Functional Safety Certification Scheme Description

QD-008

December 3, 2020

Version 3 Revision 3

Confidential Information

1 Contents

2 Purpose of the Document:

This document describes the *exida* Functional Safety Certification Scheme.

3 Scope:

The scope covers all the steps in the Functional Safety Certification Scheme.

4 Certification Scheme Elements

4.1 Key Milestones

The following are key milestones in an Functional Safety Certification project and consequently measures of success.

- *exida* will complete a technical analysis (or review a technical analysis performed by Customer Company for the Product and issue a report indicating how well the design meets technical requirements of the standard.
- If the basis of the Functional Safety assessment includes field experience, *exida* will perform a “Proven in Use” investigation and complete a Proven In Use Report in compliance to Functional Safety requirements.
- *exida* will perform a complete review of current design and testing processes and issue a gap analysis report indicating how well the current processes meet the process requirements of the Functional Safety standard(s). The review will include an onsite audit and Functional Safety training if necessary.
- *exida* will complete a full Safety Case using the *exida* Safety Case tool which will serve as the collection place of specific Functional Safety requirements, arguments why these requirements are met for the Product. As such the Safety Case will form the basis for the eventual Functional Safety certification.
- *exida* will represent Customer Company during the Functional Safety certification audit which will be conducted by an independent certification assessor from *exida*.

4.2 Value to Customer Company

exida has supported a large number of manufacturers in their endeavors to achieve Functional Safety certification for their products. The *exida* approach has proven very effective in getting manufacturers up to speed on the Functional Safety requirements and in the preparation of specific Functional Safety required evidence artifacts. Specifically the value *exida* brings to Customer Company includes:

Market Support including:

Listing on the *exida* Safety Automation Equipment List

Inclusion as a listed product in the market leading exSILentia SIL Verification Tool

News Release, etc.

4.3 *exida* Methodology

To successfully achieve product certification to Functional Safety there are two distinct areas of focus that need to be addressed, assessment and certification. During the assessment phase, one or more *exida* safety engineers will work very closely with the Customer Company development team providing any requested training, reviewing, or performing reliability analyses, and compiling/reviewing the final Safety Case. At the end of this phase the product and organization is ready to proceed to the certification phase.

In the certification phase an independent *exida* assessor will review the product and work done during the analysis phase. To ensure strict adherence to international practices the *exida* assessor will not be involved in any part of the assessment phase and reports to an independent department, *exida* Certification. As such the assessor will have limited to no knowledge of any steps taken as part of the assessment phase. Customer Company may opt to have the assessment engineer present during the Functional Safety audit performed by the independent *exida* assessor.

The project estimates outlined below represent both the assessment and certification phases of the project.

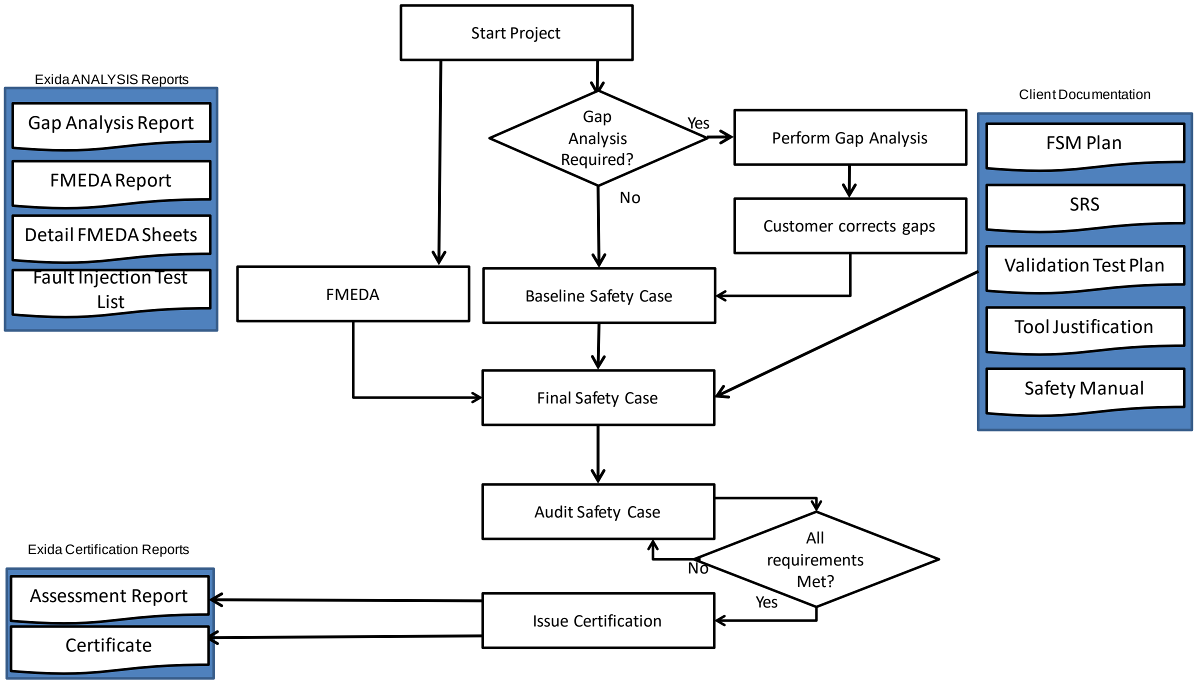

Figure 1 Functional Safety Typical Certification Process

4.4 Referenced Standards

Each project may follow one or more Functional Safety standards as requested by the Customer Company. The latest version of all referenced standards shall be used. IEC 61508 is the basic safety publication and will be used in most projects along with addtional industry specific standards. In addition, specific requirements as approved by the Advisory Board must be met. For Functional Safety, additional requirements of this Scheme are:

a. Surveillance Audits done periodically to verify continued compliance.

b. Publication of failure rates for all failure modes including false trip rates as these are very important to system users even when not required by the standard.

c. When applicable, practical proof test procedures designed to detect failures not detected by automatic diagnostics.

4.5 Scope of the Service

Our services offered herein include Functional Safety assessment and certification services. An overview of services and their deliverables is provided below.

4.5.1 Development Lifecycle Services

A. Process Analysis

The process analysis is an initial step where an *exida* engineer will typically review the Customer Company's quality management system procedures. Once it has been established that the quality management system procedures are in compliance to Functional Safety, the Baseline Safety Case is created.

The basis of the Functional Safety certification of the Customer Company Product is a detailed Safety Case. On the basis of the Process Analysis an *exida* engineer will populate the Safety Case using the *exida* Safety Case tool. The deliverable from this task will be a list with detail action items that need to be completed in order to complete the Process Analysis Phase and continue with the certification project. The Baseline Safety Case will reference Customer Company development process documents, such that it can serve as complete stand alone Functional Safety compliance body of evidence. Once the major process gaps have been resolved by Customer Company, the project may proceed. Note: Specific document templates, books and targeted training are available for most common "gap" issues.

B. Creation of Proven-in-Use Analysis

For existing products with field operating history, an *exida* engineer will review in detail the shipping and returns history of the products. The *exida* engineer will evaluate the existing return process, the details of the failure analysis, and document how the existing product has been sufficiently free of defects to be utilized in a safety rated application. The results of the Proven-In–Use Analysis will be added to the Safety Case.

C. Audit and 61508 Familiarity Session

When all the process gap issues have been addressed, an audit meeting is scheduled. The meeting is expected to be conducted over 1-2 days. During the visit the *exida* engineer will review the existing development procedures in detail and interview the respective responsible parties to discover how the process has been applied to the Product. This information is entered into the Safety Case. If there are any audit findings, a gap report is issued.

If Customer Company relevant personnel are not familiar with Functional Safety, *exida* will conduct a familiarity session. Personnel attending the session will gain a basic understanding of Functional Safety.

D. Safety Concept / Architecture Analysis Audit

In a meeting, the Customer Company presents the overall product architecture design and describe the operation of each hardware and software block. A Failure Modes and Effects Analysis (FMEA) is reviewed and completed to show the safety mitigation of block functional failures. The results are entered into the Safety Case.

E. Performing Detailed Analysis on Product Hardware

1. Perform Detailed FMEDA on Product

The detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) is a technique used to evaluate the reliability and safety integrity of a given product. Based on the functional failure modes and mitigations identified in the FMEA, an FMEDA does component level analysis and impact of the component failure modes. The results of a FMEDA analysis are a set of failure rates, proof test coverage factors, and useful life that can be used to determine product and overall SIF probability of failure.

The FMEDA analysis may be supported by means of fault injection testing where specific component failures are simulated to confirm the existence of assumed diagnostics and/or to determine exact behavior in situations where that behavior is not trivial from the design.

As part of this task, an *exida* engineer will review the detailed assembly drawings of the Product and either review an existing Failure Modes, Effects, and Diagnostics Analysis or perform a new FMEDA. The deliverable of this task is the final Product FMEDA report which will be part of the evidence documents that will be recorded in the final Safety Case. The *exida* FMEDA report is estimated to be 10 -15 pages in length. Customer Company will be able to provide this document to its customers for those customers who need to perform SIL verification calculations. The data will be entered into the *exida* exSILentia tool. This will make it very easy for customers to perform the calculations.

2. Conducting of Fault Injection Testing on Product

If necessary, the *exida* engineer will prepare a list of fault injection tests that need to be performed to confirm the FMEDA analysis. Based on the Fault Injection Test list generated the actual fault injection tests need to be executed. Test reports should indicate among others test, expected results, and actual results. The fault injection tests can be executed by Customer Company or by an *exida* engineer either on site or on the *exida* premises. The fault injection test results (If performed) will be incorporated in the original FMEDA analysis and report.

If fault testing is required or requested, *exida* time will be billed on a per hour basis at the daily rate assuming an 8 hour day.

3. Providing of detailed FMEDA Results (Optional)

The *exida* FMEDA is a product specific FMEDA report. Detailed FMEDA results are not provided. Customer Company can opt to receive the detailed FMEDA results in PDF format or a full spreadsheet file that accomplanies a license for the *exida* FMEDAx^{TM} tool. The detailed FMEDA results will provide component level detail failure mode classifications and could be useful for on-going maintenance of the FMEDA by Customer Company. Up to 4 hours of *exida* certification services to review the FMEDA details are included with the purchase of the detailed FMEDA results. Subsequent certification services will be billed on a per hour basis at the daily rate assuming an 8 hour day.

Note: A review of the detailed FMEDA results will only be conducted if the detailed FMEDA results are purchased.

4. Stress-Strength Analysis of specific parts (Optional)

The *exida* FMEDA is done with our standard component database. If there are special design considerations or "high strength" parts used, *exida* can perform specific part analysis based on design parameters, stress test reports and field failure data to obtain special part failure rates and failure modes. While this is normally not a justified expense, in certain cases it may be desired by Customer Company.

F. Safety Manual

The Safety Manual (SM) is the key communication mechanism between Customer Company and the users of the Product. The document must list any application restrictions or limits, specific maintenance requirements if applicable, useful life of the Product, and many other items. The Safety Manual is one of the key development process deliverable documents which will receive detailed scrutiny during the final audit. The Safety Manual can be a separate manual or can be incorporated in an existing user manual. It must be delivered with the Product or otherwise be made available (through the Customer Company website, for example).

If this is a first time certification for Customer Company, a Safety Manual may not exist. Therefore, the Customer Company has the option of having an *exida* engineer provide a generic Safety Manual template. The Customer Company shall include the Safety Manual information in the Product user documentation or in a separate Safety Manual that is in the Customer Company document format.

If a Safety Manual already exists for the Product, an *exida* engineer will review the existing Safety Manual to determine if it meets the requirements of IEC 61508.

G. Preparation of Final Safety Case

As explained, the basis of the *exida* Functional Safety certification of the Customer Company Product is a detailed Safety Case. In this task an *exida* engineer will update the Baseline Safety Case by including the solutions to all open action items and all analysis work done in the project. In addition, the final Safety Case should contain the actual Product development documents that the Functional Safety Management Plan claimed would be created to ensure a full Functional Safety compliant development process. The Preparation of Final Safety Case task will be performed remotely. If all solutions are correct and all analysis work complete, the deliverable will be the final Safety Case that will be provided to the assessor in the form of an electronic Safety Case file. If there are non-compliant items found in the Final Safety Case preparation, the deliverable will be a report showing the items of non-compliance. If authorized, this step may then be repeated until full compliance is achieved.

4.6 Certification Services

The Certification Services offered include a Project Audit, also referred to as the Final assessment audit. The deliverable of the Project Audit is an assessment report stating the concluded Functional Safety compliance level. If the Project Audit concludes that the Product and its development process meet the relevant requirements of Functional Safety, Functional Safety compliance certificates will be issued in addition to the assessment / certification report. Both the assessment report and the Functional Safety compliance certificates will be made publicly available through the *exida* Safety Automation Equipment List (www.sael-online.com).

If the Project Audit reveals areas of non-compliance, it is up to the assessor's discretion to either create an action item list or conclude that the Product failed the assessment. Provided that Customer Company resolves all outstanding action items satisfactorily within a reasonable time period, the assessment will be concluded positively. If the action items are not resolved satisfactorily or if the assessor immediately concludes that the Product failed the assessment, an assessment report will be issued indicating the reasons for audit failure. Note that this report will not be made public.

Once an assessment report is issued the project is considered finalized. If the Product failed the assessment, Customer Company may request that *exida* submit a quote to continue the certification process.

4.7 Certification Renewal

A Certification has a validity period of between one to three years. Before the end of the validity period the Customer Company must undergo a Surveillance Audit where continued compliance is audited. If the Certificate is not renewed, it will be suspended and references will be removed from the Safety Automation Equipment List (SAEL). *exida* will provide a proposal for Surveillance Audit services on request.

When a new version of a referenced standard is released, the Customer Company may renew two times under the old standard. After that time, the certification must be upgraded to the new version of the standard.

4.8 *exida* Project Team and Expertise

exida delivers lifecycle services, coaching, tools, and training to support users, manufacturers and engineering contractors in the cost-effective use of new technology for safety-related and highly dependable applications. At *exida* the project will be managed and executed by one of our senior safety engineers with support of other staff. If desired, *exida* would be happy to provide you with references and technical CV of our partners and associates.

4.9 Customer Company Involvement Expectations

A successful Functional Safety audit can only be achieved through dedicated Customer Company involvement in the various steps part of the development lifecycle services phase of this project. It is expected that Customer Company will provide evidence artifacts that are need for successful passing of the Functional Safety audit. It is up to Customer Company to determine the desired involvement of *exida* in analysis / review or training on those artifacts. The *exida* involvement can be limited to just the creation of the Safety Case, or could be as extensive as assisting with detailed review of the existing Customer Company development procedures, tailored training on those procedures, and providing a variety of template documents. If Customer Company decides to be responsible for specific deliverables, these are expected to be provided promptly per a defined schedule. If *exida* is responsible for certain deliverables, Customer Company should review and provide feedback to those deliverables within one week of completion. If no comments are received within this period the deliverables are considered final.

If needed, Customer Company may submit samples for testing. Depending on the type of certificate being issued samples may be prototypes or may be production pieces. Customer Company may at any time witness testing being conducted by *exida*.

If Customer Company submits sample products for testing it is the responsibility of Customer Company to assure that the test samples are fit for use prior to placing in service.

4.10 Certification Appeals and Complaints

Customer Company has the right to formally appeal any certification decision. Any appeal request should be directed to the *exida* Quality Manager.

Customer Company also has the right to submit a complaint to the *exida* Quality Manager regarding any aspect of the certification process.

4.11 Customer Agreement Requirements:

During the evaluation and certification period Customer Company must agree:

- to fulfill the certification requirements, including implementing appropriate changes when they are communicated by *exida*,
- that the certified product will continue to meet the product requirements,
- to provide evidence artifacts that are need for evaluation and surveillance Functional Safety audit,
- to provide access to relevant equipment, locations, areas, personnel and Customer Company subcontractors,

- to make claims regarding certification consistent with the scope of certification,
- to observe and comply with the applicable sections of Functional Safety,
- to keep a record of all complaints known to the Customer Company relating to the product's compliance with the requirements of the applicable standards and to make these records available to *exida* when requested,
- to take appropriate action with respect to complaints and deficiencies found in products or services that affect compliance with the applicable standards and to document the actions taken and to make said documentation available to *exida* upon request,
- to provide access to investigation of complaints,
- to notify *exida*, without delay, of any changes to the product and/or processes that would affect the safety function of the Product,
- to assure that the test samples, if submitted, are fit for use prior to placing in service,
- that the changes to the Product, including any modifications or enhancements to the hardware, software, firmware or mechanical design that might impact the ability to meet certification requirements are fully evaluated,
- that all changes shall follow the approved certified change process,
- that changes will be audited at the end of the validity period indicated on the certificate,
- to change one or more publicly disclosed identifiers to indicate to customers that any safety critical change has been made to the Product,
- to use the Certificate or Report only with respect to the Product,
- to not change a Certificate or Report or use a Certificate or Report in any way that might be deceptive or misleading or may bring the certification body into dispute,
- to, upon suspension, withdraw or termination of certification, discontinue its use of all advertising matter that contains any reference thereto and to discontinue the use of the certification mark, and
- to only provide copies of the certificate(s) and assessment report(s) to others in their entirety.

4.12 Use of the Certificate or Report

- Upon successful completion of a certification project, *exida* will grant to Customer Company a limited, restricted, non-exclusive, royalty-free non-transferable, non-assignable, revocable license to use the Certificate or Report only with respect to the Product.
- During the period of validity, *exida* will maintain a public web-accessible record of all certificates and reports. Customer Company understands and agrees that the Certificate

and Report for the Product will be part of this public record. Customer Company will have the opportunity to add a link to their web-site and to post contact information for potential customers. *Exida* will remove a Certificate and Report from the web-accessible record if the certification is revoked. *exida* may in its discretion change the web-accessible record and the information regarding listed devices.

4.13 Use of the Certification Mark

Upon successful completion of a certification project, *exida* will grant to Customer Company a limited, restricted, non-exclusive, royalty-free non-transferable, non-assignable, revocable license to use the certification mark (Mark) per the restrictions and requirements set forth in the scheme.

Customer Company may use the mark only in association with the Product that is subject to the certification while the certification is valid. If the certification is revoked or expires without renewal, Customer Company will immediately cease using the Mark in association the Product and will promptly destroy all advertising, marketing and promotional materials, product literature and packaging relating to the Product that contain the Mark.

Customer Company acknowledges that Mark and all associated goodwill are owned by *exida* Certification L.L.C. and agrees that no right, title or interest in the Mark shall be acquired other than the limited license set forth above.

4.14 Right to suspend or withdraw the certificate

exida has the right to withdraw its certificates if one of the following conditions are met:

- Customer Company made false claims, either by giving false information orally or through documentation provided;
- Customer Company modified their product or functional safety management system in breach of the requirements set out in the *exida* certification guide;
- Customer Company fails to take appropriate action to mitigate a complaint of a certified device that is found to affect the conformance to the certification requirements;
- The standard used as a basis for certification has been amended or withdrawn because of serious safety concerns and the product or functional safety management system is affected by such amendment;
- Customer Company has failed to resolve issues identified during the surveillance audit within a reasonable period, see the *exida* certification guide.
- Customer Company makes misleading or unauthorized statements regarding the product certification. This is applicable to any verbal communication and/or any communication media.
- Customer Company uses the product certification in a misleading manner.

Upon withdraw of certification, *exida* will notify Customer Company to discontinue use of the certification mark and any advertising that contains reference to the certification and to return any certification documentation requested by *exida*.

exida has the right to suspend its certificate if it is not renewed before the validity period expires. If suspended, *exida* will communicate the following to the Customer Company:

- Actions needed to end suspension and restore the certification for the Product in accordance with the certification scheme;
- Any other actions required by the certification scheme.

5 Document Status: Released

6 Author(s)

Version	Revision	Author	Date
V1	R1	Steven Close	12/2/2015

7 Revisions

Version	Revision	Change	Changed By	Date
V2	R1	Revised section 5 to include extended or reduced scope.	Steven Close	11/13/2018
V3	R1	Revised section 5.10	Steven Close	11/7/2019
V3	R2	Updated document	William Goble	11/25/2020
V3	R3	Added new version of standard clause in 4.7	William Goble	12/03/2020

8 Approvals

Version	Revision	Approved By	Approval email	Date
V1	R1	Ted Stewart	✉	12/2/15
V2	R1	Ted Stewart	✉	11/14/2018

V3	**R2**	**R. W. Fuss**	RWF	**11/27/2020**
V3	**R3**	**R. W. Fuss**	**RWF**	**12/3/2020**