
**User's
Manual**

**ADMAG TI Series
AXG/AXW Magnetic Flowmeter
Safety Manual**



IM 01E21A21-02EN

ADMAG TI Series AXG/AXW Magnetic Flowmeter Safety Manual

IM 01E21A21-02EN 1st Edition

Contents

1.	Introduction.....	1
2.	Safety Instrumented Systems Installation	4
2.1	Scope and Purpose	4
2.2	Using this instrument for an SIS Application	4
2.2.1	Safety Function	4
2.2.2	Safety Accuracy	4
2.2.3	Diagnostic Response Time	4
2.2.4	Setup	5
2.2.5	Required Parameter Setting	5
2.2.6	Proof Test	5
2.2.7	Repair and Replacement	7
2.2.8	Startup Time	7
2.2.9	Firmware Update	7
2.2.10	Reliability Data	7
2.2.11	Lifetime Limits	8
2.2.12	Environmental Limits	8
2.2.13	Application Limits	8
2.3	Definitions and Abbreviations	8
2.3.1	Definitions	8
2.3.2	Abbreviations	8

SIL Declaration of Conformity

Failure Mode, Effects and Diagnostic Analysis

Revision Information

1. Introduction

This manual provides the basic guidelines for Safety Instrumented Systems Installation of ADMAG TI (Total Insight) Series AXG and AXW magnetic flowmeters.

For the items which are not covered in this manual, read the applicable user's manuals and general specifications as listed in Table 1.1. These documents can be downloaded from the website of YOKOGAWA. To ensure correct use of the instrument, read these manuals thoroughly and fully understand how to operate the instrument before maintaining it. For method of checking the model and specifications, read the applicable general specifications in Table 1.1.

Website address: <http://www.yokogawa.com/fld/doc/>
 These manuals can be downloaded from the website of YOKOGAWA or purchased from the YOKOGAWA representatives.

Table 1.1 Manual and General Specifications List

Model	Document Title	Document No.
AXG□□□ AXW□□□□ AXG4A AXW4A AX01C	ADMAG TI Series AXG/AXW Magnetic Flowmeter Read Me First	IM 01E21A21-01Z1
	ADMAG TI Series AXG/AXW Magnetic Flowmeter Safely Manual	IM 01E21A21-02EN (this manual)
	ADMAG TI Series AXG Magnetic Flowmeter Installation Manual	IM 01E22A01-01EN
	ADMAG TI Series AXG Magnetic Flowmeter Maintenance Manual	IM 01E22A01-02EN
AXG□□□□ AXG4A AX01C	ADMAG TI Series AXG Magnetic Flowmeter BRAIN Communication Type	IM 01E22A02-01EN
	ADMAG TI Series AXG Magnetic Flowmeter HART Communication Type	IM 01E22A02-02EN
	ADMAG TI Series AXG Magnetic Flowmeter General Specifications	GS 01E22A01-01EN

Model	Document Title	Document No.
	ADMAG TI Series AXW Magnetic Flowmeter [Size: 25 to 400 mm (1 to 16 in.)] Installation Manual	IM 01E24A01-01EN
	ADMAG TI Series AXW Magnetic Flowmeter [Size: 500 to 1800 mm (20 to 72 in.)] Installation Manual	IM 01E25A01-01EN
	ADMAG TI Series AXW Magnetic Flowmeter [Size: 25 to 1800 mm (1 to 72 in.)] Maintenance Manual	IM 01E24A01-02EN
AXW□□□□ AXW□□□□G AXW□□□□W AXW4A AX01C	ADMAG TI Series AXW Magnetic Flowmeter BRAIN Communication Type	IM 01E24A02-01EN
	ADMAG TI Series AXW Magnetic Flowmeter HART Communication Type	IM 01E24A02-02EN
	ADMAG TI Series AXW Magnetic Flowmeter [Size: 25 to 400 mm (1 to 16 in.)] General Specifications	GS 01E24A01-01EN
	ADMAG TI Series AXW Magnetic Flowmeter [Size: 500 to 1800 mm (20 to 72 in.)] General Specifications	GS 01E25D11-01EN



NOTE

When describing the model name like AXG□□□□ in this manual, “□□□□” means any of the following.

For AXG□□□□:

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

For AXW□□□□:

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

For AXW□□□□G or AXW□□□□W:

500, 600, 700, 800, 900, 10L



IMPORTANT

The applicable scope of SIL 1 is as follows.

- AXG Integral Type
- Combination of AXG Remote Sensor and AXG4A Remote Transmitter
- AXW Integral Type
- Combination of AXW Remote Sensor and AXW4A Remote Transmitter

In case of combination of Remote Sensor and AXFA11G Remote Transmitter, the combination is outside the scope of SIL 1.

■ **Precautions Related to the Protection, Safety, and Alteration of the Instrument**

The following safety symbol marks are used in this manual and instrument.



WARNING

A WARNING sign denotes a hazard. It calls attention to procedure, practice, condition or the like, which, if not correctly performed or adhered to, could result in injury or death of personnel.



CAUTION

A CAUTION sign denotes a hazard. It calls attention to procedure, practice, condition or the like, which, if not correctly performed or adhered to, could result in damage to or destruction of part or the entire instrument.



IMPORTANT

An IMPORTANT sign denotes that attention is required to avoid damage to the instrument or system failure.



NOTE

A NOTE sign denotes information necessary for essential understanding of operation and features.

The following symbols are used in the Instrument and the manual to indicate the accompanying safety precautions:



Protective grounding terminal



Functional grounding terminal (This terminal should not be used as a protective grounding terminal.)



Alternating current



Direct current



Caution

This symbol indicates that the operator must refer to an explanation in the user's manual in order to avoid the risk of injury or death of personnel or damage to the instrument.

- For the protection and safe use of the instrument and the system in which this instrument is incorporated, be sure to follow the instructions and precautions on safety that is stated in user's manual as listed in Table 1.1 whenever you handle the instrument. Take special note that if you handle the instrument in a manner that violated these instructions, the protection functionality of the instrument may be damaged or impaired. In such cases, YOKOGAWA does not guarantee the quality, performance, function, and safety of instrument.
- Do not modify this instrument.
- The instrument should be disposed of in accordance with local and national legislation/regulations.

■ **Regarding This User's Manual**

- This manual should be provided to the end user.
- The contents of this manual are subject to change without prior notice.
- All rights reserved. No part of this manual may be reproduced in any form without YOKOGAWA's written permission.
- YOKOGAWA makes no warranty of any kind with regard to this manual, including, but not limited to, implied warranty of merchantability and fitness for a particular purpose.
- If any question arises or errors are found, or if any information is missing from this manual, inform the nearest YOKOGAWA sales office.
- The specifications covered by this manual are limited to those for the standard type under the specified model number break-down and do not cover custom-made instruments.
- Note that changes in the specifications, construction, or component parts of the instrument may not immediately be reflected in this manual at the time of change, provided that postponement of revisions will not cause difficulty to the user from a functional or performance standpoint.
- To ensure correct use, read this manual and the applicable user's manuals as listed in Table 1.1 thoroughly before starting operation. Read the general specifications as listed in Table 1.1 for its specification.

■ Trademark

- All the brands or names of Yokogawa Electric's products used in this manual are either trademarks or registered trademarks of Yokogawa Electric Corporation.
- All other company and product names mentioned in this manual are trade names, trademarks or registered trademarks of their respective companies.
- In this manual, trademarks or registered trademarks are not marked with TM or [®].

■ For Safe Use of Product

For the protection and safe use of the instrument and the system in which this instrument is incorporated, be sure to follow the instructions and precautions on safety that is stated in user's manual as listed in Table 1.1 whenever you handle the instrument. Take special note that if you handle the instrument in a manner that violated these instructions, the protection functionality of the instrument may be damaged or impaired. In such cases, YOKOGAWA shall not be liable for any indirect or consequential loss incurred by either using or not being able to use the Instrument.

2. Safety Instrumented Systems Installation



WARNING

The contents are cited from exida.com safety manual on this instrument specifically observed for its safety purpose. When using this instrument for Safety Instrumented System (SIS) application, the instructions and procedures on this chapter must be strictly followed in order to preserve this instrument for that safety level.

2.1 Scope and Purpose

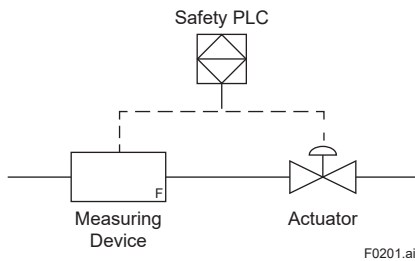
This chapter provides an overview of the user responsibilities for installation and operation of this instrument in order to maintain the designed safety level for SIS applications.

This chapter is described proof test, repair and replacement of the transmitter, reliability data, lifetime, environmental and application limits, and parameter settings.

2.2 Using this instrument for an SIS Application

2.2.1 Safety Function

This instrument is used as a Type B of Low demand mode in the SIS application.



This instrument converts Flow velocity, Volume flow, Mass flow, and Flow noise (for AXG only) to current. And it outputs “Analog Output 1” at “I/O 1” terminal as its safety functions. Other functions (display, etc...) are out of its scope. Use this “Analog Output 1” to connect the safety PLC when this instrument is used as a SIS.

It is necessary to set adequate parameters before starting to use this instrument as a SIS. Refer to Subsection 2.2.4 and Subsection 2.2.5 for details.

2.2.2 Safety Accuracy

This instrument has a specified safety accuracy of 2%. This means that the internal component failure are listed in the device failure rate if they will cause an error of 2% or larger.

2.2.3 Diagnostic Response Time

The period of the diagnostic test on this instrument is 8 seconds as its maximum. This instrument notifies the failure to the safety PLC as its host within 1 second by outputting the burnout (safety condition) at “Analog Output 1”. For countermeasure of its failure, read Chapter 4 in the user’s manual of applicable communication type as listed in Table 1.1.

2.2.4 Setup

Set the ranges and units via the BRAIN or HART configuration tool. After configuration, make sure that they are set correctly. The calibration of this instrument must be carried out after parameters are set. For its parameter settings, read Chapter 4 and Chapter 5 in the user’s manual of applicable communication type as listed in Table 1.1.

2.2.5 Required Parameter Setting

The following parameters as shown in Table 2.2.1 or Table 2.2.2 are required to be set in order to preserve this instrument for that safety level.

Table 2.2.1 Setup by Hardware

Item	Explanation
Burnout switch	Select “High” or “Low” for the output when an internal failure was detected.
Write protect switch	Enable the write protect function by setting its switch “ON”.

Table 2.2.2 Setup by Parameters

Item	Explanation
BRAIN: G04:AO1 ALM OUT HART Menu Path: Device root menu▶Detailed setup▶ Analog output/input▶Analog output 1▶ AO1 alarm out	This function is to output the signal through the “Analog Output 1” when this instrument is detected its alarm. Set the “Analog Output 1” as “> 21.6 mA” or “< 2.4 mA” when this instrument is used for SIS.
BRAIN: H50:SET SIL HART Menu Path: Device root menu▶Detailed setup▶ AUX calculation▶Set SIL	Set this parameter as “Yes” when this instrument is used for SIS. In this case, its “Analog Output 1” is fixed as “> 21.6 mA” or “< 2.4 mA” when its alarm was detected. It is able to carry out the burnout function via “Analog Output 1” without fail when this instrument is detected its alarm.
BRAIN: H30:DENSITY SEL HART Menu Path: Device root menu▶Detailed setup▶ Process variables▶Density▶ Density value select	Set this parameter as “Fixed value” when the “Analog Output 1” is used for mass flow measurement.

2.2.6 Proof Test

A proof test is a periodic test to verify that the Safety Instrumented Function work without fails.

It is mandatory to have a proof test in order to detect any failure which is not detected by the diagnostic of the instrument, which prevents any action of the Safety Instrumented Function (SIF) from its intention.

The frequency of the proof tests (or the proof test interval) is to be determined in the reliability calculations for the SIFs for which this instrument is applied. The actual proof tests must be carried out “more frequently” or “as frequently as specified” in the calculation in order to preserve required safety integrity of the SIF.

The following action as shown in Table 2.2.3 is required in the proof test, and its results are also required to be documented. And this documentation should be a part of the plant safety management system. Failures that are detected should be reported to YOKOGAWA.

The personnel carrying out the proof test of instruments should be trained in SIS operations including bypass procedures, maintenance of this instrument, and company management of change procedures.

Table 2.2.3 Proof Test

Testing method	Tool required	Expected outcome	Remarks
Loop test for “Analog output” 1. Bypass the safety PLC or take other appropriate action to avoid a false trip. 2. Verify the analog output whether it reaches the expected level by making a condition of an alarm as “> 21.6 mA” at “Analog Output 1” through BRAIN or HART communication protocol. 3. Verify the analog output whether it reaches the expected level by making a condition of an alarm as “< 2.4 mA” at “Analog Output 1” through BRAIN or HART communication protocol. 4. Confirm the condition neither error nor warning. 5. Verify their reasonability check of the analog output through both its maximum flow range and its minimum flow range. 6. Verify their reasonability check of the analog output through its flow zero. 7. Verify their reasonability check of the analog output through its typical flow rate. 8. Return the loop to the full operation. 9. Return to the normal operation from a condition of bypass or prevention of malfunction to the safety PLC.	For BRAIN: BRAIN configuration tool For HART: HART configuration tool	Proof Test Coverage; Without Intrinsic safety circuitry = 94% With Intrinsic safety circuitry = 93% Proof Test Coverage; (with a combination use between diagnostic function) Without Intrinsic safety circuitry = 99% With Intrinsic safety circuitry = 99%	The output needs to be monitored to assure that this instrument communicates the correct signal

Example of generating an alarm;

(In case of “66:Dens cfg ERR” for BRAIN (“Density configuration error” for HART));

- (1) Set parameters through BRAIN or HART communication protocol in order to generate an alarm at “Analog Output 1” by making a condition of scale out at its high limit side of current value.

BRAIN: G04: AO1 ALM OUT

HART Menu Path:

Device root menu ▶ Detailed setup ▶ Analog output/input ▶ Analog output 1 ▶ AO1 alarm out
 Select “> 21.6 mA” when generating an alarm for its high limit side.

- (a) BRAIN: H30: DENSITY SEL

HART Menu Path:

Device root menu ▶ Detailed setup ▶ Process variables ▶ Density ▶ Density value select
 Select “Fixed value” above menu.

- (b) BRAIN: H32: FIXED DENS

HART Menu Path:

Device root menu ▶ Detailed setup ▶ Process variables ▶ Density ▶ Density fixed value
 Set the parameter as “0.0” above menu.

- (c) BRAIN: C30: PV FLOW SEL

HART Menu Path:

Device root menu ▶ Detailed setup ▶ Process variables ▶ PV flow select
 Select “Mass” above menu.

An alarm, which was set at “Analog Output 1”, is generated and appeared at the result of above work.

- (2) Set parameters through BRAIN or HART communication protocol in order to generate an alarm at “Analog Output 1” by making a condition of scale out at its low limit side of current value.

BRAIN: G04: AO1 ALM OUT

HART Menu Path:

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

Select “< 2.4 mA” when generating an alarm for its low limit side.

- (a) BRAIN: H30: DENSITY SEL

HART Menu Path:

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

Select “Fixed value” above menu.

- (b) BRAIN: H32: FIXED DENS

HART Menu Path:

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

Set the parameter as “0.0” above menu.

- (c) BRAIN: C30: PV FLOW SEL

HART Menu Path:

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

Select “Mass” above menu.

An alarm, which was set at “Analog Output 1”, is generated and appeared at the result of above work.

2.2.7 Repair and Replacement

If the repair work of this instrument is required in spite of being online of the process, it should be installed by making the bypass line. The user has to establish its adequate bypass procedures.

Contact YOKOGAWA for the detected failure on this instrument when it happened.

It is required the procedure described in this manual when this instrument is replaced.

The personnel carrying out the repair or replacement work for this instrument should have a sufficient skill level.

2.2.8 Startup Time

This instrument generates a valid signal within 3 seconds when its damping time constant is set as 0.1 seconds.

2.2.9 Firmware Update

The user will not be required to carry out any firmware updates.

When its updates work is required, it must be carried out at YOKOGAWA.

2.2.10 Reliability Data

A detailed Failure Mode, Effects, and Diagnostics Analysis (FMEDA) report is available from YOKOGAWA with all failure rates and failure modes.

This instrument is adapted up to SIL1 for use in a simplex (1oo1) configuration, depending on the PFDavg calculation of the entire SIF.

The development process of this instrument is adapted up to SIL3, allowing redundant use of this transmitter up to this Safety Integrity Level (SIL), depending the PFDavg calculation of the entire SIF.

When using the transmitter of this flowmeter in a redundant configuration, the use of a common cause factor (β -factor) of 5% is suggested. If the owner-operator of the plant would institute common cause failure training and more detailed maintenance procedures for avoiding common cause failure, the β -factor of 2% would be applicable.

2.2.11 Lifetime Limits

The expected lifetime of this instrument is 10 years. The reliability data listed the FMEDA report is only valid for this period. The failure rates of this instrument may increase sometime after this period. Reliability calculations based on the data listed in the FMEDA report for its lifetimes beyond 10 years may yield results that are too optimistic, i.e. the calculated SIL will not be achieved.

2.2.12 Environmental Limits

The environmental limits on this instrument are specified in the general specifications as listed in Table 1.1.

2.2.13 Application Limits

The application limits on this instrument are specified in this manual. If it is used outside of the application limits, the reliability data listed in Subsection 2.2.10 becomes invalid.

2.3 Definitions and Abbreviations

2.3.1 Definitions

• Safety

Definition	Contents
Safety	Freedom from unacceptable risk of harm.
Functional Safety	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment/machinery/plant/apparatus under control of the system.
Basic Safety	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault condition.

• Verification

Definition	Contents
Verification	The demonstration for each phase of the life-cycle that the (output) deliverables of the phase meet the objectives and requirements specified by the inputs to the phase. The verification is usually executed by analysis and/or testing.
Validation	The demonstration that the safety-related system(s) or the combination of safety-related system(s) and external risk reduction facilities meet, in all respects, the Safety Requirements Specification. The validation is usually executed by testing.
Safety Assessment	The investigation to arrive at a judgment based on evidence of the safety achieved by safety-related systems.

Further definitions of terms used for safety techniques and measures and the description of safety-related systems are given in IEC 61508-4.

2.3.2 Abbreviations

Definition	Contents
FMEDA	Failure Mode, Effects and Diagnostic Analysis
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SLC	Safety Lifecycle

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 1H)
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.

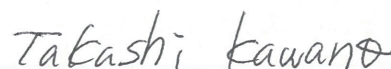
Random Capability:

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



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

The document was prepared using best effort. The authors make no warranty of any kind and shall not be liable in any event for incidental or consequential damages in connection with the application of the document.

© All rights reserved.



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 B¹ 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	<i>exida</i>	5
2.2	Roles of the parties involved	5
2.3	Standards and literature used	5
2.4	<i>exida</i> tools used	6
2.5	Reference documents.....	6
2.5.1	Documentation provided by Yokogawa Electric Corporation	6
2.5.2	Documentation generated by <i>exida</i>	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	<i>exida</i> 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	<i>exida</i> LLC, Electrical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-04-0
[N3]	Mechanical Component Reliability Handbook, 3rd Edition, 2012	<i>exida</i> LLC, Electrical & Mechanical Component Reliability Handbook, Third Edition, 2012, ISBN 978-1-934977-05-7
[N4]	Safety Equipment Reliability Handbook, 3rd Edition, 2007	<i>exida</i> 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, 3 rd 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	<i>exida</i> FMEDA Tool
[T2]	V 2.5.1.7	<i>exSILentia</i>

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.

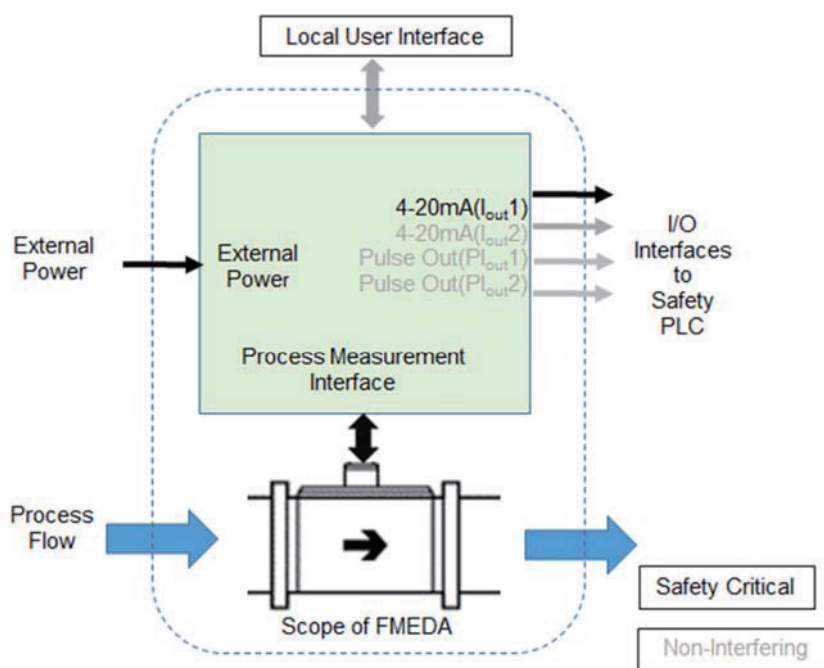


Figure 1 AXG/W Magnetic Flowmeter, Parts included in the FMEDA

The AXG/W Magnetic Flowmeter is classified as a Type B² 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:

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

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

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

Where:

λ_S = Fail Safe

λ_{DD} = Fail Dangerous Detected

λ_{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.
<i>exida</i> 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 (1×10^{-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

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 lifetime⁵ 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

<i>exida</i> 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
Humidity¹⁰	0-95% Non-Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	0-100% Condensing	N/A
Shock¹¹	10 g	15 g	15 g	15 g	15 g	N/A
Vibration¹²	2 g	3 g	3 g	3 g	3 g	N/A
Chemical Corrosion¹³	G2	G3	G3	G3	G3	Compatible Material
Surge¹⁴						
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 Susceptibility¹⁵						
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.

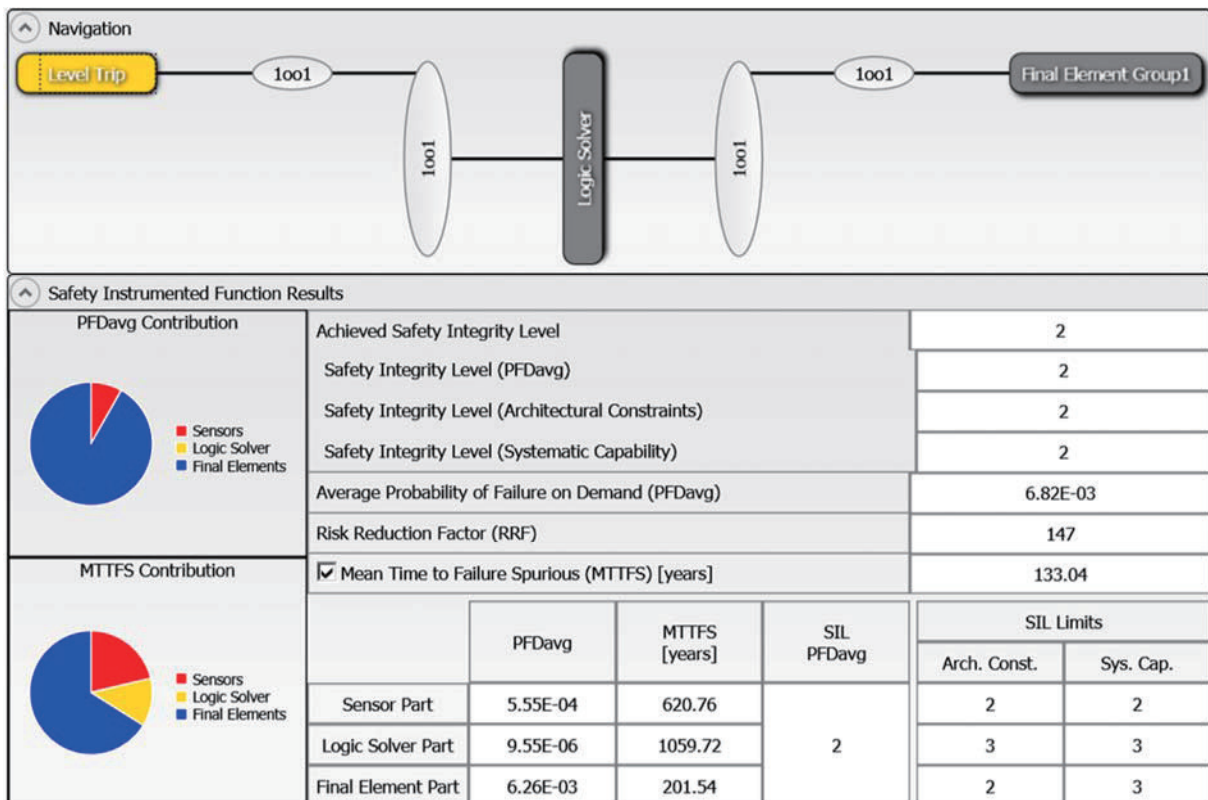


Figure 2: exSILentia results for idealistic variables.

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

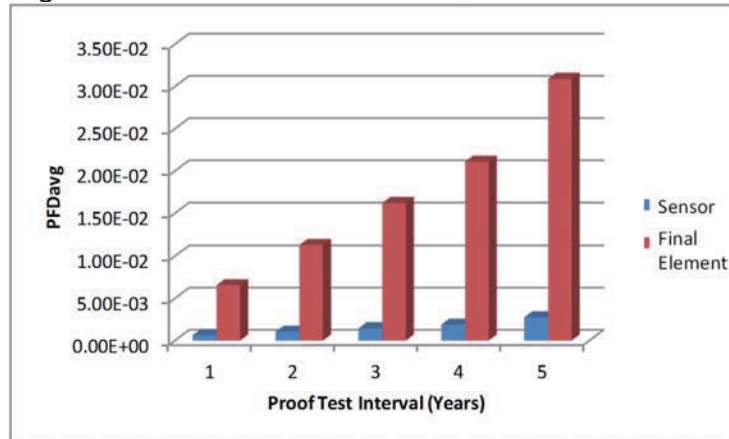


Figure 3 PFD_{avg} versus Proof Test Interval.

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).

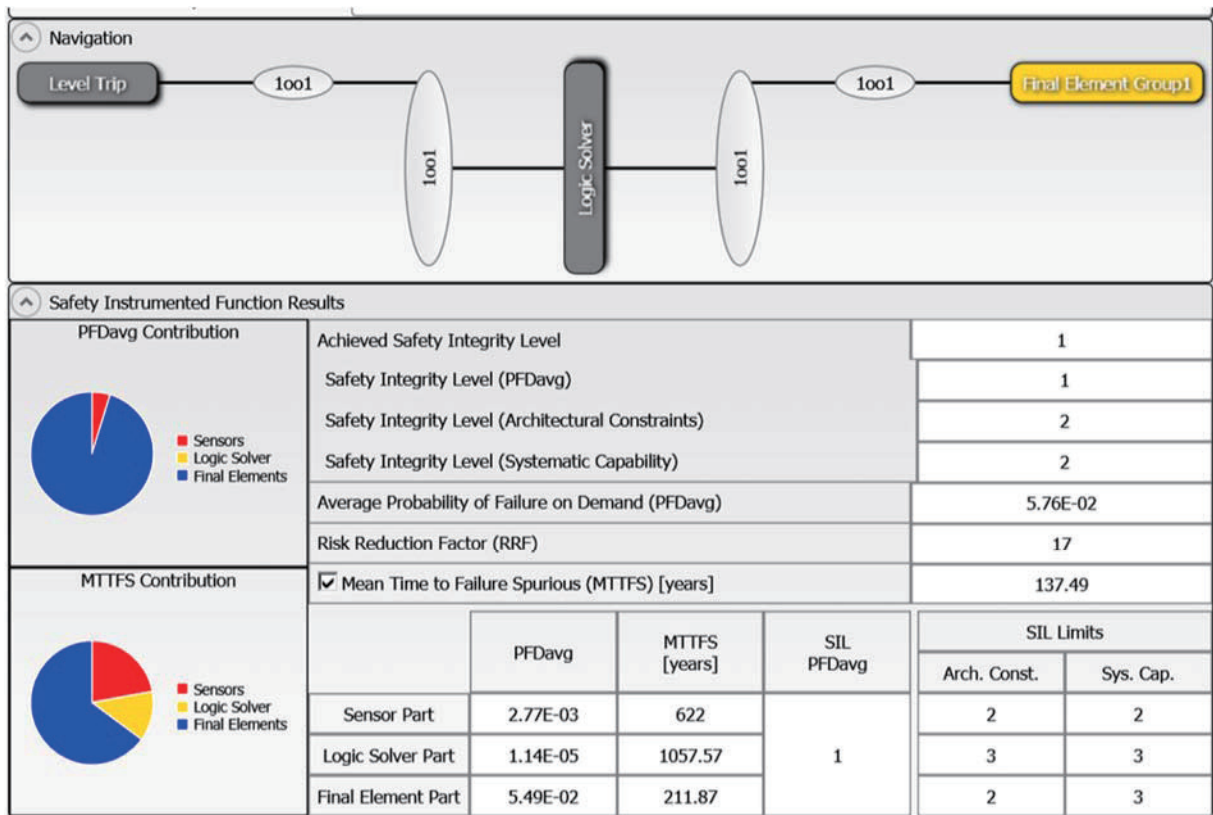


Figure 4: exSILentia results with realistic variables

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

Revision Information

- Title : ADMAG TI Series AXG/AXW Magnetic Flowmeter Safety Manual
- Manual No. : IM 01E21A21-02EN

Edition	Date	Page	Revised Item
1st	June 2017	—	New publication