DA-401-2019

Security test plan for DA RTUs

Version 1.0

23 December 2019

This document was produced in the ENCS program on Security Architectures. This program support ENCS members in selecting and implementing technical security measures for systems and their components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

Smart metering	DA-301-2019: Security requirements for procuring smart meters and data concentrators
Distribution automation	DA-101-2019: Security risk assessment for distribution automation systems DA-201-2019: Security architecture for distribution automation systems DA-301-2019: Security requirements for procuring distribution automation RTUs DA-390-2019: Market survey on distribution automation RTU security DA-401-2019: Security test plan for distribution automation RTUs
Substation automation	DA-101-2019: Security risk assessment for substation automation systems DA-201-2019: Security architecture for substation automation systems DA-301-2019: Security requirements for procuring substation gateways DA-302-2019: Security requirements for procuring IEDs DA-303-2019: Security requirements for procuring HMI software
Electric vehicles	EV-101-2019: Security risk assessment for EC charging infrastructure EV-201-2019: Security architecture for EV charging infrastructure EV-301-2019: Security requirements for procuring EV charging stations EV-401-2019: Security test plan for EV charging stations

This document is shared under the Traffic Light Protocol classification:

TLP White – public

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure

Version History

Date	Version	Description
25 October 2019	0.1	Initial draft
4 December 2019	0.2	Update after workshop on 25 November
23 December 2019	1.0	Final version in member project on procuring secure equipment

Table of Contents

Version History 3

1 Introduction 5

1.1 Scope 5

2 Tests by the vendor 7

2.1 Functional security tests 7

2.2 Automated vulnerability assessment 10

2.2.1 Vulnerability scanning 10

2.2.2 Robustness testing 11

3 Review by the grid operator 12

3.1 Development process review 12

3.1.1 Review of development process documentation 12

3.1.2 Development processes interview 13

3.2 Technical security review 13

3.2.1 Review of technical design 13

3.2.2 Review of technical implementation 15

3.2.3 Technical interview 16

4 Penetration test by an external lab 17

Appendix A: Tracking of requirements 18

References 21

1 Introduction

This document provides a plan to test distribution automation (DA) remote terminal units (RTUs) against the security requirements that ENCS has developed [1].

When the requirements are used, the need arises to evaluate the RTU against the requirements. Most procurement processes include acceptance testing to make sure that the selected RTU meets all requirements. This document provides a standardized test plan to evaluate the RTU against the security requirements in [1].

By standardizing the test plan, the test results can be more easily shared between grid operators. The vendor of the RTU can perform security tests according to the test plan and then use the test report to show compliance in all tenders that use the security requirements. This reduces the cost of testing and can give grid operators assurance in advance that there are RTUs meeting the requirements.

The test plan consists of three phases:

1. Functional tests and a vulnerability assessment by the vendor, usually performed during development;
2. A review of development processes and security design by the grid operator, usually performed during selection;
3. A penetration test by an external lab, usually performed after the RTU has been selected.

The term ‘test’ is used broadly to cover any evaluation activities, including interviews and reviews.

1.1 Scope

The test plan covers the security requirements in [1].

Using the test plan

The test plan is part of a bigger approach to creating secure systems, both when building new systems and when updating existing systems. It consists of the following steps:

1. Perform a **security risk assessment** to understand the threats to the system and the impact these can have. An assessment of the risks to a typical distribution automation systems is available in [2].
2. Design a **security architecture** that selects technical security measures to mitigate the risks. Measures are chosen for the whole system, as this is usually more effective than choosing measures per component. The architecture can act as a blueprint for system integrators and the departments maintaining the system. A recommended security architecture for distribution automation systems is available in [3].
3. Derive **security requirements for components** from the security architecture that can be used to develop or procure the components. Security requirements for distribution automation RTUs are available in [1].
4. **Test the components** to check that they meet the security requirements. In a procurement process, such tests should be part of the selection phase. This document provides a test plan to test against the requirements in [1].
5. **Test the system** once it is deployed to check that it is implemented according to the architecture and mitigates the risks. The configuration of the network and devices can be checked using a technical audit. Mitigation of the risks can be checked using penetration and red team tests simulating the threats.

These steps ensure that a secure system is delivered. After that it still needs to be operated securely. Processes and procedures should be set up for securely maintaining the system, managing keys and passwords and responding to incidents.

To ensure the consistent quality of the processes and procedures, it is recommended to use an information security management system, for instance based on the ISO/IEC 27001 [4]. To support this, the architecture is organized to match the security objectives in ISO/IEC 27001 Annex A.

2 Tests by the vendor

The test plan requires the vendor to perform all routine tests, that is the functional security tests and an automated vulnerability assessment. This is the most cost-effective way to perform these tests and ensures they can be run on each firmware release.

The full test reports should be made available to the grid operator for review (see Section 3.2.2). The grid operator can request further evidence from a test case, such as logs and traffic captures, that show that the test case was passed.

2.1 Functional security tests

The vendor should check the implementation of the requirements in Table 1 against the security design. They should at least run the test cases listed.

Table 1: Functional test cases that the vendor should perform.

Requirement	Required test cases
AC7-RTU: Centrally managed, role-based access control for local engineers	• Check that the RTU can be integrated with a central access control system • Check that new roles can be added to the RTU • Check that the privileges of roles can be changed • Check that local accounts can be used to log in when the RTU cannot reach the central access control server
AC8-RTU: Static access rights between RTUs at different locations	• Check that access privileges for RTUs at different locations are enforced
AC9-RTU: Machine-to-machine authentication for the SCADA system at the network	• Check that the SCADA system can authenticate with the authentication mechanism specified in the documentation • Check that authentication attempts with invalid credentials are rejected
AC10-RTU: Machine-to-machine authentication for	• Check that the central system can authenticate with the authentication mechanism specified in the documentation

the central maintenance system	• Check that authentication attempts with invalid credentials are rejected
AC11-RTU: Authentication using individual passwords for local engineers	• Check that it is possible to log in with a valid password • Check that the password is not shown • Check that a log in attempt with an invalid password is rejected • Check that no information about the existence of an account is leaked after a failed login attempt • Check that it is possible to block access after several failed login attempts • Check that sessions are automatically closed when they are inactive for a configurable time
AC12-RTU: Machine-to-machine authentication between RTUs at different locations	• Check that RTUs can authenticate with the authentication mechanism specified in the documentation • Check that authentication attempts with invalid credentials are rejected
CR2-RTU: Updating keys and credentials	• Check that the passwords or keys used to authenticate the SCADA system (AC9-RTU) can be updated • Check that the passwords or keys used to authenticate the central maintenance system (AC10-RTU) can be updated • Check that the (local) passwords used to authenticate engineers (AC11-RTU) can be updated • Check that the passwords or keys used to authenticated other RTUs (A12-RTU) can be updated • Check that the keys used to verify firmware signatures (OP10-RTU) can be updated • Check that the keys used for communication security (CM1-RTU, CM2-RTU) can be remotely updated
OP1-RTU: Future-proof design	• Check how much memory and computing power the RTU is using under normal operations

	• Check that the RTU can support connections using AES 256 for communication with the SCADA system and central system • If elliptic curve cryptography is used, check that the RTU can use keys of length at least 512 bits for setting up connections to the SCADA system and central system • If RSA is used, check that the RTU can use keys of length at least 4096 bits for setting up connections to the SCADA system and central system
OP4-RTU: Recovery from configuration	• Check that the RTU can be recovered to its normal configuration from a project file
OP5-RTU: Security events	• Check that the RTU logs the following security events in a local log: 1. Successful authentications 2. Failed authentication attempts 3. Firmware uploads 4. Successful firmware updates 5. Failed firmware updates 6. Changing the system time 7. Booting the device 8. Shutting down the device 9. Changing keys or credentials 10. Failed attempts to change keys or credentials 11. Changes to user accounts 12. Changes to authorizations
OP6-RTU: Collecting security events	• Check that the RTU can export the security logs over the syslog protocol
OP7-RTU: Protecting security events	• Check that user access to the security logs is restricted • Check that the RTU security log is rolling
OP9-RTU: Batched, remote firmware updates	• Check that it is possible to remotely update the firmware

OP10-RTU: Verification of firmware signatures before installation	• Check that the RTU accepts firmware updates with valid signatures • Check that the RTU rejects firmware updates with invalid signatures

2.2 Automated vulnerability assessment

The vendor should perform a vulnerability assessment to check if the RTU has any known vulnerabilities through vulnerability scanning or suffers from input validation or resilience issues through robustness testing.

2.2.1 Vulnerability scanning

During vulnerability scanning, automated scanners are run on the RTU, both on the WAN interface and on any local IP-based interfaces. The scanner report is then checked according to the test cases in Table 2.

Table 2: Test cases for vulnerability scanning.

Requirement	Test cases
CR1-RTU: Strong cryptographic keys and algorithms	• Check that all cryptographic algorithms, used in e.g. SSH or TLS, are according to the requirement
OP11-RTU: Hardening	• Check that only the documented network services are open • Check that only the required user accounts are active
OP12-RTU: Known vulnerabilities	• Check that the RTU does not have any outdated applications, libraries, or communication protocols installed for which there are known vulnerabilities
CM1-RTU: Confidentiality and integrity of network communication	• Check that all network services discovered on the WAN are protected using the network security measures defined in the security design

2.2.2 Robustness testing

Robustness testing checks for input validation issues through fuzzing or resilience errors through flooding using the tests cases in Table 3. It is recommended to also fuzz the implementation of the IEC 60870-5-104 protocol, although this is not mandatory.

Table 3: Test cases for robustness testing.

Requirement	Test cases
OP13-RTU: Input validation	• Fuzzing of the TCP/IP stack • Fuzzing of the TLS implementation • If the RTU has a web interface: scanning for known web vulnerabilities using a web vulnerability scanner

3 Review by the grid operator

The grid operator reviews the security of the RTU based on documentation and interviews. The review includes both the development processes and security design. The grid operator may ask external parties to support in performing the review.

3.1 Development process review

The assessment of development processes checks that the vendor has implemented all required measures for secure development. It is conducted in two steps. First, vendors are asked to deliver documentation on their processes and the grid operator reviews it. Second, the grid operator asks follow-up questions in an interview.

3.1.1 Review of development process documentation

For the vendor documentation review, vendors are required to deliver the documentation in Table 4. The grid operator then checks that the processes documented include the required security measures.

Table 4: Documentation the vendor must provide for the assessment of development processes.

Requirement	Documentation to be provided
SD1-RTU: Secure programming practices	• Secure coding guidelines • Training program for developers • Description of process for code reviews • Description of issue tracking method and tools • Description of version control method and tools • Description of compiler security settings for the RTU firmware
SD2-RTU: Security testing during development	• Security test plan for the RTU • Test reports for firmware version evaluated
SD3-RTU: Support for acceptance testing	*No documentation required*
SD4-RTU: Secure configuration guidelines	• Secure configuration guidelines

SD5-RTU: Vulnerability handling	• Description of process for vulnerability handling • Examples of vulnerability notifications
SR1-RTU: Protection of customer assets	• ISO/IEC 27001 certificate • Statement of applicability for certification • Summary of the risk assessment

3.1.2 Development processes interview

After reviewing the documentation, the vendor has provided, the grid operator asks follow-up questions on the development processes in an interview. The interview takes at least two hours. The vendor is responsible for ensuring the right staff is available to answer questions. It is recommended they include at least:

- Someone responsible for secure development processes;
- Developers working on the RTU;
- A security officer responsible for the ISMS.

3.2 Technical security review

Grid operators review the technical security design following the same approach as for the development processes. First documentation is gathered from the vendor and reviewed. Then additional questions are asked in an interview.

3.2.1 Review of technical design

For the technical design review, vendors are required to deliver the documentation listed in Table 5. The grid operator checks that according to this documentation, the security design meets the requirements.

Table 5: Documentation the vendor must provide for the review of technical documentation.

Requirement	**Documentation to be provided**
AC7-RTU: Centrally managed, role-based access control for local engineers	• Description of centralized access control method • Description of role-based access control method • List of default users with their roles and privileges

AC8-RTU: Static access rights between RTUs at different locations	• Description of access privileges of other RTUs and locations
AC9-RTU: Machine-to-machine authentication for the SCADA system at the network	• Description of authentication method for the SCADA system
AC10-RTU: Machine-to-machine authentication for the central maintenance system	• Description of authentication method for the central system
AC11-RTU: Authentication using individual passwords for local engineers	• Description of authentication method for local engineers
AC12-RTU: Machine-to-machine authentication between RTUs at different locations	• Description of authentication method for RTUs at other locations (if applicable)

CR1-RTU: Strong cryptographic keys and algorithms	• Cryptographic algorithms and key lengths used, including those for:
	  ○ Password hashing (AC11-RTU)
	  ○ Verifying firmware signatures (OP9-RTU)
	  ○ Communication security (CM1-RTU)
	• Random number generator used, including method for seeding it

CR2-RTU: Remote key updates	• Description of remote password and key update process

OP1-RTU: Future-proof design	• Hardware specification including
	  ○ Processor
	  ○ RAM memory
	  ○ Persistent memory (e.g. flash)

OP5-RTU: Security events	• List of security events logged by the RTU
OP7-RTU: Protecting security events	• Description of measures taken to protect the security logs
OP10-RTU: Verification of firmware signatures before installation	• Description of the firmware update process, including the algorithms used for firmware signature verification
OP11-RTU: Hardening	• List of user accounts with their use • List of network services with their use • List of hardware interfaces with their use
OP12-RTU: Known vulnerabilities	• List of third-party libraries and applications used with their versions
OP14-RTU: Hardware assisted measures against exploits	• Description of hardware security features on the RTU processor used • Description of the compiler security setting for RTU firmware
CM1-RTU: Confidentiality and integrity of network communication	• Description of encryption and authentication measures for all protocols on the WAN
CM2-RTU: Restrict direct communication between RTUs	• Description of measures taken to restrict direct communication between RTUs
BC1-RTU: Fail-secure design	• Description of watchdog implementation

3.2.2 Review of technical implementation

For the technical implementation review, vendors are required to deliver the reports of the tests in Section 2. The grid operator checks that according to the test reports, the security measures are implemented as designed.

3.2.3 Technical interview

Like for the development processes, the grid operator follows up the documentation review with an interview. The interview takes at least two hours. The vendor is responsible for ensuring the right staff is available to answer questions. It is recommended they include at least:

- The product owner responsible for the security roadmap;
- The architect responsible for the security design;
- Developers responsible for security features.

4 Penetration test by an external lab

After the grid operators have checked the design and implementation of the security measures on paper, the penetration tests check that attackers cannot bypass them.

The test time boxed. Testers are given a fixed number of days to find vulnerabilities. They choose how to spend those days based on an assessment of the security risks. While the requirements-based testing has a broad scope to cover all requirements, the penetration tests go in-depth on the measures where tester expect the highest risks. Testers used the information from the requirements-based tests to assess these risks.

The penetration test should be aimed at bypassing the security measures on the WAN interface. The WAN interface is singled out, because attacks on this interface have the highest impact. They can affect large number of RTUs.

The testers simulate attackers on the WAN interface without the credentials that central systems use to authenticate with the RTU. If a VPN is used, the tester is outside the VPN tunnel. Testers should simulate a professional attacker with access to all known vulnerabilities.

The goal of the tester is to gain unauthorized access to the RTU, e.g. to:

- Send commands to the RTU;
- Install software or firmware on the RTU;
- Make configuration changes to the RTU;
- Read measurement from the RTU

The test should be performed as a white-box test. Testers get full access to the documentation and RTU. Even though the testers simulate attackers without credentials, they should be given the credentials to be able to efficiently track their progress. At least five days should be available for this activity.

The penetration test approach assumes that the WAN security relies on operating system features and standard (e.g. open source) libraries. Testers can then test the WAN security by analyzing how these features and libraries are configured and used. If WAN security relies on code developed by the vendor, for instance if the vendor has implemented their own cryptographic protocols, additional testing is likely required. The additional tests may also include code reviews.

Appendix A: Tracking of requirements

The table below shows which requirements are checked by which test activities. The penetration test is not included, as it is not aimed at specific requirements.

	Functional security tests	Automated vulnerability assessment	Development process review	Technical security review
AC7-RTU: Centrally managed, role-based access control for local engineers	X			X
AC8-RTU: Static access rights between RTUs at different locations	X			X
AC9-RTU: Machine-to-machine authentication for the SCADA system at the network	X			X
AC10-RTU: Machine-to-machine authentication for the central maintenance system	X			X
AC11-RTU: Authentication using individual passwords for local engineers	X			X
AC12-RTU: Machine-to-machine authentication between RTUs at different locations	X			X

	Functional security tests	Automated vulnerability assessment	Development process review	Technical security review
CR1-RTU: Strong cryptographic keys and algorithms		X		X
CR2-RTU: Updating keys and credentials	X			X
OP1-RTU: Future-proof design	X			X
OP4-RTU: Recovery from configuration	X			X
OP5-RTU: Security events	X			X
OP6-RTU: Collecting security events	X			
OP7-RTU: Protecting security logs	X			X
OP9-RTU: Batched, remote firmware updates	X			X
OP10-RTU: Verification of firmware signatures before installation	X			X
OP11-RTU: Hardening		X		X
OP12-RTU: Known vulnerabilities		X		X
OP13-RTU: Input validation		X		X

	Functional security tests	Automated vulnerability assessment	Development process review	Technical security review
OP14-RTU: Hardware assisted measures against exploits				X
CM1-RTU: Confidentiality and integrity of network communication		X		X
CM2-RTU: Restrict direct communication between RTUs				X
SD1-RTU: Secure programming practices			X	
SD2-RTU: Security testing during development			X	
SD3-RTU: Support for acceptance testing			X	
SD4-RTU: Secure configuration guidelines			X	
SD5-RTU: Vulnerability handling			X	
SR1-RTU: Protection of customer assets			X	
BC1-RTU: Fail-secure design				X

References

[1] ENCS, "DA-301-2019: Security requirements for procuring distribution automation RTUs," 2019.

[2] ENCS, "DA-101-2019: Security risk assessment for distribution automation," 2019.

[3] ENCS, "DA-201-2019: Security architecture for distribution automation systems," 2019.

[4] ISO/IEC, "ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements," 2013.