User's
Manual

ADMAG TI 系列
AXG/AXW 电磁流量计
安全手册

IM 01E21A21-02ZH

YOKOGAWA

IM 01E21A21-02ZH
第 1 版

ADMAG TI 系列
AXG/AXW 电磁流量计
安全手册

IM 01E21A21-02ZH　第1版

目录

1. 简介

本手册介绍了ADMAG TI (Total Insight)系列AXG和AXW电磁流量计安全仪表系统安装的基本说明。本手册中的说明适用于中国市场。

对于本手册中未涵盖的内容，请参阅表1.1中列出的使用说明书和一般规格书。这些文档可从横河电机的网站上下载。为确保正确使用本仪表，请仔细通读这些手册，在使用前充分了解本仪表的操作方法。有关型号和规格的确认方法，请参阅表1.1中列出的一般规格书。

横河电机的网址：http://www.yokogawa.com/cn/

表1.1 手册与一般规格书列表

型号	文档标题	文档编号
AXG□□□ AXW□□□ AXG4A AXW4A AX01C	ADMAG TI系列 AXG/AXW电磁流量计 用前必读	IM 01E21A21-01ZH
	ADMAG TI系列 AXG/AXW电磁流量计 安全手册	IM 01E21A21-02ZH (本手册)
AXG□□□ AXG4A AX01C	ADMAG TI系列 AXG电磁流量计 安装手册	IM 01E22A01-01ZH
	ADMAG TI系列 AXG电磁流量计 维护手册	IM 01E22A01-02ZH
	ADMAG TI系列 AXG电磁流量计 BRAIN通信型	IM 01E22A02-01ZH
	ADMAG TI系列 AXG电磁流量计 HART通信型	IM 01E22A02-02ZH
	ADMAG TI系列 AXG电磁流量计 一般规格书	GS 01E22A01-01ZH
AXW□□□ AXW4A AX01C	ADMAG TI系列 AXW电磁流量计 [口径：25～400 mm (1～16 in.)] 安装手册	IM 01E24A01-01ZH
	ADMAG TI系列 AXW电磁流量计 [口径：25～400 mm (1～16 in.)] 维护手册	IM 01E24A01-02ZH
	ADMAG TI系列 AXW电磁流量计 BRAIN通信型	IM 01E24A02-01ZH
	ADMAG TI系列 AXW电磁流量计 HART通信型	IM 01E24A02-02ZH
	ADMAG TI系列 AXG和AXW电磁流量计 中国(NEPSI)防爆型	IM 01E21A03-05ZH
	ADMAG TI系列 AXW电磁流量计 [口径：25～400 mm (1～16 in.)] 一般规格书	GS 01E24A01-01ZH

注释

本手册在描述AXG□□□等型号名称时，“□□□”表示任意下述内容之一。

AXG□□□：

002、005、010、015、025、032、040、050、065、080、100、125、150、200、250、300、350、400

AXW□□□：

025、032、040、050、065、080、100、125、150、200、250、300、350、400

重要

SIL1的应用范围如下。

- AXG一体型
- AXG分体型传感器与AXG4A分体型变送器配套使用
- AXW一体型
- AXW分体型传感器与AXW4A分体型变送器配套使用

如果分体型传感器和AXFA11G分体型变送器配套使用，则该组合超出SIL1的范围。

■ 仪表保护、安全和改装的注意事项

本手册和仪表使用以下安全标志。

警告

“警告”标识表示危险。用于引起用户对操作步骤、操作条件等的注意，如果未能正确操作或遵守，可能会造成人员伤亡。

注意

“注意”标识表示危险。用于引起用户对操作步骤、操作条件等的注意，如果未能正确操作或遵守，可能会造成仪表局部或整体的损坏或报废。

重要

“重要”标识用于引起用户注意，以免造成仪表损坏或系统故障。

注释

“注释”标识表示仪表操作和功能相关的重要信息。

仪表和手册中使用以下符号，提示相应的安全注意事项：

接地保护端子

功能接地端子(该端子不能用作接地保护端子。)

交流电

直流电

注意
该标志表示操作人员必须遵循使用说明书中的指示，以免造成人身伤亡或设备损坏。

- 为了保护并安全使用本仪表及其系统，无论何时使用本仪表时，请务必遵循表1.1中所列使用说明书的安全说明和注意事项。特别需要注意的是，如果操作仪表的方式违反了这些指示，则仪表的安全功能可能会被损害或削弱。在这种情况下，横河电机不保证仪表的质量、性能、功能和安全。
- 请勿改装本仪表。
- 本仪表应按照地方和国家的法律/法规进行处理。

■ 关于本使用说明书

- 本手册应提供给最终用户。
- 本手册的内容如有变更，恕不另行通知。
- 保留所有权利。未经横河电机书面许可，不得以任何形式复制本手册的任何内容。
- 横河电机不对本手册作任何形式的保证，其中包括但不限于本手册的出售以及用于其它特殊目的。
- 如果发现任何问题或错误，或者发现手册中缺失任何信息，请与最近的横河电机销售部门联系。
- 本手册中的规格仅限于指定型号的标准型，不包含客户特注定制的仪表。
- 请注意，如果延迟修订不会在功能或性能方面给用户造成影响，本仪表的规格、结构或部件发生变更时可能不会立即反映到本手册中。
- 为确保正确使用，开始操作前请仔细阅读本手册及表1.1中列出的相关用户手册。有关规格请参阅表1.1中列出的一般规格书。

■ 商标

- 本手册中出现的横河电机的产品名称或品牌名称均为横河电机的商标或注册商标。
- 本手册中的公司名称及产品名称均为其所有者的商标或注册商标。
- 本手册中的商标或注册商标未使用™或®标志。

■ 产品的安全使用

为了保护并安全使用本仪表及其系统，无论何时使用本仪表，请务必遵循表1.1中所列使用说明书的安全说明和注意事项。特别需要注意的是，如果操作仪表的方式违反了这些说明和注意事项，则仪表的安全功能可能会被损害或削弱。在这种情况下，横河电机将不对由于使用或不能使用仪表造成的间接或后果性损失负责。

2. 安全仪表系统的安装

警告

本内容引自本仪表的exida.com安全说明书，为了安全，必须严格遵照该说明内容进行操作。在安全仪表系统(SIS)应用中使用本仪表时，请严格遵照本章所述的指导说明和注意事项，以保证流量计满足安全等级要求。

2.1 适用范围和用途

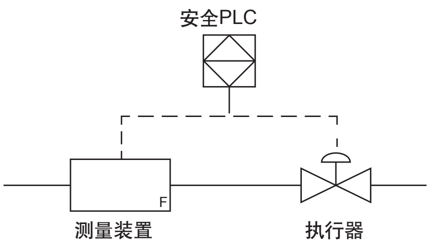
本章简要说明为满足SIS应用程序所设计的安全等级，用户在安装和操作仪表过程中应承担的责任。

本章说明的内容有：验证测试、变送器的维修与更换、可靠性数据、使用寿命、环保和应用限制以及参数设定。

2.2 在SIS应用程序中使用本仪表

2.2.1 安全功能

本仪表在SIS应用中作为低需求模式B型使用。



本仪表将流速、体积流量、质量流量和流体噪声(仅AXG)转换为电流，并在“I/O 1”端子输出“Analog Output 1”作为安全功能。其他功能(显示等)不在其范围内。本仪表作为SIS使用时，使用该“Analog Output 1”连接安全PLC。

开始使用本仪表作为SIS之前，需要设置足够的参数。详情请参阅2.2.4节和2.2.5节。

2.2.2 安全精度

本仪表的指定安全精度为2%。这意味着如果发生2%或以上的误差，将在设备故障率中列出该内部组件故障。

2.2.3 诊断响应时间

本仪表的诊断测试周期最大为8秒。本仪表将安全PLC作为其主机，在1秒内通过在“Analog Output 1”输出断偶信号(安全状况)通知故障。有关故障对策的详细信息，请参阅表1.1中列出的可应用通信型使用说明书的第4章。

2.2.4 设置

通过BRAIN或HART配置工具设置量程和单位。设置后，确保设置正确。本仪表的标定必须在参数设定之后执行。有关参数设置的详细信息，请参阅表1.1中列出的可应用通信型使用说明书的第4章和第5章。

2.2.5 需要的参数设置

以下表2.2.1或表2.2.2中显示的参数需要进行设置，以便保持本仪表的安全级别。

表2.2.1 通过硬件设置

项目	说明
断偶开关	检测到内部故障时，选择“High”或“Low”输出。
写保护开关	通过设置开关为“ON”，启用写保护功能。

表2.2.2 通过参数设置

项目	说明
BRAIN: G04:AO1 ALM OUT HART菜单路径： Device root menu►Detailed setup► Analog output/input►Analog output 1► AO1 alarm out	当检测到本仪表发生报警时，该功能通过“Analog Output 1”输出信号。 当本仪表作为SIS使用时，设置“Analog Output 1”为“> 21.6 mA”或“< 2.4 mA”。
BRAIN: H50:SET SIL HART菜单路径： Device root menu►Detailed setup► AUX calculation►Set SIL	当本仪表作为SIS使用时，设置该参数为“Yes”。在这种情况下，当检测到报警时，其“Analog Output 1”固定为“> 21.6 mA”或“< 2.4 mA”。当检测到本仪表发生报警时，通过“Analog Output 1”可以无故障地执行断偶功能。
BRAIN: H30:DENSITY SEL HART菜单路径： Device root menu►Detailed setup► Process variables►Density► Density value select	当“Analog Output 1”用于质量流量测量时，设置该参数为“Fixed value”。

2.2.6 验证测试

验证测试是一种周期测试，用于验证“安全仪表功能”是否无故障运行。

验证测试是强制执行的测试，可以检测仪表诊断未检出的任何故障，这些故障可能会影响“安全仪表功能”(SIF)的动作。

验证测试频率(或验证测试间隔)应该根据本仪表应用的SIF的可靠性计算确定。实际的验证测试必须更加频繁或与运算中指定的频率一致，以保证要求的SIF安全完整性。

验证测试需要执行以下表2.2.3中显示的动作，并且其结果也需要存成文档。保存的文档应作为工程安全管理系统的一部分。检测出来的故障应向横河电机报告。

仪表验证测试的执行人员应接受过SIS操作培训，其中包括：旁路程序、本仪表的维护和变更流程的公司管理。

表2.2.3 验证测试

测试方法	需要的工具	预期结果	备注
用于“模拟输出”的回路测试 1.对安全PLC设置旁路或采取其他适当操作，以避免误跳闸。 2.通过BRAIN或HART通信协议制造一个报警条件：“Analog Output 1”处“> 21.6 mA”，验证模拟输出是否达到预期水平。 3.通过BRAIN或HART通信协议制造一个报警条件：“Analog Output 1”处“< 2.4 mA”，验证模拟输出是否达到预期水平。 4.确认状态既非错误也非警告。 5.通过最大和最小流量量程，验证模拟输出的合理性检查。 6.通过零点流量，验证模拟输出的合理性检查。 7.通过典型流量，验证模拟输出的合理性检查。 8.使回路恢复到全面运行状态。 9.从旁路条件或防止安全PLC功能异常的状态返回一般操作。	BRAIN： BRAIN配置工具 HART： HART配置工具	验证测试范围； 不带本安电路 = 94% 带本安电路 = 93% 验证测试范围； (诊断功能间带组合使用) 不带本安电路 = 99% 带本安电路 = 99%	需要监测输出，以保证本仪表传送正确信号。

发生报警的示例；

(BRAIN的“66:Dens cfg ERR”发生时(HART的“Density configuration error”)；

(1) 通过BRAIN或HART通讯工具设置参数，以便通过在电流值上限侧制造一个向外扩展的条件，在“Analog Output 1”生成报警。

BRAIN: G04: AO1 ALM OUT

HART菜单路径：

Device root menu►Detailed setup►Analog output/input►Analog output 1►AO1 alarm out

为上限侧生成报警时选择“> 21.6 mA”

(a) BRAIN: H30: DENSITY SEL

HART菜单路径：

Device root menu►Detailed setup►Process variables►Density►Density value select

选择菜单上方的“Fixed value”。

(b) BRAIN: H32: FIXED DENS

HART菜单路径：

Device root menu►Detailed setup►Process variables►Density►Density fixed value

在菜单上方设置参数为“0.0”。

(c) BRAIN: C30: PV FLOW SEL

HART菜单路径：

Device root menu►Detailed setup►Process variables►PV flow select

选择菜单上方的“Mass”。

在“Analog Output 1”设置的报警生成，并出现在上述工作的结果中。

(2) 通过BRAIN或HART通讯工具设置参数，以便通过在电流值下限侧制造一个向外扩展的条件，在“Analog Output 1”生成报警。
BRAIN: G04: AO1 ALM OUT
HART菜单路径：
Device root menu►Detailed setup►Analog output/input►Analog output 1►AO1 alarm out

为下限侧生成报警时选择“< 2.4 mA”。

(a) BRAIN: H30: DENSITY SEL
HART菜单路径：
Device root menu►Detailed setup►Process variables►Density►Density value select
选择菜单上方的“Fixed value”。

(b) BRAIN: H32: FIXED DENS
HART菜单路径：
Device root menu►Detailed setup►Process variables►Density►Density fixed value
在菜单上方设置参数为“0.0”。

(c) BRAIN: C30: PV FLOW SEL
HART菜单路径：
Device root menu►Detailed setup►Process variables►PV flow select
选择菜单上方的“Mass”。

在“Analog Output 1”设置的报警生成，并出现在上述工作的结果中。

2.2.7 维修和更换

如果仪表需要在工艺在线状态下进行维修，则安装时需要设置旁路线路。用户需要建立足够的旁路程序。
需要维修时，请联系横河电机检测本仪表的故障。
更换本仪表时，需要执行本手册中说明的步骤。
维修或更换本仪表的执行人员应具有相应的技术水平。

2.2.8 启动时间

本仪表的缓冲时间常数设置为0.1秒时，在3秒内生成1个有效信号。

2.2.9 固件更新

用户无需执行任何固件升级相关操作。
如果需要升级，必须由横河电机执行。

2.2.10 可靠性数据

横河电机可提供详细的故障模式、影响和诊断分析(FMEDA)报表，包括整体故障率和故障模式。
用于单工(1oo1)配置时，根据整个SIF的PFDavg计算结果，本仪表调整为符合SIL1。
根据整个SIF的PFDavg计算结果，本仪表的研发过程符合SIL3，允许冗余使用符合该安全完整性等级(SIF)的变送器。
在冗余配置中使用本仪表的变送器时，建议使用5%的共因系数(β系数)。如果工厂运营商为了防止共因故障，制定共因故障培训及更多详细维护步骤，则可使用2%的β系数。

2.2.11 寿命限制

本仪表的预计寿命为10年。在FMEDA报告中列出的可靠性数据只在此期间有效。超过此期间后，本仪表的故障率可能会有所增加。基于FMEDA报告中仪表寿命超过10年的数据，可靠性计算结果可能会过于乐观，即无法达到计算得出的安全完整性等级(SIL)。

2.2.12 环保限制

本仪表的环保限制在表1.1中列出的一般规格书中说明。

2.2.13 应用限制

本仪表的应用限制在本手册中说明。如果在应用限制以外的情况下使用，2.2.10节中所列的可靠性数据将变为无效。

2.3 定义和缩写

2.3.1 定义

● 安全性

定义	说明
安全性	免于不可接受的伤害风险。
功能安全	为了达到或维持系统控制下的设备/机械/工厂/仪器的规定安全状态，系统执行必要操作的能力。
基本安全	设备的设计和生产必须能够避免触电和其它危险对人造成伤害的风险，且能够避免造成火灾和爆炸。此种防护功能必须在常规操作的所有条件和单一故障条件下都有效。

● 验证

定义	说明
验证	证实在生命周期的各个阶段，各阶段最终的输出满足输入时规定的目标和要求。验证通常通过分析和/或测试执行。
验证	证明从各个方面来看，安全相关系统或安全相关系统和外部风险降低设施的组合满足安全要求规范。验证通常通过测试执行。
安全评估	为了对安全相关系统达到的安全性做出有据判断而进行的调查。

关于安全技术和措施中使用的其它术语定义及安全相关系统的描述，请参阅IEC 61508-4。

2.3.2 缩写

定义	说明
FMEDA (Failure Mode, Effects and Diagnostic Analysis)	故障模式、影响和诊断分析
SIF (Safety Instrumented Function)	安全仪表功能
SIL (Safety Integrity Level)	安全完整性等级
SIS (Safety Instrumented System)	安全仪表系统
SLC (Safety Lifecycle)	安全生命周期

横河電機株式会社
Yokogawa Electric Corporation

YOKOGAWA

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

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.

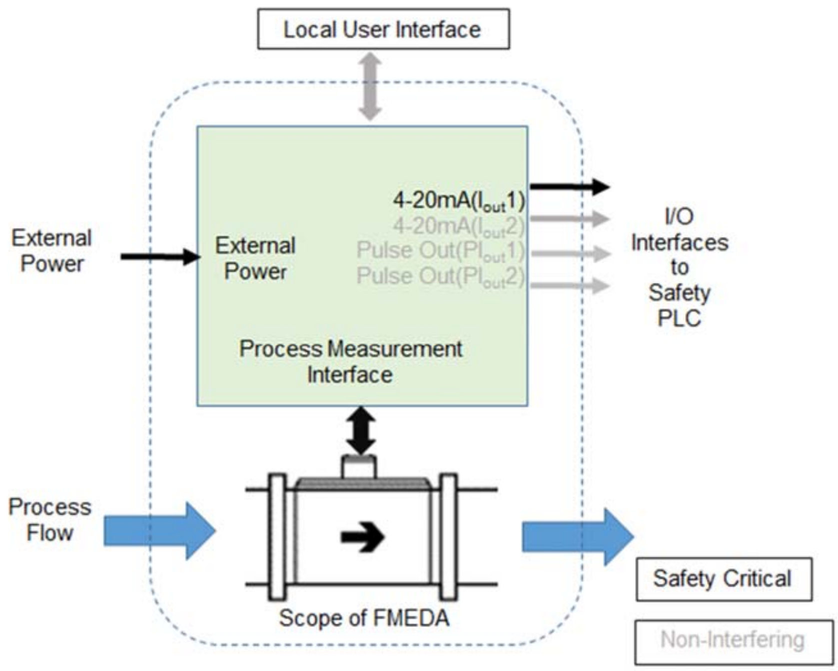


Figure 1 AXG/W Magnetic Flowmeter, Parts included in the FMEDA

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.

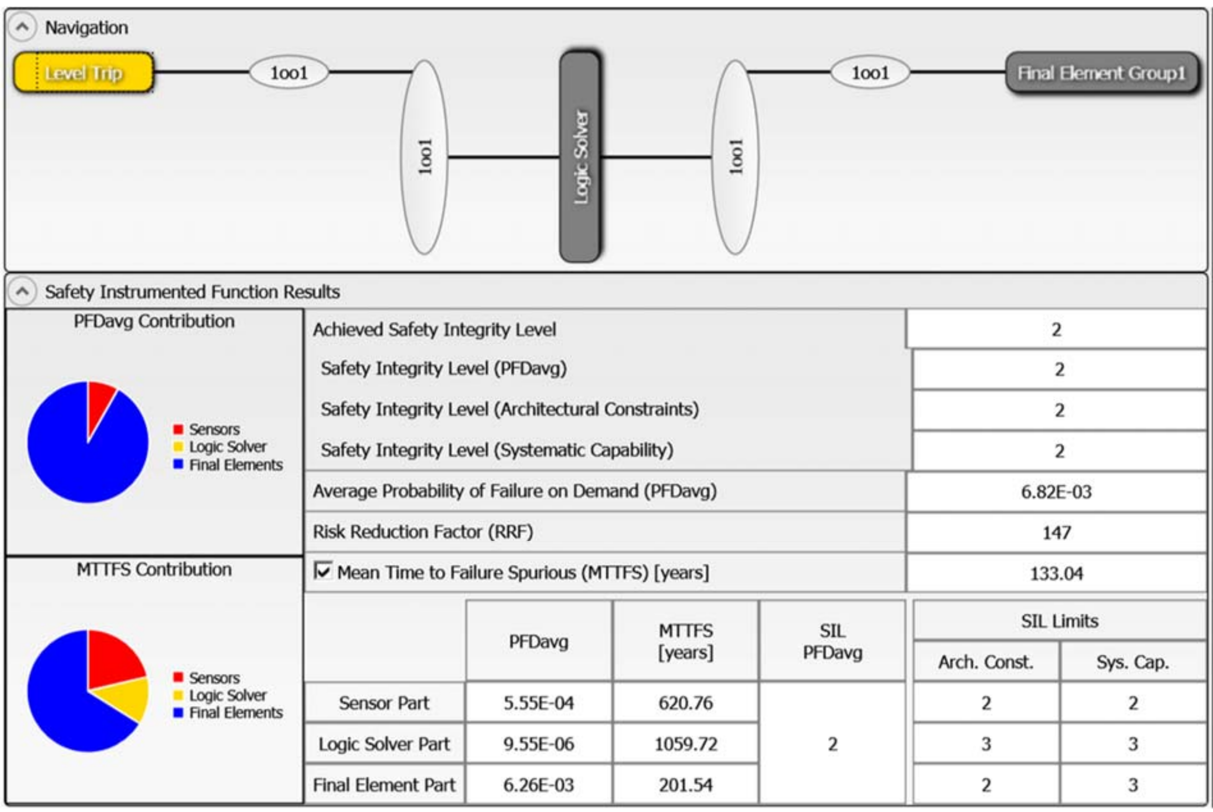


Figure 2: exSILentia results for idealistic variables.

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

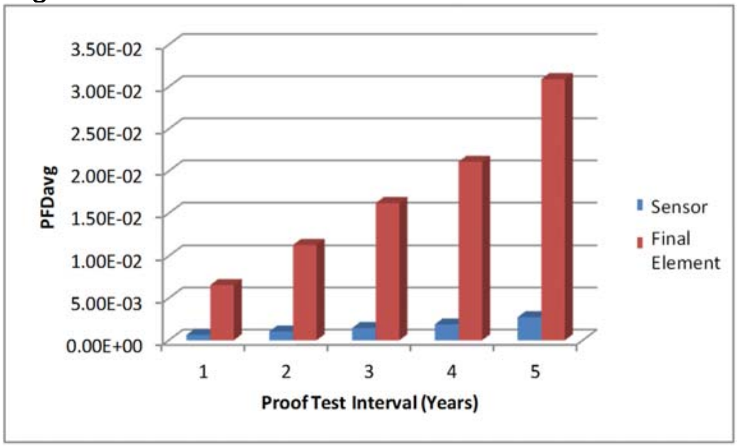


Figure 3 PFD_{avg} versus Proof Test Interval.

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).

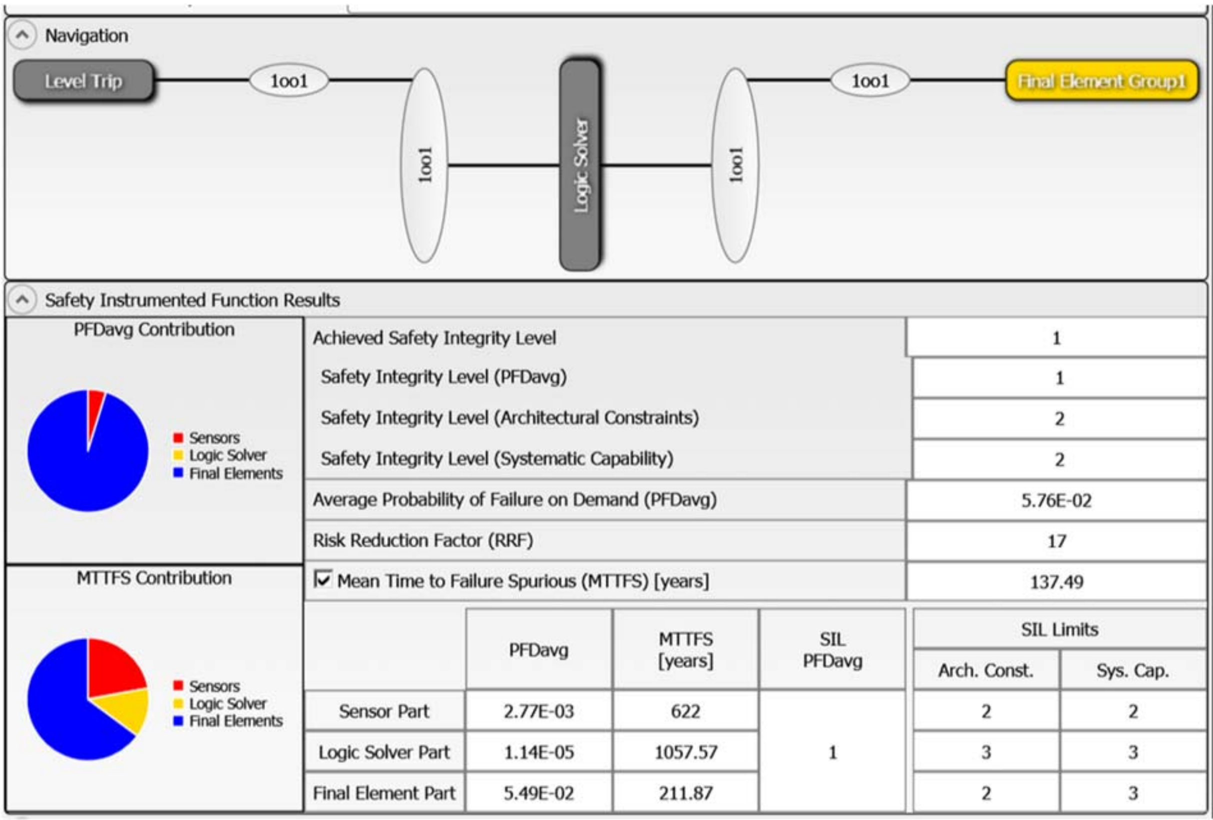


Figure 4: exSILentia results with realistic variables

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

修订记录

- 手册标题： ADMAG TI系列 AXG/AXW 电磁流量计 安全手册
- 手册编号： IM 01E21A21-02ZH

版本	日期	页码	修订项目
第1版	2018年8月	—	新发行