Results of the IEC 61508 Functional Safety Assessment

Project:

AXR Two-wire Magnetic Flow Meter

Customer:

Yokogawa Electric Corporation
Musashino, Tokyo, Japan

Contract No.:Q24/01-071
Report No.: YEC 20-02-144 R001
Version V3, Revision R1, February 26, 2024
Kaoru Sonoda

Management Summary

The Functional Safety Assessment of the Yokogawa Electric Corporation

AXR Two-wire Magnetic Flow Meter

development project, performed by *exida* consisted of the following activities:

- *exida* assessed the development process used by Yokogawa Electric Corporation through an audit and review of a detailed safety case against the *exida* certification scheme which includes the relevant requirements of IEC 61508. The assessment was executed using subsets of the IEC 61508 requirements tailored to the work scope of the development team.
- *exida* reviewed and assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) of the devices to document the hardware architecture and failure behavior.
- *exida* reviewed field failure data to verify the accuracy of the FMEDA analysis.
- *exida* reviewed the manufacturing quality system in use at Yokogawa Electric Corporation.

The functional safety assessment was performed to the SIL 3 requirements of IEC 61508:2010. A full IEC 61508 Safety Case was created using the *exida* Safety Case tool, which also was used as the primary audit tool. Hardware and software process requirements and all associated documentation were reviewed. Environmental test reports were reviewed. The user documentation and safety manual also were reviewed.

The results of the Functional Safety Assessment can be summarized by the following statements:

The audited development process, as tailored and implemented by the Yokogawa Electric Corporation AXR Two-wire Magnetic Flow Meter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA also shows that the AXR Two-wire Magnetic Flow Meter meets the requirements for architectural constraints of an element such that it can be used to implement a SIL 2 safety function (with HFT = 0) or a SIL 3 safety function (with HFT = 1).

This means that the AXR Two-wire Magnetic Flow Meter is capable for use in SIL 3 applications in Low demand mode when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual and when using the versions specified in section 3.1 of this document.

The manufacturer will be entitled to use the Functional Safety Logo.

Table of Contents

1 Purpose and Scope

This document shall describe the results of the IEC 61508 functional safety assessment of the:

- AXR Two-wire Magnetic Flow Meter

by *exida* according to the accredited *exida* certification scheme which includes the requirements of IEC 61508: 2010.

The purpose of the assessment was to evaluate the compliance of:

- the AXR Two-wire Magnetic Flow Meter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the AXR Two-wire Magnetic Flow Meter development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial IEC 61508-1, -2 and -3 requirements for SIL 3.

and

- the AXR Two-wire Magnetic Flow Meter hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been carried out based on the quality procedures and scope definitions of *exida*.

The results of this assessment provide the safety instrumentation engineer with the required failure data per IEC 61508 / IEC 61511 and confidence that sufficient attention has been given to systematic failures during the development process of the device.

1.1 Tools and Methods used for the assessment

This assessment was carried by using the *exida* Safety Case tool. The Safety Case tool contains the *exida* scheme which includes all the relevant requirements of IEC 61508.

For the fulfillment of the objectives, expectations are defined which builds the acceptance level for the assessment. The expectations are reviewed to verify that each single requirement is covered. Because of this methodology, comparable assessments in multiple projects with different assessors are achieved. The arguments for the positive judgment of the assessor are documented within this tool and summarized within this report.

The assessment was planned by *exida* agreed with Yokogawa Electric Corporation.

All assessment steps were continuously documented by *exida* (see [R1])

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 500 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 a comprehensive failure rate and failure mode database on process equipment based on 250 billion hours of field failure data.

2.2 Roles of the parties involved

Yokogawa Electric Corporation	Manufacturer of the AXR Two-wire Magnetic Flow Meter
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* scheme.

Yokogawa Electric Corporation contracted *exida* with the IEC 61508 Functional Safety Assessment of the above-mentioned devices.

2.3 Standards / Literature used

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

[N1]	IEC 61508 (Parts 1 – 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 2.4.1.1 Documentation provided by Yokogawa Electric Corporation

D01	QP-140-01-10E0.pdf	0	03-Jul-17	Quality Manual
D02	STR-MTW-A063 Rev.4.pdf	4	11-Sep-19	Functional Safety Mgt. Procedure
D03	QP-172-01-7E0.pdf	0	03-Jul-17	Overall Development Process
D04	QP-172-06-2E.pdf	0	27-Dec-10	Configuration Management Process
D05	QP-185-02-5E0.pdf	0	27-Mar-19	Field Failure Reporting Procedure
D06	QP-185-02-5E0.pdf	0	27-Mar-19	Field Return Procedure
D07	GMSe-800.pdf	0	11-Jul-18	Manufacturer Qualification Procedure
D08	QP-140-02-7E0.pdf	0	03-Jul-17	Quality Management System (QMS) Documentation Change Procedure

D09	GMSe-800-01-01.pdf	0	11-Jul-18	Non-Conformance Reporting procedure
D10	QP-185-02-5E0.pdf	0	27-Mar-19	Corrective Action Procedure
D11	QP-185-02-5E0.pdf	0	27-Mar-19	Customer Notification Procedure
D12	01_02_出荷データ、フィールドリターンデータ_rev1.xlsx		03-Mar-20	Shipment Records
D13	01_02_出荷データ、フィールドリターンデータ_rev1.xlsx		03-Mar-20	Field Returns Records
D14	ISO9001_Jan2020.pdf		11-Jan-18	ISO 900x Cert or equivalent
D15	STR-MTW-A0100-Annex1_SRS_R0.pdf	0	03-Feb-17	Safety Requirements Specification
D16	STR-MTW-G0263_SRS_SM レビュー議事録_r2a.pdf	2	21-Feb-17	Safety Requirements Review
D17	STR-MTW-A027_Rev0.pdf	0	06-Feb-07	Software Safety Requirements Specification
D18	FD1_F9840FA_0_21.pdf	0		Schematics / Circuit Diagrams
D19	FD1_F9840HC_0_21.pdf	0		Schematics / Circuit Diagrams
D20	FD1_F9840KC_0_21.pdf	1		Schematics / Circuit Diagrams
D21	FD1_F9840NA_1_21.pdf	1		Schematics / Circuit Diagrams
D22	MTW-A0101_AXR_SIL 定期更新_設計変更履歴の確認資料_R0a.pptx		06-Mar-17	Hardware Change List
D23	FH0_F9840KN_1_21.pdf	0	05-Nov-10	Software Modules Change List
D24	FH0_F9840HN_2_21.pdf	2	17-Jul-12	Software Modules Change List
D25	AXR Fault Injection Test Report.docx		25-Jun-10	Fault Injection Test Plan
D26	STR-MTW-P014.pdf	0	15-May-07	Validation Test Plan
D27	STR-MTW-A065_初期設計審査提案書.pdf	0	04-Mar-10	Validation Test Plan
D28	STR-MTW-A067_初期設計審査_記録書(議事録).pdf	0	12-Mar-10	Validation Test Plan Review Record
D29	STR-MTW-A065_初期設計審査提案書.pdf	0	04-Mar-10	Environmental Test Plan
D30	EMS_Test_Report.pdf	0	06-Feb-09	EMC Test Plan
D31	STR-MTW-A089_中間設計審査提案書.pdf	0	02-Mar-12	Validation Test Results
D32	STR-MTW-A089_中間設計審査提案書.pdf	0	02-Mar-12	Environmental Test Results

D33	STR-MTW-D336EN - AXR Ambient Temperature Test Report - Style 2.pdf	0	10-Mar-10	Environmental Test Results
D34	EMS_Test_Report.pdf	0	06-Feb-07	EMC Test Results
D35	AXR Fault Injection Test Report.docx		25-Jun-10	Fault Injection Test Results
D36	IM01E30D01-01JA_007.pdf	7	17-May-20	Operation / Maintenance Manual
D37	STR-MTW-A0105_資料 1_SafetyManual_IM01E30D01-01EN_008_draft_r1b.pdf	8	16-Mar-20	Safety Manual
D38	STR-MTW-A0105_資料 1_SafetyManual_IM01E30D01-01EN_008_draft_r1b.pdf	1	16-Mar-20	Safety Manual Review
D39	STR-MTW-A0101_AXR_SIL 定期更新_設計変更履歴の確認資料_R0a.pptx	0	06-Mar-17	Engineering Change Documentation
D40	STR-MTW-P042_Rev1.pdf	1	08-Oct-10	List of Diagnostics for FMEDA
D41	PartsList_rev0.xlsx	0	03-Mar-20	Bill of Material
D42	STR-MTW-A064_Rev4.pdf	4	05-Mar-12	Design Verification Sheet

2.4.1.1 Documentation provided by Yokogawa Electric Corporation(Q23-01-136)

D43	STR-MTW-Z0008 添付ファイル：出荷データ_rev2,フィールドリターンデータ_rev2.xlsx		24-Mar-23	Shipment /Field Return Records
D44	0066454-QMS-ENGUS-UKAS.pdf		15-Sep-21	ISO 9001 Certificate
D45	STR-MTW-Z0009_AXR_SIL2 更新_製品担当者の役割と能力.pdf	0	30-Mar-23	Skills Matrix
D46	FE1-F9840FA_20230308.zip		08-Mar-23	Schematics / Circuit Diagrams
D47	STR-MTW-C0039_AXR_A6088HF_代替品評価_r2.pdf	2	20-Mar-23	Validation Test Plan/Results
D48	STR-MTW-A067_初期設計審査_記録書(議事録).pdf	0	12-Mar-10	Validation Test Plan Review Record
D49	IM01E30D01-01EN_010_draft_r0.pdf	10	03-Apr-23	Operation / Maintenance Manual
D50	STR-MTW-B0111_AXR SIL2 更新_Safety Manual 改訂_r0 .pdf	0	03-Apr-23	Safety Manual

D51	STR-MTW-G0284_AXR SIL2 更新_Safety Manual Review_r0.pdf	0	03-Apr-23	Safety Manual Review
D52	STR-MTW-B0110_AXR_A6088HF_改廃対応の影響度分析_r0.pdf	0	20-Mar-23	Impact Analysis Record

2.4.1.2 Documentation provided by Yokogawa Electric Corporation (Q24-01-071)

D53	STR-MTW-Z141196 AXR_出荷データ、フィールドリターンデータ_r0.pdf	0	8-Feb-24	Shipment /Field Return Records
D54	0066454-QMS-ENGUS-UKAS.PDF		12-Dec-23	ISO 9001 Certificate
D55	STR-MTW-Z140817_流量計統括部開発部(AXR)_製品担当者スキルマップ_FY23_Rev.0.pdf	0	5-Feb-24	Skills Matrix
D56	STR-EDC-Y828_流量計部ハードウェア開発課__機能安全規格_異動者教育記録_Rev0.pdf	0	10-Jan-23	IEC 61508 Training Record

2.4.2 Documentation generated by *exida*

[R1]	YEC AXR Safety Case WB-61508 V2 R1.xlsm	Yokogawa AXR Two-wire Magnetic Flow Meter SafetyCaseDB
[R2]	YEC 20-02-144 R001 V3 R1 IEC 61508 Assessment AXR.docx	Yokogawa AXR Two-wire Magnetic Flow Meter Assessment (this report)
[R3]	YOK 10-06-091 V2 R4 FMEDA AXR.pdf	Yokogawa AXR Two-wire Magnetic Flow Meter FMEDA report
[R4]	YEC AXR FFA R1.xlsx	Yokogawa AXR Two-wire Magnetic Flow Meter Field Failure Analysis
[R5]	YEC 23-01-136 AXR R1 FFA.xlsx	Yokogawa AXR Two-wire Magnetic Flow Meter Field Failure Analysis
[R6]	YEC 24-01-071 AXR R1 FFA.xlsx	Yokogawa AXR Two-wire Magnetic Flow Meter Field Failure Analysis

2.5 Assessment Approach

The certification audit was closely driven by requirements of the *exida* scheme which includes subsets filtered from IEC 61508.

The assessment was planned by *exida* and agreed with Yokogawa Electric Corporation.

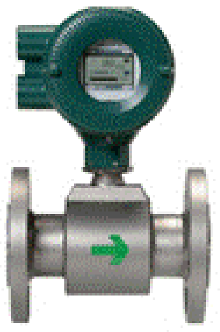
The following IEC 61508 objectives were subject to detailed auditing at Yokogawa Electric Corporation:

- FSM planning, including
    - Safety Life Cycle definition
    - Scope of the FSM activities
    - Documentation
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware design / probabilistic modeling
- Hardware and system related V&V activities including documentation, verification
    - Integration and fault insertion test strategy
- Software and system related V&V activities including documentation, verification
- System Validation including hardware and software validation
- Hardware-related operation, installation and maintenance requirements

The project teams, not individuals were audited.

3 Product Description

The AXR Two-wire Magnetic Flow Meter can be installed in the two-wire system without any AC power source, thus drastically reducing the initial instrumentation cost. The AXR is the world's first two-wire magnetic flow meter which employs the fluid noise free "Dual Frequency Excitation Method," achieving excellent stability for instrumentation. Like the ADMAG TI four-wire magnetic flow meter series, the AXR has user-friendly functions such as a full dot-matrix LCD indicator, electrode adhesion level diagnosis function, and a multi-lingual display. The magnet switches can be used for checking and setting parameters without opening the case cover.



3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of AXR Two-wire Magnetic Flow Meter:

Hardware Version: Rev. 0

Software Version:

SW1: Rev. 2.01

SW2: Rev. 3.1

4 IEC 61508 Functional Safety Assessment Scheme

exida assessed the development process used by Yokogawa Electric Corporation for this development project against the objectives of the *exida* certification scheme. The results of the assessment are documented in [R1].
All objectives have been successfully considered in the Yokogawa Electric Corporation development processes for the development.

exida assessed the set of documents against the functional safety management requirements of IEC 61508. This was done by a pre-review of the completeness of the related requirements and then a spot inspection of certain requirements, before the development audit.
The safety case demonstrated the fulfillment of the functional safety management requirements of IEC 61508-1 to 3.

The detailed development audit (see [R1]) evaluated the compliance of the processes, procedures and techniques, as implemented for the Yokogawa Electric Corporation AXR Two-wire Magnetic Flow Meter, with IEC 61508.

The assessment was executed using the exida certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team.

The result of the assessment shows that the AXR Two-wire Magnetic Flow Meter is capable for use in SIL 3 applications, when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

4.1 Product Modifications

The modification process has been successfully assessed and audited, so Yokogawa Electric Corporation may make modifications to this product as needed.

As part of the *exida* scheme a surveillance audit is conducted prior to renewal of the certificate. The modification documentation listed below is submitted as part of the surveillance audit. *exida* will review the decisions made by the competent person in respect to the modifications made.

- List of all anomalies reported
- List of all modifications completed
- Safety impact analysis which shall indicate with respect to the modification:
  - The initiating problem (e.g. results of root cause analysis)
  - The effect on the product / system
  - The elements/components that are subject to the modification
  - The extent of any re-testing
- List of modified documentation
- Regression test plans

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed the development process used by Yokogawa Electric Corporation during the product development against the objectives of the *exida* certification scheme which includes IEC 61508 parts 1, 2, & 3 [N1]. The development of the AXR Two-wire Magnetic Flow Meter was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documents.

5.1 Lifecycle Activities and Fault Avoidance Measures

Yokogawa Electric Corporation has an IEC 61508 compliant development process as assessed during the IEC 61508 certification. This compliant development process is documented in [D01].

This functional safety assessment evaluated the compliance with IEC 61508 of the processes, procedures and techniques as implemented for the product development. The assessment was executed using the *exida* certification scheme which includes subsets of IEC 61508 requirements tailored to the SIL 3 work scope of the development team. The result of the assessment can be summarized by the following observations:

The audited development process complies with the relevant managerial requirements of IEC 61508 SIL 3.

5.1.1 Functional Safety Management

Objectives

Structure, in a systematic manner, the phases in the overall safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.

- Structure, in a systematic manner, the phases in the E/E/PES safety lifecycle that shall be considered in order to achieve the required functional safety of the E/E/PE safety-related systems.
- Specify the management and technical activities during the overall, E/E/PES and software safety lifecycle phases which are necessary for the achievement of the required functional safety of the E/E/PE safety-related systems.
- Specify the responsibilities of the persons, departments and organizations responsible for each overall, E/E/PES and software safety lifecycle phase or for activities within each phase.
- Specify the necessary information to be documented in order that the management of functional safety, verification and the functional safety assessment activities can be effectively performed.
- Document all information relevant to the functional safety of the E/E/PE safety-related systems throughout the E/E/PES safety lifecycle.
- Document key information relevant to the functional safety of the E/E/PE safety-related systems throughout the overall safety lifecycle.

- Specify the necessary information to be documented in order that all phases of the overall, E/E/PES and software safety lifecycles can be effectively performed.
- Select a suitable set of tools, for the required safety integrity level, over the whole safety lifecycle which assists verification, validation, assessment and modification.

5.1.2 Safety Lifecycle and FSM Planning

Assessment

Functional Safety Lifecycle

The functional safety management of any functional safety product development is governed by the Yokogawa Product Development Process [D28]. For this development project Yokogawa Electric Corporation created a Project Plan [D33] and a Functional Safety Management (FSM) Plan [D02]. The Project Plan and FSM Plan for the AXR were reviewed. This plan includes the following sections: Definition of policy and strategy, Allocation of responsibilities, Configuration Management Requirements, Development Process, Modification Process, Documentation Requirements, Functional Safety Assessment Requirements.

Quality Management

Yokogawa Electric Corporation quality management system has been ISO 9001 certified [D14]. *exida* examined the quality management system and determined that it was adequate to ensure that the functional safety characteristics of the product are maintained through the manufacturing process.

Updated ISO 9001 [D44] certificate was reviewed on Q23/01-136.

Updated ISO 9001 [D54] certificate was reviewed on Q24/01-071.

Conclusion:

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system and new product development processes.

5.1.3 Documentation

Assessment

STR-MTW-A064 design verification sheet [D42] contains the documents which are planned for to the product including version control information. The FSM plans persons relevant for the verification of each document. The configuration management process [D04] describes detail handling of documents.

All safety related documents are required to meet the following requirements:

- Title or name indicating scope of the contents
- Contain as table of contents
- Revision index which lists versions of the document with description of what changed in the version

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system.

5.1.4 Training and competence recording

Assessment

FSM plan[D02] describes the competency requirements on organizational level and on personal level.

Updated Skill Matrix [D45] was assessed on Q23/01-136.

Updated Skill Matrix [D55] and training record [D56] were assessed on Q24/01-071.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system and internal organizational procedures.

5.1.5 Configuration Management

Assessment

The configuration of the product to be certified is documented including all hardware and software versions that make up the product.

Formal configuration control is defined and implemented for Change Authorization, Version Control, and Configuration Identification. A documented procedure exists to ensure that only approved items are delivered to customers. Master copies of the software and all associated documentation are kept during the operational lifetime of the released software.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation organizational release procedures, functional safety management system and new product development processes.

5.2 Safety Requirement Specification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Specify the requirements for each E/E/PE safety-related system, in terms of the required safety functions and the required safety integrity, in order to achieve the required functional safety.

Assessment
Safety Functions
Safety Requirements Specification [D15] defines safety accuracy.
The entering and maintenance of the safe state is further detailed in this document.
Software Safety Requirements
The Software Requirements Specifications [D16] defined detail of software safety requirements and mapped to the Safety Requirements Specification[D15].

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system.

5.3 Change and modification management

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Ensure that the required safety integrity is maintained after corrections, enhancements or adaptations to the E/E/PE safety-related systems.

Assessment

Modifications are done per the Yokogawa Electric Corporation process as documented in [D30].

Modifications are initiated with an Overall Development Process [D03]. All changes are first reviewed and analyzed for impact before being approved. Measures to verify and validate the change are developed following the normal design process.

The modification process has been successfully assessed and audited, so Yokogawa Electric Corporation may make modifications to this product as needed. An impact analysis [D22] is performed for any change related to functional safety.

The impact analysis [D52], Validation test plan/ results [D47] and Validation test plan review were assessed on Q23/01-136.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system, change management procedures, and sustaining product procedures.

5.4 System Design

Objectives

The objective of the related IEC 61508 requirements of this subclause are to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

Assessment

The AXR Two-wire Magnetic Flow Meter has been determined to meet the proven in use]requirements of IEC 61508 (See documents [D16] and [R1]). This AXR has been in the field since September 2009 and has 4 million hours of documented run time in the field. Based on field return data, the estimated field failure rate of the device is 9.6E-07 failures per hour. The documented operating hours and field failure rate are sufficient to meet the proven in use requirements for SIL 3. This meets the requirements for systematic safety integrity of IEC 61508.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system and new product development processes.

5.5 Hardware Design and Verification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Create E/E/PE safety-related systems conforming to the specification for the E/E/PES safety requirements (comprising the specification for the E/E/PES safety functions requirements and the specification for the E/E/PES safety integrity requirements).
- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Demonstrate, for each phase of the overall, E/E/PES and software safety lifecycles (by review, analysis and/or tests), that the outputs meet in all respects the objectives and requirements specified for the phase.
- Test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase.
- Integrate and test the E/E/PE safety-related systems.

5.5.1 Hardware architecture design

Assessment

Hardware architecture design [D16] has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews [D27], [D31] and [D33] are used to discover weak design areas and make them more robust. Measures against environmental stress and over-voltage are incorporated into the design.

The FSM Plan [D02] and development process and guidelines define the required verification activities related to hardware including documentation, verification planning, test strategy and requirements tracking to validation test.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system and new product development processes.

5.5.2 Hardware Design / Probabilistic properties

Assessment

To evaluate the hardware design of the AXR , a Failure Modes, Effects, and Diagnostic Analysis was performed by *exida* for each component in the system. This is documented in [R3]. The FMEDA was verified using Fault Injection Testing as part of the development, see [D35], and as part of the IEC 61508 assessment.

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. An FMEDA (Failure Mode Effect and Diagnostic Analysis) is an FMEA extension. It combines standard FMEA techniques with extension to identify online diagnostics techniques and the failure modes relevant to safety instrumented system design.

From the FMEDA failure rates are derived for each important failure category.

These results must be considered in combination with PFD_{AVG} of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL). The Safety Manual states that the application engineer should calculate the PFD_{AVG} for each defined safety instrumented function (SIF) to verify the design of that SIF.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system, FMEDA quantitative analysis, and hardware development guidelines and practices.

5.6 Software Design

Objectives

The main objectives of the related IEC 61508 requirements are to:

- Create a software architecture that fulfils the specified requirements for software safety with respect to the required safety integrity level.
- Review and evaluate the requirements placed on the software by the hardware architecture of the E/E/PE safety-related system, including the significance of E/E/PE hardware/software interactions for safety of the equipment under control.
- Design and implement software that fulfils the specified requirements for software safety with respect to the required safety integrity level, which is analyzable and verifiable, and which is capable of being safely modified.

Assessment

The Software Architecture Design was not separately submitted. Prior PIU analysis and certification via the SCDB[R1] provide support for the SWA requirements. All components are considered safety critical at the highest SIL as defined in the safety requirements specification for the product. HART communication and display components are not safety critical.

Prior PIU analysis and certification via the SCDB[R1] provide support for the SWA requirements.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system.

5.7 Software Verification

Objectives

The main objectives of the related IEC 61508 requirements are to:

- To the extent required by the safety integrity level, test and evaluate the outputs from a given software safety lifecycle phase to ensure correctness and consistency with respect to the outputs and standards provided as input to that phase.

- Verify that the requirements for software safety (in terms of the required software safety functions and the software safety integrity) have been achieved.
- Integrate the software onto the target programmable electronic hardware. Combine the software and hardware in the safety-related programmable electronics to ensure their compatibility and to meet the requirements of the intended safety integrity level.-

Assessment results

Source code standard states that software modules interact with each other through their interfaces which are fully defined and documented, completely prototyped, including name and data type of parameters, and evidence is available that this was followed.

Conclusion:

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system, software development process, and new product development processes.

5.8 Safety Validation

Objectives

- Ensure that the design and implementation of the E/E/PE safety-related systems meets the specified safety functions and safety integrity requirements.
- Plan the validation of the safety of the E/E/PE safety-related systems.
- Validate that the E/E/PE safety-related systems meet, in all respects, the requirements for safety in terms of the required safety functions and the safety integrity.
- Ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

Assessment

One or more test cases, or analysis documents, exist for each safety requirement (including software safety requirements) as shown by the requirements traceability matrix. Each test case includes a procedure for the test as well as pass/fail criteria for the test (inputs, outputs and any other acceptance criteria). The validation test plan includes the procedure used to properly judge that the validation test is successful or not. (Field experience or statistical testing are recommended alternatives to Blackbox testing to be considered in the test plan creation.) Dynamic (runtime) analysis/testing is required for SIL 3, in addition to static analysis/testing.

Fault injection testing has been previously performed on the product as defined in the fault injection test plan. The results have been analyzed and adjustments have been made to the FMEDA based on these results. Recent HW changes do not require Fault insertion retesting.

Test results are documented including reference to the test case and test plan version being executed.

The following information is documented in the test results:

a) a record of validation activities, permitting validation results to be reproduced and/or retraced.

b) The version of the validation plan used to execute the test.

c) The safety function associated with each test case.

d) The tools and equipment and calibration data.

e) The Configuration Identification of the Item Under Test.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system, software development process, and new product development processes.

5.9 Safety Manual

Objectives

- Develop procedures to ensure that the required functional safety of the E/E/PE safety-related systems is maintained during operation and maintenance.

Assessment

Yokogawa Electric Corporation created a Safety Manual for the AXR , see[D37]. This safety manual was assessed by *exida*. The final version is in compliance with the requirements of IEC 61508. The document includes all required reliability data and operations, maintenance, and proof test procedures.

Safety Manual [D51] was assessed on Q23/01-136.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system and the safety manual.

6 Terms and Definitions

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.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
SFF	Safe Failure Fraction - Summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by 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).
HART	Highway Addressable Remote Transducer
AI	Analog Input
AO	Analog Output
DI	Digital Input
DO	Digital Output
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 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.

7.2 Version History

Contract Number	Report Number	Revision Notes
Q20/02-144	YEC 20-02-144 R001 V0R1 IEC 61508 Assessment AXR	Internal draft; March 26, 2020
Q20/02-144	YEC 20-02-144 R001 V1R1 IEC 61508 Assessment AXR	Draft for customer review; March 30, 2020
Q20/02-144	YEC 20-02-144 R001 V1R2 IEC 61508 Assessment AXR	First release; March 31, 2020
Q23/01-136	YEC 20-02-144 R001 V2R1 IEC 61508 Assessment AXR	Revised with HW modification; April 5, 2023
Q24/01-071	YEC 20-02-144 R001 V3R1 IEC 61508 Assessment AXR.docx	Revised certification with customer documents updated; February 26, 2024

Review: Kiyoshi Takai, exida-Japan,

Status: Release, February 26, 2024

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Kaoru Sonoda Evaluation Assessor

Kiyoshi Takai

Kiyoshi Takai Certified Assessor