SA-111-2022

Security threat analysis 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 their components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

This document is shared under the Traffic Light Protocol classification:

TLP White – publica

ENCS

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

Version History

Date	Version	Description
20 July 2022	2022v0.1	First version of the threat analysis for SA, including context analysis to build profiles.
18 August 2022	2022v0.2	Version with ISO 27002:2022 objectives
3 October 2022	2022v0.3	Minor fixes in the objective names to stay aligned with the requirements documents

Table of Contents

1 Introduction

This document provides a threat analysis for substation automation systems. It analyzes information assets and threats to derive security objectives for the substation automation system and its operational environment. From the system objectives, objectives are also derived for gateways in the substation.

Grid operators are increasingly automating their high voltage substation with substation automation. They use these systems to get power measurements to reliably integrate renewables and electric vehicles, and to remotely control the grid to recover from power outages more quickly.

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

Making sure the substation automation systems are secure is, hence, critical. This document analyzes the threats to these systems and defines security objectives to counter these threats. Objectives are defined for both the substation automation system itself and for the environment in which it operates. The focus is on technological objectives, but organizational, people, and physical controls are also considered.

The objectives for the system are used to define security requirements for substation automation systems based on the IEC 62443-3 standard in [1]. Grid operators can use these requirements when they procure a substation automation system from a system integrator, or when they implement the system through an internal department.

The threat analysis allows grid operators to check if the security requirements are applicable in their situation. Operators can compare the assets, access control policy, and threats against their own situation. The objectives are organized according to the controls in ISO/IEC 27002:2022 [2], so that they can also be compared to the controls that the grid operator has selected. If the objectives do not cover all their needs, operators can add additional objectives to mitigate their specific risks.

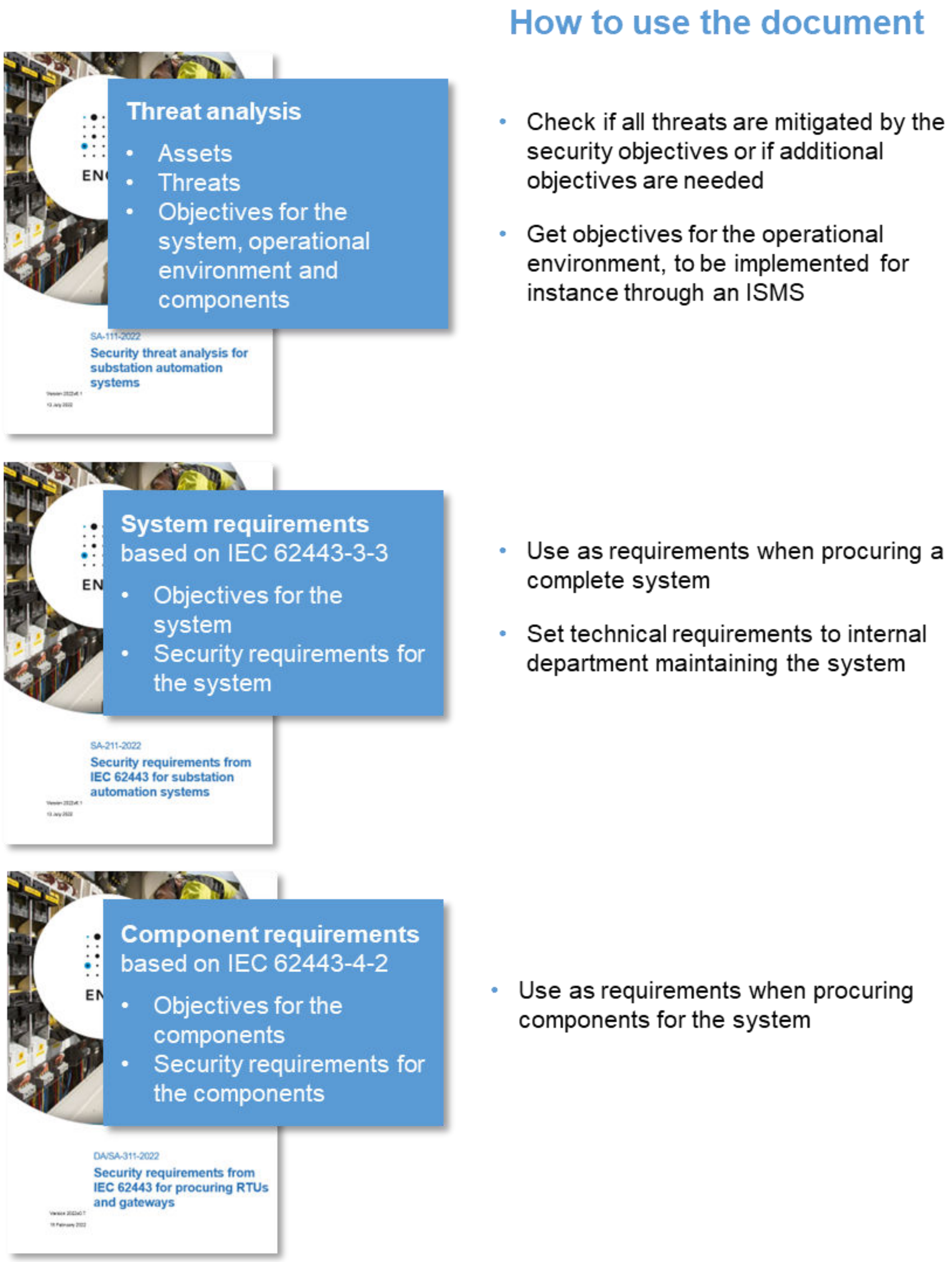
Additionally, the objectives to the operational environment give guidance to grid operators on how to securely use a substation automation system meeting the security requirements. Some threats can only be mitigated in the operational environment. Even when the substation automation system implements strong security measures, it can only be secure if its environment is protected. This document describes the organizational, people, physical, and technological controls that grid operators should take for this purpose and gives guidance on their implementation.

Based on the system objectives, objectives can also be derived for the gateway in the substation. These objectives are used to define security requirements based on IEC

62443-4-2 in [3], which can be used directly when procuring gateway. In this way, operators get a consistent set of requirements for the whole system.

1.1 Relation to other documents

This document is part of a larger series on substation automation security (see Figure 1).



How to use the document

Threat analysis
- Assets
- Threats
- Objectives for the system, operational environment and components

SA-111-2022
Security threat analysis for substation automation systems

- Check if all threats are mitigated by the security objectives or if additional objectives are needed
- Get objectives for the operational environment, to be implemented for instance through an ISMS

System requirements based on IEC 62443-3-3
- Objectives for the system
- Security requirements for the system

SA-211-2022
Security requirements from IEC 62443 for substation automation systems

- Use as requirements when procuring a complete system
- Set technical requirements to internal department maintaining the system

Component requirements based on IEC 62443-4-2
- Objectives for the components
- Security requirements for the components

DA/SA-311-2022
Security requirements from IEC 62443 for procuring RTUs and gateways

- Use as requirements when procuring components for the system

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

The system requirements document [1] gives security requirements selected from IEC 62443-3-3 to ensure that a substation automation system meets the technological objectives for the system defined in this document (Section 5.4). The component requirements for gateways give requirements that can be used to procure gateways that meet the security objectives.

2 System description

To determine the security threats to the substation automation system, we should first understand how the system works: what its intended use is, in what environment it will be used, and what information assets are processed by it.

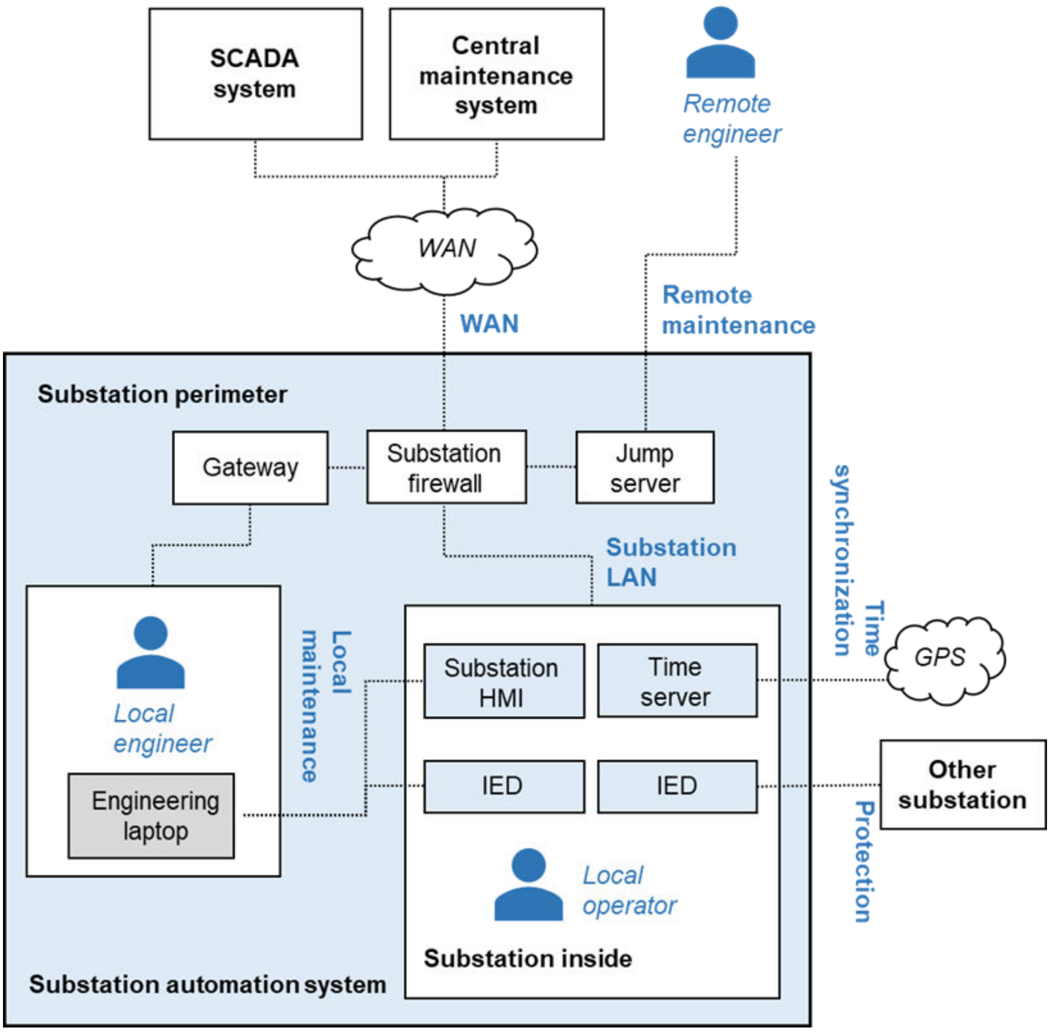


Figure 2: Reference architecture for the substation automation system, showing its users and interfaces. The requirements in this document concern the gateway.

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 automation, 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 Assets

To perform its two main functions, remote monitoring and control and local automation and protection, the substation automation system processes various information assets.

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

- 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

To be able to process this information, the substation automation must be configured by the grid operator's engineers. The information assets needed for configuration are:

- the software and firmware
- the stored configuration, including the WAN network settings and the mapping between SCADA addresses and attached sensors and actuators
- operational logs of devices to analyze and fix problems

For the protection functions, the substation automation system needs:

- measurements of electrical variables, such as voltages and currents
- internal commands to control equipment in the substation, such as circuit breakers, disconnectors, and earthing switches
- protection settings, including the protection logic and parameters

Protection settings can also include interlockings that block potentially harmful switching actions. To run this, the firmware of IEDs and protection relays is needed.

For security, the substation automation system also keeps security logs and handles keys and passwords. These include the passwords used by engineers to log in and the keys used for authentication and communication security on the WAN.

The most critical assets are those that could compromise the working of the protection functions, especially the protection settings and the firmware of the IEDs and protection relays. If attackers can compromise the integrity of these assets, protection will not work properly. Faults may then endanger the safety of staff at the substation, and cause damage to the primary equipment.

For all assets, it is most important to protect the integrity and availability. The information processed by the substation is usually not highly confidential, although it could contain commercially sensitive information about the power use of large customers. Of course, keys and passwords, especially those used for remote authentication, should be kept confidential.

3 Threats

Based on the system description we can determine the possible threats. On external interfaces, there are threats of unauthorized access, exploits of software vulnerabilities, and attacks on the communication. There are physical threats to the location and supply chain threats to the equipment used. For each normal user group, there are insider threats. And there are threats of what attackers may do to the critical assets after they have gained access.

3.1 Unauthorized access threats

Unauthorized access threats concern an attacker getting access to the substation automation system as one of the user groups (see Figure 2 in Section 2) using the normal access method on an interface. They may for instance compromise a key or password and then log in. Threats are considered per interface (see Figure 2), as usually different measures are taken on each interface.

T-UA1 Unauthorized access as the SCADA or central maintenance system on the WAN	An attacker gains access to the WAN network and then gains unauthorized access to the substation as the SCADA or central maintenance system. With this access they may send control commands or change the configuration or firmware.
T-UA2 Unauthorized access as an engineer on the remote maintenance interface	An attacker gains access to the remote maintenance interface and then gains unauthorized access to the substation as an engineer. With this access they may change the configuration or firmware.
T-UA3 Unauthorized access on the time synchronization interface	An attacker gains access to the time synchronization interface and then gains unauthorized access to the substation. With this access they may change the time in the substation automation system.
T-UA4 Unauthorized access on the protection interface	An attacker gains access to the protection interface and then gains unauthorized access to the substation. With this access they may cause protection functions using the interface to trigger.

3.2 Exploits of software vulnerability

Exploits of software vulnerabilities concern an attacker exploiting a vulnerability in the substation automation system to gain access to it. Using a software vulnerability, attackers may gain privileged access to the system, even when users on an interface normally have restricted access, as is for instance the case on the time synchronization and protection interfaces.

The WAN and remote maintenance interfaces (see Figure 2 in Section 2) are considered separately from the time synchronization and protection interfaces. The first group of interfaces may be exploited using exploits developed for normal IT systems. The second group requires more specialized exploits to be developed.

Exploits that cause only denial-of-service condition are considered as part of the communication threats (Section 3.3).

T-EX1 Exploit of a software vulnerability on the WAN or remote maintenance interface	An attacker gains access to the WAN or remote maintenance interface and then exploits a software vulnerability to gain, possibly privileged, access to the substation automation system. With this access they may send control commands or change configurations or firmware.
T-EX2 Exploit of a software vulnerability on the time synchronization or protection interface	An attacker gains access to the protection or time synchronization interface and then exploits a software vulnerability to gain, possibly privileged, access to the substation automation system. With this access they may send control commands or change configurations or firmware.
T-EX3 Malware introduced through engineering laptops	Malware is introduced in the substation through an engineering laptop. The malware may be transferred over the internal substation network, or through portable media such as USB drives. Untargeted malware, such as generic ransomware, may cause components to become unavailable, especially if they are running off-the-shelf operating systems. Targeted malware may send control commands or change configurations or firmware.

3.3 Communication threats

Communication threats concern compromising the confidentiality, integrity, or availability of the communication on an interface. Separate threats are considered on different interfaces (see Figure 2 in Section 2), as they are protected by different measures.

The threat of data disclosure on the time synchronization or the protection interface is not considered. The information sent on these interfaces is not confidential.

T-CM1 Data modification on WAN	An attacker gains access to the WAN network and then modifies information sent between the substation automation system and the SCADA system or central maintenance system. In this way, they may send control commands, alter measurements of electrical variables, or change the configuration or firmware.
T-CM2 Data disclosure on WAN	An attacker gains access to the WAN network and then eavesdrops on information sent between the substation automation system and the SCADA system or central maintenance system. In this way, they may obtain the measurements of electrical variables from the substation.
T-CM3 Network denial-of-service attack on the WAN interface	An attacker gains access to the WAN interface and disrupts the normal operation of the substation, for instance by sending malformed messages or flooding the substation automation system with data. In this way, they may stop measurements being collected, commands being received by the substation, or even protection functions to stop working.
T-CM4 Data modification on the remote maintenance interface	An attacker gains access to the network used for remote maintenance and then modifies information sent between the engineers and the substation automation system. In this way, they may send control commands, alter measurements of electrical variables, or change the configuration or firmware.
T-CM5 Data disclosure on the remote maintenance interface	An attacker gains access to the network used for remote maintenance and then eavesdrops on information sent between the engineers and the

	substation automation system. In this way, they may change the time in the substation automation system.
T-CM6 Network denial-of-service attack on the remote maintenance	An attacker gains access to the remote maintenance interface and disrupts the normal operation of the substation, for instance by sending malformed messages or flooding the interface with data. In this way, they may obtain information about the configuration in the substation.
T-CM7 Data modification on the time synchronization interface	An attacker gains access to the time synchronization interface and then modifies the information sent over it. In this way, they may change send control commands, alter measurements of electrical variables, or change the configuration or firmware.
T-CM8 Network denial-of-service attack on the time synchronization interface	An attacker gains access to the time synchronization interface and disrupts the normal operation of the substation, for instance by sending malformed messages or flooding the substation automation system with data. In this way, they may prevent time in the substation being synchronized.
T-CM9 Data modification on the protection interface	An attacker gains access to the time protection interface and then modifies the information sent over it. In this way, they may cause protection functions using the interface to trigger.
T-CM10 Network denial-of-service attack on the protection interface	An attacker gains access to the WAN interface and disrupts the normal operation of the substation, for instance by sending malformed messages or flooding the substation automation system with data. In this way, they may prevent protection functions from working.

3.4 Physical threats

Physical threats concern an attacker gaining access to the system using physical means. They may try to break into the substation and then access local interfaces, such as the HMI, tamper with the hardware, for instance by changing data stored on hard disk or in flash memory, or tamper with the networks, for instance by putting additional devices in them.

Of particular concern is the threat of an attacker breaking into one substation and using their access to get to other substations. Such an attack would allow attacker to compromise more than one substation at the same time, leading to a higher impact.

We only consider physical threats to the substation automation systems, not direct sabotage of primary equipment such as transformers or lines. Such threats should be considered separately by the grid operator.

T-PH1 Unauthorized physical access in a substation	An attacker gains physical access to a substation and uses the physical access to gain logical access to the substation automation systems. Attackers may log in on one of the ports or physically tamper with the hardware. With this access they may change the configuration or firmware.
T-PH2 Unauthorized access from one substation to another substation	An attacker gains physical access to a substation and uses the access to gain logical access to the substation automation systems at several other substations. With this access they may change the configuration or firmware in all affected substations.
T-PH3 Placing a hardware backdoor at the substation	An attacker gains physical access to the substation and adds a physical device to the substation that acts as a backdoor into the substation automation system. With this access they may send control commands or change the configuration or firmware.

3.5 Supply chain threats

Supply chain threats concern attacks on the substation automation system through suppliers. Attackers may compromise the hardware or software used in the substation before it is installed, for instance to put backdoors in it.

The threat of sensitive information leaking through suppliers is not considered here. It can only be countered by organizational measures, not by any technical measures in the substation automation system.

Threats through staff at suppliers working on the substation automation system (remotely or locally) are considered part of the insider threats (Section 3.6). The staff would be considered as engineers, and the same objectives apply to them as to internal staff.

T-SC1 Software or firmware modification before installation	An attacker modifies software or firmware before it is installed in the substation automation system. The firmware could be modified at the developer or in transit between the developer and the substation automation system. This way, attackers may for instance install backdoors or logic bombs in the substation automation system that would allow them to send control commands or change the configuration.
T-SC2 Hardware modification before installation	An attacker modifies hardware before it is installed in the substation automation system. The hardware could be modified at the manufacturer or in transit between the developer and the substation automation system. This way, attackers may for instance install backdoors or logic bombs in the substation automation system that would allow them to send control commands or change the configuration.

3.6 Insider threats

Insider threats concern threats to the substation automation system by authorized human users. Different threats are considered for the two user groups: engineers and operators (see Figure 2 in Section 2).

T-IN1 Harmful actions by engineers	An engineer with authorized access, incidentally or on purpose, performs actions that are harmful to the substation automation system or the electricity grid. They may, for instance, make incorrect changes to the configuration, install the wrong firmware, or perform unintended switching commands.
T-IN2 Harmful actions by local operators	A local operator with authorized access, incidentally or on purpose, performs actions that are harmful to the electricity grid. They may, for instance, perform unintended switching commands.

3.7 Post-exploitation threats

The following threats concern steps attackers can take to compromise the substation information assets after they have gained access to the system. They are considered separately, as they may be combined with any threat that gives an attacker access.

T-PE1 Loss of configurations	The configuration of the substation automation system is deleted or becomes corrupted through mistakes by engineers or intentional actions from an attacker that has gained access.
T-PE2 Software or firmware corruption	The software or firmware installed in the substation automation systems is corrupted, for instance, by placing a backdoor or logic bomb in it, or simply making it unusable.

4 Zoning model

To mitigate the threats, the substation will be divided into two zones: the substation perimeter and substation inside. Different objectives will be defined for each zone. To define the access control objectives, we also identify the users of each zone.

4.1 Zoning

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.

4.2 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.

5 Security objectives for substation automation systems

We can now define security objectives to mitigate the threats. The zoning model allows to set different objectives based on the scalability of the threats:

- For threats that can scale to many substations through the WAN network, the security objectives provide protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation (security level 3). Such threats must, by definition, go through the substation perimeter.
- For threats where the impact is limited to one substation or small number of substations, such as physical attacks, the security objectives provide protection against intentional violation using simple means with low resources, generic skills, and low motivation (security level 2).

Less strict objectives are set for non-scalable threat because providing the same level of security throughout the substation would be very costly. It would require replacing most legacy equipment in the substation inside and applying strict physical security measures to all substations.

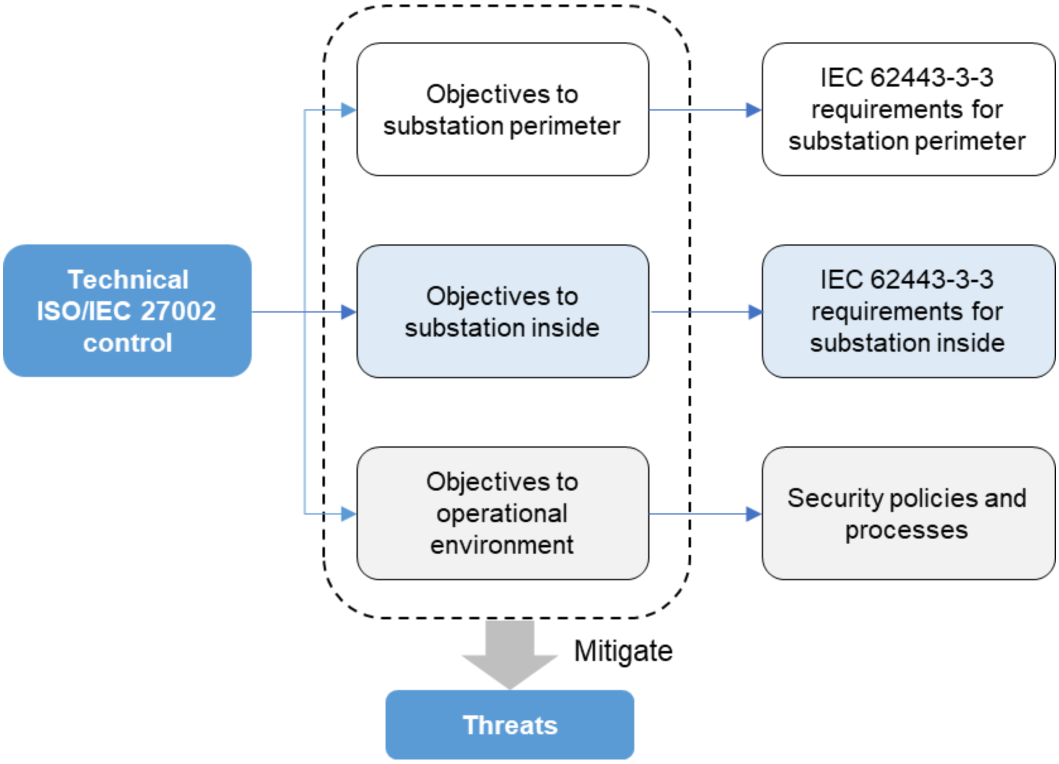

Objectives to substation perimeter
IEC 62443-3-3 requirements for substation perimeter
Technical ISO/IEC 27002 control
Objectives to substation inside
IEC 62443-3-3 requirements for substation inside
Objectives to operational environment
Security policies and processes
Mitigate
Threats

Figure 3: Relation of the security objectives to the ISO/IEC 27001 and IEC 62443 standards.

The objectives are derived from the controls in ISO/IEC 27002:2022 [2]. For the organizational, people, and physical controls, the controls themselves are used as objectives. The technological controls are refined into more detailed objectives for the perimeter, inside, and operational environment, as shown in Figure 3, as the aim of this document is in the end to define technical security requirements for substation automation systems in [1]. The objectives to the operational environment are additional organizational and technical measures that the grid operator should take to securely operate the substation automation system. These should be addressed in the internal security policies and processes of the operator.

5.1 Organizational controls

At least the following organizational controls from ISO/IEC 27002:2022 are needed to mitigate the threats:

- 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

Implementation guidance on access control (5.15, 5.16, 5.18): For the substation perimeter, objective SO-AC5 allows the accounts to be managed centrally.

In the substation inside, engineers will often use administrator accounts and share the passwords. If these accounts can only be used for local access the risks can be acceptable. Grid operators should however carefully evaluate if mitigating measures, in particular physical access control measures, are sufficient.

5.2 People controls

At least the following people controls from ISO/IEC 27002:2022 are needed to mitigate the threats:

- 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

5.3 Physical controls

At least the following physical controls from ISO/IEC 27002:2022 are needed to mitigate the threats:

- 7.1 Physical security perimeters
- 7.2 Physical entry
- 7.4 Physical security monitoring
- 7.8 Equipment siting and protection
- 7.12 Cabling security

Implementation guidance: Physical security for substations is a hard problem. The cost of physical measures is high, as they would have to be applied to often hundreds of substations. Moreover, most substations are unmanned for most of the time.

The technological objectives in this document are designed to limit the impact of a physical break-in to one substation (see objective **8.22-SO4** in Section 5.4). By restricting network communications, it can be made very difficult for physical attackers in one substation to reach other substations or central systems.

Given this design, grid operators should protect each substation based on the risks to the substation itself. They should perform a physical security risk assessment on each individual substation, taking into account for instance:

- The amount of power transported or distributed through the substation
- Its place in the grid (is it an important node in the topology?)
- The number and type of customers connected (are there critical infrastructures receiving power to the substation)
- The time needed to recover from an incident

Physical security measures should be selected based on the risk assessment. To simplify the selection, substation may be placed into several categories.

Basic passive measures would for instance be fences and gates at the substation perimeter, walls, and doors of the building with the substation automation equipment, and locks and alarms on the cabinets with this equipment. For higher risk substations, active measures such as alarm or camera systems are likely required. Different operators will likely choose different measures, based on the physical threats they face and safety restrictions.

For insider threats, it is important to have logs of who has entered a substation (control **7.2**). Equipment in the substation inside often does not allow to use individual user accounts. So, to see who has performed a certain action on them, the device logs need to be combined with logs of physical access to the substation. Physical access logs could be kept manually, for instance by requiring to report visits to the control center and keeping written logs. For high-risk substation, access card or biometrics should be considered.

5.4 Technological controls

While for the organizational, people, and physical controls we just use the controls from ISO/IEC 27002:2022, the technological controls are further specified in more detailed objectives for the substation perimeter, substation inside, and the operational environment (see Figure 3).

For the substation perimeter, strong security measures are possible through remote management. So, there are objectives for strong access control for all users, cryptographically protecting the communication, and monitoring the zone from a SIEM. If there are protection functions in the zone (which is usually not the case), they should be protected from denial-of-service attacks from the WAN. The functions should also not be disrupted by security updates, so that it is possible to remotely patch vulnerabilities.

For the substation inside, security objectives are more limited because we assume equipment is locally managed. The main goal is to separate the inside from the outside by network segregation, remote access through a jump host, and using least privileges on the interfaces. Basic access control and logging is included to protect the protection configuration and the software and firmware in the zone, as these are especially critical assets.

8.3 Information access restriction

Perimeter	**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.
	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.
Inside	**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.
	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.

8.5 Secure authentication

Perimeter	**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.
	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.
	8.5-SO3 Authentication with individual passwords for engineers: The substation perimeter enforces mutual authentication for engineers. Engineers use individual passwords or keys. The login procedure is protected against known attacks.
Inside	**8.5-SO4 Role-based authentication 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.

8.7 Protection against malware

Perimeter	**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. *Remark:* It is recommended to also use active malware protection on off-the-shelf operating systems in the substation inside, if this is possible. Often, this

	is more complex, as there is more legacy components and anti-virus signatures would have to be downloaded through the substation perimeter.
Operational environment	**8.7-SO2 Protecting engineering laptops against malware:** If engineering laptops are used for local maintenance to the substation, these are strongly protected against malware. *Implementation guidance:* Malware protection would include hardening the laptop, enforcing a strict patching policy, and using anti-virus or endpoint protection software. Additionally, it would be recommended that engineers use different laptops for their normal office work and for working in substations. This measure would significantly reduce the chance of laptops getting infected through internet use or phishing. With separate laptops it also becomes possible to block command and control traffic by whitelisting the internet sites the laptop can reach.

8.8 Management of technical vulnerabilities

Perimeter	**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.
Inside	**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.
Operational environment	**8.8-SO3 Vulnerability management process:** The grid operator manages vulnerabilities in the 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

	Implementation guidance: A clear policy should be defined for when vulnerabilities must be patched, based on their severity. The CVSS score could be used as a severity measure but must usually be complemented with information about the location of the vulnerability in the system. Patching policies may be different for the substation perimeter and inside. Patches in the perimeter may be applied remotely. So, with a good process the effort required should be low, and most vulnerabilities can be patched quickly. For the substation inside, patching will require a lot of effort. Patches need to be applied locally, often through a manual process. The protection functions in the substation usually need to be retested after the update. Hence, patches will usually be applied only in exceptional cases. With the right network segregation measures, such a policy can be acceptable.

8.9 Configuration management

Perimeter	**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.
Inside	**8.9-SO2 Local configuration management:** Through local access devices in the substation inside allow to restore the device from a backed-up configuration.

8.13 Information backup

Operational environment	**8.13-SO3 Backup process for device configurations:** The grid operator has a process to back up the configurations of the devices 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.

8.15 Logging

Perimeter	**8.15-SO1 Integration with SIEM system:** Devices in the substation perimeter log all relevant security events, such as access control events, and changes to the configuration and firmware. The devices can store the logs locally for forensic analysis. They can send them to a Security Information and Event Management (SIEM) system in a commonly supported format, (SIEM) system, so that they can be analyzed to detect incidents.

Inside	**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, so that they can be analyzed to detect incidents. *Remark:* The substation perimeter can forward the security logs to the central systems or a SIEM system over the WAN. The security logs can for instance be collected by the substation gateway.

8.16 Monitoring activities

Operational environment	**8.16-SO1: Security monitoring and incident response:** The grid operator monitors security events on the device and can respond to them. They gather security logs from the 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. *Implementation guidance:* Monitoring should try to detect at least: • unauthorized access attempts on the WAN and remote maintenance interface • unauthorized changes of the clock in the substation • unauthorized local access to devices • unauthorized changes in the configuration for protection • unauthorized installed firmware or software • new devices appearing in the substation Older devices may provide insufficient log information for some of these use cases. In that case, it could be considered to install a network-based IDS in the substation. Such an IDS may also be able to help with asset management.

8.17 Clock synchronization

Perimeter	**8.17-SO1 Clock synchronization for the perimeter:** The substation perimeter synchronizes time with a central source to have reliable timestamps for security events. *Remark:* Time may be synchronized over the WAN interface or over the time synchronization interface (if it is present).

Inside	**8.17-SO2 Clock synchronization for the perimeter:** The substation inside synchronizes time with a central source to have reliable timestamps for security events. *Remark:* Time may be synchronized over the time synchronization interface (if it is present) or over the WAN interface through a device in the perimeter such as a gateway.

8.19 Installation of software on operational systems

Perimeter	**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.
	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.
Inside	**8.19-SO3 Local software and firmware management:** Through local access devices in the substation inside allow to update their software or firmware.
Operational environment	**8.19-SO4 Manual integrity checks for substation inside:** There is a process to manually check the integrity and authenticity of firmware and software before installing it on equipment in the substation perimeter. Remark: The manual process is needed, as not all equipment in the inside supports digitally singed software and firmware. Engineers should check that the firmware comes from a trusted source and check the integrity through for instance a hash value before installation.

8.20 Network security

Perimeter	**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.
	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. *Remarks:* Often, there are no protection functions running in the substation perimeter, as they are all in the substation inside. When IEC 61850-90 is used to communicate with the substations, this can also be achieved by using a gateway or proxy, instead of directly with the IEDs. If there is no protection in the perimeter, the objective is automatically met. The security architecture however allows designs in which protection functions are in the substation perimeter, as long as this requirement is met. The resilience would have to be provided by the devices running the protection functions. They should be thoroughly tested to ensure protection functions keep running under flooding attacks or attacks with malformed packets.

8.21 Security of network services

Operational environment	**8.21-SO1 Resilience against denial-of-service attacks on the WAN:** 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.
	8.21-SO2 Use of private networks for the protection interface: The grid operator uses private networks for the protection interface.
	8.21-SO3 Point-to-point connections on the protection interface: The networks on the protection interface only allow point-to-point connections between the devices that need to communicate with each other.

8.22 Segregation of networks

Perimeter	**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.
Inside	**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. *Remark:* Network segregation should also be used on the time synchronization and protection interfaces. But this is not always possible. On the time synchronization GPS may be used, while on the protection interface serial communication is still common.
	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.
Operational environment	**8.22-SO4 Physical impact limiting to related locations:** Communication between substations and from substations to the central system is restricted to what is needed, so that the impact of a physical compromise of one substation is limited. *Implementation guidance:* On the WAN interface there should be no direct communication between the substations. The substations should only be able to communicate to the SCADA system and central maintenance systems. This restriction can for instance be enforced in the VPN configuration or the architecture of the telecom network, as long as the measure still works even when an attacker gains full access to the network equipment in the compromised substation. The firewall at the central systems should only allow through network services needed for normal communication to the substation. The services exposed to substation should be tested for vulnerabilities, assuming that a substation can be compromised. Communication between substations is needed for distance and differential protection. So, they may try to compromise other substations over the protection interface. Switching over these interfaces will not create a larger impact than switching directly from the compromised substation. So, the goal

	should be to ensure that attackers cannot exploit software vulnerabilities over this interface (see Section 6.2).

8.24 Use of cryptography

Perimeter	**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.
Inside	**8.24-SO2 Local key and password management:** Through local access devices in the substation inside allow to update all passwords and keys.
Operational environment	**8.24-SO3 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. *Implementation guidance:* In the substation perimeter, it should be possible to remotely update keys and passwords according to modern policies. In the substation inside, it may be a lot of work to update them, as often it must be done locally with a manual process. If the keys and passwords are only used for local access within the substation, the risk of not changing them could be acceptable. If it is not, mitigating measures should be defined.

6 Rationale for the security objectives

This section explains how the security threats in Section 3 are mitigated by the security objectives in Section 5.

6.1 Protection from unauthorized access threats

Unauthorized access can be stopped by preventing attackers to get access to the interface or by access control in the substation automation system. Some interfaces are protected by the first approach, others by the second, as shown in Table 4.

Table 4: Security objectives to mitigate unauthorized access threats.

Threat	**Interface access** *(operational environment)*	**System access control** *(substation perimeter)*
T-UA1 Unauthorized access as the SCADA or central maintenance system on the WAN		**8.5-SO1** Network-based authentication for the SCADA system **8.5-SO2** Role-based authentication for the central maintenance system with unique device authentication
T-UA2 Unauthorized access as an engineer on the remote maintenance interface		**8.5-SO3** Authentication with individual passwords for engineers
T-UA3 Unauthorized access on the time synchronization interface		**8.3-SO4** Least privileges on the substation LAN, time synchronization, and protection interfaces

T-UA4 Unauthorized access on the protection interface	**8.21-SO2** Use of private networks for the protection interface **8.21-SO3** Point-to-point connections on the protection interface	**8.3-SO4** Least privileges on the substation LAN, time synchronization, and protection interfaces

6.1.1 Protection on the WAN and remote maintenance interfaces (T-UA1, T-UA2)

To protect against unauthorized access on the WAN and remote maintenance interfaces, the goal is to provide protection against sophisticated threats (security level 3) through system access control (**8.5-SO1**, **8.5-SO2**, **8.5-SO3**). Attacks on these interfaces provide the largest risk, as they are scalable and would allow attackers to access all assets.

To ensure that the access control objectives provide security against sophisticated attackers (security level 3), the following supporting objectives are required:

- **Key and password management:** keys and credentials used for authentication should be regularly updated, to reduce the impact of them being compromised. Remote management (**8.24-SO1**) makes is technically possible to update the keys efficiently. The key and password management process (**8.24-SO3**) makes sure there is a process to update them.
- **Account management:** accounts of the engineers should be managed to ensure (**5.16**, **5.18**), for instance, that when an engineer changes jobs their access is revoked. To allow this process to work efficiently, the accounts of engineers in the perimeter are managed centrally (**8.3-SO2**).
- **Hardening:** the substation perimeter should be hardened by disabling unused services. Disabling unused services makes sure that there are no network services exposed without protection. Remote vulnerability management (**8.8-SO1**) allows to technically perform the hardening. The vulnerability management process (**8.8-SO3**) hardening is performed structurally.
- **Monitoring:** attempts to bypass the access control mechanisms should be monitored. The monitoring objectives allow failed and successful login attempts to be logged and gathered in a SIEM system (**8.15-SO1**). Processes to detect and respond to these alerts are ensured by the security monitoring and incident response objective (**8.16-SO1**). Clock synchronization allows making a reliable timeline of incidents (**8.17-SO1**).

The impact of the unauthorized access is also limited by separating the roles of the SCADA system and central maintenance system (**8.3-SO1**). An attacker who has gained access as the SCADA system cannot change the configuration. An attacker who has gained access as the central maintenance system cannot switch directly.

Defense-in-depth is also provided for the substation inside. Even if an attacker gains access to the substation perimeter, they do not immediately have access to the assets in the substation inside. Often these are the most critical assets, such as the protection configuration. They are protected by network segregation on the substation LAN interface between the perimeter and inside (**8.22-SO2**), by using least privileges to limit the functions that can be accessed on this interface (**8.3-SO4**), and by using a jump host for remote maintenance on the substation inside (**8.22-SO3**).

6.1.2 Protection on the protection and time synchronization interfaces (T-UA3, T-UA4)

To protect against unauthorized access on the protection and time synchronization interfaces, these interfaces should be hardened. Unnecessary network services on the interface should be closed (**8.8-SO2, 8.8-SO3** as explained above). The functions that can be accessed through the remaining services should be restricted to what is needed for normal operations (**8.3-SO4**). Hardening limits the impact by ensuring that attackers with access to the interface can only access the network services used for protection. With these services, they can only switch on the IEDs communicating on these services. They cannot affect other IEDs or manipulate the protection configuration or software and firmware.

On the protection interface (**T-UA4**), additional security is provided by using a private network to restrict access to the interface (**8.21-SO2**) that only allows point-to-point connections between IEDs (**8.21-SO3**). Because of the strict timing requirements for protection, a private network is usually required on this interface. System access control measures are usually not supported for the services used on this interface.

On the time synchronization interface (**T-UA3**), additional security is provided through monitoring. If the time would be changed significantly, this would generate log entries that would be exported to the SIEM system (**8.15-SO2**, **8.15-SO1**). The security monitoring processes would then ensure there is a response (**8.16-SO1**).

6.2 Protection from exploits of software vulnerabilities

For all software exploits threats, hardening is used to prevent vulnerabilities. Patching is used to fix vulnerabilities on the substation perimeter. But it is not as effective on the substation inside, as security updates would have to be applied locally. So, other mitigating measures are used there. See Table 5.

Table 5: Security objectives to mitigate exploits of software vulnerabilities.

Threat	Objectives
T-EX1 Exploit of a software vulnerability on the WAN or remote maintenance interface	*Hardening:* • **8.8-SO1** Remote hardening • **8.8-SO3** Vulnerability management process *Patching:* • **8.19-SO1** Remote software and firmware management • **8.19-SO2** Security updates without disrupting protection functions • **8.8-SO3** Vulnerability management process *Defense in-depth:* • **8.22-SO2** Network segregation on the substation LAN interface • **8.3-SO4** Least privileges on the substation LAN, time synchronization, and protection interfaces • **8.22-SO3** Remote management through a jump host:
T-EX2 Exploit of a software vulnerability on the time synchronization or protection interface	*Hardening:* • **8.8-SO2** Local hardening • **8.8-SO3** Vulnerability management process *Patching:* • **8.19-SO3** Local software and firmware management • **8.8-SO3** Vulnerability management process *Restriction of network access:* • **8.21-SO2** Use of private networks for the protection interface
T-EX3 Malware introduced through engineering laptops	*Hardening:* • **8.8-SO1** Remote hardening

- **8.8-SO2** Local hardening
- **8.8-SO3** Vulnerability management process

Patching:

- **8.19-SO1** Remote software and firmware management
- **8.19-SO2** Security updates without disrupting protection functions
- **8.19-SO3** Local software and firmware management
- **8.8-SO3** Vulnerability management process

Active malware protection:

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

Protection on engineering laptops:

- **8.7-SO2** Protecting engineering laptops against malware

6.2.1 Protection on the WAN and remote maintenance interfaces (T-EX1)

Protection against software exploits against the WAN and remote interfaces is provided through hardening, patching and defense-in-depth. Such strong protection is needed, as these attacks would be the most scalable.

Probably the most important effective is hardening by disabling unused services and enabling security features. The vulnerability management process (**8.8-SO3**) should ensure that unused services are disabled to reduce the attack surface and hence the likelihood of vulnerabilities. It should ensure that security features on the hardware and software platform are enabled to reduce the impact of vulnerabilities. The substation perimeter should allow the hardening to be done remotely (**8.8-SO1**) to make it easy to manage centrally.

If vulnerabilities are still found on the WAN or remote maintenance interfaces, they should be fixed through patching. Efficient patching is made possible on the perimeter through remote software and firmware management (**8.19-SO1**) and ensuring that updates cannot disrupt protection functions (**8.19-SO2**). If they could cause disruptions, the protection would have to be tested locally, and updates would require much more time and effort. The vulnerability management process (**8.8-SO3**) ensures there is a process to perform security updates.

As for the unauthorized access threats, defense-in-depth is provided for the substation inside. Even if an attacker gains access to the substation perimeter through an exploit, the substation inside is still protected by network segregation on the substation LAN interface between the perimeter and inside (**8.22-SO2**), by using least privileges to limit the functions that can be accessed on this interface (**8.3-SO4**), and by using a jump host for remote maintenance on the substation inside (**8.22-SO3**).

6.2.2 Protection on the time synchronization or protection interface (T-EX2)

Protection against software exploits against the time synchronization or protection interfaces is provided only through hardening. The vulnerability management process (**8.8-SO3**) ensures there is a process to disable unused network services and functions and enable security functions. On the substation inside, the hardening may have to be done locally (**8.8-SO2**). As the hardening would only have to be done once (and maybe checked every few years), it should still be feasible.

If vulnerabilities are found in the substation inside, they can still be patched but much less efficiently than in the perimeter. The security updates will need to be applied locally (**8.19-SO3**, **8.8-SO3**), and they may disrupt the protection functions. So, engineers will have to functionally test these functions afterwards. Hence, updates are usually only applied for the highest risk vulnerabilities.

The limited patching is considered acceptable on protection and time synchronization interface, because the attack surface on these interfaces is very small. They only expose specialized network services that would require custom exploits. At the moment there are no known vulnerabilities on such services. Moreover, the protection interface is only reachable from another substation over a private network (**8.21-SO2**).

6.2.3 Protection against malware from engineering laptops (T-EX3)

Malware introduced through engineering laptops could directly enter the substation inside. Hardening can still prevent vulnerabilities (**8.8-SO1**, **8.8-SO2**, **8.8-SO3**), but the attack surface will remain larger than on external interface. Patching can still fix vulnerabilities (**8.19-SO1**, **8.19-SO2**, **8.19-SO1**, **8.8-SO3**), but will only be used for critical vulnerabilities in the substation inside.

Additional protection is hence provided, firstly by protecting the engineering laptops themselves against malware (**8.7-SO2**), and secondly by having active malware protection on commercial off-the-shelf operating systems (**8.7-SO1**), as these are particularly vulnerable to malware.

6.3 Protection from communication threats

As for the unauthorized access threats, the communication threats are handled by the system itself on the WAN and remote maintenance interface and by the operational environment on the protection and time synchronization interfaces.

Table 6: Security objectives to mitigate unauthorized access threats.

Threat	**Protection on underlying network** *(operational environment)*	**Protection by the system** *(substation perimeter)*
T-CM1 Data modification on WAN		**8.20-SO1** Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces
T-CM2 Data disclosure on WAN		**8.20-SO1** Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces
T-CM3 Network denial-of-service attack on the WAN interface	**8.21-SO1** Resilience against denial-of-service attacks on the WAN	**8.20-SO2** Resilience of protection functions against denial-of-service attacks on the WAN and remote maintenance interface **8.22-SO1** Network segregation on the WAN and remote maintenance interfaces
T-CM4 Data modification on the remote maintenance interface		**8.20-SO1** Cryptographic protection of communication confidentiality and integrity

		on the WAN and remote maintenance interfaces
T-CM5 Data disclosure on the remote maintenance interface		**8.20-SO1** Cryptographic protection of communication confidentiality and integrity on the WAN and remote maintenance interfaces
T-CM6 Network denial-of-service attack on the remote maintenance		**8.20-SO2** Resilience of protection functions against denial-of-service attacks on the WAN and remote maintenance interface **8.22-SO1** Network segregation on the WAN and remote maintenance interfaces
T-CM7 Data modification on the time synchronization interface		
T-CM8 Network denial-of-service attack on the time synchronization interface		
T-CM9 Data modification on the protection interface	**8.21-SO2** Use of private networks for the protection interface	
T-CM10 Network denial-of-service attack on the protection interface	**8.21-SO2** Use of private networks for the protection interface	

On the WAN and remote maintenance interface, the confidentiality and integrity of information is protected through cryptographic measures. Availability is provided by network segregation with additional shielding of the protection functions if they are implemented in the substation perimeter. As availability of communication with the SCADA system is particularly important, the WAN network should also be protected at the telecom layer.

For the time synchronization interface, it is difficult to define preventive measures if GPS is used. GPS uses radio communication without cryptographic protection[1]. So, it is possible to do GPS jamming or spoofing attacks. The best solution is to monitor for deviations in the time (**8.15-SO1**, **8.15-SO2**) and respond if these occur (**8.16-SO1**).

For the protection interface, the objectives are for private networks. Because of the strict timing requirements on this interface, it is difficult to protect the communication with cryptographic measures.

6.4 Protection from physical threats

All physical threats are countered by physical security controls (**7.1**, **7.2**, **7.4**, **7.8**, **7.12**), see Section 5.3. The main goal of the technical measure is to limit the impact to one substation (**8.22-SO4**) by blocking unauthorized access form one substation to another.

Table 7: Security objectives to mitigate exploits of software vulnerabilities.

Threat	**Objectives**
T-PH1 Unauthorized physical access in a substation	*Physical security controls:* • **7.1**, **7.2**, **7.4**, **7.8**, **7.12** *Protection of configuration and firmware:* • **8.5-SO3** Authentication with individual passwords for engineers • **8.5-SO4** Role-based authentication for engineers and operators
T-PH2 Unauthorized access from one substation to another substation	*Physical security controls:* • **7.1**, **7.2**, **7.4**, **7.8**, **7.12** *Impact limiting:* • **8.22-SO4** Physical impact limiting to related locations

[1] Cryptographic protection would be possible on other solutions, such as Galileo. But such solutions are still rarely used.

T-PH3 Placing a hardware backdoor at the substation	*Physical security controls:* • **7.1**, **7.2**, **7.4**, **7.8**, **7.12**

The protection configuration and firmware and software of equipment is additionally protected against unauthorized physical access through access control. Engineers with access to the configuration should authenticate with unique credentials in the substation perimeter (**8.5-SO3**) with credentials unique to their role in the inside (**8.5-SO4**). To ensure the authentication is effective, it should be possible to change the keys and passwords after installation of devices or after an incident (**8.24-SO1**, **8.24-SO2**, **8.24-SO3**).

6.5 Protection from supply chain threats

To prevent the firmware or software from being modified during development or the hardware from being modified during manufacturing, the developers and manufacturers of the substation automation system must protect their assets (**5.25**).

To prevent the firmware from being modified during transport, the remote firmware updates on the substation perimeter are protected the firmware with a digital signature (**8.19-SO1**). Software and firmware in the substation inside are protected through a manual process (**8.19-SO4**).

Network segregation between the substation perimeter and the outside (**8.22-SO1**) and between the substation inside and the perimeter (**8.22-SO2**) make it difficult for an attacker to reach the backdoor, even if they succeed in putting it into the firmware.

6.6 Protection from insider threats

Protection against insider threats is provided through people controls, access control, and monitoring.

People controls (**6.1**, **6.2**, **6.3**, **6.4**), such as screening and training, are the most important preventive measure. Engineers need privileged access to configurations and software to do their job. Operators need to be able to switch. So, it is difficult to prevent both groups from taking harmful through technological measures without hindering them in their job.

Risks can be reduced somewhat by separating the roles, so that engineers cannot switch, and operators cannot change the configuration and firmware. This is achieved through role-based access control for engineers (**8.3-SO2**) on the perimeter and role separation on the substation inside (**8.3-SO3**). An account management process (**5.16**, **5.18**) is required to keep the access rights up to date when engineers and operators change roles or organizations.

As the preventive measures are limited, it is important to have a good monitoring and incident response process (**8.16-SO1**). Some unusual behavior by engineers and operators may be detected with monitoring. And if there is an incident the security logs should allow to find out the cause, so that corrective measures can be taken.

To technically support the monitoring and incident response process, security events are logged locally and gathered in a SIEM system (**8.15-SO1** for the substation perimeter and **8.15-SO2** for the inside). Clocks are synchronized to allow making a timeline of an incident (**8.17-SO1**, **8.17-SO2**). And engineers and administrators log in with individual user accounts on the perimeter (**8.3-SO2**), so that actions can be traced to them. Centralizing access control is not yet considered feasible for the substation inside. Logging physical access to substations could be a mitigating measure (**7.2**).

6.7 Protection from post exploitation threats

Protection against the post exploitation threats is provided through backups, monitoring, firmware and software signing, and network segregation.

6.7.1 Protection against loss of configuration (T-PE1)

The main measure to protect against loss of configurations (**T-PE1**), is to store the configurations securely in the central systems and then making backups of this system (**8.13-SO1**). For this approach to work, it must be possible to restore the substation automation system from the configuration file (**8.9-SO1** for the substation perimeter and **8.9-SO2** for the inside).

6.7.2 Protection against software or firmware corruption (T-PE2)

To protect against software or firmware corruption (**T-PE2**), changes to the firmware are logged and can be sent to the SIEM system (**8.15-SO1**, **8.15-SO2** with **8.15-SO1**, **8.15-SO2** for clock synchronization), so that operators can detect unauthorized modifications (**8.16-SO1**). The software and firmware in the substation perimeter are moreover digitally signed (**8.19-SO1**).

If an attacker would install a backdoor, it would be hard to reach because of the network segregation between the substation perimeter and the outside (**8.22-SO1**) and between the substation inside and the perimeter (**8.22-SO2**).

Annex A: Mapping of objectives to threats

To show that all technological security objectives in Section 5.4 are indeed needed to counter the threats, this annex maps them to the threats (Section 3) they are countering according to the rationale in Section 6.

A.1 Objectives for the substation perimeter

The table below shows which threats the objectives for the substation perimeter mitigate.

Objective	***Threats countered***
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by local operators
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	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN

system users to verify the unique identity of the substation.	
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN
8.5-SO3 Authentication with individual passwords for engineers: The substation perimeter enforces mutual authentication for engineers. Engineers use individual passwords or keys. The login procedure is protected against known attacks	• **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-PH1** Unauthorized physical access in a substation
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.	• **T-EX3** Malware introduced through engineering laptops
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-EX1** Exploit of a software vulnerability on the WAN or remote maintenance interface

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.	• **T-PE1** Loss of configurations
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-CM7** Data modification on the time synchronization interface • **T-CM8** Network denial-of-service attack on the time synchronization interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by local operators • **T-PE2** Software or firmware corruption
8.17-SO1 Clock synchronization for the perimeter: The substation perimeter synchronizes time with a central source to have reliable timestamps for security events.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-UA3** Unauthorized access on the time synchronization interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by local operators • **T-PE2** Software or firmware corruption
8.19-SO1 Remote software and firmware management: The software and firmware on devices in the substation perimeter can	• **T-SC2** Hardware modification before installation

be updated through remote access from the central maintenance system. The devices check the authenticity of firmware or software through digital signatures.	• **T-PE2** Software or firmware corruption • **T-EX1** Exploit of a software vulnerability on the WAN or remote maintenance interface • **T-EX3** Malware introduced through engineering laptops
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.	• **T-EX1** Exploit of a software vulnerability on the WAN or remote maintenance interface • **T-EX3** Malware introduced through engineering laptops
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.	• **T-CM1** Data modification on WAN • **T-CM2** Data disclosure on WAN • **T-CM4** Data modification on the remote maintenance interface • **T-CM5** Data disclosure on the remote maintenance interface
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.	• **T-CM3** Network denial-of-service attack on the WAN interface • **T-CM6** Network denial-of-service attack on the remote maintenance
8.22-SO1 Network segregation on the WAN and remote maintenance interfaces:	• **T-CM3** Network denial-of-service attack on the WAN interface

The substation perimeter is segregated from other zones on the WAN and remote maintenance interfaces. Only normal connections are allowed through the network perimeter.	• **T-CM6** Network denial-of-service attack on the remote maintenance • **T-SC1** Software or firmware modification before installation • **T-SC2** Hardware modification before installation • **T-PE2** Software or firmware corruption
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-PH1** Unauthorized physical access in a substation

A.2 Objectives for the substation inside

The table below shows which threats the objectives for the substation inside mitigate.

Objective	*Threats countered*
8.3-SO3 Role separation for engineers and 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.	• **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by 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	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-UA3** Unauthorized access on the time synchronization interface • **T-UA4** Unauthorized access on the protection interface

users that do authenticate themselves, are only available after authentication.	• **T-EX1** Exploit of a software vulnerability on the WAN or remote maintenance interface
8.5-SO4 Role-based authentication for engineers and 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.	• **T-PH1** Unauthorized physical access in a substation
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.	• **T-UA3** Unauthorized access on the time synchronization interface • **T-UA4** Unauthorized access on the protection interface • **T-EX2** Exploit of a software vulnerability on the time synchronization or protection interface • **T-EX3** Malware introduced through engineering laptops
8.9-SO2 Local configuration management: Through local access devices in the substation inside allow to restore the device from a backed-up configuration.	• **T-PE1** Loss of configurations
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, so that they can be analyzed to detect incidents.	• **T-UA3** Unauthorized access on the time synchronization interface • **T-CM7** Data modification on the time synchronization interface • **T-CM8** Network denial-of-service attack on the time synchronization interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by local operators

	• **T-PE2** Software or firmware corruption
8.17-SO2 Clock synchronization for the perimeter: The substation inside synchronizes time with a central source to have reliable timestamps for security events.	• **T-UA3** Unauthorized access on the time synchronization interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by local operators • **T-PE2** Software or firmware corruption
8.19-SO3 Local software and firmware management: Through local access devices in the substation inside allow to update their software or firmware.	• **T-EX2** Exploit of a software vulnerability on the time synchronization or protection interface • **T-EX3** Malware introduced through engineering laptops
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-EX1** Exploit of a software vulnerability on the WAN or remote maintenance interface • **T-SC1** Software or firmware modification before installation • **T-SC2** Hardware modification before installation • **T-PE2** Software or firmware corruption
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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface

	- **T-EX1** Exploit of a software vulnerability on the WAN or remote maintenance interface
8.24-SO2 Local key and password management: Through local access devices in the substation inside allow to update all passwords and keys.	- **T-PH1** Unauthorized physical access in a substation

A.3 Objectives for the operational environment

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

Objective	***Threats countered***
8.7-SO2 Protecting engineering laptops against malware: If engineering laptops are used for local maintenance to the substation, these are strongly protected against malware.	• **T-EX3** Malware introduced through engineering laptops
8.8-SO3: Vulnerability management process: The grid operator manages vulnerabilities in the 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	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-UA3** Unauthorized access on the time synchronization interface • **T-UA4** Unauthorized access on the protection interface • **T-EX1** Exploit of a software vulnerability on the WAN or remote maintenance interface • **T-EX2** Exploit of a software vulnerability on the time synchronization or protection interface • **T-EX3** Malware introduced through engineering laptops

8.13-SO3 Backup process for device configurations: The grid operator has a process to back up the configurations of the devices 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.	• **T-PE1** Loss of configurations
8.16-SO1: Security monitoring and incident response: The grid operator monitors security events on the device and can respond to them. They gather security logs from the 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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-UA3** Unauthorized access on the time synchronization interface • **T-CM7** Data modification on the time synchronization interface • **T-CM8** Network denial-of-service attack on the time synchronization interface • **T-IN1** Harmful actions by engineers • **T-IN2** Harmful actions by local operators • **T-PE2** Software or firmware corruption
8.19-SO4 Manual integrity checks for substation inside: There is a process to manually check the integrity and authenticity of firmware and software before installing it on equipment in the substation perimeter.	• **T-SC1** Software or firmware modification before installation
8.21-SO1 Resilience against denial-of-service attacks on the WAN: The wide-area network (WAN) is resilient against denial-of-service attacks or accidental disruptions. The impact of such attacks is minimized. The	• **T-CM3** Network denial-of-service attack on the WAN interface

telecom provider monitors the network and can respond in case of an incident.	
8.21-SO2 Use of private networks for the protection interface: The grid operator uses private networks for the protection interface.	• **T-UA4** Unauthorized access on the protection interface • **T-CM9** Data modification on the protection interface • **T-CM10** Network denial-of-service attack on the protection interface
8.21-SO3 Point-to-point connections on the protection interface: The networks on the protection interface only allow point-to-point connections between the devices that need to communicate with each other.	• **T-UA4** Unauthorized access on the protection interface
8.22-SO4: Physical impact limiting to related locations: Communication between substations and from substations to the central system is restricted to what is needed, so that the impact of a physical compromise of one substation is limited.	• **T-PH2** Unauthorized access from one substation to another substation
8.24-SO3 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.	• **T-UA1** Unauthorized access as the SCADA or central maintenance system on the WAN • **T-UA2** Unauthorized access as an engineer on the remote maintenance interface • **T-PH1** Unauthorized physical access in a substation

Glossary

APN	Access Point Name
CVSS	Common Vulnerability Scoring System
EST	Enrollment over Secure Transport
ISMS	Information Security Management System
MV	Medium Voltage
PKI	Public Key Infrastructure
RADIUS	Remote Access Dial-In User Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Incident and Event Management
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

References

[1] ENCS, "SA-211-2022: IEC 62443 security requirements for substation automations system," 2022.

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

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