EDSA-301
ISA Security Compliance Institute — Embedded Device Security Assurance –

Maintenance of ISASecure certification

Version 1.0

August 2010

Revision history

version	date	changes
1.0	2010.08.04	Initial version published to http://www.ISASecure.org

Contents

Foreword

NOTE This is one of a series of documents that defines ISASecure certification for embedded devices, which is developed and managed by the industry consortium ISA Security Compliance Institute (ISCI). The current list of documents related to ISASecure embedded device security assurance can be found on the ISCI web site http://www.ISASecure.org.

1 Scope

This document specifies the criteria for maintaining ISASecure EDSA certification for an embedded device, as the device and the ISASecure EDSA criteria evolve over time. A product is considered to be an embedded device if it satisfies the definition provided in 3.1.3. This document covers certification situations where:

- a certified device has subsequently been modified; or
- the ISASecure certification criteria have changed; or
- both the device and the certification criteria have changed.

In these cases, an assessment is required in order to determine whether, and in what manner, a previous certification may be used as evidence toward a new certification. The requirements in this document address these topics.

A certification is called an *initial* certification if it *does not* take into account the results of a prior certification for the device or for a prior version of the device. The criteria for a device to earn an initial certification are defined in [EDSA-300].

To specify when and how the results of a previous certification may be used for certification of a modified device or for a certification to a later version or higher level of the ISASecure criteria, this document discusses the three elements of ISASecure EDSA certification:

- Communication robustness testing (CRT);
- Functional Security Assessment (FSA); and
- Software Development Security Assessment (SDSA).

CRT examines the capability of the device to adequately maintain essential services while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). These tests include specific tests for susceptibility to known network attacks. The FSA examines the security capabilities of the device, while recognizing that in some cases security functionality may be allocated to other components of the device's overall system environment. Finally, the SDSA examines the process under which the device was developed.

2 Normative references

[EDSA-300] *ISA Security Compliance Institute Embedded Device Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

[EDSA-310] *ISA Security Compliance Institute Embedded Device Security Assurance – Common requirements for communication robustness testing of IP based protocol implementations,* as specified at http://www.ISASecure.org

[EDSA-311] *ISA Security Compliance Institute Embedded Device Security Assurance – Functional security assessment,* as specified at http://www.ISASecure.org

[EDSA-312] *ISA Security Compliance Institute Embedded Device Security Assurance – Software development security assessment*, as specified at http://www.ISASecure.org

3 Definitions and abbreviations

3.1 Definitions

.

3.1.1
allocatable
able to be met by other components

NOTE As used here, refers to security capabilities capable of being met by other components in a device's architectural context, although not directly provided by the device itself.

3.1.2
certifier
an accredited organization with the authority to carry out ISASecure assessments and testing, and grant ISASecure certifications

3.1.3
embedded device
special purpose device running embedded software designed to directly monitor, control or actuate an industrial process

NOTE Attributes of an embedded device are: no rotating media, limited number of exposed services, programmed through an external interface, embedded OS or firmware equivalent, real-time scheduler, may have an attached control panel, may have a communications interface. Examples are: PLC, field sensor devices, SIS controller, DCS controller.

3.1.4
essential services
specified subset of the services provided by a device that is agreed between the applicant for certification and the test lab, at the start of certification

NOTE As specified in [EDSA-310], essential services are a subset of the following 6 services: the process control/safety loop, process view, command, process alarms, provide essential history data and peer-to-peer control communication. The first four of these are always considered essential services.

3.1.5
initial certification
certification where the ISASecure certification process does not take into account any prior ISASecure certifications of the embedded device or of any prior versions of the device

3.1.6
ISASecure version
identifier for the ISASecure certification criteria in force at a particular point in time, denoted using a year, followed by a period and a release number

NOTE An example is ISASecure EDSA 2010.2. An ISASecure version will map to document versions of the ISASecure technical specifications that define the technical criteria for certification.

3.2 Abbreviations

The following abbreviations are used in this document

ASCI	Automation Standards Compliance Institute
CM	change management
CRT	communication robustness testing
EDSA	embedded device security assurance
FSA	functional security assessment
ICMP	Internet control message protocol
ISCI	ISA Security Compliance Institute
SDSA	software development security assessment

4 Overview

In this section we summarize the approach to maintenance of ISASecure EDSA certification as a device and the ISASecure EDSA certification requirements evolve over time. The intent of the overall approach is to leverage previous certification results wherever possible to achieve cost effectiveness, while maintaining the integrity of the certification result. Sections 5 - 9 provide more detailed requirements for various certification maintenance scenarios.

4.1 SDSA

The SDSA element of the certification offers opportunity for leverage and cost effectiveness of the certification process across multiple devices, whether or not these devices are related. This is because the SDSA examines development process, and in many cases this process is consistent for an organization across all development projects. Hence the applicability of SDSA results from any previous certification is always considered as input to a new certification for any device developed by the same organization. The device vendor must be able to demonstrate that the defined process examined under the previous certification was in fact followed for a new or modified device under evaluation.

Section 5 provides requirements for leveraging SDSA results across multiple certifications.

4.2 Modified devices

When a particular release of a device achieves, for example, ISASecure EDSA 2010.2 certification, this particular device version retains this specific certification indefinitely. A device vendor is not *required* to update an embedded device certification for every field patch and new release of the device. The decision to certify a later device version is ultimately an optimization of end customer opinion and cost to the vendor. However, the device vendor is required to clearly communicate to the marketplace which version of their device meets the ISASecure criteria, and which version of the criteria it meets. As stated in Requirement ISASecure_ED.R3 of [EDSA-300], “ISCI, the certifier, and the device vendor SHALL publish certification status information for certified devices in a public venue. Information provided SHALL include the most granular version identifier of the device to which the ISASecure EDSA certification applies, and the version of the certification achieved, designated by the year and release, such as ISASecure EDSA 2010.2.”

If a device has achieved certification, and a modified version of that device is submitted for certification, then a well-defined assessment is performed that determines which aspects of the certification will need to be carried out on the modified device. Given the scope of changes to the device, if such an assessment is determined not to be cost effective, the certifier may elect to perform CRT and/or FSA in full on the modified device. If an assessment of changes is performed and shows that the modifications to the device and its documentation would not affect the certification results, then no certification tests or evaluations will be necessary in order for the modified device to be granted certification. In other cases, partial evaluations may be sufficient. However, by policy, the CRT test sequence is always run as a whole if any aspects of it may have been affected.

User documentation changes are evaluated along with changes to the device itself when a modified device is submitted for certification. However, a device that has had only user documentation changes is considered to retain its certification if the device itself has not changed.

Section 6 provides requirements for certification of modified devices.

4.3 Updated ISASecure criteria

As in the case of device modifications, a device vendor is not required to update an embedded device certification to the latest ISASecure version. Hence, for example, a device certified to ISASecure EDSA 2010.2 is not required to obtain a certification to ISASecure EDSA 2011.1. However, all devices going through certification after ISASecure EDSA 2011.1 becomes available will be certified to that ISASecure EDSA version.

Consider the case where a device achieved certification under ISASecure EDSA 2010.2, and this same device version is submitted for certification to the new certification version ISASecure EDSA 2011.1. This certification process will consist of carrying out the defined delta between the two certification versions.

In many cases both the device and the ISASecure EDSA certification version may change. Consider the case where a device achieved certification under ISASecure EDSA 2010.2, and a *modified* device version is submitted for certification to ISASecure EDSA 2011.1. This certification process will be logically equivalent to first certifying this modified device to ISASecure EDSA 2010.2 using the approach described in 4.2, and then carrying out the defined delta between the two certification versions on the modified device.

Section 7 provides requirements for certification to updated ISASecure EDSA certification criteria. Section 8 provides requirements for certifications when both the device and the certification criteria have been updated.

4.4 Certification to a higher ISASecure level

Once a device has achieved certification at ISASecure EDSA certification at level *n*, the device vendor may modify the device or available process evidence as deemed necessary, and then apply for a higher level certification. In this case, the certification consists of evaluating the device modifications at level *n* per Section 4.2 and then evaluating the certification criteria that apply for the new desired level but did not apply at level *n*. Section 9 provides requirements for this case.

5 SDSA and multiple certifications

The SDSA element of an embedded device certification examines (1) the existence of a documented secure development process for an organization and (2) adherence to this process in the development of the device. Thus if an organization submits multiple devices for certification, it is likely that the assessment related to (1), the existence of the process, will be directly applicable to any number of certifications. It may also be significantly easier to provide convincing evidence of adherence to the process, once this has been demonstrated for one device. For these reasons the requirement ISASecure_ED.R6 in [EDSA-300] states “A certifier SHALL consider the applicability of SDSA evaluation evidence and results for a certified device, to certifications for any later devices from the same organization.” This applies whether multiple certifications represent several releases of the same device model, or several completely different devices.

The following submission to the process by the device vendor supports the certifier in considering the applicability of prior SDSA evidence for a later certification.

Requirement ISASecure_EDM.R1 – Submission of development process delta

If an organization has previously achieved a device certification, then when applying for a subsequent certification, the applicant SHALL submit to the certification process:

- An analysis of the SDSA matrix, that for each numbered requirement in [SDSA] either:

    a) States that no additional actions beyond those previously carried out to meet this requirement for the prior certifications were required to meet this requirement for this certification, or

b) Briefly describes additional actions beyond those previously carried out to meet this requirement for the prior certifications, which were carried out to meet this requirement for this certification.

- Where requested, the applicant SHALL submit evidence that the actions reported under (b) were completed.

Requirement ISASecure_EDM.R2 – SDSA certification element after achieving first certification

A device submitted for certification by an organization that has previously achieved a device certification SHALL pass the SDSA element of the certification if:

- the certifier determines that the development process and tools as used in creating the submitted device are the same, equivalent or better than those used in creating a prior device that achieved certification; and

- the certifier validates for the submitted device those requirements which they would judge would require additional action beyond that previously carried out to meet these requirements for prior certifications, and all are assessed as pass.

The SDSA report in this case MAY include only a summary describing the certifier's conclusion of the first bullet above, a summary of the validations performed, plus a reference to the initial SDSA evaluation for this organization.

6 Requirements for certification of modified devices

The requirements in this section cover certifying a modified device, when a previous version of the device has already been certified.

6.1 Criteria for applying certification evidence from previous device version

The following requirements provide the general criteria under which evidence from prior certifications is considered applicable toward earning certification for a modified device. Specific requirements on how these criteria are evaluated follow in Section 6.2.

Requirement ISASecure_EDM.R3 – CRT certification element for a modified device

If an embedded device has been certified, then a modified version of the device SHALL on the basis of that prior evidence pass the CRT component of certification if:

- the certifier determines that an assessment of whether the device modifications have impacted CRT results will be cost effective; and

- the certifier carries out such an assessment and shows that device modifications have not impacted CRT results.

Device modifications SHALL be shown to have no impact on CRT results by showing:

- No architectural modifications have been made to any network protocols, essential services, or their interactions; and

- No significant new code has been incorporated for any network protocol, essential service, or their interactions; and

- Any changes to user documentation that impact mitigation guidance required due to CRT results are deemed appropriate.

In this case the certification report covering CRT MAY consist of only a summary of the CRT change assessment and a reference to the initial certification reports for the device. If either of the types of code

changes in the first two bullets directly above has been made to the device itself, or if the certifier determines that such an assessment of changes will not be cost effective, the modified device SHALL undergo the full CRT certification element, for all applicable protocols, in order to achieve certification for this element and a full report SHALL be provided. If only user documentation changes per in the third bullet have taken place, then testing is not required, and the modified device SHALL pass CRT based upon an evaluation of the documentation changes that shows they meet the criteria in the third bullet above.

NOTE 1 The definition of "cost effective' is determined by the certifier. A reasonable definition would be that an assessment is cost effective if it is estimated that the assessment will take at most the amount of effort required to run the CRT tests themselves. The effort estimate for such an assessment will be influenced by the quality of the evidence provided to the certifier by the device vendor per the requirements in Section 6.2.

Requirement ISASecure_EDM.R4 – FSA certification element for a modified device

If an embedded device has been certified, then a modified version of the device SHALL on the basis of that prior evidence pass the FSA component of certification if:

- the certifier determines that an assessment of whether the device modifications have impacted FSA results will be cost effective; and
- the certifier carries out such an assessment is and shows that device modifications have either not impacted FSA results, or have impacted few FSA line items in a manner isolated from other aspects of the FSA; and
- the certifier has evaluated any impacted FSA line items and given them pass status.

Device modifications SHALL be shown to have no impact on FSA results by showing:

- No architecture change, functionality change or significant new code has been incorporated related to a security feature referenced by a line item of the FSA; and
- Any changes to user documentation that impact mitigation guidance required due to FSA requirements are deemed appropriate.

In this case the certification report covering FSA MAY consist of only a summary of the FSA change assessment, results for FSA line items evaluated, and a reference to the initial certification reports for the device. If the certifier determines that an assessment will not be cost effective, or that device changes due to the FSA are widespread, then certifier SHALL perform the full FSA for the device to complete the FSA element of the certification and a full report SHALL be provided.

NOTE 2 As for CRT, the definition of "cost effective' is determined by the certifier. This is perhaps less straightforward to define for the FSA than for CRT. However, it is well understood that security features do not stand alone and are inherently interrelated in providing coherent protection for a device. Therefore if there are sufficient changes to device security functionality which it appears may interact, the full FSA should be reconsidered.

6.2 Evidence and assessment for criteria

If based upon the criteria in Section 6.1, a device vendor believes that some or all of the evidence used to certify a previous version of a device is applicable toward certification of a modified device, they may request consideration for this evidence. In this case, their submission of data toward certification of the modified device will include supporting evidence to demonstrate that the criteria stated in the requirements of 6.1 are met. This section specifies the nature of that supporting evidence and how it is assessed.

Requirement ISASecure_EDM.R5 – Submission of device modification data

A device vendor applying for certification for a modified device, MAY request consideration for CRT and/or FSA evaluations done on a prior version of the device that achieved certification. If so, the applicant SHALL submit to the certification process:

- a high level description of modifications to the device since the previous certification;

- a mapping from the elements of this description to a detailed change log extracted from the CM system for the device software; and
- evidence that this extraction from the CM system constitutes all changes in the modified device; and
- a high level summary of any changes to user documentation related to device security.

Requirement ISASecure_EDM.R6 – Submission of analysis of device modifications

If a device vendor has submitted evidence per Requirement ISASecure_EDM.R5 – Submission of device modification, then they shall in addition submit the following to the certification process:

- If consideration is requested for CRT: an analysis of the modifications reported under Requirement ISASecure_EDM.R5 that SHALL state which if any of these changes modified the code implementing the protocols subject to ISASecure CRT as defined in or the usage of these protocols by the essential services as defined in [EDSA-310], and SHALL include rationale for the conclusion that a modification did not occur.
- If consideration is requested for FSA: an analysis of the FSA matrix, that notes for each numbered line item in [FSA] that applies to the desired certification level for the device, whether there is any change to the functionality or code described by this requirement, among the device modifications since the previous certification. If so, the applicant SHALL provide a mapping to the related code modifications at the CM level of detail (as reported under Requirement ISASecure_EDM.R5).

Requirement ISASecure_EDM.R7 – Assessment of device modifications impacting CRT

When assessing modifications for a modified device where a prior version has been certified, the certifier SHALL determine that no modifications that may impact CRT results have taken place if

- the analysis submitted of changes to protocol or essential services code as described under Requirement ISASecure_EDM.R6 reports no changes to this code since the prior certification; and
- a certifier review of the evidence submitted per Requirement ISASecure_EDM.R5 and Requirement ISASecure_EDM.R6 finds no indication of such changes after consultation with the device vendor.

Requirement ISASecure_EDM.R8 – Assessment of device modifications impacting FSA

When assessing modifications for a modified device where a prior version has been certified, the certifier SHALL determine that no modifications that may impact the assessment results for a specific FSA line item have taken place if:

- the analysis submitted of the FSA matrix as described under Requirement ISASecure_EDM.R6 reports no changes to functionality covered by this line item of the FSA since the last certification; and
- a certifier review of evidence submitted per Requirement ISASecure_EDM.R5 and Requirement ISASecure_EDM.R6 finds no indication of such changes after consultation with the device vendor.

Requirement ISASecure_EDM.R9 – Criteria for granting a certification to a modified device

If an embedded device has been certified to level *n*, then a modified version of the device SHALL be granted certification to the same level and ISASecure EDSA version if:

- criteria for passing the CRT element of the certification are met per Requirement ISASecure_EDM.R3 and Requirement ISASecure_EDM.R7; and
- criteria for passing the FSA element of the certification are met per Requirement ISASecure_EDM.R4 and Requirement ISASecure_EDM.R8; and

- if developed by the same organization as a prior device that achieved certification, criteria for passing the SDSA are met per Requirement ISASecure_EDM.R2: or

- if developed by an organization that has not achieved certification for a device, all SDSA criteria in [EDSA-312] applicable to level *n* are assessed as pass for the development of this modified device by this organization.

7 Certification to updated ISASecure criteria

The requirements in this section cover certification of a device that holds a prior certification, to a later version of the ISASecure certification criteria. These requirements suffice in the case that the device itself has not undergone modifications as well. If it has, see Section 8.

Requirement ISASecure_EDM.R10 – CRT element for certification to a later ISASecure version

A device that has been ISASecure EDSA certified SHALL pass the CRT component of a certification to a later ISASecure version if:

- for any new protocols added in this ISASecure version, applicable tests as specified by the later ISASecure CRT specification are carried out and pass; and

- if there is a change in CRT test requirements for a previously certified protocol, then a full CRT for this protocol that meets the requirements of the later ISASecure specification version is carried out and passes.

Requirement ISASecure_EDM.R11 – FSA element for certification to a later ISASecure version

A device that has been ISASecure EDSA certified SHALL pass the FSA component of a certification to a later ISASecure version if:

- any new FSA requirements added in this ISASecure version are assessed for the device as either supported or allocatable; and

- any changed FSA requirements in this ISASecure version are assessed for the device as either supported or allocatable.

Requirement ISASecure_EDM.R12 – SDSA element for certification to a later ISASecure version

A device that has been ISASecure EDSA certified SHALL pass the SDSA component of a certification to a later ISASecure version if:

- any new SDSA requirements added in this ISASecure version are assessed as pass for the device; and

- any changed SDSA requirements in this ISASecure version are assessed as pass for the device.

Requirement ISASecure_EDM.R13 – Criteria for granting a certification to a later ISASecure version

A device that has been ISASecure EDSA certified to level *n* SHALL be granted a certification to a later ISASecure version at this same level if:

- Certification criteria for passing the CRT are met per Requirement ISASecure_EDM.R10;

- Certification criteria for passing the FSA for level *n* are met per Requirement ISASecure_EDM.R11; and

- Certification criteria for passing the SDSA for level *n* are met per Requirement ISASecure_EDM.R12.

The certification report SHALL cover only the tests and assessments performed for the certification as defined by these requirements.

8 Certification when both device and ISASecure version have changed

It will be a common scenario that a device will have changed slightly by the time a new version of ISASecure EDSA certification criteria is released. Thus it will be useful to be able to certify a slightly modified device to a newer version of ISASecure, without repeating the overall process. The following requirement provides a means to achieve this. It states that requirements are met in this case for both certification of modified devices and certification to later ISASecure versions.

Requirement ISASecure_EDM.R14 – Certification of a modified device to a later ISASecure version

For a device that previously received an ISASecure certification, a certifier SHALL grant a recertification to a later ISASecure version for a modified device if the criteria in both Requirement ISASecure_EDM.R9 and Requirement ISASecure_EDM.R13 are met.

9 Certification to a higher ISASecure EDSA level

Once a device has achieved certification at ISASecure EDSA certification at level *n*, the vendor may modify the device or available process evidence as deemed necessary, and then apply for a higher level certification. The following requirement applies in this situation.

Requirement ISASecure_EDM.R15 – Certification of a modified device to a higher ISASecure level

For a device that previously received an ISASecure certification to level *n*, a certifier SHALL grant a certification to a later ISASecure version for a modified device if:

- The criteria for granting a certification at the original level for the modified device are met per Requirement ISASecure_EDM.R9; and
- The additional FSA and SDSA requirements present at the desired new level certification that are not present at level *n* have been assessed as pass.

  In this case the certification report SHALL provide content per Requirement ISASecure_EDM.R9 as well as report on the new requirements assessed for the new certification level.