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

Oesterreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

Whitepaper

Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

White Paper

Requirements for Secure Control and Telecommunication Systems

Überarbeitete Version 1.1 03/2015:

Angepasste Referenzen auf ISO/IEC 27002:2013 und ISO/IEC TR 27019:2013

Änderungshistorie

Version	Datum	Bemerkungen (Bearbeiter)
1.0 Final	17.05.2007	BDEW-Projektteam: beate.becker@bdew.de helge-werner.benke@vattenfall.de Ingo.Jensen@eon-energie.com rolf.kasper@rwe.com juergen.mueller@enbw.com reiner.winter@itecplus.de
1.1	07.10.2014	Anpassung Norm-Referenzen auf ISO/IEC 27002:2013 und ISO/IEC TR 27019:2013 s.beirer@gai-netconsult.de
1.1	25.02.2015	Anpassung Layout und Format arne.rajchowski@bdew.de

Version History

Version	Date	Remarks (editor)
1.0 Final	17.05.2007	BDEW working group: beate.becker@bdew.de helge-werner.benke@vattenfall.de Ingo.Jensen@eon-energie.com rolf.kasper@rwe.com juergen.mueller@enbw.com reiner.winter@itecplus.de
1.1	2014-10-07	Alignment of references to ISO/IEC 27002:2013 and ISO/IEC TR 27019:2013 s.beirer@gai-netconsult.de
1.1	2015-02-25	Alignment of layout and format arne.rajchowski@bdew.de

Vorwort

Anwendungshinweise

Für die Unternehmen der Energiewirtschaft wurde ein Whitepaper mit grundsätzlichen Sicherheitsmaßnahmen für Steuerungs- und Telekommunikationssysteme entwickelt. Ziel ist es dabei, die Systeme gegen Sicherheitsbedrohungen im täglichen Betrieb angemessen zu schützen. Die in diesem Whitepaper festgelegten Sicherheitsmaßnahmen werden für alle neuen Steuerungs- oder Telekommunikationssysteme empfohlen. Strategisches Ziel des Whitepapers ist die positive Beeinflussung der Produktentwicklung für die oben genannten Systeme im Sinne der IT-Sicherheit und die Vermittlung eines gemeinsamen Verständnisses in der Branche für den Schutz dieser Systeme.

Planung eines Steuerungs- oder Kommunikationssystems

In der Planungsphase eines neuen Steuerungs- oder Telekommunikationssystems ist möglichst frühzeitig eine Schutzbedarfsfeststellung durchzuführen. Der Prozess zur Durchführung einer Schutzbedarfsfeststellung ist beispielsweise in dem Grundschutzkatalog des BSI beschrieben. Ergibt sich ein niedriger/mittlerer Schutzbedarf, so ist die Umsetzung der Anforderungen des Whitepapers ausreichend. Anderenfalls (Schutzbedarf „hoch“ oder „sehr hoch“) ist eine ergänzende Risikoanalyse erforderlich.

Diese betrachtet zuerst, ob die im Whitepaper beschriebenen Sicherheitsmaßnahmen den geforderten Schutzbedarf angemessen erfüllen und ergänzt diese ggf. Zusätzlich müssen für Risiken, die nicht im Whitepaper behandelt werden, gesonderte Sicherheitsmaßnahmen formuliert werden. Die nach Umsetzung der Sicherheitsmaßnahmen des Whitepaper und der durch die ergänzende Risikoanalyse ermittelten Sicherheitsmaßnahmen verbleibenden Restrisiken sind zu bewerten und zu dokumentieren.

Im Rahmen der Planung können auch Abweichungen vom Whitepaper festgestellt werden, die z.B. aus funktionalen Gründen unumgänglich sind. In diesem Fall sind die mit der Abweichung verbundenen Risiken zu prüfen, ggf. entsprechende Alternativlösungen zu entwickeln und zu dokumentieren. Ist keine gleichwertige Sicherheitslösung umsetzbar, so sind die verbleibenden Restrisiken ebenfalls zu dokumentieren. Der vorstehende Absatz gilt unabhängig von der Schutzbedarfseinstufung.

Alle in diesem Abschnitt genannten Tätigkeiten liegen im Verantwortungsbereich der Projektleitung. Diese hat den Prozess entsprechend zu dokumentieren.

Berücksichtigung des Whitepaper bei Ausschreibungen

Ist das geplante Projekt zur Ausschreibung vorgesehen, werden nach Ende der planerischen Phase die ermittelten endgültigen Sicherheitsanforderungen in das Lastenheft integriert. Dort müssen mindestens folgende Unterlagen enthalten sein:

a) eine Kopie des aktuellen Whitepaper „Sichere Steuerungs- und Telekommunikationssysteme“

b) ggf. konkretisierte Anforderungen und zusätzliche Maßnahmen sowie Umsetzungsvorgaben aus den Ergebnissen der Risikoanalyse

c) zulässige Ausnahmen oder Workarounds

Die potentiellen Anbieter haben zu den Sicherheitsanforderungen im Lastenheft ihr Angebot zu entwickeln und dort ggf. notwendige Abweichungen, Alternativvorschläge und eine Roadmap zur Umsetzung zu dokumentieren. Die Projektleitung ist wiederum verpflichtet, diese Abweichungen aus ihrer Sicht zu bewerten. Die Bewertung fließt in die Entscheidung zur Zuschlagserteilung ein. Verbleibende Restrisiken müssen vom zukünftigen Eigentümer des zu beschaffenden Systems akzeptiert werden, bevor der Zuschlag erteilt wird.

Foreword

Application information

A white paper specifying essential security measures for control and telecommunication systems has been developed for power industry organisations. The purpose of this document is to sufficiently protect the operation of these systems against security threats. The security measures described in this document are recommended for all newly procured control and telecommunication systems. The strategic goal of this white paper is to favourably influence the future development for aforementioned systems with regard to IT security. Furthermore the document should establish a mutual understanding for the protection issues of these systems throughout the industry.

Design of a Control or Telecommunication System

During the design phase of new control or telecommunication systems a protection level determination shall be accomplished at an early stage. The protection level determination process is for example described in the IT Grundschutz manual (Baseline Protection manual) of the German BSI (Bundesamt für Sicherheit in der Informationstechnik). If the protection level determination results in a low or medium protection level the requirements of this white paper are sufficient. In case of a high or very high protection level a complementary risk analysis is mandatory. The risk analysis shall asses whether the security measures described in this white paper are adequate to fulfil the protection level requirements. Otherwise these security measures shall be enhanced. Furthermore additional security measures, covering risks which are not discussed in this white paper, shall be defined. The residual risk after the application of the security measures described in this white paper and the additional measures defined in the risk analysis shall be evaluated and documented.

In the system design phase inevitable deviations from the white paper requirements might be detected in order to meet obligatory functional requirements. In this case the risk associated with these deviations shall be assessed, if necessary appropriate alternative solutions shall be developed and documented. This approach shall be applied irrespectively of the system's protection level requirement.

The project management is responsible for all activities described in this section and shall document the process accordingly.

Consideration of the Whitepaper for Tendering Procedures

If the project is intended for tendering, the determined final security requirements shall be integrated into the requirement specifications at the end of the design phase. The requirement specifications shall at least include the following documentation:

a) An up-to-date copy of the white paper „Requirements for Secure Control and Telecommunication Systems”

b) If necessary additional requirements and measures as well as requirement specifications due to the results of risk analysis

c) Tolerable exceptions and workarounds

The potential bidders shall develop their proposal according to the security requirements defined in the requirement specifications. If necessary, the bidder shall document deviations from the requirements, alternative solutions and a implementation roadmap. The project management is obligated to evaluate these deviations from their point of view. This evaluation shall be incorporated in the decision process for the acceptance of a tender. Residual risks shall be accepted by the prospective system owner before the tender is accepted.

Inhaltsverzeichnis

Table of Contents

1 Präambel

1.1 Zielsetzung

Das hier vorgelegte Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ beschreibt unter Beachtung von technischen und betrieblichen Rahmenbedingungen Sicherheitsanforderungen an sowie Schutzmaßnahmen für IT-gestützte Steuerungs- und Telekommunikationssysteme.

Ziel ist es, diese Systeme gegen Sicherheitsbedrohungen im täglichen Betrieb angemessen zu schützen, die Auswirkungen von Bedrohungen auf den Betrieb zu minimieren und die Aufrechterhaltung des Geschäftsbetriebs auch bei Sicherheitsvorfällen sicherzustellen bzw. ein definiertes Mindestmaß an Diensten bzw. Dienstequalität schnellstmöglich wieder herzustellen.

Strategisches Ziel des Whitepapers ist die positive Beeinflussung der Produktentwicklung im adressierten Sektor im Sinne der IT-Sicherheit und die Vermittlung eines gemeinsamen Verständnisses in der Branche für den Schutz dieser Systeme.

1.2 Geltungsbereich

Das Whitepaper ist für alle neu zu beschaffenden bzw. neu einzuführenden Steuerungs- und Telekommunikationssysteme anzuwenden, die im Prozessbereich der Energieversorgungsunternehmen betrieben werden.

1.3 Adressaten

Das Whitepaper richtet sich an potenzielle

1 Preamble

1.1 Goal

This white paper „Requirements for Secure Control and Telecommunication Systems“ defines basic security measures and requirements for IT-based control, automation and telecommunication systems, taking into account general technical and operational conditions.

The purpose of this white paper is to sufficiently protect these control and telecommunication systems against common IT security threats and to minimise the impact of these threats on systems operations. Furthermore, these requirements shall help to maintain business operations in case of security incidents or at least guarantee the fast restoration of a predefined basic service level.

The strategic goal of this white paper is to favourably influence the future development of these systems with regard to IT security.

Furthermore the document should establish a mutual understanding for the protection issues of these systems throughout the industry.

1.2 Scope

The requirements of this white paper are obligatory for all control and telecommunication systems, which will be newly procured or installed and which will be operated in the process environment of a utility.

1.3 Target Audience

This white paper is intended for potential

Auftragnehmer sowie unternehmensinterne Planer, Realisierer und Betreiber von Steuerungs- und Telekommunikationssystemen. Es unterstützt sie bei der Planung, Beschaffung, Realisierung und dem Betrieb. Das Whitepaper wird an Auftragnehmer und Hersteller kommuniziert und soll ihnen bereits im Vorfeld bei der Konzeption bzw. Weiterentwicklung ihrer Systeme Hilfestellung leisten.

Insbesondere richtet sich dieses Whitepaper an:

- Systemdesigner von Steuerungs- und Telekommunikationssystemen
- Hersteller von Steuerungs- und Telekommunikationssystemen bzw. von Teilkomponenten
- Integratoren und Lieferanten von Steuerungs- und Telekommunikationssystemen
- Dienstleister in den Bereichen Betrieb, Instandhaltung und Support

contractors and in-house system designers, integrators and operators of control and telecommunication systems. It should support them in design, procurement, realisation and operation of these systems. The white paper will be supplied to contractors and vendors and shall support them in designing and further development of their control and telecommunication systems and devices.

In particular this white paper is intended for:

- Control and telecommunication system designers
- Manufacturers of systems, subsystems, and devices
- Vendors and integrators of systems, subsystems, and devices
- Operation, support, and maintenance service providers

1.4 Gültigkeit und Verfahren

Um im Rahmen einer Ausschreibung von neuen Steuerungs- und Telekommunikationssystemen die Anforderungen dieses Whitepapers zu berücksichtigen, ist die Einhaltung im Rahmen des Lastenheftes von den Anbietern verbindlich einzufordern. Hierzu wird das Whitepaper allen relevanten Ausschreibungen beigefügt.

Die im Whitepaper definierten Anforderungen sind grundsätzlich von allen neu beschafften Steuerungs- und Telekommunikationssystemen zu erfüllen, sofern das Lastenheft nichts anderes festlegt. Ist eine Umsetzung der Anforderungen nicht bzw. nur mit unvertretbar hohem Aufwand mög-

1.4 Application

To meet the requirements of this white paper during invitations to bid for new control and telecommunication systems, the compliance with these requirements shall be demanded from contractors in the contract specifications. Thus, the white paper shall be included in the tender offer.

The requirements defined in the white paper shall be met by all novel control and telecommunication systems unless otherwise agreed in the contract specifications. If compliance with a white paper requirement is technically impossible (or only realisable with unjustifiable high effort) the contractor has to justify and clearly indi-

lich, ist dies bereits im Angebot vom Anbieter deutlich kenntlich zu machen und zu begründen (u. a. mit Angabe des zur Umsetzung nötigen Mehraufwands). Dies gilt auch für die Sollbestimmungen, die im Text von der technischen Umsetzungsmöglichkeit abhängig gemacht wurden („wo technisch möglich“).

Im Falle einer Beauftragung sind nicht einzuhaltende Forderungen zu dokumentieren und Abweichungen vom Whitepaper von Auftraggeber und -nehmer schriftlich zu bestätigen.

Über eine Berücksichtigung der Anforderungen des Whitepapers für bereits vorhandene Systeme im Rahmen von Erweiterungen oder neuen Versionen entscheidet der Auftraggeber.

Dieses Dokument orientiert sich an den aktuellen technischen Entwicklungen und den Erkenntnissen über Schutzbedarf und Schwachstellen im Umfeld von Steuerungs- und Telekommunikationssystemen. Neue Technologieentwicklungen, Sicherheitsrisiken und Schutzanforderungen werden im Rahmen einer regelmäßigen Überarbeitung durch den Herausgeber des Whitepapers berücksichtigt.

1.5 Hinweis zu ISO/IEC Referenzen

In diesem Dokument wird jeweils zu Beginn eines Abschnitts auf so genannte Controls des internationalen Standards ISO/IEC 27002:2013 „Code of practice for information security controls“ und dessen Erweiterung für den Energiesektor ISO/IEC TR 27019:2013 „Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry” verwiesen.

cate non-compliance to the affected requirements already during the bidding process. Furthermore the contractor shall specify the additional costs which the realisation of the affected requirements would cause. This also applies to the requirements, for which the implementation is demanded depending on the technical feasibility.

If the contract is awarded, exceptions to the listed requirements shall be documented and confirmed in writing by both the contractor and client.

The client decides if the white paper requirements shall be applied to enhancement and upgrade projects of existing systems.

This document considers the current technical developments and findings about protection requirements and vulnerabilities of control and telecommunication systems. Novel technical developments, security threats and protection requirements shall be accounted for by regular revision of the white paper by its editors.

1.5 References to ISO/IEC standards

Where applicable, the sub-clauses of this document reference the controls of the international standard ISO/IEC 27002:2013 „Code of practice for information security controls“ and the sector specific controls for the energy utility domain of ISO/IEC TR 27019:2013 „Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility

Diese Referenzen dienen lediglich als Hinweis auf die im Standard aufgeführte „Implementation guidance“, die bei der Umsetzung der Forderungen zu Rate gezogen werden kann. **Verbindlich** umzusetzen, sind jedoch immer nur die in diesem Whitepaper explizit aufgeführten Forderungen. Zu beachten ist ebenfalls, dass sich die Systematik dieses Whitepapers von der der Standards ISO/IEC 27002 und ISO/IEC TR 27019 unterscheidet.

industry”.These references only serve as hints to the implementation guidance of the controls of the ISO/IEC documents, which might be considered when implementing the white paper requirements. However, mandatory for compliance are the explicit requirements of the white paper, not the ISO/IEC standard controls. Please note that the structure of this white paper differs from ISO/IEC 27002 and ISO/IEC TR 27019.

2 Sicherheitsanforderungen

2.1 Allgemeines/Organisation

2.1.1 Allgemeines

2.1.1.1 Sichere Systemarchitektur

ISO/IEC 27002:2013: 9.4.1, 13.1.3, 14.2.5, 14.2.7, 17.2.1

Das Gesamtsystem muss auf einen sicheren Betrieb hin entworfen und entwickelt werden. Zu den Prinzipen eines sicheren Systemdesigns gehören:

Minimal- / Need-To-Know-Prinzip: Jede Komponente und jeder Benutzer erhält nur die Rechte, die für die Ausführung einer Aktion nötig sind. So werden z. B. Anwendungen und Netzwerk-Dienste nicht mit Administratorprivilegien, sondern nur mit den minimal nötigen Systemrechten betrieben.

Defence-In-Depth Prinzip: Sicherheitsrisiken werden nicht durch einzelne Schutzmaßnahmen angegangen, sondern durch die Implementierung gestaffelter, auf mehreren Ebenen ansetzender und sich ergänzender Sicherheitsmaßnahmen begrenzt.

Redundanz-Prinzip: Das System ist so ausgelegt, dass der Ausfall einzelner Komponenten die sicherheitsrelevanten Funktionen nicht beeinträchtigt. Das Systemdesign verringert die Wahrscheinlichkeit und die Auswirkungen von Problemen, die durch das uneingeschränkte Anfordern von Systemressourcen, wie z. B. Arbeitsspeicher oder Netzwerkbandbreite entstehen (sog. Resource-Consumption- oder DoS-Angriffe).

2 Requirements

2.1 General Requirements and Housekeeping

2.1.1 General

2.1.1.1 Secure System Architecture

ISO/IEC 27002:2013: 9.4.1, 13.1.3, 14.2.5, 14.2.7, 17.2.1

The system shall be designed and build for secure operations. Examples of secure design principles are:

Minimal-privileges/Need-to-know principle: User and system components only posses the minimal privileges and access rights they need to fulfil a certain function. Applications and network services, for example, should not be run with administrator privileges.

Defence-in-depth principle: Security threats are not mitigated by a single countermeasure only, but by implementing several complementary security techniques at multiple system levels.

Redundancy principle: Due to a redundant system design the failure of a single component will not interfere with the system security functions. The system design shall reduce the likelihood and impact of problems which occur due to excessive consumption of system resources (e. g. RAM, network bandwith) or denial-of-service attacks.

2.1.1.2 Ansprechpartner

ISO/IEC 27002:2013: 12.6.1

Der Auftragnehmer muss einen Ansprechpartner definieren, der während der Angebotsphase, der System-Entwicklung und während des geplanten Betriebszeitraumes für den Bereich der IT-Sicherheit verantwortlich ist.

2.1.1.2 Contact Person

ISO/IEC 27002:2013: 12.6.1

The contractor provides a contact person, who will be the single point of contact for IT security related topics during the bidding process, the system design phase and throughout the projected period of system operations.

2.1.1.3 Patchfähigkeit, Patchmanagement

ISO/IEC 27002:2013: 12.6.1

Alle Komponenten des Gesamtsystems müssen patchfähig sein. Das Einspielen eines Patches sollte möglichst ohne Unterbrechung des normalen Betriebs und mit geringen Auswirkungen auf die Verfügbarkeit des Gesamtsystems erfolgen. Beispielsweise ist eine primärtechnische Außerbetriebnahme der kompletten Anlage zum Patchen der sekundärtechnischen Komponenten zu vermeiden. Bevorzugt werden die Patches zuerst auf den passiven Redundanz-Komponenten eingespielt und nach einem Switch-Over-Prozess (Wechsel der aktiven Komponente im Redundanzsystem) und einem darauffolgendem Test auf den restlichen Komponenten installiert.

Der Hersteller muss einen Patchmanagementprozess für das gesamte System unterstützen, anhand dessen das Testen, Installieren und Dokumentieren von Sicherheitspatches und Updates gesteuert und verwaltet werden kann. Die Updates sollen vom Betriebspersonal, das diese Systeme administriert, eingespielt werden. Das Installieren bzw. Deinstallieren von Patches muss vom Anlagenbetreiber autorisiert werden und darf nicht automatisch

2.1.1.3 Patching and Patch Management

ISO/IEC 27002:2013: 12.6.1

The system shall allow the patching of all system components during normal system operation. Installation of a patch should be possible without interruption of normal system operations and with little impact on the system's availability. For example, a complete shut down of the primary generation, transmission or distribution systems should not be necessary to install updates on secondary systems. Preferentially, the patches will be installed on passive redundant components first. After a switch-over process (change of the active component in the redundant system) and a subsequent test the patch will be installed on the remaining components. The contractor shall support a patch management process for the entire system, this process shall manage the testing, installation and documentation of security patches and system updates. In general, it should be possible that the operating staff who administrates the systems installs the patches and updates. Installation and deinstallation of patches and updates shall be authorized by the system owner and must not be performed automatically.

geschehen.

2.1.1.4 Bereitstellung von Sicherheitspatches für alle Systemkomponenten

ISO/IEC 27002:2013: 12.6.1

Der Auftragnehmer muss Sicherheitsupdates für alle Systemkomponenten während des gesamten Betriebszeitraums, der vertraglich geregelt wird, zur Verfügung stellen. Updates von Basiskomponenten, die nicht vom Auftragnehmer entwickelt wurden, wie z. B. Betriebssystem, Bibliothek oder Datenbank-Managementsystem, muss der Auftragnehmer von den jeweiligen Herstellern beziehen, diese testen und sie gegebenenfalls an den Auftraggeber weiterleiten. Die Bereitstellung der Updates muss innerhalb eines angemessenen Zeitrahmens, dessen Frist vertraglich festzulegen ist, erfolgen.

2.1.1.4 Provision of Security Patches for all System Components

ISO/IEC 27002:2013: 12.6.1

The contractor shall provide security updates for all system components throughout the entire, contractually agreed lifecycle of the system. The contractor shall obtain updates for basic system components which are not developed by the contractor but by third parties (e. g. operating system, library, database management system) from the component vendor, test them and provide them, if applicable, directly to the customer. The contractor shall provide security updates in an appropriate time frame, which will be defined in the contract specifications

2.1.1.5 Support für eingesetzte Systemkomponenten

ISO/IEC 27002:2013: 12.6.1, 14.2.7

Der Auftragnehmer muss sicherstellen, dass für die nicht von ihm entwickelten Systemkomponenten (z. B. Betriebssystem, Datenbank-Managementsystem, …) innerhalb des geplanten Betriebszeitraums, der vertraglich geregelt wird, Herstellersupport und Sicherheitsupdates zur Verfügung stehen. Das Abkündigungsverfahren und alle relevanten Fristen wie z. B. Last-Customer-Shipping und End-Of-Support müssen vertraglich festgeschrieben werden.

2.1.1.5 Third Party Support

ISO/IEC 27002:2013: 12.6.1, 14.2.7

The contractor shall ensure that during the scheduled life cycle of the system security support for third-party system components (e. g. operating systems, libraries, database management systems) is available. The end-of-life terms (e. g. Last Customer Ship Date, End of Support date) shall be defined in the contract specifications.

2.1.1.6 Verschlüsselung sensibler Daten bei Speicherung und Übertragung

ISO/IEC 27002:2013: 12.4.2, 13.1.2, 18.1.3, 18.1.4

Sensible Daten dürfen im System nur verschlüsselt gespeichert bzw. übertragen werden. Zu den zu schützenden Daten können beispielsweise Protokolldateien, Passwörter oder vertrauliche Daten nach behördlichen Vorgaben oder den relevanten Gesetzen, wie z.B. dem Bundesdatenschutzgesetz gehören. Gegebenfalls soll das System auch die sichere, selektive Löschung bestimmter Daten ermöglichen, beispielsweise durch Überschreiben mit Zufallsdaten.

2.1.1.6 Encryption of Sensitive Data during Storage and Transmission

ISO/IEC 27002:2013: 12.4.2, 13.1.2, 18.1.3, 18.1.4

Sensitive data shall be stored or transmitted in encrypted form only. Sensitive data may include, but is not limited to: log files, passwords, or sensitive data as defined by regulatory or legal requirements (e. g. data protection laws). If applicable, the system shall allow for the secure deletion of selected data, for example by overwriting with random data.

2.1.1.7 Verschlüsselungsstandards

ISO/IEC 27002:2013: 10.1.1, 10.1.2, 18.1.5
ISO/IEC TR 27019:2013: 10.6.3

Bei der Auswahl von Verschlüsselungsstandards sind nationale Gesetzgebungen zu berücksichtigen. Es dürfen nur anerkannte Verschlüsselungs-Verfahren und Schlüsselmindestlängen benutzt werden, die nach aktuellem Stand der Technik auch in Zukunft als sicher gelten. Selbstentwickelte Verschlüsselungs-Algorithmen sind nicht erlaubt. Bei der Implementierung der Verschlüsselungs-Verfahren sollte, wo möglich, auf anerkannte Verschlüsselungs-Bibliotheken zurückgegriffen werden, um Implementierungsfehler zu vermeiden.

2.1.1.7 Cryptographic standards

ISO/IEC 27002:2013: 10.1.1, 10.1.2, 18.1.5
ISO/IEC TR 27019:2013: 10.6.3

When selecting cryptographic standards regulations and national restrictions shall be considered. Only state-of-the-art cryptographic standards and key lengths shall be used. From the current state of scientific and technical knowledge these standards and key lengths shall also be considered secure for the foreseeable future. Cryptographic algorithms developed in-house shall not be used. Whenever possible, well-known cryptographic libraries should be used when implementing cryptographic functions to avoid implementation bugs.

2.1.1.8 Interne/externe Sicherheits- und Anforderungstests und zugehörige Dokumentation

ISO/IEC 27002:2013: 14.2.7, 14.2.8, 14.2.9, 15.2.1

Die einzelnen Systemkomponenten und die wesentlichen Funktionen des Gesamtsystems (in einer repräsentativen Konfiguration) müssen vor der Auslieferung vom Auftragnehmer durch eine vom Entwicklungsteam unabhängige Abteilung einem Sicherheits- und Stresstest unterzogen werden. Die Vorgehensweise ist mit dem Auftraggeber abzustimmen. Die Ergebnisse der Tests sowie die dazugehörige Dokumentation (Softwarestände, Prüfkonfiguration, etc.) werden dem Auftraggeber zur Verfügung gestellt. Zusätzlich hat der Auftraggeber das Recht, diese Tests auch selbst vorzunehmen oder durch einen externen Dienstleister durchführen zu lassen.

2.1.1.8 Internal and External Software and Security Tests and Related Documentation

ISO/IEC 27002:2013: 14.2.7, 14.2.8, 14.2.9, 15.2.1

The contractor shall perform a detailed security and stress test on the individual system components as well as on the entire system and its essential functions using a representative system configuration. The team undertaking these tests shall be independent from the development team. The test procedure shall be coordinated with the customer. The results of these tests and the according documentation (software versions, test configuration, etc.) shall be provided to the customer. Additionally, the customer is allowed to carry out the tests or let them be conducted by an external third party.

2.1.1.9 Sichere Standard-Konfiguration und Erstinstallation bzw. (Wieder-) Inbetriebnahme

ISO/IEC 27002:2013: 9.4.4, 12.5.1, 14.3.1

Das System muss nach der Erstinstallation bzw. bei der (Wieder-) Inbetriebnahme in einem betriebssicheren Zustand konfiguriert sein, wobei diese definierte Grundkonfiguration dokumentiert sein muss. Dienste, Services und Funktionen sowie Daten, die nur zur Entwicklung oder zum Testbetrieb notwendig sind, müssen vor der Auslieferung bzw. vor dem Übergang in den Produktivbetrieb nachweisbar entfernt bzw. dauerhaft deaktiviert werden.

2.1.1.9 Secure Standard Configuration, Installation and Start-Up

ISO/IEC 27002:2013: 9.4.4, 12.5.1, 14.3.1

After initial installation and start-up the system shall be configured in a fail-safe manner. This defined base configuration shall be documented. System services and daemons, data and functions, which are used during development or for system testing only shall be verifiably removed or deactivated before the systems goes productive.

2.1.1.10 Integritäts-Prüfung

ISO/IEC 27002:2013: 12.5.1, 14.2.1, 14.2.4

Systemdateien, Anwendungen, Konfigurationsdateien und Anwendungs-Parameter müssen auf Integrität überprüft werden können, beispielsweise durch Prüfsummen.

2.1.1.10 Integrity Checks

ISO/IEC 27002:2013: 12.5.1, 14.2.1, 14.2.4

It shall be possible to verify the integrity of system and application files and executables, configuration and application parameter files, for example through the use of check sums.

2.1.2 Dokumentation

2.1.2 Documentation

2.1.2.1 Design-Dokumentation, Beschreibung sicherheitsrelevanter Systemkomponenten und Implementations-Spezifikationen

ISO/IEC 27002:2013: 12.1.1, 14.1.1, 14.2.7
ISO/IEC TR 27019:2013: 10.1.1

Dem Auftraggeber muss spätestens zur Abnahme eine Gesamtdokumentation über das High-Level-Design des Gesamtsystems zur Verfügung gestellt werden. Darin beschrieben sind der grundsätzliche Aufbau des Systems und die Interaktionen aller beteiligten Komponenten. In dieser Dokumentation wird besonders auf die sicherheitsrelevanten oder schützenswerten Systemkomponenten sowie ihre gegenseitigen Abhängigkeiten und Interaktionen eingegangen. Außerdem werden sicherheitsspezifische Implementierungsdetails aufgelistet und kurz beschrieben (z. B. verwendete Verschlüsselungsstandards).

2.1.2.1 Design Documentation Specification of Security Relevant System Components and Implementation Characteristics

ISO/IEC 27002:2013: 12.1.1, 14.1.1, 14.2.7
ISO/IEC TR 27019:2013: 10.1.1

The contractor shall provide the customer with documentation covering the high level design of the entire system. The documentation shall be available not later than the time of the acceptance test and shall include the description of the system concept and of the interaction of all system components. The documentation shall characterise especially the details, interactions and dependencies of the system components which are security relevant or which deserve special protection. Furthermore the documentation shall list and describe in brief implementation details of security related functions (e. g. used cryptographic standards).

2.1.2.2 Administrator- und Benutzer-Dokumentation

ISO/IEC 27002:2013: 7.2.2, 12.1.1
ISO/IEC TR 27019:2013: 10.1.1

Es müssen getrennte Dokumentationen für

2.1.2.2 Administrator and User Documentation

ISO/IEC 27002:2013: 7.2.2, 12.1.1
ISO/IEC TR 27019:2013: 10.1.1

The contractor shall provide separate user

den Administrator und die System-Benutzer existieren. Beide Dokumentationen sollten für die jeweiligen Gruppen unter anderem eine Auflistung der sicherheitsrelevanten Einstellungen und Funktionen enthalten und Regeln für sicherheitsverantwortliches Handeln nennen.

and administrator documentation. Both documentations should include a list of security functions and parameters as well as instructions and responsibilities for secure operation of the system.

2.1.2.3 Dokumentation sicherheitsrelevanter Einstellungen und Systemmeldungen

ISO/IEC 27002:2013: 12.1.1
ISO/IEC TR 27019:2013: 10.1.1

In der Administratordokumentation existiert eine Beschreibung aller sicherheitsrelevanten Systemeinstellungen und Parameter sowie ihrer Defaultwerte. Die Dokumentation weist auf Konsequenzen von grob unsicheren Konfigurationseinstellungen hin. Außerdem sind in einer Dokumentation alle sicherheitsspezifischen Log- und Audit-Meldungen erläutert und mögliche Ursachen sowie gegebenenfalls passende Gegenmaßnahmen genannt.

2.1.2.3 Documentation of Security Parameters and Security Log Events or Warnings

ISO/IEC 27002:2013: 12.1.1
ISO/IEC TR 27019:2013: 10.1.1

The administrator documentation shall include a description of all security parameters and their default values. The documentation shall alert of the consequences of grossly insecure parameter settings. Furthermore documentation shall be provided that includes all security events, warnings and log messages the system generates, possible causes and the related administrative action that should be taken.

2.1.2.4 Dokumentation der Voraussetzungen und Umgebungs-Anforderungen für den sicheren System-Betrieb

ISO/IEC 27002:2013: 12.1.11
ISO/IEC TR 27019:2013: 10.1.1

In der Administratordokumentation existiert eine Darstellung in der die Voraussetzungen für einen sicheren Systembetrieb beschrieben werden. Dazu zählen unter anderem Anforderungen an den Benutzerkreis, Netzwerkumgebung sowie Interaktion und Kommunikation mit ande-

2.1.2.4 Documentation of Requirements and Assumptions needed for Secure System Operation

ISO/IEC 27002:2013: 12.1.11
ISO/IEC TR 27019:2013: 10.1.1

The administrator documentation shall provide a description of requirements relevant for secure systems operation. The description may contain, for example, assumptions about user behaviour and network environment or requirements for interaction and communication with other

ren Systemen und Netzwerken.

2.2 Bereich Basissystem

2.2.1 Grundsicherung und Systemhärtung

ISO/IEC 27002:2013: 9.4.4, 12.6.2, 13.1.2, 14.2.4

Alle Komponenten des Basissystems müssen anhand anerkannter Best-Practice-Guides dauerhaft gehärtet und mit aktuellen Service-Packs und Sicherheits-Patches versehen sein. Ist dieses technisch nicht durchführbar, ist für die Übergangsphase (bis zur vollständigen Erfüllung der Forderung aus 2.1.1.3) eine dokumentierte entsprechende Sicherheitsmaßnahme zu ergreifen. Unnötige Benutzer, Defaultuser, Programme, Netzwerkprotokolle, Dienste und Services sind deinstalliert, oder – falls eine Deinstallation nicht möglich ist – dauerhaft deaktiviert und gegen versehentliches Reaktivieren geschützt. Die sichere Grundkonfiguration der Systeme muss überprüft und dokumentiert sein. Insbesondere müssen die in diesem Dokument geforderten Maßnahmen, die zur Härtung der Systeme beitragen, durchgeführt sein.

2.2.2 Antiviren-Software

ISO/IEC 27002:2013: 12.2.11
ISO/IEC TR 27019:2013: 10.4.1

Alle vernetzten, IP-basierenden Systeme müssen an geeigneter Stelle mit Antiviren-Software und Malware-Schutz versehen sein. Alternativ zum Einsatz von Antiviren-Scannern auf allen Systemen ist vom Lieferanten ein umfassendes Antiviren-Konzept vorzulegen, das einen gleichwerti-

systems or networks.

2.2 Base System

2.2.1 System Hardening

ISO/IEC 27002:2013: 9.4.4, 12.6.2, 13.1.2, 14.2.4

All components of the base system shall be permanently hardened according to well-known best-practise guides. Furthermore the latest security patches and service packs shall be installed. If this is technically not feasible, a documented equivalent security measure shall be implemented for a transitional period (until the requirements of 2.1.1.3 are completely fulfilled). Unnecessary user accounts, default users, system daemons, programs, network protocols and services shall be removed, or - if removal is technically not possible – shall be permanently disabled and secured against accidental reactivation. The secure base system configuration shall be reviewed and documented. Especially, the security measures required in this document which contribute to system hardening shall be carried out.

2.2.2 Anti Virus Software

ISO/IEC 27002:2013: 12.2.11
ISO/IEC TR 27019:2013: 10.4.1

The base systems of all IP-based networked system components shall be secured with virus and malware protection software. As an alternative to installing antivirus software on each system component, the contractor may implement a comprehensive antivirus and malware pro-

gen Schutz bietet. Für eine automatische und zeitnahe Aktualisierung der Antiviren-Pattern-Dateien muss gesorgt sein, wobei keine direkte Verbindung mit Updateservern in externen Netzen, wie dem Internet benutzt werden darf. Eine Realisierungsmöglichkeit wäre zum Beispiel die Verwendung eines internen Updateservers. Der Zeitpunkt der Aktualisierung auf den Endsystemen ist konfigurierbar. Als Alternative zur automatischen Aktualisierung ist ein sicherer Prozess zu definieren und zu dokumentieren, bei dem die Updates regelmäßig und zeitnah manuell in das System eingespielt werden.

tection concept, which provides an equivalent protection. The patterns of the anti-virus and malware protection software shall be automatically and timely updated without using a direct connection to update-servers located in external networks like the internet. A possible implementation would be to use an internal update server. The time when the patterns are updated shall be configurable. An alternative to automatic updates is a well-defined and documented secure manual process, through which the pattern updates are installed in the system, for example on an isolated central update server.

2.2.3 Autonome Benutzerauthentifizierung

ISO/IEC 27002:2013: 9.2.1, 9.2.2, 9.4.2

Die zur Nutzeridentifizierung und -authentifizierung auf Betriebssystemebene nötigen Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden. Die Anbindung an einen zentralen, prozessnetz-internen Directory Service sollte in Betracht gezogen werden.

2.2.3 Autonomous User Authentication

ISO/IEC 27002:2013: 9.2.1, 9.2.2, 9.4.2

Data used for user identification and authentication shall not solely be obtained from sources located outside of the secure process network. Integration of user identification and authentication into a central isolated directory service within the process network should be considered.

2.3 Bereich Netze / Kommunikation

2.3 Networks / Communication

2.3.1 Sichere Netzwerkkonzeption und Kommunikationsverfahren

2.3.1 Secure Network Design and Communication Standards

2.3.1.1 Eingesetzte Protokolle und Technologien

ISO/IEC 27002:2013: 9.4.1, 9.4.3, 10.1.1, 13.1.1, 13.1.3
ISO/IEC TR 27019:2013: 10.6.3, 10.12.1, 11.4.5

a) Wo technisch möglich, dürfen nur si-

2.3.1.1 Deployed Communication Technologies and Network Protocols

ISO/IEC 27002:2013: 9.4.1, 9.4.3, 10.1.1, 13.1.1, 13.1.3
ISO/IEC TR 27019:2013: 10.6.3, 10.12.1, 11.4.5

a) If technically feasible, the systems

chere Kommunikationsstandards- und Protokolle benutzt werden, die Integritätsüberprüfung, Authentifizierung und ggf. Verschlüsselung bieten. Das betrifft besonders die Protokolle zur Remote-Administration oder durch welche Benutzer-Anmeldeinformationen übertragen werden. Passwort-Übertragungen im Klartext sind nicht erlaubt (z. B. kein Telnet, keine Unix r-Dienste). Eine aktuelle Liste der sicheren Protokolle kann nach den jeweils internen Regularien des Auftraggebers bereitgestellt werden.

b) Das Gesamtsystem und jede dazugehörige Netzwerkkomponente müssen sich in die Netzwerk-Konzeption des Gesamtunternehmens einbinden lassen. Relevante Netzwerk-Konfigurationsparameter wie IP-Adressen müssen zentral administriert werden können. Zur Administration und zum Monitoring werden sichere Protokolle verwendet (SSHv2, SNMPv3). Die Netzwerkkomponenten sind gehärtet, unnötige Dienste und Protokolle sind deaktiviert, Management-Interfaces sind durch ACL geschützt.

c) Netzwerkkomponenten, die vom Auftragnehmer bereitgestellt werden, müssen in ein zentrales Inventory- und Patchmanagement eingebunden werden können.

d) Wo technisch möglich, wird auf WAN-Verbindungen das IP-Protokoll verwendet und unverschlüsselte Applikations-Protokolle durch Verschlüsselung auf den unteren Netzwerkebenen geschützt (z. B. durch SSL/TLS-Verschlüsselung oder durch VPN-Technologie).

e) Wo technisch möglich, werden Firewall-

should use only secure communication standards and protocols which provide integrity checks, authentication and, if applicable, encryption. In particular, secure communication shall be used for remote administration or transmission of user log on information. The transmission of password information in clear text is not allowed (e.g. no telnet protocol, no Unix rsh services). An up-to-date list of secure protocols can be provided by the client according to its internal formalities.

b) The system and its network components shall be easily integrable into the network conception of the whole company. Relevant network configuration parameters like IP addresses can be managed centrally. For administration and monitoring secure protocols shall be used (SSHv2, SNMPv3). The network components shall be hardened, unnecessary services and protocols shall be deactivated, management interfaces shall be protected with ACLs.

c) It shall be possible to integrate network components which are provided by the contractor into a central asset and patch management process.

d) If technically feasible, the IP protocol is used on WAN lines. Unencrypted application layer protocols should be secured by encryption on lower network layers (e. g. with SSL/TLS encryption or by using VPN technologies).

e) If applicable, firewall friendly protocols should be used: e. g. TCP instead of UDP, OPC over network boundaries should be avoided.

f) If shared network infrastructure com-

freundliche Protokolle benutzt: z. B. TCP anstatt UDP, OPC über Netzgrenzen hinweg vermeiden.

f) Beim Einsatz von gemeinsam genutzten Netzwerk-Infrastrukturkomponenten (z. B. bei VLAN- oder MPLS-Technologie) definiert das Netzwerk mit dem höchsten Schutzbedarf die Anforderungen an die Hardware und deren Parametrierung. Eine gleichzeitige Nutzung der Netzwerkkomponenten bei unterschiedlichem Schutzbedarf darf nur vorgenommen werden, wenn eine Herabsetzung des Schutzniveaus oder der Verfügbarkeit durch die Gleichzeitigkeit in keinem Fall möglich ist.

2.3.1.2 Sichere Netzwerkstruktur

ISO/IEC 27002:2013: 9.4.1, 13.1.3, 13.1.2
ISO/IEC TR 27019:2013: 10.6.3, 10.12.1, 11.4.5, 11.4.8

a) Vertikale Netzwerksegmentierung: Soweit anwendbar und technisch möglich, wird die dem System zugrundeliegende Netzwerkstruktur in Zonen mit verschiedenen Funktionen und unterschiedlichem Schutzbedarf aufgeteilt. Wo technisch möglich, werden diese Netzwerk-Zonen durch Firewalls, filternden Router oder Gateways getrennt. Die Kommunikation mit weiteren Netzwerken hat ausschließlich über vom Auftraggeber zugelassene Kommunikationsprotokolle unter Einhaltung der geltenden Sicherheitsregeln zu erfolgen.

b) Horizontale Netzwerksegmentierung: Soweit anwendbar und technisch möglich, wird die dem System zugrundeliegende Netzwerkstruktur auch horizontal

ponents (e. g. VLAN or MPLS technology) will be used the network with the highest protection level requirement determines the security requirements of the used hardware components and their configuration. Concurrent use of the network hardware for networks with different protection levels is permitted only if this concurrent use does not decrease the security level or the availability.

2.3.1.2 Secure Network Design

ISO/IEC 27002:2013: 9.4.1, 13.1.3, 13.1.2
ISO/IEC TR 27019:2013: 10.6.3, 10.12.1, 11.4.5, 11.4.8

a) Vertical network segmentation: If applicable and technically feasible the network infrastructure of the system shall be divided into multiple vertical zones with different functions and protection requirements. Where technically feasible the network zones shall be separated by firewalls, filtering routers or gateways. Network connections to external networks shall be deployed only using communication protocols approved by the customer and in compliance with the security policies in effect.

b) Horizontal network segmentation: If applicable and technically feasible the network infrastructure of the system shall be divided into independent horizontal segments (e. g. according to dif-

in unabhängige Zonen (z. B. nach Standorten) aufgeteilt, wobei die Trennung der Zonen ebenfalls durch Firewalls, filternde Router oder Gateways erfolgen muss.

c) Firewalls und VPNs werden über einen vom Auftraggeber definierten Prozess zentral bereitgestellt und administriert.

ferent locations), the segments shall be separated by firewalls, filtering routers or gateways.

c) Firewalls and VPN components shall be provided and managed centrally through a defined process by the customer.

2.3.1.3 Dokumentation der Netzwerkstruktur und -konfiguration

ISO/IEC 27002:2013: 8.1.1
ISO/IEC TR 27019:2013: 7.1.1

Die Netzwerkkonzeption und -konfiguration, alle physikalischen, virtuellen und logischen Netzwerkverbindungen und die verwendeten Protokolle sowie die Netzwerk-Perimeter, die Bestandteil des Systems sind bzw. mit ihm interagieren, müssen dokumentiert sein. Änderungen, z. B. durch Updates werden innerhalb des Changemanagements in die Dokumentation aufgenommen. Die Dokumentation muss Angaben über normale und maximal zu erwartende Datenübertragungsraten enthalten, damit gegebenenfalls auf den Netzwerkkomponenten eine Limitierung der Datenübertragungsraten zur Verkehrssteuerung und Verhinderung von DoS-Problemen implementiert werden kann.

2.3.1.3 Documentation of Network Design and Configuration

ISO/IEC 27002:2013: 8.1.1
ISO/IEC TR 27019:2013: 7.1.1

The contractor shall provide documentation which shall describe the network design and configuration, all physical, virtual and logical network connections, the network protocols used, and all network perimeter components which are part of or which interact with the system. All changes (e. g. by updates) shall be included in the documentation using a document management process. To support the implementation of rate limiting functions for QoS and to mitigate DoS problems, the documentation provides values of normal and maximal expected data rate for all network connections.

2.3.2 Sichere Wartungsprozesse und RAS-Zugänge

Hinweis: Der Ausdruck „Wartung“ bezieht sich in diesem Dokument allgemein auf alle vom Auftraggeber/Betreiber zu beauftragenden Service-Maßnahmen wie Instandhaltungsarbeiten, Störungsanalysen,

2.3.2 Secure Maintenance Processes and Remote Access

Please note: the term “maintenance” used in this document denotes all service processes commissioned by the client or system operator, e. g. repairs, fault analyses, failure and fault corrections, system en-

Fehler- und Störungsbehebung, Verbesserungen, Anpassungen, usw.

hancements and adjustments etc.

2.3.2.1 Sichere Fern-Zugänge

ISO/IEC 27002:2013: 9.1.2, 9.4.1, 9.4.2

a) Administration, Wartung und Konfiguration aller Komponenten muss auch über ein Out-of-Band-Netz, zum Beispiel Zugriff lokal, via serielle Schnittstelle, Netzwerk oder direkter Steuerung der Eingabegeräte (KVM), möglich sein.

b) Fern-Zugriff muss über zentral verwaltete Zugangserver durchgeführt werden. Die Zugangserver müssen in einer DMZ betrieben werden und eine Isolation des Prozessnetzes sicherstellen. Es muss ein starkes 2-Faktor-Authentifizierungs-verfahren benutzt werden.

c) Direkte Einwahl Zugänge in Endgeräte sind grundsätzlich nicht erlaubt.

d) Der Zugriff auf einen Fern-Zugang muss (zentral) geloggt werden, wiederholte Fehlversuche werden gemeldet.

e) Alle Fern-Zugangs-Möglichkeiten müssen dokumentiert werden.

2.3.2.1 Secure Remote Access

ISO/IEC 27002:2013: 9.1.2, 9.4.1, 9.4.2

a) It shall be possible to perform administration, maintenance and configuration of all network components via out-of-band channels, like local access, serial interfaces, network or direct control of input devices (KVM).

b) Remote access shall be performed through dedicated central administered terminal servers which ensure isolation of the process network and which are located in a DMZ. Strong 2-factor authentication shall be used.

c) Direct dial-in access to devices is not allowed.

d) Remote access shall be (centrally) logged, multiple failed login-in attempts shall result in a security event audit message.

e) All remote access possibilities and ports shall be documented.

2.3.2.2 Anforderungen an die Wartungsprozesse

ISO/IEC 27002:2013: 9.1.2, 9.2.1, 9.2.2, 15.1.1, 15.1.2
ISO/IEC TR 27019:2013: 11.5.2

a) Der interaktive Fern-Zugang muss über personalisierte Accounts erfolgen. Für automatisierte Abläufe sind spezielle Kennungen einzurichten, die nur bestimmte Funktionen ausführen können und die keinen interaktiven Zugang er-

2.3.2.2 Maintenance Processes

ISO/IEC 27002:2013: 9.1.2, 9.2.1, 9.2.2, 15.1.1, 15.1.2
ISO/IEC TR 27019:2013: 11.5.2

a) Interactive remote access users shall use personal accounts. For non-interactive, automated processes restricted accounts shall be used, for which interactive access is disabled.

möglichen.

b) Es muss technisch sichergestellt sein, dass ein Fern-Zugriff nur erfolgen kann, wenn dieser vom Betriebspersonal, das diese Systeme administriert, freigegeben wird. Bei externen Dienstleister muss die Freigabe für jeden Verbindungsaufbau einzeln erfolgen. Eine Sitzung ist nach Ablauf einer angemessenen Zeit automatisch zu trennen.

c) Am Standort des Auftragnehmers muss der Fern-Zugriff durch einen definierten und geschulten Personenkreis und nur von speziell gesicherten Systemen aus erfolgen. Insbesondere sind diese Zugangs-Systeme während des Fern-Zugriffs von anderen Netzen logisch oder physikalisch zu entkoppeln. Eine physikalische Entkopplung ist der logischen vorzuziehen.

d) Durch einen definierten Wartungsprozess (siehe oben) muss sichergestellt sein, dass das Wartungspersonal im Rahmen des Remote-Zugangs nur Zugriff auf die benötigten Systeme, Dienste und Daten erhält.

e) Das Wartungspersonal muss den aktuell gültigen Anforderungen gemäß der SÜFV genügen, sofern es für Unternehmen mit überregionaler Elektrizitätsversorgung tätig ist.

f) Die Vorortwartung durch Servicetechniker stellt ein ernst zu nehmendes Sicherheitsrisiko dar. Es ist zu vermeiden, dass der Auftragnehmer eigene Hardware an das Prozessnetz anschließt (z. B. Wartungs-Notebooks, aber auch Speichergeräte wie USB-Sticks). Falls dies doch nötig sein sollte,

b) Technical measures shall ensure that remote access sessions are explicitly activated by the administrative personnel. For external service personnel the activation must be performed for each individual session. Each session shall be disconnected after a reasonable time period.

c) Maintenance shall be performed by defined and trained contractor personnel only, using secure systems only. The systems used for remote access are physically or logically disconnected from other systems and networks during a remote access session. A physical separation should be preferred.

d) A defined maintenance process (compare above) shall ensure that maintenance personnel can only access systems, services and data they need for maintenance tasks.

e) The maintenance personnel shall comply with the requirements of SÜFV if it will be deployed at supra-regional utilities.

f) Local maintenance by service personnel poses a significant security threat. Attachment of contractor's hardware (e. g. laptops, USB devices) to the process network should be avoided. If this is not feasible, the hardware must be approved by the client, specifically secured and shall be scanned for malware before attaching it. The contractor shall provide evidence that an adequate internal security policy is implemented.

muss diese Hardware speziell abgesichert und vom Auftraggeber genehmigt sein sowie zeitnah auf Malware untersucht werden. Der Auftragnehmer ist verpflichtet, die Durchsetzung einer angemessenen internen Sicherheitsrichtlinie für diese Dienstleistung nachzuweisen.

2.3.3 Funktechnologien: Bedarf und Sicherheitsanforderungen

ISO/IEC 27002:2013: 10.1.1, 13.1.1, 13.1.2, 14.1.1
ISO/IEC TR 27019:2013: 12.1.1

Der Einsatz von WLAN, Bluetooth und anderen drahtlosen Übertragungstechniken ist bei Systemen mit hohem oder sehr hohem Schutzbedarf generell verboten. Ein Einsatz ist nur nach Analyse der damit verbundenen Risiken und unter Beachtung der nachfolgend beschriebenen Mindestsicherungsmaßnahmen in Abstimmung mit dem Auftraggeber und nach Genehmigung zulässig:

- WLANs dürfen nur in dezidierten und durch Firewalls und Applikations-Proxies abgetrennten Netzwerk-Segmenten betrieben werden.
- Drahtlose Übertragungstechnik muss nach dem Stand der Technik abgesichert werden.
- Neue WLANs sind so einzurichten, dass bestehende WLANs nicht gestört oder beeinträchtigt werden.

2.3.3 Wireless Technologies: Assessment and Security Requirements

ISO/IEC 27002:2013: 10.1.1, 13.1.1, 13.1.2, 14.1.1
ISO/IEC TR 27019:2013: 12.1.1

Wireless technology like WLAN and Bluetooth shall not be used for systems with high or very high protection level requirements. In consultation with the customer WLAN technology may be deployed after a risk analysis has been performed and if the following essential security requirements are complied with:

- Wireless LANs shall only be deployed in separate networks zones, which are segregated from other networks by firewalls and application level proxies.
- Wireless technology shall be secured according to state-of-the-art practice.
- Novel WLANs shall not interfere with existing wireless networks.

2.4 Bereich Anwendung

2.4.1 Benutzerverwaltung

2.4.1.1 Rollenkonzepte

ISO/IEC 27002:2013: 6.1.2, 9.2.1, 9.2.3, 9.2.6, 9.4.1

Das System muss über ein Benutzerkonzept verfügen, in dem mindestens folgende Benutzerrollen vorgesehen sind:

- Administrator: Benutzer, der das System installiert, wartet und betreut. Der Administrator hat deshalb u. a. die Berechtigung zur Änderung der Sicherheits- und Systemkonfigura-tion.
- Auditor: Benutzerrolle, die ausschließlich die Berechtigung zum Einsehen und Archivieren der Audit-Logs besitzt.
- Operator: Benutzer, der das System im Rahmen der vorgesehenen Nutzung bedient. Dies beinhaltet auch das Recht zur Änderung von betriebsrelevanten Einstellungen.
- Data-Display: Benutzer, der den Status des Systems abrufen und definierte Betriebsdaten lesen darf, aber nicht berechtigt ist, Änderungen durchzuführen.

Gegebenenfalls wird eine Benutzerrolle „Backup-Operator“ definiert, die Datensicherungen aller relevanten System- und Anwendungsdaten durchführen kann.

Das System muss eine granulare Zugriffskontrolle auf Daten und Ressourcen erlauben. Die Zugriffsrechte entsprechen einer sicheren Systemkonfiguration. Sicherheitsrelevante Systemeinstellungen und Konfigurationswerte können nur von der Ad-

2.4 Application

2.4.1 User Account Management

2.4.1.1 Role-Based Access Model

ISO/IEC 27002:2013: 6.1.2, 9.2.1, 9.2.3, 9.2.6, 9.4.1

The system shall utilise a role-based user model, in which at least the following user roles are defined:

- Administrator: A user, who installs, maintains and administrates the system. Therefore the administrator role has the authorisation and the according privileges to change the system and security configuration and settings.
- Auditor: User role which solely has the permission to inspect and archive the audit logs.
- Operator: User who performs regular system operations. This might include the privilege to change operational system settings.
- Data-Display: User, who is allowed to view the status of the system and to read defined datasets but is not allowed to make any changes to the system.

If applicable, a “Backup Operator” role is defined, which is allowed to backup relevant system and application data.

The system shall allow for a granular access control on data and resources. The default access permissions shall conform to a secure system configuration. Security relevant system configuration data can only be read or changed by the administrator role. For normal system use the operator or data-display role permissions shall

ministrator-Rolle gelesen und geändert werden. Zur normalen Systemnutzung sind nur Operator oder Data-Display Rechte notwendig. Benutzer-Accounts können einzeln deaktiviert werden, ohne sie vom System entfernen zu müssen.

2.4.1.2 Benutzer-Authentifizierung und Anmeldung

ISO/IEC 27002:2013: 9.3.1, 9.4.2, 9.2.1, 9.2.2, 9.4.3
ISO/IEC TR 27019:2013: 11.3.1, 11.5.2

a) Die Anwendung muss eine personenspezifische Identifizierung und Authentifizierung vornehmen, Gruppenaccounts werden von Auftraggeber nur in genau spezifizierten Ausnahmefällen erlaubt.

b) Ohne erfolgreiche Benutzer-Authentifizierung darf das System keinerlei Aktionen erlauben.

c) Das System muss Passwörter mit vom Auftraggeber definierbarer Stärke und Gültigkeitsdauer erzwingen.

d) Wo technisch möglich, wird eine starke 2-Faktor-Authentifizierung verwendet, z. B. durch die Verwendung von Tokens oder SmartCards.

e) Die zur Nutzeridentifizierung und Authentifizierung benötigten Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden. Die Anbindung an einen zentralen, prozessnetzinternen Directory Service sollte in Betracht gezogen werden.

f) Erfolgreiche und fehlgeschlagene Anmeldeversuche müssen zentral geloggt werden.

Die folgenden Punkte sind gegebenenfalls

be sufficient. Individual user accounts can be disabled without removing them from the system.

2.4.1.2 User Authentication and Log-On Process

ISO/IEC 27002:2013: 9.3.1, 9.4.2, 9.2.1, 9.2.2, 9.4.3
ISO/IEC TR 27019:2013: 11.3.1, 11.5.2

a) Users shall be identified and authenticated with personal accounts, group accounts shall only be used in precise defined exceptional cases.

b) Before allowing any actions the system shall require each user to be successfully authenticated.

c) The system shall force passwords with configurable strength and expiration periods. The password strength and expiration period shall be configurable by the customer.

d) If technically feasible, 2-factor authentication shall be used, for example SmartCards or security tokens.

e) Data used for user identification and authentication shall not solely be provided from sources external to the process network. Integration with a central, process net internal directory service should be considered.

f) Successful and failed log on attempts shall be logged centrally.

If applicable, the following items shall be implemented after paramount consideration of safe system operation and availabil-

unter vorrangiger Beachtung der Anforderungen an einen sicheren Anlagenbetrieb und von Verfügbarkeitsaspekten umzusetzen:

Das System soll Mechanismen implementieren, die eine sichere und nachvollziehbare Übergabe von Benutzer-Sessions im laufenden Betrieb ermöglichen.

Wo möglich und sinnvoll sollen Benutzer-Sessions nach einer definierbaren Inaktivitäts-Zeit gesperrt werden.

Bei einer Überschreitung einer konfigurierbaren Anzahl von fehlgeschlagenen Anmeldeversuchen soll eine Alarmmeldung ausgelöst und wenn möglich das Konto gesperrt werden.

ity issues:

The system should implement mechanisms which allow for a secure and reproducible switching of user session during system operations.

If applicable and technically feasible user sessions should be locked after a configurable time of inactivity.

After a configurable number of failed logon attempts a security event message should be logged and, if applicable, the account should be locked out

2.4.2 Autorisierung von Aktionen auf Benutzer- und Systemebene

ISO/IEC 27002:2013: 9.4.1, 9.4.4

Vor bestimmten sicherheitsrelevanten/-kritischen Aktionen muss die Autorisierung des anfordernden Benutzers bzw. der anfordernden Systemkomponente überprüft werden. Zu den relevanten Aktionen können auch das Auslesen von Prozess-Datenpunkten oder Konfigurationsparametern gehören.

2.4.2 Authorisation of Activities on User and System Level

ISO/IEC 27002:2013: 9.4.1, 9.4.4

Before certain security relevant or security critical activities are performed the system shall check the authorisation of the requesting user or system. Relevant activities may already be read access to process data or configuration parameters.

2.4.3 Anwendungsprotokolle

ISO/IEC 27002:2013: 13.1.2, 10.1.1
ISO/IEC TR 27019:2013: 10.6.3, 11.4.8

Es werden nur vom Auftraggeber freigegebene standardisierte Protokolle für Dienst- und Anwendungskommunikation benutzt. Ausnahmefälle bedürfen einer expliziten Genehmigung durch den Auftraggeber und sind zu dokumentieren. Es sind Protokolle

2.4.3 Application Protocols

ISO/IEC 27002:2013: 13.1.2, 10.1.1
ISO/IEC TR 27019:2013: 10.6.3, 11.4.8

Only standard application level protocols approved by the client shall be used. Exceptions shall be approved by the customer and documented. Protocols which protect the integrity of the transferred data and ensure correct authentication and au-

vorzuziehen, welche die Integrität der Kommunikation sowie die korrekte Authentifizierung und Autorisierung der Kommunikations-partner sicherstellen und die durch Timestamps oder sichere Sequenznummern ein Wiedereinspielen bereits gesendeter Nachrichten verhindern. Bei Bedarf sollte auch eine Verschlüsselung der Protokolldaten implementiert werden. Bei nicht standardkonformen bzw. selbst entwickelten oder proprietären Protokollen sind die genannten Punkte ebenfalls zu berücksichtigen.

thorisation of the communication partners should be preferred. Furthermore the used protocols should provide timestamps or secure sequence numbers to prevent re-injection of prior sent messages. If applicable, encryption of the protocol data should be implemented. The previous requirements also apply to non-standard, proprietary or in-house developed protocols.

2.4.4 Web-Applikationen

ISO/IEC 27002:2013: 14.2.5, 14.2.7

Neben allgemeinen Aspekten der sicheren Anwendungsprogrammierung sind bei Web-Applikationen besonders die folgenden Punkte zu berücksichtigen:

a) Die Applikation ist in verschiedene Module (z. B. Präsentations-, Anwendungs- und Datenschicht) zu trennen. Gegebenenfalls sind diese Module auf verschiedene Server zu verteilen.

b) Die verschiedenen Komponenten und Prozesse sind mit den minimal möglichen Rechten zu betreiben, sowohl auf Anwendungs- als auch auf Systemebene.

c) Sämtliche Parameter, die vom Anwender (bzw. seinem Web-Browser) an die Web-Anwendung gesendet werden sind genau auf Gültigkeit, maximale Länge sowie auf korrekten Typ und Wertebereich hin zu überprüfen. Dies gilt auch für Parameter, die von der Web-Anwendung selbst in einem vorhergehenden Schritt zum Anwender geschickt wurden. Dabei ist insbe-

2.4.4 Web Applications

ISO/IEC 27002:2013: 14.2.5, 14.2.7

Additional to common secure application programming practise, the following topics shall be regarded when web applications are being developed:

a) The application shall be separated into different modules (e. g. presentation, application and data layers). If applicable, the modules shall be deployed on different servers.

b) The web application components shall be configured with the minimal possible privileges, both on the application and the system level.

c) All parameters which are passed to the web application from the user or his web browser shall extensively be tested for validity, maximum length, correct type and range. This applies also to data which has been sent from the application to the user beforehand. Special attention shall be paid to so called XSS and data injection vulnerabilities, through which an attacker can

sondere auf sog. XSS- und Injection-Sicherheitslücken zu achten, über die ein Angreifer eigene Kommandos ausführen kann.

d) Es ist besonders auf sicheres Session-Management zu achten, z. B. durch verschlüsselte oder signierte Session-IDs und zeitbeschränkte Sessions. Die Übertragung von Session-IDs ist durch SSL-Verschlüsselung zu schützen.

e) Der Anwender soll zwar bei Fehlverhalten mit Fehlermeldungen informiert werden, dabei dürfen aber keine für einen Angreifer verwertbaren Informationen mitgeliefert werden. Solche Informationen dürfen ausschließlich in einem nur intern zugänglichen Logfile gespeichert werden.

f) Web-Anwendungen mit hohem Schutzbedarf sollten vor Inbetriebnahme einem Sicherheits-Audit unterzogen werden.

execute commands.

d) Especially, secure session management has to be taken into account, for example by using singed or encrypted session IDs and session timeouts. The transmission of session IDs shall be secured by encryption.

e) In the case of application errors the user should be informed by error messages. These error messages shall not provide detailed information which can be used by an attacker to plan further attacks. Such detailed error information shall only be logged to a log file, which is accessible by internal users only.

f) Web applications with a high protection requirement shall be tested by a security audit before going productive.

2.4.5 Integritätsprüfung relevanter Daten

ISO/IEC 27002:2013: 14.2.5

Die Integrität von Daten, die in sicherheitsrelevanten Aktionen verarbeitet werden, muss vor der Verarbeitung überprüft werden (beispielsweise auf Plausibilität, korrekte Syntax und Wertebereich).

2.4.5 Integrity Checks of Relevant Data

ISO/IEC 27002:2013: 14.2.5

The system shall check the integrity of data before this data is processed in security relevant activities, (e. g. check for plausibility, correct syntax and value ranges).

2.4.6 Protokollierung, Audit-Trails, Timestamps, Alarmkonzepte

ISO/IEC 27002:2013: 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3
ISO/IEC TR 27019:2013: 10.10.1, 10.10.6

a) Jedes System muss über eine einheitli-

2.4.6 Logging, Audit Trails, Timestamps, Alarm Concepts

ISO/IEC 27002:2013: 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3
ISO/IEC TR 27019:2013: 10.10.1, 10.10.6

a) All systems shall use a uniform system

che Systemzeit verfügen und die Möglichkeit zur Synchronisation dieser Systemzeit mit einer externen Zeitquelle bieten.

b) Das System muss Benutzeraktionen sowie sicherheitsrelevante Aktionen, Vorkommnisse und Fehler in einem zur nachträglichen und zentralen Auswertung geeignetem Format protokollieren. Es werden Datum und Uhrzeit, involvierte Benutzer und Systeme sowie das Ereignis und Ergebnis für einen konfigurierbaren Mindestzeitraum aufgezeichnet.

c) Das Logging von Events soll einfach konfigurierbar und modifizierbar sein.

d) Sicherheitsrelevante Events sollen in den Systemlogs als solche markiert werden, um eine automatische Auswertung zu erleichtern.

e) Die zentrale Speicherung der Logdateien erfolgt an einem frei konfigurierbarem Ort.

f) Ein Mechanismus zur automatisierten Übertragung des Logfiles auf zentrale Komponenten muss zur Verfügung stehen.

g) Das Logfile muss gegen spätere Modifikation geschützt sein.

h) Das Logfile darf nur von der Benutzerrolle Auditor archiviert werden können.

i) Bei Überlauf des Logfiles werden die älteren Einträge überschrieben, das System muss bei knapp werdendem Logging-Speicherplatz warnen.

j) Es muss möglich sein, sicherheitsrelevante Meldungen in ein vorhandenes Alarmmanagement aufzunehmen.

time which can be synchronised with an external time source.

b) The system shall log user actions and security relevant actions, events and errors to an audit trail using a format which is appropriate for later and central analysis. The system shall record date, time, involved users and systems, as well as the event and its result for a configurable time period.

c) The logging function shall be easy to configure and customise.

d) Security events shall be highlighted in the system logs to allow for an easy automatic analysis.

e) The central storage location of the log files shall be configurable.

f) A mechanism for automatic transfer of the log files to central component shall be available.

g) The log files shall be protected against later modification.

h) The audit log shall only be archivable by the auditor role.

i) The system shall overwrite the oldest stored audit records if the audit trail is full. The system shall issue a warning if the storage capacity decreases below a reasonable threshold.

j) Security relevant events shall be integrable into an existing alarm management.

2.4.7 Self-Test und System-Verhalten

ISO/IEC 27002:2013: 14.2.5

Das System bzw. die sicherheitsspezifischen Module sollen beim Start und in regelmäßigen Abständen interne Konsistenz-Prüfungen von sicherheitsrelevanten Einstellungen und Daten durchführen. Beim Versagen dieser Konsistenzprüfungen oder sicherheitsrelevanter Komponenten muss das System in einen Betriebszustand übergehen, der die primären Systemfunktionen aufrecht erhält, solange Gefährdungen oder Schäden für Anlagen und Personen ausgeschlossen sind.

2.4.7 Self-Test und System Behaviour

ISO/IEC 27002:2013: 14.2.5

The system or the security modules, respectively, should perform integrity checks of security relevant settings and data at start-up and in regular intervals. If the security modules or the integrity checks fails, the system shall fall back into a system state which maintains the primary system functions as long as the prevention of personal injury or equipment damage can be ensured.

2.5 Entwicklung, Test und Rollout

2.5.1 Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse

ISO/IEC 27002:2013: 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
ISO/IEC TR 27019:2013: 10.1.4

a) Das System muss beim Auftragnehmer von zuverlässigen und geschulten Mitarbeitern entwickelt werden. Falls die Entwicklung oder Teile davon an einen Subunternehmer ausgelagert werden sollen, bedarf dies der schriftlichen Zustimmung durch den Auftraggeber. An den Unterbeauftragten sind mindestens die gleichen Sicherheitsanforderungen zu stellen wie an den Auftragnehmer.

b) Der Auftragnehmer muss das System nach anerkannten Entwicklungsstandards und Qualitätsmanagement/-sicherungs-Prozessen entwickeln. Das Testen des Systems erfolgt nach dem 4-Augenprinzip: Entwicklung und Tests

2.5 Development, Test and Rollout

2.5.1 Secure Development Standards, Quality Management and Release Processes

ISO/IEC 27002:2013: 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
ISO/IEC TR 27019:2013: 10.1.4

a) On the contractor side, the system shall be developed by trained and trustworthy personnel. Outsourcing of the system development as a whole or in parts to third parties shall require the written approval of the customer. The third party shall at least comply with the same security requirements as the original contractor.

b) The system shall be developed according to well known development standards and quality management/assurance processes. Development and testing of the system shall be done by independent teams. Test plans, test concepts, expected and ac-

werden von verschiedenen Personen durchgeführt. Die Testpläne und –prozeduren, sowie erwartete und tatsächliche Testergebnisse müssen dokumentiert und nachvollziehbar sein, sie können vom Auftraggeber eingesehen werden.

c) Der Auftragnehmer muss über einen dokumentierten Entwicklungs-Sicherheitsprozess verfügen, der die physikalische, organisatorische und personelle Sicherheit abdeckt und die Integrität und Vertraulichkeit des Systems schützt. Die Effektivität des o.g. Prozesses kann durch ein externes Audit überprüft werden.

d) Der Auftragnehmer muss über eine Programmierrichtlinie verfügen, in der auf sicherheitsrelevante Anforderungen explizit eingegangen wird: So sind z. B. unsichere Programmiertechniken und Funktionen zu vermeiden. Eingabedaten müssen verifiziert werden, um z. B. Pufferüberlauf-Fehler zu verhindern. Wo möglich, werden sicherheitserhöhende Compileroptionen und Bibliotheken benutzt.

e) Die Freigabe des Systems bzw. von Updates/Sicherheitspatches muss anhand eines spezifizierten und dokumentierten Freigabe-Prozesses stattfinden.

tual test results shall be documented in a comprehensible way, they shall be available for inspection by the customer.

c) The contractor shall have a documented development security program that covers the physical, procedural and personnel security measures to protect the integrity and confidentiality of the system's design and implementation. The contractor shall be available for an external audit of the effectiveness of the security program.

d) The contractor shall have a programming guideline which covers security requirements and secure programming practice. The guideline should deprecate insecure programming style and the use of insecure functions. Data input shall be verified to avoid buffer overflows. If applicable, security enhancing compiler options and libraries shall be used.

e) System release and the release of updates and security patches shall be managed and controlled through a well-defined and documented release process.

2.5.2 Sichere Datenhaltung und Übertragung

ISO/IEC 27002:2013: 13.2.4, 13.2.2, 8.3.3, 13.2.3, 6.2.1, 10.1.1, 14.3.1

Sensible Daten des Auftraggebers, die im Entwicklungs- und Wartungsprozess benötigt werden oder anfallen, dürfen über ungeschützte Verbindungen nur verschlüsselt

2.5.2 Secure Data Storage and Transmission

ISO/IEC 27002:2013: 13.2.4, 13.2.2, 8.3.3, 13.2.3, 6.2.1, 10.1.1, 14.3.1

Sensitive customer data, which is used or produced during development and maintenance, shall be transmitted encrypted if it is sent over public networks. If the data is

übertragen werden. Gegebenenfalls, z. B. bei der Nutzung auf mobilen Systemen, dürfen solche Daten auch nur verschlüsselt gespeichert werden. Das betrifft z. B. interne Informationen und Dokumente des Auftraggebers, aber auch Protokolldateien, Fehleranalysen und relevante Systemdokumentation. Die Menge und die Dauer der Aufbewahrung der gespeicherten Daten muss auf das notwendige Minimum beschränkt sein.

stored on mobile devices it shall be stored in encrypted form. Sensitive data may include, but is not limited to, internal customer information and documents, log files, error logs, and relevant system documentation. The amount of stored data and the storage time shall be limited to the necessary minimum.

2.5.3 Sichere Entwicklungs-, Test- und Staging-Systeme, Integritäts-Prüfung

ISO/IEC 27002:2013: 12.1.4, 14.3.1, 9.4.5, 14.2.7
ISO/IEC TR 27019:2013: 10.1.4

a) Die Entwicklung muss auf sicheren Systemen erfolgen, die Entwicklungsumgebung, Quellcode und Binärdateien sind gegen fremde Zugriffe zu sichern.

b) Entwicklung und Test des Systems sowie von Updates, Erweiterungen und Sicherheitspatches muss in einer vom Produktivsystem getrennten Staging-Umgebung erfolgen.

c) Auf Produktiv-Systemen darf kein Quellcode gespeichert werden.

d) Es muss möglich sein, die Integrität von Quellcode und Binärdateien auf unerlaubte Veränderungen hin zu überprüfen, beispielsweise durch gesicherte Prüfsummen.

e) Es ist eine Versionshistorie für alle eingesetzte Software zu führen, die es ermöglicht die durchgeführten Softwareänderungen nachzuvollziehen.

2.5.3 Secure Development, Test– and Staging Systems, Integrity Checks

ISO/IEC 27002:2013: 12.1.4, 14.3.1, 9.4.5, 14.2.7
ISO/IEC TR 27019:2013: 10.1.4

a) Development shall be conducted on secure computer systems, the development environment, the source code and binaries shall be protected against unauthorised access.

b) Development and testing of the system and of updates, enhancements and security patches shall be conducted on staging environments which shall be separated from the live system.

c) No source code shall be installed on live systems.

d) It shall be possible to verify the integrity of the system source code and binaries to detect unauthorised changes. For example, the integrity might be checked by secure check sums.

e) A version history of all deployed software packages shall be maintained, which allows to trace all software changes.

2.5.4 Sichere Update- und Wartungsprozesse

ISO/IEC 27002:2013: 12.5.1, 14.2.2, 14.2.3, 14.2.7, 14.2.9
ISO/IEC TR 27019:2013: 12.4.1

a) Bereitstellung und Installation von Updates, Erweiterungen und Patches muss nach einem definierten Prozess und nach Rücksprache mit dem Auftraggeber erfolgen.

b) Von Seiten des Auftragnehmers muss die Wartung durch einen definierten, geschulten Personenkreis und von speziell gesicherten Systemen aus erfolgen.

2.5.4 Secure Update and Maintenance Processes

ISO/IEC 27002:2013: 12.5.1, 14.2.2, 14.2.3, 14.2.7, 14.2.9
ISO/IEC TR 27019:2013: 12.4.1

a) Provision and Installation of updates, enhancements and patches shall be carried out in consultation with the customer according to a well-defined process.

b) On the contractor side, maintenance shall be carried out by dedicated and trained personnel, using particularly secured systems.

2.5.5 Konfigurations- und Change-Management, Rollbackmöglichkeiten

ISO/IEC 27002:2013: 12.1.2, 14.2.9, 12.5.1, 12.6.2, 14.2.2
ISO/IEC TR 27019:2013: 10.12.1, 12.4.1

a) Das System muss mit einem Konfigurations- und Changemanagement entwickelt und betrieben werden.

b) Das System muss ein Rollback auf eine festgelegte Anzahl von Konfigurationszuständen unterstützen.

2.5.5 Configuration and Change Management, Rollback

ISO/IEC 27002:2013: 12.1.2, 14.2.9, 12.5.1, 12.6.2, 14.2.2
ISO/IEC TR 27019:2013: 10.12.1, 12.4.1

a) The system shall be developed and maintained using a configuration and change management.

b) The system shall support rollback of a specified number of configuration changes.

2.5.6 Behandlung von Sicherheitslücken

ISO/IEC 27002:2013: 12.6.1, 16.1.2, 16.1.3

Der Auftragnehmer muss über einen dokumentierten Prozess verfügen, um Sicherheitslücken zu behandeln. Innerhalb dieses Prozesses soll es allen Beteiligten, aber auch Außenstehenden möglich sein, tatsächliche oder potentielle Sicherheitslü-

2.5.6 Fixing Security Vulnerabilities

ISO/IEC 27002:2013: 12.6.1, 16.1.2, 16.1.3

The contractor shall have a well-defined vulnerability management process to address security vulnerabilities. The process allows all involved and external parties to report actual or potential vulnerabilities.

cken zu melden. Außerdem muss sich der Auftragnehmer über aktuelle Sicherheitsprobleme, die das System oder Teilkomponenten betreffen könnten, zeitnah informieren. Der Prozess definiert, wie und in welchem Zeitrahmen eine bekanntgewordene Lücke überprüft, klassifiziert, gefixt und an alle System-Besitzer mit entsprechenden Maßnahmenempfehlungen weitergemeldet wird. Wenn dem Auftragnehmer eine Sicherheitslücke bekannt wird, muss er den Auftraggeber unter der Maßgabe der Vertraulichkeit zeitnah informieren, auch wenn noch kein Patch zur Behebung des Problems zur Verfügung steht.

Furthermore the contractor shall obtain up-to-date information about security problems and vulnerabilities which might affect the system or its components. The vulnerability management process shall define how a potential vulnerability is verified, classified, fixed and how recommend measurements are reported to all system owners. Furthermore the process shall define timelines for each step in the vulnerability management process. The contractor shall early inform the customer about known security vulnerabilities, even if there is no patch available. The customer shall treat this information confidentially.

2.5.7 Sourcecode-Hinterlegung

ISO/IEC 27002:2013: 14.2.7

Bei Bedarf ist die Hinterlegung des Quellcodes und der entsprechenden Dokumentation bei einem Treuhänder zu vereinbaren, um beispielsweise im Falle einer Insolvenz des Auftragnehmers sicherheitskritische Updates zu ermöglichen.

2.5.7 Source Code Escrow

ISO/IEC 27002:2013: 14.2.7

If applicable, a source code escrow agreement should be considered, to ensure security updates in case of failure of the contractor. The agreement should cover the system source code and the according source code documentation.

2.6 Datensicherung/-wiederherstellung und Notfallplanung

2.6 Backup, Recovery and Disaster Recovery

2.6.1 Backup: Konzept, Verfahren, Dokumentation, Tests

ISO/IEC 27002:2013: 12.1.1, 12.3.1
ISO/IEC TR 27019:2013: 10.1.1

Es müssen dokumentierte Verfahren zur Datensicherung und -wiederherstellung der einzelnen Anwendungen bzw. des Gesamtsystems und der jeweiligen Konfigurationen existieren. Die Konfigurationsparameter von dezentralen Komponenten müssen zentral gesichert werden

2.6.1 Backup: Concept, Method, Documentation, Test

ISO/IEC 27002:2013: 12.1.1, 12.3.1
ISO/IEC TR 27019:2013: 10.1.1

There are documented backup and recovery procedures which cover single applications and the entire system, respectively, together with the according configuration data. Configuration data of distributed systems can be saved in a central repository. The backup and recovery processes shall

können. Die Verfahren werden vom Auftraggeber regelmäßig einem Test unterzogen. Die Dokumentation und die Verfahren müssen bei relevanten System-Updates angepasst und erneut getestet werden. Das Datensicherungs-Verfahren soll eine Prüf-Operation gegen den aktuellen Datenstand ermöglichen und auch den Schutzbedarf der zu sichernden Daten berücksichtigen (z. B. durch Verwendung von Verschlüsselung).

be tested by the client regularly. Documentation and tests shall be adjusted after relevant system updates and the procedures shall be re-tested. The backup process should provide a verify operation and shall take into account the protection requirements of the backup data (e. g. by encrypting sensitive data).

2.6.2 Notfallkonzeption und Wiederanlaufplanung

ISO/IEC TR 27019:2013: 14.1.1, 14.2.1

Für relevante Notfall- und Krisenszenarien müssen vom Auftragnehmer dokumentierte Betriebskonzepte und getestete Wiederanlaufpläne (inklusive Angabe der Wiederherstellungszeiten) zur Verfügung gestellt werden. Die Dokumentation und Verfahren werden bei relevanten System-Updates angepasst und im Rahmen des Abnahmeverfahrens für Release-Wechsel erneut getestet.

2.6.2 Disaster Recovery

ISO/IEC TR 27019:2013: 14.1.1, 14.2.1

The contractor shall provide documented operational concepts and tested disaster recovery concepts and procedures for defined emergency and crisis scenarios. The recovery concepts shall include a specification of the recovery time objectives. The documentation and procedures are adjusted after relevant system updates and the procedures are re-tested during system release acceptance procedures.

3 Abkürzungsverzeichnis und Glossar

2-Faktor-Authentifizierung	Authentifizierung unter Verwendung zweier verschiedener Authentifizierungsmechanismen, z. B. Password und Chipkarte
ACL	Access Control List
AG	Auftraggeber
AN	Auftragnehmer
AV	Antivirus
Applikation	Anwendungsprogramm
Applikations-Proxy	Proxy-System, das den Datenverkehr auf Ebene der Anwendungsprotokolle überprüft und filtert
Authentifizierung	Vorgang zur Überprüfung der Identität einer Person oder einer Systemkomponente
Basissystem	Betriebsystem inklusive Grundkomponenten wie X11 oder Netzwerkdienste und entsprechender Libraries
Benutzerrolle	Gruppe von Benutzern, denen aufgrund der auszuübenden Aufgabe(n) bestimmte Rechte zugewiesen werden. Ein Benutzer kann Mitglied mehrerer Rollen sein.
Changemanagement	Managementprozess, mit dem das Testen, Anwenden und Dokumentieren von Hard- und Softwareupdates und Konfigurationsänderungen gesteuert und verwaltet wird
DBMS	Database Managementsystem
DL	Dienstleister
DMZ	Demilitarized Zone, isolierte Netzwerkzone zwischen zwei getrennten Datennetzen, in der die Netzwerk-Sicherheitssysteme angesiedelt sind, die die Kommunikation zwischen den beiden Netzen vermitteln
DoS-Angriff	Denial of Service**,** Angriff auf einen System oder eine Systemkomponente mit der Absicht, das Angriffsziel arbeitsunfähig zu machen, z. B. durch Beanspruchung der gesamten verfügbaren Rechenleistung oder Netzwerkkapazität
EnWG	Energiewirtschaftsgesetz

Fail-Safe	Konstruktionsprinzip, bei dem sicherheitsrelevante Aspekte so konzipiert sind, dass bei Versagen oder Ausfall der kleinstmögliche Schaden bzw. Gefahr für Personen oder die Anlage entsteht
Fail-Secure	Konstruktionsprinzip, bei dem sicherheitsrelevante Aspekte so konzipiert sind, dass bei Versagen oder Ausfall die Vertraulichkeit und Integrität des Systems garantiert sind
Gesamtsystem	Im vorliegenden Text alle vom Hersteller gelieferten Hard- und Software-Komponenten, z. B. Applikationen, Betriebsysteme, Rechnersysteme und die Netzwerk-Infrastruktur
HW	Hardware
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
ISO/IEC 27002	ISO/IEC-Standard für Informationssicherheit
IT	Informationstechnologie
LAN	Local Area Network
MPLS	MultiProtocol Label Switching
Netzwerk-Perimeter	Netzwerksystem, das den Übergang zu einem externen Netzwerk bildet, z. B. ein Router, eine Firewall oder ein RAS-System
Out-Of-Band	Kontrolle über die Server, selbst bei Netzwerkausfall Sicherer Fernzugriff auf die Server Zugriff via serielle Schnittstelle oder direkte Steuerung der Eingabegeräte Grundsätzlich kann jederzeit die Netzwerkschnittstelle eines Servers oder gar das ganze Netzwerk ausfallen. Somit hat der Administrator keine Chance mehr den Server "In Band" (über Ethernet) zu erreichen und der Fehler muss vor Ort am Terminal behoben werden.
OPC	**„**Openness, Productivity, Collaboration“ (ursprünglich: „OLE for Process Control“), in der Automatisierungstechnik häufig benutzte Software-Schnittstelle, auf DCOM basierend
Patchmanagement	Managementprozess, mit dem das Testen, Installieren, Verteilen und Dokumentieren von Sicherheitspatches und Software-Updates gesteuert und verwaltet wird

PKI	Public Key Infrastructure
Proxy	Computersystem, das den Datenverkehr zwischen zwei getrennten Datennetzen vermittelt und ggf. auch überwacht und filtert
QA	Quality-Assurance, Qualitätssicherung
QM	Qualitätsmanagement
QoS	Quality of Service
RAS	Remote Access Service
Rolle	siehe Benutzerrolle
rsh	Unix remote shell
SNMP	Simple Network Management Protocol
SSH	Secure Shell Protocol, verschlüsseltes Terminalprotokoll
SSL	Secure Socket Layer
Stresstest	Test, bei dem das Verhalten einer Soft- oder Hardwarekomponente unter hoher Last bzw. bei Verarbeitung von außerhalb der Spezifikation liegenden Daten überprüft wird
System	siehe Gesamtsystem
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network, Methode um auf einem physikalischen Netzwerk verschiedene logische Netze einzurichten
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
XSS	Cross Site Scripting

3 Glossary, List of Abbreviations

2-factor authentication	authentication using two different authentication factors, e. g. a password together with a token
ACL	access control list
Application proxy	a proxy system which verifies and filters network traffic at the application protocol layer
Authentication	the process used to verify the identity of a person or a system component
Base system	operating system and base components like X11 and network services with the according system libraries
Change management	process to manage and control the test, application and documentation of hard- and software changes
DMZ	demilitarized zone, isolated security zone between to separated networks.
DoS attack	denial of service attack. Attack intended to make a resource unavailable to legitimate users, e. g. through consumption of all available CPU time or network bandwith
Fail safe	construction principle which ensures that a system failure causes the lowest possible damage or risk to humans or the system
Fail secure	construction principle, which ensures that in case of a failure the system's integrity and confidentiality are still guaranteed
IEC	International Electrotechnical Commission
IP	internet protocol
ISO	International Organization for Standardization
ISO/IEC 27002	ISO/IEC standard for information security
IT	information technology
LAN	local area network
MPLS	multi protocol label switching
Network perimeter	network component which acts as an interface to an external network, e. g. a router, a firewall or RAS system

Out-of-Band	Access to the servers even in the case of network failures Secure remote access on the servers Access via serial interface or direct control of the input devices The network interface of a server or even the whole network can fail any time. In this case the administrator can no longer reach the server "in band" (using the Ethernet connection) and the problem must be solved at the local console
OPC	„Openness, Productivity, Collaboration“ (also: „OLE for Process Control“), software interface often found in industrial automation systems, based on DCOM technology
Patch management	process to manage and control the test, application, distribution and documentation of security patches and software updates
PKI	public key infrastructure
Proxy	computer system which mediates, monitors and filters the network traffic between separated networks
QA	quality assurance
QM	quality management
QoS	quality of service
RAM	random access memory
RAS	remote access service
Role	see “User role”
SNMP	simple network management protocol
SSH	secure shell protocol, encrypted terminal protocol
SSL	secure socket layer
Stress test	test to examine the behaviour of a hard- or software component under high load or while processing malformed data
System	in this white paper all hard- and software components provided by the contractor, e. g. applications, operating systems, computer systems and network infrastructure
TCP	transport control protocol
TLS	transport layer security
UDP	user datagram protocol
USB	universal serial bus

User role	group of users who are assigned permissions according to the operations they need to perform
VLAN	virtual local area network, method to set up multiple logical networks in one physical network
VPN	virtual private network
WAN	wide area network
WLAN	wireless LAN
XSS	cross site scripting

Ansprechpartner / Contact Person

Arne Rajchowski

Telefon: +49 30 300199-1526

arne.rajchowski@bdew.de