Functional Safety Certification Scheme Description

QD-008
November 14, 2018
Version 2 Revision 1

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

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.

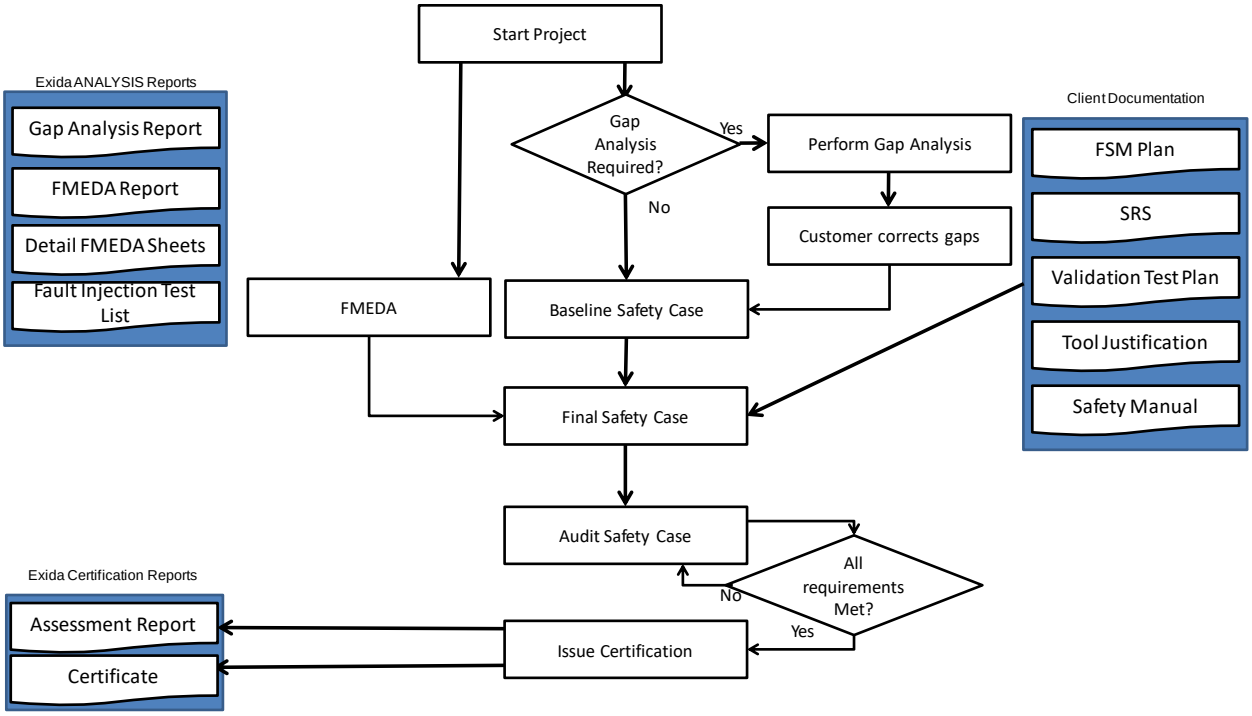

Figure 1 Functional Safety Typical Certification Process

4.4 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.

4.4.1 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. It is assumed that the Product have the same design and development procedures.

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 embed 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, 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. This approach is one of the alternative techniques from Functional Safety for pre-existing products.

C. On-site Audit and 61508 Familiarity Session

When all the process gap issues have been addressed, an on-site audit meeting is scheduled. The onsite 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. 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. The results of a FMEDA analysis are a set of failure rates and useful life that can be used to determine product and overall SIF probability of failure. The diagnostic coverage factor for a prescribed proof test is also analyzed. For products that fulfill the requirements of an element, the results of the FMEDA will allow determination of the Safe Failure Fraction (SFF), a performance parameter that may identify the required level of Hardware Fault Tolerance (HFT) needed for a given SIL level.

During the FMEDA analysis assumptions are made with regard to the existence and effectiveness of automatic diagnostics. 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.

As part of this service Customer Company is entitled to a second release of the FMEDA report. This is to take into account any errors, corrections or omissions in the first release. Subsequent releases will be billed on a per hour basis at the daily rate assuming an 8 hour day.

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. This proposal assumes testing will be done by Customer Company.

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 as part of the D-3 deliverable. Customer Company can opt to receive the detailed FMEDA results in PDF format. 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.

E. 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.

F. 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.

4.5 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.

Any subsequent Project Audits, including change process audits once the first set of modifications to the Product after certification and release are made, are outside the scope of this quote.

5 Project Estimate and Conditions

Work-item	Fixed Estimate
Development Lifecycle Services	
A. Process Analysis	
B. Creation of Proven-in-Use Analysis	
C On-site Audit and 61508 Familiarity Session	
D. Performing Detailed Analysis on Product Hardware	-
1 Perform Detailed FMEDA on Product	

2. Conducting of Fault Injection Testing on (if required or requested).	
3. Providing of detailed FMEDA Results (Optional)	
4. Stress-Strength Analysis of specific parts (Optional)	
E. Safety Manual Generic Template (Optional)	
F. Preparation of Final Safety Case	
4.5 Certification Services	
Functional Safety Certification Product **a. Project Audit and Review Meeting** **b. Assessment Report and certificate (if all requirements are met)**	

Fees for each work item are documented in the proposal. Customers are invoiced at the completion of each work item. If Travel is anticipated for the completion of this project, travel costs and out of pocket expenses will be invoiced at cost plus 10%.

All amounts payable to *exida* are payable in full without making any deduction or withholding. If Customer Company is prohibited by law from making payments free of deductions or withholdings, Customer Company will pay such amounts to *exida* as may be necessary to ensure that the actual amount received by *exida* after deduction or withholding and after any payment of any additional Taxes or other charges due as a consequence of the payment of such additional amounts will equal the amount that would have been received by *exida* if such deductions or withholdings were not required.

Customer Company has the right to cancel the contract with *exida* at any time. *exida* has the right to cancel the contract with Customer Company at any time if required input from Customer Company is not received after six months of original request for that input. All services performed by *exida* up to this cancellation date will be billed according the above-mentioned conditions. Billing will be performed at the completion of each work-item.

Customer Company may extend or reduce the scope of certification by resubmitting the certification application or by notifying *exida* in writing. If in the course of the project Customer Company extends or reduces the scope of certification, *exida* reserves the right to amend the proposal to reflect the increased or reduced effort.

It is expected that projects will take 3 – 6 months to complete.

exida does not recieve any outside financial support. *exida* is wholly dependent on fees from services and products.

5.1 Basis of the Support Activities

Standards		
[N1]	IEC 61508, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems
[N2]	ISA 84.01 / IEC 61511	Functional Safety: Safety Instrumented Systems for the Process Industry Sector

Industry References	
[I1]	Electrical and Mechanical Component Reliability Handbook, second edition, 2008, *exida*.com LLC, Sellersville, PA, USA, ISBN-13: 978-0-9727234-6-6
[I2]	Evaluating Control Systems Reliability, Techniques and Applications, W.M Goble., 1992, ISA, Research Triangle Park, NC, USA, ISBN: 1-55617-128-5
[I3]	"Using a Failure Modes, Effects and Diagnostic Analysis (FMEDA) to Measure Diagnostic Coverage in Programmable Electronic Systems", W. M. Goble and A. C. Brombacher, Reliability Engineering and System Safety, Vol. 66, No. 2, November 1999

5.2 *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.

5.3 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*.

Customer Company agrees to observe and comply with the applicable sections of Functional Safety.

During the certification period the Customer Company is required 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.

During the certification period the Customer Company is required 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.

The validation period for Functional Safety certification is 3 years. At the end of the certification validity period, the Customer Company must renew the certification. The Customer Company must successfully pass a surveillance audit to maintain certification.

Customer Company agrees to notify *exida* of any changes to the product and/or processes that would affect the safety function of the Product.

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.

It is expected that this project will take 3 – 6 months to complete exclusive of product development and process improvement time. If the project extends beyond this time frame, a price adjustment to account for increased costs may be necessary.

5.4 Responsibility and Liability

Work performed by *exida* is executed in accordance with established regulations or standards of technology. *exida* accepts no responsibility for the correctness of the regulations or standards on which the services and products are based.

The *exida* guarantee covers only its services for which it has received an order. The proper condition and functioning of a complete facility or parts of facilities for which *exida* supplied products or services are not guaranteed. In particular, *exida* does not guarantee the design of facilities or choice of products used. The *exida* guarantee is restricted to the correction of errors or deficiencies within a reasonable period. If the correction is not completed in time, or not adequately completed, Customer Company is entitled to a reduction.

Neither party shall be liable for any losses or damages of any nature whatsoever incurred or suffered as a result of any failures and delays in performance due to any cause or circumstance beyond such party's control. Claims for damages for non-performance may only be asserted if the damage is due to intentional or gross negligence.

These liability restrictions are also applicable to the personal liability of the employees of *exida* as well as to third parties acting on their behalf.

5.5 Confidentiality, Copyright, Data Protection

exida and its representatives are not permitted to disclose information on the business as well as technical data of which they become aware through their work. This obligation shall not apply to information that:

a. must be disclosed to government regulatory agencies or to a Court of law,
b. is or becomes public through no act of *exida*,
c. is rightfully received from a third party without obligations of confidentiality,
d. is known by *exida* prior to the confidential disclosure.

exida is permitted to keep copies of documents which have been delivered and which are important for the execution of the order. *exida* will take reasonable precautions to safeguard such documents.

exida holds the copyrights of the templates, any documents, expert opinions, etc. which it has prepared and may use this information in subsequent services and/or products.

5.6 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.

5.7 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 might impact the ability to meet certification requirements,
- 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,
- that the Certificate and Report for the Product will be part of a public record that is maintain on the *exida* website during the period of validity,
- 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.

5.8 Use of the Certificate or Report

- *exida* hereby grants 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.

5.9 Use of the Certification Mark

exida hereby grants 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*.com 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.

5.10 Right to withdraw the certificate

Customer Company acknowledges that *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 suspension or 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*.

6 Document Status: Released

7 Author(s)

Version	Revision	Author	Date

V1	**R1**	**Steven Close**	**12/2/2015**

8 Revisions

Version	Revision	Change	Changed By	Date
V2	**R1**	**Revised section 5 to include extended or reduced scope.**	**Steven Close**	**11/13/2018**

9 Approvals

Version	Revision	Approved By	Approval email	Date
V1	**R1**	**Ted Stewart**		**12/2/15**
V2	**R1**	**Ted Stewart**	RE Q V0R1 Functio... Safety Cer Approve ANSI OFI.msg	**11/14/2018**