BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Österreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

Verband Schweizerischer Elektrizitätsunternehmen
Hintere Bahnhofstrasse 10
5000 Aarau
Schweiz

Whitepaper Requirements for Secure Control and Telecommunication Systems

Completely revised version 3.0 09/2024:

Aarau/Berlin/Vienna, 30th September 2024

Change history

Version	Date	Comments (editor)
1.0 Final	December 2011	Project Team Oesterreichs Energie / BDEW
1.1 Final	November 2014	Adaptation of standard references to reflect the contents of ISO/IEC 27002:2013 and ISO/IEC TR 27019:2013
2.0	May 2018	Thorough update and revision (project team Oesterreichs Energie / BDEW)
3.0	September 2024	Fundamental update and revision Version 3.0 (Oesterreichs Energie / VSE / BDEW project team)

Joint publishers

Österreichs E-Wirtschaft

Brahmsplatz 3, 1040 Wien, Österreich

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32, 10117 Berlin, Deutschland

Verband Schweizerischer Elektrizitätsunternehmen

Hintere Bahnhofstrasse 10, 5000 Aarau, Schweiz

Contact

Armin Selhofer (Österreichs E-Wirtschaft)

Mathias Böswetter (BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.)

Markus Riner (Verband Schweizerischer Elektrizitätsunternehmen)

Expert advice and support

Dr. Stephan Beirer and Marl Joos (GAI NetConsult GmbH, Berlin/Germany)

Contents

1 Introduction and Scope 6
2 Outline and Structure of this document 6
3 Instructions for use 8
3.1 System planning and tendering 8
3.2 Applicability to Existing Systems 9
3.3 Service and Maintenance 9
3.4 Use of new technologies 10
4 Security Requirements 11
4.1 General Requirements 11
4.1.1 Secure System Architecture 11
4.1.2 Patching and Patch Management 13
4.1.3 Provision of Security Patches for all System Components 15
4.1.4 Support for Deployed System Components 16
4.1.5 Encryption of Confidential Data 17
4.1.6 Cryptographic Mechanisms 18
4.1.7 Public Key Infrastructure 19
4.1.8 Secure Standard Configuration 20
4.1.9 Integrity Testing 21
4.1.10 Use of Cloud Services 22
4.1.11 Documentation Requirements 24
4.1.12 Physical Security 26
4.1.13 Integration into Systems for Detection of Anomalies and Attacks 27
4.2 Project Management 29
4.2.1 Contacts 29
4.2.2 Security and Acceptance Testing 30
4.2.3 Secure Data Storage and Transmission 31
4.2.4 Delivery of Project-Specific Modifications 32
4.3 Base system 34
4.3.1 System hardening 34

4.3.2 Malware Protection 36
4.3.3 Autonomous User Authentication 37
4.3.4 Virtualization Technologies 39
4.3.5 Container Virtualization 40
4.3.6 Industrial IoT 42
4.3.7 Role Concepts Base system 43
4.4 Network and Communications 45
4.4.1 Use of Protocols and Technologies 45
4.4.2 Secure Network Structure 48
4.4.3 Documentation of Network Structure and Configuration 50
4.4.4 Secure Remote Access 51
4.4.5 Wireless Technologies 53
4.4.6 Network Authentication 54
4.5 Application 55
4.5.1 Role Concepts 55
4.5.2 User Authentication and Login 56
4.5.3 Authorization of Actions at User and System Levels 58
4.5.4 Web Applications and Web Services 59
4.5.5 Integrity testing 60
4.5.6 Logging 61
4.6 Development 63
4.6.1 Secure Development Standards, Quality Management and Approval Processes 63
4.6.2 Secure Development and Test Systems, Integrity Testing 65
4.7 Maintenance 67
4.7.1 Maintenance process requirements 67
4.7.2 Secure Update Processes 69
4.7.3 Configuration and Change Management, Rollback 70
4.7.4 Vulnerability Management and Patch Information Service 71
4.7.5 Maintenance Contract / Service Level Agreement 73
4.8 Data back-up and Emergency Planning 76
4.8.1 Backup: Concept, Procedure, Documentation, Testing 76

4.8.2 Emergency Concept and Recovery Plans 77
A Network zone diagrams 80
Network zone diagram 1 80
Network zone diagram 2 81
B List of abbreviations and glossary 82
C References and Links 87
International standards 87
Frameworks and recommendations for action 87

1 Introduction and Scope

This document defines fundamental security requirements for OT- and telecommunication systems for process control in energy supply and provides implementation instructions. For this purpose, current and industry-specific recommendations for ensuring information security compiled by technical experts are listed.

The Whitepaper defines requirements for both individual components and systems / applications assembled from these components.

To complement these requirements, the document also covers security requirements for maintenance processes, project management and development processes.

The document places prime focus on requirements related to the procurement phase of technical components and systems and to processes relevant to the project's implementation. Organizational, personnel and physical security measures in operator organisations such as the establishment of a security organization, appropriate risk management or the creation of comprehensive security awareness among employees – are equally important, but not the focus of this Whitepaper. Please refer to the standards ISO/IEC 27001 and ISO/IEC 27019 where such requirements are covered in more detail.

This document is a completely revised new edition of the BDEW Whitepaper, in which the content has been comprehensively updated and amended in line with current technological developments.

In this document, the term *Operational Technology* (abbreviated *OT*) refers to all the technologies defined and described in Table 1. It should be noted that there is no generally accepted definition of OT and that it may differ depending on the organization. Appendix B "List of abbreviations and glossary" contains further alternative definitions of this term.

2 Outline and Structure of this document

In this document, OT- and telecommunication systems for process control in energy supply are referred to as "systems" or "entire system". These systems usually consist of individual components. Such components can also be standalone devices that perform (partial) tasks in process control and telecommunications for energy supply.

The chapters 4.1 to 4.8 cover requirements for the entire system and individual components, structured by topic. In their respective sub-chapters, the first table specifies the actual security requirements, preceded by references to the so-called controls of the International Standards ISO/IEC 27002:2022 *Information security controls* and its energy sector specific expansion ISO/IEC 27019:2017 *Information security controls for the energy utility industry*. Please note that these references only cover the implementation guidance set out in these particular standards. While they can serve as a valuable reference and resource for implementing the Whitepaper requirements, the Whitepaper systematic itself differs from that of the ISO/IEC 27000 standard series. So, the referenced ISO standard controls might only cover part of the respective Whitepaper requirements.

The “Additional information and notes” section in the following table contains general remarks and implementation examples that are relevant to all technology areas pertaining to the field of OT in energy supply. Subsequently, and where applicable, specific implementation notes are listed for the three main technology areas to be found in the energy supply process environment: "operations management- / control systems and system operation", "transmission technology / voice communications" and "secondary, automation and telecontrol technologies". The following categorization is used for the three areas:

Technology category	Description and examples
Operations management- / control systems and system operation:	All centralized systems that are used for process control and -monitoring and operations management in the area of energy supply as well as required supporting central IT/OT systems, applications and related central infrastructure. Examples: • Central grid control and grid management systems • Power plant control systems • Central systems for monitoring and control of distributed generators and loads, e.g. virtual power plants, storage management, central control room systems for hydroelectric plants or photovoltaic / wind power installations • Systems for fault management and work force management • Central metering and measurement management systems • Data archiving systems • Central parameterisation, configuration and programming systems • Supporting systems required for operation of the above-mentioned systems, e.g. programming and parameterisation devices
Transmission technology / voice communications:	The transmission, telecommunications and network technology used in OT for voice and data communications. Examples: • Routers, switches and firewalls • Transmission technology-related network components • Terminal devices for voice communication • Phone installations, VoIP systems and associated servers • Digital radio systems • Central management and monitoring systems for transmission, telecommunications and network technology

Secondary, automation and telecontrol technologies:	Process-oriented control and automation technology as well as associated protection and safety systems and telecontrol components. In particular, these include the technology in substations and plants as well as the automation technology in generation and storage facilities. Examples: • Control and automation components • Control and field devices • Telecontrol devices • Controllers and PLCs including digital sensor and actuator elements • Protection devices • Safety components • Digital measuring and metering installations • Synchronisation devices • Excitation systems

Table 1 : Technology categories

Note: In this paper, the term "contractor" refers to actors to whom security requirements may be addressed directly or indirectly after the contract has been awarded. These include, for example, manufacturers, suppliers, system integrators or external planners.

3 Instructions for use

3.1 System planning and tendering

This Whitepaper is aimed at manufacturers, suppliers, system integrators and external planners on the contractor side as well as in-house planners, implementers and operators on the client side.

For contractors, the requirements and implementation instructions should already prove helpful for product and system development and should therefore be taken into account at an early stage. This applies in particular to the further development of systems and components over their entire lifecycle.

Clients are recommended to select necessary security requirements early during the planning phase and based on a custom risk analysis. Based on these risk analysis results, clients should then specify how the separate requirements should be met for the intended system The supplementary implementation recommendations listed in the chapters are intended to provide support in this phase in particular. If peripheral IT systems (e.g. directory services, file servers, backup systems, etc.) are part of the contractor's scope of supply and services, the associated security requirements of this document should also be fulfilled.

If the planned project is intended for tender, the identified security requirements need to be included in the technical specifications after the planning phase is concluded. The actual call for

tenders should include a copy of this Whitepaper and a definition of concrete requirements and additional measures as well as implementation specifications and permissible deviations and exceptions.

In their bids, contractors must include a detailed statement on how they intend to implement these technical and organisational requirements and any necessary deviations and proposals for alternatives. These must be evaluated by the tendering party and taken into account during the selection process. The non-application of measures must be evaluated and documented by the planners, implementers or operators on the client side as part of a risk analysis resp. managed within the risk treatment process.

Clients should bear in mind that there are currently no procedures recognized by the publishers of the Whitepaper for certification or conformity testing of components or systems and that information on Whitepaper-conformity must therefore be critically reviewed by the client.

The entire system's security concept should be audited during the design and technical specifications phase as well as subsequent to any substantial changes by an external security expert.

3.2 Applicability to Existing Systems

The security measures described in this Whitepaper are recommended for all new control or telecommunication systems. Technological restrictions, however, might make it impossible to fully apply these measures to existing systems. At the same time, and especially in case of upgrades or expansions, all implementation options should be reviewed and evaluated as part of a risk analysis and – where applicable – additional security measures should be included. The Whitepaper can also be used to carry out a gap analysis in order to identify possible risks to existing systems.

3.3 Service and Maintenance

Consideration of security is not restricted to the planning phase and project implementation, but also covers the entire system and product lifecycle. This is especially true for maintenance as well as ongoing further development and bug fixing.
Therefore, at the time of the tender or project realisation procedures between the client and the system supplier or respective service provider must be agreed, which regulate the relevant details of maintenance processes and security-specific services such as patch management, malware protection or system upgrades and migrations. As a rule, maintenance contracts must be concluded for this purpose and binding procedures for migration must be defined.

Maintenance services require the definition of, in particular, specific security requirements for the IT components used (and potentially also operated by) the service provider for maintenance. Any such agreements should include the right to audit to verify and review the correct implementation of the stated requirements.

3.4 Use of new technologies

The rapid development and application of new IT technologies from business and commercial IT is finding its way into the field of OT at an ever-faster pace. These novel and promising technologies can lead to cost savings and improvements in functionality. However, relevant information security aspects must be adequately considered, tested and subjected to a risk assessment prior to the introduction of any new technologies. A range of topics deserve closer attention and examination:

- Identification and assessment of known security gaps and vulnerabilities
- Assurance of reliability and stability during operations
- Availability check of the product itself resp. the associated replacement part as well as software patches across the systems' entire lifecycle (where applicable)
- Assessment of the dependency on third-party products such as open source libraries or proprietary software
- The client's patch policy throughout the product lifecycle
- Review of adaptability across the entire lifecycle, e. g. to accommodate future cryptographic algorithms and key lengths
- Clarification of complexity related to the swift restoration of normal operations after disruptions and outages
- Fulfilment of the requirements for real-time operations
- Compliance with safety requirements for people and the environment, even for high system security settings
- Manufacturer expectations concerning the product's connection to public networks or similar (internet availability or cloud connectivity)
- Fulfilment of requirements for Critical Infrastructures resp. operators of essential services.

4 Security Requirements

4.1 General Requirements

This chapter defines general and overarching security requirements that are applicable to the entire project and all areas of technology.

4.1.1 Secure System Architecture

Security requirements	ISO/IEC 27002:2022 8.3, 8.14, 8.22, 8.27, 8.30 ISO/IEC 27019:2017 13.1.3, 17.2.1 Individual components and the entire system must be designed and developed for secure operations. Secure system design principles include: **Security by design:** The entire system and its individual components are developed from the ground up with security in mind. Deliberate attacks and unauthorised actions are explicitly taken into account while any repercussions arising from a security event are minimised by the system's inherent design. **Minimal need-to-know principle**: Each component and each user is only assigned the rights they need to execute a desired action. Applications and network services, for examples, are executed with administrator privileges, but only with the bare minimum of required system access rights. **Defence-in-depth principle**: Security risks are not tackled via single protection measures, but limited through the implementation of staggered, multi-level and complementary security measures. **Redundancy principle**: The entire system is designed to ensure that the failure of individual components does not impair security-related functions. The system's design lowers the likelihood and impact of issues caused by unrestricted requests for system resources such as e.g. main memory (RAM) or network bandwidth (so-called resource consumption or DoS attacks).

Additional information and notes:	Security requirement 4.1.1 is primarily for system designers and developers. It should serve as a general guideline for the entire system design and the related development process. Beyond the above-stated, fundamental security principles, there are a range of further sensible, additional design principles that deserve consideration, a. o. access control, input sanitation and validation, default deny etc. The redundancy principle should be considered a general design principle that complements the defence-in-depth principle. It states that the failure of individual system components or security functions should never lead to a total system or security mechanism failure. For security functions, this most of all means logical redundancy in the sense of the

		defence-in-depth principle, where the entire system needs to have several, staggered security functions. At the same time, this does not necessarily mean that all components should come in duplicate (hardware redundancy). Examples of suitable measures to create redundancy and implement the defence-in-depth principle: • Implementation of runtime monitoring mechanisms, e. g. watchdogs, exception handling etc. • Real-time malware protection of the system components complemented by simultaneous scanning of all data interfaces and blocking of unnecessary interfaces like USB ports or removable storage devices • Deactivation or, preferably, deinstallation of unnecessary services like e. g. DHCP • Data consistency checks at both the external application interface and at interfaces between the different system modules within the application • Communication gateways with application level verification functions, e. g. to filter for approved resp. unauthorised telegram types • Redundancy of transmission pathways plus prevention of connections via the public internet • Verification of source addresses (IP addresses) of telecontrol telegrams not only at the substation‘s external interface (firewall), but also by the target component • Independent, fault-tolerant implementation of critical plant safety functions The implementation of a secure system architecture should be described in the system’s documentation.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.1.2 Patching and Patch Management

Security requirements	ISO/IEC 27002:2022 8.8 All system components must be patchable. The contractor must support a patch management process for the individual components and the entire system, designed to enable the control and management of security patch and update testing, installation and documentation. The operator himself resp. the assigned service provider must be able to install the security patches and updates. Patch installations resp. uninstalls must be authorised by the operator and shall not occur automatically. Any installation resp. uninstall shall be recorded in a transparent and tamper-proof way within the system. The integrity of security patches and updates must be verifiable using a cryptographic mechanism. Any security patch installation and uninstall or rollback procedure shall be documented in detail for all system components. The patches require clear versioning by the contractor. If and when the entire system resp. its components require functional testing after an update, this must be automated, if possible, and corresponding mechanisms designed into the system. The contractor has to document both the necessary test cases and the expected results of a successful test run (test book). Processes executed as part of this patch management must meet recognised operating and service management standards. In the process of awarding the project contract it must be ensured that the contractor must implement a patch management process covering the entire project term. Patch management during the operating phase is typically contractually agreed on in a separate maintenance contract, see section 4.7.5 "Maintenance Contract / Service Level Agreement".

Additional information and notes:	Patching refers to the implementation of security-relevant and functional software updates. This involves the correction of faults or errors as well as the expansion, addition and optimization of functionalities. Patching occurs at the application level, but also on all underlying system components (e. g. base and operating systems, databases, software libraries and third-party components, firmware, BIOS and management interfaces etc.). If the contractor doesn't deliver the system in its entirety, the necessary processes and requirements for installing security patches and other updates for the third-party components used in the system should be specified. Ideally, patches should be applied without disrupting normal operations and with minimal impact on the entire system's availability. For example, a primary technical shutdown of the entire installation should be

		avoided when patching secondary technical components. Therefore, patches should first be applied to inactive redundancy components and only installed on the remaining components after a switch-over process (switching of the active component in the redundancy system) and after a subsequent basic functional test resp. trial run. In particular, higher-level systems without direct process integration should be implemented in a way that would render an installation shutdown for patching unnecessary. The entire system should also be designed to reduce the number of required security patches resp. patchable components as well as, where applicable, necessary operation interruptions to a bare minimum. This can be supported by comprehensive hardening measures (see 4.3.1). Depending on the criticality of the systems, a customer-specific test system at the contractor's premises and, possibly, an additional test system at the customer's premises may be required to carry out functional tests. Fallback resp. rollback options in case of faulty patches or failed tests should be designed to facilitate a fast and easy return to the latest functional version and configuration state. Patch management should also cover embedded components, parameterisation and management systems as well as management interfaces. If patches require certain firmware versions, this must be checked and ensured separately. Recognized operational and service management standards include COBIT and ITIL, for example. Usually, patch management requires administration tools and systems for system and version management (e. g. central update servers, versioning and configuration management databases etc.). These should be run on a separate infrastructure from the office IT.
	Operations management / control systems and system operation:	In case of high availability requirements redundancy components should be used to ensure continuous operation.
	Transmission technology / voice communications:	Network components and network elements, terminal devices and central communications, management and monitoring systems should all be included.
	Secondary, automation and telecontrol technologies:	The installation of security and firmware updates for process-related components (e.g. controllers, PLCs, field units, protection devices) might require a facility shutdown, e.g. during a revision. Ideally, such components should be implemented and installed at the clients site in a way that allows for on-location patching with minimal testing efforts and without removal of the actual components. Where process-related components are subject to heightened availability requirements or where no shutdown is possible for software and/or firmware changes, it should be checked whether these components

		might be suitable for patching during operations. Usually, this will require a redundant operational set-up of the components in question.

4.1.3 Provision of Security Patches for all System Components

Security requirements	ISO/IEC 27002:2022 8.8, 8.19 ISO/IEC 27019:2017 12.5.1, 12.6.1 The contractor must ensure that security updates are made available by him for all system components throughout the entire contractually stipulated operating timeframe and in line with the patch management process and, if necessary, are installed by him. The contractor shall obtain, test and – where necessary – forward updates from the respective manufacturers for basic components that were not developed by the contractor himself such as the operating system, libraries or database management systems. All update testing, approval and delivery shall take place within an adequate, contractually stipulated timeframe.

Additional information and notes:	The patch provision process should cover all software and system components included in delivery, e. g. base and operating systems, databases, software libraries and third-party components, firmware, BIOS and management interfaces etc. For this purpose, the contractor should provide an inventory in which the software components included in the provisioning process are identified at least for all networked system components. Usually, security patches and updates need to be reviewed and approved individually by the contractor prior to installation. Depending on system criticality, this might require a client-specific testing system at the supplier‘s location and, where necessary, an additional testing system at the client’s location. Less critical applications might only require generic approval of certain patch and update categories by the contractor. Information on necessary updates should be made available to the client in a frequent and timely manner (see 4.7.4 Vulnerability Management and Patch Information Service). For many control technology types and application scenarios it makes sense to assume a longer-term operating timeframe of the entire system or individual components (e. g. secondary / automation technology components or telecontrol technologies). This timeframe usually exceeds the lifecycle of individual software products by far. Where system components are used that most likely won’t last the entire system’s envisaged operating timeframe (e. g. typical PC-based components), the system should be designed for easy replaceability, complemented by a roughly outlined and contractually stipulated procedure for migration.

		For binding agreements on this topic, which are concluded as part of a maintenance contract, see 4.7.5. "Maintenance Contract / Service Level Agreement". It should be noted that redundancy components are no replacement for dedicated test systems.
	Operations management / control systems and system operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technology:	-

4.1.4 Support for Deployed System Components

Security requirements	ISO/IEC 27002:2022 8.8, 8.30 ISO/IEC 27019:2017 12.6.1 The contractor must ensure that within the planned and contractually stipulated operating timeframe, manufacturer support and security updates are available for system components developed by both the contractor and third-parties (e. g. operating system, database management system etc.). A binding agreement should cover the discontinuation procedure as well as relevant minimum terms like e. g. last customer shipping and end of support. Security support must also include the parameterization and configuration tools required for operation. Configuration and parameterization must be possible for the defined term using a supported parameterization and configuration tool.

Additional information and notes:	Operating timeframes that exceed the lifecycle of system or software components increase security risks and should therefore be absolutely avoided. Contractorss should offer corresponding support for both their own and third-party products and, at the time of signing the contract, define migration procedures for any products with long lifecycles. To begin with, third-party components (e. g. operating system, protocol stacks etc.) should only be used if and where they are up-to-date and supported throughout the entire planned term of operations. Due to the expected extended operating timeframes of systems covered by this Whitepaper, contractors are often unable to provide such a guarantee.

		To reflect this particular concern, they should include rough concepts and cost estimates for a migration to newer versions. Furthermore, and unless there are technical reasons to the contrary, system and component versions should be up-to-date at the time of commissioning. A particular challenge lies in the significant discrepancies between the envisioned system lifecycle and the lifecycles of third-party software components. A migration concept for these systems should be developed and included. If the client insists on the use of specific products resp. versions in tenders or projects, the client needs to honour this stated requirement.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.1.5 Encryption of Confidential Data

Security requirements	ISO/IEC 27002:2022 5.33, 5.34, 8.15, 8.21, 8.24 ISO/IEC 27019:2017 10.1.1, 12.4.2, 13.1.2, 18.1.3, 18.1.4 Confidential data must only be stored resp. transmitted encrypted. Where protection requirements are obvious (e. g. for authentication information like passwords), the contractor should already include respective measures in the standard configuration.

Additional information and notes:	The protection of confidential data should take both information security aspects and data protection requirements into account. The contractor should provide a list of the data processed by the system as standard. The client determines which of these data should be considered confidential. Confidential data might, for example, include log files, passwords, parameterisation data or confidential data according to official regulations or relevant legislation such as e. g. the Federal Data Protection Act or the General Data Protection Regulation. Where applicable, the system should also facilitate the secure, selective deletion of certain data, e. g. via overwriting with random data or the anonymisation of specific data.

	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.1.6 Cryptographic Mechanisms

Security requirements	ISO/IEC 27002:2022 5.33, 8.24 ISO/IEC 27019:2017 10.1.2, 13.1.4 ENR When selecting cryptographic mechanisms, national legislation shall be taken into account. Only approved mechanisms and minimum key sizes shall be used that are considered secure for the foreseeable future according to state-of-the-art technological knowledge. Use of custom cryptographic algorithms is not permitted. Deviations from this may only be used after explicit approval by the client. Where the technology allows it, the selected cryptographic mechanisms must be replaceable by a more up-to-date equivalent as part of an update. Along similar lines, it should also be possible to deactivate or uninstall out-of-date mechanisms. Where possible, the implementation of cryptographic mechanisms must involve recognised libraries to avoid implementation errors.

Additional information and notes:	The BSI recommendations of the TR-02102 series "Cryptographic Mechanisms: Recommendations and Key Lengths" (Federal Office for Information Security, Germany) are regarded as the state of the art for hashing, signing and encryption methods and the associated key lengths. This might be of particular relevance for embedded components, which often have resource restrictions and might require different algorithms and key sizes. For its particular field of application, the IEC 62351 standard series defines clear minimum requirements for supported cryptographic mechanisms. During the selection of the mechanisms implemented and used in the project, these requirements as well as the above-mentioned recommendations by the BSI should be consulted.

		It might be advisable to use cryptographic hardware modules like a trusted platform module (TPM) for key management, random number generation etc. When selecting cryptographic mechanisms, developments in post-quantum cryptography should be taken into account, see, for example, BSI publication *Kryptografie quantensicher gestalten*.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	

4.1.7 Public Key Infrastructure

Security requirements	ISO/IEC 27002:2022 8.24 ISO/IEC 27019:2017 10.1.2 If digital certificates are used in the system, a PKI must be established. The use of untrusted, self-signed certificates (see below) is not permitted. All cryptographic keys and certificates must be replaceable by the operator. It must also be possible to integrate a PKI provided by the operator. The processes required for the exchange of certificates must be fully documented in the system documentation. Secure procedures such as SCEP or EST must be used for autoenrollment of X.509 certificates. Before using certificates, their validity and authenticity must be validated; when establishing encrypted connections, this must be done by both communication partners on each side. Certificates and certificate chains recognized as invalid or faulty must not be accepted. When using a PKI or digital certificates, potential failure and emergency scenarios must be taken into account, such as the failure of PKI systems or the invalidity of digital certificates. For these scenarios, core processes (e.g. login processes for users or services) should still be possible. If a PKI operated by the supplier or a third party is used, the following points must be contractually regulated:

	• Secure generation of key material • Secure storage / archiving of key material • Secure deletion / destruction of key material • Access protection and physical security for the above-mentioned processes • Definition and documentation of a security guideline for the use of cryptographic processes and products

Additional information and notes:	Self-signed certificates are not signed by a trustworthy CA, but with the private key belonging to the certificate. Therefore, they cannot be verified easily. If a PKI operated by the supplier or a third party is used and there are increased security requirements or increased protection requirements, an obligation to implement BSI TR-03145-1 may be appropriate. CRLs distributed automatically in the system or OCSP / OCSP stapling shall be used for the certificate check. Alternatively, a very short certificate lifetime (few hours to days) and a short-cycle, automated roll-out process can be provided. The system components should generate a warning message if a certificate expires in less than 180 days. Use cases for digital certificates include securing network communication (TLS), code signing, email encryption and signing via S/MIME or server and client authentication.
Operations management / control systems and system operation:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	-

4.1.8 Secure Standard Configuration

Security requirements	ISO/IEC 27002:2022 8.9, 8.18, 8.19, 8.33 ISO/IEC 27019:2017 12.5.1 After initial installation, resp. at start-up or restart, the entire system shall be configured for a secure operating state. This defined basic configuration shall be documented. Services and functions as well as data

	that are only needed for development or testing shall be removed demonstrably resp. permanently deactivated before delivery resp. before the switch to live operations. If and where the operator's system environment requires further security settings, configurations etc. that deviate from the standard installation, these should be explicitly documented.

Additional information and notes:		
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.1.9 Integrity Testing

Security requirements	ISO/IEC 27002:2022 8.19, 8.25, 8.32 It must be possible to check system files, applications, configuration files and application parameters for integrity, for example through cryptographic checksums.

Additional information and notes:	A secure integrity testing option is required for the operating system's system data; configuration files and application parameters; and firmware parameters and firmware versions. To preclude resp. recognize deliberate manipulations, such testing usually requires cryptographically calculated checksums. It should be possible to automatically read out component parameters defined by the client (e.g. via standardized interfaces for asset management tools or via the engineering tool). It must not be possible to read back the firmware or the parameterization / engineering data, which would enable reverse engineering.

		If and where possible, testing of patches and updates should use the same mechanisms (see 4.1.2). Integrity testing at the higher system level should be considered a minimum requirement. In the medium term, efforts should be made to enable integrity testing of all components. Such integrity checks are also of particular importance for change management processes.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	Process-related components should at least include an integrity check option in the configuration tool for parameterisation and firmware versions. Detailed comparability of parameterisation data, especially of offline and online versions and archived parameterisations, should strived for. In the process it should be possible to identify the data areas in which changes have been made.

4.1.10 Use of Cloud Services

Security requirements	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 5.22, 5.23 ISO/IEC 27019:2017 15.1.2 Where cloud services are used, the following requirements apply: a) Agreements must be made with the cloud service provider about security-related processes for cloud infrastructure operations. b) Functions for the control of Critical Infrastructures, where manipulations could threaten the energy supply, must not be realised in cloud services that are not under the control of the operator (the operator's control must include data sovereignty and control over administration and availability). c) Downtime of a cloud service resp. access to this service must not lead to significant restrictions of the system's defined basic function. Cloud service disruptions or outages shall also be considered in the emergency concept and restoration plans (see 4.8.2).

Additional information and notes:	Here, cloud services refer to and include the dynamic use of shared IT resources and IT services like infrastructure (e. g. computing resources, data storage), platforms (e. g. application servers, databases), software and applications across a network. While use of cloud services in the area of OT in energy supply is not unacceptable per se, it requires a critical review as part of a risk assessment, especially where public cloud services are concerned. A corresponding risk analysis should include the evaluation of a cloud reference architecture to ensure that all relevant aspects of cloud use and its risks are thoroughly evaluated. When a cloud service is used, the data owner relinquishes the actual data sovereignty to the cloud service provider. In terms of availability, integrity and confidentiality, the owner needs to be able to rely on the service's secure operations. Where data with heightened security requirements regarding availability, integrity and confidentiality, are involved, this requires special care in terms of data processing and storage. At the same time, the cloud service provider's actual implementation of security-related processes for secure operations isn't always transparent, a. o. when it comes to patch management, back-up, infrastructure protection, secure data transmission and client separation within the cloud infrastructure. Where data are stored in a foreign country, there is no way to assess or anticipate changes in local legislation. Under certain circumstances, third-parties could gain access to the data. It should be reviewed whether data processed or stored by a cloud service needs to be included in the operator's back-up concept. Re: a) The following issues, especially, require binding agreement: • Access authentication/authorisation • Multi-client capability / separation of client data • Specification of data transmission parameters (encryption / integrity protection) and the communications link between client and cloud service provider • Data back-up and recovery • Protection of the service provider's infrastructure • Secure data storage • Patch management of the cloud infrastructure • Human resources security • Physical security of data centres and access control • Location of the cloud provider's performance • Incident handling procedures • Malware protection • Assurance of data deletion • Emergency provisions • Option to audit the service provider • Logging and monitoring

		Recommendations on how to secure cloud services are defined in the International Standards ISO/IEC 27017:2015 *Code of practice for information security controls based on ISO/IEC 27002 for cloud services* and ISO/IEC 27018:2019 *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. Requirements for cloud service providers are also defined in the *checklist for selecting a cloud service* and in the *Cloud Computing C5 criteria catalog* of the German Federal Office for Information Security. Please note that, generally speaking, a cloud service provider's certification according these standards is not sufficient. Secure operations will most likely require additional, binding agreements on the above stated issues. Re: c) Cloud services may, for example, experience downtime due to disruptions in internet resp. cloud access. The corresponding risk can be reduced by a direct data centre connection to the cloud provider.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	

4.1.11 Documentation Requirements

Security requirements	ISO/IEC 27002:2022 5.8, 5.37, 6.3, 8.27 ISO/IEC 27019:2017 12.1.1, 14.1.1 A design documentation must be created during the engineering / specification phase and approved by and handed over to the client. The design documentation must comprehensibly describe how the contractually agreed security requirements will be implemented. Thereby traceability must be established between the individual security requirements defined in the project and the chapters or contents of the design documentation. For individual components and entire systems, the design documentation must contain a description of all security-relevant system settings and parameters as well as their default values and any project-specific settings. Furthermore, the documentation shall list and briefly describe

	security-specific implementation details (like the employed cryptographic mechanisms). The design documentation must also comprise additional information on the entire system's system architecture. This includes the system's basic and fundamental structure as well as interactions between all involved components. In particular, this part of the documentation shall highlight security-related or sensitive system components as well as their mutual dependencies and interactions. Project-specific operating documentation must be handed over to the client no later than at the time of acceptance. The documentation of potentially confidential information, e. g. access data like passwords or open ports, should not be included in the general system and security documentation, but presented to the client in a separate, secure format. The documentation must also point out the consequences of grossly insecure configuration settings. The documentation must contain a description of the requirements for secure system operation.

Additional information and notes:	The contractor should prepare security documentation that summarises all IT security-related information. For example, and besides the actual security configuration and associated parameters, the documentation should also cover system and communication settings like the maximum number of simultaneously logged in users, the maximum number of network connections, minimum network bandwidths etc. All documentation should be kept up-to-date throughout the entire lifecycle of the project. A distinction is typically made between design documentation and operational documentation. Design documentation describes basic architecture and security aspects, while operational documentation describes operational details (e.g. through operating instructions). It is assumed that operational documentation does not contain any specifications that contradict security requirements. There should be separate documentation available for administrators and system users. Both documentation types should, among others, contain a list of the security-related settings and functions for the relevant user group as well as notes on responsible, security-focused actions. In addition, all security-specific log and audit messages should be explained and possible causes and, if necessary, suitable countermeasures should be mentioned. The description of the requirements for secure system operation among other things includes requirements for the user group, network environment as well as interaction and communication with other systems and networks. Likewise, it can include requirements for physical security

		and environmental parameters such as air conditioning, power supply, EMC protection, fire and accident protection, etc. This documentation should be kept up-to-date and always available, e.g. for the on-call service. A review of the documentation should be part of acceptance testing. The design and operational documentation should cover the following topics: • System architecture (e.g. control technology configurator, system configurator, etc.) • Network diagrams and lists (overview as topology through to detailed plan incl. network lists, e.g. VLAN overview, different levels of detail required depending on the project phase) • Communications matrix • Firewall rules • Asset inventory (hardware, software) • physical and logical interfaces, • System descriptions (functional high-level description of the systems) • Software bill of materials (software parts lists), e.g. in accordance with BSI TR-03183-2 • Description of security measures (from specifications to handover documentation) • Security risk analyses from the integrator's perspective
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	Generally, security-related parameters and messages require project-specific documentation as part of the system's planning and design.

4.1.12 Physical Security

Security requirements	ISO/IEC 27002:2022 7.8, 7.9 ISO/IEC 27019:2017 11.1.7 ENR, 11.1.8 ENR, 11.1.9 ENR, 11.3.1 ENR If system components requiring protection are placed in locations where access by unauthorized persons cannot be ruled out, measures must be taken to prevent unnoticed physical access to the system components.

Additional information and notes:		Such measures may include, for example • Locked and door-status monitored cabinets • Tamper-proof housing with opening monitoring • Hardened configuration of local interfaces The opening monitoring system should report alarms to a permanently manned location, e.g. control center or SOC.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.1.13 Integration into Systems for Detection of Anomalies and Attacks

Security requirements	ISO/IEC 27002:2022 8.15, 8.16 ISO/IEC 27019:2017 12.4.1 The system design must be designed for integration into systems for detection of anomalies and attacks. a) If the network hardware is part of the contractor's scope of supply and services, it must be possible to route all network traffic to one or more sensors without any feedback, e.g. via a mirror port or network TAP. b) When using mirror ports, overbooking must not have a negative impact on the system function and performance. c) It must be possible to install host-based sensors on server / PC-based components. d) It must be possible to integrate the messages from the malware protection solution into an attack detection system or SIEM (see 4.3.2 Malware Protection). Data transmission must be cryptographically secured (encrypted, authenticated and integrity-secured). e) It must be possible to integrate the log messages and records of the system components and the entire system into an attack detection system or SIEM (see 4.5.6 Logging). Data transmission must be cryptographically secured (encrypted, authenticated and integrity-secured).

	f) All security-related events (SRE) and operational events relevant to attack detection must be documented. If no system-specific SREs are defined, a reference to the documentation of the upstream supplier, e.g. the operating system manufacturer, is sufficient. g) Baselining must be established to determine which SREs occur in the normal state of operations.

Additional information and notes:		It should be possible to actively analyse the entire system or its individual components for indicators of compromise and integrity without availability restrictions. This includes port scans, vulnerability scans and inventory scans. The use of intrusion prevention systems is only recommended after a risk analysis has been carried out. Security-related events (SRE) should be exchanged in a standardized format. If log messages are adjusted by patches, upgrades or other changes, this should be communicated (e.g. in the changelog). Re: c) The supplier should test and confirm compatibility of the host-based sensors to be used with his systems.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.2 Project Management

This chapter defines the requirements for the project's management and procedures, especially where related to project-based activities tied to the planning, realisation and commissioning of systems and components. The chapter covers basic requirements for naming contacts and minimum operative measures that should be carried out as part of the projects' implementation. Definition of a project management method is not covered by this document.

4.2.1 Contacts

Security requirements	ISO/IEC 27002:2022 5.2, 5.8, 5.20, 5.22 The contractor shall define a contact who is responsible for IT/OT security during the tender process and the system development phase as well as throughout the planned operations and maintenance timeframe. In case of absence, a stand-in should be assigned.

Additional information and notes:		Depending on company size, these tasks should be divided across the different areas and project phases and assigned to several different employees. At the project level, however, a single person should be designated to serve as the client's primary contact.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.2.2 Security and Acceptance Testing

Security requirements	ISO/IEC 27002:2022 5.22, 8.29, 8.30 Prior to acceptance or handover, the individual system components and essential functions of the entire system must be subjected to a comprehensive security and stress test. These internal security tests must be demonstrably carried out by the contractor using a representative configuration. In addition to the internal security tests, an organizational unit independent of the development team must carry out security acceptance tests for the security acceptance of the entire system. The results and the associated documentation (software versions, test configuration, etc.) of the internal tests and the security acceptance tests must be made available to the client. For both types of tests, the effective and complete implementation of the planned security measures must be checked and any existing vulnerabilities or those not adequately considered in the current design must be identified. In addition, the client shall have the right to undertake these security acceptance tests himself or to have them carried out by an external service provider. The type and scope of the acceptance tests shall be defined by the client. For these tests, the client resp. the assigned service provider shall be given system access with a maximum of technologically possible access rights. For both types of tests, before they are carried out, a procedure for rectifying any deviations identified (including a schedule) must be agreed between the client and the contractor. Likewise key points of the tests to be carried out and fulfilment criteria must also be agreed on.

Additional information and notes:	The delivery documentation should contain the documentation of the security tests in sufficient detail for an assessment. Scope and depth of testing should range from simple spot checks to a complete audit, depending on the complexity and criticality of the system. Appropriate security checks should also be repeated regularly during the operating period. For standard components, a type test per product release is usually sufficient. It should be verified, however, that the basic parameterisation (e. g. active network services and protocols) are as similar to the client's actual operating environment as possible. To this end, the settings at commissioning should be checked against a type test log. The security and requirement testing on both client and contractor side should also involve load and stress tests. As part of the security and acceptance tests, the tested system's integrity against unwanted changes should be reviewed. If necessary, a reinstall should be scheduled after testing.

		Quantity and grading of security acceptance tests ("Pre-FAT", "FAT", "SAT", "SAT Level II") should be based on the project-wide approach for acceptance tests. Objective of the acceptance tests is security approval by the client, they are therefore not to be regarded as quality assurance measures with a subsequent improvement process - this must be ensured by the contractor through the internal security tests carried out in advance.
	Operations management / control systems and system operation:	Control systems and central operations management systems are often custom developments and should usually and explicitly undergo a full audit as part of the acceptance process.
	Transmission technology / voice communications:	Security testing should cover both network elements and terminal devices as well as central servers, management and monitoring systems. Most of the time, network elements and terminal devices only require one-off security checks as part of a type test.
	Secondary, automation and telecontrol technologies:	Normally, a one-off test as part of the type test for secondary, automation and telecontrol components should be sufficient. This might need to be repeated after significant changes. When dealing with small control systems, e. g. in substations, it should be checked whether individual adjustments require acceptance testing or whether a type test would be sufficient.

4.2.3 Secure Data Storage and Transmission

Security requirements	ISO/IEC 27002:2022 5.14, 6.6, 7.10, 8.1, 8.24, 8.33 ISO/IEC 27019:2017 6.2.1 Confidential client data that is required or processed during the development and maintenance process shall be encrypted during transmission via insecure connections. When saved on mobile storage media or systems, such data shall only be stored encrypted. The amount and duration of data storage shall be limited to a contractually specified minimum. All client information and data generated or made available to the contractor as part of his work should be treated as confidential resp. internal to the project until and unless they have been reclassified by the client. The contract must specify that the client / operator needs to be notified immediately of any loss of data or data media resp. of any misuse or unauthorised access.

Additional information and notes:		Only information that is obviously not confidential may be excluded. In case of doubt, the contractor should ask the client for a classification. This applies to, for example, internal information and documents by the client, but also to log files, error analyses and relevant system documentation. An agreement between the client / operator and the contractor should clarify which data are to be considered confidential resp. internal to the project as well as the “necessary minimum” of data storage and type of data retention and transmission.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.2.4 Delivery of Project-Specific Modifications

Security requirements	ISO/IEC 27002:2022 8.30 For custom projects and project- resp. client-specific expansions, adjustments and engineering services, all project-specific parameterisations, changes and adaptations shall be comprehensively documented and supplied to the client in full.

Additional information and notes:		Where applicable, it is advisable to agree for the source code and related documentation to be deposited with a trustee. This safeguards and enables security-critical updates, e. g. in case of the contractor’s bankruptcy. If the contractor refuses to put the source code in escrow, both parties should sign a service contract stating that a separate reference system with the entire source code is kept at the contractor’s location. The respective provisions should be included in the delivery resp. service and maintenance contracts.
	Operations management / control	-

	systems and system operation:	
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	

4.3 Base system

This chapter describes requirements to be implemented at the firmware, operating system and middleware system level, such as e. g. database and server services.

4.3.1 System hardening

Security requirements	ISO/IEC 27002:2022 8.9, 8.18, 8.19, 8.21, 8.27, 8.32 ISO/IEC 27019:2017 14.2.10 ENR All standard components (operating system, firmware and, where applicable, used database systems and server services) must be permanently hardened according to recognised best practice guidelines and the latest service packs and security patches shall be installed. Unnecessary users, default users, software, network protocols and services shall be uninstalled or – where an uninstall isn't possible – permanently deactivated and protected from accidental reactivation. The entire system's secure basic configuration shall be reviewed and documented. If the contractor only delivers some of the entire system's components, he must state and describe how the other partial components can be hardened according to recognised best practice guides – without impairing the function of the entire system or system components delivered by the contractor. Where specific standard measures cannot be implemented due to technical reasons, this must be explicitly explained to the client, e. g. as part of the functional specification phase. Where the application user does not require access to the operating system, such access must be actively prevented. Where operating system access is required, standard users should only receive restricted user rights. In particular, any unauthorised manipulation of the operating system, the application software and application data as well as the application configuration and projection data need to be prevented effectively. The basic configuration and hardening measures must be reviewed and listed in the security documentation (e. g. installed software and applications, active resp. deactivated ports and services, file shares, system configuration settings etc.).

Additional information and notes:		Applicable hardening measures include, a.o.: • Uninstallation or deactivation of unnecessary software components and functions • Deactivation of insecure resp. unnecessary system and communication services (e.g. parameterization and engineering access) • Activation of local firewall functions • Deactivation resp. deletion of unnecessary standard users • Change of all default passwords • Deletion of temporary and installation files • Activation of security-enhancing configuration options • Restriction of user and software rights to the necessary minimum • Deactivation of communication and media interfaces that are not required (CD/DVD, USB, Bluetooth, WLAN, etc.) • Deactivation of unused switch ports • Activation of application whitelisting A collection of best practice hardening guides for various operating systems, server services and standard applications can be found, for example, at the *Center for Internet Security* (http://www.cisecurity.org) or obtained from the respective system or software manufacturers. Where standard hardening measures cannot be applied, alternative measures should be identified and implemented. When implementing access control measures for the operating system, particular attention should be paid to any way this could be circumvented via auxiliary applications like web and help browsers, file viewers or similar. If possible, the secure basic configuration should be verifiable by automated means. System hardening measures should be reviewed according to a risk assessment during regular security tests and, where necessary, adapted in consultation with the contractor. As a rule, such a review should be carried out by auditors independent from the contractor.
	Operations management / control systems and system operation:	In general, security tests should be repeated every year for relevant operational management-related systems.
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.3.2 Malware Protection

Security requirements	ISO/IEC 27002:2022 8.7 ISO/IEC 27019:2017 12.2.1 All networked systems must be equipped with malware protection (e.g. signature-based or allowlisting-solutions) at the appropriate location. As an alternative to malware protection provided on all system components, the contractor can submit a comprehensive malware protection concept that provides equal protection. Where the use of a signature-based solution is intended, these signature files must be updateable in a timely and automated manner. Such updates must not take place via direct connection to update servers on external networks like the internet. For terminal systems, the time of updates must be configurable. All systems and storage media delivered by the contractor should be checked for malware infection before delivery resp. approval and handover. Provided there are no technical reasons to the contrary, the contractor must ensure the use of malware protection solutions preferred by the client.

Additional information and notes:	Technical and organisational protection measures – within the system and at the interfaces – designed to ensure lasting, effective protection against malware infection while – at the same time – offering high system availability should be provided. Interface protection also includes, in particular, the logical and technical interfaces for data exchange with external networks like business IT; remote access interfaces, remote maintenance and process connections; and all stationary and mobile HMIs, parameterisation notebooks and programming devices. In principle, and where corresponding protection software is available on the market, all systems should come with the option to install and operate malware protection. All other systems – in particular, components using industrial embedded systems – require protected interfaces that minimise the danger of malware infection and malware-induced disruptions or equivalent alternative measures. Often, it makes sense to use malware protection products that are already used by the company. Elevated protection requirements, however, might necessitate the use of other or additional products. Malware protection should not only monitor media access, but also the main memory (RAM). Where pattern-based protection software is used, the planned concept for pattern updates should be reviewed accordingly. Where testing and

		approval is required, the required time limits and cycles need to be defined in a way that ensures a lasting, effective protection level. Use of dedicated central and process network-internal update servers should be the goal. The use of allowlisting solutions should be considered and reviewed. In this case, the resulting protection level needs to be sufficiently high with the intended allowlisting technology and configuration. The contractor should specify the protection programs approved for use and, where applicable, the necessary configuration options, e.g. the exclusion of certain directories, use of specific scan types or configuration of allowlisting applications. On commissioning the basic system, the contractor should explicitly test the protection software's compatibility with the entire system. All systems and storage media delivered by the contractor should be checked for malware infection before delivery resp. approval and handover. For this purpose, offline scans of computer systems via an operating system booted from an external medium are preferable. The emergency concept should also cover scenarios where errors in the malware protection software's detection or configuration may cause a system failure.
	Operations management / control systems and system operation:	
	Transmission technology / voice communications:	Currently, use of malware protection software on network components like switches, routers or network elements is rarely feasible. At the same time, plans should include the installation of protection software on (in particular) management and monitoring systems as well as configuration and maintenance devices.
	Secondary, automation and telecontrol technologies:	In the substation and automation environment, this requirement applies in particular to substation operating stations, small control systems, close controls, field displays, maintenance devices etc. On automation components the use of malware protection software is currently not possible, at least in most cases. Since the update processes within the usually distributed substation environment tend to be challenging, it is highly recommended to integrate such malware protection into a centralised solution, where possible.

4.3.3 Autonomous User Authentication

Security requirements	ISO/IEC 27002:2022 5.16, 5.18, 8.5 ISO/IEC 27019:2017 9.2.1, 9.4.2

	Data required for user identification and authentication must not be obtained exclusively from outside the process network.

Additional information and notes:		This requirement applies to all types of user identification and authentication, e. g. at the operating system and application level. Integration of the base system components into a central directory service is advisable. This should be realised via process network-internal directory servers. To this end, a custom directory service could be built, but integration into an existing directory service is also an option. New projects should enable integration of system-specific directory services into the client's existing directory service structure. It should be ensured that the selected structure does not lower the process network's overall protection level and does not create any dependencies on services outside the process network. Where a central user management is employed, provisions should be made for local emergency passwords that can be used in case of a disruption of the user directory service. Where system use requires logging into an operating system, an account with low access privileges should be used for the purpose. System accounts should never be used for regular, non-administrative application access.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	In principle, and especially for HMIs at the substation level and in automation environments, it should be possible to have multi-user mode at the system and application level. Where necessary, integration into central directory services should also be an option. Here, and in particular where distributed systems like e. g. substations are concerned, the availability issues of central directory services require sufficient attention.

4.3.4 Virtualization Technologies

Security requirements	ISO/IEC 27002:2022 8.6, 8.8, 8.13, 8.14, 8.22 ISO/IEC 27019:2017 12.6.1, 13.1.3, 17.2.1 The following requirements govern the use of virtualisation technologies: a) It must not be possible to bypass the network segmentation of segregated security zones via virtualized components or the virtualization environment. b) Networks used for management and administration services as well as data storage of the virtualisation infrastructure must be segregated from other networks by firewalls with only the minimum of required network services enabled in a restrictive manner. Access to the management and administration services and the above-mentioned networks must be restricted to administrators only. c) The virtualisation layer, the management and administration interfaces as well as the associated infrastructure shall be configured, secured and hardened identically and according to manufacturer recommendations. They shall also be included in the patch management and backup concept. d) The virtualization servers must have sufficient resources for operating all of the virtualised components they are running. This is especially important for high-load operating situations. e) Any outage of virtualisation servers or of other components of the virtualisation infrastructure shall have no negative impact on the defined availability requirements. Disruptions and outages of the virtualisation environment shall also be covered and considered in the emergency concept and restoration plans (see 4.8.2).

Additional information and notes:	The testing system should include the key components and functions of the virtualisation infrastructure to ensure that the behaviour of the virtual components in the testing environment does not deviate from the productive environment. The advantages offered by virtualisation should certainly be exploited, especially for back-ups, patch management and emergency and recovery planning, e. g. by freezing and storing operating states of virtual components (so-called snap shots). Re: a) Virtualized components that are assigned to different security or trust zones (e.g. internal components and DMZ components) should not be operated on the same virtualization servers. Virtualized components used in OT and business IT should be run on separate virtualization servers.

		Development resp. testing and productive environments should also be operated on different virtualisation servers. Re: c) In particular, the avoidance or restriction of the use of guest tools of the virtualization solution should also be taken into account, as these can introduce vulnerabilities if not configured properly. Re: d) Efforts should be made to avoid any overbooking of resources like main memory or mass storage. At no time should resource overbooking be able to have a negative impact on the productive system's availability, functional capacity and performance.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	

4.3.5 Container Virtualization

Security requirements	ISO/IEC 27002:2022 8.6, 8.8, 8.13, 8.14, 8.22 ISO/IEC 27019:2017 12.6.1, 13.1.3, 17.2.1 The following requirements must be taken into account when using container virtualization technologies: a) Separate workloads must be isolated from each other, e.g. through network policies and namespaces b) Containers that are assigned to different security or trust zones (e.g. internal components and DMZ components) must not be operated on the same host systems. It must not be possible to bypass the network segmentation of separate security zones via the container or host systems. c) Communication between the container instances and with external systems and access to resources must be limited to the operationally necessary minimum by means of correspondingly restrictive network and access guidelines d) Networks used for management and administration services such as orchestration or deployment as well as networks used

	for data storage of the container infrastructure must be segmented from other networks by firewalls, on which only the minimum required network services are restrictively enabled. Access to management and administration services and the above-mentioned networks must be restricted in accordance with a tiered role model. e) Container images, runtime, management and administration interfaces and associated infrastructure must be configured, secured and hardened uniformly in accordance with the manufacturer's recommendations and covered in the patch management and data backup concept. f) Containers must not be operated in privileged mode. g) Container images may only be obtained from trustworthy sources (base images or registries). h) Container images must be protected against unauthorized changes by cryptographic signatures; the signature must be checked before deployment or the creation of derived images. i) Container images must be checked for known vulnerabilities, such as missing security patches or misconfigurations, as part of the build process and before deployment using automated tools. Any existing vulnerability must be assessed for relevance / exploitability by the supplier. The results of the assessment / build process must be made available to the operator. j) Host systems must have sufficient resources for the operation of all container components running on them. This applies in particular to operating situations under increased load. k) Failure of host systems or other components of the container infrastructure must not have a negative impact on the defined availability requirements. Disruptions and failures of the container runtime environment must also be taken into account in the emergency concept and restart planning (see 4.8.2 Emergency Concept and Recovery).

Additional information and notes:	Following standards can be used for detailed requirements and recommendations: • "SYS.1.6 Containerization", in: "IT-Grundschutz-Kompendium - Werkzeug für Informationssicherheit. Edition 2023". Federal Office for Information Security. • NIST SP 800-190: "Application Container Security Guide". • Security standard SS-011: Containerisation. Department for Work & Pensions. United Kingdom.
Operations management / control systems and system operation:	-

	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.3.6 Industrial IoT

Security requirements	ISO/IEC 27002:2022 5.17, 7.9, 8.5, 8.9, 8.20, 8.32 ISO/IEC 27019:2017 9.4.2 The following requirements must be taken into account when integrating industrial IoT and OT technologies: a) Connection of IIoT components to the OT environment must be implemented via secure gateway components with proxy function. b) Communications of IIoT components must be carried implemented using cryptographically secured protocols (see 4.1.6 Cryptographic Mechanisms). c) IIoT components must be hardened (see 4.3.1 System hardening) d) IIoT components must have secure update mechanisms and must be integrated into vulnerability and patch management (see 4.1.2 Patching and Patch Management) e) Confidential or security-critical data (such as authentication information / credentials) on the IIoT components must be protected against unauthorized access or stored in encrypted form. f) IIoT components must be integrated into a device management system that can be used to control component management, updates, monitoring, etc. g) Publicly accessible IIoT components must be protected against physical manipulation.

Additional information and notes:		See also Industrial Internet of Things, Volume G4: Security Framework (ed. Industrial Internet Consortium)
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-

	Secondary, automation and telecontrol technologies:	-

4.3.7 Role Concepts Base system

Security requirements	ISO/IEC 27002:2022 5.3, 5.16, 5.18, 8.2, 8.3 ISO/IEC 27019:2017 9.2.1 All standard components (operating system, firmware and, where applicable, used database systems and server services) must allow granular access control to data and resources. To this end, it must support a user concept that covers at least the following user roles: • Administrator: User who installs, maintains and manages the system. The administrator is therefore authorized to change the security and system configuration, among other things. • Operator: User who operates the system within the scope of its intended use. This also includes the right to change operational settings. Default access rights must correspond to a secure system configuration. Only the administrator role shall be able to read and change security-related system settings and configuration values. Normal system use shall only require operator or read-only user rights. It must be possible to deactivate user accounts individually without having to remove them from the system. The specification of rights assigned to a role must be done by the client.

Additional information and notes:		When feasible resp. technically possible, read-only users should be created. These are users who can call up the status of the system and read defined operating data, but are not authorized to make changes. User roles facilitate the consistent and easy allocation of access rights to individual users. Role concepts also help to prevent unintended operating errors.
	Operations management / control systems and system operation:	
	Transmission technology / voice communications:	

	Secondary, automation and telecontrol technologies:	

4.4 Network and Communications

This chapter describes security requirements for network technology, network architecture and communication protocols and technologies.

4.4.1 Protocols and Technologies

Security requirements	ISO/IEC 27002:2022 8.3, 8.5, 8.20, 8.21, 8.22, 8.24 ISO/IEC 27019:2017 10.1.2, 13.1.1, 13.1.3, 13.1.4 ENR a) In general, only secure communication standards and protocols that include integrity protection, authentication and, if applicable, encryption shall be used if and where the technology allows. This is a non-negotiable requirement for any protocols used for remote administration and parameterisation and shall also be taken into account where non-standard resp. proprietary protocols are used. b) It must be possible to integrate the entire system and any associated network components into the overall company's network concept. Central administration for relevant network configuration parameters like IP addresses shall be possible. For administration and monitoring secure protocols that ensure integrity protection, authentication and encryption shall be used. Network components shall be hardened, unnecessary services and protocols deactivated and management interfaces protected via ACLs. c) Network components provided by the contractor must be able to be integrated into a central inventory and patch management. d) Where technically possible, WAN connections shall use the IP protocol and unencrypted application protocols shall be secured by encryption on the lower network layers (e. g. via TLS encryption or encrypted VPN technology). e) Where network infrastructure components are shared (e. g. by the use of VLAN or MPLS technologies), the network with the highest protection requirement level shall indicate the respective hardware and parameterisation requirements. The shared use of network components shall only be shared in case of different protection requirements when this shared use can in no way decrease the protection level or availability. f) In particular, data coupling with other control systems and with automation / telecontrol components must be carried out using standardized protocols via controlling elements such as firewalls (see 4.4.2).

Additional information and notes:	If and where the employed network protocol offers security-enhancing options, these should be activated. Generally, protocols using UDP as a transport protocol should be avoided. This is especially true for any use beyond the limits of defined security zones. Exceptions currently apply to the following standard protocols: • PTP (Precision Time Protocol) • NTP / SNTP (Network Time Protocol / Simple Network Time Protocol) • SNMP (Simple Network Management Protocol, version 3 or higher) • RADIUS (Remote Authentication Dial In User Service) • Syslog As a matter of principle, the use of protocols with dynamic port allocation (e. g. RPC/DCOM) beyond firewalls should be avoided. If this cannot be prevented, a firewall should be used that can handle dynamic port allocation and only opens these when required (related connection). Of the OPC protocol family (often used for system coupling), only the OPC-UA protocol version, which was developed under consideration of security aspects, should be used. In this case, the following settings should be activated: • The securityMode 'Sign' (messages are signed) or 'SignAndEncrypt' (messages are signed and encrypted) should be selected. Among others, this enforces authentication at the application level. The securityMode 'SignAndEncrypt' should be used where – beyond integrity concerns – confidential data requires protection. The securityMode 'None' offers no protection whatsoever. • When selecting a cryptographic method, the SecurityPolicy 'Basic256SHA256' should be selected. • User authentication: Authentication with the account 'anonymous' should be disabled. In line with the given technical capabilities, standardised IEC protocols should be used across the board. The private range of these communication protocols should only be used where necessary for technological reasons. Without additional measures, the standard protocols IEC 60870-5-101/104 and IEC 61850 offer no secure integrity protection, authentication or encryption. In such cases, the available extensions according to IEC 62351 should be used. Potential limitations, e.g. in terms of performance and error diagnostics as well as the necessary key management infrastructure and processes should be considered. For communication across zone boundaries, protocol breaks should be provided, e.g. through application layer gateways or by converting to a different protocol, to reduce potential vulnerabilities and weak points. Re: a) For remote administration, the latest versions of the following protocols should be used with activated security settings, where possible: SSH

		(Secure Shell), SCP (Secure Copy), SFTP (SSH File Transfer Protocol), HTTPS (Hypertext Transfer Protocol Secure) resp. RDP (Remote Desktop Protocol). Switching operations and write access to data and variables should only be possible after a successful authentication and authorization check. Any parameterisation and engineering access should occur via secured protocols and should also require successful authentication and authorisation. Re: b and c) Strict separation of the technical, commercial and VoIP networks as well as the creation of a central network management system for the process networks are recommended.
	Operations management / control systems and system operation:	Communications within the control system are usually proprietary. Equivalent security mechanisms are recommended.
	Transmission technology / voice communications:	Voice-over-IP communications, in particular, deserve security measures that safeguard confidential communications and guarantee secure authentication of the communication partners and components involved.
	Secondary, automation and telecontrol technologies:	Communications between individual automation components often take place via industry standards or proprietary manufacturer protocols (e. g. Industrial Ethernet, Profinet, Profibus, etc.). Standard protocols should be used to integrate these into the substation level or the control system. Re: d) In case of physically exposed or insufficiently protected components, VPN termination should be possible directly on the control units. Re: e) Where a shared network infrastructure is used in automation networks for process communications and for other network communications (such as e. g. parameterisation and administration communications), special attention should be paid to the impact of network disruptions or overload on the timing in process communications (example: IEC 61850, GOOSE/R-GOOSE and Sampled Values (SV / R-SV), VLAN usage in station automation).

4.4.2 Secure Network Structure

Security requirements	ISO/IEC 27002:2022 8.3, 8.20, 8.21, 8.22 ISO/IEC 27019:2017 12.9.1 ENR, 13.1.1, 13.1.3, 13.1.4 ENR, 13.1.5 ENR a) Vertical network segmentation: Where applicable and technologically feasible, the system's underlying network structure shall be divided into zones with different functions and protection requirements. Where the technology allows it, these network zones shall be separated by firewalls, filtering routers or gateways. Communications with other networks shall only occur via the communication protocols approved by the client and in compliance with the applicable security guidelines. b) Horizontal network segmentation: Where applicable and technically feasible, the system's underlying network structure shall also be subdivided horizontally, into independent zones (e. g. according to sites) that are also separated by firewalls, filtering routers or gateways. c) The entire system and its individual components must be embedded in the client's zone structure. d) Network perimeters must be planned in such a way that they can be integrated into the operator's attack / anomaly detection (see 4.1.13 Integration into Systems for Detection of Anomalies and Attacks).

Additional information and notes:	As a rule, implementation of these requirements is project-specific. OT networks should be segmented from business IT networks by a firewall with a restrictive rule set. A DMZ should be planned for data interfaces to third-party systems or internal networks and systems with elevated exposure to external security threats (e. g. an office LAN with internet access, distributed sites with reduced physical access protection etc.). As a rule, DMZ components should never have access to internal system components in zones of a higher security level. Any communications connection should always be initiated by the higher security level towards the lower. Interactive remote access from a DMZ via secured protocols is excepted from this stipulation (cf. 4.4.1). With the exception of WAN / long distance routes, technical networks should only be located within the inner security area of the physical object perimeter. Where technical systems are connected beyond these security areas, VPN use should be considered. Safety-related communications in the sense of functional resp. equipment safety should only take place within closed network segments built on dedicated hardware components. As a rule, configuration options of parameters governing the functional resp. equipment safety via network access should be avoided. If and where these are absolutely required, they should only be accessible via the above-stated closed network segments.

		The client should check whether network and security components like firewalls or VPN concentrators are part of the contractor's scope of delivery or should be provided in-house. Re: a) Physical separation of functional tiers is preferable to logical separation. Where such physical separation isn't feasible, the residual risk needs to be assessed. For network separation, the use of gateways that perform a protocol conversion and prohibit direct IP traffic should be considered. For more detailed requirements for network segmentation, the requirements of the IEC 62443 series of standards can be used, in particular: • IEC 62443-3-3: Industrial communication networks - Network and system security - Part 3-3 (2013-08): System security requirements and security levels; Section 9.3 "SR 5.1 - Network segmentation" • IEC 62443-4-2 (2019-02): Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components; Section 9.3 "CR 5.1 - Network segmentation" Appendix A "Network zone diagrams" contains examples to illustrate possible network zone concepts.
	Operations management / control systems and system operation:	The creation of a DMZ structure and installation of firewall functionalities is strongly recommended, especially at network transitions from system-internal networks (e. g. control system LAN) to other internal networks and WAN networks (e. g. for process coupling).
	Transmission technology / voice communications:	Where possible, in-house infrastructure should be used. Where externally operated communications infrastructure is employed instead, compliance with specified security standards should be written into the contract and, if necessary, verified. The option of securing communications in the third-party network via an in-house VPN should be reviewed.
	Secondary, automation and telecontrol technologies:	At the interface between local networks (e. g. substation or facility LAN) and other networks (e. g. control centre or neighbouring substation / facility), gateways with firewall functions at the network and application layer (telegram / profile filtering) should be installed. A physical or logical separation between the networks for productive data (process data) and management data should be planned (monitoring, logging, engineering, administration, etc.). In general, the separation of different functions is recommended. Control centre applications should implement separate network components for the terminal and system networks. Direct integration of protection devices into the general automation network should be avoided where direct communication with other automation components is not required for functional reasons. Where applicable, VLAN-based segmentation should be considered.

		Direct connection of different facilities, systems and applications via a shared facility network should be avoided. Instead, cross-system access to components of the facility network via hardened gateway components is recommended.

4.4.3 Documentation of Network Structure and Configuration

Security requirements	ISO/IEC 27002:2022 5.9 ISO/IEC 27019:2017 8.1.1 The following shall be documented: network design and configuration; all physical, virtual and logical network connections and the employed protocols, IP addresses and ports; and any network perimeters that are part of the system or interact with it. Any changes, e. g. via updates, shall be included in the documentation as part of the overall change management. This documentation shall also cover information on normal and maximum expected data transmission rates, to allow for limiting data transmission rates on the network components to prioritize traffic and prevent DoS issues, where necessary. If the corresponding network architecture / configuration is part of the project or delivery, following network layers must be documented: • Network access / bit transmission layer / data link layer (cabling, layer 2 / VLAN configuration) • Switching / transport layer (IP and routing configuration) • Application layer (protocols used and their configuration)

Additional information and notes:	The documentation should include both a graphical representation and a comprehensible description of the network. Besides cable routing diagrams, the network documentation should also describe the logical segmentation into security zones as well as related information flows. The documentation should be port-specific; cables should be labelled with a cable-unique number and for both ends of the cable with unique “end-point-numbers”. Within the documentation, information should be separated in the illustration layer to ensure that documents with different information contents (e. g. network structure without IP addresses) can be provided. The maximum permitted network load should be indicated, i.e. the level below which the entire system and the individual components are expected to function reliably.

		The latest version of the documentation should be available at any time (especially when the affected network is not available), e. g. for the on-call team.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	To support correct implementation of this security requirement, communications between the components in the substation and with the field devices also require documentation. In the substation environment, “perimeter“ denotes the “external interface“ between the individual substations and other networks (control centre, remote diagnostics etc.).

4.4.4 Secure Remote Access

Security requirements	ISO/IEC 27002:2022 5.15, 6.7, 8.3, 8.5 ISO/IEC 27019:2017 6.2.2, 9.1.2 a) It shall be possible to administrate, maintain and configure all components via an out-of-band network, e. g. via local access, a serial port, a network or direct control of the input devices (KVM). b) Any remote access shall take place via centrally administrated access servers that are under control of the system operator. These access servers shall be operated within a DMZ and ensure isolation of the process network. Here, two factor authentication is mandatory. c) Strictly no direct dial in access to terminal devices. d) Any remote access shall be logged centrally; recurring failed attempts shall be reported. e) All remote access options must be documented.

Additional information and notes:	Direct links to external networks or systems should be avoided, especially where systems with heightened security requirements are concerned. As a rule, remote maintenance should not be able to bypass network segmentation and the existing security mechanisms. For remote access, access servers controlled by the operator should always be used. This ensures that all internal security guidelines and

		requirements are fulfilled at any time and in a verifiable manner. All tools required for maintenance should be operable within resp. together with the access server environment and support multi-user operations. Access servers should be hardened, equipped with malware protection and always kept up-to-date with the latest software versions. Furthermore, it should be possible to log and monitor the remote maintenance activities. Additional access points (manual connection resp. separation or timed separation) into the respective technical network or network segment that can be activated separately are recommended. If possible, a distinct, logically separated remote access and server should be supplied for each network zone and each service provider. All remote access should be subject to at least the same security requirements as local maintenance access. The operator should log all relevant connection data, e. g. the time of establishment/disconnection of the connection resp. the maintenance session, the network addresses of the dial-in and target systems, user IDs etc. Where applicable, logging should also cover relevant actions in the direction of transmission and reception. Standardised and, depending on the application environment, centralised remote access infrastructures and processes are recommended for all service providers. Where remote access affects components that are already in use by other users, the respective legal framework, e. g. the Data Protection Act or the Works Constitution Act, needs to be referenced and taken into account. Usually, this means clearly signalling the user that remote access is in process. Re: e) Remote access options (e.g. modems) integrated into components must be documented, even if they are deactivated.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.4.5 Wireless Technologies

Security requirements	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.24 ISO/IEC 27019:2017 13.1.1, 13.1.3 Short-range wireless technologies (e. g. Wi-Fi, Bluetooth, ZigBee, RFID etc.) shall only be used after assessment of the related risks, under consideration of the following minimum-security measures and after consultation with and approval by the client: • Wireless transmission technology must be secured according to the state of the art. • Wi-Fi technology must only be operated in dedicated network segments that are separated by firewalls and application proxies. • Wi-Fi networks must be configured in a way that ensures that existing Wi-Fi networks are not affected, disrupted or impaired.

Additional information and notes:	As a rule, wireless technologies should only be employed where absolutely necessary and after explicit approval by the client. In general, potential access to other communication networks through wireless technologies should be prevented by reliable measures. Special attention should be paid to the use of wireless peripheral devices and input devices like keyboards, computer mice and monitoring installations like cameras. As a rule, safety-related communications via wireless communication technologies should be avoided and only carried out after an explicit risk analysis. In some cases, this might require special assemblies and specific protection against external radio interference. For further advice on the secure use of Wi-Fi, Bluetooth and RFID, please refer to the NIST documents “NIST Special Publication 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)“, “NIST Special Publication 800-121 - Guide to Bluetooth Security“ and “NIST Special Publication 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems”.
Operations management / control systems and system operation:	-
Transmission technology / voice communications:	In the voice communications environment, special attention should be paid to the protection of wireless / cordless telephones.

	Secondary, automation and telecontrol technologies:	-

4.4.6 Network Authentication

Security requirements	ISO/IEC 27002:2022 5.17, 8.5, 8.20, 8.24 ISO/IEC 27019:2017 9.3.1, 10.1.2 Networked system components must be authenticated on the network side. If no IEEE 802.1X-based network authentication is implemented, MAC-based authentication must be implemented. If no network authentication measures can be implemented for technical reasons, network interfaces must be deactivated or may only be accessible for authorized personnel. When using network authentication, potential failure and emergency scenarios must be taken into account, during which network authentication is not available or digital certificates have been declared invalid (see also 4.8.2 "Emergency Concept and Recovery " and 4.1.7 "Public Key Infrastructure ").

Additional information and notes:		IEEE 802.1X-based network authentication should be aimed for. Depending on availability requirements of system components, both IEEE 802.1X and MAC-based authentication procedures can be used in the entire system, whereas both procedures should not be used simultaneously for one component. When using IEEE 802.1X, use of authentication protocol EAP-TLS is preferred, as an alternative MacAuthenticationBypass should be used for supplicants that are not IEEE 802.1x-capable.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.5 Application

This chapter focuses on security requirements on the application level.

4.5.1 Role Concepts

Security requirements	ISO/IEC 27002:2022 5.3, 5.16, 5.18, 8.2, 8.3 ISO/IEC 27019:2017 9.2.1 The entire system shall support granular access control to data and resources. To this end, it must support a user concept that covers at least the following user roles: • Administrator: User who installs, maintains and manages the system. Among others, this gives the administrator the right to change security and system configurations. • Operator: User who operates the system according to the intended usage scenario, including the right to change operationally relevant settings. • Read-only user: User permitted to access the system status and pre-defined operating data without the right to make any changes. The standard access rights must reflect a secure system configuration. Only the administrator role must be able to read and change security-related system settings and configuration values. Regular system use must only require user or read-only user rights. It must be possible to deactivate user accounts individually without having to remove them from the system. Access rights must not only work on the operating and user interface, but also require consistent integration across the entire application and, where applicable, into the operating system and data base level.

Additional information and notes:	User roles facilitate the consistent and easy allocation of access rights to individual users. Role concepts also help to prevent unintended operating errors. The client should assign rights to specific roles or at least approve the rights allocation. In some cases, it might be helpful to use the role concept to enforce additional oversight via a dual control principle, e. g.: • Role "Change of parameterizations" • Role "Approval of parameterization changes" The system should not only specify user-associated rights, but also system-associated rights resp. roles to assign specific rights or limitations to the different work stations (maintenance, back office, system administration etc.) irrespective of user. Such system-related rights and roles

		must always supersede user-associated rights and roles. Where necessary, an option to restrict roles and / or allocated rights to specific timeframes should also be included. The IEC 62351-8 and 62351-90-1 standards describe role-based access control for control systems of the energy sector and may be consulted for role concept implementation. The roles defined in the system should be aligned to the organizational structure and adaptable in case of change.
	Operations management / control systems and system operation:	Examples of user roles in operational management and control system environments include: • Administrator • Parameterization / data preparation • Operating / switching authorization • Observation / monitoring • Data testing / quality assurance
	Transmission technology / voice communications:	This is of special relevance to management systems. Examples of applicable user roles in the transmission technology environment include: • Administrator • Configuration • Observation / monitoring
	Secondary, automation and telecontrol technologies:	The substation environment requires tailored and graduated roles, especially for substation HMIs. Examples of applicable user roles in the substation environment include (the terms in brackets indicate mapping examples corresponding to the roles defined in IEC 62351-8): • Administrator (INSTALLER / SECADM) • Operating / switching authorization (OPERATOR) • Observation / monitoring (VIEWER) • Parameterization (ENGINEER) • Changing operating parameters • Diagnostics (without parameterization and switching option) • Data testing / quality assurance

4.5.2 User Authentication and Login

Security requirements	ISO/IEC 27002:2022 5.16, 5.17, 5.18, 8.5, 8.15 ISO/IEC 27019:2017 9.2.1, 9.3.1, 9.4.2, 12.4.1 The application shall use personal users to identify and authenticate each individual user; group accounts require special permission by the client and shall only be used in narrowly defined exceptional cases.

	a) Without successful user authentication, the system must only allow precisely defined actions. b) The system must support a state-of-the-art password policy. c) Where technically possible, strong two factor authentication shall be employed, e. g. via tokens or smart cards. d) Data required for user identification and authentication must not be obtained exclusively from outside the process network (see also 4.3.3). e) Any successful or failed login attempts must be centrally logged. It must also be possible to centrally alarm in case of unsuccessful login attempts.

Additional information and notes:	All passwords and other authentication information need to be cryptographically secured for transmission and storage on the system (see also 4.1.5 and 4.4.1). The operator should ensure that a password policy is defined and implemented accordingly. All default user accounts of all applications and systems should be deactivated straight after system handover, see also 4.3.1. Where applicable, the following should be realised, with special emphasis on the requirements for secure operations and availability: • The system should implement mechanisms that enable the secure and traceable handover of user sessions during operations. • Where possible and appropriate, user sessions should be closed after a pre-defined period of inactivity. • Once a pre-configurable number of failed login attempts has been exceeded, the system should trigger a warning and, if necessary or relevant, suspend the related account. Re: a) The operator and the contractor should jointly specify which actions are permitted on the system without successful user authentication. Re: b) As part of the application configuration, the application administrator should have maximum configuration flexibility regarding the required password complexity (in line with the company's own password policy). Parameters to be defined include, among others: • Minimum password length • Minimum number of specific characters / character types, e.g. upper and lower case letters, numbers, special characters, etc. • Period of validity

		• Prevention of previous password use when the password is changed Maximum number of password changes per time unit (e.g. per day) Re: c) Remote workstations, especially, should use two factor authentication. Re: d) A cryptographically secured connection to a central, process network-internal directory service should be considered.
	Operations management / control systems and system operation:	To safeguard continuous system monitoring by the operating personnel and safe operations management, the required systems (e. g. HMI/control system operating station) should include an option for the secure and transparent handover of user sessions during operations, e. g. at a shift change. Respective logging requirements should also be considered.
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	Re: a) Some of the currently prevalent technology requires a local login via group accounts. In the medium term, efforts should be made to eliminate the use of group accounts. Re: d) Usually not required for local access in the substation environment. Re: e) Due to availability issues, use of central directory services might not be feasible with state-of-the-art technology on HMI systems, either, especially in the distributed substation environment. Here, efforts should be made to facilitate future integration in directory services.

4.5.3 Authorization of Actions at User and System Levels

Security requirements	ISO/IEC 27002:2022 8.3, 8.18 Certain security-related or safety-critical actions shall require prior authorisation of the requesting user resp. the requesting system component. Such actions might also include a read-out of process data points or configuration parameters.

Additional information and notes:	The security-related or safety-critical actions need to be specified by the client/system operator. The respective actions then require central logging, including the stated user ID.
Operations management / control systems and system operation:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	-

4.5.4 Web Applications and Web Services

Security requirements	ISO/IEC 27002:2022 8.27 For web applications, web interfaces and web services, the recommendations of the OWASP TOP 10 and OWASP Application Security Verification Standard projects as well as the BSI Guideline on the Development of Secure Web Applications shall be applied. Any deviations from these guidelines require justification and prior approval by the client. Where the employed system components feature browser interfaces (e. g. for parameterisation), they also require secure implementation. Otherwise, these interfaces must be deactivated. Of all the OWASP Application Security Verification Standard (ASVS) project requirements, at least Level L2 (standard) for process control environments in energy supply must be implemented.

Additional information and notes:	As a rule, the introduction of web applications should only be permitted in accordance with and after explicit approval by the client / operator. Level L3 (Advanced) of the ASVS should be implemented in the area of critical infrastructures.
Operations management / control systems and system operation:	-

	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.5.5 Integrity testing

Security requirements	ISO/IEC 27002:2022 8.27 ISO/IEC 27019:2017 14.2.5 The integrity of data that is processed in security-relevant activities shall be verified prior to processing (e. g. checked for plausibility, correct syntax and value range).

Additional information and notes:		The consistency of the processed data should be ensured at all times. A consistent input data set should always lead to a consistent output data set. It is especially important to prevent any inconsistent interim states. Data from external systems or data entered via user interfaces should always be checked for consistency and validity (e.g. type, length, scope, syntax, value range, plausibility, age). This is especially important where faulty or manipulated data could jeopardise secure system operations (e. g. during a parameterisation import). Such checks should also be carried out within the application resp. within the system, for example at the interface between application components or software modules. Examples: • Verification of the possible settings range of an operating resource • Verification of a parameterisation's "last modified" date to warn before a potentially more up-to-date version is overwritten
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-

	Secondary, automation and telecontrol technologies:	-

4.5.6 Logging

Security requirements	ISO/IEC 27002:2022 5.33, 8.15, 8.17 ISO/IEC 27019:2017 12.4.1, 12.4.4 a) The entire system must have a uniform system time as well as an option for synchronising this system time with an external secure time source. b) The system must log user actions as well as security-relevant actions, incidents and errors in a format suitable for subsequent and central evaluation. For a configurable minimum time period, these logs shall record date and time, the users and systems involved as well as the actual event and result. c) The log files are stored centrally at a freely configurable location. A mechanism for the automated transfer of log files to central components must be available. d) The log file must be protected from subsequent modification. e) Older entries shall be overwritten on the log file overflow. The system shall send an alert before the log storage runs out of space. f) It must be possible to include security-relevant messages in a pre-existing alarm management.

Additional information and notes:	Operative, regulatory or legal requirements might include a logging obligation. To ensure effective log file administration, the related criteria should be specified in a logging operating concept. The client should define targets for the minimum period resp. the minimum number of stored log messages for local and central storage. Configuration and modification of event logging should be as straightforward as possible. Security-relevant events should be marked as such in the system logs and linked to corresponding standard use cases of the system in the documentation in order to facilitate automatic evaluation. Examples include: commands rejected due to time discrepancies / command age, login attempts with an incorrect password. The criticality of an event should be classified on a system-specific basis.

		Re: a) For system time, either local time, CET or UTC should be chosen. Where systems are directly or indirectly linked to external partners, the respective time standard should be selected in consultation with these partners. For the use of the NTP protocol cryptographic authentication according to RFC 2030 / RFC 1305 should be employed. Loss of the time signal's availability resp. the external time synchronisation should have no or only carefully defined repercussions on control technology functions. Where necessary, a redundant time source should be included. Re: e) This requirement does not apply directly if and where a ring buffer mechanism is used. In this case, the minimum size of this ring buffer should be specified and storage on a central log server (see c)) arranged.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	Re: a) For substation applications, UTC should be used internally, while in-and output should be represented in the configurable local time. Re: b) Logging could, for example, take place in the operating log. Re: c) Logging related to protection and automation components usually happens on the level of the superordinate systems. In the distributed substation environments, storage within the substation and synchronisation resp. transmission to a central site is advisable. Re: d) see c)

4.6 Development

This chapter describes requirements pertaining to hardware and software development. Where standard components like e. g. operating systems or database systems are used, this chapter applies to the integration of these standard components into the entire system and / or the respective component.

4.6.1 Secure Development Standards, Quality Management and Approval Processes

Security requirements	ISO/IEC 27002:2022 5.20, 5.21, 8.32, 8.27, 8.31, 8.30, 8.29, 8.33, 8.28 ISO/IEC 27019:2017 9.4.5 a) The system shall be developed by the contractor by reliable and professionally trained employees. Where the development or parts thereof are subcontracted to a third party, this requires written permission by the client. The subcontractor shall meet at least the same security requirements as the contractor. b) The contractor must develop the system in accordance with recognized development standards and quality management / assurance processes. As part of the development process, the following security-relevant development steps require special attention: • Definition of the security requirements • Threat modeling and risk analysis • Deduction of requirements for system design and implementation • Secure programming • Requirement tests • Security checks before commissioning The processes and activities applied must be documented in a comprehensible manner. The documentation can be viewed by the client as needed. c) Testing shall be subject to the dual control principle: Development and testing shall be carried out by different people. Testing plans and procedures as well as expected and actual test results must be documented and comprehensible. It must be ensured that they can be reviewed by the client as needed. d) The contractor must have a documented development security process in place that covers physical, organisational and personal security and protects the system's integrity and confidentiality. The effectiveness of the above-stated process may be verified by an external audit. e) The contractor must have a programming guideline in place that explicitly covers security-related requirements, e.g. avoiding insecure programming techniques and functions or the verification of input data to avoid buffer overflow errors. Where possible, security-enhancing compiler options and libraries shall be used.

	f) The approval of the system resp. of updates/security patches must follow a specified and documented approval process.

Additions and comments:	Secure software development is not necessarily contingent on any particular development model, yet might require – where applicable – adaptation of the necessary security-related development steps and activities and their integration into the existing development methodology. For example, the *IEC 62443-4-1:2018* standard can be used as a basis for life cycle requirements for secure product development. Re: a) Assigning project-specific development tasks to sub-contractors, in particular, requires written approval by the client/operator since specifics of the client's/operator's installations may not be subjected to unprotected dissemination. Re: b) As far as possible, development and testing should take place on dedicated testing and development systems not connected to the productive system. Re: d) Routine checks of the source code using automated testing tools should be carried out. If possible, this verification process should be integrated automatically into the development process.
Operations management / control systems and system operation:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	-

4.6.2 Secure Development and Test Systems, Integrity Testing

Security requirements	ISO/IEC 27002:2022 8.30, 8.31, 8.33 ISO/IEC 27019:2017 9.4.5, 12.1.4 a) Development must take place on secure systems; the development environment, source code and binary files must be protected against unauthorized access. All development systems must be hardened according to recognised state-of-the-art and best practice specifications. Up-to-date malware protection must be employed on the systems and all the latest security patches must be installed. b) Development and testing of the system, updates, extensions and security patches shall take place in a testing environment that is separated from the productive system. c) No source code (except for interpreted scripting languages) must be stored on productive systems. d) It must be possible to check the integrity of source code and binary files for unauthorized changes, for example via secure checksums. e) A version history that tracks any changes to the software must be kept for all employed software.

Additional information and notes:	The development systems and environments as well as the test systems should feature state-of-the-art security measures and always be kept separate from the general company network. Access to insecure networks, e.g. for Internet or mail use, should not be possible on the above-stated systems. Where such access might be necessary for development purposes, the systems accessing such insecure networks should be comprehensively isolated from the development environment, e. g. via use of virtualisation or proxy solutions. It should be ensured that any potential risk from internet or e-mail connections is kept to an absolute minimum. The development systems and environments as well as the test systems should be equipped with secure logical access protection as well as measures to prevent unauthorised physical access. Re: c) Provision for sufficient protection against unauthorised changes should be employed, e.g. code signing. As a rule, a test system should be included (e.g. a test system of redundant components). For the purpose of error correction, it might prove necessary to simulate the respective system conditions to verify that the error has indeed been eliminated. In some cases, the test system might not be able to reproduce these conditions or error analysis might only make sense on the productive system. This, however, usually only involves debugging – a full development cycle on the productive system, including application

		compiling, could cause extensive disruptions. It also markedly complicates the correct version and change control. Any debugging and testing on the productive system should always be preceded by an individual risk assessment and formal approval by the operator.
	Operations management / control systems and system operation:	Re: b) Before commissioning, development may take place on what will later be the productive systems. After commissioning, this should no longer be an option. Re: c) A temporary source code installation could facilitate debugging. After successful bug fixing, the source code should be removed again to prevent potential manipulation of the control system application. A further option involves use of a network-based debugger. However, the respective service should only be activated temporarily and protected from unauthorised access.
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	Re: b) As a rule, all system development, testing etc. takes place at the contractor's location. Where applicable, a client-related testing environment could be kept ready there. Before commissioning, development may take place on what will later be the productive systems. After commissioning, this should no longer be an option.

4.7 Maintenance

This chapter describes security requirements pertaining to maintenance processes. For the purpose of this document, “maintenance” denotes all service measures to be commissioned by the client/operator including, but not limited to, maintenance activities, incident analyses, troubleshooting and debugging, improvements, adaptations etc.[1].

4.7.1 Maintenance process requirements

Security requirements	ISO/IEC 27002:2022 5.15, 5.16, 5.18, 5.19, 5.20 ISO/IEC 27019:2017 9.1.2, 9.2.1, 15.1.2 a) Any remote and on-site access shall only be carried out by a predefined and properly trained group of people and only originating from secured systems. Access systems and IT infrastructures used for remote and on-site access need to be hardened according to recognised state-of-the-art standards and best practice specifications. Up-to-date malware protection shall be employed and all the latest security patches shall be installed. b) A pre-defined maintenance process shall be established to ensure that maintenance personnel only receive access to the systems, services and data as well as the respective physical premises that are actually required to carry out the related maintenance activities. c) Interactive remote access shall occur via personalised accounts and using two factor authentication. Special user IDs shall be established for automated processes – these shall only be able to execute specific functions and not have interactive access d) Technical measures shall ensure that remote access is only possible if and where the responsible operator has explicitly approved this access. Each remote access session by external service providers shall require individual approval and disconnection. Sessions shall automatically disconnect after a reasonable amount of time. Access systems used for remote access, in particular, shall be logically or physically isolated from other networks during remote access. Here, a physical separation is preferable to logical uncoupling. e) To protect the systems for remote and on-site maintenance, the following aspects are of particular importance: • The maintenance systems must be equipped with secure logical access protection and also be secured against unauthorized physical access. • The maintenance systems must be hardened according to state-of-the-art standards and recognised best practice specifications. • Remote maintenance access must only take place from a secured DMZ environment protected against unauthorised access.

[1] Note: The definition of maintenance and servicing used in this white paper differs from the definition used in DIN 31051.

	• Mobile systems for on-site maintenance must be secured with a restrictively configured firewall software. • During maintenance access, the maintenance systems should have up-to-date malware protection as well as the latest security patches in place.

Additional information and notes:	These requirements should already be factored into the project design and maintenance agreements in collaboration between client and contractor resp. service provider. Data privacy and confidentiality agreements should also be covered and agreed in writing. Among others, this requirement aims to prevent any unauthorised and undetected third-party remote access. As a rule, operational management, e. g. at the control room, should be notified of any maintenance work, for example by connecting or disconnecting the remote maintenance access. This also applies to maintenance access by in-house staff. Especially for access by external service providers, this could be achieved by filing the authentication token with the control room. On-site maintenance by service technicians poses a serious security risk. Where possible, contractors should not be allowed to connect their own hardware to the process network (e. g. maintenance notebooks, but also storage media like USB sticks). Instead, they should use hardware provided by the client for this purpose. Where use of the contractor's own hardware cannot be avoided, this should require explicit approval by the client. The contractor should be obliged to provide proof that he has implemented an adequate internal security guideline for this service. This security guideline should cover at least the following aspects: • Access control and protection • Secure authentication on the device • Secure storage of customer data • Data medium encryption • Specification of data transmission (encryption / integrity protection) • Data back-up and recovery • Patch management • Malware protection • Secure measures to erase customer data For activities associated with Critical Infrastructures, maintenance personnel also need to meet the applicable legal requirements, e. g. via a security check. Where the supplier's resp. service provider's maintenance personnel require maintenance access to Critical Systems, these maintenance employees should be named individually. Maintenance process requirements should be specified in a contract. A respective, where applicable mutual, security arrangement should be

		established by the client and demonstrably be brought to the attention of the service technicians. See also 4.4.4
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.7.2 Secure Update Processes

Security requirements	ISO/IEC 27002:2022 8.19, 8.29, 8.30, 8.32 ISO/IEC 27019:2017 12.5.1 The provision and installation of updates, extensions and patches must occur according to a defined process and in coordination with the client. The contractor must verify the correct functionality and compatibility of updates and patches and approve them.

Additional information and notes:	Energy supply systems are of great economic, sociological and societal significance. To ensure their secure and reliable operations, fast reaction times as well as a defined and controlled maintenance process tend to be essential. Updates and patches should be tested on a separate test system prior to installation. A multi-step approach is recommended, especially for custom software and developments: 1. The contractor bases his test on the underlying standard product. 2. Testing and approval by the contractor are carried out in a testing environment that mirrors the operator's system as closely as possible. 3. If necessary, the operator – or the contractor on behalf of the operator – tests updates and patches on their own system according to a pre-defined testing schedule.

		Under certain circumstances, a multi-step commissioning process should be considered that supports ongoing operations in case of error (cf. 4.1.2). Depending on the affected systems 'criticality, and as part of the overall maintenance process, the operator should review whether certain changes should always be made on-site and not via remote access.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.7.3 Configuration and Change Management, Rollback

Security requirements	ISO/IEC 27002:2022 8.9, 8.19, 8.29, 8.32 ISO/IEC 27019:2017 12.1.2, 12.5.1, 12.9.1 ENR a) The system must be developed and operated with a configuration and change management in place. b) The system must support rollback to a pre-defined number of configuration states.
Additional information and notes:	Where non-trivial configuration or parameterization changes are to be expected during system operations, the system should support a satisfactory configuration and change management. In particular, it should be possible to roll back to a pre-defined number of previous configuration states. The requirements apply to both the contractor and the client / operator. The necessary processes for a suitable configuration and change management should be defined and realised by the operator. The system should support logging of changes to configuration states. Re: b) Backup of at least one prior dataset (parameterisation and firmware state, data model etc.) as well as a rollback option should be included in the design. All changes should be documented.

	Operations management / control systems and system operation:	Provisions should also be made for a rollback option for dynamic and static data at the application level. For software and system changes, all changes and extensions require project-specific administration.
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	Due to the limited non-volatile memory of current device technology, rollback options on the protection and automation component level are often not feasible (yet). However, it should be possible to back up parameterisation and firmware states via the devices' operating and maintenance software.

4.7.4 Vulnerability Management and Patch Information Service

Security requirements	ISO/IEC 27002:2022 5.20, 8.8 ISO/IEC 27019:2017 12.6.1 The Contractor must implement a documented process for the management of vulnerabilities and security patches, which ensures the systematic handling of vulnerabilities and security patches, for all individual components and the entire system during the entire contractually regulated operating period. The process must support the following requirements: a) Identification and reporting of vulnerabilities and security patches: The contractor must comprehensibly explain for all individual components how and at what intervals vulnerabilities and security patches are identified and how they are obtained. It must also be possible for all parties involved, as well as external parties, to report actual or potential vulnerabilities. b) Assessment of vulnerabilities and security patches: The criticality and relevance of the vulnerability or security patch in the context of the entire system provided must be assessed. The assessment methodology for vulnerabilities must be agreed with the client and documented in a comprehensible manner. c) Provision of security information: Subject to confidentiality, the Contractor must regularly inform the Client of any vulnerabilities that have become known and newly released security patches and their criticality and relevance. This also applies in the event that no patch is yet available to rectify the problem. It must be taken into account that vulnerabilities or security patches rated as particularly critical must be reported immediately. d) Treatment of vulnerabilities: The contractor must explain in a comprehensible manner how and in what time frame vulnerabilities are handled and security patches are installed.

	e) Management of vulnerabilities: The contractor must keep a register of currently known vulnerabilities that have not yet been conclusively addressed. f) The specific time frame for identification, information and treatment of weaknesses must be contractually regulated.

Additional information and notes:	As a rule, information and reporting on security flaws and vulnerabilities is considered a service by the contractor. Its specific scope should be further defined in a service and maintenance contract, see also 4.7.5. Information on vulnerabilities and security patches (hereinafter referred to as security information) can typically be obtained directly from the manufacturer of the individual components and/or from official sources (e.g. CERT-Bund or CISA). Already known vulnerabilities can be identified by means of vulnerability scans carried out by the supplier. In certain cases, it may make sense to proactively contact the manufacturer when vulnerabilities become known in order to check whether they are affected. The assessment methodology for security information should meet the requirements of the client. The Common Vulnerability Scoring System[2] (CVSS) in the version agreed with the contractor can be used for the assessment of security information. The assessment should take into account the circumstances of the entire system in order to better assess the actual risks. A monthly information service can be agreed for the provision of security information by providing information on vulnerabilities or security patches that have become known, including the assessment and the proposed procedure for handling them. A threshold value (e.g. CVSS score ≥ 7) should be agreed for the prompt (e.g. within one week) provision of particularly critical information. Information about updates to be installed should be made available to the client regularly and promptly. The following aspects should be taken into account for the release processes: • The contractor should obtain all relevant security patches and subject them to the necessary release and qualification tests. • Information about released security patches should be made available to the client promptly after their release, e.g. by e-mail, via a website or a support forum. • If a security patch is not classified as relevant in the given system environment, this should be documented and communicated to the client. • If a security patch is not approved by the contractor or client, alternative measures should be developed.

[2] https://www.first.org/cvss/

		• It should be explicitly documented whether a service interruption is necessary to apply a patch, for example due to restarting services or components. • For each patch, it should be documented which security gaps are addressed and which changes are made. It should be checked whether threat intelligence information should also be included in the regular information service. Vulnerabilities can be dealt with in various ways. In addition to accepting vulnerabilities rated as non-critical until the next planned patch cycle or handling them by means of configuration changes (workarounds, mitigations), vulnerabilities are usually remedied by installing patches as part of patch management (see 4.1.2 and 4.1.3). Vulnerability management is used to monitor existing vulnerabilities and, in particular, to prevent the accumulation of vulnerabilities that are not considered critical, which can themselves lead to security risks. Integration of the process into the operator's own SOC/CSIRT, if available, should be taken into account.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.7.5 Maintenance Contract / Service Level Agreement

Security requirements	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 5.22 ISO/IEC 27019:2017 15.1.2 To ensure continuous security support, a maintenance contract or service level agreement must be concluded with the system supplier(s).

Additional information and notes:	The agreement should cover the following topics if relevant to the project:
	• Runtime
	  ○ Security support should be guaranteed at the latest when the system is introduced into a productive OT environment
	• Specifications for the support model
	  ○ Assignment of support levels between contractor and client
	  ○ Support times
	  ○ Error classes and associated response times
	  ○ Contact information for contractor and client

	○ Framework conditions for support requests and processing, e.g. for telephone support, remote access or on-site deployment ○ Any necessary support tools and infrastructure, e.g. ticketing tools, components for remote maintenance ○ Requirements for restarting and emergency operation • Contractor's obligation to provide information on known security vulnerabilities or available security patches, including appropriate deadlines, including 3rd party software ○ Immediate information in the event of critical vulnerabilities • Vulnerability and patch management ○ Coverage of all necessary hardware and software components, including 3rd party software where necessary (applications, libraries, software modules, frameworks, packages, etc.) ○ Classification criteria for vulnerabilities according to the client's methodology ○ Proactive vulnerability analysis and component or system-specific documented relevance assessment of vulnerabilities/security patches ○ Testing and information obligations, test methodology and procedure for the approval of security patches including appropriate deadlines, alternative measures in the event of non-approval ○ Procedure for the provision of security patches and/or their installation by the contractor, including appropriate deadlines ○ Documentation/notification obligation and procedure in the event of business interruptions (e.g. due to restarts) ○ Cyclical patch windows and procedure for critical sub-cyclical patches ○ For each patch it should be documented which vulnerabilities are addressed and which changes are made • Obsolescence management ○ Early information obligation of the contractor to discontinue products and hardware and software components ○ Framework conditions for necessary hardware and software upgrades or corresponding upgrade projects • Spare parts stock at the contractor's or client's premises • Secure disposal of assets by the contractor • Regularly required maintenance work by the contractor • If necessary, provision of a test system at the contractor's premises ○ Scope and structure of the test system ○ Necessary maintenance work on the test system • Specifications for the contractor's personnel, e.g. training/competencies, nomination by name, security checks, etc. • Training obligations of the contractor, including on the client's security requirements • Documentation obligations

	• Obligation to report security incidents that are related to the client or may have an impact on the client or the provision of services • Definition of essential key performance indicators • Reporting by the contractor (scope and cycle) • Audit rights of the client, e.g. deadlines, procedure and assumption of costs • Requirements for configuration management • Requirements for secure maintenance processes (see 4.7.1)

	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.8 Data back-up and Emergency Planning

This chapter describes requirements related to data back-up and emergency planning.

4.8.1 Backup: Concept, Procedure, Documentation, Testing

Security requirements	ISO/IEC 27002:2022 5.37, 8.13 ISO/IEC 27019:2017 12.1.1 Documented and tested procedures for data back-up and recovery of the individual components resp. the entire system and the respective configurations must exist. There must be the possibility for central back-up of the configuration parameters of distributed components. After relevant system updates, the documentation and procedures must be updated and re-tested accordingly.

Additional information and notes:	The back-up should comprise all relevant data, including e. g. static data (parameters, application and system configurations) and dynamic data (manual settings and updates etc.). Process data aren't usually saved as part of regular back-ups. In certain circumstances, archive data like long-term archives and the system installations could also be included in the back-up. The precise scope of the backed-up data should be defined by the client. The maximum permissible data loss (recovery point objective, RPO) and the recovery time objective (RTO) should be agreed between the contractor and the client and documented. Maximum back-up and restore times should also be specified. The back-up procedure should be designed to accommodate the back-up and restore of the data volumes expected during the planned system runtime in the defined periods. The back-up / restore procedure should always be able to ensure consistent datasets for the entire system. The back-up process should include mechanisms for verifying the integrity and consistency of a back-up against the current dataset. The back-up procedure should take the protection requirements of the respective data into account, e. g. through use of encryption. The data back-up and restore procedure requires extensive documentation. As part of the acceptance testing, a full back-up and restore should be carried out with realistic data volumes. These tests should be repeated by the operator at regular intervals.
Operations management / control	In particular, a cyclical backup of all manually entered data (operational use authorization, blocking of reports, etc.) should also be provided.

	systems and system operation:	
	Transmission technology / voice communications:	For process-related components and embedded systems, the following applies: For component replacement or major malfunctions procedures for the timely import of volatile data (e. g. parameterisation data) into replacement devices should be described and tested. An import/export option for the parameterisation data is usually sufficient.
	Secondary, automation and telecontrol technologies:	-

4.8.2 Emergency Concept and Recovery Plans

Security requirements	ISO/IEC 27002:2022 5.29, 5.30, 8.14 ISO/IEC 27019:2017 17.2.1 The contractor must provide documented and tested procedures and recovery plans – including expected restoration times – for relevant emergency and crisis scenarios. After relevant system updates, this documentation and these procedures shall be updated and retested as part of the approval process for release changes.

Additional information and notes:	The emergency concept and recovery planning should conform to the client's specifications regarding the maximum permissible data loss (recovery point objective, RPO) and recovery time (recovery time objective, RTO). The operator resp. client should identify and evaluate relevant emergency and crisis scenarios as part of a business emergency and continuity management. To this end, functions and applications should be classified according to their importance for business processes, with particular attention to a secure operations management. For the identified scenarios, emergency concepts and recovery plans should be developed. The system design should also factor in the defined maximum downtime and recovery periods stated in the emergency concept. The contractor should make provisions for the mechanisms required for recovery and emergency operations of the relevant scenarios and make the necessary information available as part of the project and system documentation. A detailed documentation of the emergency procedures should be available. Where services by the contractor are required for recovery and emergency operations, this should be agreed by contract.

		As part of the approval process, both emergency operations and recovery from relevant disruption scenarios should be thoroughly tested. The respective restore times should be established and compared to the maximum acceptable periods defined in the emergency concept. Under certain circumstances, a procedure for restoring the entire system from individual components under consideration of the, in some cases, required restores of backups of parameterisation and operation data filed in the system resp. security documentation, could be sufficient. This must be reviewed by the client. The operator should review and, where necessary, update the recovery planning and emergency concepts at regular intervals.
	Operations management / control systems and system operation:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

Appendix

A Network zone diagrams

Network zone diagram 1

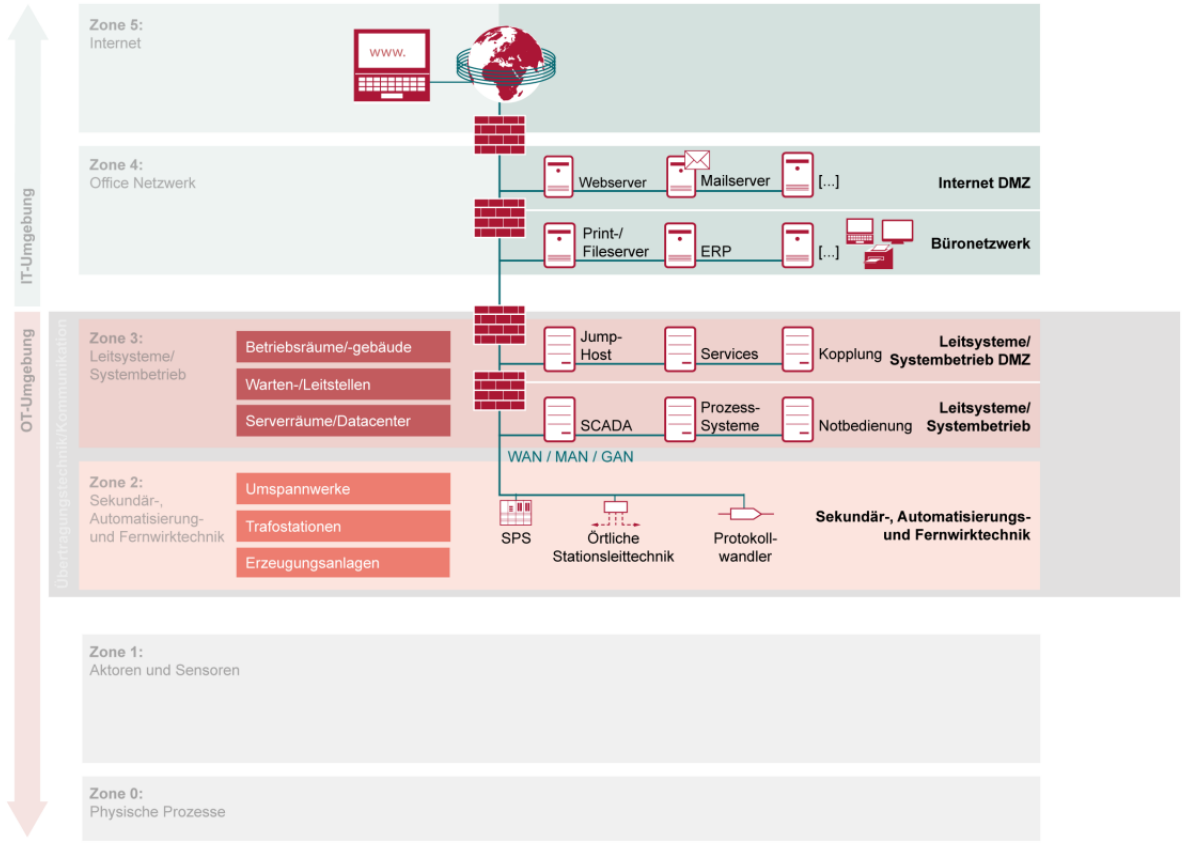

Figure 1: Generic structure plan with zones and technology categories

Network zone diagram 2

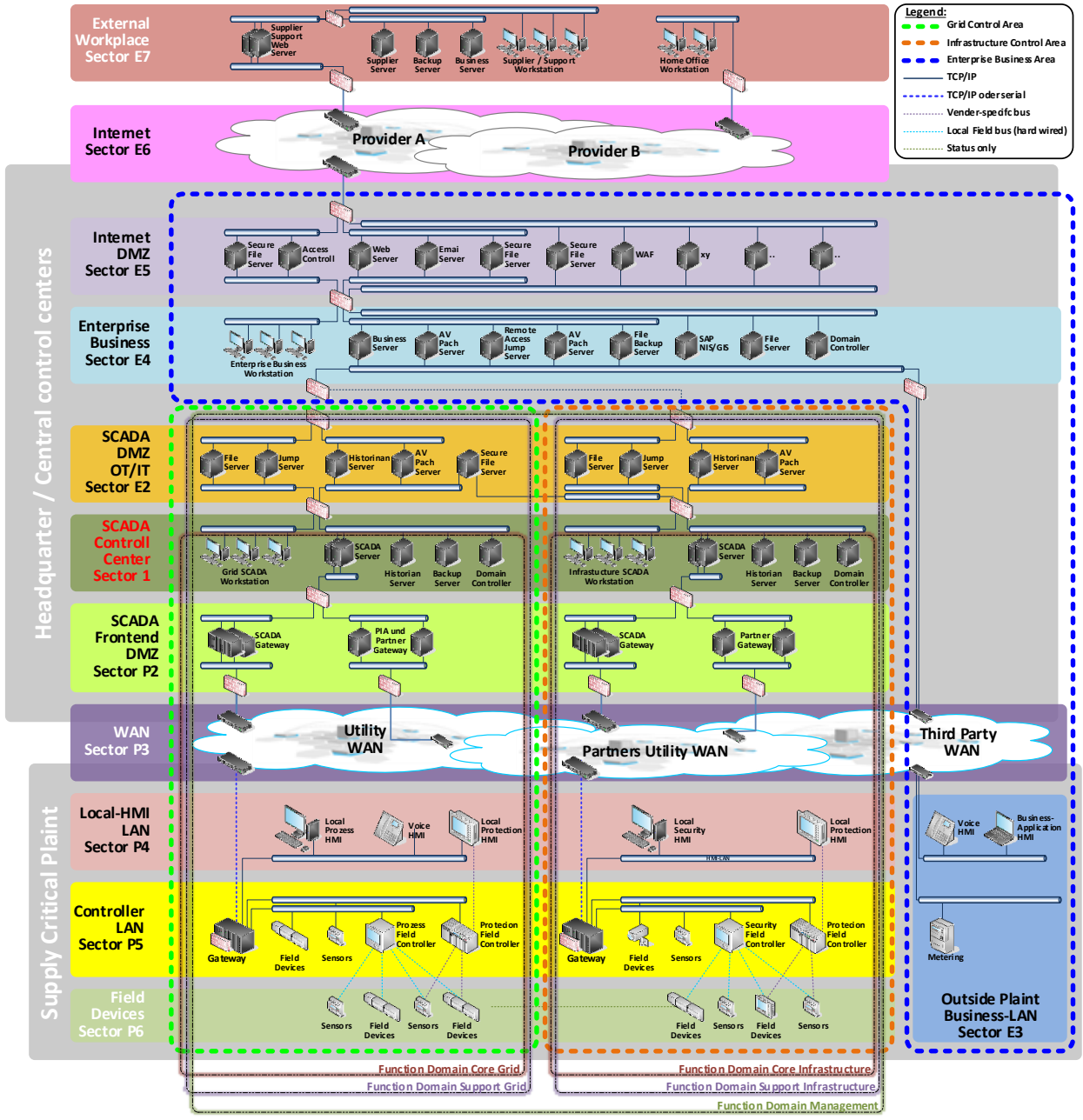

Figure 2: Example of a network architecture

B List of abbreviations and glossary

2-factor authentication	Authentication using two different authentication mechanisms, e.g. password and smart card
3rd party products	Standard software resp. hardware used by the system supplier, e.g. database, compiler, computer, network components etc.
ACL	Access Control List
Application	Application software
Application proxy or application level gateway	Proxy system that monitors and filters data traffic at the application protocol layer
Authentication	Process to verify the identity of a person or system component
Base system	Operating system / firmware and middleware including basic components such as X11 or database systems, network services and related libraries
BIOS	Basic Input/Output System, firmware of an x86 system
BNetzA	Bundesnetzagentur, the German Federal Network Agency
BSI	Bundesamt für Sicherheit in der Informationstechnik, Germany's Federal Office for Information Security
Change management	Management process for controlling and managing the testing, application and documentation of hard- and software updates, configuration modifications and other changes
CET	Central European Time
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and Related Technologies, an internationally recognized IT governance framework
CRL	Certificate Revocation List
CSIRT	Computer Security Incident Response Team
DCOM	Distributed Component Object Model
DHCP	Dynamic Host Configuration Protocol
Directory service	Network service that provides a central collection of certain data, e.g. usernames, authorizations, etc.

DMZ	Demilitarised zone – an isolated network zone located between security zones with different protection levels. Location of security systems that handle communications between the zones
DoS attack	So-called denial of service attack on a system or system component aiming to incapacitate the target, e. g. by using all the available processing power or network capacity
EAP	Extensible Authentication Protocol
ENR	Prefix of the sector-specific requirements in ISO/IEC 27019
EMC	Electromagnetic compatibility
EST	Enrollment over Secure Transport
EVU	Energy supply company
FAT	Factory Acceptance Test
Gateway	Gateways enable connections between components or networks based on different protocols
Entire system	In this document, all hardware and software components supplied by the contractor, e.g. applications, operating systems, firmware, computer systems and the network infrastructure
GOOSE	Generic Object Oriented Substation Events
HMI	Human machine interface
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISO/IEC 27002	ISO/IEC standard for information security
ISO/IEC 27019	Sector-specific ISO/IEC information security standard for energy supply
IT	Information technology
ITIL	IT Infrastructure Library, a collection of best practices or good practices in a series of publications that describe a possible implementation of IT service management and now represent a de facto international standard
KVM	Keyboard Video Mouse

LAN	Local Area Network
Lifecycle	Lifecycle of a system starting with planning and call for tenders through implementation, commissioning and actual operations all the way to dismantling and disposal
MAC	Media access control
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
Network perimeter	Network system that forms the transition to an external network, e.g. a router, a firewall or a remote access system
Network TAP	Network device for tapping (*wiretapping*) data traffic (TAP: Test Access Point)
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OPC	Open Platform Communications, communication interface frequently used in automation technology
OPC-UA	OPC Unified Architecture
OT	Operational Technology The OT definition used in this document is described in Chapter 1 "Introduction and Scope". There are various alternative definitions of the term, such as: • *"Operational technology (OT) encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.*" Source: https://csrc.nist.gov/Projects/operational-technology-security • *"Operational technology (OT) is hardware and software that monitors and controls physical devices, processes and events in the institution."* Source: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/08_IND_Industrielle_IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2021.pdf • *"Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.*" Source: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

- *"The term 'OT' refers to the technology that uses hardware and software to monitor and/or control physical devices, processes and events. OT includes specialized industrial systems such as station control, telecontrol and protection technology. OT also includes network components integrated in the OT environment, automation technology, control technology and technical building equipment, property security technology and, where applicable, safety-relevant components."*
  Source: Own definition

Out-of-band communication	Communication not using the primary communication link intended for user data communication
OWASP	Open Web Application Security Project
Patch management	Management process for controlling and managing the testing, installation, distribution and documentation of security patches
Profibus	Process Field Bus, standard for fieldbus communication in automation technology
Profinet	Industrial Ethernet standard, e.g. for real-time communications
Proxy	Computer system that conveys – and, if necessary, also monitors and filters – the data traffic between two separate data networks
PKI	Public Key Infrastructure
R-GOOSE	Routed GOOSE, see GOOSE
R-SV	Routed SV, see SV
RDP	Remote Desktop Protocol
RFC	Request for Comments
RFID	Radio-frequency identification
Rollback	The full and comprehensive reset of an IT system to a defined previous state, e. g. prior to a software update or after a failed change
Role	See user role
RPC	Remote Procedure Call
Safety	Freedom from unacceptable risks
SAT	Site Acceptance Test
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SFTP	SSH File Transfer Protocol
SIEM	Security Information and Event Management
S/MIME	Secure / Multipurpose Internet Mail Extensions

SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOC	Security Operations Center
PLC	Programmable logic controller
SSH	Secure Shell Protocol, encrypted terminal protocol
Stress test	Test designed to verify the behaviour of a soft- or hardware component under high load resp. processing data outside its stated specification
SV	Sampled Values
System	see entire system
TAP	see network TAP
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical report
UDP	User Datagram Protocol
USB	Universal Serial Bus
User role	Group of users allocated certain rights based on their assigned task(s). A user can be assigned several roles.
UTC	Universal Time Coordinated, coordinated world time
ÜT	Transmission technology
VLAN	Virtual Local Area Network, method for setting up different logical networks on a physical network
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
X.509	Standard of the International Telecommunication Union (ITU) for the format of digital certificates

C References and Links

International standards

ISO/IEC 27000 series "Information security, cybersecurity and privacy protection":

ISO/IEC 27001: Information security management systems - Requirements

ISO/IEC 27002: Information security controls

ISO/IEC 27019: Information security controls for the energy utility industry

IEC 62351 series "Power systems management and associated information exchange - Data and communications security":

IEC 62351-3: Communication network and system security - Profiles including TCP/IP

IEC 62351-4: Profiles including MMS and derivatives

IEC 62351-5: Security for IEC 60870-5 and derivatives

IEC 62351-6: Security for IEC 61850

IEC 62351-7: Network and System Management (NSM) data object models

IEC 62351-8: Role-based access control for power system management

IEC 62351-9: Cyber security key management for power system equipment

IEC TR 62351-10: Security architecture guidelines

IEC TR 62351-12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems

IEC TR 62351-90-1: Guidelines for handling role-based access control in power systems

Frameworks and recommendations for action

BSI - Federal Office for Information Security (Germany)

ICS Security Compendium

ICS Security Compendium: Test recommendations and requirements for product suppliers of components

NIST - National Institute of Standards and Technology (USA)

NIST Special Publication 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)

NIST Special Publication 800-121 - Guide to Bluetooth Security

NIST Special Publication 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems