SA-211-2022

Security requirements from IEC 62443 for substation automation systems

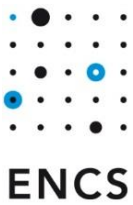
Version 2022v0.3

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 components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/resources/security-requirements/):

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	Versions	Description
14 July 2022	2022v0.1	Initial draft based on the security architecture SA-201-2022
19 August 2022	2022v0.2	Version with ISO 27002:2022 objectives
3 October 2022	2022v0.3	Added supplemental guidance for the requirements

Table of Contents

1 Introduction

This document gives technical security requirements for substation automation systems. Grid operators can use the requirements when procuring a new substation automation system from a system integrator, or internally when designing and implementing a substation automation system. The requirements are based on the IEC 62443-3-3 standard [1].

Substations are being more and more automated. Not only are they remotely monitored and controlled through a SCADA system. But local protection functions are also being implemented in software.

The automation means that cyber-attacks can have a large impact. Through remote switching, it is possible to create blackouts. Attacks that can disable the software protection functions can lead to permanent damage to transformers, lines, and busbars, and endanger the safety of engineers.

This document provides a recommended set of security requirements at system level that allows the major security threats to be mitigated with current technology. It provides guidance on what technical measures to take to secure substation automation systems.

The requirements are based on the IEC 62443 standard. They have been selected from part *IEC 62443-3-3: System security requirements and security* [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]).

When grid operators use the technical requirements in this document, it is recommended to also require that any software supplier complies full to **IEC 62443-4-1** [4] and any system integrator complies fully with **IEC 62443-2-4** [5] both at **maturity level at least 3**. Doing so, ensures that the supplier has secure development processes, so that it can correctly and consistently implement the requirements.

1.1 Relation to other documents

This document is part of a larger series on substation automation security, as shown in Figure 1. The series starts with a threat analysis [2] that determines security objectives to counter the threats posed to the assets in a typical substation 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 in this document.

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 [6]. They include organizational, people, physical, and technological objectives.

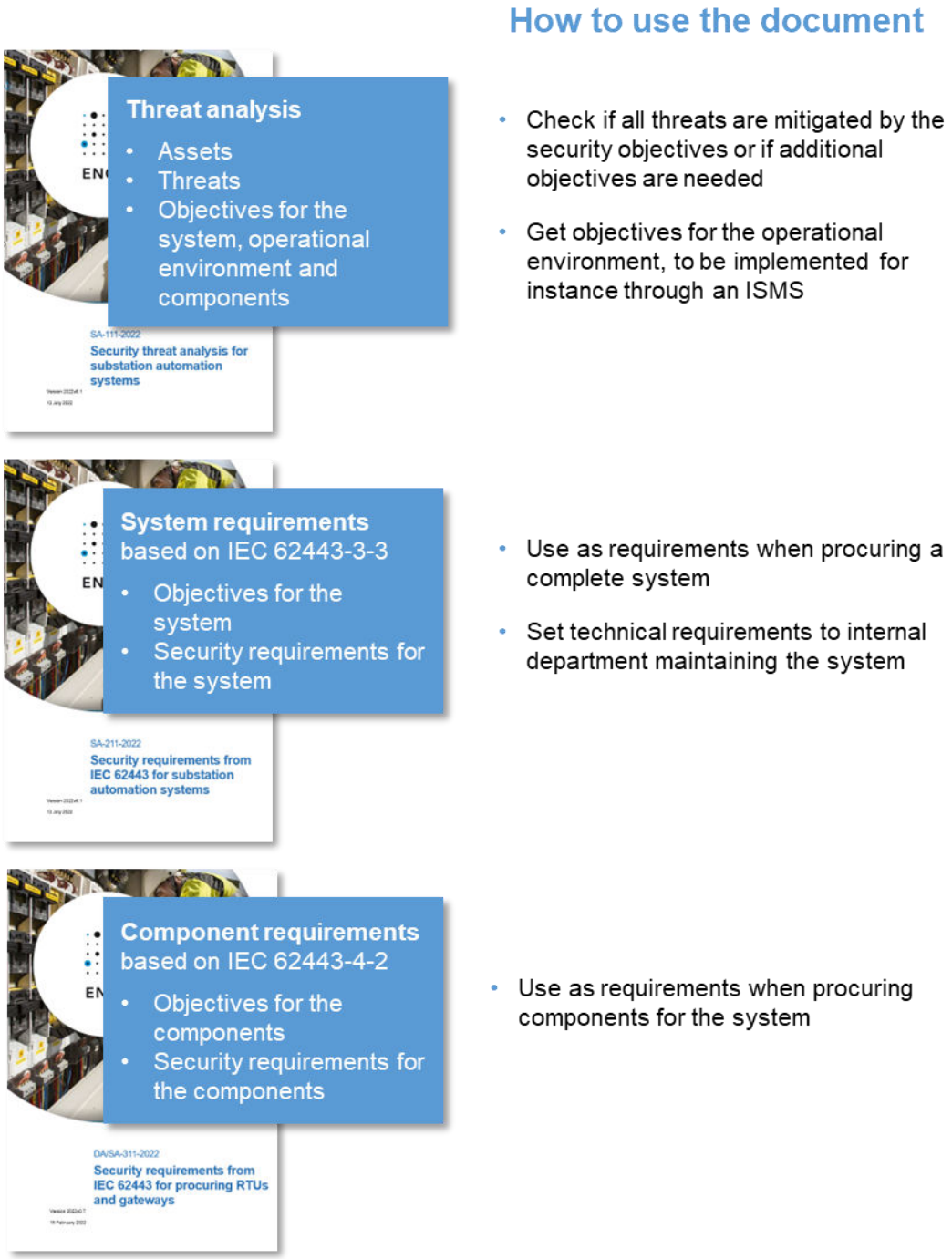


Figure 1: Relation between the different documents on substation automation security.

From the security objectives for the system, the component requirements document [7] derives security objectives for gateways. The objectives are chosen so that a gateway meeting the component objectives can be easily integrated into a system meeting the system objectives. Based on these component objectives, it selects security requirements for gateways from the IEC 62443-4-2 standards.

2 System description

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

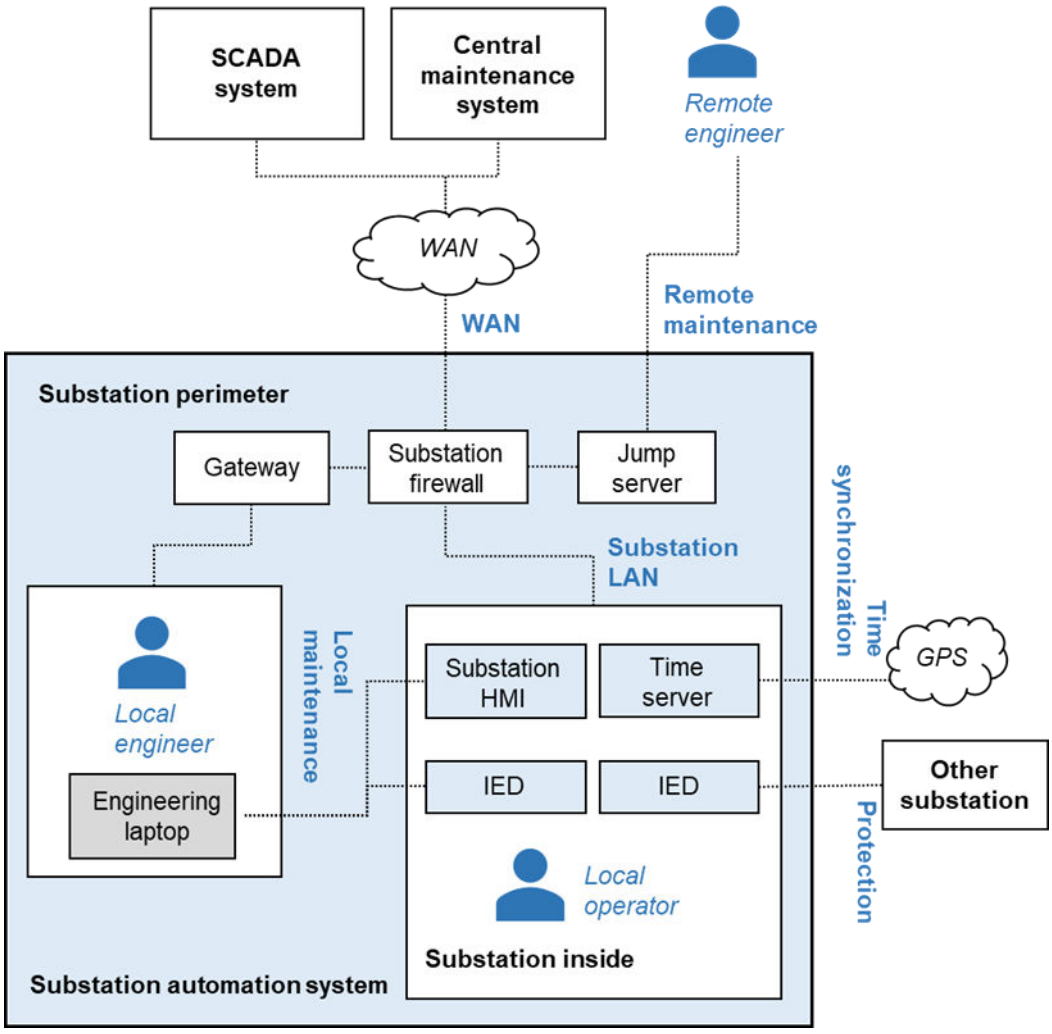


Figure 2: Reference architecture for the substation automation system, showing its users and interfaces. The requirements in this document concern the gateway.

2.1 Intended use of the system

The substation automation consists of the digital equipment in high-voltage substations that provide remote monitoring and control by the SCADA system, and local automation and protection. Figure 2 shows the reference architecture for substations automation systems used in this document.

High-voltage substations can be both transport stations at transmission system operators (TSOs) and high-to-medium voltage transformer substations at distribution system operators (DSOs). The type of equipment used is similar.

To provide remote monitoring and control, the substation automation system collects measurements on the state of the grid, such as voltage and currents. It sends these measurements to the SCADA system. The other way around, the SCADA system may send control commands, such as commands to control circuit breakers or disconnectors. The substation automation the enacts these commands in the substation.

Locally at the substation, the substation automation system provides automation and protection. For automaton, it may for instance control the voltage through a tap changer on a transformer without direct control for the SCADA system. Protection prevents faults in the grid causing damage to the primary equipment or accidents with personnel on the station. The substation automation is continuously monitoring for faults. It will quickly try to turn off power in case of a fault, while limiting the impact.

The substation may also be monitored and controlled locally by a local operator. Local operation may be used for instance during maintenance work or if there are connection problems with the SCADA system. Local operation is usually done from a central HMI in the substation. But it can also be done through the individual IEDs.

The substations are maintained by engineers. They configure the settings on the devices, can install software and firmware, and test if the devices are working properly. The same person working at substations may be both an engineer and a local operator.

This threat analysis makes as few assumptions as possible about the internal architecture of substations. Different grid operators use different designs and different naming for components. Moreover, the architectures can be expected to evolve in the coming years when more advanced features for the IEC 61850 standard are used. The threats and objectives in this analysis will only refer to the interfaces and users, not internal components. To make some of the implementation guidance more concrete, we may however sometimes refer to the components listed in Table 1.

Table 1: Components in the reference architecture.

Component name	Description
Substation firewall	The firewall, router, or modem that connects the substation to the WAN. Multiple firewalls may be used for redundancy.
Gateway	The device in the substation with which the SCADA front-end communicates. In modern substations, this is usually an IEC

	104 gateway or substation controller. In older substations, it is often called a Remote Terminal Unit (RTU). The gateway may communicate with hosts other than the SCADA front-end. It may, for instance, send disturbance recording data to analysis servers. There may also be more than one gateway for redundancy.
Substation HMI	A computer used for local monitoring and control within the substation. (Often runs Windows computer.)
IED	Intelligent Electronic Device: the devices connected to sensors and actuators. IEDs used for protection are sometimes called protection relays.
Engineering laptop	A laptop used by engineers to configure devices in the substation. It is often not a permanent part of the substation but only connected during installation and maintenance. The laptops can be connected directly using, for instance, a serial or USB connection or through the substation network. Sometimes special test equipment is also used in the same way to check IED configurations.
Jump server	Server or workstation used by engineers for remote maintenance. The engineer logs in remotely on the jump server (for instance with a remote desktop service) and from there access the local maintenance interfaces on substation equipment.
Time server	A server used to synchronize the time on all the devices in the substation. The time master function can also be implemented in the gateway or other components.

2.2 Intended operational environment

The substation is connected to several central systems at the grid operator: the SCADA system, the central maintenance system, and possibly remote engineers. It may also be connected to a time source and to other substations for protection functions. See the reference architecture Figure 2.

The SCADA system is used to remotely monitor and control the substation. It communicates with the substation using specialized protocols. Currently, IEC 60870-5-104 is most used. In the future, it is expected that MMS will be increasingly used according to the IEC 61850 standard. Communication is over a wide-area network (WAN), which in most cases will be a glass fiber network. Sometimes the grid operator owns the WAN network and sometimes they use an external service provider.

Maintenance can be done through a central maintenance system, by engineers locally in the substation, or by remote engineers. The central maintenance system consists of any systems used for remote maintenance. It can consist of specialized servers, such as element managers, but also workstations or laptops used remotely by engineers. Not all grid operators will have a central maintenance system. Some do all maintenance locally.

Engineers may locally maintain the equipment through the local maintenance interface. This interface is usually an Ethernet port or sometimes a serial or USB port. Local maintenance may also be done from internal substation networks or through the console of the HMI. The engineer connects a laptop to the local maintenance interface and can configure the equipment using specialized management software or a web interface

Some grid operators also allow engineers to remotely perform maintenance. In this analysis, we assume that engineers then first log in on a jump server in the substation perimeter. From the jump server, they may then log in on the substation equipment through internal substation networks and perform maintenance as if they are locally in the substation.

The time in the substation can be synchronized by the SCADA system over the WAN or over a separate time synchronization interface, such as GPS.

The substation may also communicate with other substations to implement distance and differential protection. These protection functions require IEDs at both ends of a power line to communicate with each other. Communication is usually done over point-to-point glass fiber connections. Specialized, often vendor proprietary protocols are used.

Physical security can differ greatly between substations. Grid operators may have hundreds of substations spread over a large area. Most of the time there will be no staff on the substations. Access to all substations will be restricted through fences or walls, and at least physical keys. More critical substations may be protected by camera or alarm systems and may use smart cards or biometrics for access controls. Sometimes the substation automation equipment is also protected by putting it in a cabinet with a lock or a door sensor.

2.3 Zoning model

In the reference architecture, the substation is divided into two zones:

- The **substation perimeter** consists of all components that can be reached from outside of the substation over the Wide Area Network (WAN). Usually, it consists of the substations firewall, gateways (or RTUs), and possibly a jump server for remote maintenance.
- The **substation inside** consists of all hosts that cannot be reached directly from the WAN. Usually, it consists of the substation HMI, time server, and IEDs.

The security architecture sets stronger security objectives for the substation perimeter than for the inside because the perimeter can be remotely attacked over the WAN. Such remote attacks could affect many substations at the same time. They can have a much larger impact than for instance physical attacks on one substation or attacks on neighboring substation through the protection interface.

The main differences in the security objectives are:

- The substation perimeter uses centralized role-based access control for engineers, while the substation inside may use local accounts.
- The substation perimeter allows keys and software to be updated remotely from a central system, while the substation inside uses local updates (possibly through a jump server).
- The substation perimeter protects communication on the WAN interface against eavesdropping, manipulation, and denial-of-service attacks. The substation inside does not protect communication on its interfaces.

The less stringent objectives for the substation inside are needed because a lot of substation equipment cannot meet the stricter objectives in the substation perimeter. Even modern equipment can often not meet the requirements on security updates.

The zoning model is designed to shield protection functions from attacks through the WAN. In most implementations, the shielding is achieved by putting the protection functions in the substation inside. But the architecture allows the functions to be in the substation perimeter if they are protected against denial-of-service attacks and if the remote software updates do not disrupt them.

2.4 Access control policy

To determine what access control measures have to be taken in each zone, we need to know the users of the zone. Table 2 and Table 3 list the users that are authorized to access the substation perimeter and the substation inside respectively, and the access they require. The last column gives the interfaces on which they access the system (see Figure 2).

Table 2: User groups on the substation perimeter zone.

User	Required access	Interface
SCADA system	• Collect electricity measurements • Send control commands	WAN
Central maintenance system	• Configure, maintain, and monitor the devices in the substation perimeter • Collect additional electricity data	WAN
Engineers	• Configure and maintain the substation equipment • Perform firmware and software updates	Remote maintenance Local maintenance

On the WAN there are two user groups accessing the substation automation system over the WAN: 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 substation automation system 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 system. The system should ensure that each system can only access the required functions.

On the local maintenance interface, the only user group are 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 system 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.

Table 3: User groups on the substation inside zone.

User	Required access	Interface
Gateway	• Collect electricity measurements • Send control commands	Substation LAN
IEDs at other substations	• Exchange measurements and alerts for distance and differential protection	Protection
Engineers	• Configure and maintain the substation equipment • Perform firmware and software updates	Local maintenance Substation LAN
Local operator	• Locally monitor and control the substation through the HMI	Substation HMI Local control on IEDs

We assume that a gateway in the substation perimeter accesses the devices in the substation inside to collect electricity measurements and send commands. Some architectures may use other devices in this role.

We call the interface on which the gateway accesses the inside the substation LAN interface. In practice, there could be multiple internal networks in the substation.

IEDs or protection relays at other substations may also communicate directly with devices in the substation inside for certain protection functions, such as distance and differential protection.

We assume that engineers maintain the equipment in the substation only through local connections. They can do this through a direct connection to the local maintenance interface on the devices, such as a serial or USB port or an Ethernet port dedicated to maintenance. They can also do this over the substation LAN, either by connecting a laptop or through a jump server in the substation perimeter.

Local operators can monitor the state of the grid and send control commands through a substation HMI, or by using controls on the IEDs themselves.

3 Security requirements for the substation perimeter

The threat assessment [2] sets security objectives to mitigate the threats to the substation automation system previously described. These objectives refine the technological security controls in ISO/IEC 27002:2022 [6]. We now break down the objectives into more detailed requirements from IEC 62443-3-3 [1] that a system integrator or department building or maintaining a substation automation system can follow (Table 4). See Section 3.1 for the full list of requirements.

Not all objectives can be fully covered through IEC 62443-3-3 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 3.2.

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** [4] and any system integrator complies fully with **IEC 62443-2-4** [5] both at **maturity level at least 3**.

Table 4: Selection of security requirements from IEC 62443-3-3 to meet the security objectives for the substation perimeter. Additional requirements not in IEC 62443-3-3 are given in italic.

Security Objective	***IEC 62443-3-3 requirements***
8.3 Information access restriction	
8.3-SO1 Role separation for the SCADA and central maintenance system: The substation perimeter enforces 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.	• SR2.1 Authorization enforcement • SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • *SR2.1 EE1 Role separation for the SCADA system and the central maintenance system*
8.3-SO2 Centrally managed, role-based access control for engineers: The substation perimeter enforces role-based access control for engineers with individual user accounts managed on a central server.	• SR1.3 Account management • SR1.3 RE1 Unified account management • *SR1.3 EE1 Centrally managed, role-based accounts* • SR1.4 Identifier management • SR2.1 Authorization enforcement

	• SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • SR2.1 RE2 Permission mapping to roles
8.5 Secure authentication	
8.5-SO1 Network-based authentication for the SCADA system: The substation perimeter enforces mutual authentication with the SCADA system at network level, for instance through a VPN. The perimeter verifies that the SCADA system is on a trusted network, while allowing SCADA system users to verify the unique identity of the substation.	• SR1.2 Software process and device identification and authentication • *SR1.2 EE2 Mutual identification and authentication for the SCADA system based on network location* • SR1.9 Strength of public key authentication • SR4.3 Use of cryptography • *SR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.5-SO2 Role-based authentication for the central maintenance system with unique device authentication: The central maintenance system identifies to the substation perimeter with information that allows the zone to determine its role. The zone authenticates the system's role and assigns it access rights based on the role. Devices in the zone uniquely identify themselves to the central maintenance system and allow the system to authenticate them.	• SR1.2 Software process and device identification and authentication • *SR1.2 EE1 Role-based identification and authentication for the central maintenance system* • SR1.9 Strength of public key authentication • SR2.6 Remote session termination • SR4.3 Use of cryptography • *SR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.5-SO3 Authentication with individual passwords for engineers: The substation perimeter enforces mutual authentication for engineers. Engineers use individual	• SR1.1 Human user identification and authentication • SR1.1 RE1 Unique identification and authentication • *SR1.5 EE1 Storing passwords*

passwords or keys. The login procedure is protected against known attacks	• SR1.7 Strength of password-based authentication • SR1.7 RE1 Password generation and lifetime restriction for human users • SR1.9 Strength of public key authentication • SR1.10 Authenticator feedback • SR1.11 Unsuccessful login attempts • SR2.5 Session lock • SR2.6 Remote session termination • SR4.3 Use of cryptography • *SR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.7 Protection against malware	
8.7-SO1 Active malware protection on commercial off-the-shelf operating systems: The commercial off-the-shelf operating systems in the substation perimeter are actively protected against malware through, for instance, anti-virus software or application whitelisting software.	• SR3.2 Malicious code protection
8.8 Management of technical vulnerabilities	
8.8-SO1 Remote hardening: Through remote access from the central maintenance system, the devices in the zone allow to remotely disable unneeded functions to reduce the likelihood of vulnerabilities and allow to enable security functions available on the hardware and software platforms to reduce their possible impact.	• SR7.7 Least functionality
8.9 Configuration management	

8.9-SO1 Remote configuration management: The devices in the substation perimeter can be restored from a backed-up configuration through remote access from the central maintenance system.	• SR7.3 Control system backup • SR7.4 Control system recovery and reconstitution • *SR7.4 EE1 Recovery from configuration file*
8.15 Logging	
8.15-SO1 Integration with SIEM system: The substation perimeter logs all relevant security events locally and sends selected events to a Security Information and Event Management (SIEM) system, so that they can be analyzed to detect incidents.	• SR2.8 Auditable events • SR2.8 RE1 Centrally managed, system-wide audit trail • SR2.9 Audit storage capacity • SR2.10 Response to audit processing failures • SR3.9 Protection of audit information • SR6.1 Audit log accessibility • SR6.1 RE1 Programmatic access to audit logs • *SR6.1 EE1 Programmatic access to audit logs through syslog*
8.17 Clock synchronization	
8.17-SO1 Clock synchronization for the perimeter: The substation perimeter synchronizes time with a central source to have reliable timestamps for security events.	• SR2.11 Timestamps • SR2.11 RE1 Internal time synchronization • SR2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
8.19-SO1 Remote software and firmware management: The software and firmware on devices in the substation perimeter can be updated through remote access from the central maintenance system. The devices check the authenticity of firmware or software through digital signatures.	• SR1.8 Strength of public key authentication • SR1.9 Strength of public key authentication • SR3.4 Software and information integrity • *SR3.10 EE1 Update capacity*

	• *SR3.10 EE3 Remote updates* • SR4.3 Use of cryptography • *SR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.19-SO2 Security updates without disrupting protection functions: The substation perimeter allows vulnerabilities on services exposed on the WAN interface to be fixed through security updates without disrupting protection functions in the substation.	• *SR3.10 EE3 Security updates for the substation perimeter without disrupting protection*
8.20 Network security	
8.20-SO1 Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces: The substation perimeter protects 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.	• SR1.9 Strength of public key authentication • SR3.1 Communication integrity • SR 3.1 RE1 Cryptographic integrity protection • SR3.8 Session integrity • SR4.1 Information confidentiality • SR4.1 RE1 Protection of confidentiality at rest or in transit via untrusted networks • SR4.1 RE2 Protection of confidentiality across zone boundaries
8.20-SO2 Resilience of protection functions against denial-of-service attacks on the WAN and remote maintenance interface: The substation perimeter shields protection functions from denial-of-service attacks on the WAN interface and remote maintenance interface, so that these functions keep working if the zone is flooded with data or receives malformed messages.	• SR7.1 Denial of service protection • SR7.1 RE1 Manage communication loads

8.22 Segregation of networks	
8.22-SO1 Network segregation on the WAN and remote maintenance interfaces: The substation perimeter is segregated from other zones on the WAN and remote maintenance interfaces. Only normal connections are allowed through the network perimeter.	• SR5.1 Network segmentation • SR5.1 RE1 Physical network segmentation • SR5.1 RE2 Independence from non-control networks • SR5.1 RE3 Logical and physical isolation of critical networks • SR5.2 Zone boundary protection • SR5.2 RE1 Deny by default, allow by exception
8.24 Use of cryptography	
8.24-SO1 Remote key and password management: All passwords and keys used in the substation perimeter can be updated through remote access from the central maintenance system.	• SR1.5 Authenticator management • *SR1.5 EE2 Remote authenticator update* • SR1.8 Public key infrastructure certificates • SR1.9 Strength of public key authentication • SR4.3 Use of cryptography • *SR4.3 EE1 Use of cryptography according to ECRYPT recommendations*

3.1 Requirements selected from IEC 62443-3-3

The table below lists the requirements selected from the IEC 62443-3-3 standard on *System security requirements and security levels* [1].

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
SR1.1	**Human user identification and authentication**	8.5-SO2

IEC	Name	Objective
		8.5-SO3
SR1.1 RE 1	**Unique identification and authentication**	8.5-SO3
SR1.2	**Software process and device identification and authentication** *Supplemental guidance:* When validating a certificate, the identity of the user can be checked through the subject name, common name, or distinguished name. The role could be checked through the attribute certificates described in IEC 62351-8 [8].	8.5-SO1 8.5-SO2
SR1.2 EE1	**Role-based identification and authentication for the central maintenance system with unique device authentication** The control system shall provide the capability to identify and authenticate the role of the central maintenance system. This capability shall enforce such identification and authentication on all interfaces which provide access to the components to support least privilege in accordance with applicable security policies and procedures. Devices in the control system uniquely identify themselves to the central maintenance system and allow the system to authenticate them.	8.5-SO2
SR1.2 EE2	**Mutual identification and authentication for the SCADA system based on network location** The control system shall provide the capability to provide authentication for the SCADA system through one of the following options: A. Based on their 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	8.5-SO1

IEC	Name	Objective
	central 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.	
SR1.3	**Account management**	8.3-SO2
SR1.3 RE1	**Unified account management**	8.3-SO2
SR1.3 EE1	**Centrally managed, role-based accounts** The control system shall provide the capability to be integrated into a central system for managing the accounts for engineers. The component shall assign an account to a role based on information from the central system. The control system shall provide a way for human users to access it when the device cannot reach the central system. *Supplemental guidance:* Substation equipment can check an engineer's access rights using different technologies. Grid operators should choose a method that works with their existing systems. It is recommended to use authentication method that does not give credentials to the field device in a reusable form (see [9]), such as certificated-based authentication using the PUSH method described in IEC 62351-8 [8] or RADIUS with the EAP-TLS or EAP-TTLS methods. When local accounts are used as a fallback, strong passwords should be used to ensure they cannot be exploited to bypass authentication. Preferably,	8.3-SO2

IEC	Name	Objective
	unique passwords are used in each substation, and these are only given to engineers when needed.	
SR1.4	**Identifier management**	8.3-SO2
SR1.5	**Authenticator management**	8.24-SO1
SR1.5 EE1	**Storing passwords** The control system shall provide the capability to store passwords salted and hashed. *Supplemental guidance:* It is recommended to use a password hashing function that is resistant against GPU cracking attacks, such as Argon2 or PBKDF2. Users should be able to change their own passwords through the central maintenance system or through the access control server.	8.5-SO3
SR1.5 EE2	**Remote authenticator update** The control system shall provide the capability to remotely update all authenticators from the central maintenance system in a way that protects their confidentiality and integrity.	8.24-SO1
SR1.7	**Strength of password-based authentication**	8.5-SO3
SR1.7 RE1	**Password generation and lifetime restriction for human users**	8.5-SO3
SR1.8	**Public key infrastructure certificates**	8.19-SO1 8.24-SO1 8.24-SO2
SR1.9	**Strength of public key authentication**	8.5-SO1 8.5-SO2

IEC	Name	Objective
		8.5-SO3 8.19-SO1 8.20-SO1 8.24-SO1 8.24-SO2
SR1.10	**Authenticator feedback**	8.5-SO3
SR1.11	**Unsuccessful login attempts**	8.5-SO3
SR2.1	**Authorization enforcement**	8.3-SO1 8.3-SO2
SR2.1 RE1	**Authorization enforcement for all users**	8.3-SO1 8.3-SO2
SR2.1 RE2	**Permission mapping to roles**	8.3-SO2
SR2.1 EE1	**Role separation for the SCADA system and the central maintenance system** The control system 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-SO1
SR2.5	**Session lock**	8.5-SO3
SR2.6	**Remote session termination**	8.5-SO2 8.5-SO3
SR2.8	**Auditable events**	8.15-SO1

IEC	Name	Objective
SR2.8 RE 1	**Centrally managed, system-wide audit trail**	8.15-SO1
SR2.9	**Audit storage capacity**	8.15-SO1
SR2.10	**Response to audit processing failures**	8.15-SO1
SR2.11	**Timestamps**	8.17-SO1
SR2.11 RE1	**Internal time synchronization**	8.17-SO1
SR2.11 RE2	**Protection of time source integrity**	8.17-SO1
SR3.1	**Communication integrity**	8.20-SO1
SR3.1 RE1	**Cryptographic integrity protection** *Supplemental guidance:* The cryptographic measures on the WAN can be taken at different network layers: at the telecom layer, through a VPN, through TLS (as specified in IEC 62351-3 **Invalid source specified.** and IEC 60870-5-7 **Invalid source specified.**), or through application layer protection. If measures on the telecom layer are used, care should be taken to avoid known vulnerabilities in some wireless protocols.	8.20-SO1
SR3.2	**Malicious code protection**	8.7-SO1
SR 3.4	**Software and information integrity** *Restriction:* The control systems shall have the capability to protect the authenticity of firmware through digital signatures. Devices shall check the firmware signature before installation.	8.19-SO1
SR 3.8	**Session integrity**	8.20-SO1

IEC	Name	Objective
SR 3.9	**Protection of audit information**	8.15-SO1
SR3.10 EE1	**Update capacity** The devices in the control system shall have enough memory (RAM and flash) and computing power to allow security updates needed during their lifetime.	8.19-SO1
SR3.10 EE3	**Remote updates** The devices in the control system shall allow the updates to be performed remotely from a centralized system.	8.19-SO1
SR3.10 EE4	**Security updates for the substation perimeter without disrupting protection** Equipment in the substation perimeter allows vulnerabilities on services exposed on the WAN interface to be fixed through security updates without disrupting the protection functions. *Supplemental guidance:* The most direct way to avoid the risk of disruptions is to only run protection functions on devices in the substation inside, such as IEDs (see also S.12.9.1). The substation perimeter equipment is then only responsible for communication to the central system and can be updated with much less risk.	8.19-SO2
SR 4.1	**Information confidentiality**	8.20-SO1
SR 4.1 RE1	**Protection of confidentiality at rest or in transit via untrusted networks**	8.20-SO1
SR 4.1 RE2	**Protection of confidentiality across zone boundaries**	8.20-SO1
SR 4.3	**Use of cryptography**	8.5-SO1

IEC	Name	Objective
		8.5-SO2 8.19-SO1 8.24-SO1 8.24-SO2
SR4.3 EE1	**Use of cryptography according to ECRYPT recommendations** The control system shall follow the recommendations in the ECRYPT – Algorithms, Key Size, and Protocols Report [10]. In particular: • It only uses the cryptographic algorithms that the ECRYPT recommends as suitable for new or future systems. • It uses keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in the ECRYPT report). • It only uses 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-SO1 8.5-SO2 8.19-SO1 8.24-SO1 8.24-SO2
SR5.1	**Network segmentation**	8.22-SO1
SR5.1 RE1	**Physical network segmentation**	8.22-SO1
SR5.1 RE2	**Independence from non-control system networks**	8.22-SO1
SR5.1 RE3	**Logical and physical isolation of critical networks**	8.22-SO1
SR 5.2	**Zone boundary protection** *Supplemental guidance:* The zone boundary protection may be applied by a firewall, router, glass	8.22-SO1

IEC	Name	Objective
	fiber modem, layer 3 switch or any other network device with the necessary capabilities.	
SR 5.2 RE 1	**Deny by default, allow by exception** *Supplemental guidance:* The firewalls should usually apply the following restrictions on the WAN interface: • The SCADA system only accesses SCADA services (such as IEC 60870-5-104 and IEC 61850 MMS) on the gateway. • The central maintenance system only accesses the jump server (S.13.1.6) and maintenance services on equipment in the substation perimeter.	8.22-SO1
SR 6.1	**Audit log accessibility**	8.15-SO1
SR 6.1 RE 1	**Programmatic access to audit logs**	8.15-SO1
SR6.1 EE1	**Programmatic access to audit logs through syslog** The control system 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-SO1
SR 7.1	**Denial of service protection** *Supplemental guidance:* In the degraded mode, at least the protection functions should continue to work properly. The most reliable way to shield the protection functions is to only run them on equipment in the substation inside. So, the protection functions would for instance only run on IEDs in the substation inside that communicate to the SCADA system through a gateway in the substation perimeter.	8.20-SO2

IEC	Name	Objective
	Even when IEC 61850 is used between the SCADA system and substations, it is recommended to use a gateway or proxy. Following the IEC 61850-90 standard, the SCADA system can communicate to the substation using IEC 61850. Doing so, reduces the burden of data engineering. The SCADA system could then also directly access IEDs. But direct access creates a risk of denial-of-service attacks on protection functions, especially because it is still tricky to apply security patches to IEDs. Protection functions can be run on equipment in the substation perimeter if the equipment segregates them internally from communication functions. Such internal segregation is more complex and should be thoroughly tested.	
SR 7.1 RE1	**Manage communication loads**	8.20-SO2
SR 7.3	**Control system backup**	8.9-SO1
SR 7.4	**Control system recovery and reconstitution**	8.9-SO1
SR7.4 EE1	**Recovery from configuration file** The control system shall provide the capability to be recovered from a from a backup configuration file.	8.9-SO1
SR 7.7	**Least functionality**	8.8-SO1

3.2 Rationale for the requirements

Below a rationale is provided for the requirements selected in Section 3.1 by showing that they cover the security objectives for the substation perimeter (Table 4).

8.3-SO1 Role separation for the SCADA and central maintenance system

General authorization for software process users is covered by *SR2.1* and *SR2.1 RE1.* The additional requirement *SR2.1 EE1* ensure separate roles for the SCADA and central

maintenance systems. 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-SO2 Centrally managed, role-based access control for engineers

Authorization is covered by *SR2.1* and *SR2.1 RE1,* and *SR2.1 RE2*. Account management is covered by requirements *SR1.3* and *SR1.4*. SR1.3 RE1 and the additional requirement *SR1.3 EE1* are needed to ensure that the accounts can be centrally managed, as requirement *SR1.3* also allows them to be managed on the device.

8.5-SO1 Network-based authentication for the SCADA system

Authentication is covered by requirement *SR1.2* with the additional requirement *SR1.2 EE2*. The additional requirement is needed to provide mutual authentication. Requirement *SR1.2* would only cover authentication from the device to the SCADA system.

Strong cryptographic keys and algorithms for the authentication are ensured by requirements SR1.9 and SR4.3. The additional requirement SR4.3 EE1 is included to further specify which recommendations on cryptography to follow.

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

8.5-SO2 Role-based authentication for the central maintenance system

Authentication is covered by requirement *SR1.2* with the additional requirement *SR1.2 EE1* to ensure mutual authentication, and *SR1.1* with the additional requirement *SR1.1 EE1* for human users. Strong cryptographic keys and algorithms for the authentication are ensured by requirements *SR1.9* and *SR4.3* with the additional requirement *SR4.3 EE1*. Remote session termination (*SR2.6*) is included to reduce the risk that authentication is bypassed by compromising a session.

8.5-SO3 Authentication with individual passwords for engineers

Authentication with individual user accounts and passwords is ensured by requirements *SR1.1* and *SR1.1 RE1*.

The login procedure is protected against known attacks as follows. Against brute-force attempts, requirement *SR1.11* ensures access can be blocked after several unsuccessful login attempts and requirement *SR1.10* ensures no information is leaked during the authentication process, while *SR1.7* and *SR1.7 RE1* allow enforcing secure passwords. Requirement *SR1.7 RE1* protects against passwords leaking by allowing to limit their lifetime. Requirement *SR1.5 EE1* protects against attacker getting passwords from a compromised device by salting and hashing them. Requirements *SR2.5* and *SR2.6*

protect against hijacking a user's session. And requirements *SR1.9*, *SR4.3*, *SR4.3 EE1* protect against cryptographic attacks.

8.7-SO1 Active malware protection on commercial off-the-shelf operating systems

Requirement *SR3.2* ensures the protection against malicious code.

8.8-SO1 Remote hardening

Disabling unneeded functions is covered by requirement *SR 7.7.*

8.9-SO1 Remote configuration management

Restoration from a backed-up configuration is covered by requirement *SR 7.3*, *SR 7.4,* and additional requirement *SR7.4 EE1*.

8.15-SO1 Integration with SIEM system

Logging security events is covered by requirement *SR2.8* and *SR2.8 RE1* covers the central management of the logs. Sending the logs to the SIEM system is covered by requirements *SR6.1* and *SR6.1 RE1*. The additional requirement *SR6.1 EE1* 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 *SR2.10* and *SR3.9*. Requirement *SR2.9* ensures that there is enough storage capacity on the device for the logs.

8.17-SO1 Clock synchronization for the perimeter

Time synchronization is covered by requirements *SR2.11* and *SR2.11 RE1*. Requirement *SR2.11 RE2* ensures that the integrity of the time source is protected.

8.19-SO1 Remote software and firmware management

Remote updates of software and firmware are covered by *SR3.10 EE3*, while *SR3.10 EE1* ensures there is enough memory and computing power for future updates.

Integrity of software and firmware are covered by *SR3.4*. Requirement *SR1.8* ensures that the system can be integrated into a PKI for the certificates needed to verify the signature. Requirements *SR1.9*, *SR4.3*, and *SR4.3 EE1* ensure the strength of the cryptography used for the signatures.

8.19-SO2 Security updates without disrupting protection functions

The objectives are covered by the additional requirement SR3.10 EE1.

8.20-SO1 Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces

Protecting the confidentiality of the information is covered by requirement *SR4.1, SR4.1 RE1, and SR4.1 RE2*. Integrity of the communication is covered by *SR3.1*, *SR3.1 RE1*, and *SR 3.8*. Requirements *SR 1.9*, *SR4.3*, and *SR 4.3 EE1* ensure that strong cryptography is used to protect the communication.

8.20-SO2 Resilience of protection functions against denial-of-service attacks on the WAN and remote maintenance interface

Protection against denial-of-service attacks on the WAN are achieved by requirements *SR7.1* and *SR7.1 RE1*.

8.22-SO1 Network segregation on the WAN and remote maintenance interfaces

Network segregations is ensured by requirement *SR5.1*. As the substation networks are highly critically, they should be physically segregated (*SR5.1 RE1*), be independent of non-control system network (*SR5.1 RE2*) and allow the substation to be isolated from non-critical networks (*SR5.1 RE3*).

Requirements *SR5.2* and *SR5.2 RE1* ensure that there is protection between different security zones, and only allowed traffic can go through.

8.24-SO1 Remote key and password management

Remote updates of keys and credentials are covered by requirements *SR1.5* and *SR1.5 EE2*. Requirement *SR1.8* allows a root certificate from the grid operator to be installed, so that it can be integrated in their PKI. Requirements *SR1.9*, *SR4.3*, and *SR4.3 EE1* ensure the strength of the cryptography used for the certificates.

4 Security requirements for the substation inside

After the requirements for the substation perimeter, we now select requirements from IEC 62443-3-3 [1] to meet the security objectives for the substation inside, as set in the threat assessment [2]. The approach is the same as for the substation perimeter in Section 3. We give the list of requirements from IEC 62443-3-3 with the additional requirements that are needed (Section 4.1), and then a rationale for selecting the requirements (Section 4.2).

Table 5: Selection of security requirements from IEC 62443-3-3 to meet the security objectives for the substation inside. Additional requirements not in IEC 62443-3-3 are given in italic.

Objective	***Threats countered***
8.3 Information access restriction	
8.3-SO3 Role separation for engineers and local operators: The substation inside enforces access control with separate roles engineers and operators, so that each user can only access the functions they need for their role.	• SR1.3 Account management • SR2.1 Authorization enforcement • SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices) • *SR2.1 EE1 Role separation for engineers and local operators*
8.3-SO4 Least privileges on the substation LAN, time synchronization, and protection interfaces: The substation inside enforces access rights on the substation LAN, time synchronization, and protection interfaces, so that users on the interfaces can only access the functions they need. Users on the interfaces do not have to authenticate themselves, unless required by another objective. Functions that are only needed by users that do authenticate themselves, are only available after authentication.	• SR2.1 Authorization enforcement • SR2.1 RE1 Authorization enforcement for all users (humans, software processes and devices)

8.5 Secure authentication	
8.5-SO4 Role-based authentication by role for engineers and local operators: The engineers and operators identify to the zone with information that allows the zone to determine their role. The zone authenticates the user's role and assigns them access rights based on the role.	• SR1.1 Human user identification and authentication • *SR1.1 EE1 Role identification and authentications for human users* • *SR1.5 EE1 Storing passwords* • SR1.9 Strength of public key authentication • SR2.6 Remote session termination • SR4.3 Use of cryptography • *SR4.3 EE1 Use of cryptography according to ECRYPT recommendations*
8.8 Management of technical vulnerabilities	
8.8-SO2 Local hardening: The devices in the zone allow to remotely or locally disable unneeded functions to reduce the likelihood of vulnerabilities and enable security functions available on the hardware and software platforms to reduce their possible impact.	• SR7.7 Least functionality
8.9 Configuration management	
8.9-SO2 Local configuration management: Through local access devices in the substation inside allow to restore the device from a backed-up configuration.	• SR7.3 Control system backup • SR7.4 Control system recovery and reconstitution
8.15 Logging	
8.15-SO2 Collecting security events from the substation inside through the perimeter: The substation perimeter logs all relevant security events locally and sends selected events to the substation perimeter,	• SR2.8 Auditable events • SR2.9 Audit storage capacity • SR2.10 Response to audit processing failures

so that they can be analyzed to detect incidents.	• SR3.9 Protection of audit information • SR6.1 Audit log accessibility • SR6.1 RE1 Programmatic access to audit logs
8.17 Clock synchronization	
8.17-SO2 Clock synchronization for the perimeter: The substation inside synchronizes time with a central source to have reliable timestamps for security events.	• SR2.11 Timestamps • SR2.11 RE1 Internal time synchronization • SR2.11 RE2 Protection of time source integrity
8.19 Installation of software on operational systems	
8.19-SO3 Local software and firmware management: Through local access devices in the substation inside allow to update their software or firmware.	• *SR3.10 EE1 Update capacity* • *SR3.10 EE2 Local updates*
8.22 Segregation of networks	
8.22-SO2 Network segregation on the substation LAN interface: The substation inside is segregated from other zones on the substation LAN interface. Only normal connections are allowed through the network perimeter.	• SR5.1 Network segmentation • SR5.1 RE1 Physical network segmentation • SR5.1 RE2 Independence from non-control networks • SR5.1 RE3 Logical and physical isolation of critical networks • SR5.2 Zone boundary protection • SR5.2 RE1 Deny by default, allow by exception
8.22-SO3 Remote management through a jump host: If remote maintenance to equipment in the substation inside is allowed, it is performed through a jump host in the substation perimeter.	• *SR5.1 EE1 Remote maintenance through a jump host*

8.24 Use of cryptography	
8.24-SO2 Local key and password management: Through local access devices in the substation inside allow to update all passwords and keys.	• SR1.5 Authenticator management • SR1.8 Public key infrastructure certificates • SR1.9 Strength of public key authentication • SR4.3 Use of cryptography • *SR4.3 EE1 Use of cryptography according to ECRYPT recommendations*

4.1 Requirements selected from IEC 62443-3-3

The table below lists the requirements selected from the IEC 62443-3-3 standard on *System security requirements and security levels* [1].

IEC	Name	Objective
SR1.1	**Human user identification and authentication**	8.5-SO4
SR1.1 EE1	**Role identification and authentication for engineers and local operators** The control system shall provide the capability to identify and authenticate the role of engineers and local operators.	8.5-SO4
SR1.3	**Account management**	8.3-SO3
SR1.5	**Authenticator management**	8.24-SO2
SR1.5 EE1	**Storing passwords** The control system shall provide the capability to store passwords salted and hashed. *Supplemental guidance:* It is recommended to use a password hashing function that is resistant against GPU cracking attacks, such as Argon2 or PBKDF2.	8.5-SO4

IEC	Name	Objective
	Users should be able to change their own passwords through the central maintenance system or through the access control server.	
SR1.8	**Public key infrastructure certificates**	8.24-SO2
SR1.9	**Strength of public key authentication**	8.5-SO4 8.24-SO2
SR2.1	**Authorization enforcement**	8.3-SO3 8.3-SO4
SR2.1 RE1	**Authorization enforcement for all users** *Supplemental guidance:* The requirement also applies to IEDs at other substations communicating for distance and differential protection. Only the data and commands needed for those functions should then be accessible. IEDs at other substations should not be able to access configuration functions or general control functions.	8.3-SO3 8.3-SO4
SR2.1 EE1	**Role separation for engineers and local operators** The control system shall provide the capability to set different authorizations for different roles, allowing to define at least roles for the engineers and local operators and apply the principle of least privileges for them. *Supplemental guidance:* The requirement can be met by having a different user accounts or different services for each role. Each account should then have its own password or keys for authentication. The requirement can also be met by using centrally managed, role-based access control. Several vendors support this for IEDs and substation HMIs. But special care should be taken that there is a fallback to access	8.3-SO3

IEC	Name	Objective
	the IEDs in case of connectivity problem, and that the connection to the central maintenance server does not create a new attack vector into the substation. *Equipment in the substation inside should at least have separate roles for engineers and operators. Preferably, the equipment has all the pre-defined roles in IEC 62351-8* [8].	
SR2.6	**Remote session termination**	8.5-SO4
SR2.8	**Auditable events**	8.15-SO2
SR2.9	**Audit storage capacity**	8.15-SO2
SR2.10	**Response to audit processing failures**	8.15-SO2
SR2.11	**Timestamps**	8.17-SO2
SR2.11 RE1	**Internal time synchronization**	8.17-SO2
SR2.11 RE2	**Protection of time source integrity**	8.17-SO2
SR 3.9	**Protection of audit information**	8.15-SO2
SR3.10 EE1	**Update capacity** The devices in the control system shall have enough memory (RAM and flash) and computing power to allow security updates needed during their lifetime.	8.19-SO1
SR3.10 EE2	**Local updates** The devices in the control system shall allow the updates to be performed locally.	8.19-SO1
SR 4.3	**Use of cryptography**	8.5-SO4

IEC	Name	Objective
		8.24-SO2
SR4.3 EE1	**Use of cryptography according to ECRYPT recommendations** The control system shall follow the recommendations in the ECRYPT – Algorithms, Key Size, and Protocols Report [10]. In particular: • It only uses the cryptographic algorithms that the ECRYPT recommends as suitable for new or future systems. • It uses keys as least as long as the ECRYPT report recommends for near term use (section 4.6 in the ECRYPT report). • It only uses 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-SO4 8.24-SO2
SR5.1	**Network segmentation** *Supplemental guidance:* The segregation on the substation LAN interface may be applied through the substation firewall. Figure 3 shows an example network setup. The hosts in the substation perimeter, the gateway and jump server, are both place in a demilitarized zone on the substation firewall, separating them from the substation LAN. Some hosts in the substation inside, the substation HMI and time server, are also placed in a demilitarized zone to provide additional protection. The diagram shows the devices directly connected to the firewall, but they may also be connected through a switch. The example segmentation in Figure 3 allows some defense-in-depth inside the substation. An attacker that compromises the gateway or HMI can for instance be denied access to the maintenance services on the	8.22-SO1

IEC	Name	Objective
	IEDs. GOOSE traffic is only broadcast to the IEDs and cannot be spoofed or manipulated by other devices. The firewall should usually apply the following restrictions on the substation LAN interface: • The gateway and HMI should only access the MMS service on IEDs • The jump server should only access the local maintenance services on substation equipment • The time server should only be accessed on NTP or similar services If the firewalls support more advanced protection, such as using detection signatures or deep-packet inspection, this should be turned on whenever possible. Communication used for protection functions should be segregated as much as possible, and should be given priority over other types of communication. This applies both to protection communication inside the substation (such as GOOSE and sampled values) and protection communication between substations (used for differential and distance protection) Possible segregation and prioritization measures are: • Using VLANs and priority tagging for GOOSE and sampled value communication • Using separate communication channels for communication between substations • Using quality-of-service features in protocols such as MPLS	
SR5.1 RE1	**Physical network segmentation**	8.22-SO1
SR5.1 RE2	**Independence from non-control system networks**	8.22-SO1
SR5.1 RE3	**Logical and physical isolation of critical networks**	8.22-SO1
SR5.1 EE1	**Remote maintenance through a jump host**	8.22-SO3

IEC	Name	Objective
	If remote maintenance to equipment in the substation inside is allowed, the control system shall provide the capability to perform it through a jump host. The jump host shall log all actions taken by the remote engineer.	
SR 5.2	**Zone boundary protection**	8.22-SO2
SR 5.2 RE1	**Deny by default, allow by exception**	8.22-SO2
SR 6.1	**Audit log accessibility**	8.15-SO2
SR 6.1 RE1	**Programmatic access to audit logs**	8.15-SO2
SR 7.3	**Control system backup**	8.9-SO2
SR 7.4	**Control system recovery and reconstitution**	8.9-SO2
SR 7.7	**Least functionality**	8.8-SO2

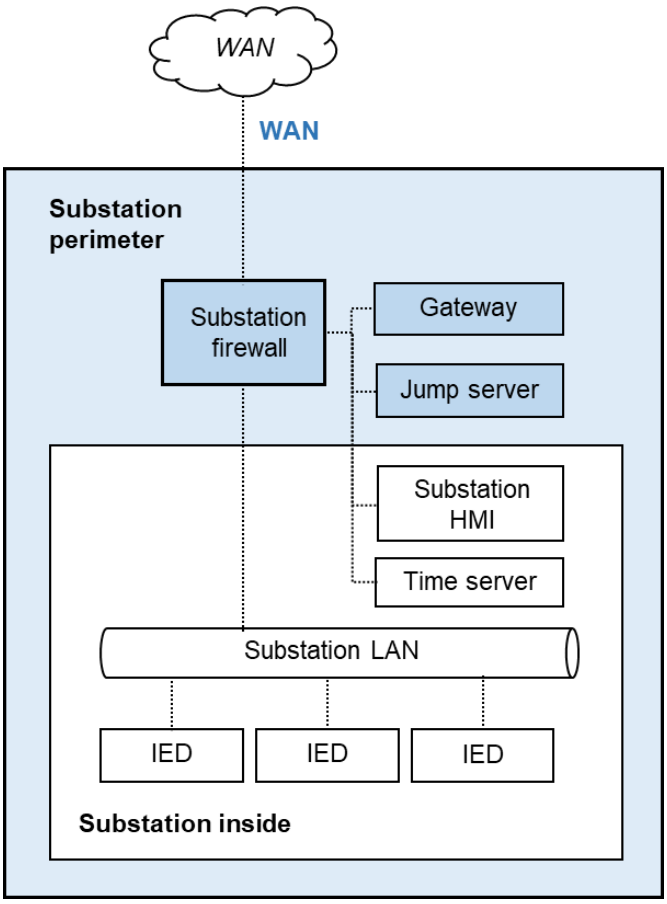


Figure 3: Example of network segmentation in the substation.

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 substation inside (Table 5).

8.3-SO3 Role separation for engineers and local operators

Authorization is covered by *SR2.1*, *SR2.1 RE1, and SR2.1 RE2* with the additional requirement *SR2.1 EE1* to ensure that roles can be separated. Account management (*SR1.3*) is required to manage the account of different roles.

8.3-SO4 Least privileges on the substation LAN, time synchronization, and protection interfaces

Authorization for all users is covered by SR2.1, SR2.1 RE1.

8.5-SO4 Authentication by role for engineers and local operators

Authentication is covered by requirement *SR1.1* with the additional requirement *SR1.1 EE1*. Requirement *SR1.5 EE1* ensures passwords are stored securely. Strong cryptographic keys and algorithms for the authentication are ensured by requirements *SR1.9* and *SR4.3* with the additional requirement *SR4.3 EE1*. Remote session termination (*SR2.6*) is included to reduce the risk that authentication is bypassed by compromising a session.

8.8-SO2 Local hardening

Disabling unneeded functions is covered by requirement *SR 7.7*

8.9-SO2 Local configuration management

Restoration from a local backup is covered by requirements *SR 7.3* and *SR 7.4*.

8.15-SO2 Collecting security events from the substation inside through the perimeter

Logging security events is covered by requirement *SR2.8*. Sending the logs to the substation perimeter is covered by requirements *SR6.1* and *SR6.1 RE1*.

Protection of the security logs is covered by requirements *SR2.10* and *SR3.9*. Requirement *SR2.9* ensures that there is enough storage capacity on the device for the logs.

8.17-SO2 Clock synchronization for the perimeter

Time synchronization is covered by requirements *SR2.11* and *SR2.11 RE1*. Requirement *SR2.11 RE2* ensures that the integrity of the time source is protected.

8.19-SO3 Local software and firmware management

Remote updates of software and firmware are covered by *SR3.10 EE2*, while *SR3.10 EE1* ensures there is enough memory and computing power for future updates.

8.22-SO2 Network segregation on the substation LAN interface

Network segregations is ensured by requirement *SR5.1*. As the substation networks are highly critically, they should be physically segregated (*SR5.1 RE1*), be independent of non-control system network (*SR5.1 RE2*) and allow the substation to be isolated from non-critical networks (*SR5.1 RE3*).

Requirements *SR5.2* and *SR5.2 RE1* ensure that there is protection between different security zones, and only allowed traffic can go through.

8.22-SO3 Remote management through a jump host

The remote maintenance objective is covered by requirement *SR 5.1 EE1*.

8.24-SO2 Local key and password management

Local updates of keys and credentials is covered by requirement *SR1.5*. Requirement *SR1.8* allows a root certificate from the grid operator to be installed, so that it can be integrated in their PKI. Requirements *SR1.9*, *SR4.3*, and *SR4.3 EE1* ensure the strength of the cryptography used for the certificates.

References

[1] ISA/IEC, "IEC 62443-3-3: Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels".

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

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

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

[7] ENCS, "DA/SA-311-2022: Security requirements from IEC 62443 for procuring RTUs and gateways," 2022.

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

[9] ENCS, "WP-032-2020: Centralized access control for field devices," 2020.

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

[11] ENCS, "SA-101-2019: Security reference architecture and risk assessment for substation automation," 2019.