exida

Functional Safety, Security, & Reliability
www.exida.com

What is Certification?

Certification is an earned credential resulting from a 3rd party assessment process that demonstrates mastery / competency / conformance as measured against a defensible set of requirements (typically derived from international standards).

exida has three certification programs to best suit a company's needs:

1. Functional Safety Certification
2. Control System Cyber Security Certification
3. Functional Integrity Certification

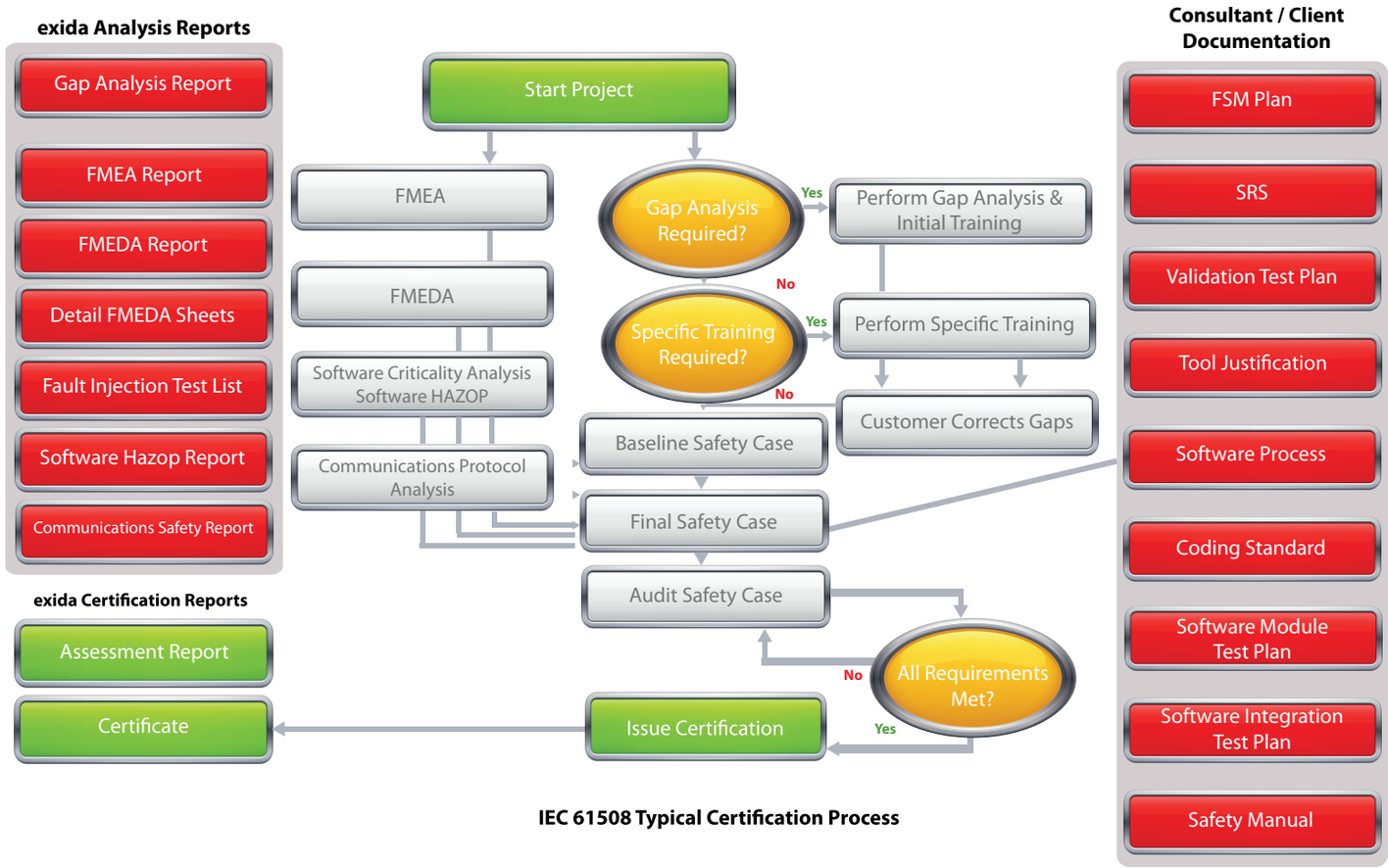
Why Certification?

Certification provides:

- ◊ Instant recognition of product reliability, safety, security, and availability characteristics
- ◊ Independent industry stamp of approval
- ◊ Criteria for product selection during procurement
- ◊ An easier way for end users to comply with industry standards and regulations

Functional Safety Certification

The IEC 61508 standard defines the requirements for suppliers to follow during product development to ensure that their products have a high level of resistance to random hardware and "systematic" design failures. Compliance is evaluated by qualified third party certification agencies which assess and certify that a product has been designed and developed in accordance with the standard. exida follows a rigorous process that verifies the Safety Integrity Level (SIL) of a product's hardware and software design, as well as its manufacturing and quality control procedures.



IEC 61508 Typical Certification Process

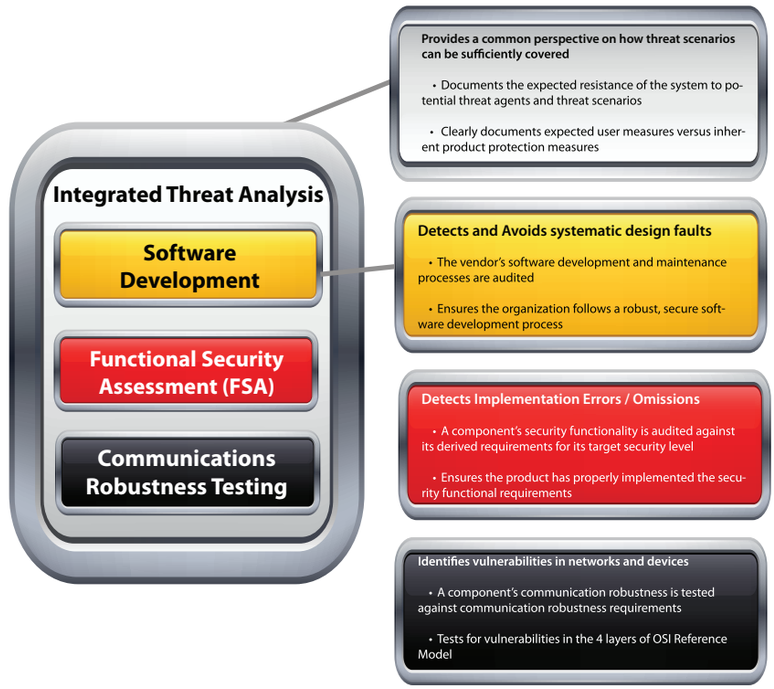
The Assessment & Certification Process at a Glance

- **Product & Process Design Review -** Review the product's current design and testing processes against the requirements of the IEC 61508 standard(s) and identify any gaps.
- **Reliability & Failure Mode Analysis -** Complete a technical analysis for the product to assess that the design meets the technical requirements of the standard. This includes performing fault injection testing and a detailed Failure Modes, Effects & Diagnostics Analysis (FMEDA) to determine the failure rate data necessary for use in SIL verification.
- **Proven in Use Evaluation -** Perform a "Proven in Use" analysis if the basis of the IEC 61508 assessment includes assessment of field experience.
- **Requirements Traceability** - Document the detailed assessment results (how / why each requirement of 61508 is met) in exida's SafetyCaseDB tool. This data forms the basis for the eventual IEC 61508 certification.
- **Audit Project Deliverables** - Perform a Final Assessment Audit to verify that the actual product development documents and process as captured in the safety case meet the associated IEC 61508 requirements. A successful audit results in the issuance of a compliance certificate, creation of an assessment / certification report and publication on the Safety Automation Equipment List (www.sael-online.com).

exida has performed more process control safety certifications than any other company worldwide.

Control System Cyber Security Certification

The ISA Security Compliance Institute (ISCI) has developed a program for the security testing and certification of critical control system products such as PLCs, controllers, digital protective relays, and communication modules. The program, called ISA Secure, utilizes test specifications and protocols developed from publicly available sources such as the ISA-99 industry standard. exida is authorized to perform the assessment and certification activities on behalf of ISCI.



**ISA Secure is a program established by the ISA Security Compliance Institute (ISCI) to establish a set of well-engineered specifications and processes for the testing and certification of critical control systems products*

Assessment & Certification Services

exida provides the following services to validate the security and reliability of industrial automation products against the ISA Secure Embedded Device Security Assurance specifications:

- **Communication Robustness Testing (CRT)** - Evaluates how well the product meets the ISA Secure EDSA communications robustness specification using the Achilles Level 2 ISA Secure EDSA recognized test platform.
- **Functional Security Assessment (FSA)** - Review how well the design meets the functional security requirements of the target ISASecure Level defined in the ISA Secure EDSA specification.
- **Software Development Security Assessment (SDSA) -** Reviews the product development processes used and evaluates how well the current processes meet the software development security requirements of the ISA Secure EDSA specifications.
- **Integrated Threat Analysis (ITA)** - Documents threats that are mitigated by the features and functions of the product vs. those that are the user's responsibility to mitigate.
- **Gap analysis** - Reviews the existing development procedures to determine any major gaps between the requirements of the applicable standard(s) and the quality management procedures

The Embedded Device Security Assurance Specifications

exida provides the following services to validate the security and reliability of industrial automation products against the ISA Secure Embedded Device Security Assurance specifications:

- ISASecure Embedded Device Security Assurance (EDSA) certification scheme (EDSA-100, V1.1, June 2010)
- ISASecure Embedded Device Security Assurance (EDSA) certification scheme (EDSA-100, V1.1, June 2010)
- EDSA Certification Requirements (EDSA 300, V2.0, June 2010)
- Common Requirements for Communication Robustness Testing (CRT) (ESDA-310, V1.47, 2010)
- Ethernet robustness test spec (ESDA-401, V2.0, 2010)
- ARP robustness test specification (ESDA-402, V2.3, 2010)
- IPv4 robustness test specification (ESDA-403, V1.3, 2010)
- ICMPv4 robustness test specification (ESDA-404, V1.3, 2010)
- UDP robustness test specification (ESDA-405, V2.6, 2010)
- TCP robustness test specification (ESDA-406, V1.4, 2010)
- Functional Security Assessment (FSA) (ESDA-311, V1.4, 2010)
- Software Development Security Assessment (SDSA) (ESDA-312, V1.4, 2010)

Functional Integrity Certification

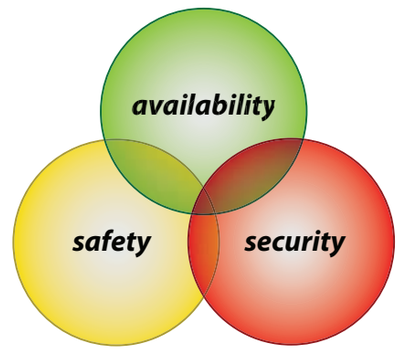
Functional Integrity Certification™ is a program that evaluates the most critical attributes of an automation product:

- Functional Safety
- Functional Security
- Availability

The goal of the program is to improve product / system performance by assessing ability to perform in critical situations.

Functional Integrity Certification is the only product certification program that covers:

- How the product was designed
- How the product was tested
- How the product was manufactured
- How the product has performed in the field
- How the product is likely to perform over time
- How easy or difficult it is to properly apply and maintain the product



Why is Functional Integrity Certification Needed?

With the evolution of technology and incidents such as Stuxnet, it has become more apparent that security vulnerabilities can impact the operation of a safety instrumented system.

Functional Integrity certification analyzes how the security design impacts SIS performance.

Traditional certification companies have given IEC 61508 SIL 3 approval to products with complicated end user programming and impractical proof testing requirements. This has resulted in failed system designs that are not safe.

Functional Integrity certification evaluates the complexity of implementation and practicality of maintenance procedures

Availability assessment ensures the dependability of automation products in critical applications. In most continuous process facilities, this means reliable 24x7x365 operation for up to several years at a time. As part of the evaluation, exida quantifies the false or spurious trip rate of a product using standardized modeling and probabilistic methods. Trip rate data is combined with empirical data to help predict product reliability.

Functional Integrity certification includes "false trip" failure rates not just safe failure rates.

How End Users Benefit from Using Certified Products

◊ **Lower lifecycle costs -**

- No need to justify use of device by costly "prior use" analysis and tracking of installed devices
- No need to perform project security assessments on devices for each new project
- Reduces effort, cost for safety system design (SIL Verification)

◊ **Independent, 3rd Party assessment ensures quality & reliability**

◊ **Easier compliance with international standards**

◊ **Reduces risk (accidents) and liability**

◊ **Helps ensure SIS is not overdesigned ($$) or under-designed (higher risk)**

Why exida Certification?

Through our extensive and on-going research, exida has developed advanced analysis tools that:

- ◊ Provide the most accurate results
- ◊ Reduce the project time and cost
- ◊ Provide essential customer design information

ACLASS Accredited TESTING

How does exida help?

- ◊ **Project Management** - exida provides a dedicated project manager to keep the project moving and ensure scheduled completion

- ◊ **Industry Recognized Evaluation Techniques** - exida publishes detailed common language methods and procedures via our textbooks and reference books

- ◊ **Market Support** - exida provides market support via exSILentia, our end-user verification tool, and via the Safety Automation Equipment List, the world's most popular reference for certified equipment. Through marketing support and sales training, exida strives to help the whole organization understand the importance of safety and cyber security certification

For more information or to request a quote:

Contact your local exida representative or visit our website at www.exida.com

Germany	USA	South Africa	Asia Pacific
exida.com GmbH Birkensteinstr. 53 83730 Fischbachau PHONE: +49-89-49000547	exida.com LLC 64 North Main Street Sellersville, PA 18960 PHONE: +1-215-453-1720	exida South Africa PTY LTD Suite 1003, 34 Essex Terrace Westville, 3629, KZN PHONE: +27 31 2671564	11 Collyer Quay #10-13, The Arcade Singapore 049317 PHONE: +65 6222-5160
Switzerland	**Canada**	**Mexico**	**United Kingdom**
exida Certification SA Chemin de Champ-Poury 2 1272 Genolier PHONE:+41 22 364 14 34	exida Canada Ltd. 2nd Floor 3003 - 23rd Street NE Calgary, Alberta T2E 7A4 Canada PHONE: +1-403-475-1943	exida Consulting Mexico Giorgione No. 6 Col. Nonoalco Mixocac Mexico, D.F. 03700 Mexico PHONE: 52-55-5-6-11-98-58	8 Hotchkiss Way Binley Industrial Estate Coventry CV3 2RL UK Phone: +44 (0) 24 76 456 195 Fax:+44 (0) 24 76 561 531