Results of the IEC 61508 Functional Safety Assessment

Project:
Vortex Flowmeter YEWFLO TI VY Series

Customer:
Yokogawa Electric Corporation
Musashino, Tokyo
Japan

Contract No.: Q22/02-065
Report No.: YEC 21/01-069 R002
Version V2, Revision R1, September 27, 2022
Kiyoshi Takai

Management Summary

The Functional Safety Assessment of the Yokogawa Electric Corporation

Vortex Flowmeter YEWFLO TI VY Series

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

- *exida* assessed the systematic capability through a detailed analysis of proven-in-use data provided by Yokogawa Electric Corporation and the creation of a detailed safety case against the requirements of IEC 61508.
- *exida* reviewed and assessed the random capability through 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 ensure that the FMEDA analysis was complete.
- *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 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 design 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 Vortex Flowmeter YEWFLO TI VY Series development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA also shows that the Vortex Flowmeter YEWFLO TI VY Series 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 Vortex Flowmeter YEWFLO TI VY Series 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.


CERTIFIED
exida
IEC 61508
SIL 3 CAPABLE

Table of Contents

Management Summary 2

1 Purpose and Scope 5

1.1 Tools and Methods used for the assessment 5

2 Project Management 6

2.1 *exida* 6

2.2 Roles of the parties involved 6

2.3 Standards / Literature used 6

2.4 Reference documents 6

2.4.1 Documentation provided by Yokogawa Electric Corporation 6

2.4.2 Documentation generated by *exida* 8

2.5 Assessment Approach 9

3 Product Description 11

3.1 Hardware and Software Version Numbers 11

4 IEC 61508 Functional Safety Assessment Scheme 12

4.1 Product Modifications 12

5 Results of the IEC 61508 Functional Safety Assessment 13

5.1 Lifecycle Activities and Fault Avoidance Measures 13

5.1.1 Safety Lifecycle and Functional Safety Management Planning 13

5.1.2 Tools (and languages) 15

5.1.3 Safety Requirement Specification and System Architecture Design 15

5.1.4 Change and modification management 17

5.1.5 Proven In Use 17

5.2 Software Design 18

5.2.1 Software Verification 19

5.2.2 Safety Validation 20

5.3 Hardware Design and Verification 21

5.3.1 Hardware Architecture Design and Probabilistic Properties 21

5.4 Safety Manual 22

6 Terms and Definitions 23

7 Status of the document 24

7.1 Liability 24

7.2 Releases 24

7.3 Future Enhancements 24

7.4 Release Signatures 24

1 Purpose and Scope

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

- Vortex Flowmeter YEWFLO TI VY Series

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:

- with the technical requirements of IEC 61508 parts 2 and 3 for SIL 3 and the derived product safety property requirements;

and

- the Vortex Flowmeter YEWFLO TI VY Series development processes, procedures and techniques as implemented for the safety-related deliveries with the managerial requirements of IEC 61508 parts 1, 2 and 3 for SIL 3;

and

- the Vortex Flowmeter YEWFLO TI VY Series hardware analysis represented by the Failure Mode, Effects and Diagnostic Analysis with the relevant requirements of IEC 61508-2.

The assessment has been performed 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 performed by using the *exida* Safety Case tool. The Safety Case tool contains the accredited *exida* certification 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.

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 350 billion hours of field failure data.

2.2 Roles of the parties involved

Yokogawa Electric Corporation	Manufacturer of the Vortex Flowmeter YEWFLO TI VY Series
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* certification 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 61508:2010 (Parts 1 – 7):	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

2.4 Reference documents

2.4.1 Documentation provided by Yokogawa Electric Corporation

[D001]	Quality Manual	QP-140-01-11E0.pdf	0	14-Jul-21
[D002]	Overall Development Process	QP-172-01-8E0.pdf	0	14-Jul-21
[D003]	Configuration Management Process	QP-172-06-2E.pdf	0	27-Dec-10
[D004]	Field Failure Reporting Procedure/Field Return Procedure	QP-185-02-5E0.pdf	0	27-Mar-19
[D005]	Manufacturer Qualification Procedure	GMSe-800.pdf		30-Nov-20
[D006]	Part Selection Procedure	ds41102E.pdf	3	13-Apr-07
[D007]	Quality Management System (QMS) Documentation Change Procedure	QP-140-02-9E0.pdf	0	14-Jul-21
[D008]	Non-Conformance Reporting procedure	GMSe-800-01-01.pdf		30-Nov-20
[D009]	Corrective Action Procedure	QP-185-02-5E0.pdf	0	27-Mar-19
[D010]	Action Item List Tracking Procedure	QS-100-12E0.pdf	0	28-Dec-20

[D011]	Customer Notification Procedure	GMSe-800-01-01.pdf		30-Nov-20
[D012]	Software Development Process	QP-172-02-6E.pdf	0	14-Jul-21
[D013]	Software Tool Qualification Procedure	QP-172-05-1E2.pdf	2	03-Jul-17
[D014]	ASIC Development Process	STR-CMNPF-A045_r0.pdf	0	28-Mar-16
[D015]	Modification Procedure	SMM-C-088_r25.pdf	25	31-May-21
[D016]	Impact Analysis Template	STR-VF10-Z0050_r0.pdf	0	15-Dec-21
[D017]	FSM Plan/ Development Plan	STR-VF10-A0041_R1.pdf	1	15-May-20
[D018]	SW Development Plan	STR-VF10-P0093_r0.pdf	0	06-Apr-20
[D019]	Configuration Management Plan	STR-VF10-A0034_R4.xlsx	4	02-Dec-21
[D020]	Verification Plan	STR-VF10-A0050_YEWFLO_TI_VY 中間設計審査(1)提案書_R0.pdf	0	04-Nov-20
[D021]	Shipment Records/Field Returns Records	DY 出荷データ、フィールドリターンデータ_rev0.xlsx		22-Nov-21
[D022]	Job Descriptions and Competency Levels	STR-VF10-A0039_R3.xlsx	3	29-Nov-21
[D023]	Training Record / Skills Matrix	STR-VF10-Z0051_r1	1	8-Feb-22
[D024]	ISO 900x Cert or equivalent	0066454-QMS-ENGUS-UKAS.pdf		15-Sep-21
[D025]	List of Design Tools	STR-VF10-P0156_r2.pdf	2	24-Jan-22
[D026]	Safety Requirements Specification	STR-VF10-B0009_VY_Safety_Requirement_Specification_r4.docx	4	08-Nov-21
[D027]	Safety Requirements Review	STR-VF10-G0408_VY_SRS_PFDavg_verification_results_SRS(Rev.4)_議事録.docx		08-Nov-21
[D028]	Software Safety Requirements Specification	STR-VF10-P096_r0.pdf	0	21-Apr-21
[D029]	System Architecture Design Specification	STR-VF10-P0122_r0.pdf	0	10-Mar-21
[D030]	Schematics	FD1-F9491JD_20210114.pdf, Rev0	0	14-Oct-21
[D031]	Schematics	FD1-F9491PB_20210507.pdf, Rev0	0	07-May-21
[D032]	Schematics	FD1-F9491LB_20210507.pdf, Rev0	0	07-May-21
[D033]	Schematics	FD1-F9491NA_20210507.pdf, Rev0	0	07-May-21
[D034]	Schematics	FD1-F9491MA_20210507.pdf, Rev0	0	07-May-21
[D035]	Schematics	FD1-F9491QA_20200302.pdf, Rev0	0	02-Mar-20
[D036]	Schematics	FD1-F9491RA_20200304.pdf, Rev1	1	04-Mar-20
[D037]	Schematics	FD1-F9491SA_20200305.pdf, Rev0	0	05-Mar-20
[D038]	Schematics	FD1-F9491TA_20200305.pdf, Rev0	0	05-Mar-20
[D039]	Schematics	FD1-F9492NA_20200521.pdf, Rev0	0	21-May-20
[D040]	Schematics	FD1-F9492PA_20200403.pdf, Rev0	0	03-Apr-20
[D041]	High Level Software Design Specification	STR-VF10-P0123_r0.pdf	0	16-Mar-21
[D042]	High Level Software Design Specification	STR-VF10-P0124_r0.pdf	0	16-Mar-21
[D043]	High Level Software Design Specification	STR-VF10-P0125_r0.pdf	0	09-Feb-21

[D044]	SW HAZOP	STR-VF10-P0096_r0.pdf	0	21-Apr-21
[D045]	Detailed Software Design Specification	STR-VF10-P0102_r2.pdf	2	25-Nov-21
[D046]	Requirements Traceability Matrix	STR-VF10-Z0044_r3.pdf	3	24-Dec-21
[D047]	Fault Injection Test Plan	YEC 20-04-072 V1R1 Fault Injection Test Plan YEWFLO TI.xlsx	V1R1	27-Jul-20
[D048]	Coding Standard	SDS-C-079_r5.pdf	5	23-Apr-20
[D049]	Validation Test Plan	STR-VF10-B0170_r1(添付資料).zip		29-Dec-21
[D050]	Validation Test Plan Review Record	STR-VF10-G0423_r1.pdf	1	14-Jan-22
[D051]	EMC Test Plan	EEN0442-A01.pdf	0	15-Dec-20
[D052]	Validation Test Result	STR-VF10-A0066_R0.pdf	0	01-Dec-21
[D053]	EMC Test Results	ENV21022.pdf		02-Aug-21
[D054]	Fault Injection Test Results	YEC 20-04-072 V1R1 Fault Injection Test Plan YEWFLO TI_result.xlsx	V1R1	29-Sep-20
[D055]	Operation / Maintenance Manual	IM01F07A01-01EN_001.pdf	1	28-Feb-22
[D056]	Operation / Maintenance Manual	IM01F07A01-02EN_001.pdf	1	28-Feb-22
[D057]	Safety Manual	IM01F07A21-02EN_001.pdf	1	06-Oct-21
[D058]	Safety Manual Review	STR-VF10-G0403_r2.pdf	2	13-Jan-22
[D059]	List of Diagnostics for FMEDA	STR-VF10-B0008_r2.pdf	2	13-Dec-21
[D060]	Tool Qualification Report	STR-VF10-P0156_r2.pdf	2	24-Jan-22

2.4.2 Documentation generated by *exida*

[R1]	YEC 21-01-069 V1 R3 SCWB-61508 YEWFLO TI.xlsm	SafetyCase file for Vortex Flowmeter YEWFLO TI VY Series
[R2]	YEC 21/01-069 R002	IEC 61508 Functional Safety Assessment for Vortex Flowmeter YEWFLO TI VY Series (This document)
[R3]	YEC 20-04-072 R001 V1R7 FMEDA YEWFLO TI.docx	FMEDA report
[R4]	YEC 21-01-069 YEWFLO TI V1R1 FFA.xlsx	Field Failure Analysis (Proven-In-Use Analysis)
[R5]	YEC 22-02-065 R004 V1 R2 YEWFLO TI VY Production Assessment.docx	YEWFLO TI VY Series Production Assessment

2.5 Assessment Approach

The certification audit was closely driven by requirements of the accredited *exida* certification scheme which includes subsets filtered from IEC 61508. The assessment was planned by *exida* and agreed with Yokogawa Electric Corporation.

For designs that have been in service for several years and have demonstrated themselves in a variety of applications and conditions, consideration of a proven in use assessment may be used as a substitute if a product didn't follow a fully compliant IEC 61508 design process. The full functional safety assessment includes an assessment of all fault avoidance and fault control measures during any hardware and software modifications needed to achieve SIL 3 capability for the Vortex Flowmeter YEWFLO TI VY Series. Other product development aspects prior to these modifications were assessed according to Proven-In-Use (PIU) requirements (see section 5.1.6). The combination of these assessments demonstrates full compliance with IEC 61508 to the end-user.

The assessment considers all requirements of IEC 61508. Any requirements that have been deemed not applicable have been marked as such in the full Safety Case report, e.g. software development requirements for a product with no software.

As part of the IEC 61508 functional safety assessment for the Vortex Flowmeter YEWFLO TI VY Series, the following evidence aspects have been reviewed:

- FMEDA
- SRS or product specification
- Safety manual
- Instruction manual
- Hardware fault inject test plan and results verification
- Software architecture design specification [if applicable]
- EMC and environmental test report
- Validation test results
- Corrective Action and prevention action plan/process
- Software and hardware drawings release process
- PIU data collection procedures and operational excellence calculation/report (evidence that the equipment is proven-in-use; analysis of field failure rates to ensure that no systematic faults exist in the product)

No safety related communications are used in this product.

Proven-In-Use (PIU) assessment provides for the prevention of systematic failures for pre-existing devices with a proven history of successful operation. As part of the PIU assessment for the Vortex Flowmeter YEWFLO TI VY Series, a number of IEC 61508 functional safety assessment requirements are satisfied without further documented evidence:

- FSM Plan
- Configuration management
- Validation of development tools
- Validation test plan
- System Architecture design
- Integration and Unit test plans
- Development process

The project teams, not individuals, were audited.

3 Product Description

The Vortex Flowmeter YEWFLO TI VY Series combines the field proven sensor and body assembly used in more than 450,000 units installed worldwide with a unique and powerful combination of digital technology that includes spectral signal processing (SSP), a Yokogawa innovation. The Vortex Flowmeter YEWFLO TI VY Series is accurate and stable, even in harsh process conditions, and has a highly reliable and robust design that delivers improvements in plant efficiency and reduced operating costs.

3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of Vortex Flowmeter YEWFLO TI VY Series:

YEWFLO TI VY Series	
Hardware	S1.01
Software	R1.01

4 IEC 61508 Functional Safety Assessment Scheme

The assessment was executed using the accredited *exida* certification scheme which includes subsets of the IEC 61508 requirements tailored to the work scope of the development team. The assessment was performed based on the information received from Yokogawa Electric Corporation [section 2.4.1] and is documented in the safety case [R1].

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 accredited *exida* certification 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(s) 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 a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R3] of the Vortex Flowmeter YEWFLO TI VY Series to document the hardware architecture and failure behavior. The FMEDA report and the Safety Case created for the YEWFLO TI documents this assessment.

exida assessed failure history of the Vortex Flowmeter YEWFLO TI VY Series [D021] and performed a detailed analysis of the data provided [R4]. This PIU assessment is done in place of a detailed functional safety assessment for systematic failures. The Safety Case created for the YEWFLO TI documents this assessment.

The result of the overall assessment can be summarized by the following observations:

The Vortex Flowmeter YEWFLO TI VY Series complies with the relevant requirements of IEC 61508 SIL 3 applications when considering PIU and when properly designed into a Safety Instrumented Function per the requirements in the Safety Manual.

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 [D002].

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 subsets of the IEC 61508 requirements tailored to the SIL 3 work scope of the development team and supported by PIU analysis.

5.1.1 Safety Lifecycle and Functional Safety Management Planning

Objectives

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

Assessment

FSM Plan

The functional safety management plan [D017] defines the safety lifecycle for this project. This includes a definition of the safety activities and documents to be created for this project. This information is communicated via these documents to the entire development team so that everyone understands the safety plan. The Software Development Procedure identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase. Manufacturer has a QMS [D007] in place. The Manufacturer has been ISO 9001 certified [D024]. All sub-suppliers have been qualified through the Manufacturer Qualification procedure. All phases of the safety lifecycle have verification steps described in the FSM plan or a separate verification plan for one or more phases. This plan includes criteria, techniques and tools used in the activities. The verification is carried out against this plan.

An FSM plan [D017] exists to document key areas of functional safety management and act as guidance for future modifications. It identifies the safety lifecycle, competencies and responsibilities of personnel, key safety activities and measures to be used, and software tools.

All documents are under version control as required by [D019]. Configuration Management practices are handled in the FSM plan [D017]. 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.

Training and competence recording

The FSM Plan lists the key people working on the project along with their roles.

A competency matrix has been created and includes the following:

a) Competency requirements for each role on project.

b) List of people who fulfill each role

c) List of competencies for each individual matched up to required competencies based on roles that they fill.

d) Training planned to fill any competency gaps.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation functional safety management system, internal organizational procedures, product change management processes, and safety lifecycle processes and supported by PIU analysis.

5.1.2 Tools (and languages)

Assessment

All tools which support a phase of the software development lifecycle and cannot directly influence the safety-related system during its run time (Off-line support tools) are documented, including tool name, manufacturer name, version number, use of the tool on this project.

This includes validation test tools. All off-line support tools have been classified as either T3 (safety critical), T2 (safety-related), or T1 (interference free). All off-line support tools in classes T2 and T3 have a specification or product manual which clearly defines the behavior of the tool and any instructions or constraints on its use. List all T3 and T2 tools along with a reference (file name, document number) to the specification or product manual. An assessment has been carried out for T2 and T3 offline support tools, to determine the level of reliance placed on the tools, and the potential failure mechanisms of the tools that may affect the executable software. Where such failure mechanisms are identified, appropriate mitigation measures have been taken.

The following information is documented for all off-line support tools classified as either T2 or T3:

All configuration baseline items for which the tool is used.

The tool configuration (compiler options, batch files, scripts, etc. for each different use of the tool.)

For each tool in class T3, evidence is available that the tool conforms to its specification or manual through a combination of confidence from use and tool validation. If evidence is not available for a given tool, measures to control faults introduced by the tool, are implemented to control a failure caused by the fault. For each tool in class T3, if tool validation was performed, the results of the validation were documented and the tool validation checklist was completed.

Conclusion

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

5.1.3 Safety Requirement Specification and System Architecture Design

Objectives

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

Assessment

All element safety functions necessary to achieve the required functional safety are specified, including, as appropriate:

- functions that enable the EUC to achieve or maintain a safe state;
- functions related to the detection, annunciation and management of sensor and actuators faults;
- functions that allow the PE system to be safely modified;

- safety-related communications (see 7.4.11 of IEC 61508-2);

- safety accuracy and stability for measurement and control (if required).

Software safety requirements [D028] have been created as derived/allocated requirements (from Safety Requirements). These requirements have been made available to the software developers and have been reviewed by software developers. The results of the review are documented and all action items are tracked through resolution.

Software Safety Requirements specify the protection of all operational parameters, with respect to invalid, out of range or untimely values; unauthorized changes; and corruption. Specific requirement for start-up and restart procedures (if required) are specified. All system, operator and software interfaces necessary to achieve the required functional safety are specified. All safety related constraints between the software and hardware have been documented in the Software Safety Requirements or other suitable requirements document.

The System Architecture Design clearly identifies the SIL of all components in the design. If a component has a lower SIL capability than that associated with the safety function(s), then sufficient independence between the components has been documented (usually in an FMEA or software HAZOP).

The System Architecture Design describes that the behavior of the device when a fault is detected is to take an action which will achieve or maintain a safety state (such as raising an output signal through an external interface or setting an output to the configured safe state).

The System Architecture Design clearly identifies that communication interfaces are not safety related.

The System Architecture Design identifies design features (such as Proof Test) that support maintainability and testability. This shows that these qualities have been considered during design and development and have been verified at review time.

(It was agreed that this req referred to maintenance and test of the final product in the field. So the requirement is saying that the plan for maintaining a part and proof testing it should be formalized during the design phase.) Maintenance should include possible software changes in the field, if applicable (such as software updates and software configuration changes), including maintaining system safety during and after such changes.

All software components or subsystems listed in the Software Architecture Design have corresponding Software Designs which further partition the design into software modules. The design has a focus on simplicity. The Software Design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified. Formal design reviews are held and the results recorded; action items are identified, assigned, and resolved.

Conclusion

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

5.1.4 Change and modification management

Objectives

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

Assessment

Modifications are initiated with an Engineering Design Change procedure [D015]. 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.

Since this was the initial assessment of Yokogawa Electric Corporation's modification procedure according to IEC 61508, it was expected that modifications to the product prior the assessment did not include a functional safety impact analysis. The modification process has been revised to include a functional safety impact analysis. The initial post assessment modification to the Vortex Flowmeter YEWFLO TI VY Series shall be audited by *exida* to confirm that a functional safety impact analysis was performed according to Yokogawa Electric Corporation's modification procedure.

A Modification Procedure requires that an Impact Analysis be performed to assess the impact of the modification, including the impact of changes to the software design (which modules are impacted) and on the Functional Safety of the system. The results of an Impact Analysis are documented. Modification Request/Records will document the reason for the change and have a detailed description of the proposed change. (affects both software and hardware) The impact analysis documents which tests must be run to validate the change and which tests must be re-run to validate that the change did not affect other functionality.

Modifications are initiated with an Engineering Design Change procedure [D015]. 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 [D016] is performed for any change related to functional safety.

Conclusion

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

5.1.5 Proven In Use

Field failure analysis [R4] shows that the failure rate based on field returns within the warranty period is lower than the expected failure rate as defined in the FMEDA report [R3]. The environmental specifications and the function of the YEWFLO TI VY Series are the same as the fielded version. Field failure analysis also shows that the number of hours achieved meets the minimum amount for the given SIL.

the Yokogawa Electric Corporation has been shipping for 30 months without any significant revisions or changes (NOTE: Based on the assumption that installation takes six months. Significant changes include any change in design structure or new features that interrelate with existing features.). This is supported by the shipping records and the PIU analysis.

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was performed on the Vortex Flowmeter YEWFLO TI VY Series. Shipment records were used to determine that the Vortex Flowmeter YEWFLO TI VY Series has greater than 300 million operating hours and has demonstrated a field failure rate less than the predicted failure rates indicated in the FMEDA reports.

All components considered in the FMEDA are standard components with greater than 100 million operating hours, and diagnostic coverage is shown to be greater than 60% (see [R3]). This provides justification for using a Route 2H approach.

Conclusion

The objectives of the standard for Proven In Use for SIL 3 are fulfilled by the Yokogawa Electric Corporation field history and return procedures and supported by PIU analysis.

5.2 Software Design

Objectives

- 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 software safety requirements 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 contains a description of the software architecture. The design is partitioned into new, existing and/or proprietary (third party) components and modules, which are identified as such.

A software criticality analysis and HAZOP was performed and the report lists all components along with their criticality (Safety Critical, Safety Related, or Non-Interfering) and their required Systematic Capability. Independence has been achieved by both spatial and temporal separation as documented in the results of the SCA / SW HAZOP. Common cause failures are identified in the SW HAZOP as failures of one component that could affect an independent component and defensive measures are listed as Safety Measures.

The Software Architecture Design uses the following diagram types:

- Logic/Function Block Diagrams
- Object Diagrams
- State Charts / State Transition Diagrams
- Sequence Diagrams
- Data Flow Diagrams
- Decision / Truth Tables

The Software Architecture Design specifies that [fault detection technique] is employed to detect software faults.

The Software Design describes the design features that maintain the safety integrity of data. The Software Design describes the design of all diagnostics required to detect faults in software control flow and data flow. The resulting behavior of the device due to a detected fault is specified.

Conclusion

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

5.2.1 Software Verification

Objectives

- 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

The Software Design describes the design of all diagnostics required to detect hardware faults. Modular approach; A modular approach has been used in the software design. Design has been broken up into classes and methods which are modular and subprograms have a single entry and a single exit. Structural test coverage (entry points) of 100 % is documented by a tool or a manual trace of test coverage. Results/evidence that all safety related Source Code Modules have been inspected. Sample code review reports were reviewed to ensure non-conformances are recorded and followed up. Module Test Results for all safety related modules were produced and documented per the Module Test Verification Plan/Specification; Sample results files were reviewed; unit tests are automated or manual; verification of data is included in tests; result files show the pass/fail output line. No unintended functions were performed. Static analysis; Results / evidence from Static Analysis of source code.

All Integration Test Cases have been successfully run, per the Integration Test Plan and Integration Test Results have been documented. The Integration Test Plan requires that Safety Functions are tested during Integration Testing using a functional testing approach.

Conclusion:

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

5.2.2 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, if required, has been 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. Test results are documented including reference to the test case and test plan version being executed.

The EMC/Environmental specifications tested (and passed) were the same as or more stringent than those reviewed and approved by the FMEDA analyst.

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, internal organizational procedures, software development process, and new product development processes and supported by PIU analysis.

5.3 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/PE safety requirements (comprising the specification for the E/E/PE safety functions requirements and the specification for the E/E/PE 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/PE 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.

5.3.1 Hardware Architecture Design and Probabilistic Properties

Assessment

Hardware architecture design [D029] has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews [D020] 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 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.

To evaluate the hardware design of the YEWFLO TI, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed by *exida* for each component in the system. This is documented in [R3]. The FMEDA was verified using Fault Injection Testing, see [D054], 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. The FMEDA 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 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 and supported by PIU analysis.

5.4 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

The Safety Manual is provided and identifies and describes the functions of the product. The functions are clearly described, including a description of the input and output interfaces. When internal faults are detected, their effect on the device output is clearly described. Sufficient information shall be provided to facilitate the development of an external diagnostics capability (output monitoring).

Specific instructions are given for use of pre-existing software components. The Safety Manual gives guidance on recommended periodic (offline) proof test activities for the product, including listing any tools necessary for proof testing. Procedures for maintaining tools and test equipment are listed. All routine maintenance tools and activities required to maintain safety are identified and described in the Safety Manual.

Conclusion

The objectives of the standard are fulfilled by the Yokogawa Electric Corporation the safety manual.

6 Terms and Definitions

E/E/PE	Electric/Electronic/Programmable Electronic safety-related system
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
PIU	Proven-In-Use
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 Releases

Version History:	V2, R1:	Updated with Production Audit, September 27, 2022
	V1, R2:	First Release, February 9, 2022
	V1, R1:	Draft for customer review, February 1, 2022
	V0, R1:	Initial draft KT, January 27, 2022
Authors:	Kiyoshi Takai	
Review:	Kaoru Sonoda	
Release status:	Release	

7.3 Future Enhancements

At request of client.

7.4 Release Signatures

Kiyoshi Takai Evaluating Assessor

Kaoru Sonoda Certifying Assessor