aifyclo

SC-301-2020

Security requirements for procuring SCADA, EMS and (A)DMS applications

Version 1.0

4 November 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

ENCS

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

Version History

Date	Version	Description
27 August 2020	0.1	Initial draft released to members for review
3 November 2020	0.2	Update after workshop with members
4 November 2020	1.0	Final version

Table of Contents

1 Introduction

This document gives security requirements that grid operators can use directly in their procurement documents for SCADA, EMS and (A)DMS application software.

The SCADA, EMS and (A)DMS systems are the core of a grid operation infrastructure for both transmission system operators (TSOs) and distribution system operator (DSOs). This core position also makes them attractive targets to anyone trying to sabotage the electricity grid. Through these systems, they can control thousands of field devices. So, the systems should be strongly secured.

But securing these systems is becoming more difficult as they are becoming more connected. The time that SCADA, EMS and (A)DMS systems were stand-alone, air-gapped systems has long passed. Most grid operators have now connected them to their enterprise IT systems to export data for grid planning and to import geographic information. The vendor of the systems often has remote access for maintenance. Control center of other grid operators are connected. Field equipment from distributed energy resources (DER) or customer feeding in gas are being connected. And field engineers are getting remote access to get a better view of the system and give feedback about executing switching actions. Each connection creates a possibility for attackers to get into the systems.

This document provides a harmonized set of security requirements that grid operators can use directly in their procurement documents. The requirements have been thoroughly reviewed by ENCS member grid operators. They are designed to fit into the processes and procedures already in place in the organizations, and to find a good balance between security and operational impact.

Harmonizing the requirements allows grid operators to get software more cost-effectively. 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. Grid operators are therefore encouraged to use these requirements when procuring new SCADA, EMS and (A)DMS software.

1.1 Scope

The requirements cover the SCADA, EMS and (A)DMS application software. For brevity, we will refer to this software as the **SCADA application**.

The requirements do not cover the underlying infrastructure, such as the servers, workstations, and networks.

The measures are aligned with ISO/IEC 27001:2013 [1] and cover the following sections from Annex A of that document:

- Access control (A.9)
- Cryptography (A.10)
- 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 corresponding objective numbers are mentioned in square brackets next to the subsection headings. All objectives for the above topics are covered, except A.9.1, A.9.3, A.13.2, and A.17.2.

Using the requirements in procurement processes should contribute to compliance with System acquisition, development and maintenance (A14), and specifically and, in specific, to Security requirements of information systems (A14.1) – OT systems in this case.

Although the requirements are meant for procuring new SCADA, EMS and (A)DMS and not for legacy systems, grid operators may use them to upgrade existing systems.

1.2 Reference architecture

Figure 1 shows the reference architecture used in this document. The reference architecture is used to give names to users and interfaces. It tries to make as few assumptions as possible about the exact architecture. The users are referenced in the access control measures in Section 2. The interfaces are referenced in the communication security measures in Section 5.

The SCADA servers are usually located at different locations for redundancy. A network connection between the locations is used to synchronize the data. The redundant locations are not shown in Figure 1 but are covered by the security architecture.

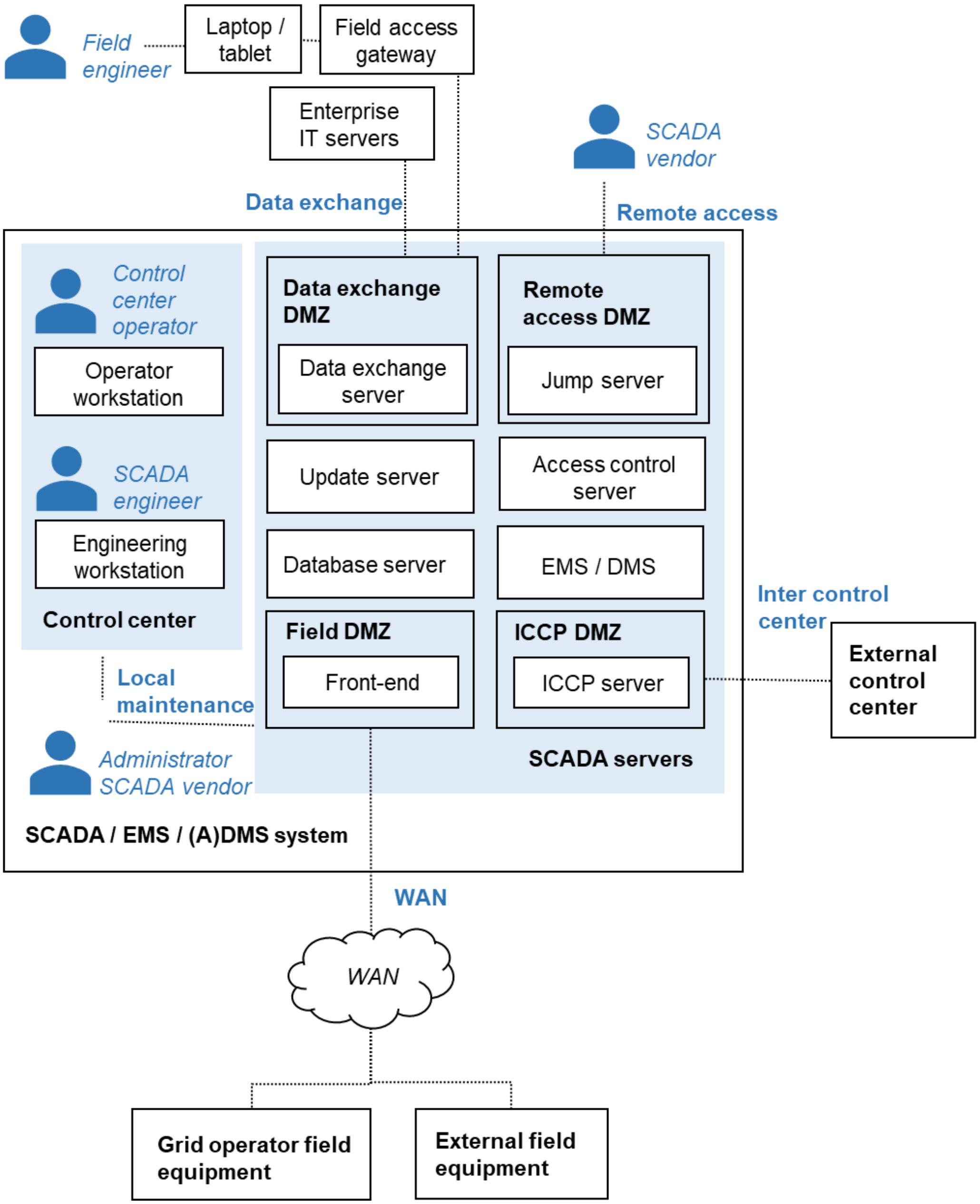

Figure 1: Reference architecture for the SCADA system, showing its users and interfaces

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.
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 SCADA systems is available in [2].
3. Derive **security requirements for components** from the security architecture that can be used to develop or procure the components. This document provides security requirements for SCADA systems, which can be used in tenders as-is or adapted and extended.
4. **Test the components** to check that they meet the security requirements. In a procurement process, such tests should be a phase within the vendor or device selection.
5. **Test the system** to check that it is implemented 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 for securely maintaining the system, manage keys and passwords, and responding 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 [1]. 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 SCADA application enforces access control for the user groups in Table 1.

Table 1: User groups on the SCADA system.

User	Required access	Interface
Human users		
Control center operator	• View grid measurements • Execute control commands	Operator workstation
Field engineers	• View grid data • Report execution of predefined switching plans	Data exchange
SCADA engineer	• Create and maintain SCADA data model	Engineering workstation
SCADA vendor	• Perform maintenance to the SCADA system	Local maintenance Remote access
Administrator	• Maintain applications, servers, workstations, and networks	Local maintenance
System users		
Enterprise IT servers	• Get live and historical grid information from the SCADA system • Provide additional grid information to the SCADA system	Data exchange

	• Provide geographic or asset information to the SCADA system	
Field equipment	• Send measurements and alarms • Receive commands	WAN
External field equipment	• Send measurements and alarms • Receive commands	WAN
External control center	• Share grid measurements • Send or receive control commands	Inter-control center interface

At most grid operators, field engineers only report back to the SCADA system that they have performed a switching action (locally at a substation). If the SCADA system allows field engineers to also switch remotely, additional security measures may be needed, such as two-factor authentication.

The remote access could also be used by control center operators or administrators, although most grid operators do not allow this by policy.

Examples of enterprise IT systems connecting to the SCADA system are:

- Outage management system
- Tools providing a live view of the grid
- Business intelligence
- Analytics platforms and tools
- Smart metering systems
- Geographic information systems
- Asset management systems

Field equipment includes remote terminal units (RTUs), or gateways owned by the grid operator in substations or recloser locations. External field equipment would for instance be RTUs owned by operators of distributed energy resources (DER) or customers feeding biogas into the gas network.

2.1 User access management [A.9.2]

The SCADA application allows to manage access rights in such a way that the grid operator can implement the principle of least privileges. For human users, it supports centrally managed, role-based access control, so that the grid operator can keep up with personnel changes and give engineers only the privileges they need. For system users, access rights are set by the administrators.

AC1-SCA: Centrally managed, role-based access control for human users

The SCADA application shall support role-based access control for all human users. The SCADA application shall be able to:

- allow users to log in with individual accounts;
- check the user's role in a central access control server;
- enforce the access right of the user's role.

The SCADA application shall allow changing the privileges of a role or adding new roles.

Remarks: The engineer's role can be checked through different methods, such as Active Directory (Kerberos), RADIUS, or LDAP.

AC2-SCA: Least privileges for system users

The SCADA application shall be able to restrict the access rights for all system users, so that they can access only the functions and data they need. The SCADA application shall allow administrators to set the access rights centrally, giving each system the minimum access rights needed for operations.

Remark: The measure can be implemented by having different external system accessing different network services. Then the access rights can be restricted by limiting what functions are available over the service. If different system users access the same network service, the service should allow giving them different access rights.

2.2 System and application access control [A.9.4]

The SCADA application supports authentication for all users. It supports individual passwords for all human users and uses machine-to-machine authentication for system users.

AC3-SCA: Authentication using individual passwords for human users

The SCADA application shall support password-based authentication for all human users. The SCADA application shall secure the log on procedure 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 has been inactive for more than an administratively configurable maximum period.

Passwords are stored salted and hashed.

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

AC5-SCA: Machine-to-machine authentication for enterprise IT systems

The SCADA application shall be able to use mutual authentication for enterprise IT systems. The SCADA application shall allow administrators to change the passwords or keys used.

Remark: Authentication can for instance be implemented using transport layer security (TLS) with client-side certificates or with passwords, if the passwords are randomly generated and sufficiently long.

3 Cryptography

The SCADA application uses cryptography for several functions:

- Machine-to-machine authentication for the SCADA system and central maintenance system (Section 2);
- Hashing passwords used by human users (Section 2);
- 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 SCADA application uses strong cryptographic keys and algorithms to protect against attacks to the cryptography itself.

CR1-SCA: Strong cryptographic keys and algorithms

For security functions, the SCADA application 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 [3] recommends as suitable for new or future systems.
- It uses keys as least as long as the ECRYPT report recommends for near-term use (section 4.6 in [3]).
- It only uses a dedicated cryptographic pseudo-random number generator meeting the requirements in the ECRYPT report [3] 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.

Remark: When validating a certificate, the identity of the user can be checked through the subject name, common name, or distinguished name. The role could be checked through the attribute certificates described in IEC 62351-8 [4].

4 Operations security

The SCADA application 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 SCADA application should allow the servers on which it runs to be upgraded without disruptions.

OP1-SCA: Future-proof design

The SCADA application shall allow to extend the computing and storage resources on the servers on which it runs without disrupting its normal working.

4.2 Protection from malware [A.12.2]

To prevent, detect and recover from malware related threats, the SCADA application should allow endpoint protection on the servers and workstations on which it runs.

OP4-SCA: Anti-virus software

The SCADA application developer shall provide recommended anti-virus software for workstations and servers that has been tested to work with the SCADA application without affecting its operations.

OP5-SCA: Hardware assisted measures against exploits

If the SCADA application is compiled in a language that is not memory-safe, it shall be compiled to use the following hardware features:

- No-Execute (NX) / Write-xor-execute (W^R);
- Address Space Layout Randomization (ASLR).

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

4.3 Logging and monitoring [A.12.4]

To support detecting and responding to security incidents, the SCADA application should log relevant security events.

OP8-SCA: Security events

The SCADA application shall be able to log security events for the following in a local log:

1. Successful authentications
2. Failed authentication attempts
3. Changing the system time
4. Changing keys or credentials
5. Failed attempt to change keys or credentials
6. Changing user accounts
7. Changing authorizations

The log entries for security events shall include a timestamp, an event description, and the role causing the event. Events caused by engineers are linked to individual users.

4.4 Control of operational software [A.12.5]

To control the software installed in the SCADA system, an efficient and secure update mechanism is set up.

OP11-SCA: Support for secure software updates

The SCADA application shall support efficient and secure updates. It allows

- Testing of updates is automated as much as possible.
- Software can be centrally updated, and the installed versions monitored.
- The authenticity of software is automatically verified during installation.

4.5 Technical vulnerability management [A.12.6]

The SCADA application must support effective vulnerability management by:

- Avoiding vulnerabilities by supporting hardening
- Allowing vulnerabilities to be detected by vulnerability scanning
- Allowing vulnerabilities exposed to the outside to be patched immediately

Other vulnerabilities can be patched during periodic updates.

OP12-SCA: Hardening

The SCADA application shall support hardening by removing or sdisabling unneeded functions. Specifically, the SCADA application station shall allow:

- all unused user accounts to be removed;
- all unused network services to be disabled.

OP13-SCA: Vulnerability scanning on the SCADA system

The SCADA application shall allow scanning with active vulnerability scanners without disrupting normal operations.

Remark: Preferably authenticated scans are used, in which the vulnerability scanner logs in on machines to get exact information on the software installed.

OP14-SCA: Immediate updates for hosts exposed to the outside

The SCADA application shall allow security updates to be applied immediately to hosts that are exposed to the outside on the data exchange and remote access interfaces without a risk of disrupting the core SCADA system.

Remark: Updates could of course cause a risk of disrupting data exchange with enterprise IT systems or remote access by the SCADA vendor. But all other functions should be unaffected. To achieve this, the exposed hosts should be isolated and should only be used for functions that require outside connections.

The SCADA application must allow security updates for vulnerabilities in all software: the application itself, middleware, operating systems, virtualization software, and network equipment firmware.

Security updates can be applied to other systems during periodic maintenance.

The SCADA application developer must provide security updates for severe vulnerabilities according to requirement SD8-SCA.

5 Communication security

5.1 Network security management [A.13.1]

The SCADA application should support securing communications to enterprise IT servers. If possible, it should support end-to-end secure connections to (external) field devices by using TLS.

CM1a-SCA: Confidentiality and integrity of network communication to IT servers

The SCADA application shall be able to cryptographically protect the integrity and confidentiality of communication on the data exchange interface to IT servers. The measures shall allow to verify the source of messages and protect against replay attacks.

CM1b-SCA: Confidentiality and integrity of network communication to field devices using TLS (optional)

The SCADA application should be able to cryptographically protect the integrity and confidentiality of communication on the WAN interface to (external) field devices using TLS as specified in IEC 62351-3 [5] and IEC 60870-5-7 [6]. Mutual authentication should be used as specified in IEC 62351-8 [4].

The SCADA application should allow to turn off encryption and use only message authentication by using the NULL cipher, so that it is possible to apply deep-packet inspection.

Remark: The NULL cipher is not allowed by IEC 62351-3 [5], but is useful to have better security monitoring.

6 System acquisition, development and maintenance

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

The SCADA application developer should integrate security throughout their development process to ensure that secure software is delivered.

SD1-SCA: Secure programming practices

The developer shall set up secure programming practices for the SCADA application. They shall:

- define secure coding guidelines;
- provide security training to developers;
- use an issue tracking system with traceability for security issues.

SD2-SCA: Version control for source code

The developer shall implement a version control system for the SCADA application source code. The version control system shall:

- provide an audit trail of all source code committed;
- allow each commit to be traced to an individual developer;
- ensure the integrity of the audit trail and committed source code.

Remark: Integrity of the source code can be ensured by using hash values as identifiers for the commits. The full history of previous commits should be included in the hash value to protect the audit trail. For additional security, the hash value should be signed with a key that is unique for each developer.

SD3-SCA: Internal code reviews

The developer shall set up a process for internal code reviews. All code shall be reviewed by at least one other developer who takes security into account. Automated static code analysis tools shall be used to detect common programming errors.

Remark: Preferable code reviews are applied to each commit, so that issues can be found and fixed quickly.

SD4-SCA: Secure build process

The developer shall secure the software build process by:

- ensuring the build server validates the integrity of source code it gets from the version control server;
- enabling compiler options to harden binaries;
- keeping the build configuration and settings under version control;
- creating unique identifiers (such as a hash value) for each build;
- signing executables and other build artifacts on the build server;
- protecting the build server and signing keys against compromise.

Remarks: 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).

It is recommended to keep the signing certificates in a Hardware Security Module (HSM) or Trusted Platform Module (TPM).

The signature generated by the built server should be checked at the endpoints before installation.

SD5-SCA: Security testing during development

The developer shall test each software release to check the implementation of the requirements in this document. Testing shall at least include:

- functional testing for all functional requirements;
- robustness testing of all custom protocol implementations;
- automated web application testing on all web interfaces;
- automated checking for known vulnerabilities in libraries or containers;
- automated vulnerability scanning.

Remark: The SCADA application developer should make sure their code checks the validity of all received data, including validating if the input 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 web interfaces or the implementation of domain-specific protocols, such as IEC 104. For web services, it is recommended to follow the recommendations from the Open Web Application Security Project (OWASP).

Where possible, tests should be an automated part of the build process. Vulnerabilities in libraries and containers can be checked using Software Composition Analysis (SCA) tools or container vulnerability scanners.

SD6-SCA: Support for independent testing

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

- allowing them to audit the development process;
- providing documentation on how the requirements have been implemented;
- providing them 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.

SD7-SCA: Secure configuration guidelines

The developer shall provide guidelines on how to securely configure and operate the SCADA application, covering at least:

- expected security measures in the operating environment;
- hardening;
- account management;
- setting up secure password policies;
- enabling authentication measures;
- configuring cryptographic measures;
- setting up key management;
- setting up backups;
- installing endpoint protection on SCADA hosts;
- setting up capacity monitoring;
- setting up security logging.

SD8-SCA: Vulnerability handling

The developer shall create security updates to fix all severe vulnerabilities found during the lifetime of the SCADA application. 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.

Remarks: 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 in 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 SCADA developer protects information of the grid operator or under his responsibility, it needs to implement an information security management system (ISMS).

SR1-SCA: Protection of customer assets

The developer shall have an ISMS to protect any information and systems that could compromise the security of the SCADA system, including:

- detailed security designs;
- source code;
- customer-specific keys and credentials;
- test systems at the SCADA developer;
- systems used for remote access.

The ISMS shall be ISO/IEC 27001 certified and the certification scope shall cover the development and support of the SCADA application and related software.

Remark: Details of measures to be implemented can be agreed during negotiations. It is recommended to further specify at least:

- screening of personnel;
- support in case of security incidents;
- protection of test systems;
- handling of confidential information;
- monitoring of compliance with agreed measures.

SR2-SCA: Remote maintenance

If the developer performs remote maintenance on the SCADA applications, its employees shall only do this from a physically secure section of the offices of the developers. The networks from which remote maintenance is performed, shall be segregated to minimize the likelihood of a compromise. A jump server in the SCADA system shall be used.

Remark: For the physical security of the location the controls in ISO/IEC 27001 Section *A.11 Physical and environmental security* [1] should be followed. Access to the location should be restricted to staff involved in remote maintenance work.

8 Information security aspects of business continuity management

8.1 Information security continuity [A.17.1]

The SCADA application is designed to be run on redundant systems to be able to resist natural disasters and power outages. It is designed to fail securely to ensure that its security is not compromised during disruptions.

BC1-SCA: Geographic redundancy

The SCADA application shall be able to support high-availability (HA) and disaster recovery (DR).

BC2-SCA: Fail-secure design

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

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

Glossary

(A)DMS	(Advanced) Distribution Management System
APN	Access Point Name
CVSS	Common Vulnerability Scoring System
DMZ	Demilitarized Zone
DoS	Denial-of-Service
DSO	Distribution System Operator
EMS	Electricity Management System
IED	Intelligent Electronic Device
ISMS	Information Security Management System
OT	Operational Technology
PKI	Public Key Infrastructure
RADIUS	Remote Access Dial-In User Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Incident and Event Management
TLS	Transport Layer Security
TSO	Transmission System Operator
VPN	Virtual Private Network
WAN	Wide Area Network

References

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

[2] ENCS, SC-201-2020: Security architecture for SCADA systems 2020.

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

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

[5] 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.

[6] 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.

[7] ENCS, SC-101-2020: Security risk assessment for SCADA systems, 2020.