aifyclo

ENCS

DA-301-2019

Security requirements for procuring distribution automation RTUs

Version 2.0

20 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

ENCS

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
January 2016	1.0	First release produced in ENCS member project on distribution automation
9 September 2019	1.1	Update shared with members in ENCS member projects on procuring secure equipment
14 October 2019	1.2	Update after first round of comments from ENCS member project on procuring secure equipment
16 October 2019	1.3	Added additional requirements for communication between RTUs.
3 November 2019	1.4	Minor changes after comments from ENCS members.
12 December 2019	1.5	Update after workshop with ENCS members on 25 November and comments E.DSO task force 4.
20 December 2019	2.0	Final version from 2019 member project on procuring secure equipment.

Table of Contents

1 Introduction

This document gives security requirements that grid operators can use directly in their procurement documents for new distribution automation (DA) remote terminal units (RTUs).

Grid operators are increasingly automating their medium voltage (MV) substations and lines with DAU. They use DA systems to get power measurements to reliably integrate renewables and electric vehicles, and to remotely control the grid to recover from power outages more quickly.

The automation increases the possible impact of cyber-attacks. Many grid operators already have thousands of substations and lines automated. If attackers succeed in switching off power in a large part of those, it can take a lot of time to recover.

Making sure the distribution automation system is secure is hence critical. Grid operators need to set good security requirements when procuring distribution automation RTUs. The requirements should not lead to excessive cost when procuring thousands of RTUs, while still ensuring all security risks can be mitigated.

This document provides a harmonized set of security requirements that grid operators use directly in their procurement documents. The requirements have been thoroughly reviewed by both grid operators and RTU vendors. They are designed to fit into the processes and procedures already in place in the organizations, and to find a good balance between the security and the operational impact.

Harmonizing the requirements allows grid operators to more cost-effectively get secure automation equipment. It saves time and effort in developing requirements, as they are already freely available. It ensures the requirements are feasible, as they have been tested in a market survey, and in previous tenders by other operators. And it saves on implementation costs, as vendors get a common baseline to aim at. Grid operators are therefore encouraged to use these requirements when procuring new RTUs.

1.1 Scope

This document gives requirements for procuring secure RTUs for use in distribution automation systems, including:

- medium to low voltage transformer substations;
- medium voltage transport substations;
- automatic circuit recloser controllers applied to overhead distribution lines.

The requirements concerns the interfaces to the distribution automation system, and the users on these interfaces (see Figure 1).

The measures are aligned with ISO/IEC 27001:2013 [1] and cover the following sections from Annex A of that document:

- Access control (A.9)
- Cryptography (A.10)
- Operations security (A.12)
- Communication security (A.13)
- System acquisition, development and maintenance (A.14)
- Supplier relationships (A15)
- Information security aspects of business continuity (A.17)

Each subsection gives requirements that grid operators can use to meet an objective of ISO/IEC 27001 Annex A. The objective number is given in square brackets.

The requirements are intended for procuring new RTUs, not for legacy systems, although grid operator may analyze if such systems can be upgraded to meet them.

1.2 Checklist for additional requirements

The requirements cover all functions needed to securely operate DA RTUs. They can be used directly in procurement documents. It is recommended not to change them, as vendors may read over the changes if they know the requirements from other tenders. But in some cases, grid operators may want to add additional requirements to extend or specify some requirements.

Grid operators are recommended to check if they want to extend the following requirements to ensure the RTUs work with their existing system:

- **AC7-RTU:** consider specifying the technology the technology used for the central server, such as RADIUS, LDAP, or Active Directory.
- **AC9-RTU, CM1-RTU:** consider specifying the method the RTU uses to authenticate and secure communication with the SCADA system such as TLS, IPsec, or OpenVPN.
- **AC12-RTU:** consider specifying the method for authentication between RTUs if they communicate directly to allow communication between RTUs from different vendors.
- **CR2-RTU:** consider posing additional requirements to integrate into existing key management solutions or implement organization-specific policies.
- **OP8-RTU:** consider specifying a method to allow integration into existing tools, or including the tools needed for firmware updates in the tender scope.

Which technologies vendors support, is described in the market survey on DA RTUs [2].

Grid operators are also recommended to check if they want to further specify some of the terms in the following requirements to make them more precise:

- **CR1-RTU:** consider specifying the regulations on cryptography the RTU needs to comply to, for instance to meet national legislation;
- **OP1-RTU, SD5-RTU:** consider specifying the expected lifetime of the RTU;
- **OP1-RTU:** consider specifying the computing power or memory reserves the RTU should have to be future-proof;
- **OP7-RTU:** consider specifying the minimum amount of log events to be stored;
- **BC1-RTU:** consider specifying how soon the RTU should recover after a watchdog event.

The above specifications depend on the situation at the grid operators and are therefore not included in this document.

1.3 Reference architecture

Figure 1 shows the reference architecture for distribution automation systems used in this document. The users are referenced in the access control measures in Section 2. The interfaces are referenced in the communication security measures in Section 5.

While it is not explicitly pictured, there can be communication between RTUs at different locations over the WAN network, for use cases involving automatic reclosers or self-restoration of the grid.

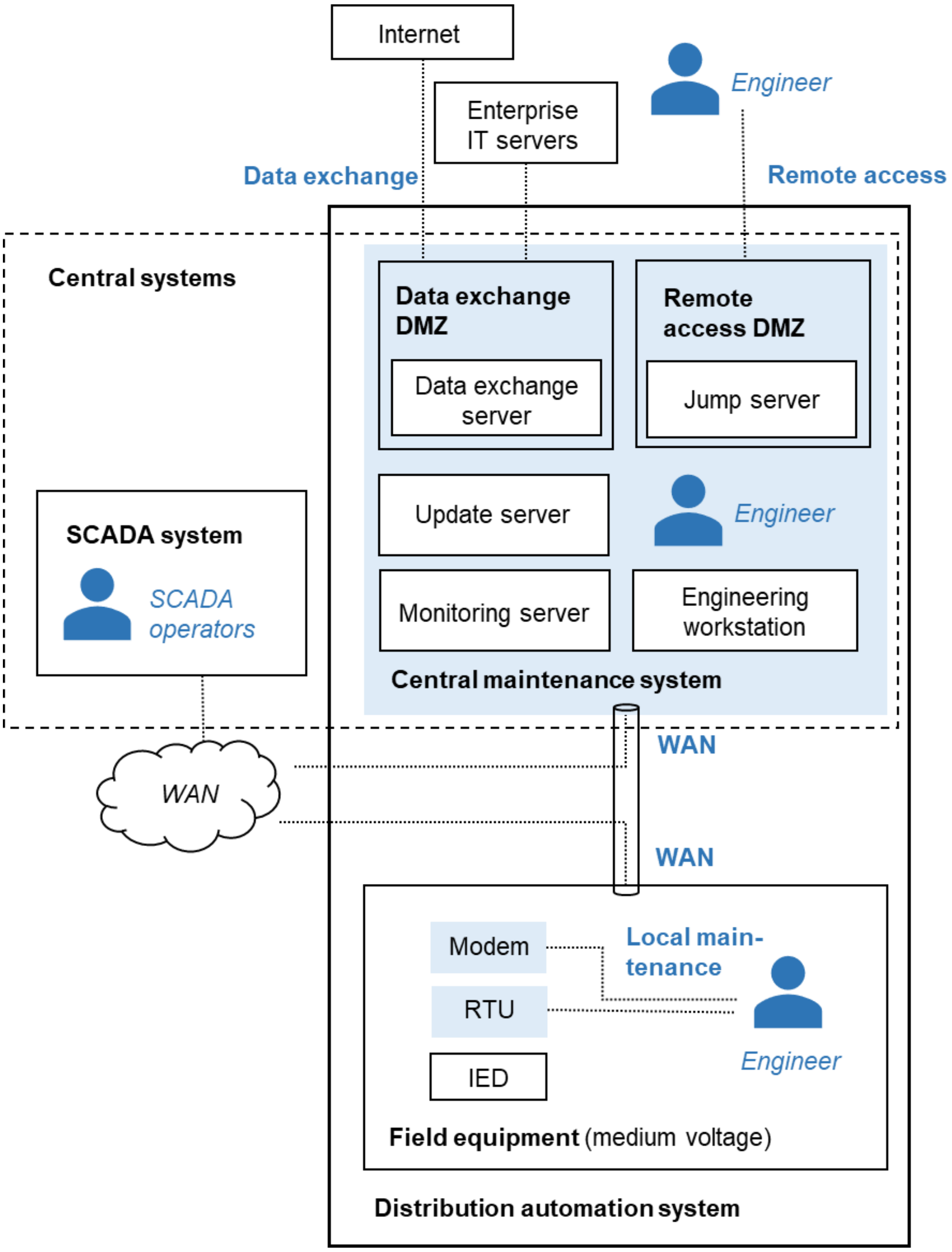

Figure 1: Reference architecture for the distribution automation system, showing its users and interfaces

Using the requirements

The security requirements are part of a larger approach to creating secure systems, both when building new systems or 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 risks can have on it. An example risk assessment for distribution automation systems is available in [3].
2. Design a **security architecture** that selects technical security measures to mitigate the risks. Measures should be 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 for the departments maintaining the system. A recommended security architecture for distribution automation systems is available in [4].
3. Derive **requirements for components** from the security architecture that can be used to develop or procure the components. This document gives security requirements for distribution automation RTUs. The requirements are mapped to the IEC 62443-4-2 standard [5], used by some vendors, in Appendix A.
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. A test plan for DA RTUs is available in [6].
5. **Test the system** to check that it is deployed according to the architecture and mitigates the risks. The implementation of the architecture 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. But after that it still needs to be operated securely. Processes and procedures should be set up to securely maintain the system, manage keys and passwords, and respond to incidents.

To ensure the quality of the processes and procedures, it is recommended to use an information security management system, for instance based on the ISO/IEC 27001 [1]. To support this, the architecture is organized by the security objectives in ISO/IEC 27001 Annex A.

2 Access control

Access control requirements concern how access rights are managed and how strong their authentication needs to be for different user groups. The RTU enforces access control for the user groups in Table 1.

Table 1: User groups on the RTU.

User	Required access	Interface
SCADA system	• Collect electricity measurements • Send control commands	WAN
Central maintenance system	• Configure the RTU • Maintain the RTU • Recover the RTU from a backup • Update the RTU firmware • Monitor the RTU • Collect additional electricity data	WAN
Local engineers	• Configure the RTU • Maintain the RTU • Recover the RTU from a backup • Update the RTU firmware	Local maintenance

2.1 User access management [A.9.2]

The RTU manages access rights in such a way that the grid operator can implement the principle of least privileges. For local engineers, it uses centrally managed, role-based access control, so that the grid operator can keep up with personnel changes and give engineers only the privileges they need.

AC7-RTU: Centrally managed, role-based access control for local engineers

The RTU shall support role-based access control for local engineers with centrally managed accounts. The RTU shall be able to:

- allow engineers to log in with individual accounts;
- check the engineer’s role in a central access control server;
- enforce the access right of the engineer’s role.

The RTU shall allow changing the privileges of a role or adding new roles.

The RTU shall provide local accounts from which engineers can log in, only accessible when the RTU cannot reach the central server.

Remarks: The engineer's role can be checked through different methods. It is recommended to use RADIUS or LDAP over TLS as specified in IEC 62351-8 [7], as these methods are most widely supported.

Roles and privileges may be managed through the RTU configuration tools. It is recommended to by default support the roles and privileges defined in IEC 62351-8 [7].

Strong passwords should be used also for the local accounts (used when the central server cannot be reached) to ensure they cannot be used to bypass authentication. Preferably, unique passwords are used in each substation, and these are only given to engineers when needed.

AC8-RTU: Least privileges between RTUs at different locations

If the RTU supports direct communication with other RTUs, the RTU shall restrict the privileges of other RTUs, so that they can access only the functions and data they need.

Remark: Direct communication between RTUs is needed for instance in use cases involving automatic reclosers or self-restoration of the grid. Only the measurements required for the use case should be shared and only the commands in the scope of the use case should be allowed. If the RTU only communicates with the central system, the requirement does not apply.

There are no requirements on how the privileges are managed. They may be static and only be changeable through software updates.

2.2 System and application access control [A.9.3]

The RTU supports authentication for all users. It uses machine-to-machine authentication for the SCADA system and individual password for local engineers.

AC9-RTU: Machine-to-machine authentication for the SCADA system at the network

The RTU shall support mutual authentication with passwords or keys for the SCADA system to gain network access.

Remarks: Authentication can be implemented using a virtual private network (VPN) or using transport layer security (TLS) with client-side certificates (as specified in IEC 62351-3 [8] and IEC 60870-5-7 [9]).

This measure is usually implemented together with the cryptographic communication security measure CM1. Passwords and keys are updated according to measure CR2.

AC10-RTU: Machine-to-machine authentication for the central maintenance system

The RTU shall support mutual authentication with passwords or keys for the central maintenance system.

Remarks: Passwords and keys are updated according to measure CR2.

AC11-RTU: Authentication using individual passwords for local engineers

The RTU shall support password-based authentication for local engineers. The RTU shall secure the log on procedure for engineers by:

- not displaying the password when it is being entered;
- not indicating if an account exists after a failed login attempt;
- blocking access after several failed login attempts;
- automatically closing as session when it has been inactive for more than an administratively configurable maximum time period.

Passwords are stored salted and hashed.

Remark: It is recommended to use a password hashing function, such as Argon2 or PBKDF2, that is resistant against GPU cracking attacks.

AC12-RTU: Machine-to-machine authentication between RTUs at different locations

If the RTU supports direct communication with other RTUs, the RTUs shall support mutual authentication with passwords or keys to access each other.

Remark: Direct communication between RTUs is needed for instance in use cases involving automatic reclosers or self-restoration of the grid. If the RTU only communicates with the central system, the requirement does not apply.

3 Cryptography

The RTU uses cryptography for several functions:

- Machine-to-machine authentication for the SCADA system and central maintenance system (Section 2);
- Hashing passwords used by human users (Section 2);
- Digitally signing the firmware (Section 4.4);
- Protecting the confidentiality and integrity of communication (Section 5.1).

Measures need to be taken to make these cryptographic techniques effective.

3.1 Cryptographic controls [A.10.1]

The RTU uses strong cryptographic keys and algorithms to protect against attacks to the cryptography itself. The RTU supports remote key updates from the central systems in order to update keys on possibly thousands of substations.

CR1-RTU: Strong cryptographic keys and algorithms

For security functions, the RTU shall use cryptography according to regulations and modern guidelines without any modifications. In particular:

- It only uses the cryptographic algorithms that the ECRYPT – Algorithms, Key Size, and Protocols Report [10] recommends as suitable for new or future systems;
- It uses keys as least as long as large as the ECRYPT report recommends for near term use (section 4.6 in [10]);
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [10] Section 3.2.3 to generate random numbers for security functions;
- If it uses certificates for authentication, it validates them by checking the signature, the certificate-chain, the revocation status, and the identity of the user or role through the subject name, common name or distinguished name.

CR2-RTU: Remote update of passwords and keys

The RTU shall support remotely changing all passwords and keys used to implement these requirements in a way that protects their confidentiality and integrity.

Where the RTU uses certificates for authentication or communication security, it shall be able to use certificates issued by the public key infrastructure (PKI) of the grid operator.

Remarks: Keys and credentials may be updated manually using the maintenance tools. When public-key cryptography is used, keys are preferably updated using an automated process, such as the Simple Certificate Enrollment Protocol (SCEP) [11] or Enrollment over Secure Transport (EST) [12] described IEC 62351-9 [13]. Key updates can only happen in compliance with the grid operator's update policy. A validation procedure should be defined to ensure proper change management.

It is allowed that keys or credentials cannot be updated if they are only used for RTU internal purposes, such as encrypting local storage or setting up secure communication between processors on the same RTU. But, as soon as they are used to implement any of the requirements in this document, they must also comply with this requirement.

The certificate used to verify firmware updates (OP10-RTU) is issued by the vendor. So, for this certificate the RTU does not need to be able to use certificates from the grid operator PKI.

4 Operations security

The RTU should support the operational processes and procedures needed to keep it secure throughout its lifetime.

4.1 Operational procedures and responsibilities [A.12.1]

To support capacity management, the RTU needs to have enough computing reserves for future updates.

OP1-RTU: Future-proof design

The RTU shall have enough memory (RAM and flash) and computation power to allow security updates needed during its lifetime, under the following assumptions:

- Cryptographic measures are updated following the standards in CR1-RTU, in particular the RTU support the key sizes recommended for long term use in Section 4.6 of the ECRYPT report [10];
- Roles and security event types will grow incrementally up to 50%.

Remarks: Compliance to the requirement can be shown through performance tests. Tests with current firmware under operational workloads should show that there are enough reserves to extend security functions. Tests with algorithms recommended for long term use in [10] should show that the RTU can run them without affecting operations. It is acceptable if the RTU can only support the long term key sizes for elliptic curve based algorithms, not for RSA-based algorithms.

4.2 Backup [A.12.3]

To support recovery processes, it should be possible to recover the RTU from configuration files, as specified below, including the file used during its installation.

OP4-RTU: Recovery from configuration

It shall be possible to recover the RTU from any failure state to its normal operation using a stored configuration, such as a project file, and possibly the firmware.

It shall be possible to remotely backup the RTU configuration, internal credentials and keys.

Remark: One method to allow easy recovery is to store a previous known correct file stored in the RTU file system, which is safely retrievable and usable by an authorized user executing the least possible number of steps.

4.3 Logging and monitoring [A.12.4]

To support detecting and responding to security incidents, the RTU needs to log relevant security events and allow them to be gathered for analysis. As the security logs are important to security, they also need to be protected themselves.

OP5-RTU: Security events

The RTU shall be able to log security events for the following 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 RTU configuration
7. Changing the system time
8. Booting the device
9. Shutting down the device
10. Changing keys or credentials
11. Failed attempt to change keys or credentials
12. Changing user accounts
13. Changing authorizations

The log entries for security events shall include a timestamp, an event description, and the role causing the event. Events caused by engineers are linked to individual users.

OP6-RTU: Collecting security events

The RTU shall allow the security logs to be read out using the normal maintenance tools.

The RTU shall be able to send all security logs to a central server using, at least, the syslog communication protocol (RFC 5424 [14]). The logs shall be sent in a commonly used format to avoid the need to develop a dedicated parser. The RTU shall allow to select from which severity level it sends log events to the central server.

The RTU shall provide the capability to create timestamps that are synchronized with a system wide time source.

Remark: The logs can be sent directly to a Security Information and Event Management (SIEM) system, or they can be gathered first by a monitoring server in the central maintenance system and then forwarded to the SIEM. The choice depends on where the SIEM system is placed in the grid operator's networks.

OP7-RTU: Protecting security logs

The RTU shall protect security logs by:

- restricting access to authorized users;
- having enough storage capacity to store the security logs;
- implementing a rolling security log, in which the oldest entries are discarded first if log storage is full.

Remark: Normally on the system and root users should be allowed to modify the logs, and only specific user groups should be authorized to read them.

4.4 Control of operational software [A.12.5]

To support patching, the RTU implements batched, remote updates. The authenticity of firmware is verified using a digital signature.

OP9-RTU: Batched, remote firmware updates

The RTU shall allow remote firmware updates through software that allows batch updates. It should be possible to update all security functions through these updates.

Remarks: Allowing batch firmware updates simplifies managing large numbers of RTUs, for instance, making it is easier to roll out security updates.

OP10-RTU: Verification of firmware signatures before installation

The RTU shall be able to verify the authenticity of firmware updates before installing the firmware using digital signatures. The vendor digitally signs each firmware release.

Remark: Verifying the firmware integrity using only a hash value does not satisfy the requirement.

4.5 Technical vulnerability management [A.12.6]

To support effective vulnerability management, the RTU is hardened, and avoids known vulnerabilities as well as input validation vulnerabilities.

OP11-RTU: Hardening

The RTU shall support hardening by disabling unneeded functions. Specifically, the RTU station shall allow:

- all unused user accounts to be removed;
- all unused network services to be disabled;
- all unused hardware interfaces to be disabled.

OP12-RTU: Known vulnerabilities

The RTU shall only use applications, libraries and communication protocols without known security vulnerabilities.

OP13-RTU: Input validation

The RTU shall apply input validation to all data it receives.

Remarks: The RTU developer should make sure their code checks the validity of all received data, including validating if the input values are within the permitted value range. They should regularly check that there are no input validation vulnerabilities in third-party libraries or applications. They should use reviews and robustness tests for code they develop in-house, such as web interfaces or the implementation of domain-specific protocols such as IEC 104. For web services, it is recommended to follow the recommendations from the Open Web Application Security Project (OWASP).

OP14-RTU: Hardware assisted measures against exploits

The RTU shall implement the following hardware features if they are available:

- *No-Execute (NX) / Write-xor-execute (W^R):* If the RTU has a Memory Protection Unit (MPU) or Memory Management Unit (MMU), it shall be used to mark code regions as read-only and data sections as non-executable.
- *Address Space Layout Randomization (ASLR):* If the RTU has a Memory Management Unit (MMU), it shall be used to load data and code at different memory addresses every time an application is run.

The software running on the RTU shall be compiled to use the hardware features.

Remark: The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR.

5 Communication security

5.1 Network security management [A.13.1]

The RTU needs to support securing communications on the WAN network.

CM1-RTU: Confidentiality and integrity of network communication

The RTU shall be able to cryptographically protect the integrity and confidentiality of communication on the WAN interface. The measures shall allow to verify the source of messages and protect against replay attacks.

If end-to-end secure protocols are used for the SCADA traffic, the RTU shall allow to turn off encryption and use only message authentication, so that it is possible to apply deep-packet inspection.

Remarks: Confidentiality and integrity of the communication can be protected by setting up a VPN tunnel or by using TLS (as specified in IEC 62351-3 [8] and IEC 60870-5-7 [9]).

Deep-packet inspection can be supported with TLS using the NULL cipher, so that authentication is applied without encryption. This TLS setting is not allowed by IEC 62351-3 [8], but may be useful for some operators to have better security monitoring.

If a VPN is used to implement the first part of the requirement, the second part does not apply. The deep-packet inspection sensor can be placed after the VPN concentrator in the central systems.

CM2-RTU: Restrict direct communication between RTUs

If the RTU supports direct communication with other RTUs, it shall be able to restrict the communication to what is needed using the cryptographic measures in CM1.

Remark: In most cases, direct communication between RTUs should be blocked, and RTUs should only communicate with the central systems. But if the distribution automation system supports use cases involving automatic reclosers or self-restoration of the grid, direct communication between RTUs may be needed. In those cases, communication should usually be restricted to RTUs on the same MV line, and to the needed protocols and ports.

6 System acquisition, development and maintenance

6.1 Security in development and support processes [A.14.2]

The developer should integrate security throughout their development process to ensure that secure firmware is delivered. They should set up secure programming practices and test each firmware release themselves. They should allow the grid operator to verify the security by acceptance testing as well as provide guidelines on secure configuration and operation. If vulnerabilities are found during the lifetime of the RTU, they should provide security updates.

SD1-RTU: Secure programming practices

The developer shall set up programming practices for the RTU firmware. They shall:

- Define secure coding guidelines;
- Provide security training to developers;
- Set up internal code reviews;
- Use an issue tracker to follow the vulnerabilities and other security issues;
- Implement a version control system;
- Enable compiler options to harden binaries or use memory-safe languages.

Remark: Examples of secure coding guidelines are the SEI CERT coding standards [15], available for different languages, and the MISRA C software development guidelines for embedded systems [16].

Compiler options that should be enabled include:

- stack cookies or canaries which make it harder to exploit stack-based buffer overflows.
- fortify source which can be used to detect buffer overflow vulnerabilities;
- Control Flow Integrity (CFI) which makes it harder for an attacker to perform code re-use attacks such as return-to-libc or Return Oriented Programming (ROP).

SD2-RTU: Security testing during development

The developer shall test each firmware release to check the implementation of the requirements in this document. Testing shall at least include:

- functional testing for all functional requirements;

- robustness testing of custom protocol implementations;
- automated web application testing on any web interfaces;
- automated vulnerability scanning.

Remark: The test plan for DA RTUs [6] includes a list of test cases that vendors can use to check the implementation of the requirements.

SD3-RTU: Support for third party testing

The developer shall support testing by the grid operator or an independent party by:

- allowing the grid operator or a third party to audit the development process;
- providing documentation on how the requirements have been implemented;
- making available RTUs for testing;
- providing all keys and credentials needed for testing;
- providing access to source code for code reviews.

Remark: The developer may require a non-disclosure agreement when providing sensitive information, if it does not prevent proper testing.

SD4-RTU: Secure configuration guidelines

The developer shall provide guidelines on how to securely configure and operate the RTU, covering at least:

- expected security measures in the operating environment;
- hardening;
- account management;
- setting up health and performance monitoring;
- setting up security logging;
- setting up backups.

SD5-RTU: Vulnerability handling

The developer shall produce security updates to fix all severe vulnerabilities found during the lifetime of the RTU. The developer shall monitor all relevant information sources on vulnerabilities, including:

- public vulnerability databases;
- notifications from developers of libraries used in the firmware;
- penetration test results from customers;
- notifications from vulnerability researchers.

The developer shall inform the grid operator about vulnerabilities as soon as possible.

Remark: To determine which vulnerabilities are severe, the Common Vulnerability Scoring System (CVSS) should be used. Vulnerabilities with a score of 7.0 or higher would be considered severe and need to be fixed.

The developer may agree with the grid operator to use another method to determine the severity of the vulnerabilities, if it can be objectively applied and gives a good indication of the risk.

7 Supplier relationships

7.1 Information security in supplier relationships [A.15.2]

To ensure that the RTU developer protects information of the grid operator or under his responsibility, it needs to implement an information security management system (ISMS).

SR1-RTU: Protection of customer assets

The developer shall have an ISMS to protect any information that could compromise the security of the RTU, including:

- detailed security designs;
- source code;
- customer-specific keys and credentials.

The ISMS shall be ISO/IEC 27001 certified and the certification scope shall cover the development and manufacturing of the RTU and related tools.

8 Information security aspects of business continuity management

8.1 Information security continuity [A.17.1]

To ensure that the security of the distribution automation system is not compromised during disruptions, the RTU is designed to fail securely.

BC1-RTU: Fail-secure design

The RTU shall be designed to minimize the impact of a failure on security. During a failure, the RTU shall:

- not leak confidential information, such as keys or credentials;
- protect the integrity of critical data;
- not allow access controls to be bypassed;
- restore availability as soon as possible.

Remarks: Examples of failures are hardware malfunctions, corruption of stored or received data and software crashes. A watchdog can be used to monitor the RTU and to automatically initiate steps to restore availability.

Appendix A: Mapping to IEC 62443

The table below maps the requirements to the component requirements in IEC 62443-4-2 [5]. If a product satisfies the requirements as specified in the table, then it also meets all requirements in this document except for:

- OP1-RTU: Future-proof design;
- System acquisition, development and maintenance requirements in Section 6;
- Supplier relationship requirements in Section 7.

The requirements in Section 6 and 7 can be covered by IEC 62443-4-1 [17].

Only the requirements from IEC 62443-4-2 that correspond to requirements in this document are included in the table. If requirements from IEC 62443-4-2 are not included, they are not required by this document.

In the last column, further specification is given. The product needs to implement the IEC 62443-4-2 requirement according to this specification to comply to this document.

IEC	Name	Arch	Specification
CR1.1	Human user identification and authentication	AC11-RTU	
CR1.1 RE 1	Unique identification and authentication	AC11-RTU	
CR1.2	Software process and device identification and authentication	AC9-RTU, AC10-RTU, AC12-RTU	SCADA system may authenticate at network level
CR1.2 RE1	Unique identification and authentication	AC10-RTU	Applies only to central maintenance system, not SCADA system
CR1.3	Account management	AC7-RTU, AC8-RTU	
CR1.4	Identifier management	AC7-RTU, AC8-RTU	

IEC	Name	Arch	Specification
CR1.5	Authenticator management	AC7-RTU, AC8-RTU	
CR1.8	Public key infrastructure certificates	CR2-RTU	
CR1.9	Strength of public key-based authentication	CR1-RTU	
CR1.10	Authenticator feedback	AC11-RTU	
CR1.11	Unsuccessful login attempts	AC11-RTU	
CR2.1	Authorization enforcement	AC7-RTU, AC8-RTU	
CR2.1 RE2	Permission mapping to roles	AC8-RTU	Applies to engineers
CR2.5	Session lock	AC11-RTU	Applies to engineers
CR2.6	Remote session termination	AC11-RTU	Applies to engineers
CR2.8	Auditable events	OP5-RTU	All security events in OP4-1 must be supported.
CR2.9	Audit storage capacity	OP7-RTU	
CR2.10	Response to audit processing failures	OP7-RTU	The RTU must implement a rolling security log.
CR2.11	Timestamps	OP6-RTU	
CR2.11 RE1	Time synchronization	OP6-RTU	

IEC	Name	Arch	Specification
CR3.1	Communication integrity	CM1-RTU	
CR3.1 RE1	Communication authentication	CM1-RTU	Only applies to the WAN interface, not for local maintenance.
CR3.4	Software and information integrity	OP10-RTU	Only applies to the firmware: must be digitally signed.
CR3.4 RE1	Authenticity of software and information	OP10-RTU	Only applies to the firmware: must be digitally signed.
CR3.5	Input validation	OP12-RTU, OP13-RTU	RTU should also not contain any known vulnerabilities
CR3.7	Error handling	BC1-RTU	In case of an error, the RTU must: not leak confidential information, such as keys or credentials; protect the integrity of critical data during failures; not allow access controls to be bypassed; restore availability as soon as possible.
CR3.8	Session integrity	CM1-RTU	
CR3.9	Protection of audit information	OP7-RTU	

IEC	Name	Arch	Specification
EDR3.10	Support for updates	OP9-RTU	The RTU maintenance software must support batch updates.
CR4.1	Information confidentiality	CM1-RTU	Information at rest may be protected by access control mechanisms. Cryptographic protection is not required. Information in transit only needs to be protected on the WAN network. It must be possible to disable encryption to allow deep-packet inspection.
CR4.3	Use of cryptography	CR1-RTU	Cryptographic algorithms must be suitable for future use according to ECRYPT – Algorithms, Key Size, and Protocols Report [10]
CR5.1	Network segmentation	CM2-RTU	If the RTU supports direct communication with other RTUs, it shall be able to restrict the communication to what is needed
CR6.1	Audit log accessibility	OP6-RTU	
CR6.1 RE1	Programmatic access to audit logs	OP6-RTU	Access must be provided through the syslog protocol.
CR7.4	Control system recovery and reconstitution	OP4-RTU	It must be possible to recover the RTU from a backup file.

IEC	Name	Arch	Specification
CR7.7	Least functionality	OP11-RTU	

Appendix B: Mapping to IEC 62351

The table below shows how some of the requirements can be implemented through compliance with the IEC 62351 standard.

Requirement	IEC 62351 part	Implementation
AC7-RTU	IEC 62351-8 [18]	A set of roles and privileges and two methods (PUSH and PULL) to authenticate users through a central server are defined
AC9-RTU	IEC 62351-3 [8] IEC 62351-5 [9]	Authentication using TLS with client-side certificates is specified
CR2-RTU	IEC 62351-9 [13]	Different methods for key management on RTUs, including the SCEP and EST protocols are specified.
CM1-RTU	IEC 62351-3 [8] IEC 62351-5 [9]	Communication security using TLS and an application layer method is specified. (Using TLS is recommended.)

Glossary

AD	Active Directory
APN	Access Point Name
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarized Zone
DoS	Denial-of-Service
EST	Enrollment over Secure Transport
IED	Intelligent Electronic Device
ISMS	Information Security Management System
MV	Medium Voltage
OT	Operational Technology
PKI	Public Key Infrastructure
RADIUS	Remote Access Dial-In User Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Incident and Event Management
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

References

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

[2] ENCS, "Market survey for distribution automation systems," 2019.

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

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

[5] ISA / IEC, "ISA 62443-4-2 Security for industrial automation and control systems - Technical security requirements for IACS components, Draft 3, Edit 4," January 12 ,2017.

[6] ENCS, "DA-401-2019: Security test plan for distribution automation RTUs," 2019.

[7] IEC, "IEC 62351-8: Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control," 2011.

[8] IEC, "IEC 62351-3:2014: Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP," 2014.

[9] IEC, "IEC 62351-5-7:2013: Telecontrol equipment and systems - Part 5-7: Transmission protocols - Security extensions to IEC 60870-5-101 and IEC 60870-5-104 protocols (applying IEC 62351)," 2013.

[10] ECRYPT - CSA, "D5.4 Algorithms, Key Size and Protocols Report," 2018.

[11] P. Gutmann, "Simple Certificate Enrolment Protocol," IETF draft, 2019.

[12] IETF, "RFC 7030: Enrollment over Secure Transport," 2013.

[13] IEC, "IEC 62351-9:2017: Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment," 2017.

[14] IETF, "RFC 5424: The syslog protocol," 2009.

[15] Carnegie Mellon University (CMU), "SEI CERT C Coding Standard," [Online]. Available: https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard. [Accessed 10 10 2019].

[16] MISRA, "Guidelines for the Use of the C Language in Critical Systems," 2013.

[17] ISA/IEC, "IEC 62443-4-1: Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements," 2018.

[18] IEC, "IEC TS 62351-8:2011: Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control," 2011.