

安全マニュアル 安全計装システム対応 スマートESDデバイス 700シリーズ



安全上の注意

■ 絵表示について

この安全上の注意は、製品を安全に正しくお使いいただき、あなたや他の人々への危害や財産への損害を未然に防止するためのものです。安全上の注意は必ず守ってください。

本書では下記に示す絵表示をしています。

その表示と意味は、次のようになっています。内容をよく理解してから本文をお読みください。



警告 取り扱いを誤った場合に、使用者が死亡または重傷を負う危険の状態が生じることが想定される場合。

1. 目的

この安全マニュアルは安全計装システム対応スマート ESD デバイス 700 シリーズ (SIS 対応 700 シリーズ) を利用して安全計装機能 (SIF) を、設計、インストール、検証、そして、維持するために必要な情報を提供します。本文書の内容は、安全ライフサイクルの一部として完全に検討され、また、実施されなければなりません。この情報は IEC 61508 もしくは IEC61511 機能安全規格を満たすために必要です。



この取扱説明補完文書は単独の文書として使われることを意図していません。必ず次に示す取扱説明書とともにご使用ください。
安全計装システム対応スマート ESD デバイス 700 シリーズ AVP77□ / 78□ / 79□ 形 取扱説明書
CM1-AVP772-2001

2. 機器の説明

SIS 対応 700 シリーズは、スマート化された緊急遮断 (Emergency Shutdown) デバイスです。本器はロジックソルバーからの DC 電流または電圧を受け取って、空気式弁を制御します。この基本的な機能に加えて、SIS 対応 700 シリーズには、HART 通信機能、自動設定機能、そして自己診断機能があります。オプションのアナログ出力または接点出力を診断通知のために使うこともできます。

型番	パイロットリレータイプ	入力信号	診断通知出力
AVP770		4-20mA	接点出力
AVP771		4 mA to trip, de-energize to trip	開度発信出力
AVP772			なし
AVP780	単動 / 複動 (パイロット調整にて変更可能)	0-20mA	接点出力
AVP781		0 mA to trip, de-energize to trip	開度発信出力
AVP782			なし
AVP790		0-24VDC	接点出力
AVP791		0 V to trip, de-energize to trip	開度発信出力
AVP792			なし

3. 用語と略語

DD	Device Description (デバイスディスクリプション) ホストアプリケーションによって利用される電子データファイルで機器固有のパラメータや機能を記述したもの。
DTM	機器パラメータへのアクセス、機器の設定や操作、不具合の診断を実行する統一化された機構を提供するデバイスドライバ。
FMEDA	Failure Mode Effect and Diagnostic Analysis 故障モード影響および診断解析
HART	Highway Addressable Remote Transducer 直流電流に重畳されたデジタル通信方法のオープン規格。 ※ HART は FieldComm Group の商標です。
HFT	Hardware Fault Tolerance (ハードウェア障害許容度) 0、1、2、3 という整数の値をとり、N+1 のハードウェア故障発生により安全機能が喪失する場合、HFT が N である、という。
Low Demand Mode	低頻度作動要求モード 安全システムへの作動要求が年 1 回以下の運用モード
LUI	Local User Interface (ローカルユーザーインターフェース)
PF Davg	Average Probability of Failure on Demand (作動要求時平均機能失敗確率)
PST	Partial Stroke Test (部分作動検査)
Safety	許容不能なリスクがないこと
Safety Function	安全計装システムにおいて使われる、特定の危険事象の発生確率を許容可能なレベルまで低減することを意図した、単一の機器もしくは複数機器の組み合わせの機能
SFF	Safe Failure Fraction (安全側故障割合)
SIF	Safety Instrumented Function (安全計装機能)
SIL	Safety Integrity Level (安全達成度水準)
SIS	Safety Instrumented System (安全計装システム)
Type A デバイス	個別部品から成る“複雑でない”デバイス。 (詳細は IEC 61508-2 の 7.4.4.1.2 を参照ください。)

4. 関連文書

- 安全計装システム対応スマート ESD デバイス 700 シリーズ AVP77□ / 78□ / 79□ 形 取扱説明書 (CM1-AVP772-2001)
- IEC 61508: 2010 Functional safety of electrical/electronic/programmable electronic safety-related systems
- ANSI/ISA 84.00.01-2004 (IEC 61511 Mod.) Functional Safety: Safety Instrumented Systems for the Process Industry Sector
- Exida FMEDA Report for Azbil AVP700 SIS-Report No. AZB 12-03-041 R001 (FMEDA レポート)

取扱説明書と FMEDA レポートの入手に付きましては弊社担当者にお問い合わせください。

5. 一般要求



安全のためにこの安全マニュアルと取扱説明書に記載されたすべての指示、警告を注意深く読まなければなりません。

- 取り付けと設定については取扱説明書 (CM1-AVP772-2001) を参照してください。
- 本器のメンテナンスとテストを実施する作業者は、バルブ、ポジショナー、および SIS についての知識を有する必要があります。そうでない場合、作業者は適切なトレーニングと教育を受けてください。

6. 安全計装システム設計

6.1. 安全機能

本器のSISへの適用は低頻度作動要求モードに限定されます。表1に本器の通常状態と安全状態を記します。本器を操作する制御信号（入力信号）は以下の通りです。

- **0-24VDC:** 通常操作時は24VDCを本器に与えます。緊急命令はループを遮断するか、電圧信号を0.5V以下とすることで発行されます。
- **0-20mA:** 通常操作時は、20mA電流ループ信号を本器に与えます。緊急命令はループを遮断するか、電流信号を0.5mA以下とすることで発行されます。
- **4-20mA:** 通常操作時は、20mA電流ループ信号を本器に与えます。緊急命令は電流信号を4mAとすることで発行されます。

表1 通常状態と安全状態

パイロットリレータイプ	入力信号	通常状態	安全状態
単動	0 VDC, 0mA, or 4 mA	-	P1 < 供給圧の5%
	24 VDC or 20 mA	P1 ≥ 供給圧の95%	-
複動	0 VDC, 0mA, or 4 mA	-	P2 - P1 ≥ 供給圧の95%
	24 VDC or 20 mA	P1 - P2 ≥ 供給圧の95%	-

P1：本器の出力圧力1

P2：本器の出力圧力2

6.2. 安全達成度水準

- **Systematic Integrity**
SIL 3 Capable— SIS対応700シリーズはIEC61508安全達成度水準SIL3の設計プロセス要求を満足しています。
- **Random Integrity**
SIS対応700シリーズはIEC61508によるType Aデバイスに分類されます。最終操作端サブシステムのSFFを決定するには、サブシステム全体を評価する必要があります。サブシステムのSFFが90%より大きく、かつPFDAvgが 10^{-3} より小さい場合、そのサブシステム設計はSIL3 @ HFT=0を満足します。

6.3. 故障率

すべての故障率についてはFMEDAレポートを参照してください。故障率データは製品寿命期間内で有効です。故障率はその期間後、増加します。FMEDAレポートに記載されたデータを基にして製品寿命期間を超える利用時間についての信頼性計算を行った場合、あまりにも楽観的な結果が得られる可能性があります。つまり、計算で得られたSIL（安全達成度水準）は、実際には達成されません。パシヤルストロークテストの診断率を主張するためには、それが自動的に実行され、かつ、その頻度が少なくともブルーテスト頻度の10倍以上でなければなりません。故障解析に使われたこのような仮定の詳細についてはFMEDAレポートを参照してください。

6.4. 利用上の制限

- 安全計装機能の設計検証は、安全計装機能に使われている本器を含む全装置に対して実施されてなければなりません。安全計装システムは安全達成度水準に従った要求、特に、作動要求時平均機能失敗確率（PFDAvg）の制限、を満足しなければなりません。
- システム応答時間は操作端サブシステム全体に依存します。各操作端についてシステム応答時間がプロセス安全時間よりも短いことを必ず検証しなければなりません。
- 本器の故障応答時間はパシヤルストロークテストのインターバルに平均修復時間を加えたものによって決定されます。
- バルブの操作手段は、本器が安全状態となったときに自動的にそのバルブが安全状態に移るような種類のものでなければなりません。この条件下でのバルブストローク時間についてもSIS設計の一部として検討される必要があります。
- 供給空気圧力は700kPaを超えてはなりません。その他、取扱説明書に記載された供給空気の条件に必ず従ってください。
- PSTを実施するには、SISポジショナーモードが“ON-OFF”にセットされていないとできません。開度制御モードではPSTは実施できません。

6.5. 使用環境の制限

- 使用温度範囲: -40 ~ +80°C *
 - 湿度範囲: 5% ~ 100%RH
- * 防爆の種類により異なります。詳細は取扱説明書を参照ください。

6.6. 診断通知への接点出力／開度発信の利用

“PSTあり”の故障率を適用する場合、システムは本器のアラーム状態をモニタリングできなければなりません。

- 本器が接点出力または開度発信付きモデルであることを確認してください。（出力なしモデルをお使いの場合、“PSTあり”の故障率は適用できません。）

PSTを含むすべての故障の診断検知時間（最大値）は設定されたPSTインターバル時間によって決まります。診断結果は故障の検知後、30秒以内に通知されます。

注記

HART通信は情報（収集、確認）目的には利用できますが、診断通知としては安全認証されていません。

7. 設置と試運転

- 本器が目的とする安全計装機能での使用に適しているか確認してください。
- 銘板のマーキングが使用するハザード地域に適しているか確認してください。（必要であれば）
- ロジックソルバーの取扱説明書および安全マニュアルを参照してロジックソルバーとの接続が適切に行われていることを確認してください。
- SISポジショナーモードが適切に選択されているか確認してください。
- パスワード保護機能が“Enabled”となっていることを確認してください。
- “PSTあり”故障率を適用する場合、SISポジショナーモードが“ON-OFF”であること、スケジュールPSTがEnabledであること、PSTインターバルが適切に設定されていること、を確認してください。
- 本器のシステム設置後、SIS全体の安全機能に伴った最終操作端サブシステムに含まれる本器の安全機能を必ずテストし、安全要求および適用されたプロセス安全時間要求を満たすことを確認してください。
- システム応答時間はプロセス安全時間を下回らなければなりません。本器は緊急命令を受けて3秒以内に出力空気を排気し始めます。

8. 運転

“In use by an Operator”のステータスが立っている場合、スケジュールPSTは予定された時間には開始せず、次の予定時間まで延期されます。“In use by an Operator”は、LUIもしくはHARTホストのいずれかが本器の設定、調整を独占的に許可された状態を意味します。HARTホストでは、“操作許可”メソッド、LUIでは左ボタンの長押しによってこの状態となります。“PSTあり”の故障率を適用する場合は、本器の状態を“In use by an Operator”にしないでください。その必要がある場合、PST時間実行時間を確認してください。

運転中はパスワード保護機能を“Enabled”に設定してください。パスワード保護機能が“Enabled”の場合、本器の状態を“In use by an Operator”に変えるためには正しいパスワードの入力が求められますので、この仕組みによって誤ってスケジュールPSTを妨害してしまうことを防ぎます。

9. 定期検査

ブルーテストから成る定期的な検査は、本器並びに、それが組み付けられているバルブ、アクチュエーターのPFDAvgを下げるのに効果的な方法です。定期検査の結果は記録され、定期的にレビューされなければなりません。

9.1. SIS対応700シリーズの検査手順

ブルーテストは手動で実施されるフルストロークテストです。テストの一部として、定義された安全状態を達成するSIFの性能が確認されなければなりません。ブルーテストインターバルはSIFに含まれるすべての構成要素の故障率、そしてリスク低減要求に基づいて定められなければなりません。この決定はSIS設計のクリティカルな部分です。ブルーテストは本器の自動診断によって検知できない危険故障のほとんどを検知します。ブルーテストは次の手順を含みます。

- “PSTあり”の故障率を適用している場合、作業者の怪我を防ぐためスケジュールPSTをDisabledにしてください。
- 本器のアラーム情報をHART通信機器（Valstaff、DD、DTMホストなど）を利用して読みます。アラームメッセージがある場合、原因を調査しすべて解決してください。
- 最終操作端をバイパスする、または、誤ったトリップを回避するための適切な措置を取ります。
- 診断通知出力を使用している場合、出力をバイパスする、または、誤ったトリップを回避するための適切な措置を取ります。
- 供給空気の消費量が過大でないことを確認します。
- 本器の入力をトリップ信号にします。（0mA、4mA、0Vのいずれか）

- 本器とバルブが、完全に、かつ、要求された安全時間内に定義された安全状態に達することを本器とは独立した手段を用いて確認します。
- 本器への入力を通常動作に戻します。
- 本器とバルブが、定義された通常状態に達することを本器とは独立した手段を用いて確認します。
- 空気漏れがないか、目に見える損傷や汚れ（油・水等の内部混入）がないか検査します。
- ネジのゆるみ等、機械的に正しくない状態がないか検査します。
- “PSTあり”故障率を適用している場合、スケジュールPSTをEnabledに設定します。
- 検査の結果、発見された異常等をSIF検査データベースに記録します。
- バイパス等の措置を取り除き、通常運転に復帰させます。

9.2. 保守

取扱説明書 (CM1-AVP772-2001) を参照ください。

9.3. 修理と交換

取扱説明書に記載されたトラブルシューティングや修正手順に従って是正措置を取ってください。

機器が故障した場合は、本器全体を交換しなければなりません。

ご注文・ご使用に際しては、下記URLより「ご注文・ご使用に際しての
ご承諾事項」を必ずお読みください。

<http://www.azbil.com/jp/product/factory/order.html>

アズビル株式会社 アドバンスオートメーションカンパニー

本 社 〒100-6419 東京都千代田区丸の内2-7-3 東京ビル

北海道支店 ☎(011)211-1136	中部支社 ☎(052)324-9772
東北支店 ☎(022)290-1400	関西支社 ☎(06)6881-3331
北関東支店 ☎(048)621-5070	中国支店 ☎(082)554-0750
東京支社 ☎(03)6432-5142	九州支社 ☎(093)285-3530

〈アズビル株式会社〉 <http://www.azbil.com/jp/>

〔ご注意〕 この資料の記載内容は、お断りなく変更する場合がありますのでご了承ください。

本資料からの無断転載、複製はご遠慮ください。(30)

発行年月：2015年12月 初版