RIKEN KEIKI

信号変換器付ガス検知部

SD-1OX

(TYPE HS)

安全マニュアル

Document Number : PT2-239

Project Number : 77PP351PP2

【注記】SD-1OX(TYPE HS)は機能安全(IEC 61508:2010 Part2 and Part3)の認証を受けています。認証書に記載されている機能を維持するには、本資料に基づいた管理をしてください。

理研計器株式会社
〒174-8744　東京都板橋区小豆沢 2-7-6
ホームページ　http://www.rikenkeiki.co.jp/

改廃履歴

Rev	内容	承認	検討	作成
0	新規作成	石橋　勝	武藤　弘樹	林　亮治
		2015 年 12 月 11 日	2015 年 12 月 11 日	2015 年 12 月 11 日
1	2-3, 2-14 修正	米村　慎一	武藤　弘樹	林　亮治
		2016 年 3 月 24 日	2016 年 3 月 24 日	2016 年 3 月 24 日
2	2-14 修正	武藤　弘樹	土屋　憲明	林　亮治
		2017 年 1 月 17 日	2017 年 1 月 17 日	2017 年 1 月 17 日
3	2-14 修正	武藤　弘樹	土屋　憲明	林　亮治
		2017 年 12 月 5 日	2017 年 12 月 5 日	2017 年 12 月 5 日
4	2-14 修正	米村　慎一	内田　雅之	佐伯　祐紀
		2018 年 4 月 10 日	2018 年 4 月 10 日	2018 年 4 月 10 日
5	2-14 修正	武藤　弘樹	土屋　憲明	林　亮治
		2019 年 10 月 9 日	2019 年 10 月 9 日	2019 年 10 月 9 日
6	2-14 修正	武藤　弘樹	土屋　憲明	林　亮治
		2019 年 12 月 3 日	2019 年 12 月 3 日	2019 年 12 月 3 日
7	2-14 修正	武藤　弘樹	土屋　憲明	林　亮治
		2020 年 3 月 18 日	2020 年 3 月 18 日	2020 年 3 月 18 日
8	2-14 修正	武藤　弘樹	土屋　憲明	林　亮治
		2020 年 7 月 14 日	2020 年 7 月 14 日	2020 年 7 月 14 日

目次

安全マニュアル
Safety Manual

1　目的

この安全マニュアルは、IEC 61508：2010 Part2 SIL 2 capable、IEC 61508：2010 Part3 SIL 3 capable 認証済み機器である、SD-1OX(TYPE HS)（以下本器）を安全計装機能の一部として使用される場合に、ユーザー様に責任のある、プルーフテスト、修理と交換、信頼性データ、製品寿命、環境制限と使用制限、各種設定パラメータなどについて記載されています。本器を安全に使用する為に、この安全マニュアルと関連する資料の全てをお読み頂くようお願いいたします。

2　使用方法

2-1　安全機能

本器の安全機能は以下の項目となります。

・サンプリングポイントにおいて、酸素ガス濃度をモニタリングする。

・モニタリングした酸素ガス濃度値に応じた電流を上位システム側に出力すること、本器の出力機能は 4-20mA 出力及び HART 通信出力（※）となります。

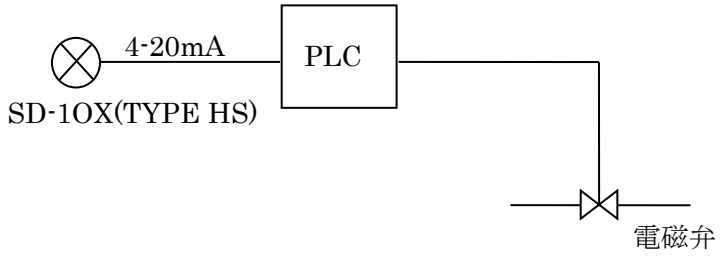
・4-20mA 出力について

測定した酸素ガス濃度値と 4-20mA 出力値は比例関係にあり、0ppm の場合に 4mA を出力し、フルスケール濃度の場合に 20mA を出力します。また、故障状態では 3.6mA 以下、または 21mA より大きい電流を出力します。

※HART 通信出力は安全機能に含まれません。

システム例

PLC を介して、電磁弁を制御し、遮断をかける場合のシステム例です。



2-2　安全精度

安全精度　：　10%

※この精度を超える誤差を生じる内部部品の故障に関しては、FMEDA の故障率に含まれます。

2-3　診断応答

自己診断結果の最大応答時間:15 秒

※自己診断により検出された部品の故障に関しては、この時間以内に通知されることを示します。また、この時間は自己診断テストの間隔と故障応答時間の合計になります。

※ROM/RAM チェックの自己診断だけは 1 日に 1 回実施されるため、最大応答時間は 24 時間となります。

2-4　セットアップ

別紙『取扱説明書』をご参照下さい。また、設定されているパラメータは必ず検査して下さい。

2-5　プルーフテスト

プルーフテストを実施する間隔は、 1 年を推奨しています。

プルーフテスト手順

1）安全機能を必ずバイパスしてください。

2）本器のガス濃度指示値が Air 値である事を確認してください。

3）ガス校正用ガスを導入して下さい。

4）ガス応答時間確認と、4-20mA 出力値確認を行って下さい。

5）安全機能のバイパスを元に戻して終了です。

※プルーフテストは間違えた操作を行うと、本器が誤作動する可能性があるため、訓練を受けたサービスマンが操作して下さい。

2-6　修理と交換

別紙『取扱説明書』をご参照下さい。

2-7　スタートアップ時間（イニシャルクリア時間）

本器の電源を入れてから、約 25 秒間はイニシャルクリア時間となっています。その間は正常なガス検知は出来ません。

2-8　ファームウェアのアップデート

ファームウェアをアップデートする際は必ず弊社工場に本器を戻してください。

2-9　信頼性データ

故障率及び故障モードなどの情報は FMEDA レポート(No.RK 15/06-015 R001)に記載されています。別紙『FMEDA レポート』をご参照下さい。

SIL2 を満足させるためには、1oo1(HFT=0)で使用して下さい。SIL3 を満足させるためには 1oo2(HFT=1)で使用して下さい。

2-10　製品寿命

製品寿命:製造年月から 10 年

FMEDA レポートの信頼性データは、この期間内でのみ有効です。

2-11　要求されるパラメータ設定

・バーンアウト(故障)時の 4-20mA 出力値は 3.6mA 以下、21mA 以上となります。

・セキュリティ上、HART 通信による設定変更を不可とするライトプロテクション機能を使用してください。

・機能安全として使用する場合は、上記項目を必ず守ってください。

2-12　環境制限

環境の制限については、別紙『取扱説明書』をご参照下さい。

2-13　アプリケーションの制限

アプリケーションの制限については、別紙『取扱説明書』をご参照下さい。

2-14　ハードウェア／ソフトウェア構成の識別

・Hardware Version : V1.1

・Software Version : V1.1

2-15　用語、略語の定義

用語

Safety 安全	Freedom from unacceptable risk of harm. 受容できないリスクから免れている状態
Functional Safety 機能安全	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment under control of system 製品に機能的な工夫（安全を確保する機能）を実装することにより確保される安全のこと。
Basic Safety 基本的安全	The equipment must be designed and manufactured such that it protects against resulting fire and explosion under explosive atmosphere 爆発性雰囲気に於いて着火源とならないような設計及び製造がなされていること。
Safety Assessment 安全アセスメント	The investigation to arrive at a judgment - based on evidence - of the safety achieved by safety-related systems 安全関連システムによって安全性が実現されたことを、証拠に基づいて判断するための調査のこと。
Fail-Safe State 安全側故障の状態	State that the defined fail-safe 定義されたフェイルセーフ状態であること。
Fail Safe 安全側故障	プロセスからの要求なしで定義されたフェイルセーフ状態になる故障のこと。 Failure that go to the defined fail-safe state without a demand from the process
Fail Dangerous 危険側故障	Failure that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state). Failure that deviates the process signal or the actual output by more than 15% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within active scale. プロセスからの要求に反応しない故障のこと （すなわち、定義された安全装置の状態に行くことができない）。

Fail Dangerous Undetected 検出されない危険側故障	Failure that is dangerous and that is not being diagnosed by automatic stroke testing. 自己診断機能では検出することができない危険側故障のこと。
Fail Dangerous Detected 検出される危険側故障	Failure that is dangerous but is detected by automatic stroke testing. 自己診断機能により検出することができる危険側故障のこと。
Fail Annunciation Undetected 検出されない自己診断機能の故障	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic and is not detected by another diagnostic. 誤警報を起こさず、機能安全を防止しないけれども、自動的な診断の損失を起こし、別の診断により検出されない故障のこと。
Fail Annunciation Detected 検出される自己診断機能の故障	Failure that does not cause a false trip or prevent the safety function but does cause loss of an automatic diagnostic or false diagnostic indication. 誤警報を起こさず、機能安全を防止しないけれども、自動的な診断の損失か、誤診断表示をする故障。
Fail No Effect 無影響故障	Failure of a component that is part of the safety function but that has no effect on the safety function. 機器を構成する部品の故障であるが、安全機能に影響を与えない故障。
Low demand mode 低頻度作動要求モード	Mode, where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency. 安全関連系に発生する作動要求頻度がプルーフテスト間隔の 2 倍以下である運用モードのこと。

略語

FMEDA	Failure Modes, Effects and Diagnostic Analysis 故障モード、影響および診断分析
HFT	Hardware Fault Tolerance Tolerance that to keep executing the function requested under the hardware fault and error condition 機器のフォールト又はエラーのある状況下で、要求される機能を遂行し続ける許容値
MOC	Management of Change Management of change the hardware or software elements, and keep traceability 機器の部品やソフトウェア等の要素の変更を管理し、追跡性を保持すること。
PFDavg	Average Probability of Failure on Demand 作動要求時の平均的な機能失敗の確率

SFF	Safe Failure Fraction The fraction of the overall failure rate of a device that results in either a safe fault or a diagnosed unsafe fault. 機器全体の故障率の内の、安全な障害または診断された危険な障害を結果として生じる故障率の割合。
SIF	Safety Instrumented Function A set of equipment intended to reduce the risk due to a specific hazard. 特定の危険のリスクを減らすことを意図した機能。
SIL	Safety Integrity Level Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems where Safety Integrity Level 4 has the highest level of safety integrity and Safety Integrity Level 1 has the lowest. E/E/PE 安全関連系に割り当てられた安全機能の安全度要件を指定するための離散的なレベル（可能である 4 つのもの）を示す。 SIL4 が安全度の中で最も高いレベルを持っており、SIL1 が最も低いレベルである。
SIS	Safety Instrumented System Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). 一つ以上の安全計装機能を有する設備。 SIS は、センサー、ロジックソルバー、および最終的な要素の組み合わせによって構成される。

以上