# SSA-310
# ISA Security Compliance Institute – System Security Assurance –
**Requirements for system robustness testing**

Version 2.0

April 2015

**A. DISCLAIMER**

ASCI and all related entities, including the International Society of Automation (collectively, “ASCI”)provide all materials, work products and, information (‘SPECIFICATION’) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the SPECIFICATION, and the provision of or failure to provide support or other services, information, software, and related content through the SPECIFICATION or otherwise arising out of the use of the SPECIFICATION. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SPECIFICATION.

WITHOUT LIMITING THE FOREGOING, ASCI DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THIS SPECIFICATION ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE SPECIFICATION AVAILABLE, ASCI IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS ASCI UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE. ANYONE USING THIS SPECIFICATION SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

**B. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES**

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL ASCI OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL,PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SPECIFICATION, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATON, SOFTWARE, AND RELATED CONTENT THROUGH THE SPECIFICATION OR OTHERWISE ARISING OUT OF THE USE OF THE SPECIFICATION, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS SPECIFICATION, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF ASCI OR ANY SUPPLIER, AND EVEN IF ASCI OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## Revision history

| version | date | changes |
|---|---|---|
| 1.02 | 9 Feb 2014 | Initial version published to http://www.ISASecure.org |
| 2.0 | 8 April 2015 | Change name and requirement number references for EDSA-310 v2,2, modify treatment of redundancy, convert SRT.R7 and R12 notes to be part of these requirements, add submission of jitter tolerance to SRT.R10, add detail to SRT.R14 rate limiting submission, change definitions for adequately maintain alarms, history, and external communication, SRT.R38 change regarding adequately maintaining control (excessive jitter criteria) to be consistent with EDSA-310 v2.2, add to SRT.R45 that embedded device may pass VIT under EDSA cert, make all reproducibility requirements consistent, clarify location of TD for testing throughout, perimeter firewall not to be CRT tested, add definition of operational mode and requirement for testing in modes that support control, no control monitoring during NST |
| | | |
| | | |

# Contents

## Figures



## Requirements

## FOREWORD

System robustness testing (SRT) is one of several elements required for ISASecure® certification of control systems. The other elements address security development lifecycle and functional security. The full current list of documents related to System Security Assurance (SSA) certification can be found on the ISASecure web site http://www.ISASecure.org.

# 1 Scope

This document is intended to provide requirements for testing the robustness of the System Under Test (SUT) as a measure of the extent to which the SUT defends itself against:

- known vulnerabilities;
- incorrectly formed messages and sequences of such messages;
- single erroneous messages.

This testing, hereby known as System Robustness Testing (SRT) will be performed in 4 phases:

- Asset Discovery Testing
- Vulnerability Identification Testing (VIT)
- Communications Robustness Testing (CRT)
- Network Stress Testing (NST).

The goal of the test approach is to identify the presence of known software vulnerabilities and known vulnerabilities of networking protocols, which impact the robustness of systems that use this software and these protocols. Tests are specified to a level such that these goals are covered, although specific test data is not defined. These tests will not necessarily identify software vulnerabilities other than the known vulnerabilities included in the latest released version of ISASecure® System Security Assurance (SSA). Development process assurances such as the Security Development Lifecycle Assessment (SDLA) mitigate the potential for software vulnerabilities.

# 2 Normative references

[EDSA-310] *ISCI Embedded Device Security Assurance – Requirements for embedded device robustness testing,* as specified at http://www.ISASecure.org

[PORT] *IANA port numbers*, as specified at http://www.iana.org/assignments/port-numbers

[SSA-300] *ISCI System Security Assurance – ISASecure Certification Requirements,* as specified at http://www.ISASecure.org

[SSA-420] ISCI System Security Assurance – Vulnerability Identification Testing Policy Specification, as specified at http://www.ISASecure.org

# 3 Definitions and abbreviations

## 3.1 Definitions

**3.1.1**
**accessible network interface**
network interface declared by the system certification applicant as suitable for use during operation or maintenance, that supports for operation or instrumentation any protocol subject to SRT, and such that connection can occur without physical reconfiguration

NOTE Some network interfaces on systems are internal connections only, and/or have physical protection intended to help prevent an unauthorized network connection. These would not be considered to be accessible network interfaces, and would not be subject to SRT testing.

**3.1.2**
**adequately maintain essential function**
maintain essential functions at a level deemed suitable for a control system while under a given type of attack

NOTE See definition below for essential function and Section 4.1.

**3.1.3**

**conduit**

logical grouping of communication channels, between connecting two or more security zones, that share common security requirements
**Reference: ISA-62443.03.02**

**3.1.4**
**control system (CS)**
hardware and software components of an IACS

**Reference: ISA-62443.03.03**

**3.1.5**
**core protocol**
protocol in the set ICMP, IPv4, ARP, IEEE 802.3 (Ethernet II), UDP or TCP

NOTE These protocols form the underlying infrastructure for many other protocols used in CS. Additional CS specific application level protocols may be added to this list in the future.

**3.1.6**
**digital output**
output that can take on two values, representing 0 and 1

**3.1.7**
**discrete output**
output that can assume a pre-defined, finite number of values (usually represented as small unsigned integers)

**3.1.8**
**external communication**
communication leaving and entering the boundaries of the system

NOTE External communications can be with another system or with components for viewing, changing or recording process parameters or alarms. External communications are essential if they are necessary for supporting an essential function (e.g. process view, command, alarms, etc.).

**3.1.9**
**essential function**
function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

NOTE Essential functions include but are not limited to the safety instrumented function (SIF), the control function, and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control, and loss of view respectively. In some industries additional functions such as history may be considered essential.

**3.1.10**
**jitter**
the difference between the time a signal event is detected and the expected time based on a reference signal

**3.1.11**
**measurement jitter**
possible error in jitter measurement

**3.1.12**
**monitoring system**
special purpose system consisting of embedded devices, PCs and/or network components which are suitably combined to directly monitor an industrial process or processes

NOTE Examples are an independent critical alarm system, wireless monitoring system, tank gauging system, temperature monitoring system, vibration monitoring system.

**3.1.13**
**network segment**
logical division of a computer network in which all nodes can reach each other by broadcast at the data link layer (broadcast domain)

**3.1.14**
**operational mode**
device state that is manually selected to allow access to particular device functions, such as configuration, control operations, update

NOTE Not all embedded devices use the concept of operational modes.

**3.1.15**
**protocol data unit**
Information that is delivered as a unit among peer entities of a network and that may contain control information, such as address information, or user data

**3.1.16**
**security zone**
grouping of logical or physical assets that share common security requirements

**Reference: ISA-62443.01.01**

**3.1.17**
**Supervisory Control And Data Acquisition (SCADA)**
computer systems that monitor and control industrial, infrastructure, or facility based processes

**3.1.18**
**test laboratory**
accredited organization that is carrying out system robustness testing for the ISASecure SSA certification process

### 3.2 Abbreviations

The following abbreviations are used in this document.

| | |
|---|---|
| ACL | Access Control List |
| ARP | Address Resolution Protocol |
| ASCI | Automation Standards Compliance Institute |
| CRT | Communication Robustness Testing |
| CS | Control System |
| DoS | Denial of Service |
| EDSA | Embedded Device Security Assurance |
| ERT | Embedded Device Robustness Testing |
| IACS | Industrial Automation Control System |
| ICMP | Internet control message protocol |
| IEEE | Institute of Electrical and Electronic Engineers |
| I/O | Input/Output |
| IP | Internet (network layer) Protocol |
| IPv4 | IP version 4 (uses 32-bit network layer addresses) |
| ISCI | ISA Security Compliance Institute |
| (*N*)PDU | (*N*-layer) protocol data unit, where *N* = D (data-link), N (network), T (transport), A (application), etc. |
| NST | Network Stress Testing |
| OS | Operating System |
| PC | Personal Computer |
| PLC | Programmable Logic Controller |
| SCADA | Supervisory Control And Data Acquisition |
| SDLA | Security Development Lifecycle Assurance or Assessment |
| SIF | Safety Instrumented Function |
| SIS | Safety Instrumented System |
| SRT | System Robustness Testing |
| SSA | System Security Assurance |
| SUT | System Under Test |
| TCP | Transmission Control Protocol |
| TD(s) | Testing Device(s) |
| UDP | User Datagram Protocol |
| VIT | Vulnerability Identification Testing |

# 4 SRT pass criteria

## 4.1 Meaning of “essential function”

Conceptually, the set of essential functions is a subset of system services that need to be available in order for the system to perform its intended function within a defined set of application environments. A system must maintain the control loop, safety instrumented function, process view, alarm and command in all environments, and maintain certain historical information in regulated environments (e.g. pharmaceutical). The impact of this concept on SRT is that to pass these tests, all functions that are identified as being essential in the intended application environment(s) for a system per the requirements following, must be “adequately maintained” under network attacks and other adverse network conditions as simulated during testing.

ISCI identifies in this specification those functions that are always considered essential, for all application environments, and therefore always subject to test. ISCI also identifies functions that are essential in some application environments. An applicant for certification may explicitly exclude testing for the latter functions. The certification report indicates whether or not the applicant excluded testing for any of these functions. If an exclusion is reported, this signifies to the end user that the system is not intended for use in application environments where those functions not tested are essential.

NOTE ISCI has not defined a taxonomy mapping of application environments to required functions. Thus the end user will determine whether a function that has not been tested for a certified system is essential for their environment.

Essential functions fall into two classes, “upward” and “downward.” Downward functions are the interface to the process being controlled. Upward essential functions are interfaces to *peer or higher level* entities in the architecture. The following are the essential functions in these classes for the purposes of SRT:

- Downward: *the control function, the safety instrumented function (SIF)*
- Upward: *process view*, *command* (meaning change parameters of process control such as set points), *process alarms*. *Providing essential process history* is an essential function unless explicitly excluded by the certification applicant.
- External process communications are essential functions if they are necessary for other essential services (e.g. process view, command, alarm, process history).
- Certification applicant added: the certification applicant may specify additional essential functions.

Thus essential functions may be time-critical or non-time-critical services.

### 4.1.1 Meaning of “adequately maintain essential functions”

#### 4.1.1.1 General

The meaning of the term “adequately maintain an essential function,” is dependent upon the particular essential function. It is defined as follows for each such function. Among all downward functions and all upward functions, these definitions are nearly identical. In summary, it is acceptable for upward functions to be lost due to interference from flooding on their own network interface, but not due to any other network traffic conditions. It is not acceptable for downward functions to be lost under any network traffic conditions.

#### 4.1.1.2 Meaning of “adequately maintain control capability”

A system is said to adequately maintain control capability if the control function is maintained with the existing control parameters, under any network traffic conditions on all accessible system network interfaces. This definition describes the opposite of “loss of control.” Note this is distinct from the capability to command a change to the parameters controlling the process, described next.

#### 4.1.1.3 Meaning of “adequately maintain command capability”

A system is said to adequately maintain command capability if network traffic on the interface used for commanding the control devices does not disable the capability to respond to commands from higher level components in a timely fashion, other than due to continuous flooding on that interface. A system component may intentionally disable command response temporarily due to invoking a defense mechanism against

flooding. However if it invokes such a defense, it returns to normal processing once flooding ceases, without operator intervention in a manner consistent with the documented design. Network traffic on other accessible system interfaces does not interfere with the capability to achieve the timely response to commands.

#### 4.1.1.4 Meaning of “adequately maintain view”

A system is said to adequately maintain view if network traffic on the interface used for providing process view cannot disable the capability to provide this view in a timely fashion, other than due to continuous flooding on that interface. A system component may intentionally disable process view temporarily due to invoking a defense mechanism against flooding. However if it invokes such a defense, it returns to normal processing once flooding ceases, without operator intervention in a manner consistent with the documented design. Network traffic on other accessible system interfaces does not interfere with the capability to provide process view in a timely fashion.

#### 4.1.1.5 Meaning of “adequately maintain alarms and alarm reporting”

A system is said to adequately maintain alarms and alarm processing if network traffic on the interface used for providing alarms cannot disable the capability to send these alarms in a timely fashion, other than due to continuous flooding on that interface. A system component may intentionally disable alarm reporting temporarily due to invoking a defense mechanism against flooding. However if it invokes such a defense, it returns to normal processing once flooding ceases, without operator intervention in a manner consistent with the documented design. Alarm state is not lost during continuous flooding, though reporting of alarms may be delayed. Network traffic on other accessible system interfaces does not interfere with the capability for timely reporting of alarms.

#### 4.1.1.6 Meaning of “adequately maintain history”

A system is said to adequately maintain essential history reporting if network traffic on the interface used for essential history reporting cannot disable the capability to send essential history data in a timely fashion, other than due to continuous flooding on that interface. A system component may intentionally disable essential history reporting temporarily due to invoking a defense mechanism against flooding. However if it invokes such a defense, it returns to normal processing once flooding ceases, without operator intervention in a manner consistent with the documented design. Essential history data is not lost during flooding, though reporting of data may be delayed. Network traffic on other accessible system interfaces does not interfere with the capability to achieve the timely reporting of essential history data.

NOTE Reasonable, acceptable time period are defined and agreed on between applicant and test laboratory prior to test as described in requirement SRT.R21.

#### 4.1.1.7 Meaning of “adequately maintain external communication”

A system is said to adequately maintain external communication if network traffic on the interface used for external communication cannot disable the capability to send this communication in a timely fashion, other than due to continuous flooding on that interface. In the case of continuous flooding, if external communication cannot be maintained, the system adequately maintains the other essential functions supported by this communication. Network traffic on other accessible component interfaces does not interfere with the capability to achieve timely external process communications. It is assumed that other than flooding of the component interface used for external control communication, the external channel is unobstructed.

#### 4.1.1.8 Meaning of “adequately maintain safety instrumented function”

A safety instrumented system (SIS) is said to adequately maintain safety instrumented function if network traffic on the interface to the SIS cannot disable the capability to perform the safety function.

### 4.1.2 Criterion for SRT pass

Requirements later in this document describe how the preceding definitions for “adequately maintain an essential function” are applied in the context of SRT. These later requirements rely upon the above definitions to provide criteria for passing the asset discovery, VIT, CRT and NST tests.

The requirement in this section specifies how a test laboratory will define for a given system, the overall criterion for passing the SRT.

**Requirement SRT.R1 – Criterion for SRT pass**

A test laboratory SHALL determine that the SRT for a system has passed if all components of the system submitted for certification pass all SRT tests listed in the Test Plan per Requirement SRT.R16 “Type and sequence of tests”. If a system as submitted for certification includes multiple accessible network interfaces, then all accessible network interfaces SHALL be required to pass applicable tests as a part of the system.

## 5 System robustness testing process

This section defines the SRT process. Figure 5-1 is a flow chart that illustrates the process. The remainder of this document will detail each step of the process and enumerate the requirements of the certification applicant and the test laboratory in each of the steps involved in the process.

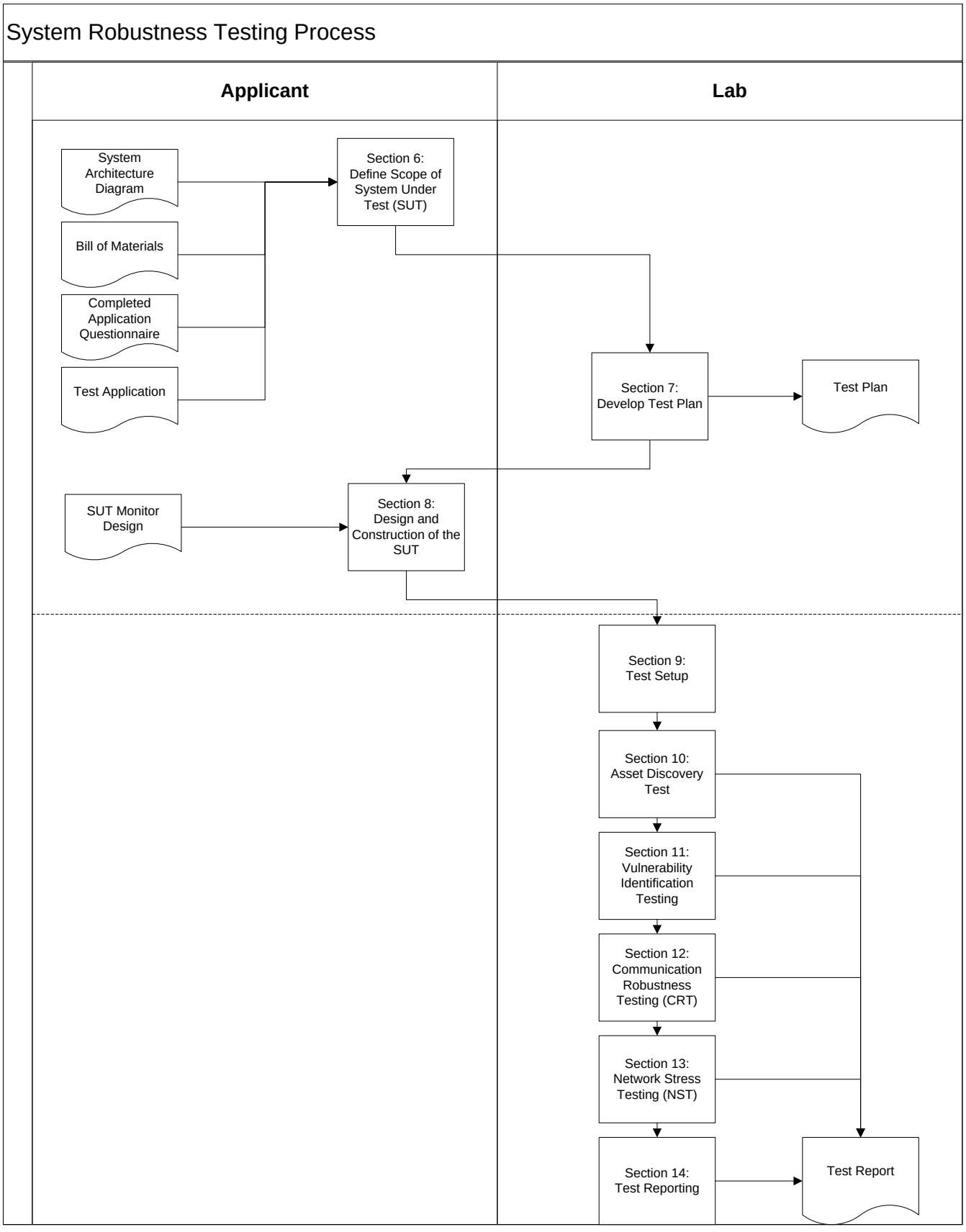


**Figure 5-1: System robustness testing process**

# 6 Define scope of System-under-Test

## 6.1 Definition of type of system

The system-under-test (SUT) is defined as a system such as a Control System (CS), SCADA system or monitoring system that is available from a single system supplier. A SUT may be comprised of hardware and software components from several manufacturers but is integrated into a single system and supported, as a whole, by a single supplier. SRT evaluation will be performed on a reference system that is clearly defined by the applicant.

## 6.2 Technical submissions from certification applicant

This section defines requirements on the *technical submission* required from a certification applicant in order to support SRT. The technical submission consists of the following items:

- System architecture diagram that shows all components with all communications connections and the security zones and conduits of the system
- List of hardware and software versions of all components and applications (e.g. Bill of Material)
- Existing ISASecure EDSA Certificates
- Configuration rules (for firewalls and network components) if included as components of the system.

A subset of the design information required from the certification applicant is related to essential functions supported by the system.

**Requirement SRT.R2 – Submission of architecture diagram of system**

A certification applicant SHALL submit for SRT an architecture diagram of the system to be certified that clearly defines its components and connections. The architecture diagram SHALL show every component (embedded, I/O, PC, network, etc.) included in the system along with its connections to other components in the system and external to the boundaries of the system. The diagram SHALL show the boundaries of the system as well as the boundaries of all included security zones within the SUT, and all communication protocols that traverse the boundary of the system, including IP as well as I/O communications protocols (wired or wireless).

NOTE 1 Figure 6-1 shows an example architecture diagram. The notation "E1" mean that the Control System Servers in the Process Control Zone are reachable from Industrial Ethernet through the perimeter firewall in the Process Operations Zone. Likewise, Control-ED is reachable via External Interface 2.

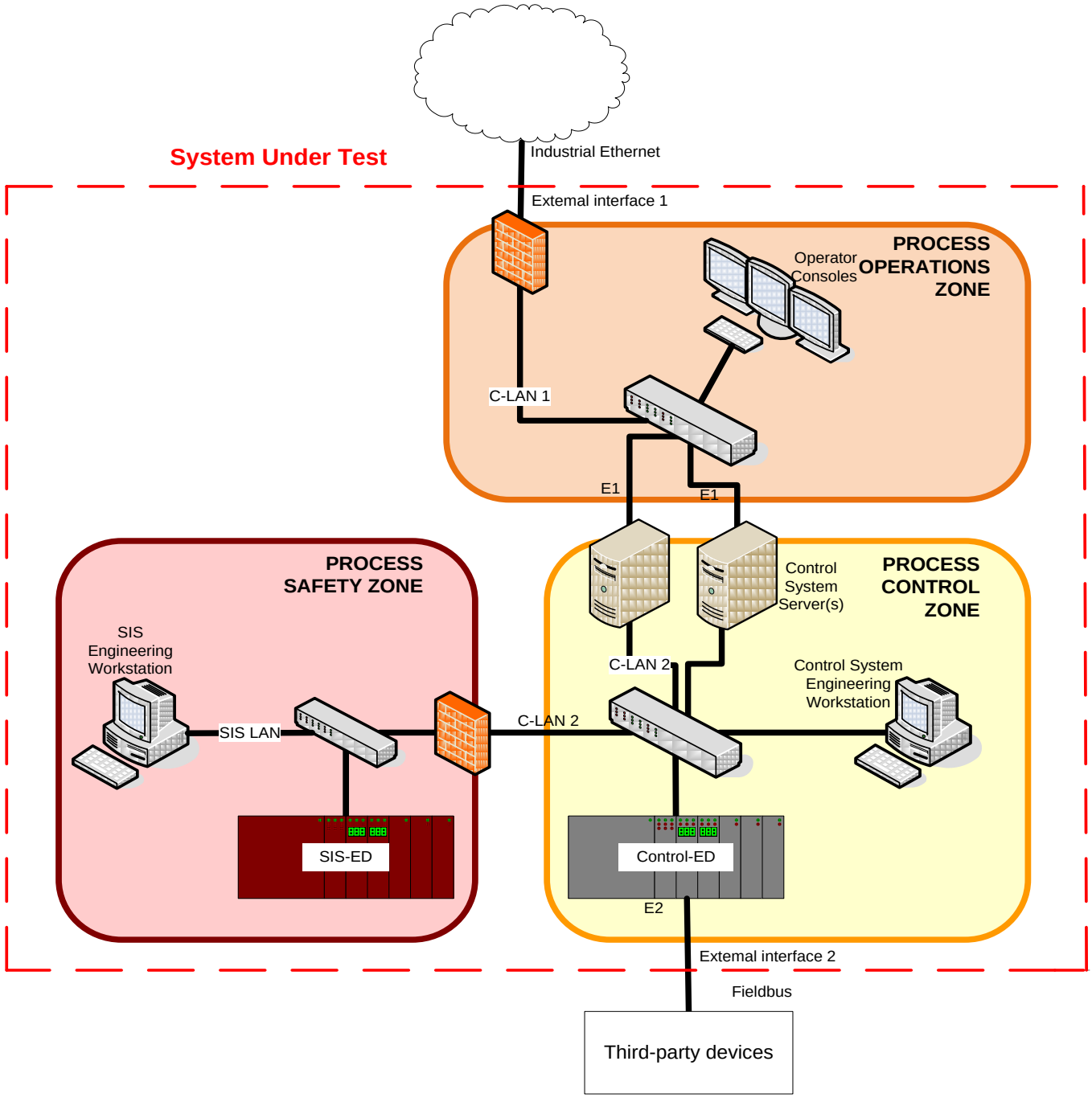


**Figure 6-1 Example architecture diagram**

**Requirement SRT.R3 – Submission of list of system hardware and software (e.g. Bill of Materials)**

A certification applicant SHALL submit for SRT a system that is or will be unambiguously identifiable and specifiable by an end customer for procurement. The information submission SHALL be for each component defined in the Bill of Material and SHALL include:

- Manufacturer, and part numbers of all embedded devices;

    - Hardware, firmware, and software versions of each embedded and I/O component.
- Manufacturer, and part numbers of all hosts;
    - Hardware;
    - OS, OS version and service pack levels;
    - VM OS versions and service pack levels (if Virtual Machines are included).
- Applications installed on all hosts:
    - Certification applicant developed and third party application name and type;
    - Versions and service pack versions of all installed and included applications.
- Manufacturer, and part numbers of all network components with:
    - Version and service pack levels;
    - Details of configuration rules (e.g. ACL's).

**Requirement SRT.R4 – Submission of ISASecure EDSA certificates for all certified embedded devices**

The certification applicant SHALL submit to the certification process any ISASecure EDSA certificates and FSA sections of EDSA certification reports the applicant has obtained for the embedded devices in the SUT. If VIT evidence for an EDSA certified embedded device is to be applied for SSA per Requirement SRT.R45, then the VIT section of the EDSA certification report SHALL also be submitted.

NOTE 2 The FSA section of the report may be needed to determine if allocatable requirements for a certified embedded device are covered by some other component of the system, as required for SSA certification.

**Requirement SRT.R5 – Submission of end user system documentation**

The certification applicant SHALL submit to the certification process all documentation (printed, on-line or otherwise) that is delivered along with, or made available to, an end customer who purchases the system submitted for certification. This SHALL include all manuals and pertinent documentation for each component of the SUT.

**Requirement SRT.R6 – Submission of list of components performing essential functions**

The certification applicant SHALL submit to the test laboratory a list of all components of the system that are performing essential functions as described in 4.1.

**Requirement SRT.R7 – Submission of essential functions**

A certification applicant SHALL indicate which essential functions the system has the capability of performing from the following list:

1. The control function
2. The safety instrumented function
3. Process view
4. Process command
5. Process alarm
6. Process history
7. External connections
8. Any additional essential functions

For items 1 through 5, if the system has the capability to perform these functions, then they SHALL be included in the submittal. Items 6 through 8 MAY be submitted as essential functions by the certification applicant.

**Requirement SRT.R8 – Submission of definition of essential history data**

A certification applicant that considers maintaining history data an essential function and does not exclude this per Requirement SRT.R7 SHALL describe those types of historical records and fields in these records that they consider to be essential history data.

**Requirement SRT.R9 – Submission of definition of essential external communications**

A certification applicant that considers external communications an essential function SHALL describe those types of external communications that they consider to be essential functions.

**Requirement SRT.R10 – Submission of response times and update rates**

A certification applicant SHALL submit time unit values for the response times and update rates of the essential system functions (i.e. display update rates, history update rates, trend display cycle times, operator response time, etc.), that represent the expected performance of the system. A certification applicant SHALL submit a time unit value for maximum jitter tolerance for control output (value and confidence) that represents the expected performance of each embedded device component of the system. The confidence SHALL be a minimum of 95%.

NOTE 3 The confidence is a percentage, for which this percentage of all jitter measurements, are expected to be less than the maximum tolerance stated. As an example, if values of 50ms and 95% were submitted, this means that 95% of all measurements of jitter are expected to be less than 50ms.

NOTE 4 These values are used in determining pass/fail, for SRT tests.

**Requirement SRT.R11 – Submission of list of accessible network interfaces**

A certification applicant SHALL submit to the certification process a list that clearly identifies all network interfaces present for each of the components of the system that they define as *accessible* interfaces. The list SHALL include and identify those accessible interfaces that provide an external interface to the system or to a security zone. The list of accessible interfaces SHOULD include all interfaces such that:

- the certification applicant recommends the interface to customers as suitable for use during operations or maintenance;
- the interface supports any protocol subject to SRT;
- the interface is used to interface with operator consoles or instrumentation; and
- connection to the interface can occur without physical reconfiguration of the normal operational configuration.

NOTE 5 For example, consider a network switch or router that is installed in a cabinet which can be locked by the end user. Physical network ports that have cables outside the cabinet are considered “accessible”. Physical network ports that are contained within the cabinet (e.g. maintenance port) are not considered “accessible.”

**Requirement SRT.R12 – Submission of list of accessible points of entry**

A certification applicant SHALL submit to the certification process a list that clearly identifies all accessible points of entry for each of the components of the system that is defined as performing essential functions. The list of accessible points of entry SHALL include all points of data entry whether they are enabled or not, and SHALL include:

- all network connections (e.g. Ethernet);
- all local connections (e.g. USB, Firewire, serial);

- all wireless communications or wireless communications options (e.g. Wireless HART, ISA100, WiFi, Bluetooth, wireless mouse, wireless keyboard, etc.);
- all insertable media points (e.g. CD, DVD, floppy disk, SD card readers, etc.).

These MAY include both hardware and software points of entry.

**Requirement SRT.R13 – Submission of implemented protocols**

The certification applicant SHALL submit a list of all IP protocols that are supported on each of the components of the system that are performing essential functions.

**Requirement SRT.R14 – Submission of description of intended system defensive behavior**

For each protocol supported by the system which is covered by SRT, a certification applicant SHALL submit information that indicates one of:

a) traffic received under that protocol is not subject to rate limiting, in other words the design of the system does not distinguish between rates of incoming traffic

b) traffic received by the system is subject to rate limiting.

In case b) the applicant SHALL also provide a *known limited rate* which is a message quantity per unit time which is known to be sufficient to ensure that the system will display its rate-limiting behavior, and SHALL describe the anticipated change in system behavior and the conditions under which behavior returns to "normal."

In particular the applicant SHALL provide the known limited rate in terms of approximate number of minimal-length valid messages per second, for the lowest-level protocol(s) implemented by the system that support protocols covered under SRT.

NOTE 6 Therefore for example, if a system device uses Ethernet as the lowest level protocol supporting all protocols covered by SRT, the supplier need only specify the rate limit at which its Ethernet receiver goes into rate-limiting when receiving minimal-length (i.e., 64 B) Ethernet frames.

Similarly, a certification applicant SHALL provide a description of any other defensive behavior employed by the system that may impact certification testing. For example the system may employ IP address blacklisting, where an IP address is blocked if it previously has sent suspicious or excessive traffic to the system, or may employ a redundant configuration that provides automatic failover if one or more of the redundant units detects adverse conditions or fails.

NOTE 7 Knowing a limiting rate in advance makes the test process more efficient, but the validity of the rate submitted will not impact pass/fail of SRT.

**Requirement SRT.R15 – Submission of suitable test configuration**

A certification applicant SHALL submit to the certification process a suitable test configuration that is representative of the specified usage of the SUT.

## 7 Develop test plan

The test laboratory will review the applicant's technical submissions and prepare a test plan that meets the following requirements:

**Requirement SRT.R16 – Type and sequence of tests**

The test plan SHALL include a list of the type of tests to be performed on each component in the system and the planned sequence of tests.

**Requirement SRT.R17 – Test points**

The test plan SHALL include a list of the access points to be tested. This SHALL include each access point for each security zone within the SUT. This SHALL include all accessible network interfaces and accessible entry points specified in Requirement SRT.R11 and Requirement SRT.R12.

**Requirement SRT.R18 – Monitor requirements**

The test plan SHALL identify the requirements for upward and downward essential functions monitors with sufficient detail for the applicant to be able to design and implement the necessary system configuration.

# 8 Design and construction of the SUT

## 8.1 Design of SUT

The applicant prepares and submits a design for the SUT to the certification laboratory that meets the following requirements:

**Requirement SRT.R19 – Submission of method to exercise essential functions**

A certification applicant SHALL submit a method that can be used to exercise each essential function to assure it maintains expected performance as defined in Requirement SRT.R10 during testing. The test configuration SHALL ensure that communications is occurring between all components within the SUT.

**Requirement SRT.R20 – Submission of method to achieve recommended system loading**

A certification applicant SHALL submit a method that can be used to load the system to the level recommended in documentation for end users, and a method to verify this load has been achieved and maintained. Each component of the system is to be configured and running at the level recommended for that component.

NOTE 1 These methods will be used to load and verify the load on the system during SRT testing, since certification will require that essential services are maintained under all network traffic conditions as well as recommended load on the system.

NOTE 2 It is expected that different certification applicants will use different parameters or combinations of parameters to specify recommended load, for example CPU and memory utilization.

**Requirement SRT.R21 – Submission of design for essential function monitors**

The certification applicant and the test laboratory SHALL agree in advance of testing on the design for testing via monitoring of the essential functions indicated by the certification applicant as required by Requirement SRT.R7 to be tested via monitoring. The design MAY utilize components included in the SUT or components external to the SUT designed to communicate with the SUT. The monitoring tests SHALL determine whether the following desirable operating conditions hold, where applicable to the system:

a) Whether the system is maintaining the integrity and availability of the safety instrumented function

b) Whether the system is responding to commands to change parameters of the controlled process, in a timely fashion (such as changing a set point)

c) Whether the system is providing a view of the process in a timely fashion

d) Whether the system is providing process alarms in a timely fashion, including maintaining alarm state although alarm delivery may be delayed, as designed;

e) Whether the system is maintaining essential history data, including history data deemed undeliverable;

f) Whether the system is providing timely external communication, where this includes successfully sending messages over an unobstructed channel, and supporting adequate maintenance of the essential functions supported by this communication;

g) Whether the system is adequately maintaining any additional essential functions submitted under SRT.R7.

NOTE 3 The method for monitoring adequate maintenance of the control function is not covered by this requirement since it is explicitly defined later in this specification, in SRT.R38.

### 8.2 Construction of the SUT

The applicant constructs and configures the system hardware and software that is submitted for SRT along with any other supporting hardware and software that may be needed to monitor external communications.

**Requirement SRT.R22 – Submission of System-under-Test**

A certification applicant SHALL submit to the certification process the hardware/software as described in Requirement SRT.R3 –"Submission of list of hardware and software (e.g. Bill of Materials)" as necessary to carry out SRT. The necessary hardware/software for monitoring per SRT.R21– "Submission of design for essential function monitors" SHALL also be submitted.

**Requirement SRT.R23 – Single configuration SUT**

All tests and assessments required for SRT SHALL pass on one physical SUT of identical components and configuration in order for SRT to pass for that model of system.

NOTE This requirement means that the certifier cannot run some of the SRT tests on one set of components of the system and others on an upgraded or otherwise modified version of the system.

## 9 Test setup

Upon arrival at the site where SRT testing will be conducted, the test laboratory will prepare for testing per the following requirements:

**Requirement SRT.R24 – Verify scope**

The test laboratory SHALL verify that the SUT provided by the applicant agrees with the information submitted by the applicant in Section 6.2 and document any variations.

**Requirement SRT.R25 – Verify loading**

The test laboratory SHALL verify that the SUT provided by the applicant has been configured to be loaded per the method provided by the applicant per Requirement SRT.R20, "Submission of method to achieve recommended system loading."

**Requirement SRT.R26 – Initialize test equipment**

The test laboratory SHALL initialize all test equipment that will be used during SRT. This includes, but is not limited to: configuration of test devices, installation of software updates, loading of test suites, and entering all applicable test parameters.

**Requirement SRT.R27 – Connect test equipment**

The test laboratory SHALL connect the test equipment to prepare for the first test and verify it is properly connected and functioning. This process SHALL be repeated every time the test equipment is disconnected and reconnected.

Figure 9-1 shows connection points for SRT testing for the example system in Figure 6-1. The TD (Test Device) connections shown are the connection points for Communication Robustness and Network Stress Testing.

As determined by SRT.R49, devices accessible from external system interfaces are targets for CRT, and CRT against these devices is performed from those external interfaces. In addition, CRT is performed using a direct network connection against all embedded device components of the system. A connection of the CRT testing device to a switch as shown in the figure below, is considered "direct" if the switch does not have functionality that may delete malformed traffic generated for basic CRT tests. If the switch may delete such traffic for some tests, then a hardwired or other direct network connection would be used to perform those tests.

The targets for NST are determined by SRT.R54 and SRT.R55 to be all network interfaces on each network segment. NST is performed from a testing device on the network segment.

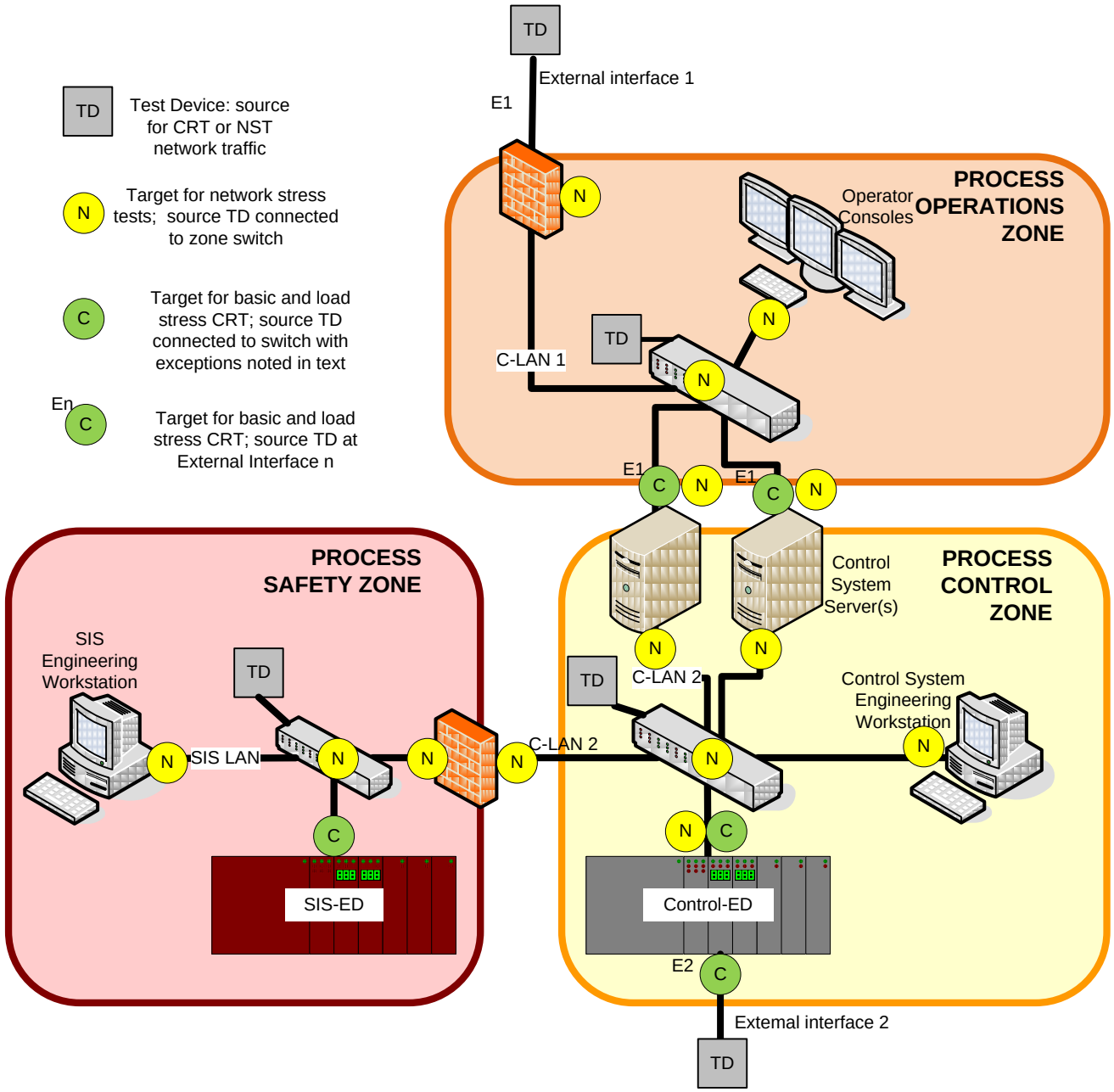


**Figure 9-1: System connection points**

**Requirement SRT.R28 – Verify monitors**

The test laboratory SHALL verify that the SUT provided by the applicant has been configured with the essential function monitors as documented in the design specified in Requirement SRT.R21, “Submission of essential function design for monitors.” The test laboratory SHALL verify the operation of the monitors under normal (non-test) conditions. The test laboratory SHALL also verify the operation of any monitors or test fixtures provided by the test laboratory.

# 10 Asset discovery testing

## 10.1 General

The asset discovery testing is the first test run as part of the SRT. It has two purposes:

- to identify IP addresses and the TCP and UDP ports and services active on each component of the system; and
- to test whether essential functions on the system are adequately maintained during a port scan.

**Requirement SRT.R29 – Asset discovery tests precedence**

Asset discovery test cases as defined in Section 10 SHALL be the first SRT tests performed and SHALL be performed from each Ethernet access point of each security zone included in the SUT.

## 10.2 Test configurations

### 10.2.1 Basic asset discovery test configuration

The basic asset discovery test configuration consists of one or more TDs sending packets to each of the components of the SUT while monitoring the performance of the SUT essential functions. Two test configuration variants are used during the asset discovery testing, corresponding to the two purposes of the test. This is due to the fact that many systems are deployed in conjunction with separate or integrated firewall functions.

For the purposes of determining ports and services that are active on the components of the SUT, where possible, any firewalls are disabled, so that the basic protocol capabilities of each component of the underlying system can be more readily determined.

For the purposes of examining how the system maintains essential functions during a port scan, the firewall functions are configured as they would be by the end customer.

**Requirement SRT.R30 – Basic asset discovery test configuration**

The configuration for the asset discovery testing SHALL include the following elements:

a) each component in the system

b) one or more testing devices that generate the network traffic/stimuli required to carry out the testing

c) the configuration required to carry out the methods for monitoring upward essential functions as described per Requirement SRT.R21

d) the configuration described per Requirement SRT.R31 that is required to monitor downward essential functions; and

e) a wired switched or non-switched network path that connects all of the above components.

NOTE Typically the system used to send the network traffic for the scanning process is the host for Nmap or a similar tool.

### 10.2.2 Configuration for downward essential functions monitoring

**Requirement SRT.R31 – Configuration for downward essential functions monitoring during asset discovery testing**

The test configuration for asset discovery testing SHALL include the following to allow monitoring of the control loop/safety instrumented function:

a) a control program on the system that provides observable expected control outputs, specified in Requirement SRT.R38 “Test criteria for adequately maintain control capability”

b) control programs necessary to load each of the components of the SUT to the predefined typical level recommended to end users, and to verify this load has been achieved and maintained by the methods specified per Requirement SRT.R20 “Submission of method to achieve recommended system loading”

c) a testing device which is a monitoring component that is capable of receiving the analog and digital control outputs of the SUT and collecting data to support the calculation of jitter on the signals received in ms, to the accuracy stated in Requirement SRT.R38 “Test criteria for adequately maintain control capability”

NOTE 1 This testing device need not be the same physical device as the testing device that generates network traffic for the test.

NOTE 2 This testing device can calculate jitter in real time or the calculation can be done off-line based on data from the testing device. Performing the calculation in real time permits more advanced test branching based upon observed results.

### 10.2.3 Configuration for firewalls

**Requirement SRT.R32 – Configuration for SUT during asset discovery testing**

The test configuration for the asset discovery testing SHALL support option a) as follows, and SHOULD support option b) where possible.

a) Any system protection SHALL be preconditioned in the configuration defined for end customer use. For example: Any system protection intermediary between the SUT and TD SHALL be so configured.

b) Any system protection available on the SUT such as firewalls intermediary between the SUT and the TD SHALL be preconditioned in a manner that will allow effective testing per section 10.3 for the purposes of determining ports and services that are active on the components of the SUT. Example: Disabling of any rules that block the transmission of any type of network traffic between the SUT and TD.

### 10.3 Test procedure

The asset discovery test procedure involves scanning for UDP and TCP ports that may be active and for IP protocol types.

A UDP TPDU addressed to a closed port SHOULD be replied to with an ICMP Port Unreachable PDU. However, since such a reply can itself be used as a multiplying factor in DoS attacks and as a means of gaining information about the queried subsystem, the SUT also MAY ignore the UDP TPDU and not generate such an ICMP reply PDU. Hence either of these results is interpreted to mean that the port is not active.

**Requirement SRT.R33 – UDP port scan**

Asset discovery testing SHALL include a scan of all (0-65535) UDP ports of each component in the system to determine which of those ports is active in each component. This port scan SHALL be performed on every component in system with a network interface. This scan SHALL be performed against all accessible interfaces of each component per Requirement SRT.R29 “Asset discovery tests precedence.” The scan SHALL take the form of UDP TPDUs with non-zero (and preferably plausible) content sent to each of the 65536 possible UDP ports that each component of the system may recognize. The system components may respond to this testing with a Port Unreachable ICMP PDU per RFC1122, 4.1.3.1, or it may ignore the received UDP TPDU. Any other response SHALL be interpreted that the port is active. The test configuration for this scan SHOULD meet Requirement SRT.R32b.

**Requirement SRT.R34 – TCP port scan**

Asset discovery testing SHALL include a scan of all (0-65535) TCP ports of each component in the system to determine which of those ports is active. This port scan SHALL be performed on every component in the system with a network interface. This scan SHALL be performed against all accessible interfaces of each component per Requirement SRT.R29 “Asset discovery tests precedence.” The scan SHALL take the form of an attempt to establish a complete TCP connection sent to each of the 65,536 possible TCP ports that each component of the system may recognize. The system component may respond to this testing with a Port Unreachable ICMP PDU, or it may ignore the connection attempt. Any other response SHALL be interpreted that the port is active. The test configuration for this scan SHOULD meet per Requirement SRT.R32b.

Example: Nmap commands that would achieve these last two requirements for an IPv4 component using the nmap tool version 5.21 are:

nmap –sU –vv –p0-65535 target_ip, for UDP

nmap –sT –vv –p0-65535 target_ip, for TCP

In these commands the parameters have meanings as follows:

- -sU designates a UDP scan
- -sT designates a TCP connection scan, which is distinct from a SYN scan (-sS) in which a complete TCP connection is not established
- -vv requests “very verbose” feedback from nmap while the scan is progressing
- -p0-65535 designates that all possible ports should be scanned
- Target_ip the IP address for the SUT

**Requirement SRT.R35 – IP protocol type scan**

Asset testing SHALL include a scan for all IP protocol types for each component of the system. The test configuration for this scan SHOULD be per Requirement SRT.R32b.

**Requirement SRT.R36 – Scan coverage of all accessible network interfaces and system modes**

Asset discovery testing SHALL include a UDP port scan, TCP port scan, and IP protocol type scan of each component in the system. The scan SHALL be performed in all operational modes over each accessible Ethernet network interface, while running all essential functions that are available in these modes in such a way as to support monitoring of upward and downward essential functions.

**Requirement SRT.R37 – Reproducibility of determination of ports that may be active**

The method for determining which UDP and TCP ports may be active SHALL be reproducible.

NOTE For example, if using nmap, one would record the version of nmap used for the scan.

### 10.4 Test pass criteria

#### 10.4.1 General

The set of potentially active UDP or TCP ports and/or other IP-based protocols does not determine whether a SUT passes asset discovery testing. Pass/fail is determined by the behavior of the SUT during the port scans that comprise these tests.

During asset discovery testing, the system is subjected to a variety of scans. In overview, a system will pass asset discovery testing if it adequately maintains essential functions throughout the tests. Section 4 defines those services that are essential.

This section defines what it means to adequately maintain essential functions. The general definitions are provided in 4.1.1 followed by requirements in 4.1.2 that specify how these definitions are applied in the context of the SRT.

**Requirement SRT.R38 – Test criteria for "adequately maintain control capability"**

A system SHALL be determined to have adequately maintained control capability during a test if a specified cyclically-repeated waveform is measured to have observed time jitter over the test period that meets or exceeds the maximum jitter tolerance and confidence value submitted by the certification applicant per Requirement SRT.R10, and does not exhibit specified anomalous behavior, as defined in detail below.

a) for systems that can create an analog output, each cycle of the waveform SHALL consist of 10 equal steps of increasing value and then 20 equal steps of decreasing value, both at one step per second, transitioning between the nominal minimum and maximum values of the output component

b) for systems that can create a digital output, the waveform SHALL consist of a rectangular wave with a 1/3 duty cycle and 3 s period, of 1 s at nominal "1" and 2 s at nominal "0"; and

c) these waveforms SHALL be generated by the ladder/control/supervisory logic of the control components of the SUT, and not autonomously by the I/O devices

d) both digital and analog outputs with these characteristics SHALL be measured if both are present

e) if digital or analog outputs can be conveyed using more than one method (such as via pneumatic, electrical, or using a Fieldbus message), then these outputs for all supported forms of conveyance SHALL be monitored per the criteria of this requirement

f) any discrete outputs for all supported forms of conveyance SHALL be monitored using the testing device described in Requirement SRT.R44c).

NOTE 1 This requirement is intended to permit the output monitoring process to detect anomalous behavior of the control software of the system, which monitoring could be defeated if low-level I/O were generating the waveform autonomously.

NOTE 2 The intent of this requirement is to test whether the supervisory logic continues to perform under adverse network conditions; it is not the intent of these tests to provide validation of the supervisory logic itself.

The jitter requirements of a) and b) are with respect to the relative timing of the transitions, not the analog value of the analog or digital output. A transition SHALL be determined to have occurred when the voltage crosses above a high threshold level of 90% of total voltage rise expected, or below a low threshold level of 90% of the total fall expected. The TD employed to test a system SHALL itself introduce a maximum measurement error (measurement jitter) of no more than 1% of the period at constant state for the test signals defined in this requirement .

NOTE 3 Since the period at constant state is 1 second, 1% is 10 ms.

The SUT SHALL be considered to adequately maintain control capability if both of the following hold:

- The percent of jitter measurements taken during the test that are less than the maximum jitter tolerance submitted per Requirement SRT.R10, is greater than or equal to the confidence percentage value also submitted under that requirement, after allowing for measurement jitter.
- There is no occurrence of jitter during the test, that is greater than the sum of measurement jitter plus 1.5 times the maximum jitter tolerance submitted per Requirement SRT.R10.

NOTE 4 For example, assuming measurement jitter of 10ms and a maximum jitter tolerance of 50 ms, a jitter observation of greater than 85ms would indicate failure to adequately maintain control capability.

**Requirement SRT.R39 – Test criteria for "adequately maintain upward essential functions"**

A system SHALL be determined to have adequately maintained upward essential functions during a test if it meets the definitions in 4.1.1.3 through 4.1.1.7, where the test criteria for determining the status of services as referenced in those definitions, are as agreed between the test laboratory and the certification applicant, per Requirement SRT.R21 "Submission of design for essential function monitors."

**Requirement SRT.R40 – Criteria for "pass asset discovery testing"**

The SUT SHALL pass the asset discovery testing if it adequately maintains all essential functions (per Requirement SRT.R38 and Requirement SRT.R39), throughout all of the UDP and TCP port scans and IP protocol type scans performed on each component of the system to meet the asset discovery testing requirements.

### 10.5 Reproducibility criteria

**Requirement SRT.R41 – Reproducibility of asset discovery test failure**

If the SUT fails to adequately maintain an essential function during a scan that is part of asset discovery testing for any component of the system, this behavior SHALL be shown to be reproducible before the test is given a failed status. If a test fails on its 1st run, then runs for 3 consecutive test runs without a failure, a pass SHALL be declared for the test.

## 11 Vulnerability Identification Testing (VIT)

### 11.1 General

Vulnerability identification testing has two purposes:

- to determine if any known vulnerabilities exists on any of the components of the SUT ; and
- to test whether essential functions on the system are adequately maintained during a vulnerability scan.

**Requirement SRT.R42 – Vulnerability identification testing**

Vulnerability identification testing SHALL be performed on the system per the VIT policy specification [SSA-420] using a PC running the Nessus® vulnerability scanner product from Tenable Network Security configured with a policy that meets the VIT policy specification [SSA-420].

### 11.2 Test configuration

#### 11.2.1 Basic vulnerability identification testing configuration

The basic vulnerability identification testing configuration consists of a PC running Nessus with the ISASecure VIT policy while monitoring the performance of the SUT essential functions. For the purposes of examining how the system maintains essential functions during a vulnerability identification test, the firewall functions are configured as they would be by the end customer.

**Requirement SRT.R43 – Basic vulnerability identification testing configuration**

The configuration for vulnerability identification testing SHALL include the following elements:

a) each component in the system that has an IP address;

b) a PC that is located in the same security zone and running Nessus with the ISASecure VIT policy;

c) authentication credentials for the system being tested;

d) the configuration required to carry out the methods for monitoring upward essential functions as described per Requirement SRT.R21 "Submission of design for essential function monitors;"

e) the configuration described in Requirement SRT.R31 "Configuration for downward essential functions monitoring during asset discovery testing" that is required to monitor downward essential functions; and

f) a wired switched or non-switched network path that connects all of the above components.

NOTE This is the same as the configuration for asset discovery testing, except that the TD in this case will be generating scans to search for specific patterns associated with known vulnerabilities rather than the network scans used for the asset discovery testing.

### 11.2.2 Configuration for downward essential functions monitoring

**Requirement SRT.R44 – Configuration for downward essential functions monitoring during vulnerability identification testing**

The test configuration for vulnerability identification testing SHALL include the following to allow monitoring of the control loop/safety instrumented function:

a) a control program on the system that provides observable expected control outputs, specified in Requirement SRT.R38 “Test criteria for “adequately maintain control capability;"

b) control programs necessary to load each of the components of the SUT to the predefined typical level recommended to end users, and to verify this load has been achieved and maintained by the methods specified per Requirement SRT.R20 "Submission of method to achieve recommended system loading;"

c) a testing device which is a monitoring component that is capable of receiving the analog and digital control outputs of the SUT and collecting data to support the calculation of jitter on the signals received in ms, to the accuracy stated in Requirement SRT.R38 “Test criteria for adequately maintain control capability."

NOTE 1 This testing device need not be the same physical device as the testing device that generates network traffic for the test.

NOTE 2 This testing device can calculate jitter in real time or the calculation can be done off-line based on data from the testing device. Performing the calculation in real time permits more advanced test branching based upon observed results.

## 11.3 Test procedure

The basic vulnerability identification test procedure involves executing the Nessus VIT policy, which is created in accordance with [SSA-420], on each component of the system. This scan checks for the existence of applicable known vulnerabilities while monitoring the performance of the SUT essential functions.

NOTE Applicable known vulnerabilities refers to only searching for known vulnerabilities for an OS or application on components that contain that OS or application.

The next requirement takes into account the fact that some systems may have several accessible network interfaces.

**Requirement SRT.R45 – Vulnerability identification test coverage of all accessible network interfaces**

If the SUT supports multiple accessible network interfaces, the vulnerability identification test SHALL be executed on each accessible network interface, one at a time, while maintaining all essential functions, with possible exception as follows. Accessible network interfaces for embedded devices that have EDSA certification need not be tested as part of SSA certification testing, if the VIT scan performed for that EDSA certification is sufficiently current per the requirements of [SSA-420]. For embedded devices, VIT SHALL be performed in all operational modes in which the control function is available.

## 11.4 Test pass criteria

**Requirement SRT.R46 – Criteria for “pass vulnerability identification testing”**

The SUT SHALL pass vulnerability identification testing if it adequately maintains all essential functions (per Requirement SRT.R38 and Requirement SRT.R39), and no “Critical” or “High” Risk Factor vulnerabilities are discovered on any component of the system by scanning. All “Medium” Factor vulnerabilities identified SHALL be mitigated. All “Low” Risk Factor vulnerabilities identified SHALL be analyzed with respect to applicable FSA requirements for the relevant ISASecure level (FSA-E Level 1 for embedded devices and FSA-S at each zone security level). If the discovered vulnerability does not violate any of the FSA requirements for the relevant ISASecure levels, the SUT SHALL pass VIT.

NOTE Vulnerability Risk Factors are categorized as critical, high, medium, low or none by the VIT scanning tool.

### 11.5 Reproducibility criteria

**Requirement SRT.R47 – Reproducibility of vulnerability identification test failure**

If the SUT fails to adequately maintain an essential function during vulnerability identification test of any component of the system, this behavior SHALL be shown to be reproducible before the test is given a failed status. If a test fails on its 1st run, then runs for 3 consecutive test runs without a failure, a pass SHALL be declared for the test.

## 12 Communication Robustness Testing (CRT)

### 12.1 General

CRT testing is performed as per the [EDSA-310] common requirements for communication robustness testing in Section 7.2 of that document.

**Requirement SRT.R48 – Types of CRT tests**

CRT for a system SHALL comply with requirements of protocol specific robustness testing as defined below, as well as [EDSA-310] requirements: ERT.R36, ERT.R37, ERT.R38, ERT.R39, ERT.R40, ERT.R41, ERT.R42, ERT.R43, ERT.R48, and ERT.R49.

NOTE 1 ERT.R37 discusses test of redundant device configurations. Even if a system device is only deployed in a redundant configuration for the system submitted for certification, a test with non-operational units is required, to assure continued operation in the event of a failed or non-operational device.

**Requirement SRT.R49 – Communication robustness testing precedence**

Communication robustness testing as defined in Section 12 SHALL be performed from each external interface to the system, against any devices reachable from that external interface, with the exception of firewall devices on the system perimeter. It SHALL also be performed using a direct network connection against every embedded device in the system that does not have ISASecure EDSA certification, using the information obtained during its asset discovery testing. For embedded devices, CRT SHALL include testing in all operational modes for in which the control function is available.

NOTE 2 "Ethernet" CRT tests performed from external interfaces will only reach devices on the same network segment as that interface.

### 12.2 Test configuration

#### 12.2.1 Basic Communication robustness test configuration

This section describes test configuration requirements that apply to communication robustness testing, as referenced by the specifications for individual protocols. This includes network, TD, and SUT configuration as well as configuration related to monitoring essential functions.

As specified by the following test configurations, the intent for SRT is that a system is tested in the environment within which it is used, which (since it is a system) includes network connections to higher level supervisory components and to entities that receive control signals.

**Requirement SRT.R50 – Basic communication robustness testing configuration**

The test laboratory SHALL support a test configuration for protocol-specific robustness testing that has the following elements:

a) the system under test;

b) one or more testing devices that generate network traffic required to carry out the CRT testing;

c) the configuration required to carry out the methods for monitoring upward essential functions as described per Requirement SRT.R21;

d) the configuration as described in Requirement SRT.R31 that is required to monitor downward essential functions;

e) a wired switched or non-switched network path that connects all of the above components.

NOTE This is the same as the configuration for asset discovery testing, except that the TD in this case will be generating packets for specific protocols rather than the network scans used for asset discovery testing.

### 12.3 Test procedure

Each embedded device that does not have ISASecure EDSA certification is tested individually. The communication robustness testing device is configured with the applicable rate limits and asset discovery information for each embedded device and external interface to the SUT (one at a time). CRT tests as defined in the [EDSA-310] common requirements for communication robustness testing in Section 7.2 of that document, are run against each embedded device and external interface to SUT while monitoring essential functions.

### 12.4 Test pass criterion

In the communication robustness tests, each component tested is subjected to a variety of protocol errors and network traffic rates. In overview, a system will pass communication robustness testing if it adequately maintains essential functions throughout the tests. Section 4 defines those functions that are essential.

**Requirement SRT.R51 – Criteria for communication robustness test pass**

A system SHALL pass the communication robustness test for a specific protocol if:

a) it adequately maintains all upward and downward essential functions throughout the test, as defined in Requirement SRT.R38 and Requirement SRT.R39;

b) it meets other pass criteria, if any, that are explicitly stated in the CRT specification for that protocol.

### 12.5 Reproducibility criteria

Test reproducibility assists both test laboratory personnel and certification applicants in demonstrating unexpected test results and identifying their causes through repetition of the testing, often after enabling instrumentation within or applied to the software under test.

**Requirement SRT.R52 – Reproducibility of communication robustness test failure**

If the SUT fails to adequately maintain an essential function or exhibits other behavior that indicates a failure during a protocol-specific robustness test, this behavior SHALL be reproducible before the test is given a failed status. If a test fails on its 1st run, then runs for 3 consecutive test runs without a failure, a pass SHALL be declared for the test.

**Requirement SRT.R53 – Generation of reproducible robustness tests**

The test laboratory SHALL document the test procedure such that the original packet sequence and timing are reproducible using the same test tool.

## 13 Network Stress Testing (NST)

### 13.1 General

NST testing is performed against all devices in a network segment as per a subset of the [EDSA-310] common requirements for communication robustness testing in Section 7.2 of that document. The subset includes only the “Load Stress Tests” as defined in [EDSA-310].

**Requirement SRT.R54 – Types of NST tests**

NST SHALL be performed from within a network segment against all devices in a network segment and SHALL comply with requirements of protocol specific robustness testing as defined below, as well as [EDSA-310] requirements:

ERT.R36 Robustness Testing Phases – Part c

ERT.R37 Test coverage for devices with redundant configurations

ERT.R43 Protocol specific load testing

ERT.R46 Reproducibility of protocol-specific robustness test failure

**Requirement SRT.R55 – Network stress testing precedence**

Network Stress testing as defined in Section 13 SHALL be performed against every network segment in every security zone in the SUT.

### 13.2 Test configuration

#### 13.2.1 Basic network stress testing configuration

This section describes test configuration requirements that apply to Network Stress testing. This includes network, TD, and SUT configuration as well as configuration related to monitoring essential functions.

As specified by the following test configurations, the intent for SRT is that a system is tested in the environment within which it is used, which (since it is a system) includes network connections to higher level supervisory components and to entities that receive control signals.

**Requirement SRT.R56 – Basic network stress testing configuration**

The test laboratory SHALL support a test configuration for network stress testing that has the following elements:

a) the system under test;

b) one or more testing devices, that generate network traffic required to carry out the NST testing;

c) the configuration required to carry out the methods for monitoring upward essential functions as described per Requirement SRT.R39;

d) a wired switched or non-switched network path that connects all of the above components.

### 13.3 Test procedure

Each network segment is tested individually. The CRT testing device is connected to the network segment and configured with asset discovery information for each device on the segment. CRT load stress tests as defined in the [EDSA-310] common requirements for communication robustness testing in Section 7.2 of that document, are run against each device in the segment while monitoring essential functions, with the exception of the control function.

### 13.4 Test pass criterion

In network stress testing, each component on the network segment under test is subjected to a variety of network stress tests. All essential functions (identified in Requirement SRT.R7) except the control function are monitored. In overview, the SUT will pass NST if it adequately maintains all of these essential functions throughout the tests.

**Requirement SRT.R57 – Criteria for network stress test pass**

A system SHALL pass the network stress test for a specific protocol if:

a) it adequately maintains all upward essential functions throughout the test, as defined in Requirement SRT.R39

b) it meets pass criteria other than adequately maintaining essential functions, if any, that are explicitly stated in the CRT specification for that protocol.

NOTE Downward essential functions (the control function and safety instrumented function) need not be monitored during NST because embedded devices will have separately undergone CRT (SRT.R49), which includes the load stress tests that are run for

NST. Passing CRT shows that the embedded devices adequately maintain downward essential functions, and therefore the system does.

### 13.5 Reproducibility criteria

Test reproducibility assists both test laboratory personnel and certification applicants in demonstrating unexpected test results and identifying their causes through repetition of the testing, often after enabling instrumentation within or applied to the software under test.

**Requirement SRT.R58 – Network stress testing test failure**

If the SUT fails to adequately maintain an essential function or exhibits other behavior that indicates a failure during a protocol-specific network stress test, this behavior SHALL be reproducible before the test is given a failed status. If a test fails on its 1st run, then runs for 3 consecutive test runs without a failure, a pass SHALL be declared for the test.

**Requirement SRT.R59 – Generation of reproducible network stress tests**

The test laboratory SHALL document the test procedure such that the original packet sequence and timing are reproducible using the same test tool.

## 14 Test Reporting Requirements

### 14.1 Common reporting requirements

This section contains requirements on test reporting that are common across all SRT tests. Additional requirements on reporting the results of asset discovery testing, vulnerability identification testing communication robustness testing and network stress testing are found in Sections 14.2, 14.3, 14.4 and 14.5 respectively.

**Requirement SRT.R60 – SRT report summary**

The SRT process SHALL produce a summary report of all results for completion of SRT Requirements (SRT.R1 – SRT.R59) indicating compliance or non-compliance for submissions, set-up, testing, in addition to providing detailed test results.

**Requirement SRT.R61 – Test report administrative information**

The SRT process SHALL produce a test report that includes the following information:

- the manufacturers of all components in system under test;
- the applicant for the certification;
- the test laboratory and contact information;
- a system product version number that defines the version of all components as well as configuration version of all components in the system under test;
- an identifier of the ISASecure SSA Test Specification version to which the testing conforms;
- Version (date code) of the selected test tools;
- the protocols tested, test suites employed and date(s) of testing;
- date of the test report;
- pass / fail status.

**Requirement SRT.R62 – Report system architecture with zones and conduits**

The SRT report SHALL include an architecture drawing for the SUT that defines all security zones and conduits.

**Requirement SRT.R63 – Report SRT test case descriptions**

The SRT report SHALL include names for and high level descriptions of test cases executed. The required certification test suite is organized into meaningful test cases at the discretion of the test laboratory. However, the test laboratory SHALL make available to the system certification applicant, a mapping from their test cases to the tests enumerated in Section 7 of the ISASecure EDSA robustness testing specification (numbered documents EDSA-40x) for each tested protocol.

**Requirement SRT.R64 – Report SRT methodology summary**

The SRT report SHALL provide a high level summary of the methodology used to conduct each type of test.

**Requirement SRT.R65 – Report SRT configuration**

The SRT report SHALL describe the test configurations used to conduct the tests, including the configurations of all components included in the system under test.

**Requirement SRT.R66 – Report ISASecure SSA reference for test failure**

For any test outcomes that result in a certification not being granted, the SRT report SHALL reference the applicable requirement(s) of the ISASecure SSA test specification upon which that test is based.

**Requirement SRT.R67 – Report test failure analysis**

For any test failures, whether or not they result in a certification not being granted, the SRT report SHALL describe the discussion, analysis and conclusions reached regarding the failure that took place between the test laboratory and the applicant for certification.

**Requirement SRT.R68 – Report conditional branches of test execution**

The test report SHALL indicate whether any branches of testing were executed based upon test branching logic that was triggered by prior anomalous observed testing results.

**Requirement SRT.R69 – Report test software version**

The SRT report SHALL provide full version identifiers or hash values that, taken together with the test laboratory's procedures, unambiguously define the specific tests and software used to carry out all tests, to support reproducibility of test results.

**Requirement SRT.R70 – Report test identification and parameters for reproducibility**

The SRT report SHALL provide information sufficient to support the unambiguous reproducibility of the test, such as a test version and any parameters such as the date level of known vulnerabilities used to generate network traffic for a test. Where applicable the report SHOULD provide a network trace of the traffic that preceded a test failure using a tool for packet capture.

### 14.2 Asset discovery reporting

A test laboratory performing asset discovery testing provides a test report that meets the following requirements.

**Requirement SRT.R71 – Report basic asset discovery test information**

The report for asset discovery testing SHALL meet all basic test reporting requirements in Section 14.1 from Requirement SRT.R60 to Requirement SRT.R70 inclusive.

**Requirement SRT.R72 – Report UDP ports that may be active**

The list of UDP ports determined to not be either ignored or unreachable for each accessible component interface and mode, and associated protocols per [PORT], SHALL be included in the asset discovery test report for each component in the system.

**Requirement SRT.R73 – Report TCP ports that may be active**

The list of TCP ports determined to not be either ignored or unreachable for each accessible component interface and mode, and associated protocols per [PORT], SHALL be included in the asset discovery test report for each component in the system.

**Requirement SRT.R74 – Report IP protocol types**

The list of IP protocol types that appear to be supported for each accessible component interface and mode SHALL be included in the asset discovery test report for each component in the system.

NOTE The appropriateness of potentially active UDP and TCP ports and supported IP protocol types is examined in the functional security assessment. Additionally, the UDP and TCP port information partially determines the scope of protocol-specific robustness testing.

**Requirement SRT.R75 – Report behavior of essential functions during asset scans**

For each essential function identified for the SUT per Section 6, the asset discovery test report SHALL state whether the function was adequately maintained (per the definition in Requirement SRT.R38 and Requirement SRT.R39) during the port scans that comprise asset discovery testing, and if not, describe its behavior, the network interface used and the component mode if applicable.

### 14.3 VIT reporting

These requirements relate to reporting on vulnerability identification testing.

**Requirement SRT.R76 – Report basic vulnerability identification test information**

The report for a vulnerability identification test SHALL meet the entire basic test reporting requirements in Section 14.1 from Requirement SRT.R60 to Requirement SRT.R70 inclusive.

**Requirement SRT.R77 – Report vulnerability identification failures**

The test report SHALL document any Critical, High, Medium or Low Risk Factor vulnerabilities which were identified during vulnerability identification testing. The test report SHALL define the mitigations performed to accommodate all medium risk factor vulnerabilities discovered. If a low risk factor vulnerability violates an FSA-S requirement applicable to the SSA certification level, or an FSA-E requirement (for embedded devices) at EDSA level 1, the test report SHALL document the FSA-S or FSA-E requirement.

**Requirement SRT.R78 – Report component with identified vulnerability**

For vulnerability identification tests which had an observed failure, the component that contains the vulnerability identified SHALL be documented.

### 14.4 CRT reporting

These requirements relate to reporting on the basic and load stress phases of the communication robustness testing.

**Requirement SRT.R79 – Report basic protocol specific robustness test information**

The report for a communication robustness test SHALL meet the entire basic test reporting requirements in Section 14.1 from Requirement SRT.R60 to Requirement SRT.R70 inclusive.

**Requirement SRT.R80 – Robustness results summary over all protocols**

The communication robustness test report SHALL include a summary section that provides a high level overview of results covering all protocols tested for robustness.

**Requirement SRT.R81 – Report robustness failures**

The communication robustness test report SHALL document any robustness test cases under which there were observed failures, where pass/fail criteria are defined in 12.4.

**Requirement SRT.R82 – Report robustness failure conditions**

For robustness tests which had an observed failure, the protocol-specific robustness test report SHALL document the test conditions that were associated with the failure.

**Requirement SRT.R83 – Report robustness test case results listing**

The communication robustness test report SHALL provide a listing of each category of robustness test cases executed, pass/fail status, a summary of any anomalous behavior observed for those test cases, and any related recommendations.

### 14.5 NST reporting

These requirements relate to reporting on network stress testing.

**Requirement SRT.R84 – Report basic network stress test information**

The report for a network stress testing SHALL meet the entire basic test reporting requirements in Section 14.1 from Requirement SRT.R60 to Requirement SRT.R70 inclusive.

**Requirement SRT.R85 – Network stress results summary over all protocols**

The network stress test report SHALL include a summary section that provides a high level overview of results covering all protocols tested for network stress.

**Requirement SRT.R86 – Report network stress test failures**

The network stress test report SHALL document any robustness test cases under which there were observed failures, where pass/fail criteria are defined in 13.4

**Requirement SRT.R87 – Report network stress test failure conditions**

For network stress tests which had an observed failure, the network stress test report SHALL document the test conditions that were associated with the failure.

**Requirement SRT.R88 – Report network stress test case results listing**

The network stress test report SHALL provide a listing of each category of network stress test cases executed, pass/fail status, a summary of any anomalous behavior observed for those test cases, and any related recommendations.

— — — — — — —