The exida IEC 61508 – Functional Safety and IEC 62443 – Cybersecurity Certification Programs

White Paper

exida
80 N. Main St.
Sellersville, PA
www.exida.com

November 2017

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Copyright exida.com L.L.C. 2018-2020

exida Certification

The exida Certification Program was established in 2005 in response to demand primarily from end users in the process/machine industries and manufacturers of control and instrumentation products. There was a global need to provide a **higher quality of technical expertise** with effective and responsive service.

exida is an accredited Certification Body (CB) authorized to perform certification by the American National Standards Institute (ANSI) in the technical fields of functional safety and cybersecurity. ANSI is the Accreditation Body (AB) for IEC standards in the United States. They are a member of the International Accreditation Forum (IAF). Most countries in the world have an AB which is a member of IAF (www.iaf.nu). IAF members have agreed to the Multilateral Recognition Agreement recognizing the equivalence of other member's accreditations. Thus IAF member accreditations are valid in most countries of the world.

exida prepares a Safety/Security Case for each certification project. A Safety/Security Case is a complete list of all requirements of the stated scheme along with arguments and evidence that the product under assessment meets all requirements. It is an essential tool to ensure completeness of the certification audit thereby finding potentially dangerous weak points in a product design. Despite the proven value of this technique, few certification agencies use this approach.

exida prepares a Certification Report summarizing the audit information in a public format. This report and a Certificate are **publicly posted** on the exida website under the "Safety Automation Equipment List," http://www.exida.com/index.php/resources/sael/. This web resource provides the most up to date and comprehensive listing of functional safety and cyber-security certifications available.

The exida Certification Program offers the most comprehensive system/product review of any Certification Body (CB) resulting in products that are safer, more secure, easier to use, and more reliable.

Functional Safety

exida operates the Functional Safety Certification Program based on a "scheme" which lists all requirements that a supplier must meet in order to receive an exida Certificate. Standards referenced in the scheme include IEC 61508, IEC 62061, ISO 13849, ISO 26262 and other related standards. The scheme requirements are documented in a "Safety Case" which lists all relevant requirements given a set of referenced standards. **However, the exida scheme goes beyond the standards** and requires:

a) that a product manufacturer do (or have done) a detailed Failure Modes, Effects, and Diagnostic Analysis (FMEDA) which derives all failure rates for each failure mode of the product. This includes false trip data not required by IEC 61508 or other CBs. As exida developed the FMEDA technique and has refined the method over the last twenty years, our level of expertise is unmatched. This valuable tool for predicting field failure rates for each failure mode has been shown to accurately match field failure data from the several different industries. Each analysis is backed up by extensive fault injection testing and a detailed field failure study. This analysis suite results in the most realistic failure rate and failure mode information. Unlike other agencies, **exida does not accept manufacturer's warranty failure studies alone as those studies typically show very optimistic results**. Unlike other agencies, exida does not perform "cycle

testing" to show random mechanical failure rates. This cycle testing technique does provide some useful life information but should never be used to represent random failure rates. Instead exida uses the FMEDA technique backed up by a detailed mechanical failure rate database. This database is the result of nearly 500 field failure studies representing over 300 billion unit operating hours in industrial environments. We believe this to be the largest set of failure data for the industrial environment in the world.

b) cybersecurity audits per IEC 62443 standards.
c) practical manual proof test procedures or automatic proof test functionality.
d) Surveillance audits where engineering changes, field failure data, and design procedures changes are audited to answer the question "Is this product still safe?" Many functional safety certification programs done per IEC 61508 do not require any surveillance audits.

Cybersecurity

exida is accredited per IEC/ISO 17065 by the American National Standards Institute (ANSI) to certify to a series of exida certification schemes for cybersecurity based on the IEC 62443 series of standards. exida is also an accredited Certification Body for the original ISA Security Compliance Institute (ISCI) certification schemes. A certification scheme specifies all requirements that must be met and the procedures that must be used in a certification project. These requirements and procedures are documented in a "Security Case."

The IEC 62443 standards are recently created as a result of a strong global committee effort and are rapidly becoming recognized world-wide. Many automation users consider the IEC 62443 standard to be required. The ISCI schemes will likely be updated to IEC 62443 in the future. A table of the various cybersecurity certification scheme certifications offered by exida is shown below:

Classification	Program Name	Source	Based On
Product Test/Evaluation	EDSA	ISA Security Compliance Institute	ISCI Specification
	eSDC	exida	IEC 62443-4-1, -4-2
System Test/Evaluation	SSA	ISA Security Compliance Institute	ISCI Specification
	eSSC	exida	IEC 62443-4-1, -4-2
Process Evaluation – Product	SDLA	ISA Security Compliance Institute	ISCI Specification
	eSDP	exida	IEC 62443-4-1, -4-2
Process Evaluation – System	System Integrator	Wurldtech (G.E.)	IEC 62443-2-4
	eSSP	exida	IEC 62443-2-4 plus

exida Cybersecurity Schemes

The exida schemes go beyond IEC 62443 and require:

a) that the product manufacturer perform network robustness testing during development for a product and for every revision to security critical software. It is not sufficient for a test lab to perform testing after a product is ready for production release. This type of requirement does not identify issues in time for corrective action. Normally the manufacturer will need to establish a cybersecurity test lab and perform frequent testing. exida will witness a sample set of tests before production release.
b) the software development process used to create the product meet requirements of the cybersecurity maturity level.
c) surveillance audits be performed by the CB at regular intervals to ensure testing is being performed and security monitoring in the field / security response systems are working well.
d) security defense mechanisms required by the referenced standards have been implemented as required.
e) equipment failure modes are evaluated per their impact on cybersecurity features.
f) practical system level cybersecurity requirements needed for the product are published in a user document. The information required by exida goes beyond existing standards per the advice of our end user Advisory Board.

ISCI Cybersecurity Schemes

The ISA Security Compliance Institute (ISCI) established the first cybersecurity certification scheme in the automation industry. exida participated as a technical member of the ISCI committee and as a contract requirements author. exida became the first CB in the world to achieve accreditation for cybersecurity under this scheme. The ISCI scheme requires:

a) that the CB perform the network robustness testing using ISCI approved test equipment.
b) no surveillance audit, however each revision of security related software to be re-certified.

Certification Operation

The exida Certification Program is operated globally by exida.com L.L.C. with work performed by its subsidiary companies. Assessors from exida are assigned on a project basis. Individuals are assigned to do the assessments such that no one who has worked on a project as a consultant may participate in the assessment. The exida program ensures an independent audit and assessment.

Frequently Asked Questions

Has exida participated on the IEC 61508 committee?

Several exida team members have been active on the IEC 61508 committee since its inception. These people continue today as the standard progresses through modification. **No other certification agency in the world has been more active in the creation of IEC 61508.**

Has exida participated on the IEC 62443 committees?

Yes, exida personnel have been active on several committees. exida has been most active on the IEC 62443-4-1 committee where the technical lead and editor was an exida person. **No other certification agency in the world has been more active in the creation of IEC 62443.**

How does exida certification differ from other certification schemes?

IEC/ISO standards are large with each subclause being a requirement. Most of the standards have a statement like IEC 61508 which says: "To conform to this standard it shall be demonstrated that the requirements have been satisfied to the required criteria specified and therefore, for each clause or sub-clause, all the objectives have been met."

In the opinion of exida, this statement requires a "Safety/Security Case" to the requirements of the standard plus any additions in the scheme. A simple certificate and certification report, as done by most other agencies, stating general compliance with a standard does not fulfill the IEC requirements. A full Safety/Security Case lists all requirements and provides the arguments and justification as to how each project meets the standard. exida does a Safety/Security Case for each certification project.

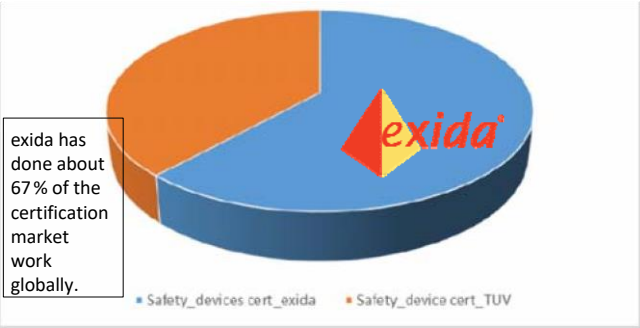
In addition, the exida Certification program looks at usability of a product from a systems perspective and evaluates the likelihood of unintended misuse. Although this is not part of many certification programs, the exida End User Advisory Council has strongly suggested this interpretation of IEC requirements.

Who are exida Certification Services customers?

The logos above represent some of the many product manufacturers who have successfully received a certification from exida.

How many certifications has exida done?

As of June 2017 exida has successfully completed over 600 IEC product certifications of currently marketed products. exida has completed more active IEC 61508 certifications in the process industries than any other organization. A study by ARC Advisory Group in November 2015 has concluded that "exida is the clear market leader in device safety certifications."



In cybersecurity, exida has done more certifications than any other Certification Body.

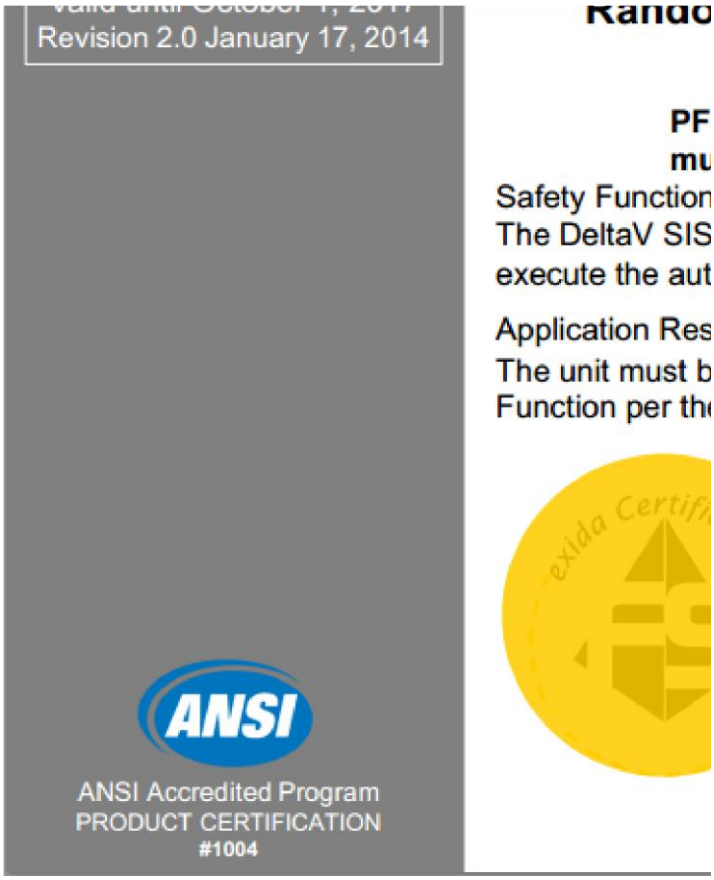
A complete overview of all products currently marketed that have been assessed is available on the exida web-site. http://www.exida.com/SAEL

Why does an exida certificate have an expiration date when others do not?

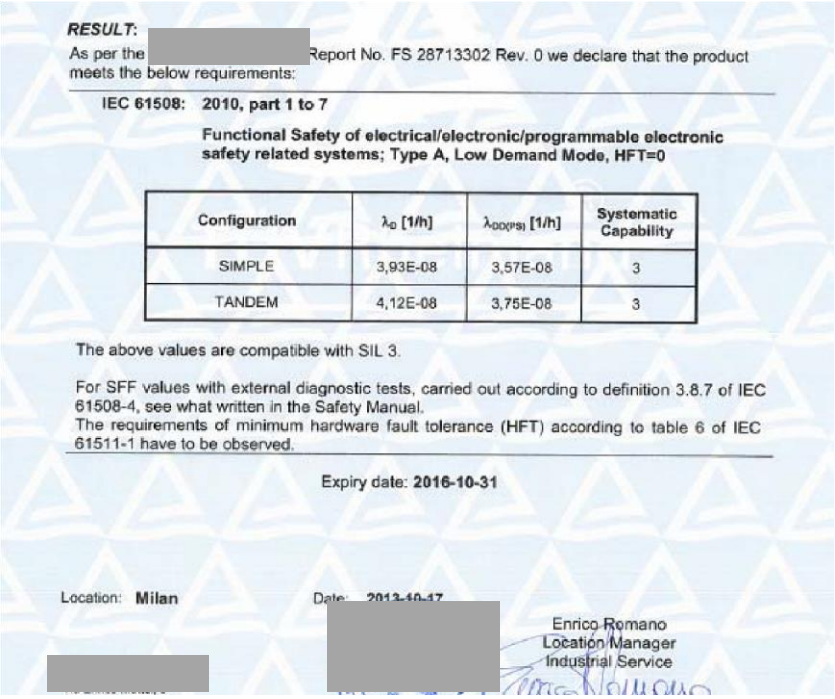
exida schemes require that product manufacturer's undergo periodic re-assessment. At that time engineering changes are examined, field failure history is reviewed and development/testing process updates are reviewed to be certain that the product still meets the requirements of the referenced standards. A visible surveillance date will clearly indicate to potential customers of any product if the manufacturer no longer verifies that the product meets the standard.

Why does exida have an AB logo on their certificates and others do not?

When a CB performs as assessment following their accredited process, they may put the AB logo on their certificate. On the exida certificate, this logo is in the lower left front page.



Some CBs, though accredited, do not follow their accredited process and are not permitted to use the AB logo on their certificates.



RESULT:

As per the [redacted] Report No. FS 28713302 Rev. 0 we declare that the product meets the below requirements:

IEC 61508: 2010, part 1 to 7

Functional Safety of electrical/electronic/programmable electronic safety related systems; Type A, Low Demand Mode, HFT=0

Configuration	λ_D [1/h]	$\lambda_{DD(PS)}$ [1/h]	Systematic Capability
SIMPLE	3,93E-08	3,57E-08	3
TANDEM	4,12E-08	3,75E-08	3

The above values are compatible with SIL 3.

For SFF values with external diagnostic tests, carried out according to definition 3.8.7 of IEC 61508-4, see what written in the Safety Manual.
The requirements of minimum hardware fault tolerance (HFT) according to table 6 of IEC 61511-1 have to be observed.

Expiry date: **2016-10-31**

Location: **Milan** Date: [redacted]

[redacted]

Enrico Romano
Location Manager
Industrial Service

References

1. [DEF97] Defence Standard 00 – 55, Parts 1 and 2, Issue 2, August 1997, U.K. Ministry of Defence.
2. [BIS98] Peter G. Bishop and Robin E. Bloomfield, "A Methodology for Safety Case Development", in Safety-
3. Critical Systems Symposium, Birmingham, UK, February 1998. http://citeseer.ist.psu.edu/bishop98methodology.html
4. [TUV00] Requirements Database Review, Report #: eS 70177T, TÜV Product Service Inc., October, 20, 2000.

Terms and Definitions

AB	Accreditation Body
ANSI	American National Standards Institute
CB	Certification Body
FIT	Failure in Time (1 x 10-9 failures per hour)
FMEA	Failure Modes Effects Analysis
FMEDA	Failure Modes, Effects and Diagnostic Analysis
IAF	International Accreditation Forum
IEC	International Electro-Technical Commission
ISA	International Society of Automation
ISCI	ISA Security Compliance Institute
ISO	International Standards Organization

Revision History

Author: William M. Goble, PhD

Version: V1

Revision: R1

Version History:

V1, R1: xxxx
V0, R1: Based on IEC 61508 document; November 10, 2017

Review:

V0, R1: William M. Goble November 28, 2017

Future Enhancements

As required.

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool

- PHAx™ (Process Hazard Analysis)
- LOPAx™ (Layer of Protection Analysis)
- SILAlarm™ (Alarm Management and Rationalization)
- SILect™ (SIL Selection and Layer of Protection Analysis)
- Process SRS (PHA based Safety Requirements Specification definition)
- SILver™ (SIL verification)
- Design SRS (Conceptual Design based Safety Requirements Specification definition)
- Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
- PTG (Proof Test Generator)
- SILstat™ (Life Event Recording and Monitoring)

- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com