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

Oesterreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

Whitepaper Requirements for Secure Control and Telecommunication Systems

Completely revised version 2.0 05/2018:

Vienna/Berlin, 8th May 2018

www.oesterreichsenergie.at

www.bdew.de

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)

Joint publishers:

Oesterreichs E-Wirtschaft
Brahmsplatz 3, 1040 Vienna, Austria

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

Contact:

Armin Selhofer (Oesterreichs E-Wirtschaft)
Kay Tidten (BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.)

Expert advice and support:

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

Despite careful checking, we cannot assume responsibility for or guarantee the accuracy of all stated contents. Unless they are the result of wilful intent or gross negligence, the publishers assume no liability for the contents of this document.

This translation of the Whitepaper should be considered as courtesy translation. In principle, the German version takes precedence

Contents

1 Introduction and Scope

This document defines fundamental security requirements for control and telecommunication systems used for process control in the energy sector. The document also provides implementation recommendations, listing up-to-date, industry-specific and expert-compiled recommendations for safeguarding information security.

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. Organisational requirements – such as in-company organisational security measures (e. g. the creation of a security organisation), adequate risk management or the establishment of a 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 constitutes a new edition of the BDEW Whitepaper and the associated Implementation Recommendations, fully revised and updated by Oesterreichs Energy and BDEW. Here, both documents have been merged and their contents comprehensively updated and amended to reflect the latest technological developments.

2 Subdivision and Structure of this Document

In this document, control and communication systems used for process control in the energy sector are described as "systems" resp. the "entire system". These systems usually consist of individual components. Such components could also be standalone devices intended for (partial) tasks related to process control and telecommunications in the energy sector.

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 27002:2013 *Code of practice for 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 classification 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 process control in the energy sector. Further down, and where applicable, the document also lists specific implementation guidelines for the three key technology areas of the energy utility process environment:

“operations management / control systems and system operations”, “transmission technology / voice communications” and “secondary, automation and telecontrol technologies”. The following categorisation applies:

Technology category	Description and examples
Operations management / control systems and system operations:	This relates to all centralised systems used for process control and monitoring; process control operations management and associated / required supporting central IT systems; applications and related central infrastructure. Examples: • Central grid control and management systems • Power plant control systems • Central systems used for monitoring and control of distributed generation 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 operations of the above-mentioned systems, e. g. programming and parameterisation devices
Transmission technology / voice communications:	The transmission, telecommunications and network technology deployed in process technology for voice and data communications. Examples: • Routers, switches and firewalls • Transmission technology-related network components • Voice communication devices • Phone installations, VoIP systems and associated servers • Wireless digital systems

	• Central management and monitoring systems of the transmission, telecommunication and network technology
Secondary, automation and telecontrol technologies:	This relates to 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 as well as the automation technology in generation and storage facilities. Examples: • Control and automation components • Control and field devices • Telecontrol devices • Programmable logic controllers, including digital sensor and actor elements • Protection devices • Safety components • Digital measurement and metering installations • Synchronisation devices • Excitation systems

3 Instructions for Use

3.1 System Planning and Call for Tenders

This Whitepaper is for manufacturers, system integrators and external planners as well as in-house planners, implementers and client-side operators.

For suppliers, these requirements and implementation recommendations should already prove helpful during product and system development and should therefore be referenced at an early stage. This is particularly important for the continuous development of systems and components across their entire lifecycle.

Clients are recommended to indicate the 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 should prove especially helpful during this particular phase.

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 be supplemented by a copy of this Whitepaper and a definition of concrete requirements and additional measures as well as implementation guidelines and permissible divergences and exceptions. In their bids, suppliers should include a detailed statement on how they intend to implement these technical and organisational requirements. Where applicable, they should also document necessary deviations and proposed alternatives. These need to be evaluated by the tendering party and taken into account during the selection process. Where suggested measures are rejected or not included, the planners, implementers resp. operators on the client's side should evaluate and document this fact as part of a risk analysis resp. review it as part of the risk management process.

The entire system's security concept should be audited during the concept 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.

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.

To this end, and at the time of tender resp. at the time of the project's realisation, the client and system supplier or respective service providers need to agree procedures governing the relevant details of maintenance processes and security-specific services such as patch management, malware protection or system upgrades and migrations. As a rule, these procedures should be specified in maintenance contracts and binding migration concepts.

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 fast-paced development and application of new IT technologies from commercial and business IT is increasingly moving into the process technology domain. All these novel and promising technologies can lead to cost savings and functional improvements. At the same time, and prior to the introduction of any new technologies, it is important to examine and test related and relevant information security aspects and to subject them to a thorough risk evaluation. A range of topics deserve closer attention and examination:

- Consideration of known security flaws and vulnerabilities
- Assurance of stability and reliability 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, i.e. where it might affect the swift restoration of normal operations after disruptions and outages
- Fulfilment of the requirements for real-time operations
- Compliance with the safety requirements 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 describes general and principal security requirements that are applicable to the entire project and all areas of technology.

4.1.1 Secure System Architecture

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 13.1.3, 14.2.5, 14.2.7, 17.2.1 Individual components and the entire system shall be designed and developed to support secure operations. Secure system design principles include: **Security by design:** The entire system and its individual components are designed on the basis of and with a focus on security. 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 not run under 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 operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.1.2 Patching and Patch Management

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.6.1 All system components shall be patchable. The supplier shall support a patch management process for both the individual components and the entire system, designed to enable the control and management of security patch testing, installation and documentation. The operator himself resp. the assigned service provider shall be able to install the security patches and updates. Patch installations resp. uninstalls shall 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 shall be verifiable using a cryptographic mechanism.

Additional information and notes:	Patching refers to the application of security-related and functional software updates. This involves the correction of faults or errors as well as the expansion, adaptation or optimisation 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.). Any security patch installation and uninstall or rollback procedure should be documented in detail for all system components. Where the supplier does not provide entire systems, he should indicate the necessary processes and requirements to install security patches and other updates on the third-party components used by the system. 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. Where possible, 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.).

		If and when the entire system resp. its components require functional testing after an update, this should be automated, if possible, and corresponding mechanisms designed into the system. The supplier needs to document both the necessary test cases and the expected results of a successful test run (test book). Depending on system criticality, functional testing might require a client-specific test system at the supplier's location and an additional testing system at the client's location. Fall-back 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. The patches require clear labelling and versioning by the supplier. Where patches need specific firmware versions, compliance should be verified and ensured separately. Processes executed as part of this patch management should meet recognised operating and service management standards (like COBIT, ITIL etc.). 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. See also **Fehler! Verweisquelle konnte nicht gefunden werden.**.
	Operations management / control systems and system operations:	Where possible, redundant components to ensure uninterrupted operations should be used.
	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 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 27002:2013 / 27019:2017: 12.5.1, 12.6.1 The supplier shall ensure that security updates are available for all system components throughout the entire contractually stipulated operating timeframe. 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. Usually, security patches and updates need to be reviewed and approved individually by the supplier 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 supplier. Where patches need to be reviewed and approved, the supplier should look for information on existing security updates for all third-party components and software products and then carry out a component- resp. facility-specific relevance assessment. This evaluation, as well as the results of the approval testing, should be documented by the supplier and made available to the client. Information on necessary updates should be made available to the client in a frequent and timely manner. The following aspects deserve consideration: • The supplier should acquire all relevant security patches and subject them to the necessary approval and qualification testing. • The client should receive information on approved security patches soon after their publication, e. g. via e-mail, via a website or via a support forum. • The client should be informed immediately of any critical vulnerabilities. • Where a security patch is considered irrelevant for the given system environment, this should also be documented and communicated to the client. • Where a security patch is not approved by the client or supplier, alternative measures should be developed.

	• It should be explicitly documented whether a particular patch requires interruption of operations, for example due to restarting services or components. • Each patch should be accompanied by documentation to indicate the addressed vulnerabilities and resulting changes. It should be ensured that all available relevant and approved security updates and security-related service packs are installed at cyclical intervals to minimise any deviation from the latest supported release version. 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 migration concept. Binding agreements should be made for procedures like testing, provision and approval of patches and updates as well as timelines and deadlines, e. g. as part of a maintenance contract. If and where possible, this should also already cover foreseeable migration scenarios.
Operations management / control systems and system operations:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	-

4.1.4 Support for Deployed System Components

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.6.1, 14.2.7 The supplier shall ensure that within the planned and contractually stipulated operating timeframe, manufacturer support and security updates are available for system components developed by both the supplier 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.

Additional information and notes:		Operating timeframes that exceed the lifecycle of system or software components increase security risks and should therefore be absolutely avoided. Suppliers should offer corresponding support for both their own and third-party products and, at the time of signing the contract, they should also be able to produce migration concepts 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 timeframe of operations. Due to the expected extended operating timeframes of systems covered by this Whitepaper, suppliers 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. The client should specify the envisaged operating and support timeframes of individual components in advance. As part of the project's documentation, the suppler should record the system and component versions as well as the corresponding support periods. The respective requirements should be defined and recorded in the contract between client and supplier. 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 operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.1.5 Encryption of Sensitive Data

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 12.4.2, 13.1.2, 18.1.3, 18.1.4 Confidential data shall only be stored resp. transmitted encrypted.

Additional information and notes:	The protection of confidential data should take both information security aspects and data protection requirements into account. The supplier should provide a list of the data processed by the system as standard. The client determines which of these data should be considered confidential. Where protection requirements are obvious (e. g. for authentication information like passwords), the supplier should already include respective measures in the standard configuration. 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 operations:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	-

4.1.6 Cryptographic Mechanisms

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 10.1.2, 13.1.4 ENR, 18.1.5 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. The supplier shall not use custom cryptographic algorithms.

Additional information and notes:		The following directives and recommendations are considered state-of-the-art for hashing, signatures and encryption as well as the related key sizes[1]: • "BSI TR-02102 Cryptographic Mechanisms (BSI, Federal Office for Information Security, Germany) • "Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung – Übersicht über geeignete Algorithmen" (BNetzA, Federal Network Agency, Germany).[2] Mechanisms or key sizes that deviate from these recommendations should only be used after explicit approval by the client. 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 and BNetzA should be consulted. Where the technology allows it, the selected cryptographic mechanisms should 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 should involve recognised libraries to avoid implementation errors. It might be advisable to use cryptographic hardware modules like a trusted platform module (TPM) for key management, random number generation etc.
	Operations management / control systems and system operations:	-
	Transmission technology / voice communications:	-
	Secondary,	

[1] Note: The translations of the documents should be considered as courtesy translations. In principle, the German versions take precedence.

[2] The signature law was replaced by the Trust Services Act. At the time of finalising this document, the algorithm catalogue published by the BNetzA and the preliminary version of the next catalogue, however, still referenced the name of the old law.

	automation and telecontrol technologies:	

4.1.7 Secure Standard Configuration

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.4.4, 12.5.1, 14.3.1 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.

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

4.1.8 Integrity Testing

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 14.2.1, 14.2.4 It shall 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. recognise deliberate manipulations, such testing usually requires cryptographically calculated checksums. 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 operations:	-
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 be a goal.

4.1.9 Use of Cloud Services

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 15.1.1, 15.1.2, 15.2.1 Where cloud services are used, the following requirements apply: a) Agreements shall 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, shall not be realised in external cloud services. c) Downtime of a cloud service resp. access to this service shall 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 for the process control of 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 design. 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

		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 27018:2014 *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. 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.
	Operations management / control systems and system operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	

4.1.10 Documentation Requirements

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 7.2.2, 12.1.1, 14.1.1, 14.2.7 At the latest, the client shall receive project-specific documentation at the system's handover. For individual components and entire systems, the documentation shall cover a description of all security-related system settings and parameters as well as their standard values. Furthermore, the documentation shall list and briefly describe security-specific implementation details (like the employed cryptographic mechanisms). The documentation shall 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.

Additional information and notes:		The supplier 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. Normally, such documentation contains a general description valid for all applications and configurations as well as a project-specific part describing the actual implementation, e. g. as an appendix to the required technical specifications. All security-related descriptions should be made available as part of a separate document. 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. 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 should highlight consequences of glaringly insecure configuration settings. Furthermore, all security-specific log and audit messages should be explained, including potential causes and, where applicable, suitable countermeasures. If applicable, the documentation should also contain a description of the prerequisites for secure system operations. These include, among others, requirements related to type of users, the network environment, any interactions and communications with other systems and networks as well as requirements related to physical security and environmental parameters like air conditioning, power supply, EMC protection, fire safety 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.
	Operations management / control systems and system operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and	Generally, security-related parameters and messages require project-specific documentation as part of the system's planning and design.

	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 27002:2013 / 27019:2017: 6.1.1, 6.1.5, 15.1.2 The supplier shall define a contact who is responsible for IT security during the tender process and the system development phase as well as throughout the planned operations and maintenance timeframe.

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. In case of absence, a stand-in should be assigned.
	Operations management / control systems and system operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.2.2 Security and Acceptance Testing

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 14.2.7, 14.2.8, 14.2.9, 15.2.1 Prior to delivery, the entire system's components and key functions shall be subjected to security and stress testing by the contractor – in a representative configuration and by an organisational unit independent of the development team. The actual procedure shall be discussed and agreed in coordination with the client. The results of these tests as well as the associated documentation (software versions, test configuration etc.) shall be made available to the client. In addition, the client shall have the right to undertake these 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.

Additional information and notes:	At the handover resp. acceptance of a system, evidence should be provided that the supplier has carried out comprehensive security testing. The delivery documentation should include documentation of such security testing and be detailed enough for a qualified assessment. Independent of the supplier's security tests, the client should carry out his own security checks as part of the acceptance and functional testing. Depending on system complexity and criticality, the scope and testing depth of these tests should range from simple, random samples all the way to a full audit. Corresponding security checks should also be repeated regularly during system operations phase. Security testing should include a check of the effective and full implementation of the agreed security measures and identify any existing or inadequately met vulnerabilities in the current design. 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 supplier 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.
Operations management / control systems and system operations:	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 27002:2013 / 27019:2017: 6.2.1, 8.3.3, 10.1.1, 13.2.2, 13.2.3, 13.2.4, 14.3.1 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.

Additional information and notes:	All client information and data generated or made available to the supplier 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[3]. Only information that is obviously not confidential may be excluded. In case of doubt, the supplier 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. The contract should 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. An agreement between the client/operator and the supplier 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.

[3] See appendix A, “Data Classification“.

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

4.2.4 Delivery of Project-Specific Modifications

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 14.2.7 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 supplier's bankruptcy. If the supplier 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 client's location. The respective provisions should be included in the delivery resp. service and maintenance contracts.
	Operations management / control systems and system operations:	-
	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 27002:2013 / 27019:2017: 9.4.4, 12.6.2, 13.1.2, 14.2.4, 14.2.10 ENR All components of the base system shall 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.

Additional information and notes:	All standard components (operating system, firmware and, where applicable, used database systems and server services) should be hardened according to recognised specifications. Applicable hardening measures include, a. o.: • Uninstall or deactivation of unnecessary software components and functions • Deactivation of insecure resp. unnecessary system and communication services • Deactivation resp. deletion of unnecessary standard users • Change of all standard 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 communications and media interfaces (CD/DVD, USB, Bluetooth, Wi-Fi etc.) that are not required • Deactivation of unused switch ports • Activation of application whitelisting A collection of best practice hardening guides for different 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 relevant system resp. software manufacturer.

		Where certain standard measures cannot be implemented due to technical reasons, this should 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 should 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 needs to be prevented effectively. During the implementation of access control measures, 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 the supplier only delivers some of the entire system’s components, he should state and describe how the other partial components (e. g. operating system or database system) could be hardened according to recognised best practice guides – without impairing the function of the entire system or system components delivered by the supplier. The basic configuration and hardening measures should 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.). 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 supplier. As a rule, such a review should be carried out by auditors independent from the supplier.
	Operations management / control systems and system operations:	In general, security tests should be repeated every year for relevant operational management-related systems.
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	Of particular importance is the deactivation of any communication services and parameterisation access on process-oriented components like controllers, PLCs and automation components or gateways that are not required for operations. Where applicable, existing standard passwords should be changed to secure values and security-enhancing configuration options should be activated.

4.3.2 Malware Protection

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.2.1 All networked systems shall be equipped with malware protection at the appropriate location. Alternatively to malware protection provided on all system components, the supplier can submit a comprehensive malware protection concept that provides equal protection. Where the use of a pattern-based solution is intended, these pattern files shall be updateable in a timely and automated manner. Such updates shall not take place via direct connection to update servers on external networks like the internet. For terminal systems, the time of updates needs to be configurable.

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 office 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. Where pattern-based protection software is not an option, so-called whitelisting solutions should be considered and reviewed. In this case, the resulting protection level needs to be sufficiently high with the intended whitelisting technology and configuration. The supplier should specify the protection software 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 whitelisting applications. On commissioning the basic system, the supplier should explicitly test the protection software's compatibility with the entire system. All systems and storage media delivered by the supplier 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 operations:	
	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 27002:2013 / 27019:2017: 9.2.1, 9.2.2, 9.4.2 Data required for user identification and authentication shall 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. 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 operations:	-
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 Virtualisation Technologies

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.1.3, 12.3.1, 12.6.1, 13.1.3, 17.2.1 The following requirements govern the use of virtualisation technologies: a) Virtualised components assigned to different security or trust zones (e. g. internal components and DMZ components) shall not be operated on the same virtualisation servers. It shall not be possible to bypass the network segmentation of segregated security zones via virtualisation servers. b) Networks used for management and administration services as well as data storage of the virtualisation infrastructure shall 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 shall 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 virtualisation servers shall 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) Virtualised components used in process control and office IT should be run on separate virtualisation servers.

		Development resp. testing and productive environments should also be operated on different virtualisation servers. 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 operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	

4.4 Network and Communications

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

4.4.1 Used Protocols and Technologies

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 9.4.2, 10.1.1, 10.1.2, 12.9.1 ENR, 13.1.1, 13.1.2, 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 shall 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 supplier shall be capable of integrating into a central inventory and patch management. d) Where the technology allows it, 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.

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) As a matter of principle, the use of protocols with dynamic port allocation (e. g. RPC/DCOM) beyond firewalls should be avoided. 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 as the 'anonymous' account 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 to error diagnostics as well as the necessary key management infrastructure and processes should be considered. 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 successful authentication and authorisation 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 operations:	In particular, data connections to further control systems and automation/telecontrol components should require the use of standardised protocols. 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) To date, most VPN tunnels still terminate on routers in the substation. In future, and where possible, these should terminate 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 and Sampled Values, VLAN use in substation automation).

4.4.2 Secure Network Structure

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 12.9.1 ENR, 13.1.1, 13.1.2, 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.

Additional information and notes:		As a rule, implementation of these requirements is project-specific. Process control networks should be separated from office IT networks via a firewall with restrictive rules. 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 supplier'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.
	Operations management / control systems and system operations:	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. 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 27002:2013 / 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.

Additional information and notes:	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 operations:	-
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 27002:2013 / 27019:2017: 9.1.2, 9.4.1, 9.4.2 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 shall 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, always access servers controlled by the operator should 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.
	Operations management / control systems and system operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.4.5 Wireless Technologies

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 13.1.1, 13.1.2, 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 shall to be secured with state-of-the-art measures. • Wi-Fi technology shall only be operated in dedicated network segments that are separated by firewalls and application proxies. • Wi-Fi networks shall 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 operations:	-
	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:	

4.5 Application

This chapter focuses on security requirements on the application level.

4.5.1 Role Concepts

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 6.1.2, 9.2.1, 9.2.3, 9.2.6, 9.4.1 The entire system shall support granular access control to data and resources. To this end, it shall support 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. • User: 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 shall reflect a secure system configuration. Only the administrator role shall be able to read and change security-related system settings and configuration values. Regular system use shall only require user or read-only user rights. It shall be possible to deactivate user accounts individually without having to remove them from the system.

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 assigns rights to specific roles or at least approves 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 parameterisations“ • role “approval of parameterisation 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.

	Access rights should 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. 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 organisational structure and adaptable in case of change.
Operations management / control systems and system operations:	Examples of user roles in operational management and control system environments include: • Administrator • Parameterisation/engineering • Operating/switching rights • 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 rights (OPERATOR) • Observation/monitoring (VIEWER) • Parameterisation (ENGINEER) • Changing of operating parameters • Diagnosis (without parameterisation or switching rights) • Data testing/quality assurance

4.5.2 User Authentication and Login

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.3.1, 9.4.2, 9.2.1, 9.2.2, 9.4.3, 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 shall only allow a range of narrowly defined actions. b) The system shall support a state-of-the-art password policy. c) Where technologically possible, strong two factor authentication shall be employed, e. g. via tokens or smart cards. d) Data required for user identification and authentication shall not be obtained exclusively from outside the process network (see also 4.3.3). e) Any successful or failed login attempts shall be centrally logged. It shall 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 **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.**). The operator should ensure that a password policy is defined and implemented accordingly. All standard user accounts of all applications and systems should be deactivated straight after system handover. 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 transparent 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 should specify in detail 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 unit of time (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 operations:	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 Authorisation of Actions at the User and System Levels

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.4.1, of.4.4 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 operations:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	Not usually required for protection and substation control technology; potential use should be reviewed by the client/operator.

4.5.4 Web Applications and Web Services

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 14.2.5 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.

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. Where the employed system components feature browser interfaces (e. g. for parameterisation), they also require secure implementation. Otherwise, these interfaces should be deactivated. Of all the OWASP Application Security Verification Standard project requirements, at least Level L2 (standard) for process control environments in the energy sector and at least Level L3 (advanced) for Critical Infrastructures should be implemented.
Operations management / control systems and system operations:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	-

4.5.5 Integrity Testing

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 14.2.5 The integrity of data processed as part of security-related activities shall be verified prior to processing (e. g. checked for plausibility, correct syntax and value range).

Additional information and notes:	The integrity of the processed data needs to be assured 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, volume, 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 operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.5.6 Logging

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3 a) The entire system shall have a uniform system time as well as an option for synchronising this system time with an external secure time source. b) The system shall log user actions as well as security-related actions, events and errors in a format that is suitable for later and central processing. 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) Log files shall be stored centrally at a freely configurable location. A mechanism for the automated transfer of the log file to central components shall be available. d) The log file shall 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 shall be possible to include security-related log 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-related events should be marked as such in the system logs to facilitate automatic analysis. Examples include: commands rejected due to time discrepancies/command age, login attempts with an incorrect password. 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 operations:	-
	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 27002:2013 / 27019:2017: 9.4.5, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, 14.3.1 a) The system shall be developed 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 supplier. b) The supplier shall develop the system in line with recognised development standards and quality management/assurance processes. As part of the development process, the following security-related development steps require special attention: • Definition of the security requirements • Threat modelling and risk analysis • Deduction of requirements for system design and implementation • Secure programming • Requirement testing • Security checks before commissioning 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 shall to be documented and comprehensible. It shall be ensured that they can be reviewed by the client as needed. d) The supplier shall 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 supplier shall 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 needs to follow a specified and documented approval process.

Additional information and notes:		The development process should reflect recognised standards and process models. All processes and activities require comprehensive documentation. 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. 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 operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.6.2 Secure Development and Testing Systems, Integrity Testing

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.4.5, 12.1.4, 14.2.7, 14.3.1 a) Development shall take place on secure systems; the development environment, source code and binary data all shall be protected from external access. All development systems shall be hardened according to recognised state-of-the-art and best practice specifications. Up-to-date malware protection shall be employed on the systems and all the latest security patches shall 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) shall be stored on productive systems. d) It shall be possible to check the integrity of source code and binary data for unauthorised changes, for example via secure checksums. e) A version history that tracks any changes to the software shall be kept for all employed software.

Additional information and notes:	The development systems and environments as well as the testing 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 and e-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 testing 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 testing 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 testing 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 operations:	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 supplier’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.[4].

4.7.1 Maintenance Process Requirements

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 9.1.2, 9.2.1, 9.2.2, 15.1.1, 15.1.2 a) Any remote and on-site access shall only be carried out by a pre-defined 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 receives 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.

Additional information and notes:	These requirements should already be factored into the project design and maintenance agreements in collaboration between client and supplier resp. service provider. Data privacy and confidentiality agreements should also be covered and agreed in writing.

[4] Note: The definition of “maintenance“ in this Whitepaper differs from the definition used in DIN 31051.

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 supplier's own hardware cannot be avoided, this should require explicit approval by the client.

To protect the systems for remote and on-site maintenance, the following aspects are of particular importance:

- The maintenance systems should be equipped with secure logical access protection and also be secured against unauthorised physical access.
- The maintenance systems should be hardened according to state-of-the-art standards and recognised best practice specifications.
- Remote maintenance access should only take place from a secured DMZ environment protected against unauthorised access.
- Mobile systems for on-site maintenance should 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.

The supplier 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 **Fehler! Verweisquelle konnte nicht gefunden werden.**
Operations management / control systems and system operations:	-
Transmission technology / voice communications:	-
Secondary, automation and telecontrol technologies:	-

4.7.2 Secure Update Processes

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 14.2.2, 14.2.3, 14.2.7, 14.2.9 The provision and installation of updates, extensions and patches needs to occur according to a defined process and in coordination with the client.

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. The supplier should always verify and approve any updates and patches. These should also be tested on a separate testing system prior to installation. A multi-step approach is recommended, especially for custom software and developments: 1. The supplier bases his test on the underlying standard product.

		2. Testing and approval by the supplier are carried out in a testing environment that mirrors the operator’s system as closely as possible. 3. If necessary, the operator – or the supplier 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 (see 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 operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

4.7.3 Configuration and Change Management, Rollback

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.1.2, 12.5.1, 12.6.2, 12.9.1 ENR, 14.2.2, 14.2.9, a) The system shall be developed and operated with a configuration and change management in place. b) The system shall support rollback to a pre-defined number of configuration states.

Additional information and notes:	Where non-trivial configuration or parameterisation changes can 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. These requirements apply to both the supplier and the client/operator. The necessary processes for a suitable configuration and change management should be defined and realised by the operator. 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 operations:	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 restricted 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 Handling of Vulnerabilities

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.6.1, 16.1.2, 16.1.3 The supplier shall have a documented vulnerability handling process in place. Within this process, all concerned – including external parties – shall be able to report actual or potential vulnerabilities. In addition, the supplier shall stay up-to-date on current security issues that might affect the system or individual components. The vulnerability handling process defines how and in what timeframe a known or reported vulnerability shall be reviewed, classified, remedied and reported to all affected clients, including respective recommended measures. When the supplier finds out about a vulnerability, he shall inform the client in a timely manner and under consideration of the necessary confidentially restrictions, even when no patch to fix the issue is available yet.

Additional information and notes:		The to-be-agreed vulnerability management processes should specify, among others, how the client is informed in a timely manner about current security issues that could potentially affect his system or system components. Where an industry CERT exists, this should also be factored into the vulnerability management processes. As a rule, information and reporting on security flaws and vulnerabilities is considered a service by the supplier. Its specific scope should be further defined in a service and maintenance contract.
	Operations management / control systems and system operations:	-
	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 Back-up: Concept, Method, Documentation, Testing

Security requirements	ISO/IEC 27002:2013 / 27019:2017: 12.1.1, 12.3.1 Documented and tested procedures for data back-up and recovery of the individual components resp. the entire system and the respective configurations shall exist. There shall be the possibility for central back-up of the configuration parameters of distributed components. After relevant system updates, the documentation and procedures shall be updated and retested 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. 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 systems and system operations:	In particular, a cyclical back-up of all manually entered data ("permit to work", "removed from operation", "control inhibit" etc.) should be included in backup schedule.

	Transmission technology / voice communications:	For process-oriented 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 27002:2013 / 27019:2017: 17.1.1, 17.2.1 The supplier shall 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 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 supplier 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 supplier 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 should 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 operations:	-
	Transmission technology / voice communications:	-
	Secondary, automation and telecontrol technologies:	-

Appendix

A Data Classification

A.1 Classification Example

Within a company, data can be divided into different confidentiality levels. Depending on their respective sensitivity and confidentiality, such data have different protection requirements and security levels. To ensure a consistent, adequate approach across all areas of business, the company should introduce and adopt a classification guideline. Its contents and aims can be summarised as follows:

- clear and consistent criteria for classifying data into defined confidentiality levels
- controlled identification and labelling of classified data
- consistent and satisfactory handling of classified data (e. g. during storage and back-up, electronic or postal transmission, personal conversations or deletion)

The following example illustrates a potential data classification scheme:

Class 1: Public Data

Class 1 data are public data that don't require any special protection. This includes and comprises any and all information already derived from publicly accessible sources or – if the company itself is the subject of this information – actively and lawfully published by the company itself.

Class 2: Internal Data

Class 2 data are internal data. This includes and comprises all data that doesn't obviously fall into either of the other two information classes or lacks obvious classification criteria. In addition, all data by partners and clients should be classified as – at least – internal or higher.

Class 3: Confidential Data

Class 3 data are confidential data. This generally includes and comprises any and all information that could cause lasting damage to the company and customer confidence when disseminated to or accessed by unauthorised third parties. Furthermore, this also includes all data that require confidentiality for legal, contractual or regulatory reasons. Examples of confidential data include:

- general company and trade secrets
- calculations and calculation frameworks relevant to market competition
- contracts or draft contracts
- technical information on Critical Infrastructures or other sensitive systems
- personally identifiable information such as e. g. religious affiliation, union membership, health information
- data handling or processing on behalf of a client that is subject to confidentiality requirements

Where it is deemed necessary by a company, further confidentiality classes can be defined and added. For example, if and where the company in question processes data that has an official security rating of “classified” resp. “classified confidential“ or higher for legal reasons.

The following table provides a sample overview of how to label and handle classified data:

Classification	Activity	Labelling	Handling
Public	filing / storage	- none	- no guidelines
	printing	- none	- no guidelines
	transmission / mailing	- none	- no guidelines
	spoken communications	- none	- no guidelines
	destruction	-	- no guidelines
Internal	filing / storage	- none	- no special guidelines within the company - outside the company, it is down to the respective person’s own judgement to ensure adequate access protection
	printing	- none	- no special guidelines within the company - outside the company, all printing must be supervised
	transmission / mailing	- none	- no special guidelines within the company - for fax transmissions to recipients outside the company, the sender needs to either coordinate the time of transmission and require a receipt or ensure that only authorised recipients have access to the fax machine in question
	spoken communications	- none	- no special guidelines within the company or over the phone - outside the company, efforts should be made to prevent potential eavesdropping by other parties in public space (train, airport etc.)
	destruction	-	- data must be destroyed in the provided data destruction containers

Classification	Activity	Labelling	Handling
Confidential	filing / storage	- mark storage medium as “confidential”	- electronic data must be encrypted within the given technological scope - paper copies must only be stored in separate, lockable units - taking a paper hard copy out of the company requires individual approval
	printing	- mark documents medium as “confidential”	- absolutely no unsupervised printing - use of encrypted network printers that require a PIN for the print job or of local single-user printers unconnected to the network
	transmission / mailing	- mark documents medium as “confidential” - when mailed by post: do not label the outer envelope, but include additional inner envelope marked as “confidential“	- encrypted transmissions only – even within the company - include no confidential contents in unencrypted elements of the transmission (e. g. e-mail header)
	spoken communications	- verbal alert before the actual conversation that the following will cover and contain confidential information	- strictly no confidential conversations in public space - no use of unencrypted phone connections - if necessary, ban of mobile phones and similar devices in meeting rooms
	destruction	-	- use of the provided data destruction containers - use of secure deletion methods for electronically stored information

A.2 Sensitive Data According to the Data Protection Act

Any data that can be used to identify a natural person – directly or by association – are considered personally identifiable data. Such data enjoy special protection to allow the affected person to exercise their right to informational autonomy and decide for themselves who, what, where and when gets to access their personal data.

At the EU level, data protection is governed by the General Data Protection Regulation. Country-specific legislation covers the respective actual implementation requirements. These usually also include detailed guidelines on the collection, storage, processing, transfer and destruction of data as well as the documentation of these procedures.

It should thus be decided whether a separate classification such as “personally identifiable information” (PII) is required to ensure the lawful handling of such data. Furthermore, projects planning to process PII data should consider involving a potential data protection officer or expert according to the EU General Data Protection Regulation from an early stage.

Manufacturers and suppliers are requested to supply the technical and organisational requirements of the existing data protection regulations as operative functions of their products.

B List of Abbreviations and Glossary

Two 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	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 base components such as e. g. X11 or database systems, network services and related libraries
User role	Group of users allocated certain rights based on their assigned task(s). A user can be assigned several roles.
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
COBIT	Control Objectives for Information and Related Technologies, an internationally recognized IT governance framework
DCOM	Distributed Component Object Model
DHCP	Dynamic Host Configuration Protocol
Directory Service	A service that provides a network with a central collection of certain data, e. g. user names, rights etc.
DMZ	Demilitarised zone – an isolated network area 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
EMC	Electromagnetic compatibility
Gateway	Gateways enable connections between components or networks based on different protocols
Entire system	In this document, all hard- and software components delivered by the contractor, e. g. applications, operating systems, firmware, computer systems and network infrastructure
GOOSE	Generic Object Oriented Substation Events
HMI	Human machine interface
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
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 utilities
IT	Information technology
ITIL	IT Infrastructure Library, a collection of best resp. good practices covered in a series of publications on the potential implementation of an IT service management – by now, 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
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
Network perimeter	Network system that marks the transition to an external network, e. g. a router, firewall or remote access system
NTP	Network Time Protocol

Out-of-band communications Communications not using the primary communication link intended for application data communications

OPC Communications interface frequently used in automation technology

Patch management Management process for controlling and managing the testing, installation, distribution and documentation of security patches

Profibus Process Field Bus; field bus communications standard in automation technology

Profinet Industry Ethernet standard, a. o. for real-time communications

Proxy Computer system that conveys – and, if necessary, also monitors and filters – the data traffic between two separate data networks

RDP Remote Desktop Protocol

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 risk which is not tolerable

SCP Secure copy

SFTP SSH File Transfer Protocol

SNMP Simple Network Management Protocol

SNTP Simple Network Time Protocol

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

System See Entire System

TCP Transmission Control Protocol

Telnet Unencrypted network protocol for character-oriented data exchange via a TCP connection; often used for interactive access at the operating system level

TLS Transport Layer Security

UDP User Datagram Protocol

USB	Universal Serial Bus
UTC	Universal Time Coordinated, coordinated global time
VLAN	Virtual Local Area Network, method for using different logic networks on a physical network
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless LAN

C Links and References

C.1 International standards

ISO/IEC 27000 series "Information technology — Security techniques — Information security management systems":

ISO/IEC 27001: "Information technology — Security techniques — Information security management systems – Requirements"

ISO/IEC 27002 "Information technology — Security techniques — Code of practice for information security management"

ISO/IEC 27019 "Information technology — Security techniques — Information security controls for the energy utility industry"

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

IEC/IS 62351-3: Security for profiles including TCP/IP

IEC/TS 62351-4: Security for profiles including MMS and derivatives

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

IEC/TS 62351-6: Security for IEC 61850 profiles

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

IEC/TS 62351-8: Role-Based Access Control

IEC/IS 62351-9: Key Management

IEC/TR 62351-10: Security Architecture

IEC/TR 62351-12: Resilience and Security Recommendations for Power Systems with DER

IEC/TR 62351-90-1: Guidelines for Using Part 8 Roles

C.2 Frameworks and recommended actions

BSI - Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)

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