ANNEX I: SUBSTATION GATEWAY CYBERSECURITY PROFILE

Annex I to the proposal of the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity, for a non-binding cybersecurity procurement recommendation on gateways used for substation automation in accordance with Article 35 of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code for cybersecurity aspects of cross-border electricity flows

1 Table of Contents

2 Introduction

This document provides a cybersecurity profile that TSOs, DSOs, and other entities can use to procure substation gateways and RTUs.

The profile was developed in accordance with Article 35, of Commission Regulation (EU) 2024/1366 establishing a network code for cybersecurity aspects of cross-border electricity flows (hereafter referred to as 'NCCS'). According to this article ENTSO-E in cooperation with the EU DSO entity shall endeavour to ensure that the non-binding cybersecurity procurement recommendations developed based on the relevant regional cybersecurity risk assessment and similar or comparable across system operation regions.

The profile defines a set of recommended cybersecurity requirements for gateways used in substation automation systems. The requirements have been selected based on a threat analysis that identified common threats to substation automation systems. The requirements are meant to be used as cybersecurity specifications when entities procure new substation gateways (see Article 33 (2) (a) of the NCCS). The requirements are not meant to be applied retroactively to already installed gateways. The profile can also be used as the basis for security evaluations using IEC 62443-6-2.

The requirements have been selected from the IEC 62443 standard, specifically parts IEC 62443-4-1 and IEC 62443-4-2. The profile has been set up to meet the requirements to IEC 62443 security profiles defined in IEC 62443-1-5.

2.1 Legal status of this document

The profile is a non-binding recommendation that entities may use when procuring substation gateways and RTUs. Entities should always perform their own risk assessment when procuring new equipment. Entities are allowed to use their own cybersecurity specifications.

2.2 Selected standards

This security profile refers to the following standards:

- IEC 62443-4-1: 2018
- IEC 62443-4-2: 2019
- IEC 62443-1-5:2023
- IEC 62351-3:2023
- IEC 62351-8:2020
- IEC 62351-9:2023

2.3 Terms and definitions

The following terms and abbreviations are needed for the correct comprehension of this document.

HMI: Human Machine Interface, the computer or device that an operator in the substation uses to interact with the substation automation system.

IED: In the electric power industry, an intelligent electronic device (IED) is an integrated microprocessor-based controller of power system equipment

NCCS: Network code on cybersecurity, the Commission delegated regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

RTU: Remote Terminal Unit

SDL: Secure Development Lifecycle

2.4 Profile consistency statement

The profile here described follows strictly the main IEC 62443 principles including the development process described in the IEC 62443-4-1.

This profile aims to identify the minimal security requirements for a family of products used in the electrical sector.

The selected security controls are complemented with security technical choices described in sector specific IEC 62351 series for solution interoperability and overall consistency.

3 Component context description

3.1 Scope

This document details security requirements with the intended use of secure **RTUs (Remote Terminal Units) and gateways used inside a typical substation automation system**. The RTUs and gateways can be used in several types of automation systems, covering sector different use cases such as generation, transmission, distribution, and grid connection but not limited to the examples given here.

The gateway or RTU is the device in the substation that connects to the central SCADA system in the operator's control centres (see Figure 1). It connects devices in the substation to the outside. The RTUs and gateways operate on the application layer. It is assumed that there is a separate substation gateway or router that connects the substation on the network layer. IEDs and other devices in the substation have an application layer connection to the gateway to send measurements and receive commands. The gateway then has an application layer connection to the SCADA system to pass on measurements from the IEDs and commands to the IEDs.

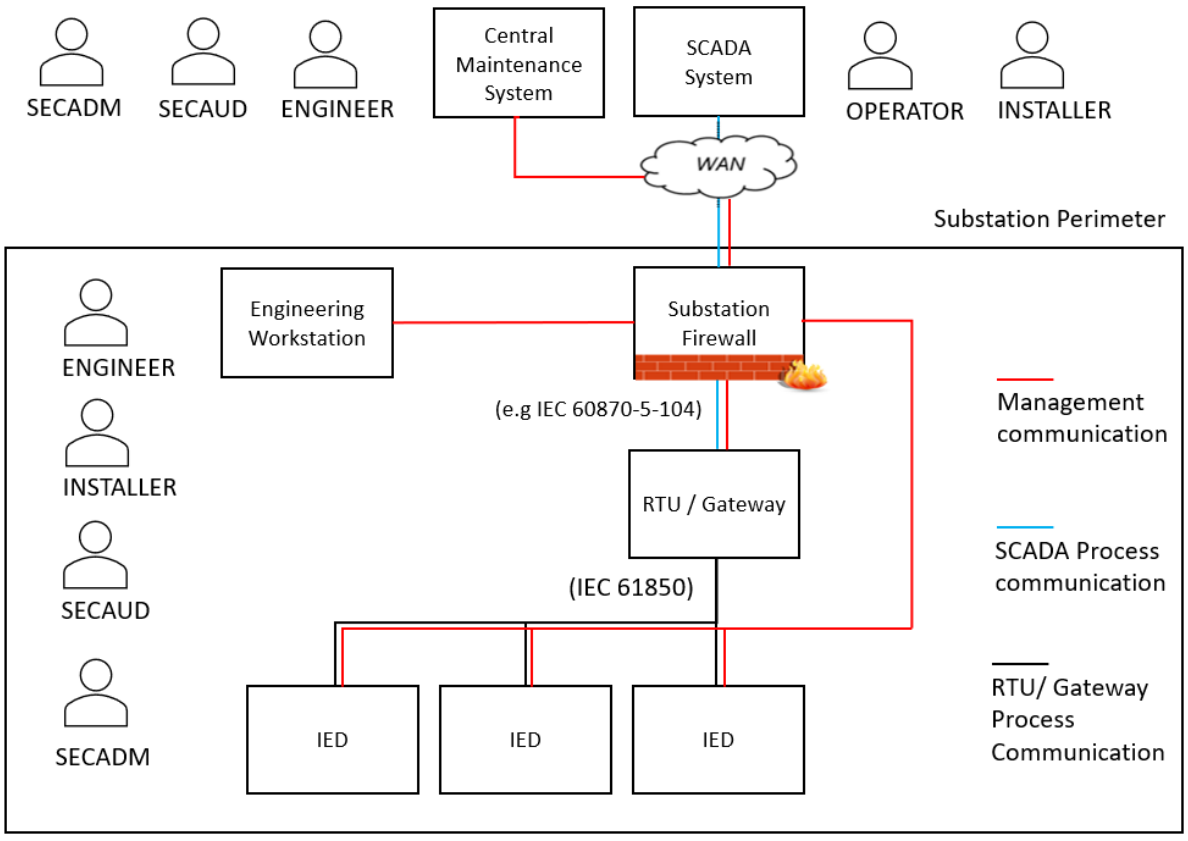

Figure 1: Reference architecture for the gateway including user roles

Equipment in the substation that only communicates with other devices inside the substation, such as IEDs, local HMIs, or local SCADA systems, are not in scope of this profile.

This profile is aimed at RTUs and gateways for substation automation systems that are typically used in high-voltage (primary) substations, including high-voltage transport substations and high- to medium-voltage transformer substations. The profile assumes that the RTU or gateway is protected logically by a substation firewall and physically by the security measures at the substation. The profile is not designed to be used for distribution automation RTUs and gateways that would be used in medium voltage substations or recloser locations. Such RTUs and gateways are more physically exposed and often include a built-in modem. Hence, additional security measures could be needed that are not considered in this profile.

The distinction between RTUs and gateways is often not clear. Many devices on the market can be used in either role, depending on their configuration. Hence, the security requirements are designed to apply to both RTUs and gateways. The name 'RTU' is normally used for devices that are connected to sensors and actuators primarily through digital and analogue input and output and 'gateway' for devices connected primarily through network communication interfaces to other devices such as power meters or protection equipment providing the needed information or actuation.

The term **gateway** will be used throughout the document to designate substation RTUs and gateways.

3.2 Gateway intended use

Grid operators use gateways to remotely monitor and control the electric grid from the SCADA system located at their control centres. The gateway is the device at a substation remote site which handles all SCADA system communication.

From the gateway, the SCADA system acquires a representative number of measured and calculated data, dynamically representing the electrical process under supervision. The number of variables and data types can vary according to the application type, but as indicator they aim to cover the needs of the operator in terms of grid observability and control capacity.

For the **remote monitoring and control function**, the primary information assets are the information sent to or received from the SCADA system:

- status representing physical state of field equipment such as open, closed, or in movement
- alarms indicating problems in the grid or at field locations
- protection functions occurrences such as Start, Trip or failure
- measurements of electrical variables, such as voltages and currents
- commands to operate equipment in the substation switchyard, such as circuit breakers, disconnectors, and earthing switches.

3.3 Gateway intended operational environment

For grid operation purposes, the gateway is connected to the SCADA system over a wide-area network (WAN), grid operators often use the networks of external telecommunication providers. Depending on the application type, the network can be a wireless mobile network, such as a GPRS, CDMA, LTE, 5G network, or a fibre-optic network.

The profile assumes that network segregation measures such as private APNs, firewall, VPN/routers, or any combination of those are used. In particular, a substation firewall is used to separate the WAN from the internal substation networks. The firewall functions may be provided by a dedicated device or by networking equipment such as routers used for the WAN.

The SCADA system communicates with the gateway using specialized protocols, currently IEC 60870-5-104 and IEC 60870-5-101 are commonly used. In the future, IEC 61850 will become more common following the IEC 61850-90-2 [1] standard. For communication with sensors and actuators in the substation, gateways often use MMS protocol following IEC 61850 standard.

Physically, the gateway is deployed in substations. These locations are unattended most of the time. Engineers only visit them when there is scheduled maintenance or there are problems to be addressed. Security physical controls are implemented in field location by the asset owner to protect installations.

For maintenance activities the gateway can be accessed by engineers and infrastructure administrators from the grid operator or its contractors.

Maintenance activities on the gateway can be done locally or remotely. Local maintenance is done at the field location with an engineering station. The engineering station connects to a local maintenance interface on the 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 gateway to configure it and troubleshoot certain problems.

Remote maintenance is done from the grid operator's offices, usually from secure locations close to the control centres. 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 gateways.

3.4 Gateway functions

For this security profile, the features of the gateway are restricted to the following gateway basic features:

Data acquisition, data concentrator and SCADA remote communication functions:

- The gateway can collect field data from IEDs in the process network and/or from I/O directly wired to its terminals with the objective to report to the SCADA system operational information.
- The gateway communicates with the SCADA system for reporting the acquired information and receiving control commands which are re-transmitted to the process.
- The gateway communicates with the central maintenance system to report electrical application maintenance information such as disturbance records or logs.

Configuration & maintenance functions:

- The gateway includes administration functions to configure settings of the gateway. Different administration interfaces are possible, such as:
    - Engineering station with dedicated software
    - Web servers

- APIs
- IEC 61850

Local and remote logging:

- The gateway supports the configuration of a local logging policy. It is possible to log security and administration events locally on gateway.
- The gateway supports the definition of a remote logging policy. It is possible to log security and administration events on a remote server.

3.5 Gateway users

The gateway users can:

- have different roles and objectives,
- be human beings interacting with the equipment, and/or
- digital entities performing automated tasks, such as other software or IEDs.

Engineers and infrastructure administrators (security administrators) from the grid operator staff or its contractors, are often responsible for the maintenance of the equipment. Someone working physically at a substation may have different roles, depending on the task to be executed.

Engineers are more often tasked with electrotechnical settings, such as the SCADA data model or other process details while Infrastructure administrators are more demanded for network settings and network maintenance aspects. Both users can perform equipment hardening activities.

3.5.1 Role-based access control according to IEC 62351-8

As introduced in the reference architecture in Figure 1, users are to be understood as human users or machine: SCADA, delimited (central) systems. Therefore, the users are naturally tied to a specific interface of the gateway.

The standard IEC 62351-8 has the scope to facilitate role-based access control (RBAC) for power system management. RBAC assigns human users, automated systems, and software applications to specified "roles", and restricts their access to only those resources, which the security policies identify as necessary for their roles.

IEC 62351-8 provides a flexible framework for the management of roles including customized, specific roles that individual utility operators may set up for their own particular use. However, due to the complexity and potentially far-reaching impact on grid operations, IEC 62351-8 has also defined a minimum set of “pre-defined roles “and associated permissions to enable proper operability.

The system-centric view of the present profile and the device-centric view of IEC 62351-8 pre-defined roles are in concordance. A standard-compliant implementation of IEC 62351-8 pre-defined roles covers the requirements of this profile.

Role	Role Description
OPERATOR	Is in charge to monitor and control electrical processes

INSTALLER	Is in charge to install and check network and electrical process digital equipment including Software/Firmware updates
ENGINEER	Is in charge to configure and maintain electrical process digital equipment settings and functions
SECAUD	Is in charge to monitor security audit logs
SECADM	Is in charge to configure and maintain network and cyber security settings e.g., subject to role assignments of electrical process digital equipment
RBACMNT	Is in charge of changing the role-to-right assignments.

Table 1 – Role description

3.5.2 User description and interfaces

Description of users, interacting with the gateway with:

- corresponding IEC 62351-8 role requirements
- respective interface for access reference.

Non-Human User	IEC 62351-8 Pre-Defined Role	Interface with gateway
SCADA system	OPERATOR	WAN
Central maintenance system	INSTALLER ENGINEER SECAUD (Security Audit, for audit logs) SECADM (Security Administrator) RBACMNT	WAN
Engineering station	ENGINEER	LAN

Table 2 - Machine Users list, role and required equipment access

Human User	IEC 62351-8 Pre-Defined Role	Interface with gateway
Engineer	ENGINEER	WAN LAN
Infrastructure administrator	INSTALLER SECAUD (for audit logs) SECADM (Security Administrator) RBACMNT	WAN LAN

Table 3 - Human Users list, role and required equipment access

4 Component threat analysis

The profile aims to deal with the baseline product family requirements here described. The product using the profile shall mitigate any additional risks associated to product features not evaluated by this profile and residual risks originated from the product implementation.

This chapter summarizes the results of a more comprehensive threat analysis that has been done to establish the security objectives and requirements of this security profile. For confidentiality purposes the full risk assessment is not included in this document.

4.1 Assets

The information assets processed by the gateway are the following:

ID	Assets
A1	**Remote monitoring and control information:** information sent to or received from the SCADA system, including: • measurements of electrical variables, such as voltages and currents • alarms indicating problems in the grid or at field locations • commands to control equipment in the substation, such as circuit breakers, disconnectors, and earthing switches The gateway receives measurements and alarms from the IEDs, and forwards commands to them.
A2	**Gateway configuration:** the configuration of the gateway, including the WAN network settings and the mapping between SCADA addresses and attached sensors and actuators.
A3	**Firmware and software:** the firmware and software installed on the gateway.
A4	**Operational logs:** logs on the gateway not related to security, such as logs of the commands sent, or the operating system logs.
A5	**Authentication information:** information such as passwords and keys that users use to authenticate to the component, or that the component uses to authenticate to other components or users.
A6	**Access control configuration:** information related to the access control of the component, including user accounts and the assignment of privileges.
A7	**Security logs:** logs of security events used to detect and analyse security incidents.

4.2 Threats

4.2.1 Threats agents

The threat analysis considers both external and internal threat actors.

Possible **external threat actors** could be ill intended people outside of the organization who want to capture data or take advantage and exploit a vulnerability.

Possible **insider threat actors** considered are malicious or non-malicious employees or contractors accidentally doing something harmful.

4.2.2 Threats to mitigate

The following threats are considered:

ID	Threats
	Unauthorized access threats
T1	**Unauthorized access as the SCADA system:** An attacker unauthorized access to the gateway as the SCADA system.
T2	**Unauthorized access to management functions:** An attacker gains to the gateway as the central maintenance system, an engineer, or an infrastructure administrator.
T3	**Exploit of a software vulnerability:** An attacker exploits a software vulnerability to gain, possibly privileged, access to the gateway.
T4	**Unauthorized physical access:** An attacker gains physical access to a substation and uses the physical access to gain logical access to the gateways. Attackers may log in on a local hardware port or physically tamper with the hardware.
	Communication threats
T5	**Data modification on the WAN network:** An attacker gains access to the WAN network and then modifies information sent between the gateway and the SCADA system or central maintenance system.
T6	**Data disclosure on the WAN network:** An attacker gains access to the WAN network and then eavesdrops on information sent between the gateway and the SCADA system or central maintenance system.
T7	**Network denial-of-service attack on the WAN network:** An attacker gains access to the WAN network and disrupts the normal operation of the substation, for instance by sending malformed messages or flooding the interface to the WAN network with data.
	Supply chain threats
T8	**Unauthorized software, firmware, or hardware modification at suppliers:** An attacker modifies software, firmware, or hardware at the supplier. This way, attackers may for instance install backdoors or logic bombs in the gateway.
T9	**Unauthorized software, firmware or hardware modification between the supplier and installation:** An attacker modifies software, firmware, or hardware after it leaves the supplier and before it is installed in the substation. This way, attackers may for instance install backdoors or logic bombs in the gateway.
	Insider threats
T10	**Harmful actions by engineers, infrastructure operators, or local operators:** An engineer, infrastructure administrator or local operator working at the grid operator or at a contractor and with authorized access, incidentally or on purpose, performs actions that are harmful to the gateway or the electricity grid.

Other threats	
T11	**Loss of configurations:** The configuration of the gateway is deleted or becomes corrupted through mistakes by engineers or infrastructure administrators or intentional actions from an attacker that has gained access.
T12	**Software or firmware corruption:** The software or firmware installed in the gateways is corrupted, for instance, by placing a backdoor or logic bomb in it, or simply making it unusable.

4.2.3 Effect of threats on assets

The matrix below shows if the threats in Section 4.2.2 can lead to a compromise of the confidentiality (C), integrity (I), or availability (A) of the assets in Section 4.1.

	A1 Remote monitoring and control information	A2 Gateway configuration	A3 Firmware and software	A4 Operational logs	A5 Authentication information	A6 Access control configuration	A7 Security logs
T1 Unauthorized access as the SCADA system	CIA						
T2 Unauthorized access to management functions	CIA	CIA	CIA	CIA	CIA	CIA	CIA
T3 Exploit of a software vulnerability	CIA	CIA	CIA	CIA	CIA	CIA	CIA
T4 Unauthorized physical access	CIA	CIA	CIA	CIA	CIA	CIA	CIA
T5 Data modification on the WAN network	I	I	I	I	I	I	I
T6 Data disclosure on the WAN network	C	C	C	C	C	C	C
T7 Network denial-of-service attack on the WAN network	A						
T8 Unauthorized software, firmware**,** or hardware modification at suppliers			I				
T9 Unauthorized software, firmware or hardware modification between the supplier and installation			I				
T10 Harmful actions by engineers, infrastructure operators, or local operators	CIA	CIA	CIA	CIA	CIA	CIA	CIA
T11 Loss of configurations		A					

T12 Software or firmware corruption			CIA				

4.3 Security objectives

This section identifies and defines the security objectives addressed by the gateway and by its operational environment, written in natural language.

The focus is on the technical security objectives to the gateway, and the processes that should be implemented by the users of the gateway in the operational environment to support these technical objectives. The technical objectives have been linked to the technological controls from ISO/IEC 27002:2022 and are numbered according to these controls. The technical objectives provide more details about how the ISO/IEC 27002 controls can be implemented for gateways in substation automation systems.

The objectives to the operational environment are provided as guidance to operators using the gateway. These objectives are **non-binding**. Besides implementing the processes listed below, users of the gateway are expected to have a cybersecurity management system as required by Article 32 of the NCCS. Within the management systems, it is recommended to implement the controls in Table 1 for the substations where the gateways are installed.

Table 1: Organizational, people, and physical controls from ISO/IEC 27002:2022 to be implemented in the operational environment.

Organizational controls	• 5.4 Management responsibilities • 5.9 Inventory of assets and other information • 5.15 Access control • 5.16 Identity management • 5.18 Access rights • 5.20 Addressing information security within supplier agreements • 5.21 Managing information security in the ICT supply chain • 5.25 Assessment and decision on information security events • 5.26 Response to information security incidents
People controls	• 6.1 Screening • 6.2 Terms and conditions of employment • 6.3 Information security awareness, education, and training • 6.4 Disciplinary process • 6.5 Responsibilities after termination or change of employment
Physical controls	• 7.1 Physical security perimeters • 7.2 Physical entry • 7.4 Physical security monitoring • 7.8 Equipment siting and protection • 7.8 Security of assets off-premises • 7.12 Cabling security

Figure 2 shows the expected zoning model in which the gateway is expected to be used.

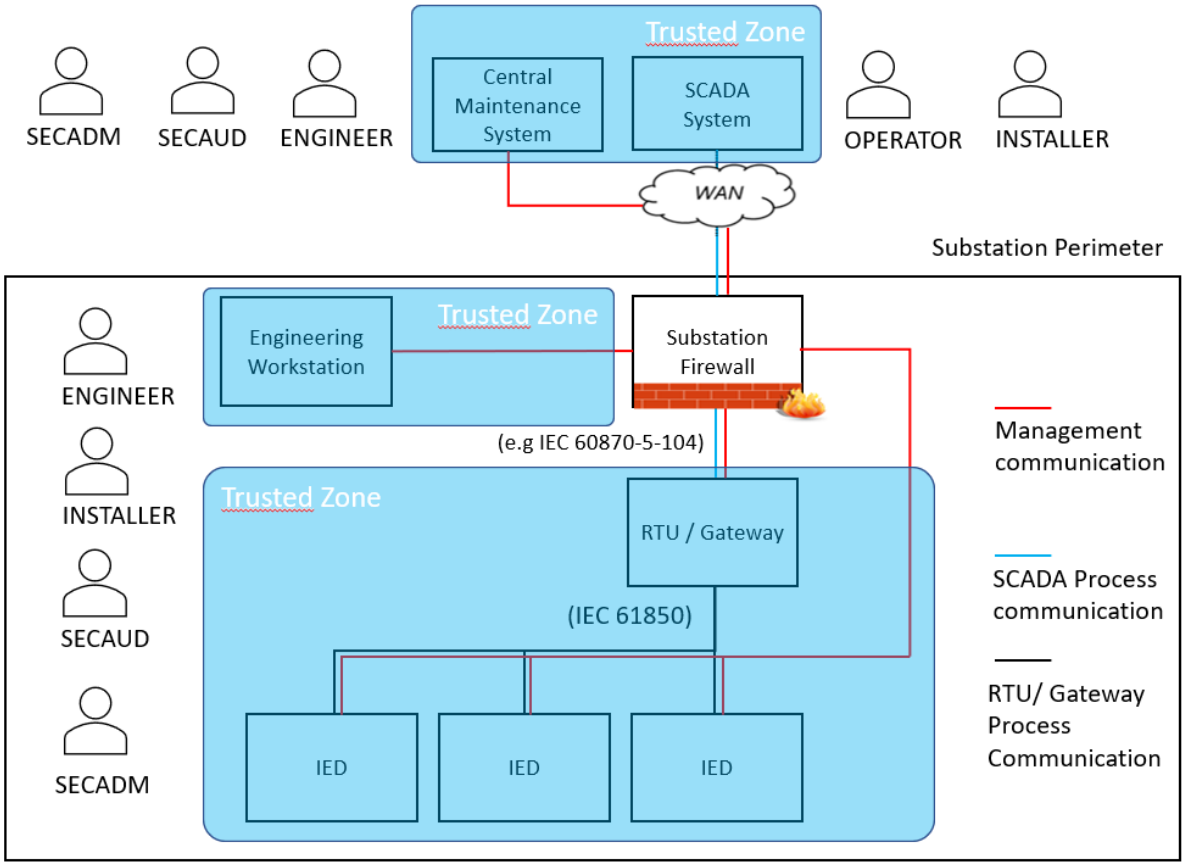

Figure 2: Zoning model for the gateway.

Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organizational security policies and assumptions.

[ISO/IEC 27002:2022] 8.3 Information access restriction

Component	**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 and infrastructure administrators: The device can enforce role-based access control for engineers and infrastructure administrators with individual user accounts managed through a central system.

[ISO/IEC 27002:2022] 8.5 Secure authentication

Component	**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 connecting through a trusted network connection, for instance by authenticating the identity of the VPN concentrator at the SCADA system. The device allows the SCADA system to verify the device's unique identity.

	8.5-CO2 Role-based authentication for the central maintenance system with unique device authentication: The central maintenance system identifies itself to the device with information that allows the device to determine its role. The device authenticates that the information on the system's role is correct and assigns the system 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 credentials for engineers and infrastructure administrators: The device can enforce mutual authentication for engineers and infrastructure administrators. They use individual credentials. The login procedure is protected against known attacks.

[ISO/IEC 27002:2022] 8.7 Protection against malware

Component	**8.7-CO1 Active malware protection on commercial off-the-shelf operating systems:** If the gateway uses a commercial off-the-shelf operating system, it can be actively protected against malware through, for instance, anti-virus software or application whitelisting software.

[ISO/IEC 27002:2022] 8.8 Management of technical vulnerabilities

Component	**8.8-CO1 Hardening:** Infrastructure administrators can harden the device both locally and through the central maintenance system. They can 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.
Operational environment	**8.8-EO3 Vulnerability management process:** The grid operator manages vulnerabilities in the substation automation system by: • disabling unused ports, services, user accounts and functions to reduce the likelihood of vulnerabilities • monitoring vulnerabilities in the system's software and firmware, assessing the risks of the vulnerabilities, and mitigating the high-risk vulnerabilities, for instance by applying security updates • limiting the impact of vulnerabilities by enabling the security features on the hardware and software platforms used

[ISO/IEC 27002:2022] 8.9 Configuration management

Component	**8.9-CO1: Restoration from configuration:** Infrastructure administrators can restore the device from a backed-up configuration both locally and through the central maintenance system.

[ISO/IEC 27002:2022] 8.13 Information backup

Operational environment	**8.13-EO3 Backup process for device configurations:** The grid operator has a process to back up the configurations of the device at their central maintenance system, and to create regular backups of this system. Older versions of the configurations are kept, so that it is possible to revert to them in case of issues.

[ISO/IEC 27002:2022] 8.15 Logging

Component	**8.15-CO1 Integration with SIEM system:** The device can log 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, so that they can be analysed to detect incidents.

[ISO/IEC 27002:2022] 8.16 Monitoring activities

Operational environment	**8.16-EO1 Security monitoring and incident response:** The grid operator monitors security events on the device and can respond to them. They gather security logs from devices centrally, for instance, in a SIEM. They establish procedures, use cases, and rules to find incidents in the logs. And they establish a process for responding to the incidents and minimizing the impact.

[ISO/IEC 27002:2022] 8.17 Clock synchronization

Component	**8.17-CO1 Clock synchronization:** The device supports synchronizing time with a central source to have reliable timestamps for security events.

[ISO/IEC 27002:2022] 8.19 Installation of software on operational systems

Component	**8.19-CO1 Software updates:** Infrastructure administrators can update the software and firmware on the device both locally and through the central maintenance system. The device checks the authenticity of firmware or software before installation through digital signatures.

[ISO/IEC 27002:2022] 8.20 Network security

Component	**8.20-CO1 Cryptographic protection of communication confidentiality and integrity on the WAN network:** The device can cryptographically protect the integrity and confidentiality of communication over the WAN network using cryptographic measures. The measures allow to verify the source of messages and protect against replay and man-in-the-middle attacks.

[ISO/IEC 27002:2022] 8.21 Security of network services

Operational environment	**8.21-EO1 Resilience against denial-of-service attacks on the WAN network:** The wide-area network (WAN) is resilient against accidental disruptions and against intentional denial-of-service attacks using simple means with low resources, generic skills, and low motivation (security level 2). The required service level is agreed with the telecom provider and is regularly monitored. The telecom provider monitors the network and can respond in case of an incident to minimize the impact of attacks.

[ISO/IEC 27002:2022] 8.22 Segregation of networks

Component	**8.22-CO1 Segregation of management and process communication:** The device can use separate networks for the management communication, SCADA process communication and gateway process communication. *Remark:* See Figure 2.
Operational environment	**8.22-EO1 Physical network segregation from the WAN network:** The substation networks are physically and logically segregated from the WAN network. Only normal connections are allowed through the perimeter to the WAN network. The communication load can be controlled at this perimeter. The networks inside the substation can work normally without a connection to the WAN network. *Remark:* Additional network segregation may be used within the substation, as indicated in Figure 2.
	8.22-EO4 No communication between substations on the WAN: There is no direct communication between substations on the WAN interface. The substations can communicate with the SCADA system and the central maintenance system.
	8.22-EO5 Logically separate networks on the WAN network: Network segregation is used on the WAN network to provide logically separate networks for at least: • Communication with the SCADA system • Remote access from engineers and infrastructure administrators • Other network services in the substation not connected to the substation automation system, such as camera and alarm systems, telephone systems, and enterprise IT access for engineers and infrastructure administrators • Connecting a network-based intrusion detection systems to a central management system (see 8.16-SO1) The segregation allows to prioritize communication with the SCADA system to ensure the required quality of service.

[ISO/IEC 27002:2022] 8.24 Use of cryptography

Component	**8.24-CO1 Key and password management:** Infrastructure administrators can update all passwords and keys used on the device both locally and through the central maintenance system. The update process protects the confidentiality and integrity of the keys.

Operational environment	**8.24-EO3 Key and password management process:** The grid operator manages the keys and passwords of the devices, so that they are properly protected and can be updated when needed.

4.3.1 Rationale

The table below shows which threats the objectives for the gateway mitigate.

Objective	Threats countered
8.3-CO1 Role separation for the SCADA and central maintenance system	• T1 Unauthorized access as the SCADA system
8.3-CO2 Centrally managed, role-based access control for engineers and infrastructure administrators	• T2 Unauthorized access to management functions • T10 Harmful actions by engineers, infrastructure administrators, or local operators
8.5-CO1 Network-based authentication for the SCADA system	• T1 Unauthorized access as the SCADA system
8.5-CO2 Role-based authentication for the central maintenance system with unique device authentication	• T2 Unauthorized access to management functions
8.5-CO3 Authentication with individual credentials for engineers and infrastructure administrators	• T2 Unauthorized access to management functions • T4 Unauthorized physical access
8.7-CO1 Active malware protection on commercial off-the-shelf operating systems	• T3 Exploit of a software vulnerability
8.8-CO1 Hardening	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions • T3 Exploit of a software vulnerability • T4 Unauthorized physical access
8.9-CO1: Restoration from configuration	• T11 Loss of configurations
8.15-CO1 Integration with SIEM system	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions • T3 Exploit of a software vulnerability • T4 Unauthorized physical access in a substation • T10 Harmful actions by engineers, infrastructure administrators, or local operators

	• T12 Software or firmware corruption
8.17-CO1 Clock synchronization	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions • T3 Exploit of a software vulnerability • T4 Unauthorized physical access in a substation • T10 Harmful actions by engineers, infrastructure administrators, or local operators • T12 Software or firmware corruption
8.19-CO1 Software updates	• T3 Exploit of a software vulnerability • T9 Unauthorized software, firmware or hardware modification between the supplier and installation • T12 Software or firmware corruption
8.20-CO1 Cryptographic protection of communication confidentiality and integrity on the WAN network	• T5 Data modification on the WAN network • T6 Data disclosure on the WAN network
8.22-CO1 Segregation of management and process communication	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions
8.24-CO1 Key and password management	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions • T4 Unauthorized physical access in a substation

The table below shows which threats the objectives for the operational environment mitigate.

Objective	Threats countered
Organizational controls (Table 1)	• T8 Unauthorized software, firmware or hardware modification at suppliers • T10 Harmful actions by engineers, infrastructure operators, or local operators
People controls (Table 1)	• T2 Unauthorized access to management functions • T10 Harmful actions by engineers, infrastructure operators, or local operators
Physical controls (Table 1)	• T4 Unauthorized physical access

8.8-EO3 Vulnerability management process	• T3 Exploit of a software vulnerability on the WAN interface
8.13-EO3 Backup process for device configurations	• T11 Loss of configurations
8.16-EO1 Security monitoring and incident response	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions • T4 Unauthorized physical access in a substation • T10 Harmful actions by engineers, infrastructure administrators, or local operators • T12 Software or firmware corruption
8.21-EO1 Resilience against denial-of-service attacks on the WAN network	• T7 Network denial-of-service attack on the WAN interface
8.22-EO1 Physical network segregation from the WAN network	• T7 Network denial-of-service attack on the WAN interface • T8 Unauthorized software, firmware or hardware modification at suppliers
8.22-EO4 No communication between substations on the WAN	• T4 Unauthorized physical access in a substation
8.22-EO5 Logically separate networks on the WAN network	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions
8.24-EO3 Key and password management process	• T1 Unauthorized access as the SCADA system • T2 Unauthorized access to management functions • T4 Unauthorized physical access in a substation

5 Component cybersecurity requirements

5.1 IEC 62443-4-1 security requirements and maturity level

The gateway manufacturer shall implement a secure software development lifecycle (SDL) process following IEC 62443-4-1, with at least a minimum maturity level 2 required. All requirements in this standard shall be implemented. For some of the requirements, contextualisations are given in the table below. Besides the contextualisations, the full text of the original requirements still applies.

Item	Subject	Contextualization
SM-12	Process verification	The supplier shall allow an independent third party to audit the secure development processes on behalf of the operator that is procuring the gateway. *Remark:* The developer may require a non-disclosure agreement when providing sensitive information, if it does not limit the audit.
SVV-4	Penetration testing	The supplier shall allow an independent third party to perform security tests on the gateway on behalf of the operator that is procuring the gateway. The supplier shall support the test by providing the relevant information and credentials. The supplier shall provide access to source code for code reviews if requested. *Remark:* The developer may require a non-disclosure agreement when providing sensitive information, if it does not prevent proper testing.
SUM-2	Security update documentation	For each firmware release, the supplier shall provide a software-bill-of-materials (SBOM) to the operator procuring the gateway.
SG-6	Account management guidelines	The supplier shall provide the credentials for all default accounts on the gateway.

5.2 IEC 62443-4-2 security requirements

IMPORTANT: Requirement specialization type and its selections (EDR, HDR,) must be observed in accordance with the gateway type of component.

Type of components	Requirement acronym	Corresponding 62443 requirement
Software application	SAR	Software application requirement
Embedded device	EDR	Embedded device requirement
Hosted device	HDR	Host device requirement
Network device	NDR	Network device requirement

The column ‘S/C’ indicates whether a requirement is selected (‘S’) or conditionally selected (‘C’) for the supplier to implement. The selected requirements in the chapter 5.2 are to be observed following the threat analysis described in chapter 4. The conditional requirements are to be applied when the condition listed in the column ‘Clarifications’ holds.

If the ‘S/C’ column is empty, the requirement was not selected for this profile. Suppliers may still implement the requirement, but it is not needed to comply with the profile.

Note: *The selected requirements are not legally required by the NCCS regulation. They would be contractually required to be implemented by the supplier if an entity uses this profile to procure substation gateway. The use of the profile in procurement is not required by the NCCS regulation. Use of the profile is only a recommendation.*

The requirements are organized according to the seven foundational requirements (FR) used in IEC 62443.

Some of the requirements have been contextualized and clarified for the specific application domain of substation automation systems to be able to meet the security objectives. Three types of contextualization and clarification have been added in the last three columns of the tables below:

- **Contextualization** further specifies how the requirement must be interpreted within the context of this profile for substation automation gateway. The contextualization must be followed to be compliant with the profile. Besides the contextualisations, the full text of the original requirements still applies.
- **Interoperability** details a recommended technical implementation choice to ensure interoperability on the context defined in the NCCS regulation. Usually, the recommendation refers to the IEC 62351 standards. The interoperability recommendations complement the IEC 62443 and do not have to be fulfilled to be compliant with the profile. Suppliers are however required to state if they have implemented the requirement according to the interoperability recommendation in the conformance statement in Annex A.
- **Implementation guidance** gives additional information and recommendation to profile users. The guidance does not have to be followed to be compliant with the profile.

5.2.1 FR 1: Identification and authentication control

Item	Sub item	Subject	SL	S/C	Contextualization	Interoperability	Implementation guidance
CR 1.1		Human user identification and authentication	1	S			
	RE (1)	Unique identification and authentication	2	S			
	RE (2)	Multifactor authentication for all interfaces	3				
CR 1.2		Software process and device identification and authentication	2	S	**[Authentication for the SCADA system]:** The component shall support identification and authentication based on the SCADA system's network location. The component shall be capable of using mutual authentication between itself and the SCADA application or a network device at the SCADA system. The component shall allow the SCADA system to uniquely identify and authenticate the component. **[Authentication for the central maintenance system]:** Components shall provide the capability to identify and authenticate the role of the central maintenance system.	**[IEC 62351-3 authentication using TLS]:** Components shall provide the capability to authenticate the SCADA system through the use of TLS with client-side certificates, as described in IEC 62351-3 [2]. The SCADA system shall be able to check that a connection comes from a unique component. The component shall be able to check that a connection comes from a unique software process in the SCADA system. **[Authentication using a VPN]:** Components shall provide the capability to authenticate the SCADA system through a VPN tunnel terminating at the component. The component shall be capable of using mutual authentication between itself and a firewall or VPN concentrator at the SCADA system and the SCADA system can uniquely identify and authenticate the component.	
	RE (1)	Unique identification and authentication	3				

CR 1.3		Account management	1	S	**[Centralized account management]:** Components shall provide the capability to be integrated into a central system for managing the accounts for engineers and infrastructure administrators used on the local maintenance interface. The component shall assign a role to each user based on information from the central system.	**[IEC 62351-8: PUSH model]:** Components shall provide the capability to be integrated into a central system for managing accounts for engineers and infrastructure administrators following the PUSH model from IEC 62351-8:2020. Components shall be conformant with the *"PUSH with LDAP over TLS"* access token distribution, as defined in Section 13.5 of IEC 62351-8:2020. For the access token format, components shall be conformant with Profile A (*"X.509 public key certificates with included role information"*) as defined in Section 13.3 of IEC 62351-8:2020. **[IEC 62351-8: PULL model]:** Components shall provide the capability to be integrated into a central system for managing accounts for engineers and infrastructure administrators following the PULL model from IEC 62351-8:2020. Components shall be conformant with the *"PULL with LDAP over TLS"* access token distribution, as defined in Section 13.5 of IEC 62351-8:2020. For the access token format, components shall be conformant with Profile A (*"X.509 public key certificates with included role information"*) as defined in Section 13.3 of IEC 62351-8:2020.	The requirement does not specify the technology to use for integrating into a central system for account management. Components may use any technology that meets the functional requirements, including RADIUS, LDAP, or Active Directory. To provide access when they cannot reach the central authentication server, components can for instance use local accounts. Strong passwords should be used for the local accounts to ensure they cannot be used to bypass authentication (as enabled by CR 1.5 and CR 1.7). Preferably, unique passwords are used in each substation or field location, and these are only given to engineers and infrastructure administrators when needed. When implementing the IEC 61351-8 push or pull method, components may support other access token formats and distribution methods besides those specified in the interoperability column.
CR 1.4		Identifier management	1	S			
CR 1.5		Authenticator management	1	S	**[Authenticator updates from the central maintenance system]:** Components shall provide the	**[Key updates following IEC 62351-9 using SCEP]:** For enrolment in a public key infrastructure, components	It is allowed that keys or credentials cannot be updated if they are only used for device internal purposes,

					capability to update all authenticators from the central maintenance system over the WAN interface. It shall be possible to update them without support from the supplier. [**Password storage]:** Components shall at least protect passwords from unauthorized disclosure when stored by storing them salted and hashed.	shall support the Simple Certificate Enrolment Protocol (SCEP) as described in Section 5.8.6 and 7.3.7 of IEC 62351-9:2023 [3] Components shall provide the capability to update all other authenticators from the central maintenance system over the WAN interface. It shall be possible to update them without support from the supplier **[Key updates following IEC 62351-9 using EST]:** For enrolment in a public key infrastructure, components shall support Enrolment over Secure Transport (EST) as described in Section 5.8.6 and 7.3.7 of IEC 62351-9:2023	such as encrypting local storage or setting up secure communication between processors on the same device. Allowing authenticators to be only updated through firmware updates does not meet the requirement, as preparing the firmware update would require support from the supplier. For storing passwords, it is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2. EST is recommended over SCEP for key updates, as it is the more modern protocol and is on a standards track with IETF.
	RE (1)	Hardware security for authenticators	3				
NDR 1.6		Wireless access management	1				
	RE (1)	Unique identification and authentication	2				
CR 1.7		Strength of password-based authentication	1	S			
	RE (1)	Password generation and lifetime restrictions for human users	3				
	RE (2)	Password lifetime restrictions for all users (human, software process, or device	4				
CR 1.8		Public key infrastructure certificates	2	C			*Condition:* When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the

							capability to interact and operate in accordance with IEC 62443-3-3 SR1.8. Note that in some member states the use of a PKI is mandatory.
CR 1.9		Strength of public key-based authentication	2	S			
	RE (1)	Hardware security for public key-based authentication	3				
CR 1.10		Authenticator feedback	1	S			
CR 1.11		Unsuccessful login attempts	1	S			
CR 1.12		System use notification	1	S			
NDR 1.13		Access via untrusted networks	1	S			
	RE (1)	Explicit access request approval	3				
CR 1.14		Strength of symmetric key-based authentication	2	S			
	RE (1)	Hardware security for symmetric key-based authentication	3				

5.2.2 FR 2: Use control

Item	Sub item	Subject	SL	S/C	Contextualization	Interoperability	Implementation guidance
CR 2.1		Authorization enforcement	1	S	**[Separation of roles]:** Components shall provide the capability to separate the following roles while implementing the principle of least privilege:		The roles and their access rights are described in Section 3.5. Components should allow access to the audit information and audit logs

					• The SCADA system • The central maintenance system • Engineers • Infrastructure operators Additionally, it shall be able to have separate roles for the SECADM and RBACMNT roles as defined in IEC 62351-8 [4].		to be restricted to privileged users, such as administrators.
	RE (1)	Authorization enforcement for all users (humans, software processes, and devices)	2	S			
	RE (2)	Permission mapping to roles	2				
	RE (3)	Supervisor override	3				
	RE (4)	Dual approval	4				
CR 2.2		Wireless use control	1				
CR 2.3		Use control for portable and mobile devices					
SAR 2.4 EDR 2.4 HDR 2.4 NDR 2.4		Mobile code	1	C			*Condition:* In the event that a component utilizes mobile code technologies, the component shall provide the capability to enforce a security policy for the usage of mobile code technologies.
	RE (1)	Mobile code authenticity check	2				
CR 2.5		Session lock	1	S			Session lock may not be desirable for some users, such as engineers performing local operation. The system should therefore allow administrators to disable session lock for specific users and interfaces.

CR 2.6		Remote session termination	2	S			
CR 2.7		Concurrent session control	3				
CR 2.8		Auditable events	1	S			Access control events should include at least: • Successful authentications • Failed authentication attempts • Changing user accounts • Changing authorizations Configuration change events should include: • Firmware uploads • Successful firmware updates • Failed firmware updates • Changing the system time • Changing keys or credentials • Failed attempt to change keys or credentials The component should also generate events for shutting down and booting the device.
CR 2.9		Audit storage capacity	1	S			
	RE (1)	Warn when audit record storage capacity threshold reached	3				
CR 2.10		Response to audit processing failures	1	S			
CR 2.11		Timestamps	1	S			
	RE (1)	Time synchronization	2	S			If PTP is used for time synchronization, it is recommended to use PTPVv2.1 (IEC 61588:2021 [5]), as it provides additional security

							features compared to previous versions.
	RE (2)	Protection of time source integrity	4	C			*Condition:* Integrity shall be protected if the time source is business critical.
CR 2.12		Non-repudiation	1	S			The requirement is considered fulfilled if the component logs the user identity of human users in the audit logs, as required by CR 2.8.
	RE (1)	Non-repudiation for all users	4				
EDR 2.13 HDR 2.13 NDR 2.13		Use of physical diagnostic and test interfaces	2				
	RE (1)	Active monitoring	3				

5.2.3 FR 3: System integrity

Item	Sub item	Subject	SL	S/C	Contextualization	Interoperability	Implementation guidance
CR 3.1		Communication integrity	1	S			
	RE (1)	Communication authentication	2	S	**[Authentication of WAN communication]:** Components shall provide the capability to verify the authenticity of information received over the WAN network using cryptographic methods. Inside substations, information in transit or at rest may be protected through network segregation, access control and physical protection. Cryptographic protection is not required for such information.	**[Authentication using TLS following IEC 62351-3]:** Components shall provide the capability to authenticate communication with the SCADA system through the use of TLS= as described in IEC 62351-3.	Conformance test cases for IEC 62351-3 are available in IEC 62351-100-3 [6].

SAR 3.2 EDR 3.2 HDR 3.2		Protection from malicious code	1	S			The suppliers should define and follow secure define best practices according to requirement SD-4 in IEC 62443-4-1. Whenever possible, the device should be delivered with security features from the underlying hardware and operating system enabled, or it should allow infrastructure administrators to enable them. 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) compiler options should be enabled to be able to use ASLR.
	RE (1)	Report version of code protection	2				
CR 3.3		Security functionality verification	1	S			The requirement is considered fulfilled if the component's documentation defines procedures or guidance on how users can verify its

							security functionality. The procedures may be manual. They could be provided as part of the hardening guidelines required by requirement SG-3 in IEC 62443-4-1.
	RE (1)	Security functionality verification during normal operation	4				
CR 3.4		Software and information integrity	1	S			• The requirement is considered fulfilled if the device checks the authenticity of the firmware before installation according to EDR 3.10 RE (1) Preferably, users should be able to verify the integrity of the installed software and firmware for instance by checking a hash value.
	RE (1)	Authenticity of software and information	2				
	RE (2)	Automated notification of integrity violations	3				
CR 3.5		Input validation	1	S			The requirement is considered fulfilled if the device has been tested for input validation vulnerabilities using all activities listed in requirement SVV-3 in IEC 62443-4-1.
CR 3.6		Deterministic output	1	C			*Condition:* When the device directly controls a process.
CR 3.7		Error handling	1	S			It is sufficient that error messages, including messages for failed login attempts, do not contain information useful for attackers.
CR 3.8		Session integrity	2	S			
CR 3.9		Protection of audit information	2	S			Audit information and audit logs should be persistent under reboots of the component and firmware updates.

							According to the access control policy access control policy in Section 3.5, it should be possible to restrict access to the audit information and audit logs to infrastructure administrators. See also CR 2.1.
	RE (1)	Audit records on write-once media	4				
EDR 3.10 HDR 3.10 NDR 3.10		Support for updates	1	S	**[Remote updates]:** The embedded device shall allow updates to be performed over the WAN interface by a centralized system and over the local maintenance interface by infrastructure operators. **[Future proof hardware]:** The embedded device shall have enough memory (RAM and flash) and computing power to allow security updates needed during its lifetime.		Compliance with the requirement can be shown through performance tests (see also requirement SVV-1 in IEC 62443-4-1). Tests with current firmware under operational workloads should show that there are enough reserves to extend security functions. Tests with algorithms recommended for future use 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.
	RE (1)	Update authenticity and integrity	2	S	**[Digitally signed firmware]:** Components shall validate the authenticity and integrity of any software or firmware update by validating a digital signature before installing it. The update shall be signed by the supplier. The signature shall protect the entire update.		It is not required that the integrity or authenticity of the firmware or software is validated during boot ("secure boot"). The embedded device should not allow the mechanisms that protect the authenticity and integrity of software updates to be bypassed through the recovery process, required by CR 7.4.
EDR 3.11 HDR 3.11 NDR 3.11		Physical tamper resistance and detection	2				

	RE (1)	Notification of a tampering attempt	3				
EDR 3.12 HDR 3.12 NDR 3.12		Provisioning product supplier roots of trust	2				
EDR 3.13 HDR 3.13 NDR 3.13		Provisioning asset owner roots of trust	2				
EDR 3.14 HDR 3.14 NDR 3.14		Integrity of the boot process	1	S			It is sufficient to verify the integrity of the firmware, software, and configuration data through a checksum (such as CRC) or error correcting code. It is not required that the component uses a cryptographic hash or checks the authenticity through a digital signature.
	RE (1)	Authenticity of the boot process	2				

5.2.4 FR 4: Data confidentiality

Item	Sub item	Subject	SL	S/C	Contextualization	Interoperability	Implementation guidance
CR 4.1		Information confidentiality	1	S	**[Encryption on WAN]** Components shall support the protection of the confidentiality of information in transit over the WAN network using encryption. Inside substations, information in transit or at rest may be protected through network segregation, access control and physical protection.	**[Encryption using TLS following IEC 62351-3]:** Components shall provide the capability to encrypt communication with the SCADA system through the use of TLS as described in IEC 62351-3.	

					Cryptographic protection is not required for such information.		
CR 4.2		Information persistence	2				
	RE (1)	Erase of shared memory resources	3				
	RE (2)	Erase verification	3				
CR 4.3		Use of cryptography	1	S			Guidance on cryptographic algorithms and key lengths is given in: • the ANSSI selection guide for cryptographic algorithms [7] and rules and recommendations on the choice and parameters of cryptographic algorithms [8]. • the BSI technical guideline Cryptographic Mechanisms: Recommendations and Key Lengths [9] • the ECCG – Agreed Cryptographic Mechanisms [10] • the NIST Recommendation for key management [11]. The latest version of these reports should be followed. Algorithms and key sizes should be used that are recommended for new systems at the time of deployment, and preferably also for the full lifetime of the product. A dedicated cryptographic (pseudo-)random number generator should be used to generate random numbers for all security functions.

							For storing passwords, it is recommended to use a hashing function that is resistant to GPU cracking attacks, such as Argon2 or PBKDF2.

5.2.5 FR 5: Restricted data flow

Item	Sub item	Subject	SL	S/C	Contextualization	Interoperability	Implementation guidance
CR 5.1		Network segmentation	1	S	**[Segregation of management and process communication]:** Components shall support segregating the management communication, SCADA process communication, and gateway process communication on different networks.		See Figure 2 for the different communication streams. The requirement is to support three different networks for the three streams. The networks may be supported by using different physical network interfaces or through the use of VLANs.
NDR 5.2		Zone boundary protection	1	S			
	RE (1)	Deny all, permit by exception	2				
	RE (2)	Island mode	3				
	RE (3)	Fail close	3				
NDR 5.3		General-purpose person-to-person communication restrictions	1				
CR 5.4		Application partitioning					*Note:* There is no component level requirement associated with IEC 62443-3-3 SR 5.4.

5.2.6 FR 6: Timely response to events

Item	Sub item	Subject	SL	S/C	Contextualization	Interoperability	Implementation guidance
CR 6.1		Audit log accessibility	1	S			

	RE (1)	Programmatic access to audit logs	3	S			Components should provide the capability to send the audit records using the syslog communication protocol in a commonly used format, so that they can be easily imported into a SIEM system without the need for a customized parser.
CR 6.2		Continuous monitoring	2				

5.2.7 FR 7: Resource availability

Item	Sub item	Subject	SL	S/C	Contextualization	Interoperability	Implementation guidance
CR 7.1		Denial of service protection	1	S			
	RE (1)	Manage communication load from component	2				
CR 7.2		Resource management	1	S			
CR 7.3		Control system backup	1	S			
	RE (1)	Backup integrity verification	2				
CR 7.4		Control system recovery and reconstitution	1	S			
CR 7.5		Emergency power					*Note:* There is no component level requirement associated with IEC 62443-3-3 SR 7.5.
CR 7.6		Network and security configuration settings	1	S			
	RE (1)	Machine-readable reporting of current security settings	3				
CR 7.7		Least functionality	1	S			
CR 7.8		Control system component inventory	2				

5.3 Rationale

The table below shows how the IEC 63442-4-2 requirements in Section 5.2 have been derived from the objectives for the gateway in Section 4.3.

Security objective	*IEC 62443-4-2 requirements*
8.3 Information access restriction	
8.3-CO1 Role separation for the SCADA and central maintenance system	• CR 2.1 Authorization enforcement • CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)
8.3-CO2 Centrally managed, role-based access control for engineers and infrastructure administrators	• CR 1.3 Account management • CR 1.4 Identifier management • CR 1.12 System use notification • CR 2.1 Authorization enforcement • CR 2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • CR 2.1 RE2 Permission mapping to roles
8.5 Secure authentication	
8.5-CO1 Network-based authentication for the SCADA system	• CR 1.2 Software process and device identification and authentication • CR 1.9 Strength of public key-based authentication • CR 1.14 Strength of symmetric key-based authentication • CR 4.3 Use of cryptography
8.5-CO2 Role-based authentication for the central maintenance system with unique device authentication	• CR 1.2 Software process and device identification and authentication • CR 1.9 Strength of public key-based authentication • CR 1.14 Strength of symmetric key-based authentication • CR 2.6 Remote session termination • CR 4.3 Use of cryptography
8.5-CO3 Authentication with individual credentials for engineers and infrastructure administrators	• CR 1.1 Human user identification and authentication • CR 1.1 RE1 Unique identification and authentication • CR 1.5 Authenticator management • CR 1.7 Strength of password-based authentication

	• CR 1.7 RE1 Password generation and lifetime restrictions for human users • CR 1.9 Strength of public key-based authentication • CR 1.10 Authenticator feedback • CR 1.11 Unsuccessful login attempts • CR 1.14 Strength of symmetric key-based authentication • CR 2.5 Session lock • CR 2.6 Remote session termination • CR 4.3 Use of cryptography
8.8 Management of technical vulnerabilities	
8.8-CO1 Hardening over the local maintenance or WAN interface	• CR 3.5 Input validation • CR 7.7 Least functionality • SAR, EDR, HDR 3.2 Protection from malicious code
8.9 Configuration management	
8.9-CO1 Restoration from configuration over the local maintenance or WAN interface	• CR 7.3 Control system backup • CR 7.4 Control system recovery and reconstitution • CR 7.6 Network and security configuration settings
8.15 Logging	
8.15-CO1 Integration with SIEM system	• CR 2.8 Auditable events • CR 2.9 Audit storage capacity • CR 2.10 Response to audit processing failures • CR 2.12 Non-repudiation • CR 3.7 Error handling • CR 3.9 Protection of audit information • CR 6.1 Audit log accessibility • CR 6.1 RE1 Programmatic access to audit logs
8.17 Clock synchronization	
8.17-CO1 Clock synchronization	• CR 2.11 Timestamps • CR 2.11 RE1 Time synchronization
8.19 Installation of software on operational systems	
8.19-CO1 Software updates over the local maintenance or WAN interface	• CR 1.8 Public key infrastructure certificates • CR 1.9 Strength of public key-based authentication • CR 4.3 Use of cryptography • SAR, EDR, HDR, NDR 2.4 Mobile code

	• CR 3.4 Software and information integrity • EDR, HDR, NDR 3.10 Support for updates • EDR, HDR, NDR 3.10 RE1 Update authenticity and integrity • EDR, HDR, NDR 3.14 Integrity of the boot process
8.20 Network security	
8.20-CO1 Cryptographic protection of communication confidentiality and integrity on the WAN interface	• CR 1.9 Strength of public key-based authentication • CR 1.14 Strength of symmetric key-based authentication • CR 3.1 Communication integrity • CR 3.1 RE1 Communication authentication • CR 3.6 Deterministic output • CR 3.8 Session integrity • CR 4.1 Information confidentiality • CR 4.3 Use of cryptography
8.22 Segregation of networks	
8.22-CO1 Segregation of management and process communication	• NDR 1.13 Access via untrusted networks • CR 5.1 Network segmentation • NDR 5.2 Zone boundary protection • CR 7.1 Denial of service protection • CR 7.2 Resource management •
8.24 Use of cryptography	
8.24-CO1 Key and password management over the local maintenance and WAN interface	• CR 1.5 Authenticator management • EDR 3.13 Provisioning asset owner roots of trust

6 Annex A: Conformance statement

Suppliers can use the following conformance statement to specify how they conform to the profile.

Selected / Optional	Profile requirement	Conformance response by vendor
	General	
S	Product is in conformance with NCCS security profile: • Conformance with IEC 62443-4-1 requirements in *Section 4.1 IEC 62443-4-1 security requirements and maturity level* • Conformance with IEC 62443-4-2 requirements in *section 4.2 IEC 62443-4-2 security requirements*	[Yes / No / Partial]
O	Does the product have a valid IEC 62443 certification available? If yes, please indicate where the certificate can be found?	[Yes / No / Partial]
	Contextualization	
S	CR 1.2: Authentication for the SCADA system	[Yes / No / Partial]
S	CR 1.2: Authentication for the central maintenance system	[Yes / No / Partial]
S	CR 1.3: Centralized account management	[Yes / No / Partial]
S	CR 1.5: Authenticator updates from the central maintenance system	[Yes / No / Partial]
S	CR 1.5: Password storage	[Yes / No / Partial]
S	CR 2.1: Separation of roles	[Yes / No / Partial]
S	CR 3.1 RE(1): Authentication of WAN communication	[Yes / No / Partial]
S	CR 4.1: Encryption on WAN	[Yes / No / Partial]
S	CR 5.1: Segregation of management and process communication	[Yes / No / Partial]
S	EDR / HDR / NDR 3.10: Remote updates	[Yes / No / Partial]
S	EDR / HDR / NDR 3.10: Future proof hardware	[Yes / No / Partial]
S	EDR / HDR / NDR 3.10 RE(1): Digitally signed firmware	[Yes / No / Partial]
	Interoperability using IEC 62351	
O	CR 1.2: IEC 62351-3 authentication using TLS	[Yes / No / Partial]
O	CR 1.2: Authentication using a VPN	[Yes / No / Partial]
O	CR 1.3: Centralized access control following IEC 62351-8 with the PUSH model	[Yes / No / Partial]
O	CR 1.3: Centralized access control following IEC 62351-8 with the PULL model	[Yes / No / Partial]
O	CR 1.5: Key updates following IEC 62351-9 using SCEP	[Yes / No / Partial]
O	CR 1.5: Key updates following IEC 62351-9 using the EST	[Yes / No / Partial]

O	CR 3.1 RE(1): Authentication using TLS following IEC 62351-3	[Yes / No / Partial]
O	CR 4.1: Encryption using TLS following IEC 62351-3	[Yes / No / Partial]

To be fully conformant with the profile, the supplier must be conformant with all requirements marked as selected in the first column. If a supplier is not compliant with a profile requirement, they should specify in the last column why they are not compliant. If suppliers are partially compliant with a profile requirement, they should further specify in the last column what parts of the requirement they have implemented, and why they have not implemented the other parts.

Entities may select which requirements they make select when they procure gateways. They do not have to include all selected requirements from the profile.

7 References

[1] IEC, “IEC TR 61850-90-2:2016 Communication networks and systems for power utility automation - Part 90-2: Using IEC 61850 for communication between substations and control centres,” 2016.

[2] IEC, “IEC 62351-3:2023 Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP,” 2023.

[3] IEC, “IEC 62351-9:2023 Power systems management and associated information exchange - Data and communications security - Part 9: Cyber security key management for power system equipment,” 2023.

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

[5] IEC , “IEC 61588:2021 Precision Clock Synchronization Protocol for Networked Measurement and Control Systems,” 2021.

[6] IEC, “IEC TS 62351-100-3:2020 Power systems management and associated information exchange - Data and communications security - Part 100-3: Conformance test cases for the IEC 62351-3, the secure communication extension for profiles including TCP/IP,” 2020.

[7] ANSSI, “ANSSI-PA-079: Guide de Sélection d'algorithmes cryptographiques,” 2021.

[8] ANSSI, “ANSSI-PG-083: Guide de mécanismes cryptographiques: Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques,” 2020.

[9] Federal Office for Information Security (BSI), “BSI - Technical Guideline TR-02101-1: Cryptographic Mechanisms: Recommendations and Key Lengths,” 2022.

[10] European Cybersecurity Certification Group - Sub-group on Cryptography, “Agreed Cryptographic Mechanisms,” 2025.

[11] National Institute for Standards and Technology, “NIST Special Publication 800-57 Part 1 Revision 5: Recommendation for Key Management: Part 1 - General,” 2020.

[12] IEC, “IEC62443-2-4: Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers,” 2015.

[13] IEC/ISA, IEC 62443-2-4: Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers, 2017.