033366

- 1 レベルレーダー
- 2 4~20 mA HART
- 3 Tank Side Monitor
- 4 フィールドバス (Modbus、V1 など)
- 5 Tankvision Tank Scanner NXA820
- 6 イーサネット
- 7 Fieldcare を搭載したコンピュータ

保護システムの使用に関する説明

Tank Side Monitor は、タンクセンサを在槽管理システムに統合するためのフィールド機器です。接続されたすべてのタンクセンサにアクセス可能で、すべての測定値と計算値を組み込みのディスプレイに出力します。さらに、フィールド通信プロトコルを介して在槽管理システムに転送できます。

最小安全、最大安全および範囲監視の安全計装システムでは、この配置を使用できます。

 機器操作の安全性を確保するには、適切な設置が前提条件になります。

ブルーテスト

システム固有のデータ	
会社	
測定点/タグ (TAG) 番号	
施設	
機器タイプ/オーダーコード	
機器のシリアル番号	
名称	
日付	
アクセスコード (各機器に個々のユーザーがアクセスする場合)	
使用するロックコード	SIL <input type="checkbox"/> 7452
署名	

機器固有の設定パラメータ	
パイプ直径 (液体測定 ; パイプ/バイパス)	
空校正	
満タン (スパン) 調整	

ブルーテストプロトコル		
テストステップ	セットポイント	実際の値
1. 電流値 1		
2. 電流値 2		
3. 電流値 3 (必要な場合)		
4. 電流値 4 (必要な場合)		
5. 電流値 5 (必要な場合)		
リレーの抵抗値 (Ω)		

詳細情報



機能安全 (SIL) に関する全般的な情報については、以下を参照してください。

www.de.endress.com/SIL (ドイツ語) または www.endress.com/SIL (英語) および関連資料『Functional Safety in the Process Industry- Risk Reduction with Safety Instrumented Systems』(CP01008Z)



www.addresses.endress.com
