Results of the IEC 61508 Functional Safety Assessment

Project:
3051SMV MultiVariable™ Transmitter

Customer:
Emerson Automation Solutions
(Rosemount, Inc.)
Shakopee, MN
USA

Contract No.: Q16/12-041
Report No.: R001 16-12-041
Version V1, Revision R1, July 12, 2017
Dave Butler

Management Summary

The Functional Safety Assessment of the Rosemount, Inc.

3051SMV MultiVariable™ Transmitter

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 Rosemount, Inc. 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 Rosemount, Inc.

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. 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 Rosemount, Inc. 3051SMV MultiVariable™ Transmitter development project, complies with the relevant safety management requirements of IEC 61508 SIL 3.

The assessment of the FMEDA, done to the requirements of IEC 61508, has shown that the 3051SMV MultiVariable™ Transmitter can be used in a low demand safety related system in a manner where the PFD_{AVG} is within the allowed range for SIL 2 (HFT = 0) per table 2 of IEC 61508-1.

The assessment of the FMEDA also shows that the 3051SMV MultiVariable™ Transmitter 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; Low demand applications only) or a SIL 3 safety function (with HFT = 1).

This means that the 3051SMV MultiVariable™ Transmitter 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

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 Rosemount, Inc. 6

2.4.2 Documentation generated by exida 7

2.5 Assessment Approach 7

3 Product Description 9

3.1 Variants and Software Versions 10

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 Safety Requirement Specification 14

5.1.3 Proven In Use 14

5.1.4 Safety Validation 14

5.1.5 Hardware Design Component Failure Analysis 14

5.1.6 Safety Manual 15

6 Terms and Definitions 16

7 Status of the document 17

7.1 Liability 17

7.2 Releases 17

7.3 Future Enhancements 17

7.4 Release Signatures 17

1 Purpose and Scope

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

- 3051SMV MultiVariable™ Transmitter

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 relevant 3051SMV MultiVariable™ Transmitter processes, procedures and techniques as implemented for the safety-related deliverables with the managerial requirements of IEC 61508 parts 1, 2 and 3 for SIL 3;

and

- the 3051SMV MultiVariable™ Transmitter 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 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

Rosemount, Inc.	Manufacturer of the 3051SMV MultiVariable™ Transmitter
exida	Performed the hardware assessment [R3]
exida	Performed the Functional Safety Assessment [R1] per the accredited *exida* certification scheme.

Rosemount, Inc. 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 Rosemount, Inc.

Doc. ID	Typical Name
D001	Quality Manual
D003	Overall Development Process
D004	Configuration Management Process
D005	Field Failure Reporting Procedure
D006	Field Return Procedure
D007	Manufacturer Qualification Procedure
D008	Part Selection Procedure
D010	Quality Management System (QMS) Documentation Change Procedure
D012	Non-Conformance Reporting procedure
D013	Corrective Action Procedure
D016	Action Item List Tracking Procedure
D019	Customer Notification Procedure

Doc. ID	Typical Name
D021	Software Development Process
D021b	Software Tool Qualification Procedure
D023	Modification Procedure
D023b	Impact Analysis Template
D030	Shipment Records
D031	Field Returns Records
D036	ISO 900x Cert or equivalent
D040	Safety Requirements Specification
D047	Schematics / Circuit Diagrams
D055	FMEDA Report
D059	Fault Injection Test Plan
D069	Validation Test Plan
D071	Environmental Test Plan
D072	EMC Test Plan
D074	Validation Test Results
D075	Environmental Test Results
D076	EMC Test Results
D077	Fault Injection Test Results
D078	Operation / Maintenance Manual
D079	Safety Manual
D083	PIU Analysis

2.4.2 Documentation generated by *exida*

[R1]	ROS 16-12-041 V1R0 SafetyCaseWB - 3051SMV.xlsm	SafetyCaseWB file for 3051SMV MultiVariable™ Transmitter
[R2]	ROS 16-12-041 R001 V1R1 Assessment Report 3051S MV	IEC 61508 Functional Safety Assessment for 3051SMV MultiVariable™ Transmitter (This document)
[R3]	ROS 09-05-36 R001 V3 R1 FMEDA Model 3051SMV	FMEDA report
[R4]	Q16-12-041 3051SMV Certification Proposal	Assessment Plan Agreement
[R5]	ROS 16-12-041 PIU001 V1R0 PIU Analysis - 3051S MV	Proven-in-Use Analysis

2.5 Assessment Approach

The certification audit was performed by assessing the compliance of the product and its development with respect to a relevant subset of the requirements in the accredited *exida*

certification scheme. The assessment was planned by *exida* and agreed with Rosemount, Inc. (see [R4]).

For designs that have been in service for several years and have demonstrated themselves in a variety of applications and conditions, a proven in use assessment may be able to be used as a substitute when evidence that the product development followed a fully compliant IEC 61508 design process cannot be provided. This product has been assessed per the IEC 61508 Proven-in-Use route (2_S) requirements.

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 3051SMV MultiVariable™ Transmitter, the following evidence aspects have been reviewed:

- FMEDA
- Product specification
- Safety manual
- Instruction manual
- Hardware fault inject test plan and results verification
- EMC and environmental test report
- Validation test results
- Corrective Action and prevention action plan/process
- Software and hardware drawings release process
- Procedures to record and analyze product operational hours and field failures (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 3051SMV MultiVariable™ Transmitter, many IEC 61508 functional safety assessment requirements are satisfied without further documented evidence, including:

- 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 Rosemount 3051SMV Multivariable Transmitter is a two-wire 4 – 20 mA smart device used in multiple industries for both control and safety applications. For safety instrumented systems (SIS) usage it is assumed that the 4 – 20 mA output is used as the primary safety variable. The Transmitter contains self-diagnostics and is programmed to send its output to a specified failure state, either high or low, upon internal detection of a failure (output state is programmable). The device is equipped with or without display.

Figure 1 provides an overview of the 3051SMV Transmitter and the boundary of the FMEDA.

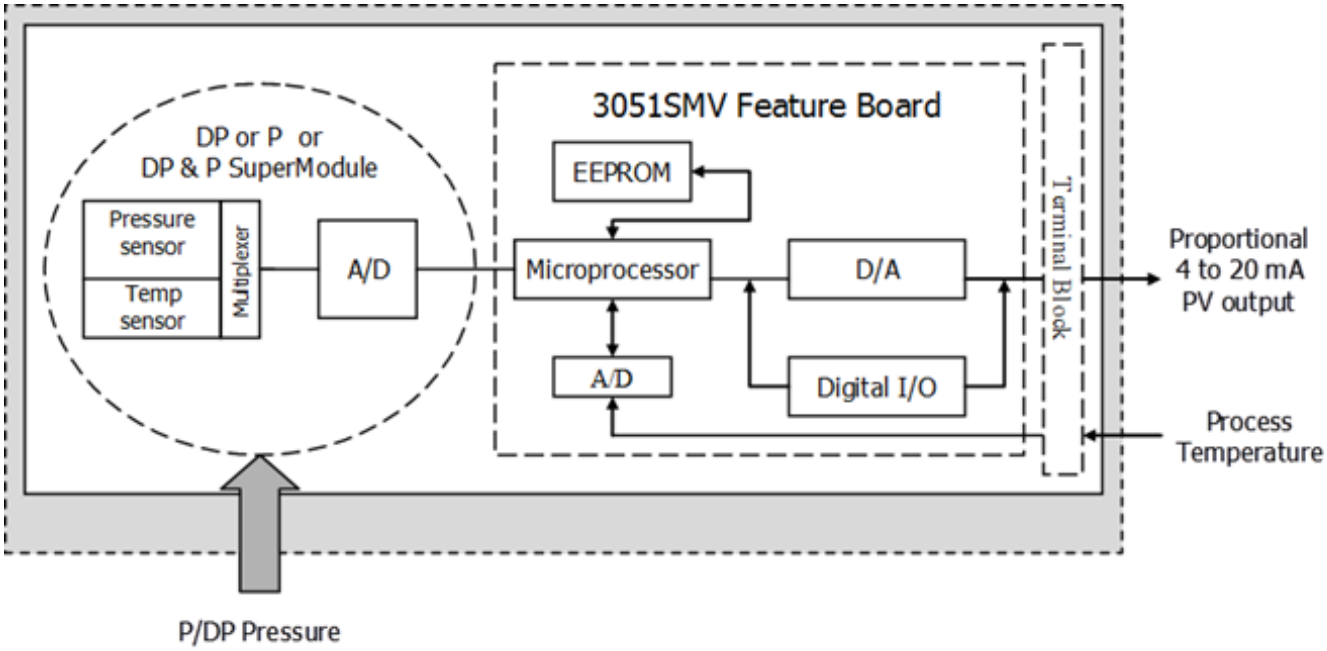


Figure 1 3051SMV Transmitter

The assessment includes 8 different configurations of the 3051S MultiVariable transmitter. Table 1 lists the models and versions of the 3051SMV transmitter that have been considered for the assessment. The different configurations include the following:

- Two different Feature Boards of Direct Process Variable Measurement and Fully Compensated Mass, Volumetric, and Energy Flow
- Three different measurements of Differential Pressure (DP), Static Line Pressure (P), and Process Temperature (T)
- Two different configurations in the 3051S Super Module Platform of Coplanar and In-Line Static Pressure (P) and Process Temperature (T)

3.1 Variants and Software Versions

This assessment is applicable to the following model variants of 3051SMV MultiVariable™ Transmitter:

3051SMV_P1	Rosemount 3051SMV, Direct Process Variable Measurement using DP and P with Process Temperature
3051SMV_P2	Rosemount 3051SMV, Direct Process Variable Measurement using DP and P without Process Temperature
3051SMV_P3, 3051SMV_P5, 3051SMV_P6	Rosemount 3051SMV, Direct Process Variable Measurement using DP or P with Process Temperature
3051SMV_P4, 3051SMV_P7, 3051SMV_P8	Rosemount 3051SMV, Direct Process Variable Measurement using DP or P without Process Temperature
3051SMV_M1	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P with Process Temperature
3051SMV_M2	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P without Process Temperature
3051SMV_M3	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP with Process Temperature
3051SMV_M4	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP without Process Temperature

Table 1 - Version Overview

There are also three 3051SMV MultiVariable™ Transmitter flowmeter options:

- Rosemount™ 3051SFA which uses the Rosemount 485: Annubar™ Primary Element
- Rosemount™ 3051SFC which uses the Rosemount 405: Compact Conditioning Orifice Plate Primary Element
- Rosemount™ 3051SFP which uses the Rosemount 1195: Integral Orifice Primary Element

Figure 2 provides an overview of the 3051SMV with primary element and the boundary of the FMEDA.

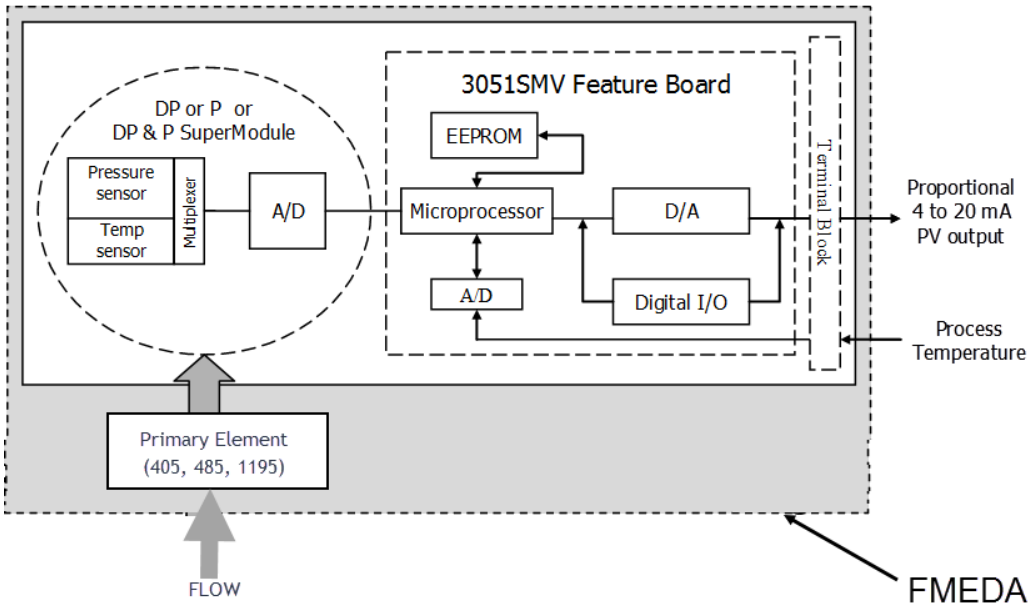


Figure 2 3051SMV with Primary Element, Parts included in the FMEDA

Table 2 lists the versions of the 3051SMV transmitter flowmeter options that have been considered for the assessment.

Table 2 Version Overview, 3051SMV with Primary Element

3051SFA1, 3051SFC1, 3051SFP1	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P with Process Temperature
3051SFA2, 3051SFC2, 3051SFP2	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP and P without Process Temperature
3051SFA3, 3051SFC3, 3051SFP3	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP with Process Temperature
3051SFA4, 3051SFC4, 3051SFP4	Rosemount 3051SMV, Fully Compensated Mass and Energy Flow using DP without Process Temperature
3051SFA5, 3051SFC5, 3051SFP5	Rosemount 3051SMV, Direct Process Variable Measurement using DP and P with Process Temperature
3051SFA6, 3051SFC6, 3051SFP6	Rosemount 3051SMV, Direct Process Variable Measurement using DP and P without Process Temperature
3051SFA7, 3051SFC7, 3051SFP7	Rosemount 3051SMV, Direct Process Variable Measurement using DP or P with Process Temperature

This assessment is applicable to the following software version for the models listed in Table 3.

3051SMV	
Software/Firmware	3

Table 3 - Software Version

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 Rosemount, Inc. [section 2.4.1] and is documented in the safety case [R1].

4.1 Product Modifications

The modification process that impacts the safety function has not yet been assessed and audited for this product, so modifications to the safety function are not currently covered by this assessment. No modifications to the safety function are permitted to the certified versions of the 3051SMV MultiVariable™ Transmitter without reassessment.

5 Results of the IEC 61508 Functional Safety Assessment

exida assessed a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) [R3] of the 3051SMV MultiVariable™ Transmitter to document the hardware architecture and failure behavior. The FMEDA report and the Safety Case created for the 3051 SMV documents this assessment.

exida assessed failure history of the 3051SMV MultiVariable™ Transmitter [D030, D031] and performed a detailed analysis of the data provided [R5]. This PIU assessment (route 2_S) is done in place of a detailed functional safety assessment (route 1_S) for systematic failures. The Safety Case created for the 3051 SMV documents this assessment.

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

The 3051SMV MultiVariable™ Transmitter 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

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

FSM Plan

The manufacturer has a quality management system in place. The manufacturer has been ISO 9001 certified. All sub-suppliers have been qualified through the Manufacturer Qualification procedure.

The product has limited functionality that is restricted by configuration.

The PIU report shows that the actual field failure rate, based on field returns within the warranty period, is lower than the expected failure rate as calculated in the FMEDA. The environmental specifications and the function of the product are generally the same as the fielded version. The PIU report also shows that the number of hours achieved meets the minimum required for the given SIL.

Documentation

All documents are under version control as required by [D001 and D010]. 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.

The objectives of the standard are fulfilled by the Rosemount, Inc. functional safety management system, safety lifecycle processes and supported by PIU analysis.

5.1.2 Safety Requirement Specification

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

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

Protection against unauthorized modifications is properly implemented.

5.1.3 Proven In Use

In addition to Design Fault avoidance techniques, a Proven-in-Use evaluation was performed on the 3051SMV MultiVariable™ Transmitter. Shipment records were used to determine that the 3051SMV MultiVariable™ Transmitter has greater than 30 million operating hours. The product has been shipping for at least 18 months without any revisions or changes, based on the assumption that installation takes six months. The software has the same operational profile for all field installations that were used to calculate PIU hours. The PIU report [R5] 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. There are no functions that are not covered by the PIU demonstration.

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] and [R4]). This provides justification for using a Route 2H approach.

5.1.4 Safety Validation

One or more test cases, or analysis documents, exist for each safety requirement. 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.

Functional and performance test results show that the product has been designed to function properly within its specified environmental limits. The results have been verified.

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.

5.1.5 Hardware Design Component Failure Analysis

Hardware architecture design has been partitioned into subsystems, and interfaces between subsystems are defined and documented. To evaluate the hardware design of the 3051 SMV, a Failure Modes, Effects, and Diagnostic Analysis (FMEDA) was performed by *exida* for each component in the system. This is documented in [R3].

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} or PFH of other devices of a Safety Instrumented Function (SIF) to determine suitability for a specific Safety Integrity Level (SIL).

5.1.6 Safety Manual

The product Reference Manual is provided and identifies and describes the functions of the product, and includes the Safety Manual information required by IEC 61508. 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 is provided to facilitate the development of an external diagnostics capability (output monitoring).

The Reference Manual identifies the hardware and software configuration of the product (part numbers, version numbers, etc.) to provide the device user with information about exactly what device to use in a Safety Instrumented Function (SIF).

The Reference Manual states the diagnostic test interval of the product.

The Reference Manual gives guidance on recommended periodic (offline) 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 Reference Manual.

The Reference Manual includes valuable information for the user of the device regarding safe operation and avoidance of hazards. It considers user/maintenance friendliness, limited operation modes, and protection against operator mistakes.

6 Terms and Definitions

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode where the demand interval for operation made on a safety-related system is greater than twice the proof test interval.
High demand mode	Mode where the demand interval for operation made on a safety-related system is less than 100x the diagnostic detection/reaction interval, or where the safe state is part of normal operation.
PFD_{AVG}	Average Probability of Failure on Demand
PFH	Probability of dangerous Failure per Hour
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).
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.

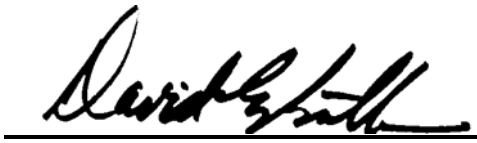
7.2 Releases

Version History:	V1, R1:	Added primary elements, R. Chalupa, 2017-07-12
	V1, R0:	Initial Version Dave Butler, 5/31/2017
Authors:	Dave Butler	
Review:	Loren Stewart	
Release status:	Released	

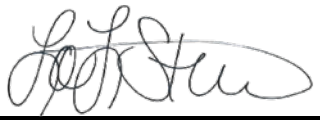
7.3 Future Enhancements

At request of client.

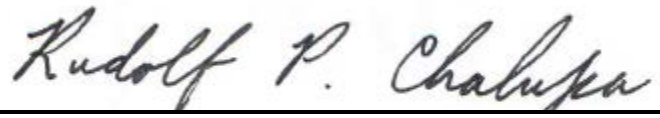
7.4 Release Signatures



David Butler, CFSE, Senior Safety Engineer



Loren L. Stewart, CFSE, Senior Safety Engineer



Rudolf P. Chalupa, CFSE, Senior Safety Engineer