DA/SA-311-2022

Security requirements from IEC 62443 for procuring RTUs and gateways

Version 2022v0.3

3 October 2022

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):

This document is shared under the Traffic Light Protocol classification:

TLP White – public

The European Network for Cyber Security (ENCS) is a non-profit membership 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
14 July 2022	2022v0.1	First release of the IEC 62443 requirements
19 August 2022	2022v0.2	Version with ISO 27002:2022 objectives
3 October 2022	2022v0.3	Added supplemental guidance for the requirements

ENCS

Table of Contents

1 Introduction

This document gives security requirements that grid operators can use in their procurement documents for new remote terminal units (RTUs) and gateways for distribution automation or substation automation. The requirements are based on the IEC 62443-4-2 standard [1].

Grid operators are increasingly automating their medium voltage substations and lines with distribution automation and high voltage substation with substation automation. They use these 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 the power in a large part of those, it can take a lot of time to recover.

Making sure the distribution and substation automation systems are secure is hence critical. Grid operators need to set good security requirements when procuring RTUs and gateways. 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 vendors. They are designed to fit into the processes and procedures already in place in the organizations and to find a good balance between security and the operational impact.

Harmonizing the requirements allows grid operators to get secure automation equipment more cost-effectively. 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 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 or gateways.

The requirements are based on the IEC 62443 standard. They have been selected from part *IEC 62443-4-2: Technical security requirements for IACS components* [1]. This standard is widely supported by manufacturers and grid operators, allowing the requirements to be more easily implemented.

The requirements have been designed to allow certification based on the new certification schemes being developed for IEC 62443. Together with the threat analysis for substation automation systems in [2] they form a profile for IEC 62443 (following the rules in [3]). The profile also meets the requirements for a component context analysis, as defined in

the JRC *Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS)* [4].

When grid operators use the technical requirements below, it is recommended to also require that the supplier complies fully to **IEC 62443-4-1** [5] **at maturity level at least 3**. Doing so, ensures that the supplier has secure development processes, so that they can correctly and consistently implement the requirements.

1.1 Relation to other documents

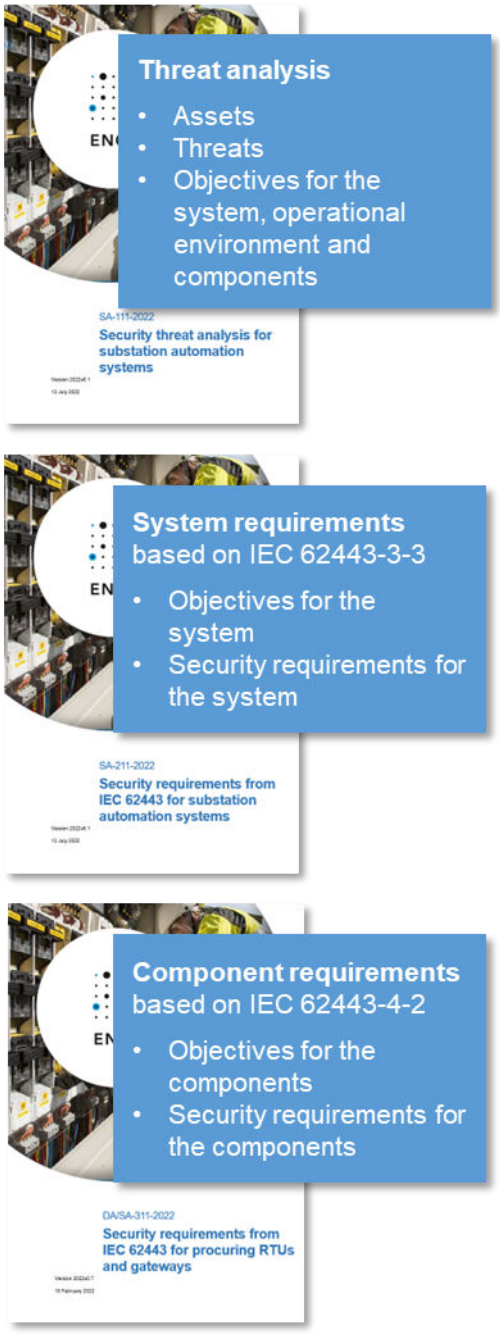
This document is part of two larger series of documents on substation automation and distribution automation security, as shown in Figure 1. Both series starts with a threat analysis [2] that determines security objectives to counter the threats posed to the assets in a typical substation or distribution automation system. The objectives are split into objectives for the system and operational environment. The objectives for the system are the basis for the security requirements for the system in [6].

The objectives for the operational environment should be implemented by grid operators outside of the system to operate it securely. Many grid operators will meet these security objectives through their information security management system. Hence, the objectives are linked to controls from the ISO/IEC 27002:2022 standard [7]. They include organizational, people, physical, and technological objectives.

From the security objectives for the system, Section 3 derives security objectives for gateways and RTUs. The objectives are chosen so that a gateway meeting the component objectives can be easily integrated into a system meeting the system objectives. The security objectives are the basis for the requirements for gateways and RTUs in Section 4.

The same objectives are chosen for gateways and RTUs in substation and distribution automation systems, because often vendors are offering the same devices or platforms for both types of systems. By setting the same objectives and requirements, it will be easier for vendors to define their security roadmap and for grid operators to procure devices that meet the requirements.

How to use the document



- Check if all threats are mitigated by the security objectives or if additional objectives are needed
- Get objectives for the operational environment, to be implemented for instance through an ISMS
- Use as requirements when procuring a complete system
- Set technical requirements to internal department maintaining the system
- Use as requirements when procuring components for the system

Figure 1: Relation between the different documents on substation automation security.

2 Device description

To effectively use the security requirements, it is important to know the assumptions they make about how the RTU, or gateway is works. This includes the intended use of device system, its operational environment, and the access control model used in the threat assessment [2] to set security objectives.

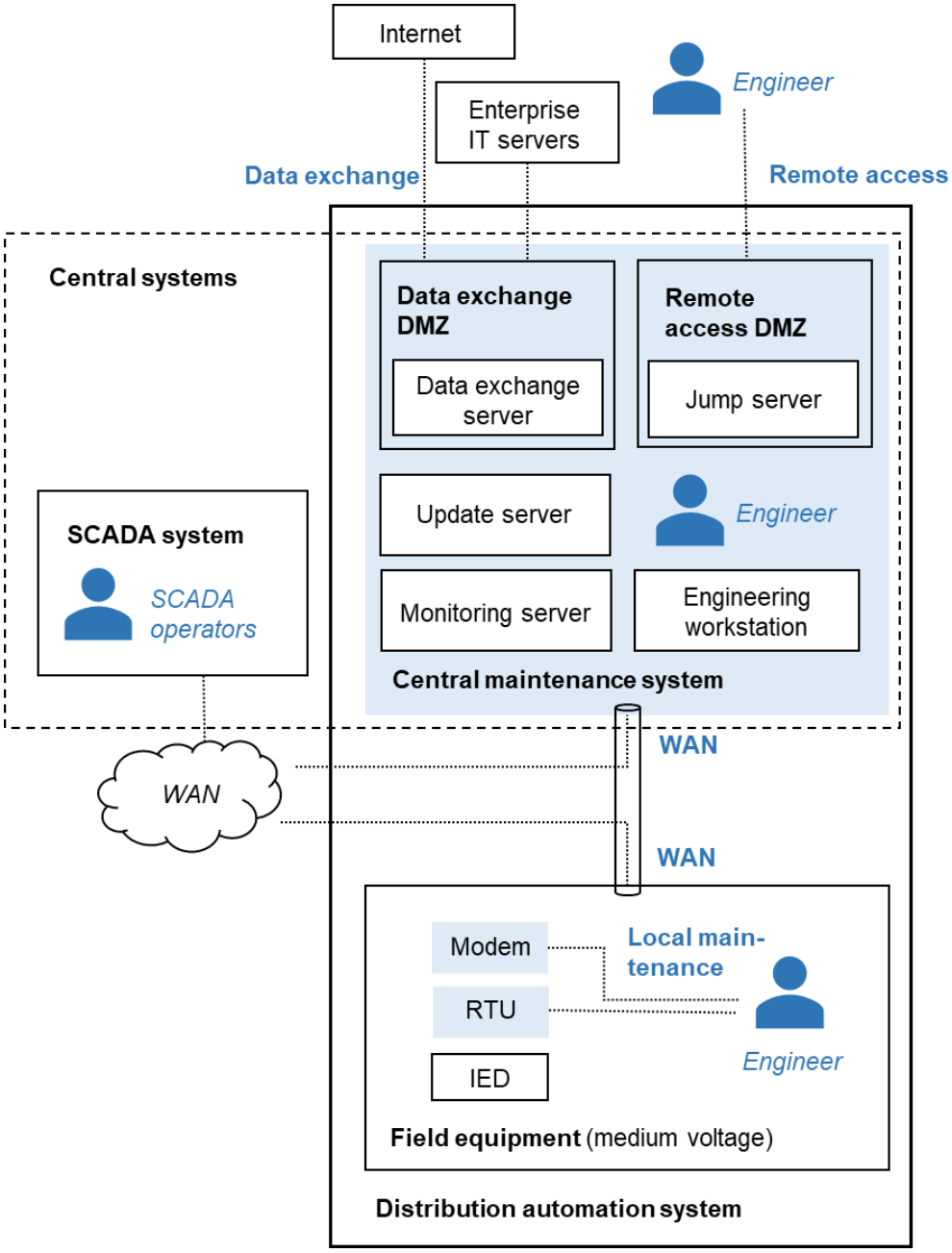


Figure 2: Reference architecture for distribution automation systems, showing its users and interfaces. The requirements in this document concern the RTU.

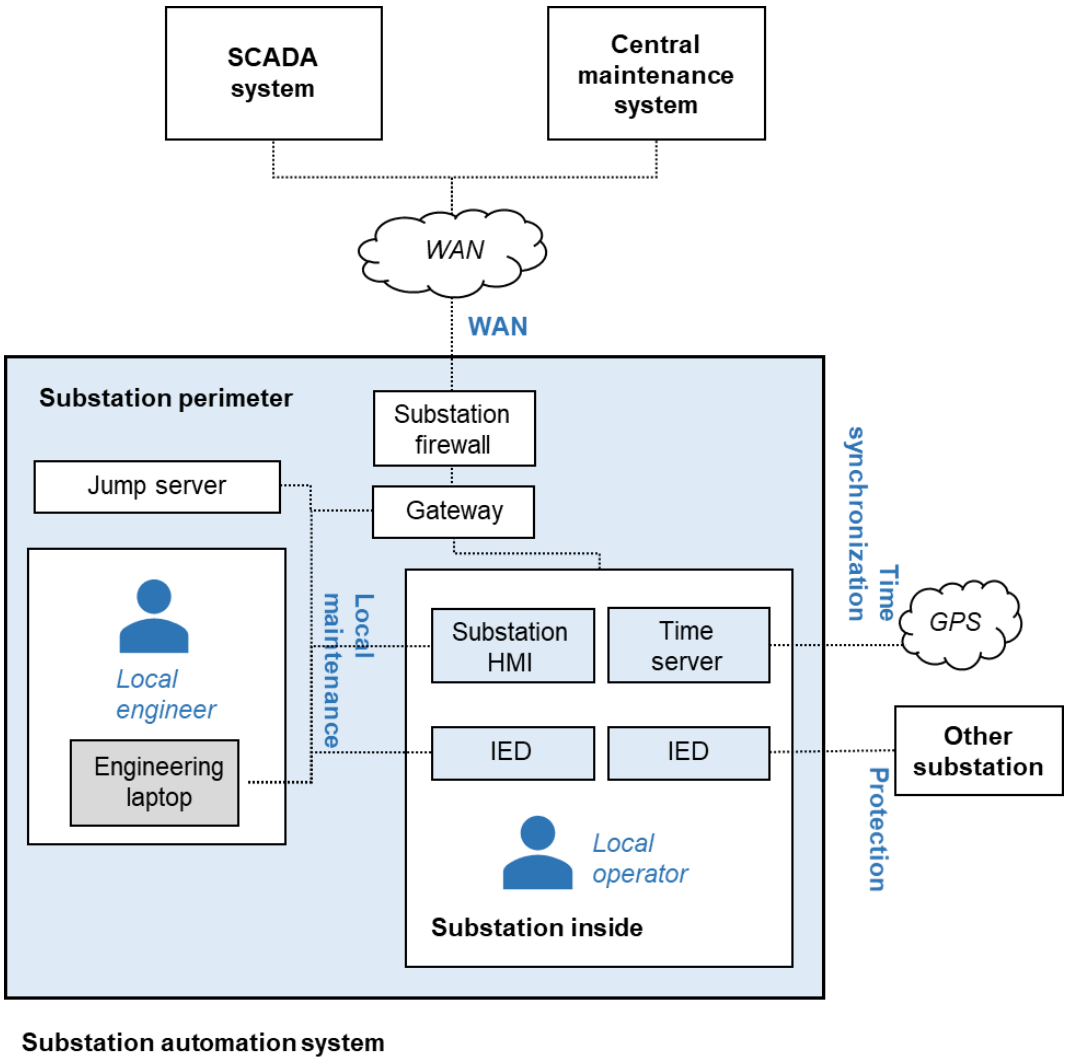


Figure 3: Reference architecture for the substation automation system, showing its users and interfaces. The requirements in this document concern the gateway.

2.1 Intended use of the device

This document gives requirements for procuring secure RTUs and gateways for distribution automation and substation automation systems. The RTUs and gateways can be used in:

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

The same security requirements are used for distribution automation (medium voltage) and substation automation (high voltage), as manufacturers often offer the same devices or platforms in both domains.

Grid operators use RTUs and gateways to monitor and control the medium and high voltage electricity grid from the SCADA systems at their control centers. The RTU or gateway is the device at a substation with which the SCADA system communicates. From the RTU or gateway, the SCADA system gets measurements on the state of the grids, and alarms from, for instance, short circuit indicators from the RTU or gateway, and it sends commands to control the grid, for instance by switching circuit breakers, to the RTU or gateway.

We will use the name '**RTU**' for devices that are connected to sensors and actuators primarily through digital and analog input and output (Figure 2), and '**gateway**' for devices connected primarily through network communication (Figure 3). RTUs are more commonly used in distribution automation (medium voltage substations), whereas gateways are more commonly used in substation automation (high-voltage substations). But the distinction between RTUs and gateways is often not clear. Many devices on the markets can be used in either role, depending on their configuration. Hence, the security requirements are designed to apply to both RTUs and gateways.

In this document, the term **"device"** will be used for both **RTUs** and **gateways**.

2.2 Intended operational environment

Figure 2 and Figure 3 show the reference architecture for distribution and substation automation systems used in this document. The reference architectures give a simplified view of the intended operational environment for the RTUs and gateways. Security objectives for the operational environment are given in the risk assessments [8] and [9].

The RTU or gateway is connected to the SCADA system over a wide-area network (WAN). For distribution automation, this is usually a wireless mobile network, such as a GPRS, CDMA, or LTE network. For substation automation, it is usually a glass fiber network. Grid operators often use the networks of external telecom providers, especially for distribution automation. Network segregation measures such as private APNs are commonly used. But the WAN network is usually not considered trusted for the type of grid control that RTUs and gateways are used for.

The SCADA systems communicate with the RTU or gateway using specialized protocols. Currently, IEC 60870-5-104 is most commonly used. In the future, it is expected that MMS will be increasingly used according to the IEC 61850 standard. For communication with sensors and actuators in the substation, gateways often also use MMS following IEC 61850.

The RTU or gateway is maintained by engineers from the grid operator or its contractors. They can maintain the RTU or gateway locally or remotely. Local maintenance is done at the field location with an engineering laptop. The laptop connects to a local maintenance interface on the RTU or gateway, which can for instance be an Ethernet, USB, or serial port. The engineer then uses specialized engineering software or a web interface on the RTU or gateway to configure it and troubleshoot problems.

Remote maintenance is done from the grid operator's offices, usually from secure locations close to the control centers. Remote maintenance can be done with the same tools as local maintenance. Alternatively, specialized maintenance servers are used to monitor and configure large numbers of RTUs or gateways, and to apply batch firmware updates. Such servers are more commonly use in distribution automation, as this involves many more devices than substation automation.

Physically, the RTUs and gateways are deployed in substations and other field locations. These locations are unattended most of the time. Engineers only visit them when there are problems or there is scheduled maintenance. Some locations may not be visited for years.

Physical security differs greatly between locations. Large high-voltage substations may be protected by advanced alarm and camera systems, monitored by physical security companies. Distribution automation substations usually are in separate buildings or rooms that are locked. Sometimes there is a sensor to detect door openings. But reacting to the alarms from such sensors make take considerable time. RTUs on overhead distribution lines are, at most, protected by a locked cabinet.

The security requirements assume that motivated attackers can physically reach the RTU. They may also steal an RTU to prepare physical attacks. The goal is to allow grid operators to limit the impact of such physical attacks.

2.3 Access control policy

Table 1 lists the users that are authorized to access the RTU and gateway and the access they require. See Figure 2 and Figure 3 for the interfaces. The access control policy should be designed to implement the principle of least privileges, so that each user group can only access the functions it requires.

Table 1: User groups on the device.

User group	Required access	Interface
SCADA system	• Collect measurements of electrical variables	WAN

	• Send control commands	
Central maintenance system	• Configure the device • Recover the device from a backed-up configuration • Update the device firmware • Monitor the operational logs • Collect additional measurements of electrical variables	WAN
Engineers	• Configure the device • Recover the device from a backed-up configuration • Update the device firmware • Analyze the operational logs	Local maintenance

On the WAN there are two user groups accessing the device: the SCADA system and the central maintenance system. These user groups have different access requirements. The SCADA system only requires access to grid related assets. It should be able to collect the measurements of electrical variables and send control commands.

The central maintenance system should normally only access the configuration and the firmware. In some cases, the central maintenance system may however collect additional measurements of electrical variables, such as high frequency measurements related to faults.

The device should be able to distinguish between the two user groups on the WAN to limit the impact if one of the groups is compromised. Each user group should separately authenticate to the device. The device should ensure that each system can only access the required functions.

On the local maintenance interface, the only user group is engineers from the grid operator or its contractors. These should be able to change the configuration and update the firmware. In case of problems, they should be able to configure the device from a backup configuration. Grid operators may define roles within the group of engineers to apply more fine-grained access rights.

The access control model assumes that engineers do not access the device directly over the WAN. They always work through the central maintenance system.

3 Security objectives for gateways and RTUs

Below are the security objectives for a gateway that are the basis for the security requirements in for gateways and RTUs in Section 4.

8.3-CO1 Role separation for the SCADA and central maintenance system: The device can enforce access control with a separate role for the SCADA system and central maintenance system, so that they can only access the functions they need for their role.
8.3-CO2 Centrally managed, role-based access control for engineers: The device can enforce role-based access control for engineers with individual user accounts managed on a central server.
8.5-CO1 Network-based authentication for the SCADA system: The device can enforce mutual authentication with the SCADA system at network level, for instance through a VPN. The device can verify that the SCADA system is on a trusted network, while allowing SCADA system users to verify the device's unique identity.
8.5-CO2 Mutual authentication for the central maintenance system: The central maintenance system identifies to the device with information that allows the zone to determine its role. The device authenticates the system's role and assigns it access rights based on the role. The device uniquely identifies itself to the central maintenance system and allows the system to authenticate it.
8.5-CO3 Authentication with individual passwords for engineers: The device can enforce mutual authentication for engineers. Engineers use individual passwords or keys. The login procedure is protected against known attacks
8.8-CO1 Remote hardening: Through remote access from the central maintenance system, the device allows to disable unneeded functions to reduce the likelihood of vulnerabilities and allows to enable security functions available on the hardware and software platforms to reduce their possible impact.
8.9-CO1 Remote configuration management: The device can be restored from a backed-up configuration through remote access from the central maintenance system.

8.15-CO1 Integration with SIEM system: The device logs all relevant security events, such as access control events, and changes to the configuration and firmware. The device can store the logs locally for forensic analysis. It can send them to a Security Information and Event Management (SIEM) system in a commonly supported format, (SIEM) system, so that they can be analyzed to detect incidents.
8.17-CO1 Clock synchronization: The device supports synchronizing time with a central source to have reliable timestamps for security events.
8.19-CO1 Remote software and firmware management: The software and firmware on the device can be updated through remote access from the central maintenance system. The device checks the authenticity of firmware or software through digital signatures.
8.20-CO1 Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces: The device can cryptographically protect the integrity and confidentiality of communication on the WAN and remote maintenance interfaces using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.
8.24-CO1 Remote key and password management: All passwords and keys on the device can be updated through remote access from the central maintenance system.

3.1 Rationale for the component objectives

The component objectives are derived from the system level objectives for substation automation systems in [2] and for distribution automation systems in [10]. Each component objective is a direct translation of the system level objective with the same number.

For the substation automation system objectives, all technological objectives for the substation perimeter are covered, except the following:

- **8.7-SO1:** Malware protection on commercial off-the-shelf operating systems is excluded, because the gateway is assumed to be an embedded device, and not use an off-the-shelf operating system.
- **8.19-SO2** and **8.20-SO2**: The resilience of protection functions under denial-of-service attacks and firmware updates is excluded because the gateway is assumed not to implement protection functions. Providing such resilience would be technically complex, and hence could raise the cost of the gateway.

- **8.22-SO1**: The gateway is not required to provide network segregation on the WAN as it is assumed to be provided by a substation firewall. The gateway may have a host-based firewall but should not be responsible for segregating the internal substation networks from the WAN.

To do: link to distribution automation objectives.

4 Security requirements

Section 3 sets security objectives for RTUs and gateways to align with the overall objectives for the substation automation system. These objectives refine the technological security controls in ISO/IEC 27002:2022 [7]. We now break down the objectives into more detailed requirements from IEC 62443-4-2 [1] that a system integrator or department building or maintaining a substation automation system can follow (Table 2). See Section 4.1 for the full list of requirements.

Not all objectives can be fully covered through IEC 62443-4-2 requirements. So, some additional requirements are included. They are given in italic in the table below. The rationale for selecting the requirements is give in Section 4.2.

As mentioned in the introduction, it is recommended that besides the technological requirements selected here, grid operators also require that any software supplier complies full to **IEC 62443-4-1** [11] at **maturity level at least 3**.

Table 2 Breakdown of objectives into IEC 62443-4-2 requirements

Security objective	***IEC 62443-4-2 requirements***
8.3 Information access restriction	
8.3-CO1 Role separation for the SCADA and central maintenance system: The device can enforce access control with a separate role for the SCADA system and central maintenance system, so that they can only access the functions they need for their role.	• CR2.1 Authorization enforcement • CR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • *CR2.1 EE1 Role separation for software processes*
8.3-CO2 Centrally managed, role-based access control for engineers: The device can enforce role-based access control for engineers with individual user accounts managed on a central server.	• CR1.3 Account management • *CR1.3 EE1 Centrally managed, role-based accounts* • CR1.4 Identifier management • CR2.1 Authorization enforcement • CR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • CR2.1 RE2 Permission mapping to roles

8.5 Secure authentication	
8.5-CO1 Network-based authentication for the SCADA system: The device can enforce mutual authentication with the SCADA system at network level, for instance through a VPN. The device can verify that the SCADA system is on a trusted network, while allowing SCADA system users to verify the device's unique identity.	• CR1.2 Software process and device identification and authentication • *CR1.2 EE2 Mutual identification and authentication for software processes and devices based on network location* • CR1.9 Strength of public key-based authentication • CR4.3 Use of cryptography • *CR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.5-CO2 Role-based authentication for the central maintenance system: The central maintenance system identifies to the device with information that allows the zone to determine its role. The device authenticates the system's role and assigns it access rights based on the role. The device uniquely identifies itself to the central maintenance system and allows the system to authenticate it.	• CR1.2 Software process and device identification and authentication • *CR1.2 EE1 Mutual identification and authentication for software processes and devices* • CR1.9 Strength of public key-based authentication • CR2.6 Remote session termination • CR4.3 Use of cryptography • *CR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.5-CO3 Authentication with individual passwords for engineers: The device can enforce mutual authentication for engineers. Engineers use individual passwords or keys. The login procedure is protected against known attacks	• CR1.1 Human user identification and authentication • CR1.1 RE1 Unique identification and authentication • CR1.5 Authenticator management • *CR1.5 EE1 Storing passwords* • CR1.7 Strength of password-based authentication

	• CR1.7 RE1 Password generation and lifetime restrictions for human users • CR1.9 Strength of public key-based authentication • CR1.10 Authenticator feedback • CR1.11 Unsuccessful login attempts • CR2.5 Session lock • CR2.6 Remote session termination • CR4.3 Use of cryptography • *CR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.8 Management of technical vulnerabilities	
8.8-CO1 Remote hardening: Through remote access from the central maintenance system, the device allows to disable unneeded functions to reduce the likelihood of vulnerabilities and allows to enable security functions available on the hardware and software platforms to reduce their possible impact.	• CR 7.7 Least functionality • EDR 3.2 Protection from malicious code
8.9 Configuration management	
8.9-CO1 Remote configuration management: The device can be restored from a backed-up configuration through remote access from the central maintenance system.	• CR 7.3 Control system backup • CR 7.4 Control system recovery and reconstitution • *CR7.4 EE1 Recovery from configuration file*
8.15 Logging	
8.15-CO1 Integration with SIEM system: The device logs all relevant security events, such as access control events, and changes to the configuration and firmware. The	• CR2.8 Auditable events • CR2.9 Audit storage capacity • CR2.10 Response to audit processing failures

device can store the logs locally for forensic analysis. It can send them to a Security Information and Event Management (SIEM) system in a commonly supported format, (SIEM) system, so that they can be analyzed to detect incidents.	• CR3.9 Protection of audit information • *CR3.9 EE1 Audit information persistence* • CR6.1 Audit log accessibility • CR6.1 RE1 Programmatic access to audit logs • *CR6.1 EE1 Restricted access to logs* • *CR6.1 EE2 Programmatic access to audit logs through syslog*
8.17 Clock synchronization	
8.17-CO1 Clock synchronization: The device supports synchronizing time with a central source to have reliable timestamps for security events.	• CR2.11 Timestamps • CR2.11 RE1 Time synchronization • CR2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
8.19-CO1 Remote software and firmware management: The software and firmware on the device can be updated through remote access from the central maintenance system. The device checks the authenticity of firmware or software through digital signatures.	• CR1.8 Public key infrastructure certificates • CR1.9 Strength of public key-based authentication • CR4.3 Use of cryptography • *CR4.3 EE1 Use of cryptography according to ECRYPT recommendations* • EDR 3.10 Support for updates • EDR 3.10 RE1 Update authenticity and integrity • *EDR3.10 EE1 Update capacity* • *EDR3.10 EE3 Remote updates* • *EDR3.10 EE4 Software authenticity under recovery*
8.20 Network security	

8.20-CO1 Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces: The device can cryptographically protect the integrity and confidentiality of communication on the WAN and remote maintenance interfaces using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.	• CR 1.9 Strength of public key-based authentication • CR3.1 Communication integrity • CR3.1 RE1 Communication authentication • CR 3.8 Session integrity • CR4.1 Information confidentiality • CR4.3 Use of cryptography • *CR 4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.24 Use of cryptography	
8.24-CO1 Remote key and password management: All passwords and keys on the device can be updated through remote access from the central maintenance system.	• CR1.5 Authenticator management • *CR1.5 EE2 Remote authenticator update* • EDR 3.13 Provisioning asset owner roots of trust

4.1 Requirements selected from IEC 62443-4-2

The table below lists the requirements selected from the IEC 62443-4-2 standard on *Technical security requirements for IACS components* [1].

We are assuming here that the RTU, or gateway is an embedded device, and is using the embedded device requirement (EDR) from IEC 62443-4-2. If the RTU or gateway is implemented as application software running on an off-the-shelf computer, the corresponding software application requirements (SAR) should be used instead.

Some additional requirements to the IEC 62443 requirements are needed to fully cover the security objectives. These requirements are marked in the table below in blue. They have an extension number starting with ‘EE’.

IEC	Name	Objective
CR1.1	**Human user identification and authentication**	8.5-CO3
CR1.1 RE 1	**Unique identification and authentication**	8.5-CO3

IEC	Name	Objective
CR1.2	**Software process and device identification and authentication**	8.5-CO1 8.5-CO2
CR1.2 EE1	**Role-based identification and authentication for the central maintenance system** Components shall provide the capability to identify and authenticate the role of the central maintenance system. This capability shall enforce such identification and authentication to support least privilege in accordance with applicable security policies and procedures.	8.5-CO2
CR1.2 EE2	**Mutual identification and authentication for the SCADA system based on network location** Components shall provide the capability to provide authentication for the SCADA system through one of the following options: A. Based on its network location through a VPN terminating at the device. Mutual authentication shall be used between the device and a network device (e.g., firewall or concentrator) at the SCADA system during the setup of the VPN. Unique passwords or keys can be used for each device. B. Using unique mutual authentication, so that the SCADA system can check that a connection comes from a unique device, and the device can check that a connection comes from the SCADA system.	8.5-CO1
CR1.3	**Account management**	8.3-CO2
CR1.3 EE1	**Centrally managed, role-based accounts for engineers** Components shall provide the capability to be integrated into a central system for managing the accounts for	8.3-CO2

IEC	Name	Objective
	engineers. The component shall assign an account to a role based on information from the central system. Components shall provide a way for human users to access it when the device cannot reach the central system. *Supplemental guidance:* The components may integrate with the central account management system through different technologies, such as RADIUS, LDAP or Active Directory. It is recommended to by default support the roles and privileges defined in IEC 62351-8 [12]. To provide access when it cannot reach the central authentication server, the device can for instance use local accounts. 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.	
CR1.4	**Identifier management**	8.3-CO2
CR1.5	**Authenticator management**	8.5-CO3 8.24-CO1
CR1.5 EE1	**Storing passwords** Components shall store passwords salted and hashed. *Supplemental guidance:* It is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.	8.5-CO3
CR1.5 EE2	**Remote authenticator update**	8.24-CO1

IEC	Name	Objective
	Components shall provide the capability to remotely change all authenticators in a way that protects their confidentiality and integrity. *Supplemental guidance:* 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) [13] or Enrollment over Secure Transport (EST) [14] described IEC 62351-9 [15]. It is allowed that keys or credentials cannot be updated if they are only used for device internal purposes, such as encrypting local storage or setting up secure communication between processors on the same device. But, as soon as they are used to implement any of the requirements in this document, they must also comply with this requirement.	
CR1.7	**Strength of password-based authentication**	8.5-CO3
CR1.7 RE1	**Password generation and lifetime restrictions for human users**	8.5-CO3
CR1.8	**Public key infrastructure certificates**	8.19-CO1
CR1.9	**Strength of public key-based authentication**	8.5-CO1 8.5-CO2 8.5-CO3 8.19-CO1 8.20-CO1
CR1.10	**Authenticator feedback**	8.5-CO3
CR1.11	**Unsuccessful login attempts**	8.5-CO3

IEC	Name	Objective
CR2.1	**Authorization enforcement**	8.3-CO1 8.3-CO2
CR2.1 RE1	**Authorization enforcement for all users (humans, software processes and devices)**	8.3-CO1 8.3-CO2
CR2.1 RE2	**Permission mapping to roles**	8.3-CO2
CR2.1 EE1	**Role separation for the SCADA system and the central maintenance system** Components shall provide the capability to set different authorizations for different roles, allowing to define at least roles for the SCADA system and the central maintenance system, and to apply the principle of least privileges for these roles.	8.3-CO1
CR2.5	**Session lock**	8.5-CO3
CR2.6	**Remote session termination**	8.5-CO2 8.5-CO3
CR2.8	**Auditable events**	8.15-CO1
CR2.9	**Audit storage capacity**	8.15-CO1
CR2.10	**Response to audit processing failures**	8.15-CO1
CR2.11	**Timestamps**	8.17-CO1
CR2.11 RE1	**Time synchronization**	8.17-CO1
CR2.11 RE2	**Protection of time source integrity**	8.17-CO1
CR3.1	**Communication integrity**	8.20-CO1

IEC	Name	Objective
CR3.1 RE1	**Communication authentication** *Restriction:* Authenticity is only required to be protected on the WAN interface. *Supplemental guidance:* The integrity and authenticity of the communication can be protected by setting up a VPN tunnel or by using TLS (as specified in IEC 62351-3 [11] and IEC 60870-5-7 [12]). If end-to-end secure protocols are used for the SCADA traffic, it is recommended that the device allows to turn off encryption and use only message authentication, so that it is possible to apply deep-packet inspection. With TLS this can be achieved by using the NULL cipher (although this is not allowed by IEC 62351-3 [11]). If a VPN is used to implement the first part of the requirement, the deep-packet inspection sensor can be placed after the VPN concentrator in the central systems. So, encryption can be used without limiting visibility.	8.20-CO1
CR3.8	**Session integrity**	8.20-CO1
CR3.9	**Protection of audit information**	8.15-CO1
CR3.9 EE1	**Audit information persistence** Components shall ensure that audit information and audit logs are persistent under reboots of the component and firmware updates.	8.15-CO1
CR4.1	**Information confidentiality** *Restriction:* Information in transit only needs to be protected on the WAN network using cryptographic measures. Information at rest may be protected by access control mechanisms. Cryptographic protection is not required at rest.	8.20-CO1

IEC	Name	Objective
	Supplemental guidance: Confidentiality of the communication can be protected by setting up a VPN tunnel or by using TLS (as specified in IEC 62351-3 [11] and IEC 60870-5-7 [12]).	
CR4.3	**Use of cryptography**	8.5-CO1 8.5-CO2 8.5-CO3 8.19-CO1 8.20-CO1
CR4.3 EE1	**Use of cryptography according to ECRYPT recommendations** Components shall follow the recommendations in the ECRYPT – Algorithms, Key Size, and Protocols Report [16]. In particular: • They only use the cryptographic algorithms that the ECRYPT recommends as suitable for new or future systems. • They use keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in the ECRYPT report). • They only use a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report (Section 3.2.3) to generate random numbers for security functions.	8.5-CO1 8.5-CO2 8.19-CO1 8.20-CO1
CR6.1	**Audit log accessibility**	8.15-CO1
CR6.1 RE1	**Programmatic access to audit logs**	8.15-CO1
CR6.1 EE1	**Restricted access to audit logs**	8.15-CO2

IEC	Name	Objective
	Components shall allow access to the audit information and audit logs to be restricted to privileged users, such as administrators.	
CR6.1 EE2	**Programmatic access to audit logs through syslog** Components shall provide the capability to send the audit records using the syslog communication protocol in a commonly used format to avoid the need to develop a dedicated parser.	8.15-CO1
CR7.3	**Control system backup**	8.9-CO1
CR7.4	**Control system recovery and reconstitution**	8.9-CO1
CR7.4 EE1	**Recovery from configuration file** The device shall allow for its configuration to be recovered from a from a backup configuration file.	8.9-CO1
CR7.7	**Least functionality**	8.8-CO1
EDR3.2	**Protection from malicious code** *Supplemental guidance:* It is recommended to use the following hardware features when they are supported: • No-Execute (NX) / Write-xor-execute (W^R): A Memory Protection Unit (MPU) or Memory Management Unit (MMU) shall be used to mark code regions as read-only and data sections as non-executable. • Address Space Layout Randomization (ASLR): A Memory Management Unit (MMU) shall be used to load data and code at different memory addresses every time an application is run. The software running on the device must be compiled to use the hardware features. The Position Independent Code (PIC) or Position Independent Executable (PIE)	8.8-CO1

IEC	Name	Objective
	compiler options should be enabled to be able to use ASLR.	
EDR3.10	**Support for updates**	8.19-CO1
EDR 3.10 RE1	**Update authenticity and integrity** *Restriction:* Authenticity shall be protected through a digital signature.	8.19-CO1
EDR3.10 EE1	**Update capacity** The embedded device shall have enough memory (RAM and flash) and computing power to allow security updates needed during its lifetime. *Supplemental guidance:* Compliance with 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 the ECRYPT report [16] should show that the device can run them without affecting operations. It is acceptable if the device can only support the long-term key sizes for elliptic curve-based algorithms, not for RSA-based algorithms.	8.19-CO1
EDR3.10 EE3	**Remote updates** The embedded device shall allow the updates to be performed remotely from a centralized system.	8.19-CO1
EDR3.10 EE4	**Software authenticity under recovery** The embedded device shall not allow the mechanisms that protect the authenticity and integrity of software updates to be bypassed through the recovery process, required by CR7.4.	8.19-CO2
EDR3.13	**Provisioning asset owner roots of trust**	8.24-CO1

4.2 Rationale for the requirements

Below a rationale is provided for the requirements selected in Sections 4.1 by showing that they cover the security objectives for the device.

8.3-CO1 Role separation for the SCADA and central maintenance system

General authorization for software process users is covered by *CR2.1* and *CR2.1 RE1.* The additional requirement *CR2.1 EE1* ensure separate roles for the SCADA and central maintenance systems. No requirements on account management are included, as there may not be a clear account associated with the access if for instance a VPN is used.

8.3-CO2 Centrally managed, role-based access control for engineers

Centrally managed access control is covered by *CR2.1, CR2.1 RE1,* and *CR2.1 RE2.*

Account management is covered by requirements *CR1.3* and *CR1.4*. The additional requirement *CR1.3 EE1* is needed to ensure that the accounts can be centrally managed, as requirement *CR1.3* also allows them to be managed on the device.

8.5-CO1 Network-based authentication for the SCADA system

Authentication is covered by requirement *CR1.2* with the additional requirement *CR1.2 EE2*. The additional requirement is needed to provide mutual authentication. Requirement *CR1.2* would only cover authentication from the device to the SCADA system.

Strong cryptographic keys and algorithms for the authentication are ensured by requirements *CR1.9* and *CR4.3*. The additional requirement *CR4.3 EE1* is included to further specify which recommendations on cryptography to follow.

Remote session termination is not included because the SCADA system connection often stays open indefinitely.

8.5-CO2 Role-based authentication for the central maintenance system

Authentication is covered by requirement *CR1.2* with the additional requirement *CR1.2 EE1* to ensure mutual authentication. Strong cryptographic keys and algorithms for the authentication are ensured by requirements *CR1.9* and *CR4.3* with the additional requirement *CR4.3 EE1*. Remote session termination (*CR2.6*) is included to reduce the risk that authentication is bypassed by compromising a session.

8.5-CO3 Authentication with individual passwords for engineers

Authentication with individual user accounts and passwords is ensured by requirements *CR1.1* and *CR1.1 RE1*.

The login procedure is protected against known attacks as follows. Against brute-force attempts, requirement *CR1.11* ensures access can be blocked after a number of unsuccessful login attempts, while *CR1.7* and *CR1.7 RE1* allow enforcing secure passwords. Requirement *CR1.7 RE1* also protects against passwords leaking by allowing to limit their lifetime. Requirements *CR1.5* and *CR1.5 EE1* protects against attacker getting passwords from a compromised device by salting and hashing them. Requirement *CR1.10* obfuscates feedback during authentication. Requirements *CR2.5* and *CR2.6* protect against hijacking a user's session. And requirements *CR1.9*, *CR4.3*, *CR4.3 EE1* protect against cryptographic attacks.

8.8-CO1 Remote hardening

Disabling unneeded functions is covered by requirement *CR 7.7*, enabling security features of the platform by *EDR 3.2*.

8.9-CO1 Remote configuration management

Restoration from a backed-up configuration is covered by requirement *CR 7.3*, *CR 7.4,* and additional requirement *CR7.4 EE1*.

8.15-CO1 Integration with SIEM system

Logging security events is covered by requirement *CR2.8*. Sending the logs to the SIEM system is covered by requirements *CR6.1* and *CR6.1 RE1*. The additional requirement *CR6.1 EE2* is included to ensure that the logs can be sent using syslog in a format supported by most SIEM systems.

Protection of the security logs is covered by requirements *CR2.10* and *CR3.9* with the extensions *CR3.9 EE1* to ensure the logs are persistent and *CR6.1 EE1* to ensure access to the logs can be restricted to privileged users. Requirement *CR2.9* ensures that there is enough storage capacity on the device for the logs.

8.17-CO1 Clock synchronization

Clock synchronization is covered by requirements *CR2.11* and *CR2.11 RE1*. Requirement *CR2.11 RE2* ensures that the integrity of the time source is protected.

8.19-CO1 Remote software and firmware management

Updates of software and firmware are covered by *EDR3.10*. The additional requirement *EDR3.10 EE3* ensures that the updates can be performed remotely, while *EDR3.10 EE1* ensures there is enough memory and computing power for future updates.

The authenticity of the software and firmware is protected by digital signatures according to requirement *EDR3.10 RE1*. The extension *EDR3.10 EE4* ensures that the digital signatures cannot be bypassed through the process to restore backups. Requirement

CR1.8 ensures that the device can be integrated into a PKI for the certificates needed to verify the signature. Requirements *CR1.9*, *CR4.3*, and *CR4.3 EE1* ensure the strength of the cryptography used for the signatures.

8.20-CO1 Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces

Protecting the confidentiality of the information is covered by requirement *CR4.1*. Integrity of the communication by *CR3.1*, *CR3.1 RE1*, and *CR 3.8*. Requirements *CR 1.9*, *CR4.3*, and *CR 4.3 EE1* ensure that strong cryptography is used to protect the communication.

8.24-CO1 Remote key and password management

Remote updates of keys and credentials are covered by requirements *CR1.5* and *CR1.5 EE2*. Requirement *EDR 3.13* allows a root certificate from the grid operator to be installed, so that it can be integrated in their PKI.

Appendix A: 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
CR1.3 EE1	IEC 62351-8 [12]	A set of roles and privileges and two methods (PUSH and PULL) to authenticate users through a central server are defined
CR1.2 EE2	IEC 62351-3 [17] IEC 62351-5 [18]	Authentication using TLS with client-side certificates is specified
CR1.5 EE2	IEC 62351-9 [15]	Different methods for key management on devices, including the SCEP and EST protocols are specified.
CR3.1 RE1 CR4.1	IEC 62351-3 [17] IEC 62351-5 [18]	Communication security using TLS and an application layer method is specified. (Using TLS is recommended.)

Glossary

APN	Access Point Name
CVSS	Common Vulnerability Scoring System
EST	Enrollment over Secure Transport
ISMS	Information Security Management System
MV	Medium Voltage
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] 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.

[2] ENCS, "SA-111-2022: Security threat analysis for substation automation systems," 2022.

[3] IEC, "IEC 62443-1-5: Rules for IEC 62443 profiles," 2022.

[4] Joint Research Center, "Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme," 2020.

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

[6] ENCS, "SA-211-2022: Security requirements from IEC 62443 for substation automation systems," 2022.

[7] ISO/IEC , "ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls," 2022.

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

[9] ENCS, "SA-101-2022: Security risk assessment for substation automation systems," 2022.

[10] ENCS, "DA-111-2022: Security threat analysis for distribution automation systems," 2022.

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

[12] IEC, "IEC 62351-8: Power systems management and associated information exchange - Data and communications security - Part 8: Role-based access control," 2020.

[13] Internet Engineering Task Force (IETF), "RFC 8894: Simple Certificate Enrolment Protocol," 2020.

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

[15] 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.

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

[17] 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.

[18] 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.