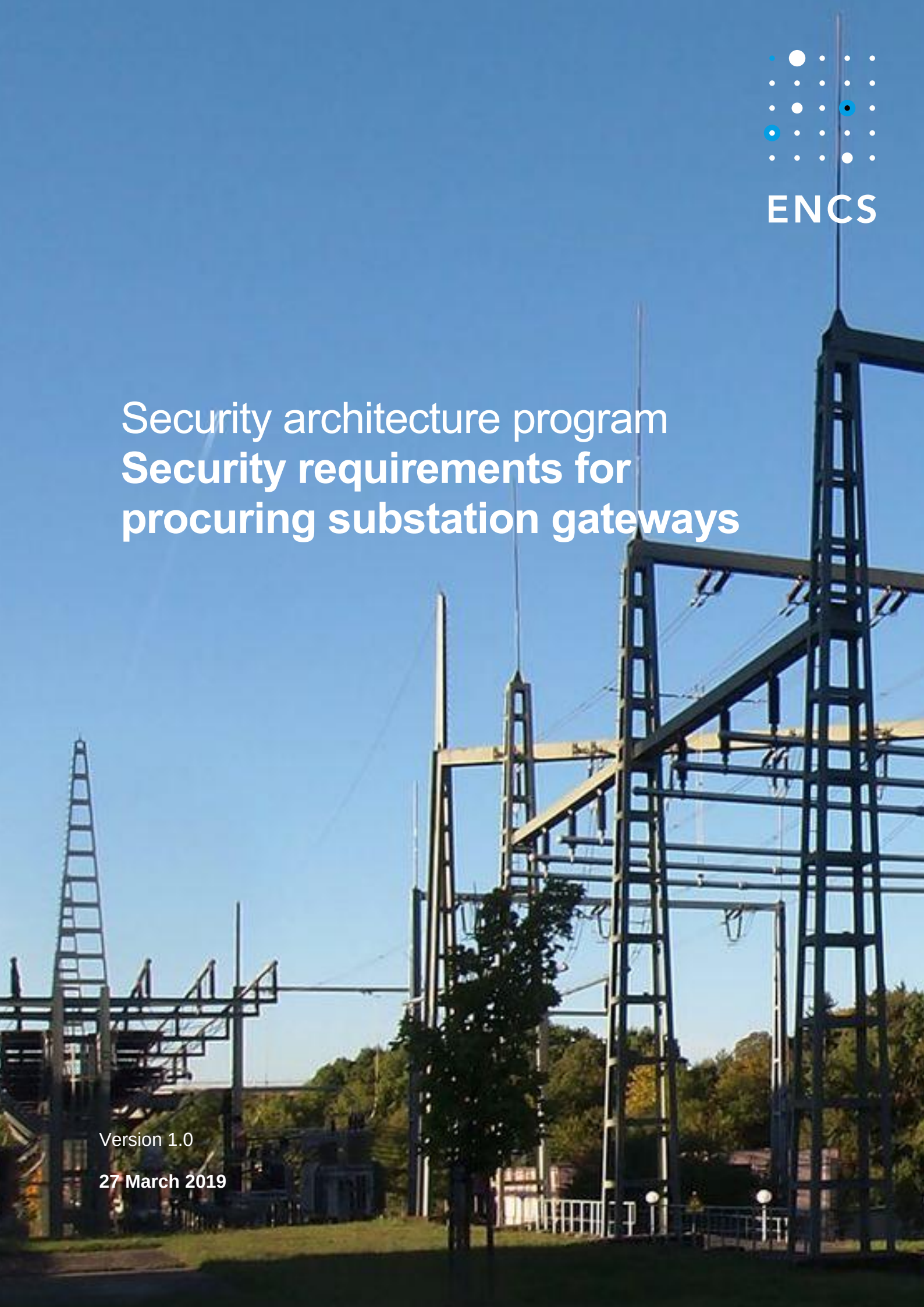

ENCS

Security architecture program

Security requirements for procuring substation gateways

Version 1.0

27 March 2019

This document was produced in the ENCS member project on substation security. In it, ENCS members shared their knowledge and experiences in the security of high-voltage substations, including substation automation and protection systems. The project developed common best practices on all aspects of substation security: from policies and security monitoring, to current and future security architectures, and requirements for procuring equipment.

It resulted in the following documents:

- Security reference architecture and risk assessment for substation automation
- Security architecture for substation automation
- Improving the security of legacy substations
- Security monitoring for substation automation
- Security market survey for substation automation
- Security requirements for procuring substation gateways
- Security requirements for procuring substation IEDs
- Security requirements for procuring substation HMI software
- Security roadmap for substation automation
- Security policy for substation automation

The documents are available through the ENCS port (https://encs.eu/documents).

This document is shared under the Traffic Light Protocol classification:

> **TLP GREEN - community wide -** information intended for ENCS Members. Anyone within the Member organizations can have access to the information

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training.

Version history

Date	Version	Description	Authors
7 December 2018	0.1	Initial draft shared for the third workshop	Maarten Hoeve (ENCS)
14 February 2019	0.2	Final draft for review	Maarten Hoeve (ENCS)
27 March 2019	1.0	Final version after member comments	Maarten Hoeve (ENCS)

ENCS

Table of Contents

1 Introduction

To get more secure equipment in future substations, it is important to set security requirements during procurement. Without good requirements, insecure equipment may be selected. Moreover, vendors are given no incentive to improve their security. The experience in other parts of the grid have shown that consistently asking for good security in procurement will lead to substantial improvement in the security offered in the market.

The IEC 62443 standard forms a good basis for defining security requirements. It includes technical security requirements for both systems (in IEC 62443-3-3 [1]) and components (in IEC 62443-4-2 [2]). These requirements are widely supported by vendors. Some are even beginning to certify against the standard using the IECEE scheme.

But the requirements in IEC 62443 are not yet tweaked to specific components in the electricity grid. IEC 62443 provides a large catalog from which requirements need to be selected based on a risk assessment. Currently, vendors are selecting themselves which requirements they implement. Consequently, there may be large differences in the security of components from different vendors even when they are IEC 62443 compliant.

Moreover, some requirements in IEC 62443 are very generic, so that they can be interpreted in many ways. To have the same level of security from different components, these requirements may have to be further specified. In some cases, specific implementations need to be specified to allow for interoperability.

This document defines procurement requirements for gateways based on IEC 62443. It selects the requirements based on the security architecture and risk assessment from the ENCS member project (see Figure 1). Moreover, where needed it further specifies and clarifies these requirements, and provides guidance on how they should be evaluated.

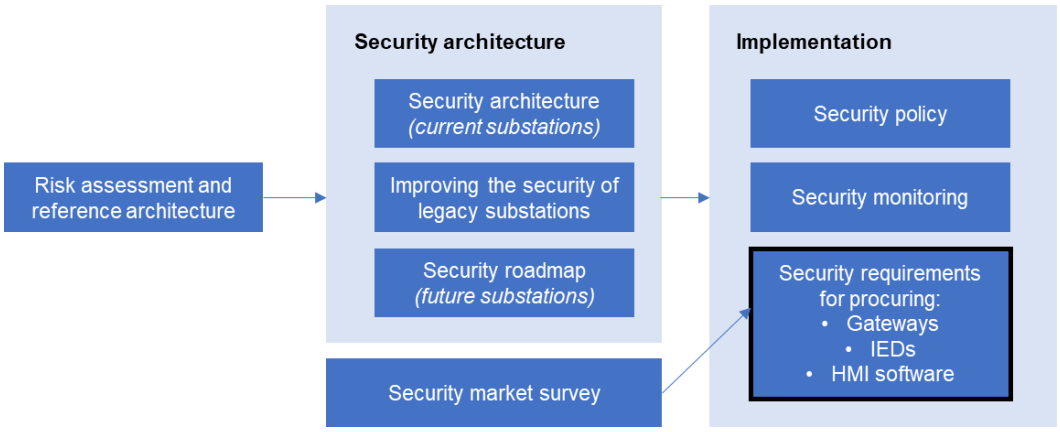

Figure 1: Relation of the procurement requirements to the other documents from the ENCS substation security member project.

2 Selection of requirements

The procurement requirements have been selected based on a risk assessment [3]. The risks are mitigated at system level using the security architecture defined in [4]. To implement this architecture, the gateways need to have certain capabilities. In this section we derive these capabilities.

2.1 Scope

The requirements concern the gateways as defined in the reference architecture [3]:

Gateway	The device in the substation with which central systems, such as the SCADA front-end communicates. In modern substations, this is usually an IEC 104 gateway, which converts the IEC 61850 protocol used within the substation to the IEC 60870-5-104 protocol used by the SCADA system on the WAN. In older substations, this device is usually called a Remote Terminal Unit (RTU). The gateway is also sometimes called a substation controller.

The reference architecture is shown in Figure 2 below.

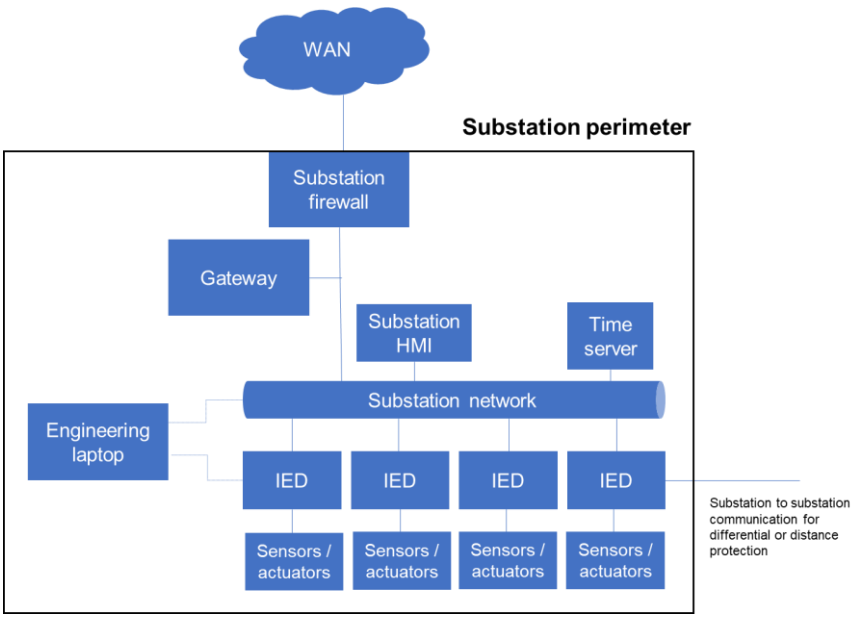

Figure 2: Simplified substation reference architecture.

2.2 Selected minimum requirements

To fulfill their role in the security architecture [4], the gateways should meet the following security objectives:

Architecture Measure from [4]	Security Objective for gateways
Secure communication to the control center	**O1:** Support secure communication channels on the WAN interface
Protect the gateway and HMI against malware	**O2:** Minimize the attack surface on the gateway
Protect the gateway and HMI against malware	**O3:** Allow authentication of human users on the maintenance service
Protect the gateway and HMI against malware	**O4:** Allow secure remote software or firmware updates for gateways
Protect the gateway and HMI against malware	**O5:** Support the detection of exploits or payloads against the gateway

Based on these objectives, the following requirements have been selected from IEC 624433-4-2 [2]. Requirement names and identifiers have been taken from this standard. The abbreviation “CR” stand for “component requirement”, “SAR” for “software application requirements, and “EDR” for “embedded device requirement”.

Requirement	O1	O2	O3	O4	O5
CR 1.1 Human user identification and authentication			■		
CR 1.1 RE1 Unique identification and authentication			■		
CR 1.2 Software process and device identification and authentication	■				
CR 1.3 Account management			■		

Requirement	O1	O2	O3	O4	O5
CR 1.4 Identifier management			■		
CR 1.5 Authenticator management			■		
CR 1.9 Strength of public key-based authentication	■		■		
CR 1.14 Strength of symmetric key-based authentication	■		■		
CR 2.1 Authorization enforcement			■		
CR 2.1 RE2 Permission mapping to roles			■		
CR 2.6 Remote session termination			■		
CR 2.8 Auditable events					■
CR 2.9 Audit storage capacity					■
CR 2.11 Timestamps					■
CR 2.11 RE1 Time synchronization					■
CR 3.1 Communication integrity	■				
CR 3.1 RE1 Communication authentication	■				
SAR / EDR 3.2: Protection from malicious code					■
CR 3.5 Input validation		■			■
CR 3.9 Protection of audit information					■
EDR 3.10 Support for updates				■	

Requirement	O1	O2	O3	O4	O5
CR 4.1 Information confidentiality					
CR 4.3 Use of cryptography					
CR 6.1 Audit log accessibility					
CR 6.1 RE1 Programmatic access to audit logs					
CR 7.1 Denial of service protection					
CR 7.4 Control system recovery and reconstitution					
CR 7.7 Least functionality					

2.3 Selected awarding criteria

There are certain capabilities on the gateway that would make it possible to implement stronger barriers in the security architecture. These capabilities have been selected as awarding criteria.

Requirement	O1	O2	O3	O4	O5
SR 1.3 RE1 Unified account management					
CR 1.8 Public key infrastructure certificates					
CR 1.11 Unsuccessful login attempts					
CR 3.4 RE2 Automated notification of integrity violations					
EDR 3.10 RE1 Update authenticity and integrity					

Requirement	O1	O2	O3	O4	O5
CR 4.1 Information confidentiality – use of authentication without encryption					

The requirements SR 1.3 RE1 was selected from the system level requirements in IEC 62443-3-3 [1], as no equivalent component level requirement was available in IEC 62443-4-2 [2]. “SR” stands for “system requirement”

3 Minimum requirements

Each requirement is labelled with the identifier, and title from IEC 62443, followed by four items:

- **Requirement:** the requirement text from IEC 62443-4-2 or 3-3
- **RE1, RE2, …:** requirement extensions from IEC 62443-4-2 or 3-3
- **Specification:** further specification of the requirement to the case of IEDs.
- **Recommended Evaluation:** Activities that are recommended for the Purchaser to make sure that the requirement is indeed met.

After these two items, recommendations are sometimes given on implementing the requirement.

For the evaluation, three types of activities can be recommended:

1. **Documentation review:** The Vendor supplies information on the topics listed. The Purchaser evaluates the information against the requirements.
2. **Functional tests:** The Vendor or Purchaser tests if the functionality in the requirement is indeed implemented on the device.
3. **Penetration tests:** The Vendor or Purchaser performs tests that simulate attacker activities to discover vulnerabilities on the device.

Both the Vendor and Purchaser can choose to let some activities be performed by a third party. If the Vendor performs tests, they should share both the test method and results with the Purchaser.

3.1 FR 1 – Identification and authentication control

CR 1.1 Human user identification and authentication

Requirement	The component shall provide the capability to identify and authenticate all human users according to ISA-62443-3-3 [1] SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures.
RE1	*Unique identification and authentication:* The component shall provide the capability to uniquely identify and authenticate all human users.

Recommended evaluation	• Documentation review on the user authentication measures. • Functional tests to verify measures are implemented correctly.

Human users include all engineers accessing the system. The SCADA front-ends, time synchronization, or other machine-to-machine access are covered by requirement CR 1.2 below.

CR 1.2 Software process and device identification and authentication

Requirement	The component shall provide the capability to identify itself and authenticate with any other component (software application, embedded devices, host devices and network devices), according to ISA-62443-3-3 [1] SR1.2.
Specification	1. The gateway shall provide the capability to identify and authenticate itself to other components on the WAN interface. 2. The gateway shall provide the capability to require other components to identify and authenticate themselves to the gateway on the WAN interface.
Recommended evaluation	• Documentation review on the user authentication measures. • Functional tests to verify measures are implemented correctly.

Components on the WAN interface include the SCADA front-end, and monitoring systems such as syslog and SNMP servers. Components are not required to uniquely identify themselves, as sometimes this is technically not possible. Authentication can be done for instance with passwords, pre-shared keys, certificates.

The requirement does not cover internal communication within the substation, such as MMS communication to IEDs. Using authentication there is recommended, but not required.

CR 1.3 Account management

Requirement	The component shall provide the capability to support the management of all accounts and/or provide the management of all accounts directly according to ISA-62443-3-3 [1] SR 1.3.
Recommended evaluation	• Documentation review on the user authentication measures. • Functional tests to verify that accounts can be modified.

Accounts may be managed through the normal gateway configuration tools or methods.

CR 1.4 Identifier management

Requirement	The component shall provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to ISA-62443-3-3 [1] SR 1.4.
Recommended evaluation	• Documentation review on the user authentication measures. • Functional tests to verify that identifiers can be changed.

Identifiers are the names of users or other components used in authentication and authorization. Identifiers may be managed through the normal gateway configuration tools or methods.

CR 1.5 Authenticator management

Requirement	Components shall provide the capability to: a) support the use of initial authenticator content; b) support the recognition of changes to default authenticators made at installation time; c) function properly with periodic authenticator change/refresh operation; and d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.
Specification	1. The gateway shall support changing all authenticators used by human users and software processes. 2. The gateway shall store passwords hashed and salted.
Recommended evaluation	• Documentation review on the user authentication measures. • Functional tests to verify that all authenticators can be changed.

Authenticators are means used to confirm the identity of a user, such as passwords or keys.

The gateway does not have to fulfill points a) and b) of the requirement. The gateway may be provided with initial authenticator content, such as default credentials, when it is delivered. But these will be changed during the initial configuration. So, this is not mandatory.

CR 1.9 Strength of public key-based authentication

Requirement	For components that utilize public key-based authentication, the component shall provide directly or integrate into a system that provides the capability within the same IACS environment to: support the use of initial authenticator content; a) validate certificates by checking the validity of the signature of a given certificate; b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued; c) validate certificates by checking a given certificate's revocation status; d) establish user (human, software process or device) control of the corresponding private key; e) map the authenticated identity to a user (human, software process or device) by checking either subject name, common name or distinguished name against the requested destination; and f) ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3 – Use of cryptography.
Recommended evaluation	• Documentation review on the use of certificates by the device. • Functional tests to verify that the component properly validates the user certificates.

Public key-based authentication is for instance used by TLS and SSH. Point d) means that the gateway checks that a user has the private key by using a public key-based authentication protocol.

CR 1.14 Strength of symmetric key-based authentication

Requirement	For components that utilize symmetric keys, the component shall provide the capability to: a) establish the mutual trust using the symmetric key; b) store securely the shared secret (the authentication is valid as long as the shared secret remains secret); c) restrict access to the shared secret; and d) ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3 – Use of cryptography

Recommended evaluation	• Documentation review on the use of symmetric keys by the device. • Functional tests to verify that symmetric key-based authentication works properly. • Penetration testing to extract the keys using privilege escalation.

Symmetric keys can be protected by normal access control mechanisms. It is recommended, but not required to protect them against physical attacks that try to extract them from memory, for instance by storing them in secure hardware.

3.2 FR 2 – Use control

CR 2.1 Authorization enforcement

Requirement	The component shall provide an authorization enforcement mechanism for all identified and authenticated human users based on their assigned responsibilities and least privilege.
RE1	*Permission mapping to roles:* The component shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.
Recommended evaluation	• Documentation review on the authorization measures. • Functional tests to verify the correct enforcement of the authorization. • Penetration testing to attempt privilege escalation.

CR 2.6 Remote session termination

Requirement	If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.
Recommended evaluation	• Functional tests to verify that the session is closed after the configured time period.

The requirement also applies to local maintenance interfaces such as serial and USB ports to ensure that these do not stay open after an engineer disconnects a cable.

CR 2.8 Auditable events

Requirement	The component shall provide the capability to generate audit records relevant to security for the following categories: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events. Individual audit records shall include: a) timestamp; b) source (originating device, software process or human user account); c) category; d) type; e) event ID; and f) event result.
Recommended evaluation	• Functional tests to verify that audit records are created for relevant events and in the right format.

CR 2.9 Audit storage capacity

Requirement	The component shall a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and b) provide mechanisms to prevent a failure of the component when it reaches or exceeds the audit storage capacity.
Recommended evaluation	• Documentation review on the storage capacity for audit records. • Functional testis to verify that the component can indeed hold enough records.

	• Functional test to verify that the component does not fail if the audit storage gets full.

CR 2.11 Timestamps

Requirement	The component shall provide the capability to create timestamps (including date and time) for use in audit records.
RE1	*Time synchronization:* The component shall provide the capability to create timestamps that are synchronized with a system wide time source.
Recommended evaluation	• Functional tests to verify that the time synchronization works.

3.3 FR3 - System integrity

CR 3.1 Communication integrity

Requirement	The component shall provide the capability to protect integrity of transmitted information.
RE1	The component shall provide the capability to authenticate information during communication.
Specification	1. The device shall be able to cryptographically verify the authenticity of all application layer data it receives on the WAN interface, except for data that cannot be sent authenticated, and has been explicitly accepted as an exception by the Purchaser. 2. The device shall authenticate all application layer data it sends on the WAN interface, except for data for which authentication is not possible, and which has been explicitly accepted as an exception by the Purchaser.
Recommended evaluation	• Documentation review on measures for message authenticity. • Functional tests to verify that the message authentication measures are implemented correctly, and that it is not possible

	to bypass these measures by downgrading to weaker security settings.

The requirement is usually implemented by verifying a message authentication code (MAC) of each received message, and attaching a MAC to each sent message. The requirement is usually implemented by verifying a message authentication code (MAC) of each received message, and attaching a MAC to each sent message.

SAR / EDR 3.2: Protection from malicious code

Requirement SAR 3.2	The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.
Requirement EDR 3.2	The embedded device shall provide the capability to protect from installation, execution of malicious code or unauthorized software.
Specification	The interpretation of the requirement depends on how the gateway is implemented: 1. If the gateway consists of application software running on an off-the-shelve operating system: a. the vendor shall document which measures against malicious code are possible on the operating system. b. the vendor shall provide information on which anti-virus or application whitelisting software is compatible. At least one program should be supported. 2. If the gateway is an embedded device with the operating system developed or adapted by the vendor, the vendor shall use the malicious code protection measures of the underlying platform where possible.
Recommended evaluation	• Documentation review of implemented measures.

Possible measures against malicious code on embedded platforms are:

- The use of processor security features such as No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR),
- Putting restrictions on the use of removable media.
- Checking the integrity of binaries and configuration files.

CR 3.5 Input validation

Requirement	The component shall validate the syntax and content of any input that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.
Recommended evaluation	• Penetration tests, which include fuzzing tests to see how the device reacts to malformed messages.

CR 3.9 Protection of audit information

Requirement	Components shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.
Recommended evaluation	• Penetration tests that try to manipulate the audit information without authorization.

EDR 3.10 Support for updates

Requirement	The embedded device shall support the ability to be updated and upgraded once installed.
Specification	1. The gateway shall support remote updates over the WAN interface.
Recommended evaluation	• Functional tests to verify that the device software can be updated.

The requirement covers all software installed on the gateway, including the operating system, application software, and firmware.

3.4 FR 4 – Data confidentiality

CR 4.1 Information confidentiality

Requirement	The component shall a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and

	b) support the protection of the confidentiality of information in transit as defined in ISA-62443-3-3 [1] SR 4.1.
Specification	1. The gateway shall encrypt all application layer data that it sends on the interfaces below, except for data that cannot be sent encrypted, and has been explicitly accepted as an exception by the Purchaser. 2. The gateway shall enforce that all application layer data that it receives on the interface below is encrypted, except for data that cannot be sent encrypted, and has been explicitly accepted as an exception by the Purchaser.
Recommended evaluation	• Documentation review on the measures for encryption. • Functional tests to verify that the encryption measures are implemented correctly, and that it is not possible to bypass these measures by downgrading to weaker security modes defined for the communication protocols used.

CR 4.3 Use of cryptography

Requirement	If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.
Recommended evaluation	• Documentation reviews of the cryptographic algorithms used. • Functional tests to verify that only strong cryptographic security mechanisms are used, e.g. by scanning the algorithms supported by TLS and SSH.

It is recommended to follow the standards set by NIST, such as NIST SP 800-57 Part 1 [5], unless there are national standards that take precedence.

3.5 FR 6 – Timely response to events

CR 5.1 Audit log accessibility

Requirement	The component shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

RE1	*Programmatic access to audit logs:* The component shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit logs to a centralized system
Extension	1. The gateway shall allow all security logs to be read out using the normal maintenance tools. 2. The gateway shall be able to send all security logs to a central server using syslog.
Recommended evaluation	• Functional tests to verify that logs can be read out using the maintenance tools and send over syslog.

3.6 FR 7 – Resource availability

CR 7.1 Denial-of-service protection

Requirement	Components shall provide the capability to maintain essential functions in a degraded mode during a DoS event.
Extension	1. The gateway shall not become unavailable for long times when network interfaces are flooded with data. 2. The gateway shall not become unavailable for long times when malformed messages are sent on network interfaces.
Recommended evaluation	• Penetration tests including robustness test. The robustness tests should include both flooding and fuzzing (systematically generating malformed packet). The availability of the gateway will be monitoring by looking at its response times to request and the status of network services.

The gateway may become slower to react when flooded or when dealing with malformed packets. But it should not crash or reboot so that it is not reachable for a longer time.

CR 7.4 Control system recovery and reconstitution

Requirement	The component shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.

Specification	1. It shall be possible to recover the gateway to its normal operation from a stored configuration, such as a project file.
Recommended evaluation	• Functional test to verify that the component can be recovered from a stored configuration.

CR 7.7 Least functionality

Requirement	The component shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services
Specification	1. The gateway shall allow all user accounts that are not used to be removed. 2. The gateway shall allow all network services that are not used to be disabled. 3. In particular, the gateway shall allow any maintenance network services to be disabled on the WAN interface if a grid operator only uses local configuration. 4. The gateway shall allow all unused hardware interfaces to be disabled.
Recommended evaluation	• Functional test to verify that accounts, services and interfaces • Penetration tests to try to access unused accounts, services, and interfaces.

Hardware ports would be for instance serial or USB ports. The requirement does not cover hardware interfaces inside the gateway casing, such as JTAG debug ports. It is recommended, but not required, to disable these.

4 Awarding criteria

4.1 FR 1 – Identification and authentication control

CR 1.3 RE1 Unified account management

Requirement	The control system shall provide the capability to support unified account management.
Specification	1. The gateway should integrate with role-based access control on the central server: it should allow the role of the user to be set on the central authentication server. 2. The gateway should provide a secure way to log in when it cannot reach the central authentication server.
Recommended evaluation	• Functional test to verify that the IED can be integrated with a central authentication server, and that it is possible to access the IED when it cannot reach the central server. • Penetration tests that try to get access to the IED when it cannot reach the central server.

Unified account management means that user accounts are managed from a central server. This can be done with protocols such as RADIUS, LDAP, or Active Directory.

The management of users will then be done on the central authentication server. In particular, the server manages the mapping of users to roles in role-based access control. During authentication, the gateway gets the role of the user from the server. It then gives the user privileges based on this role.

When the central authentication server cannot be reached, a fallback can be provided by for instance local accounts. But the authentication on such an account should be strong enough that it cannot be used as a backdoor.

CR 1.8 Public key infrastructure certificates

Requirement	When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with ISA-62443-3-3 [1] SR1.8.

Specification	Where the gateway uses certificates to secure communication, it should be able to use certificates issued by the PKI of the grid operator.
Recommended evaluation	• Documentation review on the support for PKI integration. • Functional tests to verify that the component properly validates the user certificates.

Certificates used for firmware signing are not covered by the requirement. A certificate from the vendor or a public certificate authority is allowed.

Certificates may be set manually or automatically. Automatic management of certificates is preferred.

CR 1.11 Unsuccessful login attempts

Requirement	When a component provides an authentication capability, the component shall provide the capability to: a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and b) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.
Recommended evaluation	• Functional tests to verify that the number of attempts and time period can be configured. • Functional tests to verify that access is denied after the configured number of attempts.

4.2 FR 3 – System integrity

CR 3.4 RE2 Automated notification of integrity violations

Requirement	If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.

Recommended evaluation	• Penetration tests that try to bypass the integrity checks.

EDR 3.10 RE1 Update authenticity and integrity

Requirement	Host devices shall validate the authenticity and integrity of any update prior to installation.
Specification	1. The IED should be able to verify the integrity of firmware updates using digital signatures.
Recommended evaluation	• Functional tests to verify that the IED accepts updates with valid signatures, and rejects updates with invalid signatures. • Penetration tests that try to bypass the signature verification.

4.3 FR4 – Data Confidentiality

CR 4.1 Information confidentiality

Requirement	*The main requirement is included as minimum requirement in Section . The specification below is added as awarding criterion.*
Specification	1. The gateway shall allow encryption to turn of encryption on the SCADA traffic, and using only message authentication.

Turning of encryption allows deep-packet inspection on the SCADA traffic. TLS allows using authentication without encryption by using the NULL cipher.

References

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

[2] ISA / IEC, "ISA 62443-4-2 Security for industrial automation and control systems - Technical security requirements for IACS components, Draft 3, Edit 4," January 12 ,2017.

[3] ENCS, "Security reference architecture and risk assessment for substation automation," 2019.

[4] ENCS, "Security architecture for substation automation," 2019.

[5] National Institute for Sandards and Technology (NIST), "Special Publication 800-57 Part 1 Rev. 3: Recommendation for Key Management," 2012.