Security Certification Scheme

QD-005
September 20, 2021
Version 3 Revision 4

Confidential Information

All rights reserved. No parts of this procedure may be re-used
without the prior written permission of the authors.

1 Contents

2 Purpose of the Document:

exida strives to operate the most useful and relevant functional safety and cybersecurity certification program in the world. These programs go beyond referenced international standards to add additional requirements defined in this Scheme. This document describes the Security Certification Scheme used by *exida*. It provides the needed details to understand the scope and normative documents that form the basis of the certification.

3 Scope:

The scope covers all the steps in the Security Certification Scheme. It will apply to any process, product or collection of products that use software to perform their required functionality. The presumption is that the software can be corrupted in some way so as to prevent or alter the designed functionality of the product.

4 Definitions (list abbreviations and definitions)

4.1 Definitions

4.1.1 accreditation

assessment and recognition process via which an organization is granted Certification Body status by a nationally recognized Accreditation Body which is a member of the International Accreditation Forum (IAF)

4.1.2 accreditation body

third party organization that performs attestation, related to a conformity assessment body, conveying a formal demonstration of its competence to carry out specific conformity assessment

4.1.3 certifier

an organization that is qualified to perform cybersecurity assessment evaluation

4.1.4 certificate

a document that signifies that a person, product or organization has met the criteria defined under a specific evaluation program

4.1.5 certification

the process of impartial third-party evaluation, review, decision, attestation, and surveillance as specified by the certification scheme and its requirements in order to provide assurance that the specified requirements have been demonstrated

4.1.6 certification scheme

certification system (4.1.7) related to specified products, services, or processes to which the same specified requirements, specific rules and procedures apply as specified by the certification scheme document and its referenced normative documents.
[Source: IEC 17067]

4.1.7 certification system

rules, procedures and management for carrying out certification

[Source: ISO/IEC 17000:2004, 2.7, modified]

4.1.8 certified device

a well-defined version of a product or collection of products that have undergone an evaluation and have been granted certified status

4.1.9 communication robustness testing

tests that determine the extent to which an embedded device maintains its essential functions under adverse network traffic conditions

4.1.10 device vendor

an organization that applies for certification and is responsible for compliance of a device per the defined scheme

4.1.11 end user

organization that purchases, uses or is impacted by the security of embedded devices

4.1.12 “Ethernet”

IEEE802.3 as Ethernet II or IEEE 802.3 Type 1 plus IEEE 802 SNAP

4.1.13 functional security assessment

assessment of a defined list of security features for an embedded device

4.1.14 pass

meet the criteria for passing an evaluation as defined within the technical specifications

4.1.15 tool supplier

provider of a test tool to support communication robustness testing

4.1.16 version (of embedded device)

a well-defined release of an embedded device, typically identified by a release number

4.2 Abbreviations

The following abbreviations are used in this document.

ARP	address resolution protocol
CRT	communication robustness testing
EN	European Norm
EUC	Equipment under Control
IETF	Internet engineering task force
IAF	International Accreditation Forum
ICMPv4	internet control message protocol version 4
IEEE	Institute of Electrical and Electronic Engineers
Ipv4	internet protocol version 4
ILAC	International Laboratory Accreditation Cooperation
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization

OP	Operating Procedure
TCP	transmission control protocol
UDP	user datagram protocol

5 Reference Material

5.1 Normative references

5.1.1 International standards for certification programs

[ISO/IEC 17025] ISO/IEC 17025:2017, "*General requirements for the competence of testing and calibration laboratories*"***, November 2017***

[ISO/IEC 62443-4-1] ISO/IEC 62443-4-1 Security for industrial automation and control systems – *Part 4-1: Secure Product Development Lifecycle Requirements*"**,** Edition 1.0, Jan. 2018

[ISO/IEC 62443-4-2] ISO/IEC 62443-4-2 Security for industrial automation and control systems – Part 4-2 *Technical Security Requirements for IACS Components***,** Edition 1.0, Feb. 2019

[ISO/IEC 62443-2-4] ISO/IEC 62443-2-4 Security for industrial automation and control systems – *Part 2-4 Security program requirements for IACS service providers,* Edition 1.0, June 2015 and Amendment 1, August 2017

[ISO/IEC 62443-3-3] ISO/IEC 62443-3-3 Security for industrial automation and control systems – Part 3-3 *System Security Requirements and Security Levels***,** Edition 1.0, Aug. 2013

[ISO/IEC 27001] ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements, Second edition, Oct. 2013

[ISO/SAE 21434] ISO/SAE 21434 Road vehicles — Cybersecurity engineering, 2021

5.1.2 International standards for accreditation programs

[ISO/IEC 17011] ISO/IEC 17011, "*Conformity assessment – General requirements for accreditation bodies accrediting conformity assessment bodies*", 01 September 2004

6 Responsibility and Authority:

The Director - Certification of *exida* and his appointee are responsible for the content and maintenance of the scheme and this document. This is an informative document and is not meant to be an operating procedure.

7 Certification Scheme

7.1 Requirements

exida will obtain a list of required normative standards for each security certification job. The requirements against which a product or system is evaluated are then obtained from the Security Case for each referenced standard. The specific requirements and interpretations in

each Security Case are formulated by those personnel deemed competent to perform as an Evaluating Assessor per OP 1020 (Competency, Training, and Awareness).

7.2 Activities

Certification assessment functions including Evaluation (Selection and Determination of characteristics), Review, Decision of certification, Attestation, and Surveillance are specified in OP1023 (Certification Procedure).

7.3 Client Requirements

Requirements that must be met by the client are specified in the Certification Agreement and in the applicable Security Case set for each project. This includes:

- All information required to perform the determination of characteristics (testing, test witnessing, analysis of design, inspection, design appraisal, assessment of services or processes, etc.)
- All requirements and restrictions on usage of the certification mark,
- All requirements for how non-conformities with certification requirements are dealt with and resolved,
- All conditions for continuing surveillance, and
- Certificate withdrawal requirements including discontinuation of advertising and product marking.

7.4 Certification Body Requirements

exida and any other Certification Body shall be accredited per ISO/IEC 17065 by a national Accreditation Body who is a member of International Accreditation Forum (IAF) which has a Multilateral Recognition Agreement. The Certification Body shall utilize competent personnel as specified OP 1020 (Competency, Training, and Awareness). All competency evaluations shall be done by the Scheme Owner, *exida*.

7.5 Statement of Conformity

The Statement of Conformity (e.g. the Certificate) shall contain the information described in the applicable *exida* Certificate Template. Reference templates are stored in the *exida* Quality US SharePoint space.

7.6 Surveillance Audits

Surveillance audits are required as specified in OP 1030 (Surveillance Audits).

7.7 Personnel

All personnel assigned by *exida* to perform certification tasks shall be employed by *exida* or shall be under contract to *exida* per OP1023.

7.8 Retention of Records

All data shall be retained per OP1027 (Control of Data).

7.9 Integrity and Consistency

Integrity shall be maintained by the use of impartiality analysis. All certification projects shall utilize a hazard and risk analysis approach to evaluate impartiality per OP 1035 (Impartiality). Consistency shall be obtained by the use of the applicable Security Case on each project.

7.10 Certification Marks

All certification marks are shown in the Certification Agreement. These marks are the intellectual property of *exida*.

7.11 Scheme Resources

This Scheme is reviewed annually as part of *exida's* internal quality review process. Management and Quality personnel are required for this task. An Advisory Board must be established and must hold regular meetings (at least once per year) to review scheme issues.

7.12 Certification Results and Reporting

Certification results shall be expressed per OP 1032 (Report Procedure). Successful results (Certificate and assessment Report) will be posted on the *exida* website in order that the validity of a certificate may be verified by the public.

7.13 Scheme Description

This document and a simple to understand description of the Security Scheme are posted on the *exida* web site. One or more web seminars are also available.

7.14 Complaints and Appeals

Scheme complaints and appeals shall be processed following OP 1003 (Complaints, Appeals).

7.15 Fraudulent Claim of Certification

When the Certification Body discovers fraudulent claims of certification, a message must be sent to the company perpetrating the fraud stating that the fraudulent certificates must be immediately stopped. An announcement on the certification list warning potential consumers of the fraudulent certificate shall be placed on the *exida* web site.

7.16 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 suspension or withdrawal 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*.

If certification is 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.

7.17 Update and Maintenance of the Functional Security Scheme

This document is reviewed annually as part of *exida's* internal quality review process. All suggestions for improvement will be reviewed with the Advisory Board. Client input is continuously sought and incorporated after review with the Advisory Board, allowing the scheme to rapidly adjust to the needs of the user community and enhance the overall robustness of the certification process.

7.18 Financial Support and Fees

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

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.

8 Document Status: Released

9 Revisions

Version	Revision	Author		Date
V0	R5	David Johnson	review with WMG	29 Apr 2015
V1	R1	William Goble	Edits to clarify requirements	24 Jul 2015
V2	R1	Steven Close	Add Section 7.17	21 Dec 2015
V3	R1	Steven Close	Added Section 7.16	7Nov 2019
V3	R2	Ted Stewart	Corrected spelling errors and provided links to reference documents	3Nov2020
V3	R3	William Goble	Corrected titles, phrases, added new cyber reference standards	31Aug2021
V3	R4	Russell Fuss	5,5.1 updated to latest IEC17025 rev. and 7.17 to reflect Security Cert Scheme instead of Safety	9/20/2021

10 Approvals

Version	Revision	Approved By	Approval email	Date
V1	R1	William Goble	 Approve QD-005 V1R1 Security Certific	7/28/2015
V1	R1	Mike Medoff	 Approve QD-005 V1R1 Security Certific	7/28/2015
V2	R1	William Goble	Verbal	12/21/2015
V3	R1	William Goble	 Approve_ QD-004 .msg  QD-004 .msg	11/8/2019
	R2	N/A; due to minimal changes	N/A	

V3	R3	William Goble	 Approve_ QD004 and QD005.msg	9/15/2021
V3	R4	Russell Fuss	N/A; due to minimal changes	9/20/2021