



## **Results of the IEC 61508 Functional Safety Assessment**

Project:

ROTAMASS Total Insight Coriolis Mass Flow and Density Meter

Customer:

Yokogawa Electric Corporation

Musashino, Tokyo, Japan

ROTA Yokogawa GmbH & Co. KG

Wehr, Germany

Contract No.: Q25/01-223

Report No.: YEC 14-11-026 R001

Version V7, Revision R3, July 14, 2025

Kiyoshi Takai

## Management Summary

The Functional Safety Assessment of the **Yokogawa Electric Corporation, ROTAMASS Total Insight Coriolis Mass Flow and Density 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.**

**The assessment of the FMEDA also shows that the ROTAMASS Total Insight Coriolis Mass Flow and Density 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 ROTAMASS Total Insight Coriolis Mass Flow and Density 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

\_Toc202436069

Management Summary .....	2
Table of Contents .....	3
1 Purpose and Scope .....	5
1.1 Tools and Methods used for the assessment .....	5
2 Project Management .....	6
2.1 <i>exida</i> .....	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 <i>exida</i> .....	13
2.5 Assessment Approach .....	14
3 Product Description .....	15
3.1 Hardware and Software Version Numbers .....	15
4 IEC 61508 Functional Safety Assessment Scheme .....	16
4.1 Product Modifications .....	16
5 Results of the IEC 61508 Functional Safety Assessment .....	17
5.1 Lifecycle Activities and Fault Avoidance Measures .....	17
5.1.1 Functional Safety Management .....	17
5.1.2 Safety Lifecycle and FSM Planning .....	18
5.1.3 Documentation .....	18
5.1.4 Training and competence recording .....	18
5.1.5 Configuration Management .....	19
5.1.6 Tools (and languages) .....	19
5.1.7 Proven In Use .....	19
5.2 Safety Requirement Specification .....	19
5.3 Change and modification management .....	20
5.4 System Design .....	21
5.5 Hardware Design and Verification .....	21
5.5.1 Hardware architecture design .....	21
5.5.2 Hardware Design / Probabilistic properties .....	22
5.6 Software Design .....	22
5.7 Software Verification .....	23
5.8 Safety Validation .....	23
5.9 Safety Manual .....	24
6 Terms and Definitions .....	25
7 Status of the document .....	26
7.1 Liability .....	26

7.2 Version History.....	26
7.3 Future Enhancements.....	27
7.4 Release Signatures.....	27

# 1 Purpose and Scope

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

➤ **ROTAMASS Total Insight Coriolis Mass Flow and Density 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter with the technical IEC 61508-2 and -3 requirements for SIL 3 and the derived product safety property requirements

and

- the ROTAMASS Total Insight Coriolis Mass Flow and Density 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 ROTAMASS Total Insight Coriolis Mass Flow and Density 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], [R9])

## 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 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter
<i>exida</i>	Performed the hardware assessment [R3]
<i>exida</i>	Performed the Functional Safety Assessment [R1] per the accredited <i>exida</i> 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 – 3)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Normative Parts
[N2]	IEC 61508:2010 (Parts 4 – 7)	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems – Informative Parts

### 2.4 Reference documents

#### 2.4.1 Documentation provided by Yokogawa Electric Corporation

Doc ID	Document Description	Project Document Name	Version	Date
D01	Quality Manual	QP-140-01-8.pdf	8	18-Jul-14
D02	Overall Development Process	QP172-01-6.pdf	6	26-Sep-12
D03	Configuration Management Process	QP172-06-2.pdf	2	01-Sep-09
D04	Field Failure Reporting Procedure	QP185-02-3.pdf	3	20-Oct-09
D05	Manufacturer Qualification Procedure	SMS台帳 (Manufacturing Standard).pdf		15-Apr-14
D06	Part Selection Procedure	ds41102E.pdf	3	13-Apr-07

D07	Quality Management System (QMS) Documentation Change Procedure	QP140-02-6.pdf	6	15-Apr-10
D08	Quality Management System (QMS) Documentation Change Procedure	GMj-800.pdf	4	27-Apr-15
D09	Non-Conformance Reporting procedure	GMj-804.pdf	9	27-Apr-15
D10	Corrective Action Procedure	QP-185-01-1E0.pdf	0	20-Apr-11
D11	Internal Audit Procedure	QP-150-03-5E0.pdf	0	19-Sep-13
D12	Action Item List Tracking Procedure	QS-100-8E0.pdf	0	31-Mar-14
D13	Training Procedure	QP-160-02-2E.pdf	0	15-Oct-10
D14	Test Equipment Calibration Procedure	QP-175-03-9E0.pdf	0	30-Mar-15
D15	Management Review Process	ds10101E.pdf	6	28-Sep-12
D16	Software Development Process	QP-172-05-1E1.pdf	0	20-Apr-11
D17	ASIC Development Process	STR-CMNPF-B072_r4_フィールド共通プラットフォーム_FPGA_TOP_設計マニュアル.doc	4	27-Aug-13
D18	ASIC On-Chip Redundancy Checklist	STR-CMNPF-B083_Rev1_フィールド共通プラットフォーム TOPモジュール構文解析報告書.xlsx	1	29-Nov-12
D19	Modification Procedure	SMM-C-088_18_設計変更作業基準.doc	18	01-Jul-13
D20	FSM Plan or Development Plan	STR-CT4_YHQ-A006_コリオリ流量計Phase1_製品開発計画書R4.doc	4	05-Sep-14
D21	Configuration Management Plan	STR-CT4_YHQ-A004_2011_0427_PR2_Rev03.ppt	3	23-Jul-11
D22	Verification Plan	STR-CT4_YHQ-A005_R3_new coriolis technical investigation records_PR3-2 - 4WPF統合版.xls		06-Aug-14
D23	Shipment Records	2015-03-19_MTBF_ROTAMASS_Berechnung.pdf	0	19-Mar-15
D24	Training Record	教育記録_アナログ技術者.doc		
D25	Skills Matrix	STR-EDC-Z010_15(スキルマップ)_リーダー明記.xls		22-Mar-16
D26	ISO 900x Cert or equivalent	ISO9001認証書.pdf		24-Dec-14
D27	List of Design Tools	STR-CT4_YHQ-P042r2.docx	2	21-Apr-16
D28	Safety Requirements Specification	STR-CT4_YHQ-A049(Safety Requirements of ROTAMASS TI).docx	0	05-Jan-16
D29	Safety Requirements Review	STR-CT4_YHQ-G080_SIL2_Safety_Requirement_Specification_and_Safety_Manualレビュー議事録.docx	0	01-Apr-16
D30	System Architecture Design Specification	STR-CT4_YHQ-A024_R0_proposal of new coriolis_PR3-2.pptx		05-Aug-14
D31	Schematics / Circuit Diagrams	FD1_F9480VA_Rev0.pdf / FE1_F9480VA_Rev0.xlsx	0 / 0	

D32	Schematics / Circuit Diagrams	FD1_F9481CA_Rev1.pdf / FE1_F9481CA_Rev3.xlsx	1 / 3	
D33	Schematics / Circuit Diagrams	FD1_F9481LA_Rev0.pdf / FE1_F9481LA_Rev3.xlsx	0 / 3	
D34	Schematics / Circuit Diagrams	FD1_F9481SA_Rev1.pdf / FE1_F9481SA_Rev2.xlsx	1 / 2	
D35	Schematics / Circuit Diagrams	FD1_F9481SP_Rev1.pdf / FE1_F9481SP_Rev1.xlsx	1 / 1	
D36	Schematics / Circuit Diagrams	FD1_F9481XA_Rev0.pdf / FE1_F9481XA_Rev3.xlsx	0 / 3	
D37	Schematics / Circuit Diagrams	FD1_F9484AA_Rev1.pdf / FE1_F9484AA_Rev3.xlsx	1 / 3	
D38	Schematics / Circuit Diagrams	FD1_F9484AG_Rev0.pdf / FE1_F9484AG_Rev4.xlsx	0 / 4	
D39	Schematics / Circuit Diagrams	FD1_F9484EA_Rev1.pdf / FE1_F9484EA_Rev2.xlsx	1 / 2	
D40	Schematics / Circuit Diagrams	FD1_F9484EP_Rev1.pdf / FE1_F9484EP_Rev1.xlsx	1 / 1	
D41	High Level Software Design Specification	STR-CMNPF_4W-P013_RCCT4 Main Board ファームウェア全体設計書.docx	0	24-Jul-14
D42	Detailed Software Design Specification	STR-CMNPF_4W_P040_RCCT4_SIL2_Software_Specification_E.doc	0	12-Nov-13
D43	Detailed Software Design Specification	STR-CT4_YHQ-P013_RCCT4 Alarm Specification.pdf	0	11-Nov-13
D44	Detailed Software Design Specification	STR-CT4_YHQ-P017(Sensor alarm of RCCT4).docx	0	04-Mar-14
D45	Detailed Software Design Specification	STR-CMNPF_4W-P018_Rev1_RCCT4 OptionB Analog Input 設計仕様書.docx	1	06-Mar-14
D46	Detailed Software Design Specification	STR-CT4_YHQ-A026(新コリオリ流量計Phase1ソフトウェア機能仕様書).docx	0	04-Aug-14
D47	Detailed Software Design Specification	STR-CT4_YHQ-P008_Main-DSP間通信.docx	0	19-Jul-13
D48	Detailed Software Design Specification	STR-CT4_YHQ-P035_RCCT4 HART specification.docx	0	14-Dec-15
D49	Detailed Software Design Specification	STR-CT4_YHQ-P037_RCCT4 IO機能仕様書.docx	0	16-Dec-15
D50	Design Review Record	STR-CT4_YHQ-A048_FinalDesignReviewRecord_Phase1PR4-2.doc		25-Oct-15
D51	Design Review Record	性能項目_開発仕様rev2用_ks_as2.xls		25-Oct-15
D52	Impact Analysis Template	SMM-C-088-18_設計変更作業基準 別紙1_設計変更計画.xls書	18	01-Jul-13
D53	Requirements Traceability Matrix	STR-CT4_YHQ-P053(ROTAMASS TI ソフト開発のトレーサビリティ報告書).docx	0	26-Feb-16
D54	Fault Injection Test Plan and Results	Fault Injection List ROTAMASS_RCCx4_rev2.xls	2	04-Dec-14
D55	Coding Standard	SDS-C-079_C／C++_コーディングルール_rev3.doc	3	11-Nov-14
D56	Coding Standard	WZ-LOGIC-DSGN-00_論理回路設計手順書.pdf	7	07-Sep-12
D57	Validation Test Plan	STR-CT4_YHQ-P014(DSPファームウェア単体動作確認).docx	0	14-Nov-13

D58	Validation Test Plan and Results	STR-CT4_YHQ-P039_Internal_Verification_Plan_Report_of_RCCT4_Step2_Rev1.docx	1	22-Oct-15
D59	Validation Test Plan and Results	STR-CT4_YHQ-P052(reverse calculation単体動作確認).docx	0	26-Feb-16
D60	Validation Test Plan Review Record	STR-CT4_YHQ-A044_R0_proposal_of_new_coriolis_PR4-2_R00_1029.pptx	0	29-Oct-15
D61	Environmental Test Plan	STR-CT4_YHQ-A005_R5_new_coriolis_technical_investigation_records_PR4-2_-4WPF統合版.xls	0	29-Oct-15
D62	EMC Test Plan	EMC test plan and result summary.xlsx	0	12-Apr-16
D63	Environmental Test Results	Evaluation test (except for EMC) plan and result summary.xlsx	0	12-Apr-16
D64	Fault Injection Test Results	STR-CT4_YHQ-D110(Fault Injection Test result of Pre_PP).doc	0	02-Jun-15
D65	Operation / Maintenance Manual	IM 01U10B00-00EN-R_000.pdf		20-Apr-15
D66	Safety Manual	IM01U10D00-00EN-R_001.pdf		02-May-16
D67	Safety Manual Review	MoM_Customer_Documentation_Review.docx		21-Apr-16

#### 2.4.1.1 Documentation provided by Yokogawa Electric Corporation (Q17/06-069)

Doc ID	Document Description	Project Document Name	Version	Date
D68	Impact Analysis Template	STR-CT4_YHQ-P088(rev1).pdf	1	20-Apr-17
D69	Impact Analysis Record	STR-CT4_YHQ-B176_SIL2再認証_A6382EV改廃に伴う影響度分析(Impact_Analysis).pdf	1	17-Apr-17
D70	Configuration Management Process	STR-CT4_YHQ-P089.pdf	0	13-Apr-17
D71	Detailed Software Design Specification	STR-CT4_YHQ-P062.pdf	0	28-Mar-17
D72	Design Review Record	STR-CT4_YHQ-G127.pdf	0	28-Mar-17
D73	Validation Test Plan/Result	STR-CT4_YHQ-P066.pdf	0	28-Mar-17
D74	Validation Test Result Review Record	STR-CT4_YHQ-G128.pdf	0	28-Mar-17
D75	Safety Manual	Safety Manual_IM01U10D00-00EN-R_002.pdf	2	17-Mar-17
D76	Safety Manual Review	STR-CT4_YHQ-G130.pdf	0	20-Apr-17
D77	Digital Signature	FH0_F9481CA.pdf	4	24-Apr-17
D78	ISO 900x Cert or equivalent	ISO9001 Certificate.pdf		01-Oct-16

#### 2.4.1.2 Documentation provided by Yokogawa Electric Corporation (Q17/12-084)

Doc ID	Document Description	Project Document Name	Version	Date
--------	----------------------	-----------------------	---------	------

D79	modified parts list	M-2017-0060	0	22-Jun-17
D80	modified VI ASIC	M-2017-0190	0	22-Jun-17
D81	EEPROM parts change	M-2017-0191	0	22-Jun-17
D82	Impact Analysis	STR-CT4_YHQ-B177	0	21-Feb-18
D83	Impact Analysis review	STR-CT4_YHQ-G153	1	23-May-18
D85	Validation Test Plan and result	STR-CT4_YHQ-D169	0	27-Dec-17
D86	Flash ROM Validation Test Plan and result	STR-CT4_YHQ-D168	0	20-Feb-18
D87	VI ASIC Validation test plan and result	STR-CMNP4_4W-D133	0	21-Feb-18
D88	Main Indicator EEPROM changed review	STR-CT4_YHQ-G154	0	26-Feb-18
D89	VI ASIC changed review	STR-CT4_YHQ-G155	0	26-Feb-18
D90	Safety Manual	Safety Manual IM01U10D00-00EN-R_003	3	20-Feb-18

#### 2.4.1.3 Documentation provided by Yokogawa Electric Corporation (Q20/02-160)

Doc ID	Document Description	Project Document Name	Version	Date
D91	ISO 9001 Certificate	ISO9001_Jan2020.pdf		18-Jan-20
D92	Safety Manual	STR-CT4_YHQ-B186_APP4_Safety Manual ed4 EN_2020-05-13.pdf	4	13-May-20
D93	Safety Manual Review	STR-CT4_YHQ-G220_ROTAMASS TI_SIL2更新 Safety Manual改訂レビュー議事録_202004_R1.docx	1	13-May-20
D94	Impact Analysis Record	STR-CT4_YHQ-B183_ROTAMASS TI_SIL2更新 MLCC改廃対応の影響度分析_R0.docx	0	02-Apr-20
D95	Impact Analysis Record	STR-CT4_YHQ-B184_ROTAMASS TI_SIL2更新 Terminal.Bタイプ追加の影響度分析_R0.docx	0	02-Apr-20
D96	Impact Analysis Record	STR-CT4_YHQ-B185_ROTAMASS TI_SIL2更新 Neck Terminal.Bタイプ追加の影響度分析_R0.docx	0	02-Apr-20

#### 2.4.1.4 Documentation provided by Yokogawa Electric Corporation (Q21/07-100)

Doc ID	Document Description	Project Document Name	Version	Date
D97	Safety Requirements Specification	STR-CT4_YHQ-A049-1_Safety_Requirements_of_ROTAMASS_TI_r3.pdf	3	20-Dec-22
D98	Safety Requirements Review	STR-CT4_YHQ-G287-1_ROTAMASS_TI_Safety_Requirements_レビュー議事録_r1.pdf	1	20-Dec-22
D99	Software Safety Requirements Specification	STR-CMNP4_4W-P040_RCCT4_SIL2_Software_Specification_r2.pdf	2	17-Jan-23
D100	SW HAZOP	STR-CT4_YHQ-B196.zip	0	16-Jan-23
D101	Requirement Traceability Matrix	STR-CT4_YHQ-P053 トレーサビリティ報告書.zip	3	03-Feb-23
D102	Validation Test Plan/ Results	STR-CT4_YHQ-P157_ROTAMASS_TI_HART_DR4_システムテスト計画書・報告書_r2.pdf	2	19-Jan-23
D103	Validation Test Plan Review Record	STR-CT4_YHQ-G230_ROTAMASS_TI_HART_DR4_システムテスト計画レビュー議事録_r1.pdf	1	19-Jan-23

D104	Safety Manual	STR-CT4_YHQ-A062.zip	5	08-Feb-23
D105	Safety Manual Review	STR-CT4_YHQ-G284-1_ROTAMASS_TI_Safety_Manual_レビュー議事録_r2.pdf	3	08-Feb-23
D106	Impact Analysis Record	STR-CT4_YHQ-P158_ROTAMASS_TI_HART_DR4_ソフトウェア設計変更_影響度分析報告書_r5.pdf	5	11-Jan-23

#### 2.4.1.5 Documentation provided by Yokogawa Electric Corporation (Q23/02-128)

Doc ID	Document Description	Project Document Name	Version	Date
D107	Shipment Records/ Field Return Records	STR-CT4_YHQ-Z055_R2.xlsx	R2	12-May-23
D108	ISO 9001 Certificate	ISO_9001_Yokogawa_Europe_All_sites.pdf		01-May-23
D109	Safety Manual	STR-CT4_YHQ-A062-2_IM01U10D00-00EN-R_r6.pdf	6	19-May-23
D110	Safety Manual Review	STR-CT4_YHQ-G302.docx	0	19-May-23
D111	Impact Analysis Record	STR-CT4_YHQ-B199.docx	0	24-Mar-23
D112	Impact Analysis Record	STR-CT4_YHQ-B200.pdf	0	10-Apr-23

#### 2.4.1.6 Documentation provided by Yokogawa Electric Corporation (Q23/09-101)

Doc ID	Document Description	Project Document Name	Version	Date
D113	Verification Plan	STR-CMNPF_4W-A024_LCD ドライバの改廃_Cランク設計変更_中間レビュー資料_rev2.pptx	2	20-Jul-23
D114	Design Review Record	STR-CMNPF_4W-G230_LCD ドライバの改廃_Cランク設計変更_最終レビュー議事録_rev1.docx	1	25-Aug-23
D115	Verification Results	STR-CMNPF_4W-A025_LCD ドライバの改廃_Cランク設計変更_最終レビュー資料_rev1.pptx	1	28-Aug-23
D116	Requirements Traceability Matrix	STR-CT4_YHQ-P053-2_トレーサビリティマトリックス_r4.zip	4	26-Sep-23
D117	Safety Manual	STR-CT4_YHQ-A062-1_Safety_Manual_of_ROTAMASS_TI_r7.zip	7	02-Oct-23
D118	Safety Manual Review	STR-CT4_YHQ-G319 Safety Manual of ROTAMASS TI_LCD改廃修正確認議事録.docx	0	02-Oct-23
D119	Impact Analysis Record	STR-CT4_YHQ-P192_ROTAMASS_TI_LCD ドライバIC改廃影響度分析報告書.docx	4	01-Sep-23

#### 2.4.1.7 Documentation provided by Yokogawa Electric Corporation (Q24/02-079)

Doc ID	Document Description	Project Document Name	Version	Date
D120	Shipment Records/ Field Return Records	RMTI data of shipment and nonconformity_20240418.xlsx	1	18-Apr-24
D121	Skill Matrix	STR-CT4_YHQ-Z146855_流量計統括部開発部(ROTAMASS TI)_製品担当者スキルマップ_FY23.pdf	0	03-Apr-24
D122	Safety Requirements Specification	STR-CT4_YHQ-A049-1_Safety_Requirements_of_ROTAMASS_TI_r4.pdf	4	19-Apr-24
D123	Safety Requirements Review	STR-CT4_YHQ-G149878_ROTAMASS TI_安全要求仕様書改定内容の確認レビュー議事録.pdf	0	24-Apr-24
D124	Operation/Maintenance Manual	IM01U10B00-00EN-R_005.pdf	5	15-Mar-24
D125	Safety Manual	STR-CT4_YHQ-A062-2_IM01U10D00-00EN-R_r8_20240422.pdf	8	19-Apr-24

D126	Safety Manual Review	STR-CT4_YHQ-G149877_ROTAMASS TI_Safety Manual改定内容の確認レビュー議事録.pdf	0	24-Apr-24
D127	Impact Analysis Record	STR-CT4_YHQ-B146000_Rotamass TI_BARRIER BOARD ASSY A6259LAの影響度分析_r1.pdf	1	11-Apr-24
D128	Impact Analysis Record	STR-CT4_YHQ-B146002_ROTAMASS TI_BARRIER BOARD ASSY ヒューズ変更_影響度分析.pdf	0	27-Mar-24

#### 2.4.1.8 Documentation provided by Yokogawa Electric Corporation (Q25/01-223)

Doc ID	Document Description	Project Document Name	Version	Date
D129	Safety Requirements Specification	STR-CT4_YHQ-A049_r5_Safety_Requirements_of_ROTAMASS_TI.pdf	5	09-May-25
D130	Safety Requirements Review	STR-CT4_YHQ-G287_ROTAMASS_TI_Safety_Requirements_レビュー議事録_r2.zip	2	13-May-25
D131	Software Safety Requirements Specification	STR-CMNPF_4W-P040_RCCT4_SIL2_Software_Specification_r3.pdf	3	12-May-25
D132	Detailed Software Design Specification	STR-CT4_YHQ-P168_r3_ROTAMASS_TI_DR4_Update_実装報告書.pdf	3	13-May-25
D133	Design Review Record	STR-CT4_YHQ-P171796_r2_ROTAMASS_TI_HART_MODBUS_TCオプション_ファームウェア障害対策_最終レビュー1説明資料.pdf	2	15-May-25
D134	Verification Results	STR-CT4_YHQ-G182787_APP1_STR-CT4_YHQ-P168_ROTAMASS_TI_HART_DR4_Update_実装報告書_r2.pdf	2	03-Dec-24
D135	Requirements Traceability Matrix	STR-CT4_YHQ-P053_Rev.5_トレーサビリティマトリックス.zip	5	15-May-25
D136	Validation Test Plan	STR-CT4_YHQ-P172394_r1_ROTAMASS_TI_HART_Modbus_TuHCオプション_ファームウェア障害対策_Cランク設計変更_M-2024-1676111_検証計画書.pdf	1	15-May-25
D137	Validation Test Plan Review Record	STR-CT4_YHQ-G169575_r2_ROTAMASS_TI_HART_MODBUS_TuHCオプション_ファームウェア障害対策_検証計画レビュー(HART)議事録_M-2024-167611.pdf	2	16-May-25
D138	Validation Test Results	STR-CT4_YHQ-P172937_r1_ROTAMASS_TI_HART_Modbus_TuHCオプション_ファームウェア障害対策_Cランク設計変更_M-2024-167611_検証報告書.zip	1	15-May-25
D139	Safety Manual	STR-CT4_YHQ-A062-2_IM01U10D00-00EN-R_r10.zip	10	25-Jun-25
D140	Safety Manual Review	STR-CT4_YHQ-G284_r5_ROTAMASS_TI_Safety_Manual_レビュー議事録.pdf	5	26-Jun-25
D141	Impact Analysis Record	STR-CT4_YHQ-P171998_r0_ROTAMASS_TI_HART_DR4_Cランク設計変更(M-2024-167611)_影響度分析報告書.pdf	0	21-Apr-25

## 2.4.2 Documentation generated by *exida*

[R1]	Safety Case WB-61508 v1.7.2e_ROTAMASS TI Rev11-4.xlsm	SafetyCase Workbook for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter
[R2]	YEC 14-11-026 R001 V7R3 Assessment ROTAMASS TI.docx	Assessment Report for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter (this report)
[R3]	YEC 20-02-160 R002 V3R1 FMEDA ROTAMASS TI.pdf	FMEDA report for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter
[R4]	PIU-2015 Q14-110026 ROTAMASS RCCT4(RCCT3 result)_Rev2.xlsx	PIU Analysis for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter
[R5]	Q17-06-069 ROTAMASS TI Change Audit Checklist.xls	Change Audit Checklist for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter
[R6]	Q17-12-084 ROTAMASS TI Change Audit Checklist.xls	Change Audit Checklist for ROTAMASS TI Series Coriolis Mass Flow and Density Meter
[R7]	YEC 20-02-160 ROTAMASS TI Revised Certification PIU R1.xlsx	Field Failure Analysis for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter
[R8]	YEC 23-02-128 ROTAMASS TI R1 FFA.xlsx	Field Failure Analysis for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter
[R9]	YEC 24-02-079 ROTAMASS TI R1 FFA.xlsx	Field Failure Analysis for ROTAMASS Total Insight Coriolis Mass Flow and Density Meter

## 2.5 Assessment Approach

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

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. Proven-In-Use (PIU) assessment provides for the prevention of systematic failures for pre-existing devices with a proven history of successful operation. 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter. Other product development aspects prior to these modifications were assessed according to PIU requirements (see section 5.1.7). The combination of these assessments demonstrates full compliance with IEC 61508 to the end-user.

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
  - Activities and Responsibilities (Training and competence)
  - Configuration management
  - Tools and languages
- Safety Requirement Specification
- Change and modification management
- Software architecture design process, techniques and documentation
- Hardware 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.

The certification audit was done at Musashino, Tokyo on Jun 8, 2016.

### 3 Product Description

The ROTAMASS Total Insight Coriolis Mass Flow and Density Meter is designed to directly measure mass flow of liquids, liquids with solid content, multi-phase mixtures and some gases. The measurement system uses the Coriolis principle and is suitable for a wide range of continuous flow measurement applications in all branches of process technology.

ROTAMASS Total Insight has two components: the detector and the converter. The detector measures the mass flow directly and converts it into electrical signals. The converter evaluates the electrical signals and outputs the following values:

- mass flow, independent of media properties, such as density, temperature, viscosity
- fluid density
- fluid temperature



Picture 1. ROTAMASS Total Insight Coriolis Mass Flow and Density Meter

#### 3.1 Hardware and Software Version Numbers

This assessment is applicable to the following hardware and software versions of ROTAMASS Total Insight Coriolis Mass Flow and Density Meter:

Table 1. Hardware and Software Version Combination

Hardware Version	Software Version		
	Main	Sensor	Indicator
S1.01	R1.01.02	R1.01.03	R1.01.01
	R2.01.01		R2.01.01
	R3.01.01		R2.01.02
	R4.01.01	R1.01.04	R3.01.02
	R4.01.02		R4.01.01
	S2.01	R4.01.02	R4.01.02

## 4 IEC 61508 Functional Safety Assessment Scheme

*exida* assessed the development process used by Yokogawa Electric Corporation and ROTA Yokogawa GmbH & Co. KG 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 ROTAMASS Total Insight Coriolis Mass Flow and Density 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter is capable for use in SIL 2 or 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 not yet been assessed and audited, so modifications are not currently covered by this assessment. No modifications are permitted to the certified versions of the ROTAMASS Total Insight Coriolis Mass Flow and Density Meter without reassessment.

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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter was done per this IEC 61508 SIL 3 compliant development process. The Safety Case was updated with project specific design documents.

*exida* assessed failure history of the ROTAMASS Total Insight Coriolis Mass Flow and Density Meter [D23] 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter documents this assessment.

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

**The ROTAMASS Total Insight Coriolis Mass Flow and Density Meter complies with the relevant requirements of IEC 61508 SIL 2 and 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 [D04] and [D20].

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

##### FSM Planning

The functional safety management of any Yokogawa Electric Corporation Safety Instrumented Systems Product development is governed by [D02]. This process requires that Yokogawa Electric Corporation create a functional safety management plan [D20] or project plan which is specific for each development project. This plan defines all of the tasks that must be done to ensure functional safety as well as the person(s) responsible for each task. These processes and the procedures referenced herein fulfill the requirements of IEC 61058 with respect to functional safety management.

##### Version Control

All documents are under version control as required by [D07] and [D08].

#### Training, Competency recording

Competency is ensured by the creation of a competency and training matrix for the project [D13] and [D24]. The matrix lists all of those on the project who are working on any of the phases of the safety lifecycle. Specific competencies for each person are listed on the matrix which is reviewed by the project manager. Any deficiencies are then addressed by updating the matrix with required training for the project.

### **5.1.2 Safety Lifecycle and FSM Planning**

#### **Assessment**

The functional safety management plan 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. [D02], [D20]

The Software Development Procedure identifies the phases of the software development lifecycle and the inputs/outputs associated with each phase. [D16]

Manufacturer has a QMS in place. The Manufacturer has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure. [D01], [D05]

Updated ISO9001 certificate [D108] was reviewed by exida on Q23/02-128.

#### **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**

There is a document management system in place. This system controls how all safety relevant documents are changed, reviewed and approved. [D02], [D07], [D08], [D20]

All safety related documents are met the following requirements:

- Have titles or names indicating scope of the contents
- Contain a table of contents
- Have a revision index which lists versions of the document along with a description of what changed in that 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**

The FSM Plan lists the key people working on the project along with their roles. [D20]

A competency matrix has been created. [D24]

#### **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**

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. [D21]

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

#### **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.

### **5.1.6 Tools (and languages)**

#### **Assessment**

All off-line support tools have been classified as either T3 (safety critical), T2 (safety-related), or T1 (interference free). [D27]

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.

#### **Conclusion**

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

### **5.1.7 Proven In Use**

In addition to the Design Fault avoidance techniques listed above, a Proven in Use evaluation was performed on the ROTAMASS Total Insight Coriolis Mass Flow and Density Meter. Shipment records were used to determine that the ROTAMASS Total Insight Coriolis Mass Flow and Density Meter has greater than 1 billion operating hours and has demonstrated a field failure rate less than the predicted failure rates indicated in the FMEDA reports[R3].

#### **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 [R4] , [R7] on Q20/02-160, [R8] on Q23/02-128, and [R9] on Q24/02-079.

## **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**

The SRS provides a basis for tracking the fulfillment of the requirements. All element safety functions necessary to achieve the required functional safety are specified. [D28]

Updated SRS [D97] was reviewed by exida on Q21/07-100.

Updated SRS [D122] was reviewed by exida on Q24/02-079.

Updated SRS [D129] was reviewed by exida on Q25/01-223.

## **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 initiated with an Engineering Design Change procedure [D19]. 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter shall be audited by *exida* to confirm that a functional safety impact analysis was performed according to Yokogawa Electric Corporation's modification procedure.

*exida* confirmed that the change of Non-Safety part was done correctly according to Impact Analysis [D68] on Q17/06-069.

Impact Analysis [D82] was reviewed by exida on Q17/12-084.

Impact Analysis [D94], [D95] and [D96] were reviewed by exida on Q20/02-160.

Impact Analysis [D106] was reviewed by exida on Q21/07-100.

Impact Analysis [D111] and [D112] were reviewed by exida on Q23/02-128.

Impact Analysis [D119] was reviewed by exida on Q23/09-101.

Impact Analysis [D127] and [D128] were reviewed by exida on Q24/02-079.

Impact Analysis [D141] was reviewed by exida on Q25/01-223.

## **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 sub clause are to specify the design requirements for each E/E/PE safety-related system, in terms of the subsystems and elements.

### Assessment

The System Architecture Design describes that the behavior of the device when a fault is detected is to annunciate the detected fault through an external interface. [D29], [D30]

### 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 [D28] and [D30] has been partitioned into subsystems, and interfaces between subsystems are defined and documented. Design reviews [D29] 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.

#### 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 ROTAMASS Total Insight Coriolis Mass Flow and Density Meter, 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 [D54], and as part of the IEC 61508 assessment. The FMEDA had updated on Q20/02-160, Q21/07-100, Q23/02-128 and Q24/02-079.

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 uses Function Block Diagrams. [D41]

The Software Architecture Design contains a description of the software architecture.

A software criticality analysis and FMEA was performed and the report lists all components along with their criticality (Safety Critical, Safety Related, or Non-Interfering) and their required Systematic Capability. [D41]

[D99] and [D100] were reviewed by exida on Q21/07-100.

[D131] and [D132] were reviewed by exida on Q25/01-223.

### **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**

The Software Architecture Design uses semi-formal methods, such as Function Block Diagram and Data Flow Diagrams. Various design specifications represent software design sections. These designs were subject to review. [D42] – [D51]

[D71] and [D72] were reviewed by exida on Q17/06-069

[D79] and [D90] were reviewed by exida on Q17/12-084

[D99] was reviewed by exida on Q21/07-100

[D113], [D114] and [D115] were reviewed by exida on Q23/09-101.

[D134] was reviewed by exida on Q25/01-223.

### **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**

Test results are documented including reference to the test case and test plan version being executed. [D57], [D58], [D59] Test plan reviews were documented. [D60]

[D73] and [D74] were reviewed on Q17/06-069.

[D85], [D86] and [D87] were reviewed on Q17/12-084.

[D101], [D102] and [D103] were reviewed by exida on Q21/07-100.

[D116] was reviewed by exida on Q23/09-101.

[D136], [D137] and [D138] were reviewed by exida on Q25/01-223.

Calibration information is documented in the test results.

Test failures are documented in the test results with references to the change request made for the fix.

## **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**

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. [D66], [D67]

[D75] and [D76] were reviewed on Q17/06-069.

[D83] and [D90] were reviewed on Q17/12-084.

[D92] and [D93] were reviewed on Q20/02-160.

[D104] and [D105] were reviewed on Q21/07-100

[D109] and [D110] were reviewed on Q23/02-128.

[D117] and [D118] were reviewed by exida on Q23/09-101.

[D125] and [D126] were reviewed by exida on Q24/02-079.

[D139] and [D140] were reviewed by exida on Q25/01-223.

The Safety Manual gives guidance on recommended periodic proof test activities for the product, including listing any tools necessary for proof testing.

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 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 ( $1 \times 10^{-9}$ 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.
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 <sub>Avg</sub>	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 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
Q14/11-026	YEC 14-11-026 R001 V1, R0 Assessment ROTAMASS TI.docx	KT, 1-Jul-2016; Initial draft for review
Q14/11-026	YEC 14-11-026 R001 V1, R1 Assessment ROTAMASS TI.docx	KT, 11-Jul-2016; add Rota Yokogawa GmbH
Q14/11-026	YEC 14-11-026 R001 V1, R2 Assessment ROTAMASS TI.docx	KT, 12-Jul-2016; change from ROTAMASS to ROTAMASS TI
Q16/06-127	YEC 14-11-026 R001 V1, R3 Assessment ROTAMASS TI.docx	KT, 23-May-2017; Revised Certification
Q17/06-069	YEC 14-11-026 R001 V1, R4 Assessment ROTAMASS TI.docx	KT, 20-July-2017; Revised Certification
Q17/12-084	YEC 14-11-026 R001 V1, R5 Assessment ROTAMASS TI.docx	KT, 24-May-2018; Revised Certification
Q20/02-160	YEC 14-11-026 R001 V2, R0 Assessment ROTAMASS TI.docx	KT, 15-May-2020; Internal Draft for Revised Certification Update FMEDA and FFA
Q20/02-160	YEC 14-11-026 R001 V2, R1 Assessment ROTAMASS TI.docx	KT, 18-May-2020; Revised Certification released
Q21/07-100	YEC 14-11-026 R001 V3R2 Assessment ROTAMASS TI.docx	KT, 10-Feb-2023; Update after customer review
Q23/02-128	YEC 14-11-026 R001 V4R1 Assessment ROTAMASS TI.docx	KT, 23-May-2023; Update with HW parts modification
Q23/09-101	YEC 14-11-026 R001 V5R1 Assessment ROTAMASS TI.docx	KT, 12-Oct-23; Update with Indicator SW modification
Q24/02-079	YEC 14-11-026 R001 V6R1 Assessment ROTAMASS TI.docx	KT, 25-Apr-24; Update with HW modification

Q24/02-079	YEC 14-11-026 R001 V6R2 Assessment ROTAMASS TI.docx	KT, 19-Oct-24; Update section 2.3
Q25/01-223	YEC 14-11-026 R001 V7R1 Assessment ROTAMASS TI.docx	KT, 02-Jul-25; Update with SW modification.
Q25/01-223	YEC 14-11-026 R001 V7R2 Assessment ROTAMASS TI.docx	KT, 02-Jul-25, Release to customer
Q25/01-223	YEC 14-11-026 R001 V7R3 Assessment ROTAMASS TI.docx	KT, 14-Jul-25, Update after customer review

Review: V1, R3, John Yozallinas, May 23, 2017  
 V2, R0, Kaoru Sonoda, May 15, 2020  
 V3, R1, Kaoru Sonoda, February 8, 2023  
 V4, R1, Kaoru Sonoda, May 23, 2023  
 V6, R1, Kaoru Sonoda, April 25, 2024  
 V6, R2, Kaoru Sonoda, October 19, 2024  
 V7, R1, Kaoru Sonoda, July 02, 2025

Status: V7, R3 Released, July 14, 2025

### 7.3 Future Enhancements

At request of client

### 7.4 Release Signatures



Kiyoshi Takai, Evaluating Assessor



Kaoru Sonoda, Certifying Assessor

END OF DOCUMENT