SE-301-2020

Security requirements for procuring sensors

Version 1.0

28 December 2020

This document was produced in the ENCS program on Security Architectures. This program support ENCS members in selecting and implementing technical security measures for systems and their components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

Smart metering	DA-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	DA-101-2019: Security risk assessment for substation automation systems DA-201-2019: Security architecture for substation automation systems DA-301-2019: Security requirements for procuring substation gateways DA-302-2019: Security requirements for procuring IEDs DA-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

This document is shared under the Traffic Light Protocol classification:

TLP White – public

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

Version History

Date	Version	Description
9 March 2020	0.1	Initial draft
22 March 2020	0.2	Update after feedback from member RFP
28 December 2020	1.0	Final version from 2020 program

Table of Contents

1 Introduction

This document gives security requirements that grid operators can use directly in their procurement documents for new sensors, in particular sensors based on internet-of-things (IoT) technologies.

Grid operators depend on grid information for effective and efficient operation, maintenance and planning. This information is traditionally collected by the SCADA system through remote terminal units (RTUs) or gateways placed at substations.

But in this way grid operators are only monitoring part of the grid. For many use cases, information cannot be collected in the traditional way. Examples are oil quality monitoring in the transformers, hot spot temperature monitoring in transformers and lines, copper theft detection, and fault passage indication in overhead lines. Sensors collecting information for these cases can often not easily be connected to substation RTUs or gateways, because they are physically too far, or it is too costly to logically integrate them into the systems.

New sensors, often based on IoT technologies, are used to fill this gap. These sensors allow grid operators to get more data about the grid, at a lower cost.

But because of the goal of low cost, it is often not clear what security requirements can be set for the sensor systems. To keep the cost of sensors down, they have less computing power than RTUs or gateways. To reduce installation cost, the sensors are sometimes battery powered. So, some measures may not be feasible on the sensors. Also, to minimize the cost of installation and maintenance, security configuration and key management should take as little time as possible from engineers. So, these functions should be automated where possible.

This document provides a harmonized set of security requirements that grid operators use directly in their procurement documents for sensors. The requirements have been reviewed by both grid operators and sensor vendors. They are designed to fit into existing processes and procedures.

Harmonizing the requirements allows grid operators to more cost-effectively get secure equipment. It saves time and effort in developing requirements, as they are already freely available. It ensures the requirements are feasible, as they have been tested in a market survey, and in previous tenders by other operators. And it saves on implementation costs, as vendors get a common baseline to aim at.

1.1 Scope

The architecture covers sensor systems gathering data on the grid, from the central maintenance systems to the sensors (Figure 1). The sensors may be placed anywhere in

the grid: in high or medium voltage substations, on lines, or in overhead distribution poles.

The sensors may be used to gather operational data, such as voltages and currents or fault indications, or for asset monitoring, such as oil quality monitoring in the transformers or hot spot temperature monitoring in transformers and lines.

The requirements make two assumptions:

- The sensors cannot be used to directly control the grid.
- There is no local access for maintaining the sensors.

If these assumptions do not hold, the requirements for distribution automation RTUs [1] may be better suited. The sensors may be used to control equipment not used for grid control, such as public lighting. Sensors that do not communicate with central systems are not covered.

The security measures are technology independent. They can be applied to sensors using different communication protocols, such as SCADA protocols (IEC 60870-5-104, IEC 61850), smart metering protocols (DLMS), and IoT protocols (JSON, MQTT, AMQP).

The measures are aligned with ISO/IEC 27001:2013 [2] and cover the following sections from Annex A of that document:

- Access control (A.9)
- Cryptography (A.10)
- Physical and environmental security (A.11)
- Operations security (A.12)
- Communication security (A.13)
- System acquisition, development and maintenance (A.14)
- Supplier relationships (A15)
- Information security aspects of business continuity (A.17)

Each subsection gives requirements that grid operators can use to meet an objective of ISO/IEC 27001 Annex A. The objective number is given in square brackets.

1.2 Reference architecture

Figure 1 shows the reference architecture for sensor systems used in this document. The users are referenced in the access control measures in Section 2. The interfaces are referenced in the communication security measures in Section 5.

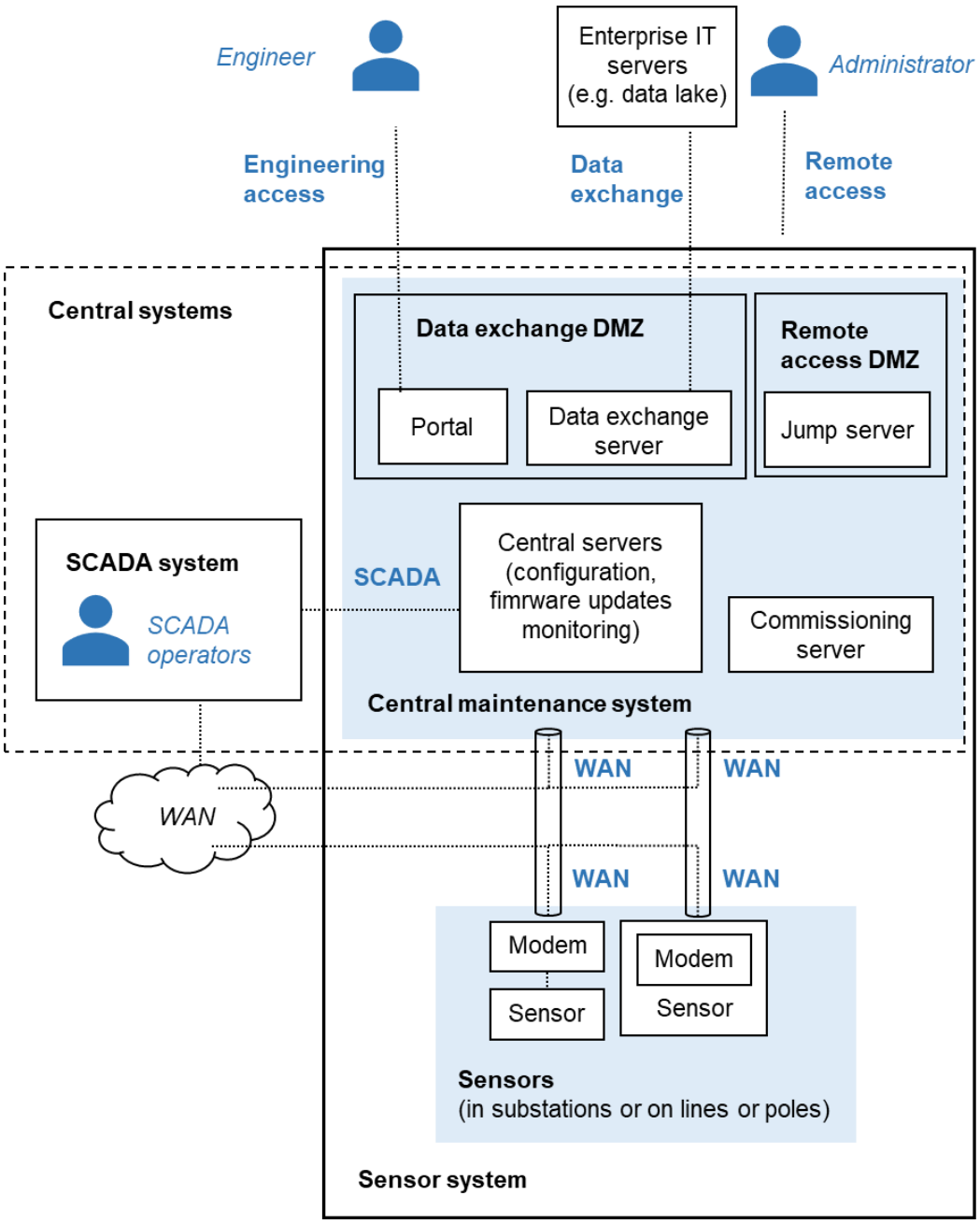

Figure 1: Reference architecture for the sensor system, showing its users and interfaces

Using the requirements

The security requirements are part of a larger approach to creating secure systems, both when building new systems or 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 risks can have on it. An example risk assessment for sensor systems is available in [3].
2. Design a **security architecture** that selects technical security measures to mitigate the risks. Measures should be 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 for the departments maintaining the system. A recommended security architecture for sensor systems is available in [4].
3. Derive **requirements for components** from the security architecture that can be used to develop or procure the components. This document gives security requirements for sensors.
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. A standardized test plant to evaluate the sensors against the requirements in this document is available in [5].
5. **Test the system** to check that it is deployed according to the architecture and mitigates the risks. The implementation of the architecture 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. But 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 quality of the processes and procedures, it is recommended to use an information security management system, for instance based on the ISO/IEC 27001 [2]. To support this, the architecture is organized by the security objectives in ISO/IEC 27001 Annex A.

2 Access control

Access control requirements concern how access rights are managed and how strong their authentication needs to be for different user groups. The sensors enforce access control for the user groups in Table 1.

Table 1: User groups on the sensors.

User	Required access	Interface
Central maintenance system	• Configure , monitor, and maintain the sensors • Collect information from the sensors	WAN
SCADA system (optional)	• *Optional:* Collect information from the sensors	WAN

2.1 System and application access control [A.9.3]

The sensors support authentication for all users. It uses machine-to-machine authentication for the SCADA system and individual password for local engineers.

AC8-SEN: Machine-to-machine authentication for the SCADA system at the network

If the sensor is designed to communicate with the SCADA system, it shall support mutual authentication with passwords or keys for the SCADA system to gain network access.

Remarks: Authentication can be implemented using a virtual private network (VPN) or using transport layer security (TLS) with pre-shared keys or client-side certificates (as specified in IEC 62351-3 [6] and IEC 60870-5-7 [7]).

This measure is usually implemented together with the cryptographic communication security measure CM1 (Section 5.1). Passwords and keys are updated according to measure CR2 (Section 3.1).

AC9-SEN: Machine-to-machine authentication for the central maintenance system

The sensor shall support mutual authentication with passwords or keys for the central maintenance system.

Remarks: Mutual authentication can be implemented using transport layer security (TLS) or datagram transport layer security (DTLS) with pre-shared keys or client-side certificates.

This measure is usually implemented together with the cryptographic communication security measure CM1 (Section 5.1). Passwords and keys are updated according to measure CR2 (Section 3.1).

3 Cryptography

The sensor uses cryptography for several functions:

- machine-to-machine authentication for the SCADA system and central maintenance system (Section 2)
- digitally signing the firmware (Section 4.4)
- protecting the confidentiality and integrity of communication (Section 5.1)

Measures need to be taken to make these cryptographic techniques effective.

3.1 Cryptographic controls [A.10.1]

The sensor uses strong cryptographic keys and algorithms to protect against attacks to the cryptography itself. The sensor supports remote key updates from the central systems in order to update keys on possibly thousands of substations.

CR1-SEN: Strong cryptographic keys and algorithms

For security functions, the sensor shall use cryptography according to regulations and modern guidelines without any modifications. In particular:

- It only uses the cryptographic algorithms that the ECRYPT – Algorithms, Key Size, and Protocols Report [8] recommends as suitable for new or future systems;
- It uses keys at least as long as the ECRYPT report recommends for near term use (section 4.6 in [8]);
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [8] Section 3.2.3 to generate random numbers for security functions;
- If it uses certificates for authentication, it validates them by checking the signature, the certificate-chain, the revocation status, and the identity or role of the user.

CR2-SEN: Automated key management

The sensor shall allow all passwords and keys to be updated by the central maintenance system in such a way that their confidentiality and integrity is cryptographically protected during transport.

If public key cryptography is used to protect communication, the sensor shall be able to use certificates given out by the grid operator’s public key infrastructure (PKI).

Remarks: It is allowed that some keys or credentials used for internal purposes cannot be updated remotely. But as soon as they are used to implement any of the requirements in this document, the requirement applies.

The certificate used to verify firmware updates (OP10-SEN in Section 4.4) is issued by the vendor. So, for this certificate the sensor does not need to be able to use certificates from the grid operator PKI.

4 Operations security

The sensor should support the operational processes and procedures needed to keep it secure throughout its lifetime.

4.1 Operational procedures and responsibilities [A.12.1]

To support capacity management, the sensor needs to have enough computing reserves for future updates.

OP1-SEN: Future-proof design

The sensor shall have enough memory (RAM and flash) and computation power to allow security updates needed during its lifetime, under the following assumptions:

- Cryptographic measures are updated following the standards in CR1-SEN (Section 3.1), in particular the sensor supports the key sizes recommended for long term use in Section 4.6 of the ECRYPT report [8];
- Roles and security event types will grow incrementally up to 50%.

Remarks: Compliance to the requirement can be shown through performance tests. Tests with current firmware under operational workloads should show that there are enough reserves to extend security functions. Tests with algorithms and key sizes recommended for long-term use in [8] should show that the sensor can run them without affecting operations. It is acceptable if the sensor can only support the long term key sizes for elliptic curve based algorithms, not for RSA-based algorithms.

OP2-SEN: Zero-touch deployment

The sensor shall support zero-touch deployment: it can be installed without any local access, through the following steps.

- The vendor delivers the sensor to the grid operator with an initial configuration, passwords, and keys installed.
- Once the sensor has been physically installed and is powered one, it automatically connects to a commissioning server.
- The commissioning server loads the operational configuration to the sensor, including new passwords and keys.

4.2 Backup [A.12.3]

To support recovery processes, it should be possible to recover the sensor from the configuration data stored on the central maintenance system.

OP4-SEN: Automated configuration management for sensors

The sensor shall allow the central system to change and monitor its configuration.

Remark: As the central maintenance system keeps all sensor configurations, these are automatically backed up when back-ups of the servers are made. No separate back-up process is needed for the sensors.

4.3 Logging and monitoring [A.12.4]

To support detecting and responding to security incidents, the sensor needs to log relevant security events and allow them to be gathered for analysis. As the security logs are important to security, they also need to be protected themselves.

OP5-SEN: Security events

The sensor shall be able to send an alarm to the central maintenance systems in case of the following security events:

1. booting the device
2. changing the sensor security setting
3. changing keys or credentials
4. successful firmware updates
5. failed firmware updates

The alarms shall include timestamps. The sensors shall be able to synchronize time with a time source at the central system.

Remarks: The sensor does not have to store the security events in a local log file, although this is recommended. Sensors may store the alarms in a buffer and send them during the next communication window.

4.4 Control of operational software [A.12.5]

To support patching, the sensor implements batched, remote updates. The authenticity of firmware is verified using a digital signature.

OP9-SEN: Batched, remote firmware updates

The sensor shall allow remote firmware updates through software in the central maintenance system that allows batch updates. It should be possible to update all security functions through these updates.

Remarks: Allowing batch firmware updates simplifies managing large numbers of sensors, for instance, making it is easier to roll out security updates.

OP10-SEN: Verification of firmware signatures before installation

The sensor shall verify the authenticity of firmware updates before installing the firmware using digital signatures. The vendor digitally signs each firmware release.

Remark: Verifying the firmware integrity using only a hash value does not satisfy the requirement.

4.5 Technical vulnerability management [A.12.6]

To support effective vulnerability management, the sensor is hardened, and avoids known vulnerabilities as well as input validation vulnerabilities.

OP11-SEN: Hardening

The sensor shall be delivered to the grid operator with all unneeded functions disabled. Specifically, it is delivered with:

- all unused user accounts removed
- all unused network services disabled
- all unused hardware interfaces disabled

Remark: It is recommended to disable hardware ports in software and to remove traces, pins and components from the PCB.

OP12-SEN: Hardware assisted measures against exploits

The sensor shall implement the following hardware features if they are available:

- *No-Execute (NX) / Write-xor-execute (W^R):* If the sensor has a Memory Protection Unit (MPU) or Memory Management Unit (MMU), it shall be used to mark code regions as read-only and data sections as non-executable.
- *Address Space Layout Randomization (ASLR):* If the sensor has a Memory Management Unit (MMU), it shall be used to load data and code at different memory addresses every time an application is run.

The software running on the sensor shall be compiled to use the hardware features.

Remark: The Position Independent Code (PIC) or Position Independent Executable (PIE) compiler options should be enabled to be able to use ASLR.

5 Communication security

5.1 Network security management [A.13.1]

The sensor needs to support securing communications on the WAN network.

CM1-SEN: Confidentiality and integrity of network communication

The sensor shall be able to use cryptographic measures to protect the integrity and confidentiality of communication on the WAN interface. The measures shall allow to verify the source of messages and protect against replay attacks.

Remarks: Confidentiality and integrity of the communication can be protected by using TLS or DTLS.

6 System acquisition, development and maintenance

6.1 Security in development and support processes [A.14.2]

The developer should integrate security throughout their development process to ensure that secure firmware is delivered. They should set up secure programming practices and test each firmware release themselves. They should allow the grid operator to verify the security by acceptance testing as well as provide guidelines on secure configuration and operation. If vulnerabilities are found during the lifetime of the sensor, they should provide security updates.

SD1-SEN: Secure programming practices

The developer shall set up programming practices for the sensor firmware. They shall:

- define secure coding guidelines
- provide security training to developers
- set up internal code reviews
- use an issue tracker to follow the vulnerabilities and other security issues
- implement a version control system
- enable compiler options to harden binaries or use memory-safe languages

Remark: Examples of secure coding guidelines are the SEI CERT coding standards [9], available for different languages, and the MISRA C software development guidelines for embedded systems [10].

Compiler options that should be enabled include:

- stack cookies or canaries which make it harder to exploit stack-based buffer overflows
- fortify source which can be used to detect buffer overflow vulnerabilities
- Control Flow Integrity (CFI) which makes it harder for an attacker to perform code re-use attacks such as return-to-libc or Return Oriented Programming (ROP)

SD2-SEN: Security testing during development

The developer shall test each firmware release to check the implementation of the requirements in this document using at least functional tests.

Remark: It is also recommended to include in the tests for each firmware release:

- robustness testing of custom protocol implementations
- automated web application testing on any web interfaces
- automated vulnerability scanning

SD3-SEN: Support for third party testing

The developer shall support testing by the grid operator or an independent party by:

- allowing the grid operator or a third party to audit the development process
- providing documentation on how the requirements have been implemented
- making available sensors for testing
- providing all keys and credentials needed for testing
- providing access to source code for code reviews

Remark: The developer may require a non-disclosure agreement when providing sensitive information, if it does not prevent proper testing.

SD4-SEN: Secure initial configuration

The developer shall deliver the sensors with a secure initial configuration:

- access control and communication security measures are turned on
- unique initial keys and passwords are installed
- security alarms are sent to the central system as described in OP5-SEN (Section 4.3)
- the sensors are hardened as described in OP11-SEN (Section 4.5)

SD5-SEN: Vulnerability handling

The developer shall produce security updates to fix all severe vulnerabilities found during the lifetime of the sensor. The developer shall monitor all relevant information sources on vulnerabilities, including:

- public vulnerability databases
- notifications from developers of libraries used in the firmware
- penetration test results from customers
- notifications from vulnerability researchers

The developer shall inform the grid operator about vulnerabilities as soon as possible.

Remark: To determine which vulnerabilities are severe, the Common Vulnerability Scoring System (CVSS) should be used. Vulnerabilities with a score of 7.0 or higher would be considered severe and need to be fixed.

The developer may agree with the grid operator to use another method to determine the severity of the vulnerabilities, if it can be objectively applied and gives a good indication of the risk.

7 Supplier relationships

7.1 Information security in supplier relationships [A.15.2]

To ensure that the sensor developer protects information of the grid operator or under his responsibility, it needs to implement an information security management system (ISMS).

SR1-SEN: Protection of customer assets

The developer shall have an ISMS to protect any information that could compromise the security of the sensor, including:

- detailed security designs
- source code
- initial keys and credentials

8 Information security aspects of business continuity management

8.1 Information security continuity [A.17.1]

To ensure that the security of the sensor system is not compromised during disruptions, the sensor is designed to fail securely.

BC1-SEN: Fail-secure design

The sensor shall be designed to minimize the impact of a failure on security. During a failure, the sensor shall:

- not leak confidential information, such as keys or credentials
- protect the integrity of critical data
- not allow access controls to be bypassed
- restore availability as soon as possible

Remarks: Examples of failures are hardware malfunctions, corruption of stored or received data and software crashes. A watchdog can be used to monitor the sensor and to automatically initiate steps to restore availability.

Glossary

AD	Active Directory
APN	Access Point Name
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarized Zone
DoS	Denial-of-Service
EST	Enrollment over Secure Transport
IED	Intelligent Electronic Device
ISMS	Information Security Management System
MV	Medium Voltage
OT	Operational Technology
PKI	Public Key Infrastructure
RADIUS	Remote Access Dial-In User Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Incident and Event Management
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

References

[1] ENCS, "DA-301-2019," 2019, Security requirements for procuring distribution automation RTUs.

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

[3] ENCS, "SE-101-2020: Security risk assessment for sensor systems," 2020.

[4] ENCS, "SE-201-2020: Security architecture for sensor systems," 2020.

[5] ENCS, "SE-401-2020: Security test plan for sensors," 2020.

[6] 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.

[7] 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.

[8] ECRYPT - CSA, "D5.4 Algorithms, Key Size and Protocols Report," 2018.

[9] Carnegie Mellon University (CMU), "SEI CERT C Coding Standard," [Online]. Available: https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard. [Accessed 10 10 2019].

[10] MISRA, "Guidelines for the Use of the C Language in Critical Systems," 2013.