User's
Manual

ADMAG TI シリーズ
AXG/AXW 電磁流量計
安全マニュアル

IM 01E21A21-02JA

YOKOGAWA
横河電機株式会社

IM 01E21A21-02JA
初版

ADMAG TI シリーズ
AXG/AXW 電磁流量計
安全マニュアル

IM 01E21A21-02JA 初版

目　次

1.　はじめに..1

2.　安全計装システムの設置にあたって 4

2.1　適用範囲と目的..4

2.2　安全計装システム用途における本計器の使用 4

2.2.1　安全機能..4

2.2.2　安全確度..4

2.2.3　診断応答時間 4

2.2.4　設定...4

2.2.5　安全度を保つための設定...5

2.2.6　プルーフテスト 5

2.2.7　修理・交換..7

2.2.8　起動時間...7

2.2.9　ファームウェアの更新 7

2.2.10　安全性データ 7

2.2.11　耐用年数の制限...7

2.2.12　環境の制限..7

2.2.13　用途の制限..7

2.3　適用範囲と目的..8

2.3.1　用語...8

2.3.2　略語...8

SIL Declaration of Conformity

Failure Mode, Effects and Diagnostic Analysis

説明書　改訂情報

1. はじめに

このたびは当社の ADMAG TI（Total Insight）シリーズ AXG/AXW 電磁流量計をご採用いただき，まことにありがとうございます。
本書は，AXG/AXW 電磁流量計の安全計装システムの設置について説明した取扱説明書です。
本書に記載されていない項目については，当社 Web ページより該当する機器の取扱説明書をダウンロードし，その内容を必ずお読みいただき，正しくお使いください。
形名および仕様の確認は，表 1.1 の一般仕様書を参照してください。
当社 Web ページのアドレス：
http://www.yokogawa.co.jp/fld/download/
また，取扱説明書の印刷物はご購入もいただけます。詳しくは当社営業／代理店までお問い合わせください。

表 1.1　形名と必要なドキュメント番号

形名	ドキュメント名称	ドキュメント番号
AXG□□□ AXW□□□ AXG4A AXW4A AX01C	ADMAG TI シリーズ AXG/AXW 電磁流量計 はじめにお読みください	IM 01E21A21-01Z1
	ADMAG TI シリーズ AXG/AXW 電磁流量計 安全マニュアル	IM 01E21A21-02JA (本書)
AXG□□□ AXG4A AX01C	ADMAG TI シリーズ AXG 電磁流量計 スタートアップマニュアル	IM 01E22A01-01JA
	ADMAG TI シリーズ AXG 電磁流量計 保守マニュアル	IM 01E22A01-02JA
	ADMAG TI シリーズ AXG 電磁流量計 BRAIN 通信形	IM 01E22A02-01JA
	ADMAG TI シリーズ AXG 電磁流量計 HART 通信形	IM 01E22A02-02JA
	ADMAG TI シリーズ AXG 電磁流量計 一般仕様書	GS 01E22A01-01JA
AXW□□□ AXW□□□G AXW□□□W AXW4A AX01C	ADMAG TI シリーズ AXW 電磁流量計 [口径：25～400 mm] スタートアップマニュアル	IM 01E24A01-01JA
	ADMAG TI シリーズ AXW 電磁流量計 [口径：500～1800 mm] スタートアップマニュアル	IM 01E25A01-01JA
	ADMAG TI シリーズ AXW 電磁流量計 [口径：25～1800 mm] 保守マニュアル	IM 01E24A01-02JA
	ADMAG TI シリーズ AXW 電磁流量計 BRAIN 通信形	IM 01E24A02-01JA
	ADMAG TI シリーズ AXW 電磁流量計 HART 通信形	IM 01E24A02-02JA
	ADMAG TI シリーズ AXW 電磁流量計 [口径：25～400 mm]	GS 01E24A01-01JA
	ADMAG TI シリーズ AXW 電磁流量計 [口径：500～1800 mm]	GS 01E25D11-01JA

注記

本書中で製品について，AXG □□□等の表記がされている場合，下記のいずれかが□□□に適用できることを示します。
AXG □□□の場合：
002, 005, 010, 015, 025, 032, 040, 050, 065, 080, 100, 125, 150, 200, 250, 300, 350, 400
AXW □□□の場合：
025, 032, 040, 050, 065, 080, 100, 125, 150, 200, 250, 300, 350, 400
AXW □□□ G，または AXW □□□ W の場合：
500, 600, 700, 800, 900, 10L

重要

SIL 1 の対象は，以下になります。
- AXG 一体形
- AXG 分離形検出器と AXG4A 分離形変換器の組み合わせ
- AXW 一体形
- AXW 分離形検出器と AXW4A 分離形変換器の組み合わせ

AXFA11G または AXFA11P 分離形変換器との組み合わせの場合，SIL 1 の対象外になりますので，注意してください。

■ 本計器の保護・安全・改造および廃棄に関する注意

本計器および本書では，安全に関する次のようなシンボルマークとシグナル用語を使用しています。

⚠ 警告

回避しないと，死亡または重傷を招く恐れがある危険な状況が生じることが予見される場合に使う表示です。本書ではそのような場合その危険を避けるための注意事項を記載しています。

⚠ 注意

回避しないと，軽傷を負うかまたは物的損害が発生する危険な状況が生じることが予見される場合に使う表示です。本書では取扱者の身体に危険が及ぶ恐れ，または計器を損傷する恐れがある場合，その危険を避けるための注意事項を記載しています。

重要

計器を損傷したり，システムトラブルになるおそれがある場合に，注意すべきことがらを記載しています。

注記

操作や機能を知るうえで，注意すべきことがらを記載しています。

機器本体にはいくつかの記号が書かれています。その意味は以下のとおりです。

- 保護接地端子
- ⏚ 機能接地端子（保護接地端子として使用しないこと）
- ∿ 交流
- ⎓ 直流
- ⚠ 取扱注意
  人体および機器を保護するために取扱説明書を参照する必要がある場所についています。

- 本計器および本計器を含むシステムの保護・安全のため，本計器を取り扱う際は，表 1.1 の取扱説明書の安全に関する指示事項に従ってください。なお，これらの指示事項に反する扱いをされた場合，本計器の保護機能が損なわれるなど，その機能が十分に発揮されない場合があります。この場合，当社は製品の品質・性能・機能および安全性を保証いたしかねます。
- 本計器を改造することは固くお断りいたします。
- 本計器は，地域および国の法律 / 規制に従って，廃棄する必要があります。

■ 本書に対するご注意

- 本書は，最終ユーザまでお届けいただきますようお願いいたします。
- 本書の内容は，将来予告なしに変更することがあります。
- 本書の内容の全部または一部を無断で転載，複製することは禁止されています。
- 本書は，本計器の市場性またはお客様の特定目的への適合などについて保証するものではありません。
- 本書の内容に関しては万全を期していますが，万一ご不審の点や誤りなどお気づきのことがありましたら，当社各営業拠点または購入の代理店までご連絡ください。
- 特別仕様につきましては記載されておりません。
- 機能・性能に支障がないと思われる仕様変更，構造変更，および使用部品の変更につきましては，その都度の本書改訂が行われない場合がありますのでご了承ください。
- 本計器をご使用前に，本書と表 1.1 の取扱説明書をよくお読みいただき，正しくお使いください。
  製品の仕様は表 1.1 の一般仕様書をお読みください。

■ 商標

- 本文中で使用されている横河電機製品の商品名は，横河電機の登録商標または商標です。
- 本文中で使用されている会社名，商品名は，各社の登録商標または商標です。
- 本文中の各社の登録商標または商標には，「™」，「®」マークは表示しておりません。

■　本計器を安全にご使用いただくために

本計器および本計器を含むシステムの保護・安全のため，本計器を取り扱う際は，表 1.1 の取扱説明書の安全に関する指示事項に従ってください。なお，これらの指示事項に反する扱いをされた場合，本計器の保護機能が損なわれるなど，その機能が十分に発揮されない場合があります。この場合，本計器のご使用または使用不能から生じる間接損害について，当社は責任を負いかねます。

2. 安全計装システムの設置にあたって

警告

本計器を安全計装システム用途として使用する場合，本計器の安全度を保つため，本章で述べる指示と手順を遵守してください。

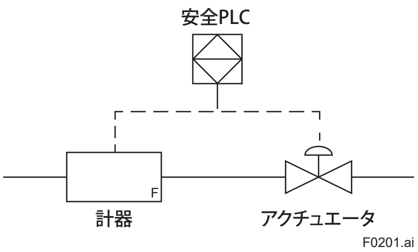
2.1 適用範囲と目的

本章では，安全計装システム用途として設計され，安全度を保つ上で求められる，本計器の設置と操作に必要な使用上の注意と行うべき作業の概要について説明します。本章は，機器のプルーフテストと修理・交換，安全性データ，耐用年数，環境および用途に関する制限，パラメータの設定です。

2.2 安全計装システム用途における本計器の使用

2.2.1 安全機能

本計器は，安全計装システムの計器（低デマンドモード，Type-B）として使用されます。



本計器は，電流出力 1 を安全機能の対象とします。電流出力 1 は，流速，体積流量，質量流量，フローノイズ (AXG のみ) を電流に変換して出力できます。それ以外の機能（表示器など）は，安全機能の範囲外となります。安全計装システムとして使用する場合，安全 PLC との接続は電流出力 1 を使用してください。また，安全度を保って本計器をご使用いただくには，事前に設定が必要です。詳細は，2.2.4 項および 2.2.5 項を参照してください。

2.2.2 安全確度

本計器の規定安全確度は 2% です。この規定安全確度は，内部部品の故障により生じる誤差が 2% 以上の場合に機器の故障として扱われることを示します。

2.2.3 診断応答時間

本計器の診断テストの間隔は，最大 8 秒です。診断テストで故障を検出した場合，1 秒以内に電流出力 1 のバーンアウト（安全状態）によって, 故障発生を上位の安全 PLC に通知します。故障発生時の対応方法は, 表 1.1 の各通信形マニュアルの 4 章を参照してください。

2.2.4 設定

BRAIN 設定ツールまたは HART 設定ツールを用いて，レンジと単位を設定してください。機器の設置後，レンジと単位が正しく設定されていることを確認してください。機器の校正は，パラメータの設定後に行ってください。
パラメータの設定方法は，表 1.1 の各通信形マニュアルの 4 章および 5 章を参照してください。

2.2.5 安全度を保つための設定

安全度を保つため，表 2.2.1 または表 2.2.2 の設定が必要です。

表 2.2.1 ハードウェアによる設定

項目	説明
バーンアウトスイッチ	内部故障を検出した場合の電流出力のバーンアウト方向を設定します。スイッチを High 側または Low 側に設定してください。
ライトプロテクトスイッチ	スイッチを ON 側に設定し，ライトプロテクト機能を有効にしてください。

表 2.2.2 パラメータによる設定

項目	説明
BRAIN 通信：G04:AO1 ALM OUT HART 通信メニューパス： Device root menu ▶ Detailed setup ▶ Analog output/input ▶ Analog output 1 ▶ AO1 alarm out	アラームが発生した場合の電流出力 1 の動作を設定します。安全計装で使用する場合，“> 21.6 mA” または “< 2.4 mA” に設定してください。
BRAIN 通信：H50:SET SIL HART 通信メニューパス： Device root menu ▶ Detailed setup ▶ AUX calculation ▶ Set SIL	安全計装で使用する場合，“Yes” に設定してください。この設定により，アラームが発生した場合の電流出力 1 を “> 21.6 mA” または “< 2.4 mA” 以外に設定できなくなります。アラームが発生した場合，確実に電流出力 1 をバーンアウトするように設定できます。
BRAIN 通信：H30:DENSITY SEL HART 通信メニューパス： Device root menu ▶ Detailed setup ▶ Process variables ▶ Density ▶ Density value select	電流出力 1 を質量流量として使用する場合，“Fixed value” に設定してください。

2.2.6 プルーフテスト

プルーフテストとは，安全計装機能が正しく機能しているかどうかを確認するために定期的に行う機能確認試験です。機器が意図した安全計装機能の実行を阻害するような，自己診断で検知されない故障を検出するため，プルーフテストの実施が必要です。

プルーフテストの間隔は，本計器を含む安全計装機能ごとに行われる安全度計算により決定します。安全計装機能の安全度を維持するには，安全度計算で指定した頻度またはそれ以上でプルーフテストを行う必要があります。

プルーフテストでは，表 2.2.3 の試験が必要です。プルーフテストの結果は，文書化が必要であり，その文書はプラントの安全管理の一部にする必要があります。故障が検出された場合は当社までご連絡ください。

機器のプルーフテストを行う作業者は，バイパス手順，本計器のメンテナンス，変更管理の手順など，安全計装システムの運用について熟知している必要があります。

表 2.2.3 プルーフテスト

試験方法	必要なツール	予想される結果	備考
電流出力ループテスト 1. 安全 PLC のバイパスや誤動作を回避するための適切な処理を行います。 2. BRAIN 通信または HART 通信から, 電流出力 1 のアラーム出力を “> 21.6 mA” に設定後，実際にアラームを発生させ, 電流値が 21.6 mA 超にあることを検証します。 3. 次に，BRAIN 通信または HART 通信から，電流出力 1 のアラーム出力を “< 2.4 mA” に設定後, 実際にアラームを発生させ，電流が 2.4 mA 未満にあることを検証します。 4. エラーやワーニングがない状態にします。 5. レンジの最大流量と最小流量の 2 点で，電流出力の正当性を検証します。 6. 流量 0 の状態で，電流出力の正当性を検証します。 7. 典型的な流量で，電流出力の正当性を検証します。 8. ループを通常状態に戻します。 9. 安全 PLC のバイパスや誤動作を回避するための状態から，通常状態に戻します。	BRAIN 通信： BRAIN 設定ツール HART 通信： HART 設定ツール	プルーフテストカバー率 本質安全回路なし：94% 本質安全回路あり：93% プルーフテストカバー率 (診断機能と組み合わせた場合) 本質安全回路なし：99% 本質安全回路あり：99%	本計器が正確な信号を出しているか確認するため，出力を確認する必要があります。

アラーム発生例（BRAIN 通信：66:Dens cfg ERR，HART 通信：Density configuration error の場合）：

(1) アラーム発生時に電流出力 1 を 21.6 mA 超に振り切らせるために，下記の設定を行います。
BRAIN 通信：G04:AO1 ALM OUT
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Analog output/input ▶ Analog output 1 ▶ AO1 alarm out
アラーム発生時に電流出力 1 を 21.6 mA 超に設定する場合，“> 21.6 mA”に設定します。

① BRAIN 通信：H30: DENSITY SEL
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Process variables ▶ Density ▶ Density value select
上記のパラメータで，“Fixed value”に設定します。

② BRAIN 通信：H32:FIXED DENS
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Process variables ▶ Density ▶ Density fixed value
上記のパラメータで，“0.0”に設定します。

③ BRAIN 通信：C30:PV FLOW SEL
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Process variables ▶ PV flow select
上記のパラメータで，“Mass”に設定します。

この結果，電流出力 1 が 21.6 mA 超に振り切れます。

(2) アラーム発生時に電流出力 1 を 2.4 mA 未満に振り切らせるために，下記の設定を行います。
BRAIN 通信：G04:AO1 ALM OUT
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Analog output/input ▶ Analog output 1 ▶ AO1 alarm out
アラーム発生時に電流出力 1 を 2.4 mA 未満に設定する場合，“< 2.4 mA”に設定します。

① BRAIN 通信：H30: DENSITY SEL
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Process variables ▶ Density ▶ Density value select
上記のパラメータで，“Fixed value”に設定します。

② BRAIN 通信：H32:FIXED DENS
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Process variables ▶ Density ▶ Density fixed value
上記のパラメータで，“0.0”に設定します。

③ BRAIN 通信：C30:PV FLOW SEL
HART 通信メニューパス：
Device root menu ▶ Detailed setup ▶ Process variables ▶ PV flow select
上記のパラメータで，“Mass”に設定します。

この結果，電流出力 1 が 2.4 mA 未満に振り切れます。

2.2.7 修理・交換

プロセスがオンライン中に本計器の修理を行う場合，本計器を安全計装システムからバイパスしてください。ユーザーはバイパス手順を正しく設定する必要があります。検出された故障は，当社までご連絡ください。本計器の交換を行う場合，本書の手順に従ってください。本計器を修理または交換を行う場合，訓練を受けたエンジニアが行ってください。

2.2.8 起動時間

本計器は，ダンピング時定数を 0.1 秒に設定した場合，電源投入後 3 秒以内に有効な信号を出力します。

2.2.9 ファームウェアの更新

ユーザーがファームウェアを更新することはありません。ファームウェアの更新が必要と判断された場合，更新は引き取りによって行います。

2.2.10 安全性データ

当社が提供する FMEDA レポートには，故障率と故障モードが記載されています。
本計器の単独使用において，安全計装機能全体の PFDavg 計算により SIL 1 まで適用できる能力を有します。また，本計器は SIL3 まで適用可能な開発プロセスに対応し，冗長構成の使用において，安全計装機能全体の PFDavg 計算による SIL 3 まで適用することができます。
冗長構成で使用する場合, 安全計装機能の PFD 計算のための β-factor（共通原因故障率）は 5% にすることを推奨します。プラントの作業者が，共通原因故障のトレーニングと共通原因故障防止に向けた明確な詳しいメンテナンス手順を設けた場合，β -factor は 2%にすることができます。

2.2.11 耐用年数の制限

本計器の予測耐用年数は 10 年です。FMEDA レポートの信頼性データは 10 年を有効とします。10 年を超えて使用した場合，本計器の故障率が上昇する可能性があり，FMEDA レポートに記載された安全性データに基づいた安全度水準は達成できない場合があります。

2.2.12 環境の制限

本計器の環境に関する制限は，表 1.1 の一般仕様書を参照してください。

2.2.13 用途の制限

本書で規定した，本計器の用途に関する制限を外れて使用する場合，2.2.10 項に記載された安全性データは無効になります。

2.3 適用範囲と目的

2.3.1 用語

● 安全

用語	内容
安全	受容できないリスクから免れている状態です（JIS C 0508 の表現）。
機能安全	機器・機械・プラント・装置に対して，安全と定義された状態を達成または維持するために必要な動作を実行するシステムの能力を指します。
基本的安全	感電，火災，爆発などの危険から人間を保護するよう，機器は設計および製造されなければなりません。こうした保護は，通常時および故障時でも常に有効でなければなりません。

● 検証

用語	内容
適合確認	ライフサイクルの各段階で，各段階の最初に意図した目的と要求事項に見合うものが最終的に得られたことを実証します。検証は，分析，試験，またはその両方により行われるのが普通です。
妥当性確認	安全関連システムまたはその組み合わせと外的リスク軽減施設が，あらゆる点において安全要求仕様を満たしていることを実証します。妥当性検査は，試験により行われるのが普通です。
安全アセスメント	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を指します。

その他の安全手法および対策で用いられる用語の定義および安全関連システムの説明は，JIS C 0508-4（IEC 61508-4）を参照してください。

2.3.2 略語

用語	内容
FMEDA (Failure Mode, Effects and Diagnostic Analysis)	故障モード，影響および診断分析
SIF (Safety Instrumented Function)	安全計装機能
SIL (Safety Integrity Level)	安全度水準
SIS (Safety Instrumented Systems)	安全計装システム
SLC (Safety Lifecycle)	安全ライフサイクル

SIL Declaration of Conformity Functional Safety according to IEC61508:2010 Parts 1-7. ADMAG TI Series AXG/AXW Magnetic Flowmeter

Yokogawa Electric Corporation
Musashino-shi, Tokyo, Japan

Systematic Capability: SC 3 (SIL 3 Capable)
Random Capability: Type B Element (Route 1_H)
SIL 1 @ HFT = 0; SIL 2 @ HFT = 1; SIL 3 @ HFT = 2;

IEC 61508 Failure Rates in FIT

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Non-IS version for; AXG Magnetic Flowmeter (*1) AXW Magnetic Flowmeter (*2)	0	256	2461	315	89.6%
IS version for; AXG Magnetic Flowmeter (*1) AXW Magnetic Flowmeter (*2)	0	223	2248	325	88.4%

*1: AXG Integral type and its Remote type which is connected to AXG4A transmitter.

*2: AXW Integral type and its Remote type which is connected to AXW4A transmitter.

Systematic Capability:
Above products satisfy the requirements of manufacturer's design process for Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer. A Safety Instrumented Function (SIF) designed for above products must not be used at a SIL level higher than stated.

Random Capability:
The SIL limit imposed by the Architectural Constraints must be met for each element.

Tokyo Japan, 28 March 2017,
IA Platform Business Headquarters Product Business Center Flowmeters Dept.

General Manager: Takashi Kawano

Takashi Kawano
Signature

Failure Modes, Effects and Diagnostic Analysis

Project:
AXG/W Magnetic Flowmeter
Company:
Yokogawa Electric Corporation
Musashino, Tokyo
Japan

Contract Number: Q16/03-009
Report No.: YEC 16/03-009 R001
Version V1, Revision R5, November 7, 2016
Kiyoshi Takai

Management Summary

This report summarizes the results of the hardware assessment in the form of a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the AXG/W Magnetic Flowmeter, hardware software revision per Section 2.5.1. A Failure Modes, Effects, and Diagnostic Analysis is one of the steps to be taken to achieve functional safety certification per IEC 61508 of a device. From the FMEDA, failure rates are determined. The FMEDA that is described in this report concerns only the hardware of the AXG/W Magnetic Flowmeter. For full functional safety certification purposes all requirements of IEC 61508 must be considered.

The AXG/W Magnetic Flowmeter uses excitation coils and electrodes to measure fluid flow. HART or BRAIN communication signal are superimposed on 4-20 mA signal. Besides the analog 4-20mA current output is a Pulse Output signal. Diagnostics include monitoring electrodes for the adherence of insulating material that would affect the flow measurement and a reverse calculation of the process variables.

The AXG/W Magnetic Flowmeter is classified as a Type B[1] element according to IEC 61508, having a hardware fault tolerance of 0.

Based on the assumptions listed in 4.3, the failure rates for the AXG/W Magnetic Flowmeter are listed in section 4.4.

These failure rates are valid for the useful lifetime of the product, see Appendix A.

Failure rates listed in this report do not include failures due to wear-out of any components. They reflect random failures and include failures due to external events, such as unexpected use, see section 4.2.

A user of the AXG/W Magnetic Flowmeter can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

[1] Type B element: “Complex” element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

Table of Contents

2.1 *exida* 5
2.2 Roles of the parties involved 5
2.3 Standards and literature used 5
2.4 *exida* tools used 6
2.5 Reference documents 6
2.5.1 Documentation provided by Yokogawa Electric Corporation 6
2.5.2 Documentation generated by *exida* 7
4.1 Failure categories description 9
4.2 Methodology – FMEDA, failure rates 10
4.2.1 FMEDA 10
4.2.2 Failure rates 10
4.3 Assumptions 11
4.4 Results 12
5.1 PFD_{avg} calculation AXW/G Magnetic Flowmeter 14
7.1 Liability 16
7.2 Releases 16
7.3 Future Enhancements 16
7.4 Release signatures 17
Appendix A Lifetime of Critical Components 18
Appendix B Proof Tests to Reveal Dangerous Undetected Faults 19
B.1 Suggested Proof Test 19
Appendix C *exida* Environmental Profiles 20
Appendix D Determining Safety Integrity Level 21

1 Purpose and Scope

This document shall describe the results of the hardware assessment in the form of the Failure Modes, Effects and Diagnostic Analysis carried out on the AXG/W Magnetic Flowmeter. From this, failure rates and example PFD_{avg} values may be calculated.

The information in this report can be used to evaluate whether an element meets the average Probability of Failure on Demand (PFD_{AVG}) requirements and if applicable, the architectural constraints / minimum hardware fault tolerance requirements per IEC 61508 / IEC 61511.

A FMEDA is part of the effort needed to achieve full certification per IEC 61508 or other relevant functional safety standard.

2 Project Management

2.1 *exida*

exida is one of the world's leading accredited Certification Bodies and knowledge companies specializing in automation system safety and availability with over 400 years of cumulative experience in functional safety. Founded by several of the world's top reliability and safety experts from assessment organizations and manufacturers, *exida* is a global company with offices around the world. *exida* offers training, coaching, project oriented system consulting services, safety lifecycle engineering tools, detailed product assurance, cyber-security and functional safety certification, and a collection of on-line safety and reliability resources. *exida* maintains the largest process equipment database of failure rates and failure modes with over 100 billion unit operating hours.

2.2 Roles of the parties involved

Yokogawa Electric Corporation	Manufacturer of the AXG/W Magnetic Flowmeter
exida	Performed the hardware assessment

Yokogawa Electric Corporation contracted *exida* in March 2016 with the hardware assessment of the above-mentioned device.

2.3 Standards and literature used

The services delivered by *exida* were performed based on the following standards / literature.

[N1]	IEC 61508-2: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	Electrical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	*exida* LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	*exida* LLC, Safety Equipment Reliability Handbook, Third Edition, 2007, ISBN 978-0-9727234-9-7
[N5]	Goble, W.M. 2010	Control Systems Safety Evaluation and Reliability, 3rd edition, ISA, ISBN 97B-1-934394-80-9. Reference on FMEDA methods
[N6]	IEC 60654-1:1993-02, second edition	Industrial-process measurement and control equipment – Operating conditions – Part 1: Climatic condition
[N7]	Scaling the Three Barriers, Recorded Web Seminar, June 2013,	Scaling the Three Barriers, Recorded Web Seminar, June 2013, http://www.exida.com/Webinars/Recordings/SIF-Verification-Scaling-the-Three-Barriers

[N8]	Meeting Architecture Constraints in SIF Design, Recorded Web Seminar, March 2013	http://www.exida.com/Webinars/Recordings/Meeting-Architecture-Constraints-in-SIF-Design

2.4 *exida* tools used

[T1]	V7.1.18	*exida* FMEDA Tool
[T2]	V 2.5.1.7	*exSILentia*

2.5 Reference documents

2.5.1 Documentation provided by Yokogawa Electric Corporation

[D1]	Doc # AXG_Block Diagram_r1	Block Diagram
[D2]	Doc # FD1-F9482PA, Rev 0	Schematic Drawing, Main Board (100V)
[D3]	Doc # FD1-F9482PB, Rev0	Schematic Drawing, Main Board (24V)
[D4]	Doc # FD1-F9482SA00_r2, Rev 0	Schematic Drawing, Sensor Board
[D5]	Doc # FD1-F9484AA_1_21, Rev 1	Schematic Drawing, Multi-Option Board
[D6]	Doc # FD1-F9482XA_r0, Rev 0	Schematic Drawing, Neck Terminal Board
[D7]	Doc # FD1-F9482YA00_r0, Rev 0	Schematic Drawing, Neck Barrier Board
[D8]	Doc # FD1-F9480VA_0_21, Rev 0	Schematic Drawing, Terminal Board
[D9]	Doc # FDI-F9481LA_0_21, Rev 0	Schematic Drawing, Indicator Board
[D10]	Doc # FD1-F9484EP_1_21, Rev 1	Schematic Drawing, IS Base Board
[D11]	Doc # FD1-F9484EC_r0, Rev 0	Schematic Drawing, Non-IS Base Board
[D12]	Doc # FD1-F9484AG_0_21, Rev 0	Schematic Drawing, IS Option Board
[D13]	Doc # FE1-F9482PA_PB_20160405, Rev 0	Bill of Material, Main Board (100V)
[D14]	Doc # FE1-F9482PA_PB_20140405, Rev 0	Bill of Material, Main Board (24V)

[D15]	Doc # FE1-F9482SA00_r2, Rev 0	Bill of Material, Sensor Board
[D16]	Doc # FE1-F9484AA_3_21, Rev 3	Bill of Material, Multi-Option Board
[D17]	Doc # FE1-F9482XA_r0, Rev 0	Bill of Material, Neck Terminal Board
[D18]	Doc # FE1-F9482YA00_r0, Rev 0	Bill of Material, Neck Barrier Board
[D19]	Doc # FE1-F9480VA_0_21, Rev 0	Bill of Material, Terminal Board
[D20]	Doc # FE1-F9481LA_3_21, Rev 3	Bill of Material, Indicator Board
[D21]	Doc # FE1-F9484EP_1_21, Rev 1	Bill of Material, IS Base Board
[D22]	Doc # FE1-F9484EC_r0, Rev 0	Bill of Material, Non-IS Base Board
[D23]	Doc # FE1-F9484AG_4_21, Rev 4	Bill of Material, IS Option Board

2.5.2 Documentation generated by *exida*

[R1]	AXG_W Magnetic Flowmeter FMEDA - Non IS- 01Aug2016.efm	Failure Modes, Effects, and Diagnostic Analysis – AXG/W Magnetic Flowmeter (includes sensor) - Non IS
[R2]	AXG_W Magnetic Flowmeter FMEDA -IS - 01Aug2016.efm	Failure Modes, Effects, and Diagnostic Analysis – AXG/W Magnetic Flowmeter (includes sensor) - IS
[R3]	YEC 16-03-009 R001 V1R5 FMEDA AXG_W.pdf	FMEDA report, AXG/W Magnetic Flowmeter (this report)
[R4]	YEC 16-08-013 AXG_W Magnetic Flowmeter FMEDA - Non IS-V1R1_After FIT.efm	Failure Modes, Effects, and Diagnostic Analysis – AXG/W Magnetic Flowmeter (includes sensor) -Non IS, after FIT
[R5]	YEC 16-08-013 AXG_W Magnetic Flowmeter FMEDA -IS – V1R1_After FIT.efm	Failure Modes, Effects, and Diagnostic Analysis – AXG/W Magnetic Flowmeter (includes sensor) – IS, After FIT

3 Product Description

The AXG/W Magnetic Flowmeter uses excitation coils and electrodes to measure fluid flow. HART or BRAIN communication signal are superimposed on 4-20 mA signal. Besides the analog 4-20mA current output is a Pulse Output signal. Diagnostics include monitoring electrodes for the adherence of insulating material that would affect the flow measurement and a reverse calculation of the process variables and coil open or short detection.

The FMEDA includes the coils, electrodes and the four wire powered electronics. See diagram below.

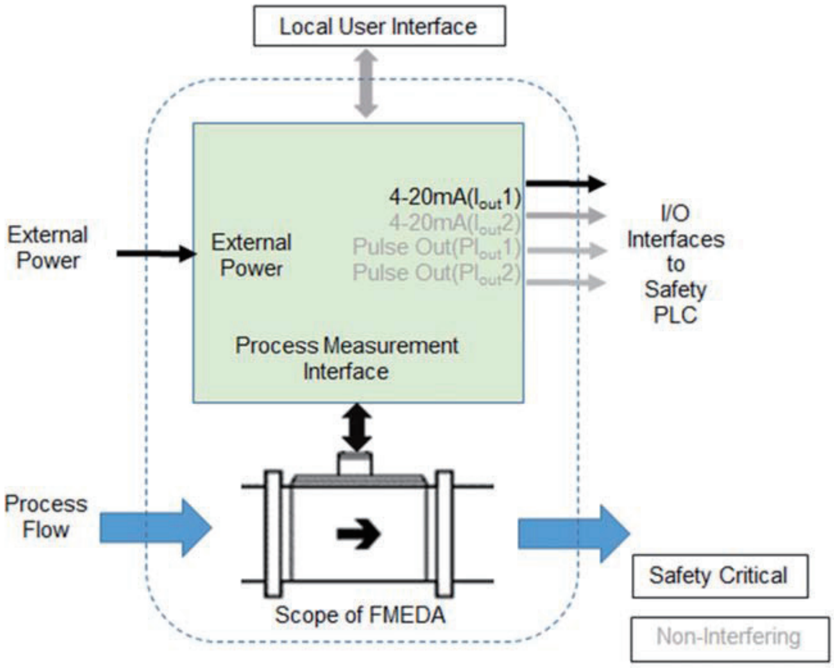


Figure 1 AXG/W Magnetic Flowmeter, Parts included in the FMEDA

The AXG/W Magnetic Flowmeter is classified as a Type B[2] element according to IEC 61508, having a hardware fault tolerance of 0.

[2] Type B element: "Complex" element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2, ed2, 2010.

4 Failure Modes, Effects, and Diagnostic Analysis

The Failure Modes, Effects, and Diagnostic Analysis was performed based on the documentation in section 2.5.1 and is documented in [R1] , [R2], [R3], [R4]and [R3].

4.1 Failure categories description

In order to judge the failure behavior of the AXG/W Magnetic Flowmeter, the following definitions for the failure of the device were considered.

Fail-Safe State	Failure that deviates the process signal or the actual output by more than 2% of span drifts toward the user defined threshold (Trip Point) and that leaves the output within the active scale.
Fail Safe	Failure that causes the device to go to the defined fail-safe state without a demand from the process.
Fail Detected	Failure that causes the output signal to go to the predefined alarm state (3.6 or 21.6 mA, user selectable).
Fail Dangerous	Failure that deviates the process signal or the actual output by more than 2% of span, drifts away from the user defined threshold (Trip Point) and that leaves the output within the active scale.
Fail Dangerous Undetected	Failure that is dangerous and that is not being diagnosed by automatic diagnostics.
Fail Dangerous Detected	Failure that is dangerous but is detected by automatic diagnostics.
Fail High	Failure that causes the output signal to go to the over-range or high alarm output current (> 21 mA).
Fail Low	Failure that causes the output signal to go to the under-range or low alarm output current (< 3.6 mA).
No Effect	Failure of a component that is part of the safety function but that has no effect on the safety function.
Annunciation Detected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics. A Fail Annunciation Detected failure leads to a false diagnostic alarm.
Annunciation Undetected	Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.

The failure categories listed above expand on the categories listed in IEC 61508 which are only safe and dangerous, both detected and undetected. In IEC 61508, Edition 2010, the No Effect failures cannot contribute to the failure rate of the safety function. Therefore they are not used for the Safe Failure Fraction calculation needed when Route 2_H failure data is not available.

Depending on the application, a Fail High or a Fail Low failure can either be safe or dangerous and may be detected or undetected depending on the programming of the logic solver. Consequently, during a Safety Integrity Level (SIL) verification assessment the Fail High and Fail Low failure categories need to be classified as safe or dangerous, detected or undetected.

The Annunciation failures are provided for those who wish to do reliability modeling more detailed than required by IEC61508. It is assumed that the probability model will correctly account for the Annunciation failures. Otherwise the Annunciation Undetected failures have to be classified as Dangerous Undetected failures according to IEC 61508 (worst-case assumption).

4.2 Methodology – FMEDA, failure rates

4.2.1 FMEDA

A Failure Modes and Effects Analysis (FMEA) is a systematic way to identify and evaluate the effects of different component failure modes, to determine what could eliminate or reduce the chance of failure, and to document the system in consideration.

A FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with the extension to identify automatic diagnostic techniques and the failure modes relevant to safety instrumented system design. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, dangerous undetected, fail high, fail low, etc.) in the safety models. The format for the FMEDA is an extension of the standard FMEA format from MIL STD 1629A, Failure Modes and Effects Analysis.

4.2.2 Failure rates

The failure rate data used by *exida* in this FMEDA is from the Electrical and Mechanical Component Reliability Handbooks [N2] and [N3] which was derived using over 100 billion unit operational hours of field failure data from multiple sources and failure data from various databases. The rates were chosen in a way that is appropriate for safety integrity level verification calculations. The rates were chosen to match *exida* Profile 2, see Appendix C. The *exida* profile chosen was judged to be the best fit for the product and application information submitted by Yokogawa Electric Corporation. It is expected that the actual number of field failures due to random events will be less than the number predicted by these failure rates.

For hardware assessment according to IEC 61508 only random equipment failures are of interest. It is assumed that the equipment has been properly selected for the application and is adequately commissioned such that early life failures (infant mortality) may be excluded from the analysis.

Failures caused by external events should be considered as random failures. Examples of such failures are loss of power, physical abuse, or problems due to intermittent instrument air quality.

The assumption is also made that the equipment is maintained per the requirements of IEC 61508 or IEC 61511 and therefore a preventative maintenance program is in place to replace equipment before the end of its “useful life”. Corrosion, erosion, coil burnout etc. are considered age related wear out failures, provided that materials and technologies applied are indeed suitable for the application, in all modes of operation.

The user of these numbers is responsible for determining their applicability to any particular environment. *exida* Environmental Profiles listing expected stress levels can be found in Appendix C. Some industrial plant sites have high levels of stress. Under those conditions the failure rate data is adjusted to a higher value to account for the specific conditions of the plant.

Accurate plant specific data may be used for this purpose. If a user has data collected from a good proof test reporting system such as *exida* SILStat™ that indicates higher failure rates, the higher numbers shall be used.

4.3 Assumptions

The following assumptions have been made during the Failure Modes, Effects, and Diagnostic Analysis of the AXG/W Magnetic Flowmeter.

- Only a single component failure will fail the entire AXG/W Magnetic Flowmeter.
- Failure rates are constant; wear-out mechanisms are not included.
- Propagation of failures is not relevant.
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- Failures caused by operational errors are site specific and therefore are not included.
- The stress levels are average for an industrial environment and can be compared to the *exida* Profile 3 with temperature limits within the manufacturer's rating. Other environmental characteristics are assumed to be within manufacturer's rating.
- Practical fault insertion tests can demonstrate the correctness of the failure effects assumed during the FMEDA and the diagnostic coverage provided by the automatic diagnostics.
- The HART or BRAIN protocol is only used for setup, calibration, and diagnostics purposes, not for safety critical operation.
- The application program in the logic solver is constructed in such a way that Fail High and Fail Low failures are detected regardless of the effect, safe or dangerous, on the safety function.
- Materials are compatible with process conditions.
- The device is installed per manufacturer's instructions.
- External power supply failure rates are not included.
- Worst-case internal fault detection time is less than 1 hour.

4.4 Results

Using reliability data extracted from the *exida* Electrical and Mechanical Component Reliability Handbook the following failure rates resulted from the AXG/W Magnetic Flowmeter FMEDA.

Table 1 Failure rates AXG/W Magnetic Flowmeter

Failure Category	Failure Rate (FIT)			
	non-IS version		IS version	
Fail Safe Undetected		256		223
Fail Dangerous Detected		2461		2248
Fail Detected (detected by internal diagnostics)	2003		1977	
Fail High (detected by logic solver)	14		0	
Fail Low (detected by logic solver)	444		271	
Fail Dangerous Undetected		315		325
No Effect		748		502
Annunciation Undetected		6		6

These failure rates are valid for the useful lifetime of the product, see Appendix A.

According to IEC 61508 the architectural constraints of an element must be determined. This can be done by following the 1_H approach according to 7.4.4.2 of IEC 61508 or the 2_H approach according to 7.4.4.3 of IEC 61508.

The 1_H approach involves calculating the Safe Failure Fraction for the entire element.

The 2_H approach involves assessment of the reliability data for the entire element according to 7.4.4.3.3 of IEC 61508.

According to 3.6.15 of IEC 61508-4, the Safe Failure Fraction is the property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures. This ratio is represented by the following equation:

$SFF = (\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg})/(\Sigma\lambda_S \text{ avg} + \Sigma\lambda_{DD} \text{ avg} + \Sigma\lambda_{DU} \text{ avg})$

When the failure rates are based on constant failure rates, as in this analysis, the equation can be simplified to:

$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$

Where:

$\lambda_S =$ Fail Safe

$\lambda_{DD} =$ Fail Dangerous Detected

$\lambda_{DU} =$ Fail Dangerous Undetected

Table 2 lists the failure rates for the AXG/W Magnetic Flowmeter according to IEC 61508.

Table 2 Failure rates according to IEC 61508 in FIT

Device	λ_{SD}	λ_{SU}[3]	λ_{DD}	λ_{DU}	SFF[4]
AXG/W Magnetic Flowmeter non-IS version	0	256	2461	315	89.6%
AXG/W Magnetic Flowmeter IS version	0	223	2248	325	88.4%

[3] It is important to realize that the No Effect failures are no longer included in the Safe Undetected failure category according to IEC 61508, ed2, 2010.
[4] Safe Failure Fraction if needed, is to be calculated on an element level

5 Using the FMEDA Results

The following section(s) describe how to apply the results of the FMEDA.

5.1 PFD_{avg} calculation AXW/G Magnetic Flowmeter

Using the failure rate data displayed in section 0, and the failure rate data for the associated element devices, an average the Probability of Failure on Demand (PFD_{avg}) calculation can be performed for the element.

Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

Probability of Failure on Demand (PFD_{avg}) calculation is the responsibility of the owner/operator of a process and is often delegated to the SIF designer. Product manufacturers can only provide a PFD_{avg} by making many assumptions about the application and operational policies of a site. Therefore use of these numbers requires complete knowledge of the assumptions and a match with the actual application and site.

Probability of Failure on Demand (PFD_{avg}) calculation is best accomplished with *exida's* exSILentia tool. See Appendix D for a complete description of how to determine the Safety Integrity Level for an element. The mission time used for the calculation depends on the PFD_{avg} target and the useful life of the product. The failure rates and the proof test coverage for the element are required to perform the PFD_{avg} calculation. The proof test coverage for the suggested proof test is listed in Appendix B.

6 Terms and Definitions

Automatic Diagnostics	Tests performed online internally by the device or, if specified, externally by another device without manual intervention.
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3).
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
PFD_{avg}	Average Probability of Failure on Demand
Random Capability	The SIL limit imposed by the Architectural Constraints for each element.
SFF	Safe Failure Fraction, summarizes the fraction of failures which lead to a safe state plus the fraction of failures which will be detected by automatic diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
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).
Type A element	"Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	"Complex" element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

7 Status of the Document

7.1 Liability

exida prepares FMEDA reports based on methods advocated in International standards. Failure rates are obtained from a collection of industrial databases. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

Due to future potential changes in the standards, product design changes, best available information and best practices, the current FMEDA results presented in this report may not be fully consistent with results that would be presented for the identical model number product at some future time. As a leader in the functional safety market place, *exida* is actively involved in evolving best practices prior to official release of updated standards so that our reports effectively anticipate any known changes. In addition, most changes are anticipated to be incremental in nature and results reported within the previous three year period should be sufficient for current usage without significant question.

Most products also tend to undergo incremental changes over time. If an *exida* FMEDA has not been updated within the last three years, contact the product vendor to verify the current validity of the results.

7.2 Releases

Version History:	V1, R5:	Update after FIT, November 7, 2016
	V1, R4:	First Release, August 3, 2016
	V1, R3:	Update after customer review, August 2, 2016
	V1, R2:	Second Draft for Customer Review, August 2, 2016
	V1, R1:	Draft for Customer Review, July 31, 2016
	V0, R1:	Draft for Internal Review, 25 July, 2016
Author(s):	Kiyoshi Takai	
Review:	V0, R1:	Rudolf Chalupa (*exida*), July 26, 2016
	V1, R2:	Kaoru Sonoda, August 2, 2016
	V1, R3:	Kaoru Sonoda, August 2, 2016
Release Status:	Second Draft for Customer Review	

7.3 Future Enhancements

At request of client.

7.4 Release signatures

Kiyoshi Takai

Kiyoshi Takai, Safety Engineer

Rudolf P. Chalupa

Rudolf Chalupa, CFSE, Senior Safety Engineer

Kaoru Sonoda, Principle Engineer

Appendix A Lifetime of Critical Components

According to section 7.4.9.5 of IEC 61508-2, a useful lifetime, based on experience, should be assumed.

Although a constant failure rate is assumed by the probabilistic estimation method (see section 4.2.2) this only applies provided that the useful lifetime[5] of components is not exceeded. Beyond their useful lifetime the result of the probabilistic calculation method is therefore meaningless, as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the subsystem itself and its operating conditions.

This assumption of a constant failure rate is based on the bathtub curve. Therefore, it is obvious that the PFD_{avg} calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

Table 3 shows which components are contributing to the dangerous undetected failure rate and therefore to the PFD_{avg} calculation and what their estimated useful lifetime is.

Table 3 Useful lifetime of components contributing to dangerous undetected failure rate

Component	Useful Life
Capacitor (electrolytic) - Tantalum electrolytic, solid electrolyte	Approx. 500,000 hours
Capacitor (electrolytic) - Aluminum electrolytic, non-solid electrolyte	Approx. 90,000 hours

It is the responsibility of the end user to maintain and operate the AXG/W Magnetic Flowmeter per manufacturer's instructions. Furthermore regular inspection should show that all components are clean and free from damage.

When plant experience indicates a shorter useful lifetime than indicated in this appendix, the number based on plant experience should be used.

[5] Useful lifetime is a reliability engineering term that describes the operational time interval where the failure rate of a device is relatively constant. It is not a term which covers product obsolescence, warranty, or other commercial issues.

Appendix B Proof Tests to Reveal Dangerous Undetected Faults

According to section 7.4.5.2 f) of IEC 61508-2 proof tests shall be undertaken to reveal dangerous faults which are undetected by automatic diagnostic tests. This means that it is necessary to specify how dangerous undetected faults which have been noted during the Failure Modes, Effects, and Diagnostic Analysis can be detected during proof testing.

B.1 Suggested Proof Test

The suggested proof test described in Table 4 will detect 94% of possible DU failures in the AXG/W Magnetic Flowmeter non-IS version. The suggested proof test in combination with automatic diagnostics will detect 99% of possible DU failures in the AXG/W Magnetic Flowmeter non-IS version. The numbers for the AXG/W Magnetic Flowmeter IS version are 93% for the proof test and 99% for the proof test in combination with automatic diagnostics.

The suggested proof test consists of a setting the output to the min and max, and a calibration check, see Table 4.

Table 4 Suggested Proof Test

Step	Action
1.	Bypass the safety function and take appropriate action to avoid a false trip
2.	Use HART communications to retrieve any diagnostics and take appropriate action.
3.	Send a HART or BRAIN command to the transmitter to go to the high alarm current output and verify that the analog current reaches that value[6].
4.	Send a HART or BRAIN command to the transmitter to go to the low alarm current output and verify that the analog current reaches that value[7].
5.	Perform a two-point calibration[8] of the transmitter over the full working range.
6.	Check current output when there is no flow in the meter[9].
7.	Check current output when there is a typical flow in the meter.
8.	Remove the bypass and otherwise restore normal operation

[6] This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance. This also tests for other possible failures.
[7] This tests for possible quiescent current related failures.
[8] If the two-point calibration is performed with electrical instrumentation, this step of the proof test will not detect any failures of the coils and electrodes.
[9] Checking the current output at no flow and a typical flow rate allows some coil and electrode failure detection.

Appendix C *exida* Environmental Profiles

Table 5 *exida* Environmental Profiles

exida **Profile**	**1**	**2**	**3**	**4**	**5**	**6**
Description (Electrical)	Cabinet mounted/ Climate Controlled	Low Power Field Mounted no self-heating	General Field Mounted self-heating	Subsea	Offshore	N/A
Description (Mechanical)	Cabinet mounted/ Climate Controlled	General Field Mounted	General Field Mounted	Subsea	Offshore	Process Wetted
IEC 60654-1 Profile	B2	C3 also applicable for D1	C3 also applicable for D1	N/A	C3 also applicable for D1	N/A
Average Ambient Temperature	30 C	25 C	25 C	5 C	25 C	25 C
Average Internal Temperature	60 C	30 C	45 C	5 C	45 C	Process Fluid Temp.
Daily Temperature Excursion (pk-pk)	5 C	25 C	25 C	0 C	25 C	N/A
Seasonal Temperature Excursion (winter average vs. summer average)	5 C	40 C	40 C	2 C	40 C	N/A
Exposed to Elements / Weather Conditions	No	Yes	Yes	Yes	Yes	Yes
Humidity[10]	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock[11]	10 g	15 g	15 g	15 g	15 g	N/A
Vibration[12]	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion[13]	G2	G3	G3	G3	G3	Compatible Material
Surge[14]						
Line-Line	0.5 kV	0.5 kV	0.5 kV	0.5 kV	0.5 kV	N/A
Line-Ground	1 kV	1 kV	1 kV	1 kV	1 kV	
EMI Susceptibility[15]						
80 MHz to 1.4 GHz	10 V/m	10 V/m	10 V/m	10 V/m	10 V/m	N/A
1.4 GHz to 2.0 GHz	3 V/m	3 V/m	3 V/m	3 V/m	3 V/m	
2.0Ghz to 2.7 GHz	1 V/m	1 V/m	1 V/m	1 V/m	1 V/m	
ESD (Air)[16]	6 kV	6 kV	6 kV	6 kV	6 kV	N/A

[10] Humidity rating per IEC 60068-2-3
[11] Shock rating per IEC 60068-2-27
[12] Vibration rating per IEC 60068-2-6
[13] Chemical Corrosion rating per ISA 71.04
[14] Surge rating per IEC 61000-4-5
[15] EMI Susceptibility rating per IEC 61000-4-3
[16] ESD (Air) rating per IEC 61000-4-2

Appendix D Determining Safety Integrity Level

The information in this appendix is intended to provide the method of determining the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). **The numbers used in the examples are not for the product described in this report.**

Three things must be checked when verifying that a given Safety Instrumented Function (SIF) design meets a Safety Integrity Level (SIL) [N5] and [N7].

These are:

A. Systematic Capability or Prior Use Justification for each device meets the SIL level of the SIF;

B. Architecture Constraints (minimum redundancy requirements) are met; and

C. a PFD_{avg} calculation result is within the range of numbers given for the SIL level.

A. Systematic Capability (SC) is defined in IEC61508:2010. The SC rating is a measure of design quality based upon the methods and techniques used to design and development a product. All devices in a SIF must have a SC rating equal or greater than the SIL level of the SIF. For example, a SIF is designed to meet SIL 3 with three pressure transmitters in a 2oo3 voting scheme. The transmitters have an SC2 rating. The design does not meet SIL 3. Alternatively, IEC 61511 allows the end user to perform a "Prior Use" justification. The end user evaluates the equipment to a given SIL level, documents the evaluation and takes responsibility for the justification.

B. Architecture constraints require certain minimum levels of redundancy. Different tables show different levels of redundancy for each SIL level. A table is chosen and redundancy is incorporated into the design [N8].

C. Probability of Failure on Demand (PFD_{avg}) calculation uses several parameters, many of which are determined by the particular application and the operational policies of each site. Some parameters are product specific and the responsibility of the manufacturer. Those manufacturer specific parameters are given in this third party report.

A Probability of Failure on Demand (PFD_{avg}) calculation must be done based on a number of variables including:

1. Failure rates of each product in the design including failure modes and any diagnostic coverage from automatic diagnostics (an attribute of the product given by this FMEDA report);
2. Redundancy of devices including common cause failures (an attribute of the SIF design);
3. Proof Test Intervals (assignable by end user practices);
4. Mean Time to Restore (an attribute of end user practices);
5. Proof Test Effectiveness; (an attribute of the proof test method used by the end user with an example given by this report);
6. Mission Time (an attribute of end user practices);
7. Proof Testing with process online or shutdown (an attribute of end user practices);
8. Proof Test Duration (an attribute of end user practices); and
9. Operational/Maintenance Capability (an attribute of end user practices).

The product manufacturer is responsible for the first variable. Most manufacturers use the *exida* FMEDA technique which is based on over 100 billion hours of field failure data in the process industries to predict these failure rates as seen in this report. A system designer chooses the second variable. All other variables are the responsibility of the end user site. The exSILentia® SILVer™ software considers all these variables and provides an effective means to calculate PFD_{avg} for any given set of variables.

Simplified equations often account for only for first three variables. The equations published in IEC 61508-6, Annex B.3.2 [N1] cover only the first four variables. IEC61508-6 is only an informative portion of the standard and as such gives only concepts, examples and guidance based on the idealistic assumptions stated. These assumptions often result in optimistic PFD_{avg} calculations and have indicated SIL levels higher than reality. Therefore idealistic equations should not be used for actual SIF design verification.

All the variables listed above are important. As an example consider a high level protection SIF. The proposed design has a single SIL 3 certified level transmitter, a SIL 3 certified safety logic solver, and a single remote actuated valve consisting of a certified solenoid valve, certified scotch yoke actuator and a certified ball valve. Note that the numbers chosen are only an example and not the product described in this report.

Using exSILentia with the following variables selected to represent results from simplified equations:

- Mission Time = 5 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 100% (ideal and unrealistic but commonly assumed)
- Proof Test done with process offline

This results in a PFD_{avg} of 6.82E-03 which meets SIL 2 with a risk reduction factor of 147. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 5.55E-04, Logic Solver PFD_{avg} = 9.55E-06, and Final Element PFD_{avg} = 6.26E-03. See Figure 2.

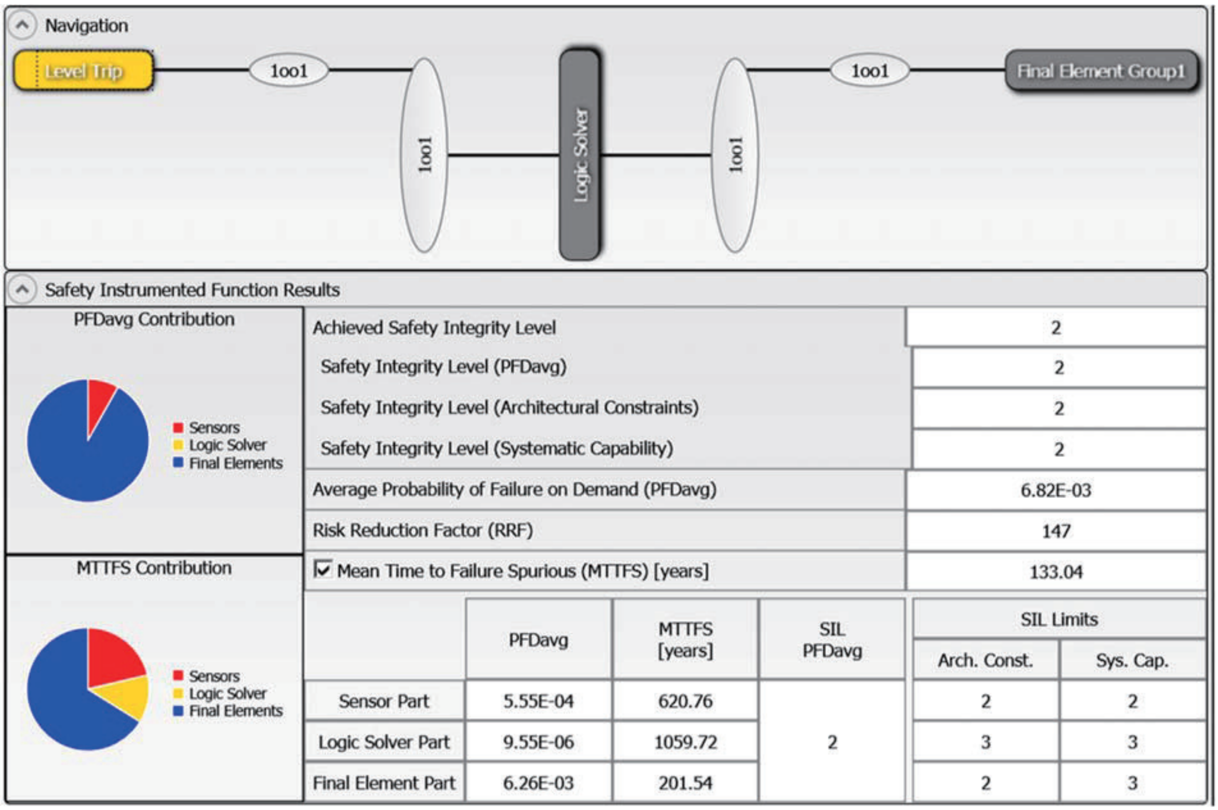


Figure 2: exSILentia results for idealistic variables.

If the Proof Test Interval for the sensor and final element is increased in one year increments, the results are shown in Figure 3.

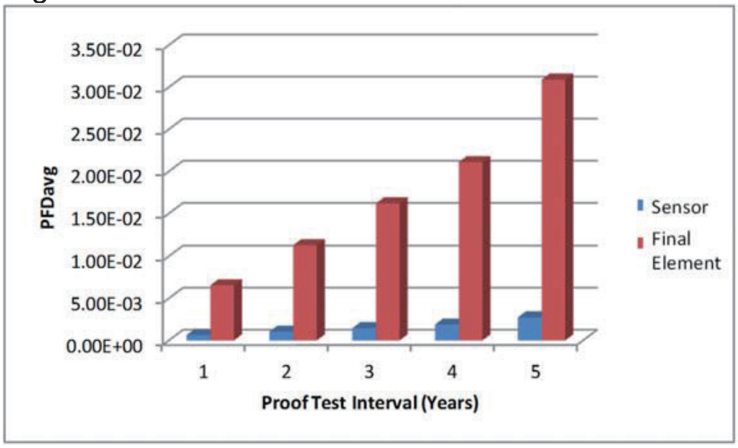
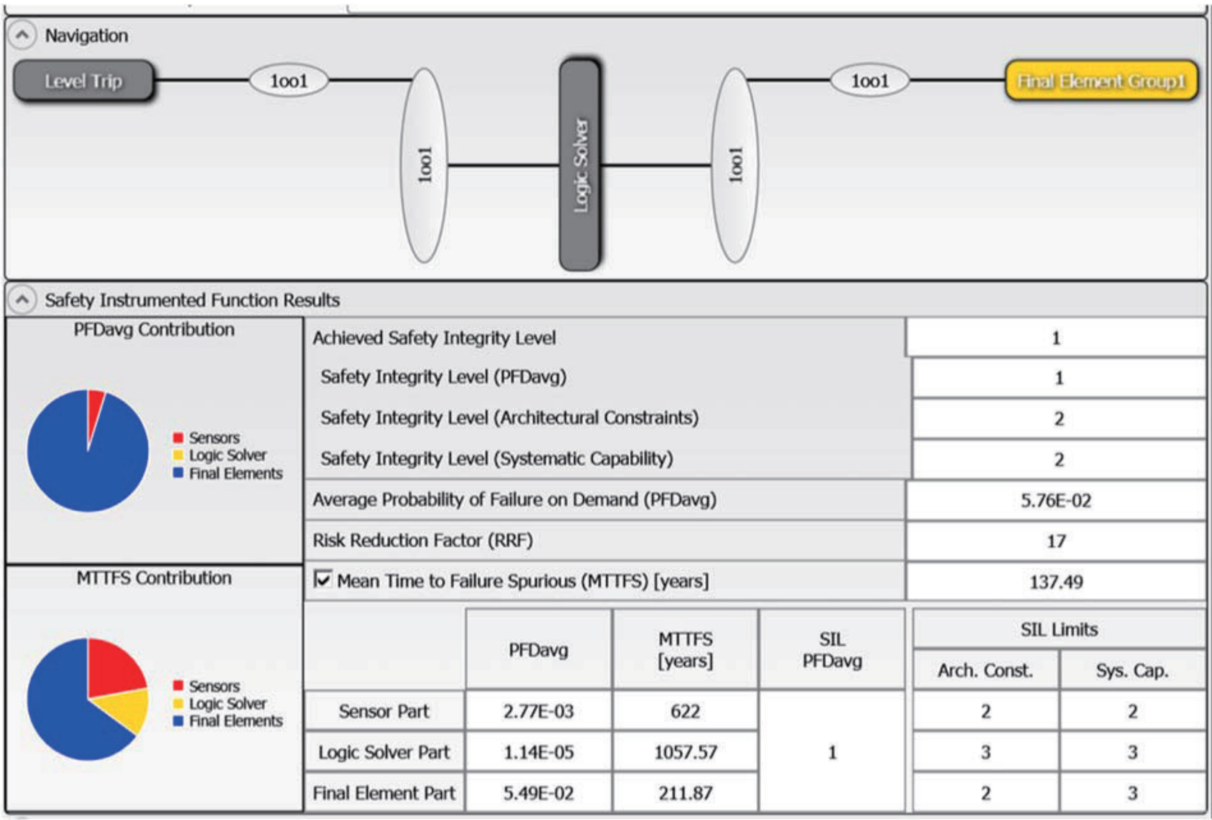


Figure 3 PFD_{avg} versus Proof Test Interval.

If a set of realistic variables for the same SIF are entered into the exSILentia software including:

- Mission Time = 25 years
- Proof Test Interval = 1 year for the sensor and final element, 5 years for the logic solver
- Proof Test Coverage = 90% for the sensor and 70% for the final element
- Proof Test Duration = 2 hours with process online.
- MTTR = 48 hours
- Maintenance Capability = Medium for sensor and final element, Good for logic solver

with all other variables remaining the same, the PFD_{avg} for the SIF equals 5.76E-02 which barely meets SIL 1 with a risk reduction factor 17. The subsystem PFD_{avg} contributions are Sensor PFD_{avg} = 2.77E-03, Logic Solver PFD_{avg} = 1.14E-05, and Final Element PFD_{avg} = 5.49E-02 (Figure 4).



Achieved Safety Integrity Level	1
Safety Integrity Level (PFDavg)	1
Safety Integrity Level (Architectural Constraints)	2
Safety Integrity Level (Systematic Capability)	2
Average Probability of Failure on Demand (PFDavg)	5.76E-02
Risk Reduction Factor (RRF)	17
Mean Time to Failure Spurious (MTTFS) [years]	137.49

	PFDavg	MTTFS [years]	SIL PFDavg	SIL Limits	
				Arch. Const.	Sys. Cap.
Sensor Part	2.77E-03	622	1	2	2
Logic Solver Part	1.14E-05	1057.57		3	3
Final Element Part	5.49E-02	211.87		2	3

Figure 4: exSILentia results with realistic variables

It is clear that PFD_{avg} results can change an entire SIL level or more when all critical variables are not used.

説明書　改訂情報

資料名称　：ADMAG TI シリーズ AXG/AXW 電磁流量計 安全マニュアル

資料番号　：IM 01E21A21-02JA

版 No.	改訂日付	ページ	訂正・変更箇所
初版	2017 年 6 月	ー	新規発行