DR-201-2020

Security measures for DER systems

Version 0.2

9 December 2020

This document was produced in the ENCS project on distributed energy resources (DER) security, which supports grid operators and parties with roles in the wind or solar systems in selecting and implementing technical security measures for distributed systems, wind farms, solar parks, and their components. The document is part of a set of requirements available through the ENCS portal (https://encs.eu/documents):

Smart metering	SM-301-2019: Security requirements for procuring smart meters and data concentrators
Distribution automation	DA-101-2019: Security risk assessment for distribution automation systems DA-201-2019: Security architecture for distribution automation systems DA-301-2019: Security requirements for procuring distribution automation RTUs DA-390-2019: Market survey on distribution automation RTU security DA-401-2019: Security test plan for distribution automation RTUs
Substation automation	SA-101-2019: Security risk assessment for substation automation systems SA-201-2019: Security architecture for substation automation systems SA-301-2019: Security requirements for procuring substation gateways SA-302-2019: Security requirements for procuring IEDs SA-303-2019: Security requirements for procuring HMI software
Electric vehicles	EV-101-2019: Security risk assessment for EC charging infrastructure EV-201-2019: Security architecture for EV charging infrastructure EV-301-2019: Security requirements for procuring EV charging stations EV-401-2019: Security test plan for EV charging stations
Distributed energy resources	DR-101-2020: Risk assessment for DER security DR-201-2020: Security measures for DER systems DR-301-2020: Procurement requirements for DER controllers WP-027-2020: Security measures for grid operators connecting to DER WP-029-2020: Why cybersecurity is critical for DER systems and how to protect them

This document is shared under the Traffic Light Protocol classification:

TLP White – public

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

ENCS

Version History

Date	Version	Description
26 May 2020	0.1	Initial draft for internal and external review
9 December 2020	0.2	Partial revision after the reviews

Table of Contents

1 Introduction

Europe uses distributed photovoltaic systems to such a degree that the sudden loss or repeated disconnection and connection of a significant amount can severely affect the electricity grid. The security of these systems is mostly unknown. Still, a coordinated cyberattack on thousands of systems can have that impact. Professional attackers like nation-states can be motivated and capable of doing this, with communications and central systems that can remotely access large field locations being at greater risk.

The attackers can also target utility-scale systems like wind farms or solar parks to reach a similar impact with only about a dozen of the largest systems.

This document recommends security measures for distributed systems, wind farms, and solar parks, including a set of technical measures that those designing and maintaining these systems can use to mitigate security risks in [1]. These measures consider the different architectures between smaller systems and larger systems, and the tens of megawatts threshold from which wind farms, solar parks, or central systems controlling or configuring distributed systems can become targets for attackers.

We assume there is an information security management system (ISMS) in operation. The measures can be used to implement this ISMS or to improve an existing one. This is the same approach used by grid operators, contributing to harmonizing the security effort in the energy sector.

The measures are aligned with the objectives from the ISO/IEC 27001:2013 [2] standard, which is commonly used for ISMSs, including those of multiple grid operators. They also consider the additional guidance provided by the ISO/IEC 27019:2017 [3] standard for the energy utility industry. Each subsection gives the relevant technical security measures to meet an objective in the ISO/IEC 27001 Annex A. The following topics are covered:

- Access control (A.9)
- Cryptography (A.10)
- Physical and environmental security (A.11)
- Operations security (A.12)
- Communication security (A.13)
- Information security aspects of business continuity (A.17)

Additional security measures to the digital connection between these systems and grid operator systems are available in [2].

1.1 Objective

This document provides guidance on technical measures for securing distributed photovoltaic systems, wind farms, and solar parks. It can be used in an ISMS implementation, or to choose a set of measures that can reduce specific risks.

1.2 Scope

The security measures cover the risks to distributed photovoltaic systems, wind farms, and solar parks, including the field location, the central systems, and the communications between them. The risks have been defined in [1], with a summary being provided in Section 1.3. The measures apply to the reference architectures in Section 1.4.

With the focus of this document being technical information assets, additional measures might be needed to cover non-technical information assets. Therefore, wind or solar parties implementing an ISMS are recommended to cover the following scope, either by itself or as a part of a larger scope.

"Information Security Management System (ISMS) protects the confidentiality, integrity, and availability of the information needed to operate and maintain all field locations of the party, which can be local and from a remote location."

Its formal definition is aligned with the generic scope agreed by grid operators in [5]. If implemented correctly, it will help to harmonize the security effort in the energy sector.

ISMS implementations following the ISO/IEC 27001:2013 [2] and 27019:2017 [3] standards can use the guidance more easily due to the alignment of the security measures with the objectives in ISO/IEC 27001:2013 Annex A.

Additional security measures for the digital connection to grid operator systems are covered in [6]. They should be used to complement this document for the cases in which the connection exists.

1.3 Risks mitigated

The security measures primarily aim at protecting field locations from malicious control or configuration by malicious threats, which might be tried through the communications and central systems for distributed systems, wind farms, and solar parks, and also through local and physical attacks for larger wind farms and solar parks. The ultimate goal is avoiding the attackers to compromise a significant amount of field locations that can disrupt the electricity grid and, through it, society. The measures protect availability, integrity, and confidentiality in the attack paths that might lead to this scenario.

The measures protect in different ways against advanced attacks by professional actors, traditional IT attacks, insiders, and non-malicious threats. Professional attackers like

nation-states can have unlimited resources. Therefore, not all attacks can be prevented, but they can be made more difficult and their impact can be reduced. Attacks by malicious employees or mistakes by authorized personnel can be impossible to prevent, but they can be detected and their impact can also be reduced. Traditional IT attacks can be mostly prevented with the measures isolating the OT systems from IT systems as much as possible. Multiple natural events are also impossible to prevent, but their impact can be reduced with redundancy and recovery measures on information, systems, and locations.

Additional details on the threats mitigated and the links between risks and measures can be seen in [1].

1.4 Reference architecture

The security measures apply to different reference architectures for distributed systems and utility-scale systems. Figure 1 represents the architecture of distributed systems like residential, commercial, or industrial photovoltaic systems. Figure 2 represents utility-scale systems like wind farms or solar parks.

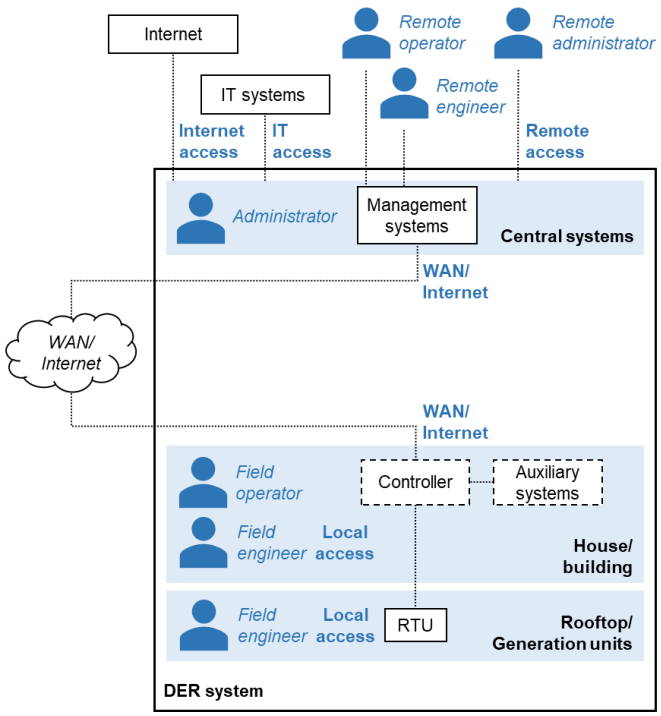

Figure 1: Reference architecture for DER.

- Typically, the controller and auxiliary systems exist in commercial and industrial systems.
- Auxiliary systems: weather station.
- Often, the controller or RTUs (e.g., PV inverters) support local management through wireless from mobile apps.
- The management systems can be local or remote, supporting at least system monitoring and maintenance.
- The owner, in the role of operator, monitors the system to ensure a high return on investment. He can do this locally or remotely. He can delegate this function to O&M providers.
- O&M providers fill in the roles of operators or engineers.

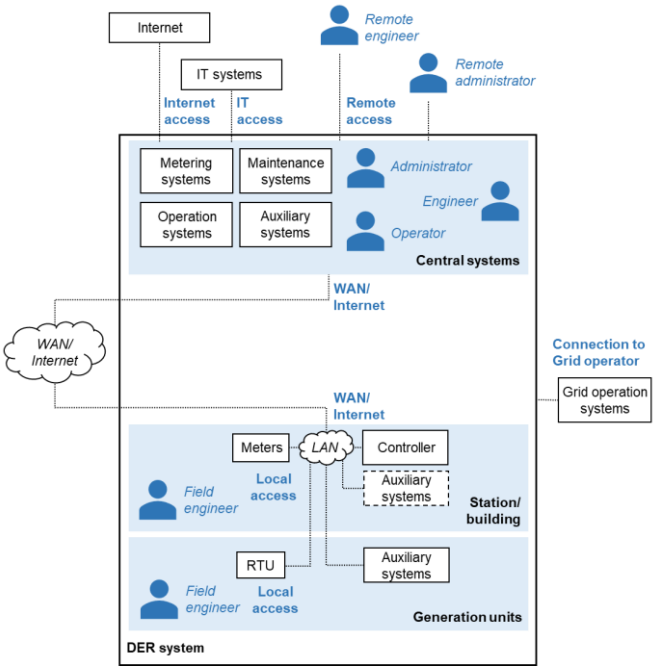

Figure 2: Reference architecture for wind farms and solar parks.

- There can be different central systems, local or remotely hosted by different parties, supporting at least system operation and maintenance.
- Central operation system: SCADA servers, operation workstations, historian.
- Maintenance system: engineering/ administrative/ security servers, jump servers, workstations.
- Auxiliary systems in wind: ice detection, bird protection, shadow mitigation.
- Additional parties like asset managers, metering point operators, direct traders, aggregators, or the military might also take the roles of operators or engineers.
- The station area can be in the grid operator substation that connects electrically to the generation system.

Distributed systems tend to have a simpler architecture, with most central functions being concentrated in one central system, and the components connecting directly to each other in the field location. Utility-scale systems can have different central systems, and there can be a network connecting the local components in the field location. We refer to the station, house, rooftop, and generation units generically as field location.

The users are referenced in the access control measures in Section 2. The interfaces are referenced in the communication security measures in Section 6.

1.5 Checklist for additional measures

All measures apply to all central systems and field locations unless the measures or this section provide exclusions or redefinitions for specific cases. Some measures do not directly apply to all cases because:

- We used the architecture in Figure 2 as a starting point for the measures because most wind farms and solar parks are over the tens of megawatts threshold. However, some measures need adjusting to apply also to the architecture for distributed systems in Figure 1.

- Central systems and field locations over the tens of megawatts threshold need stronger protection than those under the threshold. Therefore, some remarks become mandatory for cases over the threshold, while some mandatory parts become recommendations for cases under the threshold.
- Some measures might not be supported on legacy equipment, requiring alternatives.

The list below contains the exclusions and redefinitions for the earlier cases:

- **AC6:** central systems over the ten megawatts threshold supporting remote operation must also have specific roles for these users, allowing them to first establish secure connections to the central systems, and then to access an operation workstation through a jump server, or to access a read-only interface of the operating system or management system. Central systems under the threshold must at least differentiate between the roles of operators, engineers, and administrators.
- **AC7:** not applicable to central systems with only one field location (e.g., a central system hosted in a field location for that location only).
- **AC15:** central systems supporting remote operation must also apply two-factor authentication to the remote operators.
- **AC18 and AC25:** apply only to field equipment in field locations over the tens of megawatts threshold that communicates with an access control server in the central maintenance system. Field operators must also be included if the local operation is supported. Remote maintenance on legacy field equipment in field locations over the threshold that does not support centralized access control is done through jump servers at the central maintenance systems as described in CM4.
- **AC20:** applies only to field locations over the tens of megawatts threshold.
- **AC26:** the local passwords of field operators must also be protected by the equipment if the local operation is supported. However, there are no requirements on how the local passwords are saved by operators and engineers for field locations under the tens of megawatts threshold.
- **CR3:** the passwords and keys of all field equipment in field locations below the tens of megawatts threshold can be updated only when there is suspicion or evidence that they have been compromised. The updates are made through the LAN or local access interface if there is no central maintenance system or local engineering station. Field locations over the threshold must comply with the full requirement.

- **PH4:** if a central system is hosted in a field location, covering only that field location, then the physical security measures of the data center can be at the same level of security as those of the field equipment. Additionally, at least the central systems, if any, and field equipment in field locations over the tens of megawatts threshold must have back-up power supplies, and the behavior of visitors must be monitored through CCTV.
- **PH5:** field locations over the tens of megawatts threshold must be guarded by security personnel, and access authorization must match, as much as possible, the schedules and participants in the planned interventions and incident response plans.
- **PH7:** a field location under the tens of megawatts threshold can have only tamper evidence, while field locations over the threshold must provide tamper detection capabilities through the central systems.
- **OP3, OP6, OP11, OP13, and OP15:** the activities monitoring resources, collecting logs, doing back-ups and updates, and the application of hardening measures must be executed through the LAN of the field location or local access interface if the field equipment is not remotely maintained through a central maintenance system.
- **OP3, OP4, OP11, OP13, OP15 to OP18:** if legacy field equipment cannot be monitored, protected against malware, provide security logs, apply security updates or it does not allow to manage technical vulnerabilities, then its security must rely on access control measures (Section 2) and communication security (Section 6).
- **CM1 and CM2:** field locations over the tens of megawatts threshold must use dedicated wired connections or, if this is impossible, at least a dedicated logical connection, such as an APN. Field locations below the threshold must use at least a dedicated logical connection or, if this is impossible, at least secure protocols when communicating to a central system.
- **CM2:** if legacy field equipment cannot support cryptographic integrity and confidentiality protection measures at the application layer, then they are still applicable at the network layer.
- **CM3**: field locations with an internal network must have a perimeter network-based firewall. It can be integrated with the gateway router for field locations below the tens of megawatts threshold or, if this is impossible, at least a host-based firewall when communicating with a central system. Penetration tests to the firewalls must be regularly made for field locations above the tens of megawatts threshold.

- **CM1 to CM9:** legacy field locations that cannot comply with these requirements must be refurbished quickly if they are over the tens of megawatts threshold.
- **BC1:** does not apply to legacy equipment in field locations below the tens of megawatts threshold, which should still comply with the access control measures (Section 2) and communication security measures (Section 6). If legacy equipment at field locations over the tens of megawatts threshold cannot comply with this requirement, they should be replaced quickly.
- **BC2:** central systems and field locations over the tens of megawatts threshold must comply with this requirement. Central systems or field locations below the threshold do not need to comply.
- **BC3:** central systems over the tens of megawatts threshold must comply with this requirement.
- **BC4**: field locations over the tens of megawatts threshold must comply with this requirement.

Using the measures

These security measures are part of a bigger approach to creating secure systems, both when building new systems and when updating existing systems. It consists of the following steps:

1. Perform a **security risk assessment** to understand the threats to the system and the impact these can have. An assessment of the risks associated with distributed photovoltaic systems, wind farms, and solar parks is available in [1]. A risk assessment for the digital connection with grid operator systems is available in [4].
2. Design a **security architecture** that selects technical security measures to mitigate the risks. Measures are chosen for the whole system, as this is usually more effective than choosing measures per component. The architecture can act as a blueprint for system integrators and the departments maintaining the system. This document recommends security measures for distributed photovoltaic systems, wind farms, and solar parks. These are mapped to the IEC 62443-3-3 standard [7], used by some vendors, in Appendix A. Security measures covering the digital connection with grid operator systems are available in [6].
3. Derive **security requirements for components** from the security architecture that can be used to develop or procure the components. Security requirements for controllers are available in [8].
4. **Test the components** to check that they meet the security requirements. In a procurement process, such tests should be part of the selection phase.
5. **Test the system** once it is deployed to check that it is implemented according to the architecture and mitigates the risks. The configuration of the network and devices can be checked using a technical audit. Mitigation of the risks can be checked using penetration and red team tests simulating the threats.

These steps ensure that a secure system is delivered. After that, it still needs to be operated securely. Processes and procedures should be set up to securely maintain the system, manage keys and passwords, and respond to incidents.

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

2 Access control

The security measures provide a way to manage access rights and to implement authentication for all user groups. Most measures are defined considering only the external interfaces of the systems. However, they should also be considered for the interfaces between the internal system components.

2.1 Central systems

The central systems enforce access control for the user groups in Table 1. Both human users and other systems accessing the system are considered users.

Table 1: User groups on the central systems.

System	User	Required access	Interface
Operation system (local or remote)	Controller or Generation units (e.g., inverters, RTUs, etc.)	• Send event data • Report status of command execution	Central system LAN WAN/Internet
	Control center operator	• View electricity data from his responsibility area • Execute control commands within his responsibility area, according to scheduled activities or incident response plans	Central system LAN
Central auxiliary system (local or remote)	Local auxiliary systems	• Send asset condition or environmental safety data	Central system LAN WAN/Internet
	Remote engineer	• View asset condition or environmental safety data from his responsibility area	Remote access Central system LAN

	Control center operator Engineer		
Maintenance system	Remote engineer Engineer	• Configure field equipment • Maintain field equipment • Monitor field equipment • Collect additional data	Remote access Central system LAN
Metering system	Meters	• Send metering data	WAN/Internet
	Metering entity personnel	• Ensure the availability and quality of the metering data	Central system LAN
All systems	Remote administrator Administrator	• Maintain systems and components	Remote access Local maintenance
All systems	Other systems	• Collect data for further processing	Central system LAN

The operation and engineering workstations are assumed to be in a central, secured area (see PH3 in Section 4.1).

2.1.1 User access management [A.9.2]

The central systems manage access rights in such a way that the principle of least privileges can be implemented. As a result, the users are only allowed to access the functions and data they need.

AC1: Mandatory access control for field equipment and other systems

The central systems enforce mandatory access control for field equipment and other systems based on access rights to functions and data.

Access rights, user accounts, and the assignment of access rights to user accounts are managed by the administrators in each endpoint.

AC2: Centrally managed, role-based access control for operators, engineers, and administrators

The central systems enforce role-based access control for operators, engineers, and administrators with centrally managed accounts:

- users log in with individual accounts;
- a central access control server determines their role;
- the endpoint accessed enforces the access rights of that role.

Roles, individual user accounts, the assignment of roles to accounts, and policies on password complexity, length, and lifetime are managed by the administrators in the central access control server. The access rights and their assignment to roles are managed by the administrators in each endpoint.

The user accounts and their roles are reviewed periodically and whenever there are changes to the functions of the users within the organization.

Remarks: The central access control server can be shared with other OT systems, but it should not be shared with the IT systems. Further, the second level of role management is recommended for the operation system, using different access control servers and administrators than the first level.

AC3: Schema-based access to databases

Access rights on databases restrict access to schemas that in turn restrict access to database objects. Restrictions on writing and read-only access to the database objects can be managed at the schema level.

Remarks: This applies to the databases that are inside a system and accessed by other components of that system. Access to the objects of external databases should first need access to the hosts or applications of the system where the database is hosted.

AC4: Different access rights on central systems for accessing their own functions and data and for accessing those of the business processes

The central systems allow either write or read-only access rights on functions and data. Further, the access rights on functions and data of the endpoint itself, such as writing or reading its configuration, are different than the access rights on the functions and data of the business process, such as sending a command to a field location or viewing its data.

AC5: Different roles for accessing hosts and for accessing the applications inside

The roles restrict the access of users to hosts and applications. A user can access only the hosts that are defined in his roles, such as an operator workstation. In the hosts, he can access only the applications that are defined in his roles, such as a SCADA client. He logs out of the applications and hosts before leaving his virtual or physical workspace.

AC6: Indirect access to critical or sensitive central components and field locations

The roles assigned restrict:

- The control center operators to monitor and control the field locations through operation workstations in the central operating system.
- The engineers to maintain the field equipment through maintenance workstations or jump servers in the central maintenance system.
- The administrators to use admin workstations or jump servers whenever possible to maintain the central systems.
- The remote engineers and administrators to use a secure connection to the central maintenance system network and jump servers when they maintain the central systems or the field equipment, respectively, from outside a central secured area.

Communications between the central system components are restricted (see CM4 and CM5 in Section 6.1).

AC7: Area-based access to central components and field locations

The central systems restrict the access of users to only one or a subset of field locations.

The systems that allow access to a set of field locations can be physically separated from the systems that allow access to other field locations and the operation or engineering teams that are assigned to each set are different and unrelated. For instance, this is the case when the operation, auxiliary, or maintenance systems are hosted at field locations.

Otherwise, the restrictions are enforced on the communications (see CM5 and CM7 in Section 6.1) and on role assignment, as follows. Each operator or engineer is assigned an area of responsibility containing a subset of field locations that he can access. His user account is assigned only roles with access rights on the functions and data of the hosts and applications that are assigned to field locations in that area. The roles must enable the exact access that the user needs with a combination of write or read-only rights to operate or maintain each equipment in each field location.

Remarks: Each area should always correspond to the smallest possible subset of field locations. The whole set should be visible in the grouping of all areas of responsibility.

Each user can be assigned higher privileged access rights to an area of responsibility and lower privileged access rights to additional areas if needed. For instance, an operator can execute commands in his main area of responsibility, and he can only view the field locations in other areas.

AC8: Validation of configuration changes and command execution

The operation, maintenance, and administration processes allow the execution of configurations or control commands only according to scheduled work or incident response plans.

The host or application always prompts the user for confirmation of the intended action.

Remarks: Only operators should have command execution rights, or the central systems should validate all the control commands executed by engineers against scheduled work orders. Only the valid commands should be processed further.

AC9: Manual assignment of access rights and roles

New access rights and roles can be assigned only manually to user accounts or centrally managed user groups.

New centrally managed user accounts can be assigned automatically to only the access rights or roles that allow the users to renew their cryptographic material, such as passwords or keys.

AC10: Asset owners are involved (also) in the assignment of access rights

The administrators assign access rights to user accounts at the request of the owner of the field location or other system that needs the access, but only after validating with the owner of the system accessed and ensuring compliance with the data protection and information security policies.

AC11: Review of the assigned access rights triggered (also) on system changes

The access rights that are assigned to user accounts or roles are reviewed when there are changes in the functions or data of the system or endpoint accessed.

AC12: Contingency local accounts for administrators

The system components provide local accounts that the administrators use to log in if the central access control server is not reachable.

Remarks: The access to the local accounts can be managed with privileged access management (PAM) platform. The platform itself enforces role-based access control for the administrators that are used when the contingency allows. It also has local accounts that the administrators can use otherwise.

The PAM platform can be shared with other OT systems, but it should not be shared with the IT systems.

2.1.2 System and application access control [A.9.4]

The central systems enforce authentication for all their users.

AC13: Machine-to-machine authentication for field equipment and other systems

The central systems use mutual authentication with passwords or keys for field equipment and other systems. The administrators and the engineers change the passwords or keys at the central systems and the field equipment, respectively. They protect against compromises of the keys and passwords by:

- using unique passwords or keys for all endpoints;
- generating them randomly with enough entropy to resist brute-force attacks or enforcing these properties when they are set by a user.

Remark: Authentication can be implemented using a virtual private network (VPN) or transport layer security (TLS) (see CM2 in Section 6.1) with client-side certificates or passwords. For the communication between the operating system and the field locations, it can comply with the specifications in IEC 62351-3 [7] and IEC 60870-5-7 [8].

Passwords and keys are updated according to measure CR3 (see Section 3.1).

AC14: Authentication using individual passwords for operators, engineers, and administrators using centrally managed accounts

The central systems require operators, engineers, and administrators to log in with individual passwords. The login procedure is protected by:

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

Users can change their own passwords through a client to the central access control server. The server enforces policies on password reuse, entropy, and lifetime, making the users choose strong passwords and update them regularly. They are also trained on how to create strong passwords (see CR2 in Section 3.1), how to keep them, not to share them, and to log out before leaving their virtual or physical workspace. In the central access control server, the passwords are stored salted and hashed in such a way that the original password cannot be seen or recreated.

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

AC15: Two-factor authentication for remote access by remote engineers and administrators

The central maintenance system requires the remote engineers and administrators to log in on individual accounts using two-factor authentication when they access the central systems or field equipment, from outside a central secured area.

Remarks: The control center, network operations center (NOC), security operations center (SOC), and similar locations are considered secure areas (see PH3 in Section 4.1).

Two-factor authentication may be implemented at the network layer by having remote engineers and administrators set up a virtual private network (VPN) connection (see CM2 in Section 6.1) with their own passwords and client-side certificates to the central maintenance system network.

AC16: Secure storage of local accounts passwords for administrators

The administrators log in to local accounts with shared passwords when system components cannot reach the central access control server. The components enforce the users to choose strong passwords with high entropy, and they store them salted and hashed in such a way that the original password cannot be seen or recreated.

The administrators keep a record of the passwords in only an encrypted file or dedicated database in the admin servers, where they must always be accessible through at least one admin workstation. The file or database is also protected by a strong password or key. These are known to only the administrators that are responsible for keeping the records up to date. Further, they are stored in a physical vault inside a secured area, together with the local passwords of the hosts that are in their access path. The other administrators can only get to know them in a contingency, and they are updated after the contingency is over.

Remarks: Unique passwords should be used by equipment or, at least, by service and its role in that.

It is recommended to use a password hashing function that is resistant against GPU cracking attacks, such as Argon2 or PBKDF2, in the central system components.

The admin server that stores the passwords can be part of the PAM platform mentioned in AC12. The platform can log in to the endpoints for the administrators, hiding the passwords from them. It can also make passwords unique by the equipment. If the administrators need to know a password, then it must be updated by the platform after the contingency is over.

This component of the platform can also be shared with other OT systems, but it should not be shared with the IT systems.

2.2 Field equipment

The field equipment enforces access control for the user groups in Table 2. Both human users and other systems accessing the field equipment are considered users.

Table 2: User groups on the field equipment.

Field equipment	User	Required access	Interface
Controller or Generation units (e.g., inverters, RTUs, etc.) (if there is no controller)	Operation system (local or remote)	• Collect electricity measurements • Send control commands	Central system LAN WAN/Internet
	Field operator	• Monitor the generation • Execute simple control commands	Field location LAN Local access
Generation units (e.g., inverters, RTUs, etc.)	Controller	• Collect electricity measurements • Send control commands	Field location LAN
Local auxiliary system	Central auxiliary system (local or remote)	• Collect asset condition or environmental safety data	Local auxiliary system LAN WAN/Internet
Meters	Metering system	• Collect metering data	WAN/Internet
All equipment	Central maintenance system (local or remote), or engineers through it	• Configure and maintain the field equipment	Local maintenance system LAN WAN/Internet

All equipment	Field engineers	• Configure and maintain the field equipment	Local maintenance

The local maintenance interface is usually an Ethernet port, serial port, or optical port on the field equipment. The field engineers connect their laptops to this port and can configure the equipment using specialized management software or a web interface.

2.2.1 User access management [A.9.2]

The field equipment manages access rights in such a way that the principle of least privileges can be implemented. As with the central systems, the users are only allowed to access the functions and data they need. However, centrally managed, role-based access control is not mandatory for field equipment that does not communicate with the central maintenance system directly.

AC17: Mandatory access control for central systems and other field equipment

The field equipment enforces mandatory access control for the central systems and other field equipment based on access rights to functions and data.

Access rights, user accounts, and the assignment of access rights to user accounts are managed by the engineers in each equipment.

Remark: There are no requirements on how the user accounts and their access rights are managed. They may be static and only be changeable through software updates (see OP13 in Section 5.5).

AC18: Centrally managed, role-based access control in boundary equipment for engineers

The field equipment that communicates directly with the central maintenance system enforces centrally managed, role-based access control for engineers as described in AC2. However, the access rights and their assignment to roles are managed by the engineers in each endpoint.

Remarks: Field equipment can check an engineer's access rights using different technologies. A method that works with the existing systems should be chosen. It is recommended to use RADIUS or LDAP over TLS as specified in IEC 62351-8 [6].

AC19: Different access rights on field equipment for accessing their own functions and data and for accessing those of the business processes

The field equipment separates access rights as described in AC4. For instance, writing or reading the configuration of the controller needs different access rights than controlling a generation unit or viewing its data.

AC20: Indirect local access to the equipment in field locations

The field engineers avoid using the LAN or local interfaces of the field equipment as much as possible. Instead, they try to access the equipment through a local engineering station (see CM7 in Section 6.1).

Remark: The local engineering station should be behind a firewall. The access through the LAN should use a DMZ that could be behind the same firewall. The local engineering station and the DMZ (firewall) should enforce centrally managed, role-based access control for the field engineers.

AC21: Manual assignment of access rights and roles

The field equipment restricts the automatic assignment of access rights and roles as described in AC9.

AC22: Process owners are involved (also) in the assignment of access rights

The engineers assign access rights to user accounts at the request of the owner of the central system that needs the access, but only after assessing any possible impacts, validating with the operators or the metering entity in case their processes are involved, and ensuring compliance with the data protection and information security policies.

AC23: Local accounts for contingency, equipment that cannot communicate with the central maintenance systems, and legacy equipment

The field equipment provides local accounts that the engineers can use to log in only if:

- it cannot reach the central access control server;
- the architecture design does not allow it to communicate with the central maintenance system;
- it does not support centralized role-based access control.

Remarks: The access to the local accounts can be managed with the same PAM platform mentioned in AC12 to provide remote access through the central maintenance system to boundary equipment. The platform itself enforces role-based access control for the remote engineers.

This component of the PAM platform can also be shared with other OT systems, but it should not be shared with the IT systems.

2.2.2 System and application access control [A.9.4]

The field equipment enforces authentication for all its users.

AC24: Machine-to-machine authentication for the central systems and other field equipment

The field equipment uses mutual authentication with passwords or keys for the central systems and other field equipment as described in AC13.

AC25: Authentication using individual passwords for engineers using centrally managed accounts

The field equipment that communicates directly with the central maintenance system requires local engineers to log in with individual passwords as described in AC14.

AC26: Secure storage of local accounts passwords for engineers

The engineers log in to local accounts with shared passwords in the conditions listed in AC23. The local passwords are protected as described in AC16, but the encrypted file or dedicated database is stored in the central engineering servers, where it must always be accessible through at least one engineering workstation. The password or key to the file or database is known to only the engineers. The engineers can get to also know the local accounts of the hosts that are in the access path to the file or database in contingency, and they are updated as soon as possible after the contingency is over.

The field engineers use remote access to the central maintenance system from the field location to access the local passwords they need, or they get them through an authorized colleague if the remote access is not functioning properly.

Remarks: Unique passwords should be used by service and the role of the equipment in that or, at least, by field location.

The file or database can be in the same PAM platform as the local passwords of the central systems. The platform can log in to the boundary equipment for the remote engineers, hiding the password from them. It can also make the password unique for this equipment, at least.

Access to the local passwords can be provided by an engineering service supporting field operations if the remote access to the central maintenance systems is not functioning properly.

3 Cryptography

Several security measures use cryptography:

- Machine-to-machine authentication for various users (Section 2);
- Hashing passwords used by human users (Section 2);
- Digitally signing the firmware (Section 5.5);
- Protecting the confidentiality and integrity of communication (Section 6.1).

Additional measures need to be taken to make their use effective.

3.1 Cryptographic controls [A.10.1]

Strong cryptographic keys, algorithms, and passwords are used to protect against attacks on the cryptography itself. It must be possible to replace compromised passwords and keys.

CR1: Strong cryptographic keys and algorithms

The central systems and field equipment apply cryptography according to regulations and modern guidelines:

- Algorithms and protocols are selected according to expert recommendations, such as those from the ECRYPT project [9];
- Key lengths and other parameter are chosen to resist attacks over the infrastructure's lifetime;
- Random numbers used for security are generated with a cryptographic pseudo-random number generator, following the requirements in Section 3.2.3 of the ECRYPT report [9];
- When certificates are used for authentication, the validity of the certificate is checked, and the provided identity is used to determine authorizations.

Remark: Legacy equipment must be configured to comply with the above, or to approach it as much as possible, according to what they support.

CR2: Strong passwords

The uniqueness, randomness, entropy, and lifetime of passwords vary with how they are used, as described in Sections 2.1.2 and 2.2.2. Nevertheless, they must always comply with the existing password policy.

Remarks: The password policy can build on the baseline provided in Section 5 of the NIST SP 800-63B [13].

CR3: Update of passwords and keys

The administrators and the engineers use the tools provided by the central maintenance system to update the passwords and keys in the central components and the field equipment, respectively. It follows a process that meets the following requirements:

- New keys and passwords comply with CR1 and CR2, respectively;
- The confidentiality and integrity of passwords and keys are cryptographically protected during transport;
- If public-key cryptography is used, the components can use certificates issued by the public key infrastructure (PKI) in the central maintenance systems.

The update is made through remote access for the central systems and boundary field equipment. It is made through the local access interface, LAN, or local engineering station for the field equipment that cannot communicate with the central maintenance system.

Updates are performed according to the existing update policy. Key users are notified if the passwords or keys are changed during an incident response process.

Remarks: The passwords and key updates to the equipment that does not communicate with the central maintenance system could be made through a local engineering station that has access to both.

When public-key cryptography is used, keys are preferably updated using an automated process between the endpoints and the central maintenance servers.

The PKI or CA can be shared with other OT systems, but it should not be shared with the IT systems. Otherwise, system components that communicate with different systems, with each using a different CA, must have the root certificates from each CA or a root certificate that is common in their certification paths.

The central systems and field equipment do not need to be able to use certificates from the PKI in the central maintenance system for the certificate used to verify firmware updates (see OP14 in Section 5.5). This certificate is issued by the vendor through a secure process.

4 Physical and environmental security

Physical security is provided by the perimeter protection of control centers, data centers, field locations, base stations, and generation units. The field equipment is placed in a protective cabinet to prevent tampering.

4.1 Secure areas [A.11.1]

The control centers, data centers, or base stations covering several field locations, that house the central systems are protected against advanced threats. Base stations housing central systems dedicated to one field location, or only field equipment, are protected against at least lesser threats.

PH1: Secure design or choice of central systems facilities

The entities responsible for the central systems avoid hosting locations that are more susceptible to natural or manmade disasters. It includes selecting an existing building, a site for construction, buying or renting a building, and using a third-party infrastructure such as a cloud.

Remarks: In the third-party case, the provider should be asked to describe where the data centers are located, what environmental risks they are exposed to, and how the hosting of the applications and hosts is managed. The data centers should not be exposed to high risks. If they are, the applications and hosts should be protected by business continuity measures (see BC1 in Section 7.1).

PH2: Physical security of the central systems

Data centers hosting central systems have at least a Tier III [14] classification, fire detection and extinction, flood protection and are protected against advanced physical attacks. If the building provides additional services (e.g., administrative, maintenance) or it is shared with other organizations, then the central systems are kept in their own secure areas that are physically separated from the others and enforce access control at their entrance. All entries to own buildings are detected, for instance, using a door sensor that is monitored in a NOC or SOC.

Central systems that are hosted in a base station and cover several field locations are kept in a secure area that provides capabilities like those of a Tier III data center, fire detection and extinction, flood protection and is also protected against physical attacks.

Remark: Entries to third-party buildings should also be detected and notified to a NOC or a SOC.

PH3: Physical security of the control center and engineering workstations

The control center equipment and the engineering workstations used at the auxiliary and maintenance systems are each placed in secure areas, protected against advanced physical attacks.

There is always an authorized person or operator in each control room.

Workstations that cannot be placed in secure areas have access to the corresponding central systems through a remote maintenance interface using two-factor authentication (see AC15 in Section 2.1) and a jump server (see CM4 in Section 6.1).

PH4: Physical security of the station and generation units

The perimeter around the field location is visibly delimited and signaled against unauthorized entries whenever there are physical conditions to install barriers.

The base station and generation units with internal work areas are locked and able to keep out threats with limited resources and motivation. A base station that contains central systems complies also with PH2. In case a station is shared with a grid operator, then it has different secure areas for the wind farm or solar park equipment and the grid operator equipment. Each area is a separate locked room with a different key that is only owned by the corresponding owner and building emergency responsible. All entries are detected, for instance, using a door sensor that is monitored in the control center.

Remarks: It might not be possible to delimit the perimeters of offshore wind farms or onshore field locations in remote areas of difficult access. This is acceptable due to the environment itself already providing protection to deter an attacker.

Each field location should have a unique set of keys. These are stored in secure locations that are only accessible to the field engineers and maintenance personnel.

Physical security measures at the field locations are mostly aimed to increase the difficulty of attacks. The impact of such attacks is mitigated by using unique keys (see AC24 in Section 2.2), blocking communication between substations (see CM6 in Section 6.1), protecting central systems from attacks from field locations with firewalls (see CM3 in Section 6.1) and input validation (see OP17 in Section 5.6).

PH5: Identification and authentication to access secure areas

The acceptable physical access identification and authentication methods are well defined and communicated to the building receptions and physical security teams. The users are trained on how to keep them and not to share them.

As for logical access in AC2 and AC11, the physical access rights are also reviewed periodically and whenever there are changes to the functions of the personnel within the organization.

Before being allowed to proceed to the secure areas in control centers, data centers, or base stations with central systems that cover several field locations, they are required to sign in at, at least, the building receptions or with the security team. They are required to sign out when leaving the building.

Visitors wear visible visitor badges.

Temporary badges, keys, or access cards are returned when work is finished. If any is missing by the end of the day, a process is started to discover the reason, and to expire their validity if necessary.

Remarks: The identification and authentication methods should be hard to compromise. For instance, the entity can accept only official identification methods, such as company cards or citizen cards.

PH6: Visits to secure areas

Visitors are guided by authorized personnel through a predefined path, minimizing the exposure of classified information assets. They are informed that they cannot film or photograph unless it is explicitly authorized to do so.

Remarks: Visitors should be monitored through CCTV.

4.2 Equipment [A.11.2]

To further protect field equipment, it is placed in protective cabinets.

PH7: Physical security of the central systems equipment and field equipment

The central systems equipment and field equipment are placed in locked cabinets. The keys are stored in secure locations that are only accessible to the administrators in the case of central systems' keys, or to the field engineers in the case of field equipment.

PH8: Protection against harsh operating environments in field locations

The central systems that are hosted in field locations and the field equipment are prepared to operate in harsh industrial environmental conditions.

Remark: They can have redundant internal components (e.g., power supply units) in case the primary fails.

PH9: Secure decommissioning of central system components and field equipment

When central system components or field equipment are decommissioned, the data in their storage units are erased or destroyed through a certified process. Secure transport should be arranged if the process is executed off-premises. The data owners are informed when the process ends.

Remarks: The process, or initial conditioning at least, should be done on premises for critical central system components and field equipment, such as firewalls or storage devices.

PH10: Hardware security measures on field equipment

Hardware security measures on field equipment are enabled when they are supported, including:

- Secure boot;
- Hardware security for keys;
- Protection of stored data.

5 Operations security

The security architecture supports the operational processes and procedures needed to keep the central systems and field equipment secure throughout their lifetime.

5.1 Operational procedures and responsibilities [A.12.1]

To support capacity management, the central systems have technology renewal cycles, and the field equipment needs to have enough memory and computing power reserves for updates, as it will stay in the field for a long time and is costly to replace. Both allow health and performance monitoring.

OP1: Technology renewal for central systems

The central system components have enough reserves in memory and computing power to allow updates of security functions during their lifecycle. They support extending their computing and storage resources without disrupting their normal behavior. When a security function cannot be updated due to, for instance, design limitations, performance impact, or end of vendor support, a new technological renewal iteration is triggered.

Remark: One life cycle can last typically between four and eight years.

OP2: Future-proof design for field equipment

The field equipment has enough reserves in memory and computing power to allow updates to security functions during its lifetime.

Remark: The lifetime of field equipment can last typically between eight and 15 years or more.

OP3: Resource monitoring

The central maintenance system provides tools to centrally monitor the health and performance of central systems and boundary field equipment. This includes computing, memory, storage, and network resources of the overall system and by component.

The data is sent/collected by/from the central system components through standard protocols, such as SNMP. The boundary field equipment allows access to this information from the central maintenance system through automated tools or by the engineers.

The central system components and field equipment allow the monitoring data to be read directly. The administrators can read it at central system components through the local maintenance interface or LAN. The engineers can read it in the field equipment through the local maintenance interface, LAN, or local engineering station.

Evidence that the central system components or field equipment are failing or in the imminence of failure must trigger the replacement of recovery activities.

Remarks: The boundary field equipment should also send or allow the collection of the monitoring information through standard protocols.

The monitoring of the field equipment that does not communicate with the central maintenance system could be made remotely through a local engineering station that has access to both (see CM7 in Section 6.1).

5.2 Protection from malware [A.12.2]

Endpoint protection is used in all the hosts and appliances in the central systems and field locations. The type of protection varies with the usage or function of the asset.

OP4: Endpoint protection

Antivirus is used in the hosts with operating systems that are used or maintained by the operators, engineers, or administrators. This includes at least workstations and servers at the central systems and local engineering stations at the field locations.

A host-based firewall is used in hosts and appliances in the central systems and at least the controller and local engineering stations at the field locations. It can be managed together with the applications upon their installation or change, complementing the perimeter and zoning firewalls against threats in the same network security zone.

Remarks: Whitelisting should be used in the hosts where the applications are known and mostly never change. This includes at least operation and engineering workstations and servers at the central systems and at least the controller and local engineering stations at the field locations.

Host-based intrusion detection can be used in the workstations and servers at the central systems. However, the recommendation is to use a network-based intrusion detection system (IDS) (see CM3 in Section 6.1).

OP5: Secure use of external devices

In addition to OP15, autorun is disabled for external devices and USB ports are disabled by default, except for keyboard and mouse, if necessary.

The users are trained to use only external devices from known trustworthy sources.

Remarks: Files can be transferred to the central system components or field equipment through the network. USB ports can be enabled by administrators or engineers when network access is not available.

Users should use only the equipment provided and validated by their employers.

5.3 Backup [A.12.3]

The central systems and field equipment can be backed-up and recovered through timely and reliable processes. Consistency between the back-ups of related components is ensured. The back-ups are protected during transport and storage.

OP6: Back-ups for central systems and field equipment

The central maintenance system provides tools to timely and reliably back-up the software, running configurations, configuration files, data files, and databases of the central systems and field equipment. This includes the data of the system components themselves and the data of the business processes. The engineers and administrators define the frequency, extent, and type of back-ups to keep the expected losses and recovery times acceptable to asset owners and enable business continuity.

At the central systems, the back-up process is automated and keeps at least the business process data also in an off-site location. The automation keeps up with the continuous updates to the operating system databases and reduces human error in the trigger and execution of back-up tasks. The off-site back-ups prevent irreversible loss of irreproducible historical data such as received electrical measurements, events, issue control commands, results of command execution, consumption data, and production data in case the local infrastructure is destroyed. In the same case, they also allow recovering critical configurations like process graphic displays without the need to test extensively. The administrators are responsible for the central system back-ups, which are stored in the admin servers, where they can be accessed by only the administrators.

The field equipment allows execution and retrieval of back-ups on its configurations. It is done remotely for boundary equipment, and through the local maintenance interface, LAN, or local engineering station for the equipment that does not communicate with the central maintenance system. The engineers are responsible for the field equipment back-ups, which are stored in the engineering servers, where they can be accessed by only the engineers.

Large changes to configurations or data trigger full backups before and after their implementation.

Remarks: Virtualized components can be backed-up by making, for instance, clones or disk images in addition or as a replacement for copying running configurations, files, and databases.

The back-ups of the field equipment that does not communicate with the central maintenance system could be made remotely through a local engineering station that has access to both (see CM7 in Section 6.1).

The back-up processes can complement and be complemented by business continuity solutions (see BC1 in Section 7.1). The off-site locations can be second datacenters.

The back-up storage servers can be shared with other OT systems, but it should not be shared with the IT systems.

OP7: Consistency between complementary back-ups

If separate back-up processes are used for several components with some degree of dependency between them, and the recovery process requires combining the different back-ups, then the trigger conditions and lifetimes must be consistent between the back-up processes. For instance, the back-up of an encrypted database must be aligned with the back-up of the right key to enabling a successful recovery of the data.

OP8: Security of centrally stored back-ups

The back-ups are stored in servers protected by the following measures:

- Individual user accounts are used to monitor access as described in AC14;
- Version control is used to facilitate change management;
- The server is hardened, kept fully patched, and has endpoint protection, as described in OP15, OP13, and OP4, respectively.

Remarks: The back-ups should be protected against attacks on integrity and confidentiality during transport and in storage. Cryptographic checksums or signatures can be used to protect the integrity, and they can be encrypted to protect confidentiality (see CM2 in Section 6.1 for the transport component).

OP9: Recovery from back-ups

The central maintenance system provides tools that the administrators can use to retrieve back-ups and recover data and components from an incident at the central systems. After the infrastructure is recovered and it is possible to connect and access it, the administrators perform the recovery procedures through the admin workstations.

The field equipment can be recovered by the engineers to normal operations from backed-up configurations, as they do not store important information apart from their configuration. This can be done through the local maintenance interface, LAN, or local engineering station.

The recovery procedures are frequently trained to ensure the accuracy of the back-up processes, the integrity of the back-ups, and that the administrators and engineers can execute the recovery tasks within the expected timeframes.

Remark: Virtualized components can be recovered with the use of a VM template or clone image in replacement to reinstalling the operating systems and applications, over which the remaining patches, specific configurations, and data are applied. For instance, maintenance workstations could be mainly recovered from VM images.

The engineers can initially try to contain an incident in the field equipment from the central maintenance system. They can do this if the boundary equipment is still reachable and accessible. They could also access the field equipment that does not communicate with the central maintenance system through a local engineering station that has access to both (see CM7 in Section 6.1).

Remote recovery of field equipment should be avoided if the safety of the process cannot be ensured. For instance, the field equipment could enter an unsafe state and become unreachable after that, allowing little time for an engineer to go to the field and avoid a larger incident.

Field equipment could, for instance, be recoverable from a corrupted configuration by storing a previously known correct configuration in its file system and allowing it to be safely retrieved and used by a field engineer executing a well-defined procedure.

5.4 Logging and monitoring [A.12.4]

The central system components and field equipment generate security logs. These can be gathered centrally or consulted locally to detect and responding to security incidents. As the logs are important for security, they also need to be protected.

OP10: Security events

The central systems and field equipment log all the events that are relevant to security in local logs, including:

- access control events (e.g. successful and failed authentication);
- changes to security settings (e.g. keys or credentials, authentication settings);
- changes to software or firmware (e.g. software or firmware updates);
- possible signs of attacks (e.g. physical tamper events, invalid certificates).

The log entries for security events include a timestamp, an event description, and the user, role, or process causing the event.

OP11: Collecting security events

The central maintenance system provides tools to centrally monitor the security events of the central systems and boundary field equipment.

The security events are sent by the central system components and boundary field equipment to a central logging server through standard protocols, such as Syslog. In the alternative, they are collected through automated tools. The boundary field equipment allows also access to the events from the central maintenance system by the security team with support from the engineers.

The central system components and field equipment allow all security events to be read directly. The security team can read them at central system components through the local maintenance interface or LAN with support from the administrators, and in the field equipment through the local maintenance interface, LAN, or local engineering station with support from the engineers.

Time is synchronized between endpoints to ensure that a consistent timeline can be created. The events shall allow parsing (i.e., easy interpretation) by the central logging server, avoiding the need to develop a dedicated parser.

Operators, engineers, and administrators notify the security team of any security-related events that they observe or come to their knowledge in the scope of their activities.

Remarks: The boundary field equipment should also send or allow the collection of the security events through standard protocols or, in the alternative, the security events should be gathered in a central maintenance server and then forwarded to the central logging server. The central maintenance server could filter or enrich the security events with additional context.

The security events of the field equipment that does not communicate with the central maintenance system could be monitored remotely through a local engineering station that has access to both (see CM7 in Section 6.1).

A label linking the event to its origin endpoint should be added to each log entry either at the endpoint or an aggregation point, enabling the central logging server to identify its source.

Not all events need to be gathered. Instead, it is recommended to define detection use cases based on risks and to gather only events needed for those.

The central logging server can be a security information and event management (SIEM) platform. It can be shared with other OT systems, but it should not be shared with the IT systems. However, some security monitoring use cases as, at least, the ones related to the borders with IT and the Internet, might need to correlate OT security events with IT security events or other information that exists only in IT. This correlation can happen on the OT side, IT side, or both. Therefore, the forwarding of security events between OT and IT, or the other way around, can happen through a data exchange demilitarized zone (DMZ) (see CM4 in Section 6.1).

If a third-party telco network is used to connect the central systems and field locations, then the security logs must be collected and monitored by the provider. He should notify the parties responsible for each system of security events and collaborate in incident response. This should be included in contracts with defined SLAs on response times and resolution times.

OP12: Protecting security logs

The central system components and field equipment protect the security logs by:

- restricting access to them to authorized users as described in OP11;
- having enough storage capacity for the security logs;
- implementing a rolling security log, in which the oldest entries are discarded first if log storage is full.

Remark: The security logs should be in dedicated files. Only the system and root users should be allowed to modify the files.

5.5 Control of operational software [A.12.5]

The central maintenance system has efficient update mechanisms for the central systems and field equipment. The authenticity of all software and firmware is verified using digital signatures.

OP13: Secure updates to central systems and field equipment

The central maintenance system provides tools to update the central system components and boundary field equipment. This includes operating systems, application software, and network equipment in the central systems.

The administrators and the engineers apply the updates through the central maintenance system to the central system components and the boundary field equipment, respectively.

The central system components and field equipment allow updates to be applied directly. The administrators can apply the updates to central system components through the local maintenance interface or LAN. The engineers can apply the updates to the field equipment through the local maintenance interface, LAN, or local engineering station.

The security team monitors notifications from the vendors regarding software and firmware security updates (see OP16). Security updates are prioritized considering, at least, their criticality as classified by the vendor and the level of risk to the processes of the distributed system, wind farm, or solar park.

Updates can be immediately applied to non-critical central system components, starting with a small representative group of the components to update, and then rolling out to the remaining components once any issues found in the initial deployment are fixed. The components in the initial group are used by aware users and closely monitored by the administrators and security team as described in OP3 and OP11.

For critical components, such as operation or monitoring software and field equipment, the updates can only be applied after validation from the software vendor, assuring that the update has either no impact or a limited impact that can be disregarded in the normal

working of the component and overall system. The process is the same as for the non-critical components after this initial step.

Remarks: Update servers can be used to allow efficient updates to the central systems. These servers should be in a DMZ between OT and the network through which the back-ups are acquired (see CM4 in Section 6.1).

The field equipment that does not communicate with the central maintenance system could be updated remotely through a local engineering station that has access to both.

The security team should consider intermediate remediation actions for critical security updates that cannot be immediately applied.

OP14: Verification of software and firmware signatures before installation

All software and firmware are digitally signed by their vendors. The central system components and field equipment check the signatures before installation to verify their authenticity.

Remark: The signature may be verified in software. It is not required that it is verified by hardware security functions, such as secure boot, but this can further improve security.

5.6 Technical vulnerability management [A.12.6]

To support effective vulnerability management, the central system components and field equipment are hardened and avoid known vulnerabilities, as well as input validation vulnerabilities.

OP15: Hardening

The central system components and field equipment are hardened by disabling all unneeded functions, in particular:

- all unneeded hardware interfaces are disabled;
- all unneeded network services are disabled;
- all unneeded user accounts are removed;
- if default user accounts must be used, then their passwords are changed before the production stage.

OP16: Known vulnerabilities

The central system components and field equipment use only applications, libraries, and communication protocols without known security vulnerabilities.

Vendors disclose found vulnerabilities through a defined process and participate actively in vulnerability remediation. The details of the process and SLAs on response times and resolution times, according to the severity of the vulnerabilities, are contractually defined.

OP17: Input validation

The central system components and field equipment apply input validation to all the received data.

Remarks: The developers should make sure their code checks the validity of all received data, including validating if the input is received in the right context and its values are within the permitted value range. They should regularly check that there are no input validation vulnerabilities in third-party libraries or applications. They should use reviews and robustness tests for code they develop in-house, such as the web interfaces or the implementation of domain-specific protocols such as IEC 104.

OP18: Hardware-assisted measures against exploits

The central system components and field equipment use hardware-assisted measures, such as No Execute (NH) and Address Space Layout Randomization (ASLR), to make exploits more difficult.

Remarks: Long term cryptographic keys used in communications or data encryption should be protected through secure elements, satisfying the following requirements:

- The keys do not leave the secure element. Instead, needed cryptographic functions are performed inside it.
- Stored keys are protected against advanced software and physical attacks.
- Communication to the secure element is cryptographically protected to prevent man-in-the-middle (MITM) attacks.

The secure element is Common Criteria (CC) Certified against a security target that covers the above requirements and has an assurance level of EAL 3 or higher. The vendor must present all the Common Criteria certificates.

OP19: Restriction on physical resource sharing

Applications or VMs are hosted in different physical hosts if they have different criticality to the business processes or different exposure to external networks or users.

Remark: In shared data centers or cloud environments, each group of applications or VMs supporting a different critical infrastructure should have physically separated security systems and computing, networking, and storage resources.

OP20: Vendor and manufacturer diversity

Procurement processes for central systems components and services balance vendor and manufacturer diversity with operational requirements.

Remarks: At least, the external perimeter firewalls should be of a different manufacturer than those used for segmenting the internal networks (see CM3 and CM5).

The field equipment manufacturer should vary between field locations, so long as it would not impact quality negatively. Although this could be difficult to implement between field locations of different parties, it should be feasible between substations of the same party.

6 Communication security

6.1 Network security management [A.13.1]

The central systems and field locations cryptographically protect the integrity and confidentiality of communication over untrusted networks. They restrict network access by:

- restricting communication between field devices at different locations;
- having a DMZ between OT and external networks;
- segregating networks in the central systems and access to the field locations;
- placing firewalls on network boundaries.

CM1: Robust and resilient telecom networks

Robust and resilient telecom networks with alternative paths and redundant connections are used to connect remote central systems to the field locations through the WAN/ Internet interfaces. It includes designing a proprietary network or procuring third-party infrastructures.

Remarks: In the third-party case, the providers should be asked to describe the topology and coverage of their networks and what environmental risks they are exposed to. Telecom networks should not be exposed to high risks. If they are, the communication between the central systems and field locations should be protected by business continuity measures (see BC in Section 7.1).

CM2: Cryptographic protection of communication confidentiality and integrity

Cryptographic measures are used to protect the integrity and confidentiality of communication on the following interfaces:

- Internet;
- OT/IT data exchange;
- remote access;
- local access (local network and local maintenance interface);
- WAN/Internet.

The measures allow to verify the source of messages and protect against replay attacks.

If the central systems are at a field location, the measures on the WAN/Internet interface are replaced with what is described in CM7.

Remark: A combination of different cryptographic measures can be taken at different network layers: at the telecom layer, through a VPN, through TLS, or through application

layer protection. For the communication between the operating system and the field locations, TLS can be implemented as specified in IEC 62351-3 [7] and IEC 60870-5-7 [8].

For third-party networks connecting remote central systems to the field locations through the WAN/Internet interfaces, procurement processes should consider the security measures of the providers' networks and what security risks they are exposed to in procurement processes.

The communications on the local maintenance interface (not using the local network) do not need to be encrypted as long as authenticity and non-repudiation are still assured.

CM3: Network perimeter protection

Firewalls are placed to control the network traffic across all network boundaries by:

- only allowing through the communication needed for normal operations and foreseen in the incident response plans of the relevant parties;
- limiting the traffic in case of a denial-of-service (DoS) attack through flooding.

Periodic audits are performed on the firewall configurations by comparing them with the security policies and previously defined configurations.

Remarks: Regular penetration tests should also be performed on the firewalls, at least to the interfaces that are exposed to external networks.

If the firewalls support more advanced protection, such as using detection signatures or deep-packet inspection, this should also be turned on whenever possible.

Firewall functions in the field location can be implemented in a network firewall, in the telecom modem, or in host-based firewalls at the boundary field equipment.

Measures should also be taken to detect and respond to DoS attacks in the WAN/Internet network. If an external telecom provider is used, the measures the provider must take should be part of the contractual agreements. Physical links to the central systems, a private access point name (APN) network, or similar should be used to restrict who can access the network.

Network access control (NAC) can be used at the central systems and in the LANs of field locations.

An IDS can be used at the network level to monitor the communications in the central systems, in the field location, and between both, focusing on the more critical industrial protocols, such as IEC 60870-5-104.

The IDS can be shared with other OT systems, but it cannot be shared with IT.

CM4: Demilitarized zones for connecting to IT and Internet at the central systems

The central systems are segregated from external networks using the following DMZs, as necessary:

- data exchange;
- Internet access;
- remote access.

The data exchange DMZ is used to forward/ receive security events to/from IT (see OP11 in Section 5.4), or to get updates through IT (see OP13 in Section 5.5). In the latter case, the update servers are in the DMZ.

Internet access DMZ is used to get updates directly from vendors' support servers on the Internet. The update servers get the updates through a proxy server in the DMZ.

The remote access DMZ is used to receive external connections from the remote engineers and administrators in IT or the Internet. They access the engineering or admin workstations through jump servers in the DMZ.

Remarks: A data loss prevention (DLP) system can be used in the metering system workstations and servers and the DMZs between these and the internet.

The security team should monitor known public repositories, such as “pastebin.com” for possibly leaked data. This process can be more efficient and effective by collaborating with National and European CERT and CSIRT associations.

CM5: Network segmentation in the central systems

The central system networks are segmented into logical security zones based on the functions, criticality, and exposure of each type of component. At least each type in each of the following lines is hosted in a separated zone than those of the other types:

- central systems and field equipment;
- the operation, auxiliary, metering, and maintenance systems;
- application servers, workstations, jump servers, and security servers in each central system;
- each group of workstations used by the operators, engineers, administrators, or the security team.

Remarks: Network separation between central systems and field equipment can occur naturally when the central systems are remote. It can also occur naturally between different central systems when each of them is hosted in a different location or by a different entity than those of the other systems.

Otherwise and for the other cases, the separation can be implemented with the use of firewalls, VLANs, and routing. The firewalls allow only necessary communications

between known hosts or networks that use the defined protocols and ports. The VLANs allow group hosts per type behind the logical interfaces of the firewalls. Only the necessary routes are announced to each network.

CM6: Blocked communication between field equipment at different field locations

Direct communication between field equipment at different field locations is blocked through the measures in CM2 and CM3. Further, the field equipment can communicate with only the central systems corresponding to its field location. This applies also in case the central systems are in a field location. In this case, the communication between the central systems and the field equipment is protected as described in CM7.

CM7: Segmentation of the access to field locations

Each central system is allowed to communicate with only the corresponding field equipment through the defined protocols and ports. This is enforced by at least the perimeter firewalls on the central systems side.

Remarks: It should also be enforced by the firewall functions in the field location in case the central systems are remote. This is especially important when the central systems are hosted by different entities. The firewall would be managed from the central maintenance system by the security team. The firewall rules should be aligned with the engineers.

The field engineers should maintain the field equipment through a local engineering station, avoiding connecting their laptops to the LAN or local maintenance interfaces. It could also communicate with the central maintenance system for remote maintenance.

The communication from a local engineering station to the other field equipment can be protected by placing the former in a separate security zone than that of the other field equipment. If necessary, the field engineers could still connect their laptops to the LAN through a dedicated DMZ. Both use cases could be implemented with a network firewall. It would communicate with the central access control server to enforce centrally managed, role-based access control for the field engineers to access the DMZ.

CM8: Wireless LAN communications not allowed in central systems and avoided in field locations

Wireless communications are not allowed to access the central systems through the LAN.

Remarks: They should be avoided in field locations by privileging access through local engineering stations or cabled networks. If they must be used, then the capability is enabled right before interventions and disabled right afterward. The intervention procedures include a verification that it is disabled before the maintenance team leaves the premises.

CM9: Legal notices regarding the access to system components or field equipment

If the system components or field equipment can show a pre-login banner message, it is configured to notify the users regarding the consequences of unauthorized access,

7 Information security aspects of business continuity management

7.1 Information security continuity [A.17.1]

To ensure that the security of the central systems and field equipment is not compromised during disruptions, it is designed to fail securely.

BC1: Fail-secure design

The central systems and field equipment are designed to fail in a manner that limits the security impact. During a failure, the system:

- does not leak confidential information, such as keys or credentials;
- protects the integrity of critical data;
- does not allow access controls to be bypassed;
- restores availability as soon as possible and within a timeframe that enables business continuity.

Remarks: Examples of failure are hardware malfunctions, corruption of stored or received data, and software crashes.

A watchdog can be used to monitor the central system components and field equipment and to automatically initiate steps to restore availability. The recovery process can use back-ups (see OP7 and OP9 in Section 5.3).

BC2: Redundancy for central systems and telecom networks

The central systems and telecom networks have redundant components and communication paths that allow a piece of alternative equipment or path to be used while or if the original does not recover. The redundant components offer the same services with the same quality as that of the original components.

Remarks: The alternative components or paths can be used in normal operations. This ensures that the alternative components have the right configurations and access to data. However, they should still be tested in incident response exercises to ensure that the dependencies they have in common with the originals still enable business continuity.

The redundancy should also be geographic.

High availability can be used to avoid interruption of the business process.

BC3: Alternative central system locations

There are alternative central system locations where the business process can be resumed in case the original locations are lost. This is not applicable if the central systems are hosted in a field location and are dedicated to that one only.

Remarks: These locations can host geographically redundant components and some high availability instances (see BC2). They can also have a disaster recovery system that allows the business process to resume if the original and redundant components fail at the same time.

BC4: Alternative telco networks

There is a secondary telco network that the central systems can use to communicate with the field locations in case the primary network fails. The secondary network has at least the same levels of coverage and security as those of the primary network. This is not applicable if the central systems are hosted in a field location and are dedicated to that one only.

Remarks: The primary and secondary networks should have separate infrastructures.

Appendix A: Mapping to IEC 62443

Table 3 maps the measures in the architecture to the system requirements in IEC 62443-3-3 [7]. If a system satisfies the requirements in the table, then it also meets at least partially the requirements in this document.

Only the requirements from IEC 62443-3-3 that correspond to the requirements in this document are included in the table. If requirements from IEC 62443-3-3 are not in the table, they are not required by this document.

In the last column, further specification is given. The product needs to implement the IEC 62443-3-3 requirement according to this specification to comply with this document.

Table 3: Mapping to IEC 62443-3

IEC	Name	Arch	Specification
SR1.1	Human user identification and authentication	AC14, AC25	
SR1.1 RE 1	Unique identification and authentication	AC14, AC25	
SR1.1 RE 2	Multifactor authentication for untrusted networks	AC15	Applies to operators monitoring the generation through the central systems, to engineers doing remote maintenance through the central systems, and to administrators doing remote maintenance on the central systems
SR1.2	Software process and device identification and authentication	AC13, AC24	Applies to field equipment, IT systems, and other systems accessing a central system, and to the central systems and other field equipment accessing a field equipment
SR1.2 RE1	Unique identification and authentication	AC13, AC24	Applies to field equipment, IT systems, and other systems

IEC	Name	Arch	Specification
			accessing a central system, and to the central systems and other field equipment accessing a field equipment
SR1.3	Account management	AC1, AC2, AC12, AC17, AC18, AC23	The central access control server allows administrators to manage central accounts, the central systems allow administrators to manage local accounts, and the field equipment allows engineers to manage local accounts
SR1.3 RE1	Unified account management	AC2, AC18	Applies to the centralized accounts of operators, engineers, and administrators
SR1.4	Identifier management	AC1, AC2, AC12, AC17, AC18, AC23	The central access control server allows to map central users to groups, the central systems and boundary field equipment allow to map the central groups to local groups, roles, or rights, and the central systems and field equipment allow to manage local users, groups, and roles
SR1.5	Authenticator management	AC13, AC14, AC24, AC25, CR3	Central systems and field equipment allow to manage and protect the passwords and keys of enterprise IT systems, central systems, field equipment, operators, engineers, and administrators

IEC	Name	Arch	Specification
SR1.5 RE1	Hardware security for software process identity credentials	PH10, OP18	
SR1.6	Wireless access management	AC14, AC25, CM8	Applies to field operators and engineers accessing field equipment when the use of wireless communications cannot be avoided
SR1.6 RE1	Unique identification and authentication	AC14, AC25, CM8	Applies to field operators and engineers accessing boundary field equipment when the use of wireless communications cannot be avoided
SR1.7	Strength of password-based authentication	AC2, AC13, AC14, AC18, AC24, AC25, CR2	The central access control server allows to set and enforce a password policy for centralized accounts, and central systems and field equipment allow to set and enforce a password policy for local accounts of administrators and engineers, respectively
SR1.7 RE1	Password generation and lifetime restriction for human users	AC2, AC14, AC18, AC25, CR2	The central access control server allows to set and enforce a password policy for centralized accounts
SR1.8	Public key infrastructure certificates	CR3	Central systems and field equipment use only certificates issued by the PKI in the central maintenance system, excluding the ones used for software or firmware signing

IEC	Name	Arch	Specification
SR1.9	Strength of public-key authentication	CR1	Central systems and field equipment use certificates issued by the PKI in the central maintenance system
SR1.9 RE1	Hardware security for public-key authentication	PH10, OP18	It is recommended to use HSMs
SR1.10	Authenticator feedback	AC14, AC25	Applies to the authenticators entered by operators, engineers, and administrators in central systems and field equipment
SR1.11	Unsuccessful login attempts	AC14, AC25	Applies to the logins of operators, engineers, and administrators to the central systems and boundary field equipment with centralized accounts
SR1.12	System use notification	CM9	Applies to central systems and field equipment, including also the VPN interfaces
SR1.13	Access via untrusted networks	AC6, AC15, AC20, CM4, CM5	Applies to the central system interfaces: remote access, Internet access, IT access, and WAN/ Internet, and to the WAN/ Internet interface in the field location
SR1.13 RE1	Explicit access request approval	AC2, AC6, AC10, AC22	Applies to engineers doing remote maintenance through the central systems, and to administrators doing remote maintenance on the central systems. They can only access the VPN and jump servers if

IEC	Name	Arch	Specification
			they are assigned to specific groups in the central access control server
SR2.1	Authorization enforcement	AC2, AC4, AC5, AC12, AC18, AC19, AC23	Central systems and boundary field equipment allow to map the central groups to local groups, roles, or rights, and central systems and field equipment allow to map local users to local groups, roles, or rights
SR2.1 RE1	Authorization enforcement for all users	AC1, AC17	
SR2.1 RE2	Permission mapping to roles	AC2, AC12, AC18, AC23	Central systems and boundary field equipment allow to map the central groups to local groups, roles, or rights, and central systems and field equipment allow to map local users to local groups, roles, or rights
SR2.2	Wireless use control	AC2, AC12, AC18, AC23, OP10, OP11, CM8	Applies at least to boundary field equipment when the use of wireless cannot be avoided
SR2.3	Use control for portable and mobile devices	AC20, OP5	Applies to field engineers accessing field equipment with their laptops if they cannot use one of the provided alternatives, and to engineers and administrators using external

IEC	Name	Arch	Specification
			storage devices if they cannot use one of the given alternatives
SR2.5	Session lock	AC14, AC25	
SR2.6	Remote session termination	AC14, AC25	
SR2.8	Auditable events	OP10, OP11	
SR2.8 RE 1	Centrally managed, system-wide audit trail	OP11	
SR2.9	Audit storage capacity	OP12	
SR2.11	Timestamps	OP11	
SR2.11 RE1	Internal time synchronization	OP11	
SR3.1	Communication integrity	CM2	
SR3.1 RE1	Cryptographic integrity protection	CM2	Applies to all the interfaces in the central systems, and the WAN/ Internet interface in the field location
SR3.2	Malicious code protection	OP2, OP18	Anti-virus is required at least on servers and workstations at the central systems, and on the HMI or engineering station used by field engineers to locally maintain the field location. Hardware measures are required for the central systems and field equipment. Access

IEC	Name	Arch	Specification
			control measures and communication security measures control a spreading virus
SR 3.4	Software and information integrity	OP13, OP14	Firmware integrity is verified before installation through a digital signature
SR3.5	Input validation	OP16, OP17	The central systems and field equipment should also not contain any known vulnerabilities
SR 3.7	Error handling	BC1	In case of an error, the system: • does not leak confidential information, such as keys or credentials; • protects the integrity of critical data; • does not allow access controls to be bypassed; • restores availability as soon as possible.
SR 3.8	Session integrity	CM2	Applies to all the interfaces in the central systems, and the WAN/ Internet interface in the field location
SR 3.9	Protection of audit information	OP12	
SR 4.1	Information confidentiality	AC16, AC26, OP8, OP12, CM2	Information at rest may be protected by access control mechanisms. Information in transit needs to be protected on all interfaces of the central systems excluding the local

IEC	Name	Arch	Specification
			maintenance interfaces, and the interface of the field equipment with the central systems
SR 4.1 RE1	Protection of confidentiality at rest or in transit via untrusted networks	CM2	Applies to the central system interfaces: remote access, Internet access, IT access and WAN/ Internet, and to the WAN/ Internet interface in the field location
SR 4.1 RE2	Protection of confidentiality across zone boundaries	CM2	Applies to all boundaries of the central systems, and the boundaries between the central systems and field locations
SR 4.2	Information persistence	PH9	
SR 4.3	Use of cryptography	CR1	
SR 5.1	Network segmentation	CM3, CM4, CM5, CM6, CM7	
SR 5.2	Zone boundary protection	CM3	
SR 5.2 RE 1	Deny by default, allow by exception	CM3	
SR 5.2 RE 2	Island mode	CM3	The firewalls can deny all network traffic
SR 5.4	Application partitioning	OP19, CM4, CM5	Also applicable to VM hosting in the central systems, as applications or VMs with different criticality or exposure

IEC	Name	Arch	Specification
			must be in different physical hosts
SR 6.1	Audit log accessibility	OP11, OP12	Access to the local logs and the logs in the central logging server is protected by the access control measures
SR 6.1 RE 1	Programmatic access to audit logs	OP11	
SR 7.1	Denial of service protection	CM3	
SR 7.1 RE1	Manage communication loads	CM3	Network traffic is limited by firewalls in case of flooding
SR 7.1 RE2	Limit DoS effects to other systems or networks	CM3	Network traffic is limited by firewalls in case of flooding
SR 7.3	Control system backup	OP6, OP7, OP8, (OP9)	Applies to the running configurations, file systems, and databases of the central systems, and the configurations of the field equipment
SR 7.3 RE1	Backup verification	OP7	The measures allow verifying the integrity of the backups
SR 7.3 RE2	Backup automation	OP6	Applies at least to the central systems
SR 7.4	Control system recovery and reconstitution	OP6, OP7, OP9	It must be possible to recover the central systems to an earlier state, and the field equipment to a stable configuration
SR 7.7	Least functionality	OP15	

Glossary

APN	Access Point Name
CA	Certification Authority
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DoS	Denial-of-Service
HSM	Hardware Security Module
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
ISMS	Information Security Management System
LAN	Local Area Network
NOC	Network Operations Center
OT	Operational Technology
PAM	Privileged Access Management
PKI	Public Key Infrastructure
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident and Event Management
SOC	Security Operations Center
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

References

[1] ENCS, "DR-101-2020: Risk assessment for DER security," 2020.

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

[3] ISO/IEC, "ISO/IEC 27019:2017: Information technology - Security techniques - Information security controls for the Energy Utility Industry," 2017.

[4] ENCS, "DR-202-2020: Security measures for grid operators," 2020.

[5] ENCS, "ISMS Best Practice Guide," 2019.

[6] ENCS, "DR-201-2020: Security measures for grid operators," 2020.

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

[8] ENCS, "DR-301-2020: Procurement requirements for DER controllers," 2020.

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

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

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

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

[13] NIST, "NIST Special Publication 800-63B: Digital Identity Guidelines on Authentication and Lifecycle Management," June 2017 (updated February 2020).

[14] Uptime Institute, "Data Center Site Infrastructure Tier Standard: Topology," 2018.