oesterreichs energie.

bdew
Energie. Wasser. Leben.

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

Oesterreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Ausführungshinweise zur Anwendung des Whitepaper

Überarbeitete Version 1.1 11/2014:
Angepasste Referenzen auf ISO/IEC 27002:2013 und ISO/IEC TR 27019:2013

Wien/Berlin, 17. November 2014

Änderungshistorie

Version	Datum	Bemerkungen (Bearbeiter)
1.0 Final	Dezember 2011	Projektteam Oesterreichs Energie / BDEW
1.1 Final	November 2014	Anpassung Norm-Referenzen auf ISO/IEC 27002:2013 und ISO/IEC TR 27019:2013

Gemeinsame Herausgeber:

Oesterreichs E-Wirtschaft

Brahmsplatz 3, 1040 Wien, Österreich

BDEW Bundesverband für Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32, 10117 Berlin, Deutschland

Ansprechpartner:

Armin Selhofer (Österreichs E-Wirtschaft)

Erwin Bosin (TIWAG-Netz AG)

Arne Rajchowski (BDEW Bundesverband für Energie- und Wasserwirtschaft e.V.)

Rolf-Dieter Kasper (RWE Deutschland AG)

Fachliche Unterstützung:

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

Inhalt

1 Vorwort

1.1 Einleitung

Vom deutschen BDEW Bundesverband für Energie- und Wasserwirtschaft wurde im Jahre 2008 mit dem Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ ein Dokument mit grundsätzlichen Sicherheitsmaßnahmen für Steuerungs- und Telekommunikationssysteme für die Prozesssteuerung in der Energieversorgung entwickelt. Ziel dieses BDEW-Whitepapers ist es, die Systeme bereits in der Standardkonfiguration gegen Sicherheitsbedrohungen im täglichen Betrieb angemessen zu schützen.

Auf Basis des Whitepapers wurde von *Oesterreichs Energie* und BDEW gemeinsam das vorliegende Best-Practice-Papier mit Ausführungshinweisen zur Anwendung des Whitepapers erarbeitet. Ziel dieser Ausführungshinweise ist es, zu den einzelnen Anforderungen des BDEW-Whitepapers Umsetzungsbeispiele und Anwendungshinweise für die unterschiedlichen Technologiebereiche im Bereich der Prozesssteuerung in der Energieversorgung zu geben. Insbesondere fließen dabei auch die bisherigen praktischen Erfahrungen vieler Projekte und die Ergebnisse der Diskussionen mit den Herstellern der Systeme ein. Die vorliegenden Ausführungshinweise dienen dabei als Ergänzung zu den Anforderungen des BDEW-Whitepapers, welches seine Gültigkeit unverändert beibehält.

Die Umsetzung einzelner Sicherheitsanforderungen verursacht gegebenenfalls einen nicht zu vernachlässigenden Mehraufwand. Diese Mehraufwendungen zur Sicherstellung eines zuverlässigen, effektiven und sicheren Systembetriebs müssen bereits in der Planung Berücksichtigung finden. Dies betrifft sowohl funktionstechnische Erweiterungen, die aus Sicherheitsgründen notwendig werden, als auch organisatorische Mehraufwendungen auf Seiten des Betreibers oder Dienstleisters.

Das BDEW-Whitepaper und diese Ausführungshinweise definieren grundlegende Anforderungen für Systeme, Anwendungen und Komponenten und die zugehörigen Wartungs- und Serviceprozesse. Ebenso wichtig sind organisatorische Sicherheitsmaßnahmen im Unternehmen, wie der Aufbau einer Sicherheitsorganisation oder die Schaffung eines umfassenden Sicherheitsbewusstseins bei den Mitarbeitern (Security Awareness). Diese organisatorischen Anforderungen stehen nicht im Fokus des BDEW-Whitepapers und dieser Ausführungshinweise, hierzu sei insbesondere auf die ISO/IEC 27001 und die ergänzenden, branchen-spezifischen Normen verwiesen (vgl. Anhang 0).

1.2 Gliederung und Aufbau

Die Umsetzungshinweise sind entsprechend den Anforderungskapiteln des BDEW-Whitepapers gegliedert. Zu Beginn jedes Anforderungskapitels wird zunächst die zugehörige Whitepaper-Anforderung zitiert.

In der folgenden Tabelle werden dann im Abschnitt „Ergänzungen und Anmerkungen“ allgemeingültige Hinweise gegeben, die alle Technologiebereiche im Bereich der Prozesssteuerung in der Energieversorgung betreffen.

Anschließend werden für die drei im EVU-Prozessumfeld anzutreffenden Haupttechnologiebereiche „Betriebsführungs-/Leitsysteme und Systembetrieb“, „Übertragungstechnik/Sprachkommunikation“ und „Sekundär, Automatisierungs- und Fernwirktechnik“ spezifische Ausführungshinweise aufgeführt. Dabei wird für die drei Bereiche die folgende Kategorisierung angewendet:

Technologie-kategorie	**Beschreibung und Beispiele**
Betriebsführungs- / Leitsysteme und Systembetrieb:	Alle zentralisierten Systeme, die der Prozessteuerung und -überwachung sowie der Betriebsführung im Bereich der Prozesssteuerung dienen, sowie die hierzu notwendigen unterstützenden zentralen IT-Systeme, Anwendungen und die zugehörige zentrale Infrastruktur. Beispiele: • Zentrale Netzleit- und Netzführungssysteme • Systeme zur Überwachung und Steuerung von Erzeugern, z.B. Kraftwerksleitstände, zentrale Leitsysteme von dezentralen Wasserkraftwerken oder Windenergieanlagen • Systeme zur Störungsannahme und zur Einsatzplanung • Zentrale Zähler-und Messwerterfassungssysteme • Datenarchivierungssysteme • Zentrale Parametrier-, Konfigurations- und Programmiersysteme • die für den Betrieb der o.g. Systeme notwendigen unterstützenden Systeme, wie z.B. Programmier- und Parametriergeräte
Übertragungs-technik / Sprach-kommunikation:	Die in der Prozesstechnik zur Sprach- und Datenkommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik. Beispiele: • Router, Switches und Firewalls • Übertragungstechnische Netzelemente • Endgeräte der Sprachkommunikation • Telefonanlagen und VoIP-Systeme und zugehörige Server • Digitale Funksysteme

	• Zentrale Management- und Überwachungssysteme der Übertragungs-, Telekommunikations- und Netzwerktechnik
Sekundär-, Automatisierungs- und Fernwirktechnik:	Die prozessnahe Steuerungs- und Automatisierungstechnik sowie die zugehörigen Schutz- und Safetysysteme und fernwirktechnische Komponenten. Hierzu gehören insbesondere die Technik in den dezentralen Stationen sowie die Automatisierungstechnik in Erzeugungs- und Speicheranlagen. Beispiele: • Steuerungs- und Automatisierungskomponenten • Leit- und Feldgeräte • Controller und SPSen inklusive digitaler Sensor- und Aktorelemente • Schutzgeräte und Safetykomponenten • Fernwirkgeräte • Digitale Mess- und Zählvorrichtungen

Dort, wo die Anforderungen insbesondere auch auf organisatorischer Ebene berücksichtigt werden müssen, ist dies im Abschnitt „Organisatorische Anmerkungen“ vermerkt.

1.3 Anwendungshinweise

1.3.1 Systemplanung und Ausschreibung

Die vorliegenden Ausführungshinweise richten sich sowohl an Hersteller, Systemintegratoren und externe Planer auf Auftragnehmerseite als auch an unternehmensinterne Planer, Realisierer und Betreiber auf der Auftraggeberseite.

Beim Auftragnehmer sind die Ausführungshinweise bereits für die Produkt- und Systementwicklung hilfreich und sollten deshalb entsprechend frühzeitig berücksichtigt werden. Dies betrifft insbesondere auch die Weiterentwicklung von Systemen und Produkten.

Auf der Auftraggeberseite wird weiterhin die im BDEW-Whitepaper vorgesehene Vorgehensweise empfohlen, nachdem in der Planungsphase eine frühzeitige Schutzbedarfsfeststellung und ggf. eine ergänzende individuelle Risikoanalyse durchgeführt werden sollte (vgl. hierzu Seite 3 im BDEW-Whitepaper „Planung eines Steuerungs- oder Kommunikationssystems“). Aufbauend auf den Ergebnissen der Schutzbedarfsfeststellung und der Risikoanalyse ist dann für das geplante System detailliert zu spezifizieren, wie die einzelnen BDEW-Anforderungen erfüllt werden sollen. Insbesondere in dieser Phase sollen die vorliegenden Umsetzungshinweise unterstützend wirken.

Ist das geplante Projekt zur Ausschreibung vorgesehen, werden nach Ende der planerischen Phase die ermittelten Sicherheitsanforderungen in das Lastenheft integriert. In der Ausschrei-

bung sollten dann eine Kopie des BDEW-Whitepapers, konkretisierte Anforderungen und zusätzliche Maßnahmen sowie Umsetzungsvorgaben sowie die zulässigen Abweichungen und Ausnahmen definiert werden. Von den Anbietern ist im Angebot detailliert Stellung zur Umsetzung der technischen und organisatorischen Anforderungen zu nehmen und dort ggf. notwendige Abweichungen und Alternativvorschläge zu dokumentieren. Diese müssen seitens des Ausschreibenden bewertet und bei der Zuschlagserteilung berücksichtigt werden (vgl. hierzu S. 3 im BDEW-Whitepaper „Berücksichtigung des Whitepapers bei Ausschreibungen"). Die Nicht-Anwendung von Maßnahmen ist durch die Planer, Realisierer bzw. Betreiber im Rahmen einer Risikoanalyse zu bewerten und auf der Auftraggeberseite zu begründen und zu dokumentieren.

1.3.2 Anwendung für Bestandssysteme

Die im BDEW-Whitepaper und diesen Ausführungshinweisen beschriebenen Sicherheitsmaßnahmen werden für alle neuen Steuerungs- oder Telekommunikationssysteme empfohlen. Eine Anwendung für Bestandssysteme ist auf Grund technologischer Beschränkungen häufig nur mit Einschränkungen möglich. Insbesondere bei Upgrades oder Erweiterungen sollten aber im Rahmen einer Risikoanalyse alle Umsetzungsoptionen geprüft und bewertet und ggf. ergänzende Sicherheitsmaßnahmen eingeplant werden.

1.3.3 Wartung und Service

Die Sicherheitsbetrachtung ist nicht nur auf die Planungsphase/Projektumsetzung begrenzt, sie hat auch Auswirkungen auf den gesamten Lebenszyklus der Systeme. Dies betrifft insbesondere die Wartung sowie die kontinuierliche Weiterentwicklung und Fehlerkorrekturen.
Mit den Systemlieferanten bzw. entsprechenden Dienstleistern müssen deshalb zum Zeitpunkt der Ausschreibung bzw. zur Projektumsetzung Vorgehensweisen vereinbart werden, die die relevanten Details zu Wartungsprozessen und sicherheitsspezifischen Dienstleistungen wie dem Patchmanagement, Schadsoftwareschutz oder Systemupgrades und Migrationen regeln.

Für die Wartungsdienstleistungen sind insbesondere auch spezifische Sicherheitsanforderungen für die zur Wartung genutzten (ggf. auch auf Seiten des Dienstleisters betriebenen) IT-Komponenten zu definieren. Zur Überprüfung der korrekten Umsetzung der Anforderungen sollte ein Auditrecht vereinbart werden.

1.3.4 Verwendung neuer Technologien

Die rasante Entwicklung und Anwendung neuer IT-Technologien aus der kaufmännischen und kommerziellen IT hält immer schneller Einzug in den Bereich der Prozesstechnik. Alle diese neuen und vielversprechenden Technologien können Kosteneinsparungen und zu Verbesserungen der Funktionalität führen. Allerdings müssen vor dem Einsatz neuer Technologien relevante Informationssicherheits-Aspekte hinreichend berücksichtigt werden.

Hierbei sollten verschiedene Themenpunkte betrachtet werden

- Berücksichtigung bekannter Sicherheitslücken und Schwachstellen

- Sicherstellung von Zuverlässigkeit und Stabilität im betrieblichen Einsatz
- Klärung der Komplexität im Sinne einer raschen Wiederherstellung des Normalbetriebes
- Erfüllung der Vorgaben für den Echtzeitbetrieb
- Erfüllung der Erfordernisse im Sinne der Kritischen Infrastruktur
- Prüfen der Verfügbarkeit über den Lebenszyklus der Systeme

2 Umsetzungshinweise zu den BDEW-Sicherheitsanforderungen

2.1 Allgemeines/Organisation

2.1.1 Allgemeines

2.1.1.1 Sichere Systemarchitektur

Sicherheits-anforderungen	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).

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ☑
Ergänzungen und Anmerkungen:	Sicherheitsanforderung 2.1.1.1 richtet sich in erster Linie an Systemdesigner und Entwickler und soll eine Leitlinie für das gesamte Systemdesign und den Entwicklungsprozess darstellen. Dies betrifft alle unten angeführten Systeme. Neben den genannten grundlegenden Sicherheitsprinzipien existieren weitere sinnvolle und ergänzende Designprinzipien, die ebenfalls berücksichtigt werden sollten, wie z.B. Access Control, Input Sanitation, Default Deny etc. Das Redundanzprinzip ist als allgemeines Designprinzip in Ergänzung des Defence-in-Depth-Prinzips zu verstehen und besagt, dass es beim Ausfall einzelner Systemkomponenten oder Sicherheitsfunktionen nicht zu einem Totalausfall des Systems bzw. der Sicherheitsme-			

	chanismen kommen darf. In Hinblick auf Sicherheitsfunktionen ist hier insbesondere eine logische Redundanz im Sinne des Defence-in-Depth-Prinzips gemeint, nachdem das Gesamtsystem über mehrere, gestaffelte Schutzfunktionen verfügen muss. Hieraus ist aber nicht zwingend abzuleiten, dass alle Komponenten im Sinne einer Hardware-Redundanz doppelt ausgelegt werden müssen. Beispiele für das Redundanz- und Defence-in-Depth-Prinzip: • Echtzeit-Schadsoftwareschutz auf den Systemkomponenten bei gleichzeitiger Prüfung aller Datenschnittstellen und Blockierung der nicht benötigten Datenträgerschnittstellen wie USB-Ports und Wechseldatenträgern • Konsistenzprüfung von Daten sowohl an der Außenschnittstelle einer Anwendung als auch bei der Übergabe zwischen den verschiedenen Systemmodulen innerhalb der Applikation • Redundante Übertragungswege • Überprüfung der Quelladressen (IP-Adressen) von Fernwirktelegrammen nicht nur an der Außenschnittstelle (Firewall) der Station, sondern auch durch die Zielkomponente • Fehlertolerante und unabhängige Implementierung von kritischen Funktionen der Anlagensicherheit Die Umsetzung der sicheren Systemarchitektur sollte in der High-Level-Systemdokumentation beschrieben werden.
Betriebsführungs-/ Leitsysteme und Systembetrieb:	-
Übertragungs-technik / Sprach-kommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:	**-**

2.1.1.2 Ansprechpartner

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ☑
Ergänzungen und Anmerkungen:	-			
Betriebsführungs-/ Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	-			
Organisatorische Anmerkungen:	Bei entsprechender Unternehmensgröße sollten die Aufgaben in den verschiedenen Bereichen und Projektphasen von mehreren Mitarbeitern wahrgenommen werden. Auf Projektebene sollte allerdings ein einzelner Verantwortlicher benannt werden, der dem Auftraggeber als primärer Ansprechpartner dient. Für den Fall der Abwesenheit sollte eine Vertretung vorgesehen werden.			

2.1.1.3 Patchfähigkeit, Patchmanagement

Sicherheits-anforderungen	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 geschehen.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ❑
Ergänzungen und Anmerkungen:	Unter Patchen wird das Implementieren von sicherheitsrelevanten und funktionalen Systemupdates verstanden. Dies umfasst sowohl die reine Fehlerbeseitigung als auch die Erweiterung, Ergänzung und Optimierung von Funktionalitäten und betrifft sowohl die Anwendungsebene als auch unterlagerte Systemkomponenten (z.B. Basis- und Betriebssysteme, Datenbanken, Programmbibliotheken und Komponenten von Drittherstellern, Firmware, usw.). Die Vorgehensweise zur Installation von Sicherheitspatches sowie für Deinstallation und Rollback sollten für alle Systemkomponenten unterstützt und detailliert dokumentiert werden. Werden keine Komplettsysteme geliefert, sollten vom Auftragnehmer die notwendigen Prozesse und Voraussetzungen zur Installation von Sicherheitspatches und sonstigen Updates für die im System genutzten Drittkomponenten genannt werden. Das System sollte so aufgebaut sein, dass die Anzahl der notwendigen Sicherheitspatches bzw. der zu patchenden Komponenten sowie ggf. notwendiger Betriebsunterbrechungen auf das Minimum reduziert werden kann. Eine umfassende Härtung kann hierbei unterstützend wirken (vgl. 2.2.1).Grundsätzlich ist anzustreben, sämtliche Systeme und Komponenten patchfähig auszuführen. Insbesondere übergeordnete Systeme ohne direkte Prozess-Anbindung sollten dabei so aus-			

		geführt werden, dass eine (primärtechnische) Außerbetriebnahme der Anlage zur Installation i.d.R. nicht notwendig ist. Erfordert das System nach einem Update die Durchführung von Funktionstests, sollten diese soweit wie möglich automatisiert werden und die hierfür notwendigen Mechanismen im System vorgesehen sein. Der Auftragnehmer sollte die notwendigen Testfälle und die bei einem erfolgreichen Testdurchlauf zu erwartenden Ergebnisse dokumentieren. Fallback- bzw. Rollbackfunktionen für den Fall von fehlerhaften Patches oder bei fehlgeschlagenen Tests sollten so konzipiert sein, dass eine rasche und möglichst einfache Rückkehr auf den letzten funktionsfähigen Versions- und Konfigurationsstand möglich ist. Im Patchmanagement sind auch die Parametrier- und Managementsysteme zu berücksichtigen. Die Patches sollten durch den Hersteller eindeutig versioniert werden und mit Integritätsprüfungsmechanismen versehen sein. Vergleiche auch 2.5.4.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Grundsätzlich sollten sämtliche Systeme patchfähig ausgeführt sein. Wo möglich sollten zur Sicherstellung eines kontinuierlichen Betriebs Redundanzkomponenten genutzt werden.
	Übertragungstechnik / Sprachkommunikation:	Berücksichtigt werden sollten sowohl Netzwerkkomponenten und Netzelemente, Endgeräte und zentrale Management- und Überwachungssysteme.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	Übergeordnete Systeme ohne direkte Prozess-Anbindung sollten so ausgeführt werden, dass im Regelfall eine primärtechnische Außerbetriebnahme der Station bzw. Anlage zur Patchinstallation nicht notwendig ist. Die Installation von Sicherheits- und Firmwareupdates in prozessnahen Komponenten (z.B. Steuerungen, SPSen, Feldeinheiten, Schutzgeräten) ist unter Umständen nur während eines Anlagenaußerbetriebnahme, wie z.B. während einer Revision, möglich. Diese Komponenten sollten möglichst so ausgeführt sein, dass dann ein Patchen vor Ort und ohne Ausbau der Komponenten durchführbar ist und nur einen möglichst geringen Prüfaufwand erfordert. Falls für die prozessnahen Komponenten stark erhöhte Verfügbarkeitsanforderungen bestehen und eine Außerbetriebnahme für Software/Firmware-Änderungen nicht möglich ist, sollte für diese Komponenten die Notwendigkeit der Implementierung einer Patchfähigkeit im laufenden Betrieb geprüft werden. In der Regel wird dies eine redundante Ausführung der betroffenen Komponenten erfordern.
Organisatorische Anmerkungen:		Die im Rahmen des Patchmanagements durchgeführten Prozesse sollten sich an anerkannten Betriebs- und Servicemanagement-Standards orientieren (z.B. COBIT, ITIL etc.) In der Regel sind für das Patchmanagement Administrationswerkzeuge und Systeme zum System- und Versionsmanagement notwendig

	(z.B. zentrale Updateserver, Versionierungs- und Konfigurationsmanagement-Datenbanken etc.).

2.1.1.4 Bereitstellung von Sicherheitspatches für alle Systemkomponenten

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:** **Ja ☑**	**Projektplanung / -umsetzung:** **Ja ☑**	**Produkt- / Systemservice:** **Ja ☑**	**Systembetrieb:** **Ja ☑**
Ergänzungen und Anmerkungen:	Die Installation von Sicherheitspatches und Updates erfordert i.d.R. eine individuelle Prüfung und Freigabe der einzelnen Patches und Updates durch den Systemhersteller. Für weniger kritische Anwendungen ist ggf. eine generische Freigabe bestimmter Patch- und Updatekategorien durch den Systemhersteller möglich. Ist eine Prüfung und Freigabe notwendig, sollte sich der Auftragnehmer für alle im System genutzten Komponenten und Softwareprodukten Dritter selbsttätig über vorliegende Sicherheitsupdates informieren und eine komponenten- bzw. anlagenspezifische Relevanzbewertung vornehmen. Informationen über zu installierende Updates sollten dem Auftraggeber regelmäßig und zeitnah zur Verfügung gestellt werden. Für die Freigabeprozesse sollten die folgenden Aspekte beachtet werden: • Der Auftragnehmer sollte alle relevanten Sicherheitspatches beziehen und den notwendigen Freigabe- und Qualifizierungstests unterziehen. • Informationen über freigegebene Sicherheitspatches sollten dem Auftraggeber zeitnah nach deren Veröffentlichung zur Verfügung gestellt werden, z.B. per E-Mail, über eine Webseite oder ein Supportforum. • Wenn ein Sicherheitspatch im gegebenen Systemumfeld als nicht relevant eingestuft wird, sollte dies dokumentiert und dem Auftraggeber mitgeteilt werden. • Wird für einen Sicherheitspatch keine Freigabe durch den Auftragnehmer oder Auftraggeber erteilt, sollten Alternativmaßnahmen entwickelt werden. • Es sollte explizit dokumentiert werden, ob zur Anwendung eines Patches eine Betriebsunterbrechung notwendig ist, beispielsweise			

		auf Grund von Neustarts von Diensten oder Komponenten. Für viele Leittechniktypen und Anwendungsszenarien ist für das Gesamtsystem oder einzelne Teilkomponenten (z.B. Sekundär-/ Automatisierungstechnikkomponenten oder Fernwirktechnik) von einem längerfristigen Betriebszeitraum auszugehen, der den Lebenszyklus von einzelnen Softwareprodukten i.d.R. weit übertrifft. Für die Systemkomponenten, für die der angestrebte Betriebszeitraum des Gesamtsystems absehbar nicht erreichbar ist (z.B. typische PC-basierte Komponenten), sollte durch ein entsprechendes Systemdesign eine leichte Austauschbarkeit vorgesehen werden und ein Migrationskonzept grob skizziert und vertraglich festgeschrieben werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		Verbindliche Vereinbarungen zur Vorgehensweisen wie Überprüfung, Bereitstellung und Freigabe der Patches und Updates sowie zu Zeitrahmen und Fristen sollten vertraglich, z.B. im Rahmen eines Wartungsvertrags, berücksichtigt werden. Wo möglich, sollten hier auch schon absehbare Migrationsszenarien behandelt werden.

2.1.1.5 Support für eingesetzte Systemkomponenten

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ☑
Ergänzungen und Anmerkungen:	Betriebszeiträume, die den Lebenszyklus von System- oder Softwarekomponenten überschreiten, erhöhen das sicherheitstechnische Risiko und sollten daher unbedingt vermieden werden. Die Lieferanten sollten den entsprechenden Support auch für 3rd-Party-Produkte bieten und bei Produkten mit langen Lebenszyklen bei Vertragsabschluss Migrationskonzepte vorweisen können. Es sollten zunächst nur Drittkomponenten (z.B. Betriebssystem, Protokoll-Stacks, usw.) genutzt werden, die aktuell und während der geplanten Laufzeit noch unterstützt werden. Auf Grund der üblicherweise langfristigen Betriebszeiträume in den betrachteten Bereichen kann dies der Hersteller allerdings häufig nicht garantieren. Deshalb sollten hier dann Grobkonzepte und Kostenschätzungen für eine Migration auf neuere Versionen vorgelegt werden. Gegebenenfalls sollte zusätzlich gefordert werden, dass bei Inbetriebnahme möglichst die zu diesem Zeitpunkt aktuellen System- und Komponentenversionen eingesetzt werden, falls dem keine technischen Gründe entgegenstehen. Die angestrebten Betriebszeiträume einzelner Komponenten sollten vom Auftraggeber vorab definiert werden. Der Hersteller sollte im Rahmen der Projektdokumentation die System- und Komponentenversionen und die zugehörigen Supportzeiträume dokumentieren.				
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und	-			

Fernwirktechnik:	
Organisatorische Anmerkungen:	Die entsprechenden Anforderungen sind durch Auftraggeber und Auftragnehmer bereits bei Vertragsabschluss zu berücksichtigen. Eine besondere Herausforderung stellen die stark unterschiedlichen Lebenszeiten der genutzten Drittsoftwarekomponenten und des gewünschten Lebenszyklus‘ eines Leittechniksystems dar. Für die Migration der Systeme sollte ein Konzept erstellt werden. Falls der Auftraggeber in Ausschreibungen oder Projekten den Einsatz konkreter Produkte bzw. Versionen vorschreibt, ist die Umsetzung dieser Anforderung auf Auftraggeberseite entsprechend zu berücksichtigen.

2.1.1.6 Verschlüsselung sensibler Daten bei Speicherung und Übertragung

Sicherheits-anforderungen	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. Gegebenenfalls soll das System auch die sichere, selektive Löschung bestimmter Daten ermöglichen, beispielsweise durch Überschreiben mit Zufallsdaten.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ❑
Ergänzungen und Anmerkungen:	Beim Schutz sensibler[1] Daten sollten sowohl Informationssicherheitsaspekte als auch Datenschutzanforderungen berücksichtigt werden. Welche Daten als sensibel anzusehen sind, sollte primär vom Auftraggeber festgelegt werden, da dies vom Einsatzgebiet, internen Richtlinien und der nationalen Gesetzgebung abhängt. Dort wo der Schutzbedarf offensichtlich ist (z.B. bei Authentisierungsinformationen wie Passwörtern), sollten entsprechenden Maßnahmen durch den Hersteller bereits in der Standardkonfiguration umgesetzt sein. Zu den sensiblen Daten der einzelnen Systembereiche können wie im BDEW-Whitepaper bereits aufgeführt Passwörter und Betriebsprotokolle, aber ggf. auch Parametrierdaten gehören.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	-			
Organisatorische Anmerkungen:	Die als sensibel und schützenswert eingestuften Daten sind mit dem Lieferanten abzustimmen.			

[1] Siehe Anhang A „Datenklassifikation“.

2.1.1.7 Verschlüsselungsstandards

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:** Ja ☑	**Projektplanung / -umsetzung:** Ja ☑	**Produkt- / Systemservice:** Ja ❑	**Systembetrieb:** Ja ❑
Ergänzungen und Anmerkungen:	Als Stand der Technik für Verfahren für Hashbildung, Signaturen und Verschlüsselung und die zugehörigen Schlüssellängen werden insbesondere die folgenden Verordnungen und Empfehlungen angesehen: • „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung – Übersicht über geeignete Algorithmen“ (Bundesnetzagentur, Deutschland) • „Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008)“, Anhang Algorithmen und Parameter für qualifizierte elektronische Signaturen (Bundeskanzleramt Österreich) • Special Publication 800-57 “Recommendation for Key Management“ (National Institute of Standards and Technology, USA) Hiervon abweichende Verfahren oder Schlüssellängen sollten nur nach expliziter Freigabe durch den Auftraggeber eingesetzt werden.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	Insbesondere im Embbeded-Bereich müssen bei der Spezifikation von Algorithmen und Schlüssellängen die teilweise beschränkten Ressourcen der Komponenten berücksichtigt werden.			
Organisatorische Anmerkungen:	-			

2.1.1.8 Interne/externe Sicherheits- und Anforderungstests und zugehörige Dokumentation

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ❑	Ja ❑
Ergänzungen und Anmerkungen:	Bei der Übernahme bzw. Abnahme eines Systems sollte der Nachweis erbracht werden, dass ein umfangreicher Sicherheitstest durch den Lieferanten erfolgt ist. In der Auslieferungsdokumentation sollte die Dokumentation des Sicherheitstests in einer für eine Bewertung hinreichenden Detailtiefe enthalten sein. Bei Standardkomponenten ist im Regelfall eine Typprüfung pro Produktrelease ausreichend. Dabei ist aber zu berücksichtigen, dass die Grundparametrierung (z.B. aktive Netzwerkdienste und genutzte Protokolle) des Testsystems mit der Einsatzumgebung des Auftraggebers möglichst weitgehend übereinstimmen muss. Hierzu sollten die Einstellungen entsprechend eines Typprüfungsprotokolls bei der Inbetriebnahme überprüft werden. Im Rahmen von Abnahme- und Funktionsprüfungen sollten auch durch den Auftraggeber Sicherheitsprüfungen durchgeführt werden. Umfang und Testtiefe sollte dabei je nach Systemkomplexität und -kritikalität von einfachen Stichproben bis hin zu einem vollständigen Audit reichen. Die Sicherheits- und Anforderungsprüfungen auf Seiten von Auftraggeber und Auftragnehmer sollten auch Last- und Stresstests beinhalten.			

	Betriebsführungs- / Leitsysteme und Systembetrieb:	Leitsysteme und zentrale Betriebsführungssysteme sind häufig angepasste Individualentwicklungen und sollten i.d.R. bei der Abnahme explizit durch ein vollständiges Audit überprüft werden.
	Übertragungs-technik / Sprach-kommunikation:	Im Rahmen der Sicherheitstests sollten sowohl Netzelemente und Endgeräte als auch zentrale Server, Management- und Überwachungssysteme berücksichtigt werden. Für Netzelemente und Endgeräte sind i.d.R. einmalige Sicherheitstests im Rahmen eines Typtests ausreichend.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	In der Regel ist ein einmaliger Test im Rahmen des Typtests für Sekundär-, Automatisierungs- und Fernwirkkomponenten als ausreichend anzusehen, der ggf. nach signifikanten Änderungen wiederholt werden sollte. Bei Klein-Leitsystemen, z.B. im Stationsbereich sollte geprüft werden, ob individuelle Anpassungen eine Abnahmeprüfung notwendig machen oder ob hier eine Typprüfung ausreichend ist.
Organisatorische Anmerkungen:		**-**

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

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:** Ja ☑	**Projektplanung / -umsetzung:** Ja ☑	**Produkt- / Systemservice:** Ja ❑	**Systembetrieb:** Ja ❑
Ergänzungen und Anmerkungen:	Sind in der Systemumgebung des Betreibers gegenüber der Standard-Installation noch weitere Sicherheitseinstellungen, Konfigurationen, etc. notwendig, sollten diese explizit dokumentiert werden.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	-			
Organisatorische Anmerkungen:	**-**			

2.1.1.10 Integritäts-Prüfung

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ❑	Ja ❑

Ergänzungen und Anmerkungen:	Neben den Systemdateien des Betriebssystems sollten insbesondere Konfigurationsdaten, Anwendungsparameter sowie Firmwareparameter und Firmwareversionen sicher auf Integrität geprüft werden können. Um gezielte Manipulationen verhindern bzw. erkennen zu können, sind hierzu i.d.R. kryptographisch berechnete Prüfsummen notwendig. Nach Möglichkeit sollten die Prüfungen für Patches und Updates die gleichen Mechanismen nutzen (vgl. 2.1.1.3). Die Möglichkeit zur Integritätsprüfung auf der Ebene übergeordneter Systeme sollte eine Mindestanforderung sein. Mittelfristig sollte die Möglichkeit zur Integritätsprüfung auf allen Komponenten angestrebt werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungs-technik / Sprach-kommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	Bei prozessnahen Komponenten sollte eine Integritätsprüfung mindestens im Konfigurationstool für Parametrierstände und Firmwareversionen vorhanden sein. Eine detaillierte Vergleichbarkeit von Parametrierständen insbesondere von Offline- und Onlineversionen und archivierten Parametrierungen ist anzustreben.
Organisatorische Anmerkungen:	Die Integritätsprüfungen sollten insbesondere auch im Rahmen der Change Management-Prozesse berücksichtigt werden.

2.1.2 Dokumentation

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

Sicherheits-anforderungen	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).

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ❑	Ja ❑

Ergänzungen und Anmerkungen:	Der Auftragnehmer sollte eine Sicherheitsdokumentation erstellen, in der alle IT-sicherheitsrelevanten Informationen zusammengefasst sind. Die Dokumentation sollte u.a. die Beschreibung aller sicherheitsrelevanten Systemeinstellungen und Parameter sowie ihrer Standardwerte enthalten. Neben der konkreten Sicherheitskonfiguration und der zugehörigen Parameter fallen darunter z.B. auch System- und Kommunikationseinstellungen wie maximale Anzahl gleichzeitig angemeldeter Nutzer, maximale Anzahl von Netzwerkverbindungen, minimale Netzwerkbandbreiten usw. In der Regel enthält die Dokumentation eine grundsätzliche Beschreibung, die für alle Anwendungen und Konfigurationen gültig ist, sowie einen projektspezifischen Anteil, in dem die konkrete Umsetzung beschrieben ist, z.B. als Anhang zum Pflichtenheft. Alle sicherheitsrelevanten Beschreibungen sollten in einem separaten Dokument bereitgestellt werden. Die Prüfung der Dokumentation sollte Teil der Abnahmeprüfung sein.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-

	Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		**-**

2.1.2.2 Administrator- und Benutzer- Dokumentation

Sicherheits-anforderungen	2.1.2.2 Administrator- und Benutzer-Dokumentation ISO/IEC 27002:2013: 7.2.2, 12.1.17 ISO/IEC TR 27019:2013: 10.1.1 Es müssen getrennte Dokumentationen für den Administrator und die System-Benutzer existieren. Beide Dokumentationen sollten für die jeweiligen Gruppen unter anderem eine Auflistung der sicherheits-relevanten Einstellungen und Funktionen enthalten und Regeln für sicherheitsverantwortliches Handeln nennen.

Ausführungshinweise betreffen:		**Produkt- / Sys-tementwicklung:** Ja ☑	**Projektplanung / -umsetzung:** Ja ☑	**Produkt- / Sys-temservice:** Ja ☑	**System-betrieb:** Ja ☑
Ergänzungen und Anmerkungen:		Die Dokumentation von Zugangsdaten wie Passwörtern sollte nicht in der allgemeinen System- oder Sicherheitsdokumentation erfolgen, sondern sollte dem Auftraggeber separat übergeben werden.			
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
	Übertragungs-technik / Sprach-kommunikation:	Unter Umständen erfolgt keine Anwendung dieser Anforderung für Netzwerk- und übertragungstechnische Komponenten, da hier eine Trennung zwischen Administrator und Nutzer häufig nicht durchsetz-bar und sinnvoll ist.			
	Sekundär-, Auto-matisierungs- und Fernwirktechnik:	Unter Umständen erfolgt keine Anwendung dieser Anforderung im Bereich der Sekundär-/Automatisierungstechnik, da im Stations-Umfeld eine Trennung zwischen Administrator und Nutzer häufig nicht durchsetzbar und sinnvoll ist.			
Organisatorische Anmerkungen:		**-**			

2.1.2.3 Dokumentation sicherheitsrelevanter Einstellungen und Systemmeldungen

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ❑	Ja ❑
Ergänzungen und Anmerkungen:	Im Prozess-Umfeld sind hiermit nicht die primärtechnischen Anlagenparameter gemeint, sondern in erster Linie System- und Kommunikationseinstellungen und zulässige Grenzwerte, z.B. maximale Anzahl gleichzeitig angemeldeter Nutzer, maximale Anzahl von Netzwerkverbindungen, minimale Netzwerkbandbreiten und maximale Auslastungsgrenzen (z.B. des Netzwerkverkehrs) zur Sicherstellung eines störungsfreien Betriebs.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	In der Regel sind die genannten Parameter und Meldungen projektspezifisch und im Zuge der Anlagenplanung zu dokumentieren.			
Organisatorische Anmerkungen:	**-**			

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

Sicherheits-anforderungen	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 anderen Systemen und Netzwerken.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:** Ja ❑	**Projektplanung / -umsetzung:** Ja ☑	**Produkt- / Systemservice:** Ja ❑	**Systembetrieb:** Ja ❑
Ergänzungen und Anmerkungen:	Zu den Voraussetzungen und Umgebungs-Anforderungen für den sicheren Betrieb zählen u.a. auch Anforderungen an physische Sicherheit und Umgebungsparameter wie Klimatisierung, Energieversorgung, EMV-Schutz, Brand- und Havarieschutz, etc. Vgl. auch 2.1.2.3.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	-			
Organisatorische Anmerkungen:	**-**			

2.2 Bereich Basissystem

2.2.1 Grundsicherung und Systemhärtung

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ❑
Ergänzungen und Anmerkungen:	Alle Standard-Komponenten (Betriebssystem und ggf. eingesetzte Datenbanksysteme und Serverdienste) sollten nach anerkannten Vorgaben gehärtet werden. Zu den anzuwenden Härtungsmaßnahmen zählen u.a. o Deinstallation oder Deaktivierung unnötiger Softwarekomponenten o Deaktivierung unnötiger System- und Kommunikationsdienste o Deaktivierung unnötiger Standardnutzer o Änderung von Standardpassworten o Aktivierung sicherheitserhöhender Konfigurationsoptionen o Einschränkung der Rechte von Nutzern und Programmen o Deaktivierung unnötiger Kommunikations- und Datenträgerschnittstellen (CD/DVD, USB, Bluetooth, WLAN, usw.) o Deaktivierung nicht benutzter Switch-Ports Eine Sammlung von Best-Practice Härtungsguides für verschiedene Betriebssysteme, Serverdienste und Standardanwendungen findet sich z.B. beim *Center for Internet Security* (http://www.cisecurity.org)			

		oder bei den jeweiligen System- bzw. Softwareherstellern. Können gewisse Standardmaßnahmen aus technischen Gründen nicht angewandt werden, sollte dies durch den Auftragnehmer explizit begründet werden, z.B. im Rahmen der Pflichtenheftphase. Benötigen die Anwendungsnutzer keinen Zugriff auf das Betriebssystem, sollte ein solcher Zugriff wirksam verhindert werden. Ist ein Betriebssystemzugriff notwendig, sollte dieser für einen Standardanwender nur mit eingeschränkten Nutzerrechten erfolgen. Insbesondere ist hierbei eine unberechtigte Manipulation des Betriebssystems, der Anwendungsprogramme und Anwendungsdaten sowie der Anwendungskonfiguration und der Projektierungsdaten wirksam zu verhindern. Bei der Implementierung des Zugriffschutzes ist insbesondere darauf zu achten, dass dieser nicht durch das Starten von Hilfsanwendungen wie Web- und Hilfebrowsern, Dateibetrachtern o.ä. umgangen werden kann. Wird vom Auftragnehmer nur ein Teil der Komponenten des Gesamtsystems geliefert, sollte von ihm beschrieben werden, wie die weiteren Teilkomponenten (z.B. Betriebssystem oder Datenbanksysteme) auf Basis anerkannter Best-Practice-Guides gehärtet werden können, ohne dass die Funktion der vom Auftragnehmer gelieferten Systemkomponenten und des Gesamtsystems beeinträchtigt wird. Die Grundkonfiguration und die Härtungsmaßnahmen sollten geprüft und in der Sicherheitsdokumentation aufgeführt werden (z.B. installierte Programme und Anwendungen, aktive bzw. deaktivierte Dienste und Ports, Dateifreigaben, Einstellungen zur Systemkonfiguration etc.).
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	Auf prozessnahen Komponenten wie Steuerungen, SPSen und Automatisierungskomponenten oder Gateways sollten insbesondere alle nicht für den Betrieb notwendigen Kommunikationsdienste und Parametrierzugänge deaktiviert werden. Ggf. vorhandene Standardpasswörter sollten auf sichere Werte gesetzt werden sowie sicherheitserhöhender Konfigurationsoptionen aktiviert werden.
Organisatorische Anmerkungen:		Die Systemhärtung sollte im Rahmen regelmäßig (i.d.R. jährlich) durchzuführender Sicherheitstests überprüft und ggf. angepasst werden. Die Überprüfung sollte dabei im Regelfall von vom Hersteller unabhängigen Prüfern durchgeführt werden.

2.2.2 Antiviren-Software

Sicherheits-anforderungen	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 gleichwertigen 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ❑
Ergänzungen und Anmerkungen:	Es sollten technische und organisatorische Schutzmaßnahmen im System und an den Schnittstellen vorgesehen werden, durch die ein dauerhaft effektiver Schutz gegen Schadsoftwarebefall bei einer gleichzeitig hohen Systemverfügbarkeit sichergestellt werden kann. Der Schnittstellenschutz umfasst insbesondere auch die logischen und technischen Schnittstellen zum Datenaustausch mit externen Netzen wie der Büroumgebung, die Schnittstellen für Fernzugriff, Fernwartung und Prozessankopplung sowie alle stationären und mobilen Arbeitsplätze, Parametriernotebooks und Programmiergeräte. Die Möglichkeit zur Installation und zum Betrieb eines Schadsoftwareschutzes („Antiviren-Software“) sollte prinzipiell für alle Systeme gegeben sein, für die entsprechende Schutzsoftware am Markt verfügbar ist. Für alle anderen Systeme, insbesondere für Komponenten, bei denen industrielle Embedded-Systeme eingesetzt werden, sollten abgesicherte Schnittstellen, die die Gefahr eines Schadsoftwarebefalls oder von durch Schadsoftware induzierten Störungen reduzieren, oder gleichwertige Alternativmaßnahmen vorgesehen werden. Der Einsatz von bereits im Unternehmen vorhandenen Antivirus-Produkten ist häufig sinnvoll. Allerdings kann bei erhöhtem Schutzbedarf der Einsatz anderer oder ergänzender Produkte notwendig sein.			

		Für patternbasierte Schutzsoftware sollte das vorgesehene Konzept für Patternupdates geprüft werden. Falls hier Freigaben und Tests notwendig sind, müssen die realisierbaren Fristen und Zyklen so gewählt sein, dass ein dauerhaft effektives Schutzniveau gewährleistet werden kann. Die Verwendung dedizierter zentraler, prozessnetzinterner Updateserver sollte angestrebt werden. Falls sog. Whitelisting-Lösungen genutzt werden sollen, ist sicherzustellen, dass mit der vorgesehen Technik und Konfiguration ein hinreichend hohes Schutzniveau erreicht werden kann. Der Auftragnehmer sollte die zum Einsatz freigegebenen Schutzprogramme und die ggf. notwendigen Konfigurationsoptionen spezifizieren, z.B. Ausschluss von bestimmten Verzeichnissen, Nutzung bestimmter Scan-Arten, Konfiguration der Whitelisting-Anwendungen. Bei der Inbetriebnahme des Basissystems sollte seitens des Lieferanten die Kompatibilität der Schutzsoftware mit der Lieferantensoftware explizit geprüft werden. Alle vom Auftraggeber gelieferten Systeme und Datenträger sollten vor der Auslieferung bzw. Übergabe einer Untersuchung auf Schadsoftwarebefall unterzogen werden. Bevorzugt sollten dabei Rechnersysteme durch einen Offline-Scan mit einem von einem externen Medium gebooteten Betriebssystem geprüft werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	s.o.
	Übertragungstechnik / Sprachkommunikation:	Derzeit ist der Einsatz von Antivirus-Software auf Netzwerkkomponenten wie Switches, Router oder Netzelementen i.d.R. nicht möglich. Die Installation von Schutzsoftware sollte aber insbesondere auf Management- und Überwachungssystemen sowie auf Konfigurations- und Wartungsgeräten vorgesehen werden.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	Im Stations- und Automatisierungsumfeld betrifft die Anforderung insbesondere Stationsbedienplätze, Kleinleitsysteme, Nahsteuerungen, Feldanzeigen, Wartungsgeräte, usw. Der Einsatz von Antivirus-Software auf Automatisierungskomponenten ist derzeit i.d.R. nicht möglich. Eine Möglichkeit zur Einbindung in eine zentralisierte Lösung, insbesondere mit Hinblick auf die Problematik von Update-Prozessen innerhalb der i.d.R. dezentral aufgebauten Stationsumgebungen, sollte angestrebt werden.
Organisatorische Anmerkungen:		

2.2.3 Autonome Benutzerauthentifizierung

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ❑

Ergänzungen und Anmerkungen:	Die Integration der Basissystemkomponenten in einen zentralen Directory-Service ist anzustreben, wobei dies mit prozessnetz-internen Directory-Servern realisiert werden sollte. Dabei kann ein eigener Directory-Service aufgebaut werden oder die Integration in einen bestehenden Directory-Service erfolgen. Hierbei ist auf eine Struktur zu achten, die das Schutzniveau des Prozessnetzes nicht herabsetzt und auch keine Abhängigkeiten zu Diensten außerhalb des Prozessnetzes schafft. Bei der Nutzung einer zentralen Benutzerverwaltung sollten lokale Notfallpassworte für den Fall einer Störung des Benutzerverwaltungsdienstes vorgesehen werden. Ist für die Nutzung der Systeme ein Betriebssystem-Login erforderlich, sollte hierzu ein niedrig privilegierter Account verwendet werden. Systemaccounts sollten nicht für die normale, nicht-administrative Anwendungsnutzung verwendet werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	Die Verwendung eines Mehrnutzerbetriebs auf System- und Anwendungsebene sollte insbesondere für HMI-Arbeitsplätze auf Stationsebene und in Automatisierungsumgebungen prinzipiell möglich sein. Die Anbindung an zentrale DirectoryDienste sollte bei Bedarf realisierbar sein. Hierbei muss insbesondere für dezentrale Systeme wie z.B. verteilte Stationen die Verfügbarkeitsproblematik zentraler Directory-Dienste hinreichend berücksichtigt werden.
Organisatorische Anmerkungen:	**-**

2.3 Bereich Netze / Kommunikation

2.3.1 Sichere Netzwerkkonzeption und Kommunikationsverfahren

2.3.1.1 Eingesetzte Protokolle und Technologien

Sicherheits-anforderungen	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 sichere 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 bereit gestellt 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 ACLs 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-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.

Ausführungshinweise betreffen:	Produkt- / Systementwicklung: Ja ☑	Projektplanung / -umsetzung: Ja ☑	Produkt- / Systemservice: Ja ❑	Systembetrieb: Ja ☑
Ergänzungen und Anmerkungen:	Bieten die genutzten Netzwerkprotokolle sicherheitserhöhende Optionen, sollten diese aktiviert werden. zu a) Für interaktive Nutzerzugänge (z.B. zur Fernadministration) sollten ausschließlich sichere Protokolle – wie beschrieben – eingesetzt werden. Zur Fernadministration sollten bevorzugt SSH / SCP / SFTP bzw. RDP in den aktuellen Versionen und mit aktivierten Sicherheitseinstellungen verwendet werden. Schreibende Zugriffe auf Daten und Variablen sollten nur nach einer erfolgreichen Authentisierungs- und Autorisierungsprüfung möglich sein. Parametrier- und Engineering-Zugriffe sollten nur über gesicherte Protokolle erfolgen und sollten ebenso nur nach einer erfolgreichen Authentisierungs- und Autorisierungsprüfung möglich sein. zu b und c) Zu empfehlen ist eine strikte Trennung der technischen und kaufmännischen Netze und der Aufbau eines zentralen Netzwerkmanagementsystems für die Prozessnetze. zu e) Protokolle, die UDP als Transportprotokoll nutzen, sollten generell vermieden werden. Ausnahmen gelten momentan für die folgenden Standardprotokolle: • PTP (Precision Time Protocol) • NTP / SNTP (Network Time Protocol / Simple Network Time Protocol) • SNMP (Simple Network Management Protocol) Die Nutzung von Protokollen mit dynamischer Portvergabe (z.B. RPC/DCOM) sollte über Firewalls hinweg prinzipiell vermieden werden. Für das häufig zur Systemkopplung eingesetzte OPC-Protokoll sollten die im Folgenden aufgeführten Hinweise berücksichtigt werden. Diese gelten primär für die DCOM-basierten OPC-Versionen. Für OPC-XML und OPC-UA sind die Hinweise entsprechend angepasst umzusetzen: • Netzwerkbasierter OPC-Zugriff sollte auf OPC-Serverbasis selektiv freigegeben werden. Wird nur ein lokaler OPC-Zugriff benötigt, sollte für den OPC-Server der Remotezugriff unterbunden werden. • OPC-Kommunikation sollte über Firewallgrenzen nur über kryptographisch gesicherte OPC-Tunnellösungen geführt werden.			

		• OPC-Zugriff auf Systeme mit erhöhtem Schutzbedarf sollte nur über gesicherte und gehärtete Proxysysteme erfolgen, die mit einem aktiven Schadsoftwareschutz und unter Anwendung eines Patchmanagementprozesses betrieben werden. • Wird nur lesender OPC-Zugriff benötigt, sollten Schreibzugriffe generell unterbunden werden. Notwendige Schreibzugriffe sollten möglichst selektiv auf die benötigten Datenpunkte eingeschränkt werden. Wird dies vom OPC-Server nicht nativ unterstützt, sollten hierzu ggf. zusätzliche OPC-Sicherheitslösungen eingesetzt werden. • Kritische Systemvariablen sollten nicht zum Schreibzugriff freigegeben werden. • Die OPC- bzw. DCOM-Rechtevergabe sollte möglichst restriktiv erfolgen. Dies beinhaltet u.a. die Nutzung niederprivilegierter Nutzeraccounts für den Datenzugriff und die Nutzung verschiedener Accounts für *Launch*- und *Access*-Permissions. Freigaben für die *Everyone*-Gruppe sollten nicht erfolgen. OPC-Server- und OPC-Serverbrowserdienst sollten nicht mit SYSTEM-Privilegien betrieben werden. • Die Option „Authentisierungslevel“ sollte mindestens auf „Packet Integrity“ gesetzt sein. • OPC sollte nur für die benötigten Protokolle aktiviert werden. I.d.R. ist dies ausschließlich TCP/IP. Zugriffe über andere Protokolle wie UDP, NetBEUI, HTTP bzw. COM Internet Services oder IPX sollten deaktiviert werden. Die Standard-Protokolle IEC 60870-5 und IEC 61850 bieten ohne zusätzliche Maßnahmen keine sichere Integritätsüberprüfung, Authentifizierung und Verschlüsselung, vgl. hierzu 2.4.3.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	zu d) Derzeit werden die VPN-Tunnel zumeist noch auf Routern in der Station terminiert. Zukünftig sollte in Absprache mit dem Auftraggeber ggf. eine Terminierung direkt auf den Steuerungseinheiten erfolgen. zu e) Die Nutzung von OPC über Anlagengrenzen hinweg sollte vermieden werden. zu f) Beim Einsatz einer gemeinsamen Netzwerk-Infrastruktur in Automati-

		sierungsnetzen für Prozesskommunikation und zur sonstigen Netzkommunikation (wie z.B. Parametrier- und Verwaltungskommunikation) sind insbesondere die Auswirkungen von Netzwerkstörungen oder Überlasten auf das Zeitverhalten in der Prozesskommunikation zu berücksichtigen (Beispiel: IEC 61850, GOOSE und Sampled Values, VLAN-Nutzung in der Stationsautomatisierung).
Organisatorische Anmerkungen:		**-**

2.3.1.2 Sichere Netzwerkstruktur

Sicherheits-anforderungen	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 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ☑
Ergänzungen und Anmerkungen:	Die Anforderungen sind in der Regel projektspezifisch umzusetzen. Für Datenschnittstellen zu Fremdsystemen oder internen Netzen und Systemen, die in erhöhtem Maße externen Sicherheitsbedrohungen ausgesetzt sind (z.B. ein Büro-LAN mit Internetnutzung, dezentrale Anlagen mit vermindertem physikalischem Zugangsschutz etc.), sollte die Funktion einer DMZ vorgesehen werden. Hierbei sollte immer die Regel gelten, dass DMZ-Komponenten keinen Zugriff auf interne Systemkomponenten in den Zonen mit höherem Sicherheitslevel haben dürfen. Die Kommunikationsrichtung sollte immer vom hohen Sicherheitslevel zum geringeren gerichtet sein. Mit Ausnahme von WAN/ÜT-Strecken sollten sich technische Netzwerke nur im inneren Sicherheitsbereich des physischen Objektschutzes befinden. Werden technische Systeme über diese Sicherheitsbereiche hinweg gekoppelt, sollte der Einsatz von VPNs geprüft werden. Sicherheitsgerichtete Kommunikation im Sinne der funktionalen bzw. Anlagensicherheit sollte nur innerhalb abgeschlossener, aus dedizierten Hardwarekomponenten aufgebauten Netzwerksegmenten erfolgen. Möglichkeiten zur Konfiguration der Parameter der funktionalen bzw. Anlagensicherheit über Netzwerkzugriffe sollten generell ver-			

		mieden werden. Werden diese zwingend benötigt, sollten sie nur über die o.g. abgeschlossenen Netzwerksegmente zugänglich sein. zu a) Eine physikalische Trennung funktionaler Ebenen sollte einer logischen Trennung vorgezogen werden. Wenn eine physikalische Trennung nicht möglich ist, ist das Restrisiko zu bewerten. Zur Netzwerktrennung sollte die Nutzung von Gateways, die eine Protokollwandlung durchführen und keinen direkten IP-Verkehr zulassen, geprüft werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Insbesondere an Netzwerkübergängen von systeminternen Netzwerken (z.B. Leitsystem-LAN) zu weiteren internen Netzwerken und zu WAN-Netzen (z.B. zur Prozessankopplung) sollte eine DMZ-Struktur und die Installation von Firewallfunktionalitäten vorgesehen werden.
	Übertragungstechnik / Sprachkommunikation:	Wo möglich, sollte betriebseigene Infrastruktur verwendet werden. Bei Fremdanbietern sollte die Einhaltung von Sicherheitsstandards vertraglich eingefordert und ggf. überprüft werden. Es sollte geprüft werden, ob die Kommunikation im Fremdnetz durch ein eigenbetriebenes VPN abgesichert werden muss.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	An Übergängen von lokalen Netzwerken (z.B. Stations- oder Anlagen-LAN) zu weiteren Netzwerken (z.B. Leitstellen oder benachbarte Stationen/Anlagen) sollte die Installation von Firewallfunktionalitäten vorgesehen werden. Eine Trennung unterschiedlicher Funktionen ist generell zu empfehlen. So sollten bei leittechnischen Anwendungen Terminal- und Anlagennetzwerk durch getrennte Netzwerkkomponenten realisiert werden. Die direkte Anbindung von Schutzgeräten an das allgemeine Automatisierungsnetz sollte vermieden werden, falls eine direkte Kommunikation mit anderen Automatisierungskomponenten funktional nicht notwendig ist. Gegebenenfalls sollte eine Segmentierung mit VLANs geprüft werden (vgl. 2.3.1.1 f). Die direkte Kopplung unterschiedlicher Anlagen, Systeme und Anwendungen über ein gemeinsames Anlagennetzwerk sollte vermieden werden. Ein systemübergreifender Zugriff auf Komponenten am Anlagennetzwerk sollte stattdessen über gehärtete Gatewaykomponenten realisiert werden.
Organisatorische Anmerkungen:		-

2.3.1.3 Dokumentation der Netzwerkstruktur und -konfiguration

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Neben Kabellaufplänen sollten auch die logische Segmentierung in Sicherheitszonen und die Informationsflüsse in der Netzwerkdokumentation enthalten sein. Hier sollten bei IP-basierten Protokollen insb. die genutzten Dienste und Protokolle sowie die verwendeten Portnummer(n) und die Kommunikationspartner aufgeführt werden. Die Dokumentation sollte z.B. Port-genau sein, Kabel sollten mit Kabelnummer und Gegenziel beschriftet werden. Informationen in der Dokumentation sollten im Zeichnungs-Layer getrennt werden, um Dokumente mit unterschiedlichem Informationsgehalt (z.B. Netzwerkstruktur ohne IP-Adressen) zur Verfügung zu haben. Die Dokumentation sollte Angaben über normale und maximal zu erwartende Datenübertragungsraten enthalten, damit gegebenenfalls auf den Netzwerkdevices eine Limitierung der Datenübertragungsraten zur Verkehrssteuerung und Verhinderung von DoS/Überlast-Problemen implementiert werden kann. Ebenso sollte die maximal zulässige Netzwerkbelastung angeben werden, unterhalb der eine zuverlässige Funktion des Gesamtsystems und der Einzelkomponenten gewährleistet ist.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-

	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Auto-matisierungs- und Fernwirktechnik:	Zur korrekten Umsetzung der Sicherheitsanforderung sollte auch die Kommunikation zwischen den Komponenten in der Station und mit dem Feld dokumentiert werden. Mit dem Begriff „Perimeter“ ist im Stations-Umfeld die „Außenschnitt-stelle“ zwischen der einzelnen Station und anderen Netzen gemeint (Leitstelle, Ferndiagnose, etc.).
Organisatorische Anmerkungen:		Die aktuelle Dokumentation sollte jederzeit verfügbar sein, z.B. für den Bereitschaftsdienst.

2.3.2 Sichere Wartungsprozesse und RAS-Zugänge

Hinweis: Der Ausdruck „Wartung“ bezieht sich im BDEW-Whitepaper und in diesem Dokument allgemein auf alle vom Auftraggeber/Betreiber zu beauftragenden Service-Maßnahmen wie Instandhaltungsarbeiten, Störungsanalysen, Fehler- und Störungsbehebung, Verbesserungen, Anpassungen, usw.

2.3.2.1 Sichere Fern-Zugänge

Sicherheits-anforderungen	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-Authentifizierungsverfahren 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ☑
Ergänzungen und Anmerkungen:	Eine direkte Kopplung mit externen Netzwerken oder Systemen sollte insbesondere für Systeme mit erhöhten Sicherheitsanforderungen vermieden werden. Generell darf die Fernwartung eine Netzwerktrennung und die vorhandenen Sicherheitsmechanismen nicht umgehen. Für Fernzugriffe sollte Zugangsserver unter Kontrolle des Betreibers genutzt werden. Damit wird sichergestellt, dass alle internen Sicherheitsanforderungen und Richtlinien jederzeit überprüfbar erfüllt werden. Alle für die Wartung benötigten Werkzeuge sollten dann in bzw. mit der Zugangsserver-Umgebung lauffähig sein und einen Mehrbenutzerbetrieb unterstützen. Zusätzlich zu empfehlen, sind separat aktivierbare Zugangspunkte in das jeweilige technische Netz bzw. Netzsegment. Für jede Netzwerkzone und jeden Dienstleister sollte nach Möglichkeit ein eigener, logisch separierter Fernwartungszugang geschaffen werden. Für alle Fernzugriffe müssen mindestens die gleichen Sicherheitsanforderun-			

		gen gelten wie für lokale Wartungszugriffe. Auf Betreiberseite sollte eine Protokollierung aller relevanten Verbindungsdaten, wie z.B. der Zeitpunkt des Auf-/Abbaus der Verbindung bzw. der Wartungssitzung, die Netzwerk-Adressen von Einwahl- und Zielsystemen, die Nutzerkennungen etc. erfolgen. Ggf. sollten auch relevante Aktionen in Sende- und Empfangsrichtung protokolliert werden. Auf Betreiberseite sollten für alle Dienstleister standardisierte und je nach Anwendungsumfeld zentralisierte Fernwartungsinfrastrukturen und –prozesse genutzt werden. Bei einem Fernzugriff auf vom Endanwender genutzte Komponenten sind die entsprechenden gesetzlichen Rahmenbedingungen wie z.B. Datenschutzgesetze oder Betriebsverfassungsgesetz zu berücksichtigen. In der Regel ist dem Endanwender der Fernzugriff eindeutig zu signalisieren.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		**-**

2.3.2.2 Anforderung an die Wartungsprozesse

Sicherheits-anforderungen	2.3.3.2 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 ermöglichen. 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, 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ☑
Ergänzungen und Anmerkungen:	Die hier genannten Anforderungen sollten bereits bei Projektplanungen und bei Wartungsvereinbarungen in Zusammenarbeit zwischen Auftraggeber und Hersteller bzw. Dienstleister berücksichtigt werden. Ein Ziel der Anforderung ist u.a., dass kein unbemerkter und unbe-			

		fugter Fernwartungszugang von Extern erfolgen kann. Generell sollte bei Wartungsarbeiten die Betriebsführung, z.B. in der Warte, über Arbeiten an den Anlagen informiert werden, beispielsweise durch Zu- oder Abschalten des Fernwartungszuganges. Dies gilt auch für Wartungszugriffe durch internes Personal. Insbesondere bei Zugriffen externer Dienstleister kann dies ggf. durch die Hinterlegung des Authentisierungstokens in der Warte erreicht werden. Vergleiche hierzu auch 2.5.4. zu f) Für Arbeiten vor Ort sollte eine Bereitstellung von Auftraggeber-eigener Hardware erfolgen. Ein Anschluss von Hardware des Lieferanten sollte vermieden werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		Die Anforderungen an Wartungsprozesse sollten vertraglich geregelt sein. Eine entsprechende, ggf. gegenseitige Sicherheitsregelung sollte durch den Auftraggeber festgelegt und den Servicetechnikern nachweislich zur Kenntnis gebracht werden.

2.3.3 Funktechnologien: Bedarf und Sicherheitsanforderungen

Sicherheits-anforderungen	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 dedizierten 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Alle Funktechnologien sollten generell nur bei zwingendem Bedarf und nach expliziter Freigabe durch den Auftraggeber eingesetzt werden. Generell muss bei einem Einsatz von Funktechnologien ein möglicher Durchgriff in weitere Kommunikationsnetze sicher verhindert werden. Drahtlose Peripheriegeräte und Eingabegeräte wie Tastaturen, Mäuse sowie Überwachungseinrichtungen wie Kameras sollten ebenfalls berücksichtigt werden. Die Nutzung von sicherheitsgerichteter Kommunikation über drahtlose Kommunikationstechnologien sollte i.d.R. vermieden und darf nur nach einer expliziten Risikoanalyse durchgeführt werden. Ggf. sind hierfür spezielle Baugruppen und ein spezifischer Schutz gegen externe Störstrahlung nötig. Für weitere Hinweise zum sicheren Einsatz von WLAN und Bluetooth siehe die NIST-Dokumente „NIST Special Publication 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks“ bzw. „NIST Special Publication 800-121 - Guide to Bluetooth Security“.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-

	Übertragungs-technik / Sprach-kommunikation:	Im Umfeld der Sprachkommunikation sollte insbesondere auch die Absicherung von draht-/schnurlosen Telefonen berücksichtig werden.
	Sekundär-, Auto-matisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		**-**

2.4 Bereich Anwendung

2.4.1 Benutzerverwaltung

2.4.1.1 Rollenkonzepte

Sicherheits-anforderungen	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 Systemkonfiguration. • 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 Administrator-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.

Ausführungshinweise betreffen:	Produkt- / Systementwicklung:	Projektplanung / -umsetzung:	Produkt- / Systemservice:	Systembetrieb:
	Ja ☑	Ja ☑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Benutzerrollen ermöglichen eine einheitliche und leichtere Zuordnung von Berechtigungen für die einzelnen Benutzer. Rollenkonzepte dienen auch dazu, unabsichtliche Fehlhandlungen zu verhindern. Eine Festlegung der den Rollen zugewiesenen Rechte sollte durch den Auftraggeber erfolgen bzw. mit ihm abgestimmt werden. Gegebenenfalls kann es sinnvoll sein, durch das Rollenkonzept ein Vier-Augen-Prinzip zu erzwingen, z.B.: • Rolle „Änderung von Parametrierungen“ • Rolle „Freigabe der Parametrierungsänderungen“ Neben den benutzergebundenen Berechtigungen sollten auch systemgebundene Berechtigungen bzw. Rollen vorgesehen sein, um den unterschiedlichen Arbeitsplätzen (Warte, Backoffice, Systembetreuung, …) unabhängig vom Benutzer bestimmte Rechte oder Einschränkungen zuzuordnen. Die systemgebundenen Berechtigungen und Rollen müssen dabei immer stärker sein als die benutzergebundenen Berechtigungen und Rollen. Die Berechtigungen sollten nicht nur auf Ebene der Bedien- und Benutzeroberfläche realisiert sein, sondern sollten durchgehend in der gesamten Applikation und ggf. auch auf System- und Datenbankebene umgesetzt werden. Die Möglichkeit zur zeitlichen Befristung von Rollen sollte bei Bedarf vorgesehen werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	Beispiele für Nutzerrollen im Umfeld von Betriebsführungs- und Leitsystemen sind z.B.: • Administrator • Parametrierung/Datenaufbereitung • Bedien-/Schaltberechtigung • Beobachtungsbetrieb • Datentest/Qualitätssicherung
Übertragungstechnik / Sprachkommunikation:	Anzuwenden insbesondere für Management-Systeme. Beispiele für im ÜT-Umfeld anwendbare Nutzerrollen sind: • Administrator • Konfiguration • Beobachtung/Überwachung
Sekundär-, Automatisierungs- und Fernwirktechnik:	Im Stationsumfeld sollen angepasste und abgestufte Rollen umgesetzt werden. Dies gilt insbesondere für Stationsbediensysteme. Beispiele für im Stationsumfeld anwendbare Nutzerrollen sind: • Administrator • Schaltberechtigter

		• Beobachter • Parametrierung • Änderung von Betriebsparametern • Beobachtungsbetrieb • Diagnose (ohne Parametrier- und Schaltmöglichkeit) • Datentest/Qualitätssicherung. Für aktuelle Geräte der Schutz- und Automatisierungstechnik sind Rollenkonzepte derzeit häufig noch nicht umfassend realisierbar. In diesem Fall sollte mindestens ein Passwortschutz und/oder ein Schlüsselschalter vorgesehen werden. Zukünftig sollten auch bei diesen Geräten eine Trennung von Nutzerrollen sowie eine Einbindung in Directory-Dienste möglich sein.
Organisatorische Anmerkungen:		Die im System hinterlegten Rollen sollten mit der Organisationsstruktur abgeglichen werden und sich bei Änderungen anpassen lassen.

2.4.1.2 Benutzer-Authentifizierung und Anmeldung

Sicherheits-anforderungen	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 Smart-Cards. 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 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.

Ausführungshinweise betreffen:	Produkt- / Systementwicklung:	Projektplanung / -umsetzung:	Produkt- / Systemservice:	Systembetrieb:
	Ja ☑	Ja ☑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Passworte und andere Authentisierungsinformationen dürfen nur kryptographisch gesichert übertragen und im System gespeichert werden (vgl. 2.1.1.6 und 2.3.1.1). zu c) Im Rahmen der Anwendungskonfiguration sollte die erforderliche Passwortkomplexität durch den Anwendungsadministrator möglichst umfassend konfigurierbar sein. Zu definierende Parameter umfassen z.B. • minimale Passwortlänge • minimale Anzahl von bestimmten Zeichen/Zeichengruppen, z.B. Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen, etc. • Gültigkeitsdauer • Verhinderung der Nutzung eines vorherigen Passwortes beim Passwortwechsel • maximale Anzahl von Passwortänderungen pro Zeiteinheit (z.B. pro Tag) zu d) Insbesondere bei Fernarbeitsplätzen sollte eine 2-Faktor-Authentifizierung vorgesehen werden. Die Standardbenutzeraccounts aller Applikationen und Systeme sollten bei Übernahme des Systems deaktiviert werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	Um eine kontinuierliche Anlagenüberwachung durch das Bedienpersonal und eine sichere Betriebsführung sicherstellen zu können, sollten auf den hierfür notwendigen Systemen (z.B. HMI/Bedienplatz der Leitsysteme) Möglichkeiten für eine sichere und nachvollziehbare Übergabe von Benutzer-Sessions im laufenden Betrieb, beispielsweise beim Schichtwechsel, vorhanden sein. Hierbei sollten auch Protokollierungsanforderungen berücksichtigt werden.
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	zu a) Die derzeit verbreitete Technik erfordert zum Teil eine lokale Anmeldung über Gruppen-Accounts. Mittelfristig sollte eine Umsetzung ohne die Nutzung von Gruppen-Accounts angestrebt werden. zu d) Für lokale Zugriffe im Stationsumfeld in der Regel nicht notwendig. zu e) Aktuelle Schutz- und Automatisierungskomponenten unterstützen

		häufig keine Einbindung von Directory-Diensten. Insbesondere im dezentralen Stationsumfeld ist auch für HMI-Systeme die Nutzung zentraler Directory-Dienste aus Verfügbarkeitsgründen u.U. mit aktueller Technik derzeit nicht zu realisieren. Zukünftig sollte auch hier eine Einbindung in Directory-Dienste möglich sein.
Organisatorische Anmerkungen:		Der Betreiber sollte sicherstellen, dass eine Passwortpolicy festgelegt ist und umgesetzt wird.

2.4.2 Autorisierung von Aktionen auf Benutzer- und Systemebene

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ❑	Ja ☑
Ergänzungen und Anmerkungen:	Die hier angeführten sicherheitsrelevanten/-kritischen Aktionen sind vom Auftraggeber/Betreiber der Systeme im Einzelnen zu spezifizieren. Diese Aktionen sind dann auch mit der Angabe der Benutzerkennung zentral zu loggen.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	Für Schutz- und Stationsleittechnik in der Regel nicht notwendig, eine Anwendung sollte durch den Auftraggeber/Betreiber geprüft werden.			
Organisatorische Anmerkungen:	-			

2.4.3 Anwendungsprotokolle

Sicherheits-anforderungen	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 vorzuziehen, welche die Integrität der Kommunikation sowie die korrekte Authentifizierung und Autorisierung der Kommunikationspartner 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Entsprechend den technischen Möglichkeiten sollten in allen Bereichen standardisierte IEC-Protokolle angewendet werden. Der private Bereich dieser Kommunikationsprotokolle sollte nach Möglichkeit nicht verwendet werden. Eine Verschlüsselung der Protokolle nach IEC 62351 sollte durch den Betreiber geprüft werden, wobei ggf. auftretende Einschränkungen bei der Fehlerdiagnose sowie die notwendige Infrastruktur und Prozesse zur Schlüsselverwaltung berücksichtigt werden sollten. Dort, wo aktuelle Systeme und Geräte noch nicht die Möglichkeit der Verschlüsselung nach IEC 62351 bieten, sollte die Fernwirkübertragung daher auf den unterlagerten Netzwerkebenen geschützt werden, z.B. durch Nutzung von VPN-Technologie oder SSL/TLS-Tunnelung. Insbesondere für IP-basierte Protokolle sollten entsprechend sichere Netzwerkstrukturen vorgesehen werden (siehe 2.3).
Betriebsführungs- / Leitsysteme und Systembetrieb:	Insbesondere die Datenkopplung mit weiteren Leitsystemen und mit Automatisierungs-/Fernwirkkomponenten sollte über genormte Protokolle erfolgen. Die Kommunikation innerhalb des Leitsystems ist i.d.R. herstellerabhängig. Hier sollten gleichwertige Sicherungsmechanismen vorgesehen werden.

	Übertragungs-technik / Sprach-kommunikation:	Insbesondere für Voice-over-IP-Kommunikation sollten Sicherheits-mechanismen eingesetzt werden, die die Vertraulichkeit der Kommu-nikation sicherstellen und eine sichere Authentisierung der Kommuni-kationspartner und -komponenten gewährleisten.
	Sekundär-, Auto-matisierungs- und Fernwirktechnik:	Die Kommunikation zwischen einzelnen Automatisierungskomponen-ten erfolgt vielfach über Industriestandards oder proprietäre Herstel-lerprotokolle (z.B. Industrial Ethernet, Profinet, Profibus etc.). Die Anbindung an die Stationsebene und an das Leitsystem sollte über die angeführten Standardprotokolle erfolgen. Der Einsatz von Authentifizierung und Verschlüsselung innerhalb eines Stationsnetzwerks ist bei entsprechend strikter Sicherung der Außenschnittstellen i.d.R. nicht notwendig.
Organisatorische Anmerkungen:		-

2.4.4 Web-Applikationen

Sicherheits-anforderungen	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 insbesondere 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ❑	Ja ❑	Ja ❑
Ergänzungen und Anmerkungen:	Die Einführung von Webanwendungen sollte generell nur in Abstimmung und nach einer expliziten Freigabe durch den Auftraggeber/Betreiber erlaubt werden. Beim Einsatz von Web-Anwendungen sollten allgemein anerkannte Sicherheitsempfehlungen und Hinweise wie z.B. die des Open Web Application Security Project (OWASP, http://www.owasp.org) oder der ÖNORM A-7700 „Informationsverarbeitung — Sicherheitstechni-			

		sche Anforderungen an Webapplikationen“ berücksichtigt und umgesetzt werden. Sollten die eingesetzten Systemkomponenten über Browserschnittstellen (z.B. zur Parametrierung) verfügen, ist auch hier eine sichere Implementierung zu gewährleisten. Andernfalls sollten die Schnittstellen deaktiviert werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		**-**

2.4.5 Integritätsprüfung relevanter Daten

Sicherheits-anforderungen	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).

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ❑	Ja ☑

Ergänzungen und Anmerkungen:	Es muss auf Konsistenz der verarbeiteten Daten geachtet werden. Ein konsistenter Eingangsdatensatz muss in einen konsistenten Ausgabedatensatz übergeführt werden – insbesondere darf es zu keinen inkonsistenten Zwischenzuständen kommen. Daten aus externen Systemen oder über Nutzerschnittstellen eingegebene Daten sollten immer auf Konsistenz und Gültigkeit geprüft werden (z.B. Typ, Länge, Umfang, Syntax, Wertebereich, Plausibilität, Alter). Dies gilt insbesondere, wenn fehlerhafte oder manipulierte Daten den sicheren Systembetrieb gefährden könnten (z.B. beim Import von Parametrierungen). Ebenso sollte eine solche Prüfung innerhalb der Anwendung bzw. innerhalb des Systems realisiert werden, z.B. an der Schnittstelle zwischen Anwendungskomponenten oder Programmmodulen. Beispiele: • Überprüfung des möglichen Stellbereichs eines Betriebsmittels • Prüfung des Änderungsdatums einer Parametrierung, um vor dem Überschreiben einer ggf. aktuelleren Version zu warnen.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:	**-**

2.4.6 Protokollierung, Audit-Trails, Timestamps, Alarmkonzepte

Sicherheits-anforderungen	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 einheitliche 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.

Ausführungshinweise betreffen:	Produkt- / Systementwicklung:	Projektplanung / -umsetzung:	Produkt- / Systemservice:	Systembetrieb:
	Ja ☑	Ja ☑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Eine Pflicht zur Protokollierung kann auf Grund von betrieblichen, behördlichen oder rechtlichen Anforderungen bestehen. zu a) Als Systemzeit sollte entweder die lokale Zeit, CET oder UTC verwendet werden. Für alle Systeme, die direkt oder indirekt an externe Partner angebunden sind, sollte der genutzte Standard mit diesen abgestimmt werden. Ausfälle der Verfügbarkeit des Zeitsignals bzw. der externen Zeitsynchronisierung sollten keine bzw. nur wohldefinierte Auswirkungen auf leittechnische Funktionen haben. zu d) Beispiele: abgewiesener Befehl wegen Zeitdifferenz/Befehlsalter, Einlogversuche mit falschem Passwort.
Betriebsführungs-/ Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	zu a) Im Stationsbereich sollte systemintern UTC verwendet werden. Die Ein- und Ausgabe sollte dann in der konfigurierbaren Ortszeit erfolgen. zu b) Die Protokollierung kann z.B. im Betriebsprotokoll erfolgen. zu e) Für Schutz- und Automatisierungskomponenten erfolgt das Logging i.d.R. auf Ebene der übergeordneten Systeme. Im Umfeld der dezentralen Stationstechnik sollte eine Speicherung in der Station und eine Synchronisation bzw. Übertragung auf eine Zentrale vorgesehen werden. zu f) siehe e)
Organisatorische Anmerkungen:	Um eine zielgerichtete Verwaltung der Logfiles zu gewährleisten, sollten die Kriterien dafür in einem Logging-Betriebskonzept festgelegt werden.

2.4.7 Self-Test und System-Verhalten

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ❑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Das System sollte bei Fehlern oder einfachen Manipulationen in einen sicheren Betriebszustand übergehen. Bei der Konzeption des Systems ist ein sicherer Betriebszustand bei Fehlern festzulegen. Das System sollte bei erkannten Versagen der o.g. Konsistenzprüfungen oder sicherheitsrelevanter Komponenten eine Warnung ausgeben und den Vorfall protokolieren.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	In der Regel ist es im Stationsbereich ausreichend, wenn die Systeme sich selbst überwachen und bei Fehlerzuständen einen Alarm absetzen. Weiterführende Aktionen sind i.d.R. nicht notwendig.
Organisatorische Anmerkungen:	-

2.5 Entwicklung, Test und Rollout

2.5.1 Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse

Sicherheits-anforderungen	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 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.

Ausführungshinweise betreffen:	Produkt- / Systementwicklung:	Projektplanung / -umsetzung:	Produkt- / Systemservice:	Systembetrieb:
	Ja ☑	Ja ❑	Ja ☑	Ja ❑

Ergänzungen und Anmerkungen:

Anerkannte Vorgehensmodelle und Standards sollten im Entwicklungsprozess angewendet werden. Die angewandten Prozesse und Aktivitäten sollten umfassend dokumentiert werden.

Sichere Softwareentwicklung setzt kein bestimmtes Entwicklungsmodell zwingend voraus, ggf. müssen aber die notwendigen sicherheitsbezogenen Entwicklungsschritte und Aktivitäten angepasst und in die vorhandene Entwicklungsmethodik integriert werden.

zu a)

Besonders die Weitergabe von projektspezifischen Entwicklungen an Subunternehmen bedarf der schriftlichen Zustimmung des Auftraggebers/Betreibers, da Spezifika der Anlagen des Auftraggebers/Betreibers nicht ungeschützt verbreitet werden dürfen.

zu b)

Die Entwicklung und das Testen sollten so weit wie möglich auf vom Produktivsystem getrennten Test- und Entwicklungssystemen erfolgen.

zu d)

Es sollten auch routinemäßige Kontrollen des Quellcodes mit automatisierten Prüftools durchgeführt werden. Diese Prüfung sollte möglichst automatisiert in den Entwicklungsprozess integriert werden.

Beispiele für anerkannte Entwicklungs- und Qualitätsmanagementstandards und Initiativen:

- BSI – Build Security In
- BSIMM – Building Security In Maturity Model
- CERT Secure Coding Standards
- CMMI - Capability Maturity Model Integration
- EFQMM - European Foundation for Quality Management Model
- ISO 9001
- Microsoft SDL - Security Development Lifecyle
- OWASP
- SAFECode
- SAMM – Software Assurance Maturity Model
- Software Assurance Consortium

	• Software Engineering Body of Knowledge • V-Model
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungs-technik / Sprach-kommunikation:	-
Sekundär-, Auto-matisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:	**-**

2.5.2 Sichere Datenhaltung und Übertragung

Sicherheits-anforderungen	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 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ❑
Ergänzungen und Anmerkungen:	Alle Informationen und Daten des Auftraggebers, die dem Auftragnehmer im Rahmen seiner Tätigkeit bekannt werden bzw. anfallen, sollten zunächst als vertraulich behandelt werden, bis sie vom Auftraggeber anderweitig klassifiziert worden sind[2]. Hiervon sollten nur offensichtlich nicht vertrauliche Informationen ausgenommen sein. In Zweifelsfällen sollte der Auftragnehmer eine Klassifizierung durch den Auftraggeber anzufordern. Vertrauliche und sicherheitsrelevante Projektinformationen sollten generell verschlüsselt übertragen werden.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungstechnik / Sprachkommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	-			

[2] Siehe Anhang A „Datenklassifikation“.

Organisatorische Anmerkungen:	Es sollten vertragliche Regelungen getroffen werden, nach denen der Verlust von Daten oder Datenträgern bzw. missbräuchliche Verwendung oder missbräuchlicher Zugriff umgehend dem Auftraggeber/Betreiber zu melden ist. Das „notwendige Minimum“ der Datenspeicherung sowie die Art der Datenhaltung und Übertragung sollte in einer Vereinbarung zwischen Auftraggeber/Betreiber und Auftragnehmer geregelt werden.

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

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ❑
Ergänzungen und Anmerkungen:	Die Entwicklungssysteme und -umgebungen sowie die Test- und Staging-Systeme sollten immer nach Stand der Technik gesichert und vom allgemeinen Unternehmensnetz getrennt sein. Ein Zugriff auf unsichere Netze, z.B. zur Internet- oder Mailnutzung sollte von den genannten Systemen nicht möglich sein. Ist für die Entwickler ein solcher Zugriff notwendig, sollten die Systeme, von denen der Zugriff erfolgt von der Entwicklungsumgebung umfassend abgeschottet sein, z.B. durch die Nutzung von Virtualisierungslösungen. Alle Entwicklungssysteme sollten anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet sein. Alle Entwicklungssysteme sollten über einen aktuellen Schadsoftwareschutz verfügen und mit allen aktuellen Sicherheitspatches versehen sein. Die Entwicklungssysteme und -umgebungen sowie die Test- und Staging-Systeme sollten mit einem sicheren logischen Zugangsschutz versehen sowie vor unberechtigten physischen Zugriff geschützt sein. zu c)			

		Dort, wo dies technisch nicht anders möglich ist, ist eine Ablage der Projektierungsdaten auf dem Produktivsystem erlaubt. Ein ausreichender Schutz gegen unerlaubte Veränderung sollte vorgesehen werden. Ein Staging- bzw. Test-System (z.B. als Testsäule aus Redundanzkomponenten) sollte generell vorgesehen werden. Bei der Korrektur nach einem Fehlerfall kann es notwendig sein, die konkreten Rahmenbedingungen herzustellen, um die Korrektur des Fehlers zu überprüfen. Diese Rahmenbedingungen sind ggf. im Test-System nicht immer nachbildbar. Eine Fehleranalyse ist ggf. auch nur im Produktiv-System sinnvoll. Dies beinhaltet in der Regel aber nur das Debuggen des Fehlers - ein vollumfänglicher Entwicklungszyklus inklusive Anwendungs-Kompilierung kann zu weitreichenden Störungen führen. Ebenso ist die korrekte Versions- und Änderungskontrolle stark erschwert. Vor einer Fehleranalyse und Tests im Produktiv-System sollten immer eine individuelle Risikoabschätzung und eine formale Freigabe durch den Betreiber erfolgen.
	Betriebsführungs-/ Leitsysteme und Systembetrieb:	zu b) Vor der Inbetriebnahme darf eine Entwicklung auf den späteren Produktivsystemen erfolgen. Nach erfolgter Inbetriebnahme sollte dies nicht mehr geschehen. zu c) Zur Fehleranalyse („Debugging“) kann die temporäre Installation des Quellcodes hilfreich sein. Nach Abschluss der Fehlerbehebung sollte der Quellcode wieder entfernt werden, um Manipulationen der Leitsystemanwendung zu verhindern. Eine weitere Möglichkeit ist die Nutzung eines netzwerkbasierten Debuggers. Der hierfür notwendige Dienst sollte aber nur temporär aktiviert werden und gegen unbefugte Zugriffe geschützt sein.
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	zu b) Systementwicklung, Tests, etc. finden i.d.R. beim Lieferanten statt. Ggf. kann dort eine Auftraggeber-bezogene Testumgebung bereitgehalten werden. Vor der Inbetriebnahme darf eine Entwicklung auf den späteren Produktivsystemen erfolgen. Nach erfolgter Inbetriebnahme sollte dies nicht mehr geschehen.
Organisatorische Anmerkungen:		**-**

2.5.4 Sichere Update- und Wartungsprozesse

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ❑
Ergänzungen und Anmerkungen:	Der Stellenwert der Systeme der Energieversorgung ist gesellschaftlich, soziologisch und ökonomisch sehr hoch. Um einen sicheren und zuverlässigen Betrieb zu gewährleisten, ist es deshalb i.d.R. notwendig, schnelle Reaktionszeiten zu ermöglichen sowie gleichzeitig einen definierten und geregelten Wartungsprozess einzuhalten. zu a) Updates und Patches sollten vom Hersteller immer überprüft und freigegeben sein. Sie sollten zudem vorab auf einem Testsystem getestet werden. Insbesondere bei Individualentwicklungen bietet sich hierfür ein mehrstufiges Vorgehen an: 1. Der Hersteller prüft auf Basis des zugrundeliegenden Standardprodukts. 2. Test und Freigabe durch den Hersteller erfolgen auf einer Testumgebung, die dem System des Betreibers möglichst entspricht. 3. Gegebenenfalls prüft der Betreiber bzw. der Hersteller im Auftrag des Betreibers Updates und Patches auf dem eigenen System entsprechend eines vorher definierten Testplans. Unter Umständen sollte eine mehrstufige Inbetriebnahme vorgesehen werden, die es im Fehlerfall ermöglicht, den Betrieb aufrecht zu erhalten (vgl. 2.1.1.3). In Abhängigkeit von der Kritikalität der betroffenen Systeme sollte im Rahmen der Wartungsprozesse durch den Betreiber geprüft werden, ob bestimmte Änderungen nicht per Fernzugriff sondern vor Ort durchgeführt werden müssen.			

		zu b) Die für Vor-Ort- und Fernwartung genutzten Systeme sollten nach aktuellem Stand der Technik gesichert sein. Die Sicherung sollte insbesondere die folgenden Punkte umfassen: • Die Wartungssysteme sollten mit einem sicheren logischen Zugangsschutz versehen sowie vor unberechtigten physischen Zugriff geschützt sein. • Die Wartungssysteme sind anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik zu härten. • Fernwartungszugriffe sollten nur aus einer abgesicherten und gegen unberechtigte Zugriffe geschützten DMZ-Umgebung erfolgen. • Mobile Systeme zur Vor-Ort-Wartung sollten mit einer restriktiv konfigurierten Firewallsoftware geschützt werden. • Die Wartungssysteme sollten beim Wartungszugriff über einen aktuellen Schadsoftwareschutz verfügen und mit allen aktuellen Sicherheitspatches versehen sein.
	Betriebsführungs-/ Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		-

2.5.5 Konfigurations- und Change-Management, Rollbackmöglichkeiten

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ☑	Ja ☑	Ja ☑	Ja ❑

Ergänzungen und Anmerkungen:	Sind im Laufe des Systembetriebs nicht-triviale Konfigurations- oder Parametrierungsänderungen zu erwarten, sollte das System ein ausreichendes Konfigurations- und Changemanagement unterstützen. Insbesondere sollte ein Rollback auf eine festzulegende Anzahl von vorhergehenden Konfigurationszuständen möglich sein. zu a) Die entsprechenden Prozesse sollten vorgesehen werden. zu b) Eine Sicherung von mindestens einem älteren Datenstand (Parametrier- und Firmwarestand, Datenmodell, etc.), sowie eine Rollbackmöglichkeit sollten vorgesehen werden. Alle Änderungen sollten dokumentiert werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	Eine Rollbackmöglichkeit sollte auf Anwendungsebene für dynamische und statische Daten vorgesehen werden. Für Software- und Systembasisänderungen sollten alle Änderungen und Erweiterungen projektspezifisch verwaltet werden.
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	Aufgrund des eingeschränkten Speicherausbaus der aktuellen Gerätetechnik sind Rollback-Möglichkeiten auf Ebene der Schutz- und Automatisierungskomponenten häufig noch nicht realisierbar. Die Sicherung von Parameter- und Firmwareständen sollte aber über die Bedien- und Wartungsprogrammen der Geräte möglich sein.
Organisatorische Anmerkungen:	Die Anforderung gilt sowohl für den Lieferanten als auch für den Auftraggeber/Betreiber. Auf Betreiberseite sollten die für eine Konfigurations- und Changemanagement notwendigen Prozesse definiert und

	realisiert werden.

2.5.6 Behandlung von Sicherheitslücken

Sicherheits-anforderungen	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 Sicherheitslücken 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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ❑

Ergänzungen und Anmerkungen:	Die zu vereinbarenden Prozesse zum Schwachstellenmanagement sollten u.a. festlegen, wie der Auftraggeber zeitnah über aktuelle Sicherheitsprobleme, die sein System oder Teilkomponenten betreffen könnten, informiert wird.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:	Die Meldung und Information durch den Auftragnehmer zu Schwachstellen und Sicherheitslücken erfolgt i.d.R. als Dienstleistung, deren genauer Umfang individuell in einem Service- und Wartungsvertrag festgelegt wird.

2.5.7 Sourcecode-Hinterlegung

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:** Ja ❑	**Projektplanung / -umsetzung:** Ja ☑	**Produkt- / Systemservice:** Ja ❑	**Systembetrieb:** Ja ❑
Ergänzungen und Anmerkungen:	Die Umsetzung dieser Sicherheitsanforderung ist insbesondere im Rahmen von Individualprojekten und bei projekt- bzw. kundenspezifischen Erweiterungen und Anpassungen sinnvoll. Wird hierbei seitens des Lieferanten einer Sourcecode-Hinterlegung nicht zugestimmt, sollte ein Service-Vertrag abgeschlossen werden, der zum Inhalt hat, dass ein separates Referenzsystem mit dem gesamten Sourcecode beim Lieferanten vorgehalten wird. Generell sollten projektspezifische Parametrierungen, Änderungen und Anpassungen dem Auftraggeber vollständig und umfassend dokumentiert ausgehändigt werden.			
Betriebsführungs- / Leitsysteme und Systembetrieb:	-			
Übertragungs-technik / Sprach-kommunikation:	-			
Sekundär-, Automatisierungs- und Fernwirktechnik:	Im Bereich der Schutz- und Automatisierungstechnik stehen der Aufwand für Anpassungen am Sourcecode und eine entsprechende Hinterlegung i.d.R. in keinem sinnvollen Verhältnis zum Ersatz von defekten Komponenten bzw. einer Anlagenanpassung.			
Organisatorische Anmerkungen:	Die entsprechenden Regelungen sollten in den Liefer- bzw. Service- und Wartungsverträgen berücksichtigt werden.			

2.6 Datensicherung/-wiederherstellung und Notfallplanung

2.6.1 Backup: Konzept, Verfahren, Dokumentation, Tests

Sicherheits-anforderungen	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 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).

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ❑

Ergänzungen und Anmerkungen:	Die Datensicherung sollte alle relevanten Daten umfassen. Hierzu gehören z.B. statische Daten (Parameter, Applikations- und System-Konfigurationen), dynamische Daten (Handeingaben, Nachführungen, etc.). In der Regel werden Prozessdaten nicht im Rahmen der regelmäßigen Backups gesichert. Unter Umständen können Archivdaten wie Langzeitarchive und die Systeminstallationen ebenfalls in die Datensicherung einbezogen werden. Der genaue Umfang der zu sichernden Daten sollte vom Auftraggeber definiert werden. Es sollten maximale Sicherungs- und Rücksicherungszeiten definiert werden. Die Sicherungsverfahren sollten dabei so konzipiert sein, dass die in der geplanten Systemlaufzeit zu erwartende Datenmenge in den definierten Zeiten gesichert und rückgesichert werden können. Es sollten Mechanismen vorgesehen werden, mit denen die Vollständigkeit und Korrektheit einer Datensicherung geprüft werden kann. Die Datensicherungs- und Rücksicherungsverfahren sollten ausführlich dokumentiert werden. Im Rahmen des Abnahmetests sollte eine vollständige Sicherung und Rücksicherung mit realistischen Datenmengen geprüft werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	Es sollte insbesondere eine zyklische Sicherung aller manuell eingegebenen Daten (Verfügungserlaubnis, Meldesperre, usw.) vorgesehen werden.

	Übertragungs-technik / Sprach-kommunikation:	Für prozessnahe Komponenten und Embedded-Systeme sollten Verfahren beschrieben und exemplarisch getestet werden, mit denen volatile Daten (z.B. Parametrierdaten) bei Tausch einzelner Komponenten, aber auch bei größeren Ausfällen zeitnah in Ersatzgeräte eingespielt werden können. In der Regel ist hier eine Import/Export-Möglichkeit für die Parametrierdaten ausreichend.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	
Organisatorische Anmerkungen:		-

2.6.2 Notfallkonzeption und Wiederanlaufplanung

Sicherheits-anforderungen	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.

Ausführungshinweise betreffen:	**Produkt- / Systementwicklung:**	**Projektplanung / -umsetzung:**	**Produkt- / Systemservice:**	**Systembetrieb:**
	Ja ❑	Ja ☑	Ja ☑	Ja ☑

Ergänzungen und Anmerkungen:	Relevante Notfall- und Krisenszenarien sollten auf Seiten des Betreibers bzw. Auftraggebers im Rahmen eines bereichsübergreifenden Risiko- und Notfallmanagements identifiziert und bewertet werden. Hierbei sollte eine Klassifikation der Funktionen und Applikationen nach der Wichtigkeit der Geschäftsprozesse mit einem besonderen Augenmerk auf der gesicherten Betriebsführung in den Anlagen erfolgen. Für die identifizierten Szenarien sollten Notfallkonzepte und Wiederanlaufplanungen vorgesehen werden. Im Rahmen der Systemplanung sind die in der Notfallplanung definierten maximalen Ausfall- und Wiederanlaufzeiten zu berücksichtigen. Der Auftragnehmer sollte für die relevanten Szenarien die für Wiederanlauf und Notbetrieb notwendigen Mechanismen vorsehen und im Rahmen der Projekt- und Systemdokumentation die notwendigen Informationen zur Verfügung stellen. Eine genaue Dokumentation der Abläufe für den Notfall sollte vorliegen. Sowohl der Notbetrieb als auch der Wiederanlauf aus relevanten Störszenarien sollten in der Abnahme als Testpunkte umfassend geprüft werden. Die Wiederherstellungszeiten sollten dabei ermittelt und mit den im Rahmen der Notfallplanung definierten Maximalzeiten abgeglichen werden. Eine in der System- bzw. Sicherheitsdokumentation hinterlegte Vorgehensweise zum Wiederaufsetzen des Gesamtsystems aus Einzelkomponenten unter Beachtung der ggf. notwendigen Rücksicherungen der Backups von Parametrier- und Betriebsdaten kann ggf. als ausreichend angesehen werden. Dies ist durch den Auftraggeber zu prüfen.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-

	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Auto-matisierungs- und Fernwirktechnik:	-
Organisatorische Anmerkungen:		Auf Betreiberseite sollten Wiederanlaufplanung und die Notfallkon-zepte zyklische geprüft und ggf. angepasst werden.

Anhang

A Datenklassifikation

A.1 Beispiel einer Klassifikation

Die Daten eines Unternehmens haben jeweils unterschiedliche Vertraulichkeitsgrade. Je nach Vertraulichkeit muss der Umgang mit diesen Daten auf unterschiedlichem Niveau abgesichert werden. Um hier ein unternehmensweit einheitliches und angemessenes Vorgehen sicher zu stellen, sollte eine Klassifikationsrichtlinie verabschiedet werden. Die Inhalte und Ziele einer solchen Klassifikationsrichtlinie sind:

- einheitliche und nachvollziehbare Kriterien zur Einstufung von Daten in definierte Vertraulichkeitsstufen
- geregelte Kennzeichnung von klassifizierten Daten
- einheitlicher und adäquater Umgang mit klassifizierten Daten (z.B. bei Speicherung, elektronischem oder postalischem Versand, im persönlichen Gespräch oder bei der Vernichtung)

Im Folgenden wird beispielhaft ein mögliches Datenklassifikations-Schema beschrieben:

Klasse 1: Public / öffentliche Daten

Daten der Klasse 1 sind öffentliche Daten und nicht besonders schutzwürdig. Dies umfasst alle Informationen, die bereits aus öffentlich zugänglichen Quellen stammen oder, sofern das eigene Unternehmen Gegenstand dieser Informationen ist, aktiv und rechtmäßig vom Unternehmen veröffentlicht wurden.

Klasse 2: Interne Daten

Daten der Klasse 2 sind interne Daten. In diese Klasse fallen alle Daten, die nicht in eine der anderen beiden Klassen einzuordnen sind.

Klasse 3: Vertrauliche Daten

Daten der Klasse 3 sind vertrauliche Daten. Dies umfasst generell alle Informationen, deren Weitergabe an unberechtigte Dritte das Unternehmen und das Kundenvertrauen nachhaltig schädigen können. Ferner umfasst dies auch alle Daten, deren Vertraulichkeit aufgrund gesetzlicher, vertraglicher oder regulatorischer Anforderungen zu gewährleisten ist. Beispiele für Informationen in dieser Vertraulichkeitsklasse sind:

- allgemeine Betriebs- und Geschäftsgeheimnisse
- Kalkulationen und Kalkulationsgrundlagen für den Wettbewerb am Markt
- Verträge oder Vertragsentwürfe
- Technische Informationen über Kritische Infrastrukturen oder andere sensible Systeme
- Sozialdaten und andere personenbezogene Daten
- Datenverarbeitung im Kundenauftrag mit Vertraulichkeitsauflagen

Sollte es ein Unternehmen für erforderlich halten, so können auch noch weitere Vertraulichkeitsklassen definiert werden. Dies ist zum Beispiel dann der Fall, wenn das Unternehmen Daten verarbeitet, für die aus gesetzlichen Gründen die Geheimhaltungsstufen „Verschluss“ bzw. „VS-Vertraulich“ oder höher festgelegt wurden.

Die nachstehende Tabelle gibt einen beispielhaften Überblick zur Kennzeichnung und Handhabung klassifizierter Daten:

Klasse	Tätigkeit	Kennzeichnung	Umgang
Öffentlich	Ablage / Speicherung	- keine	- keine Vorgaben
	Druck	- keine	- keine Vorgaben
	Übertragung / Versand	- keine	- keine Vorgaben
	Verbale Kommunikation	- keine	- keine Vorgaben
	Vernichtung	-	- keine Vorgaben
Intern	Ablage / Speicherung	- keine	- innerhalb des Unternehmens keine besonderen Vorgaben - außerhalb muss der Betreffende in eigenem Ermessen für einen angemessenen Zugriffsschutz sorgen
	Druck	- keine	- innerhalb des Unternehmens keine besonderen Vorgaben - außerhalb darf der Druck nicht unbeaufsichtigt erfolgen
	Übertragung / Versand	- keine	- innerhalb des Unternehmens keine besonderen Vorgaben - bei Faxversand an Empfänger außerhalb des Unternehmens ist entweder der Zeitpunkt der Sendung abzustimmen und eine Bestätigung des Empfangs erforderlich oder es ist die ausschließliche Zuordnung des Faxgerätes zu berechtigten Empfängern gewährleistet
	Verbale Kommunikation	- keine	- innerhalb des Unternehmens oder telefonisch keine besonderen Vorgaben - außerhalb des Unternehmens sind Mithörer im öffentlichen Raum zu vermeiden (Zug, Flughafen, etc.)
	Vernichtung	-	- Nutzung der bereitgestellten Datenvernichtungscontainer

Klasse	Tätigkeit	Kennzeichnung	Umgang
Vertraulich	Ablage / Speicherung	- Datenträger mit dem Begriff „Vertraulich“ kennzeichnen	- elektronische Daten sind generell zu verschlüsseln - Ablage in Papierform nur in separat abschließbaren Behältnissen - Mitnahme in Papierform außerhalb des Unternehmens erfordert Einzelfallgenehmigung
	Druck	- Dokumente mit dem Begriff „Vertraulich“ kennzeichnen	- generell kein unbeaufsichtigter Druck - Nutzung verschlüsselter Netzwerkdrucker mit Jobfreigabe per PIN oder lokale Einzelplatzdrucker ohne Netzanbindung
	Übertragung / Versand	- Dokumente mit dem Begriff „Vertraulich“ kennzeichnen - bei Postversand keine Kennzeichnung des äußeren Umschlags, zusätzlichen inneren Umschlag mit Kennzeichnung „Vertraulich“ verwenden	- ausschließlich verschlüsselter Versand, auch innerhalb des Unternehmens - keine vertraulichen Inhalte in unverschlüsselten Bestandteilen der Datenübertragung (z.B. Betreff einer E-Mail)
	Verbale Kommunikation	- verbale Ankündigung vor Gesprächsbeginn, dass vertrauliche Informationen Gegenstand sind	- keine vertraulichen Gespräche im öffentlichen Raum - keine Nutzung unverschlüsselter Telefonverbindungen - ggf. Verbot von Mobiltelefonen und ähnlichen Geräten in Besprechungsräumen
	Vernichtung	-	- Nutzung der bereitgestellten Datenvernichtungscontainer - Nutzung sicherer Löschverfahren bei elektronisch gespeicherten Informationen

A.2 Schützenswerte Daten nach dem Datenschutzgesetz

Alle Daten, die direkt oder durch Verknüpfung einer natürlichen Person zugeordnet werden können, werden als personenbezogene Daten bezeichnet. Diese Daten genießen einen besonderen Schutz, damit die betroffene Person ihr Recht auf informationelle Selbstbestimmung wahrnehmen und selbst entscheiden kann, wer wann welche Informationen über sie erhält.

Auf europäischer Ebene ist der Datenschutz durch die Richtlinie 95/46/EG geregelt. Sie wird im Bereich der elektronischen Datenverarbeitung ergänzt durch die Richtlinie 2002/58/EG, die hierzu speziellere Anforderungen enthält. Konkrete Umsetzungsvorgaben finden sich entsprechend in den landesspezifischen Gesetzgebungen. Diese werden im Allgemeinen auch detaillierte Vorgaben zur Erhebung, Speicherung, Verarbeitung, Weitergabe und Vernichtung der Daten sowie zur Protokollierung dieser Vorgänge umfassen.

Es ist daher zu entscheiden, ob eine gesonderte Klassifikation wie z.B. „Personenbezogen“ erforderlich ist, um die regelkonforme Handhabung dieser Daten sicher zu stellen. Des Weiteren ist bei Projekten, bei denen die Verarbeitung von personenbezogenen Daten geplant ist, im Rahmen der Projektplanung frühzeitig der Datenschutzbeauftragte des Unternehmens mit einzubeziehen.

B Abkürzungsverzeichnis und Glossar

Dieses Kapitel umfasst alle Abkürzungen und Begriffserklärungen aus dem vorliegende Best-Practice-Papier und dem als Basis dienenden BDEW-Whitepaper.

2-Faktor-Authentifizierung	Authentifizierung unter Verwendung zweier verschiedener Authentifizierungsmechanismen, z. B. Password und Chipkarte
3rd Party-Produkte	Standard-Software bzw. –Hardware, die vom Systemlieferanten zugekauft wird, z.B. Datenbank, Compiler, Rechner, Netzwerk-komponenten, usw.
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	Betriebssystem / Firmware inklusive Grundkomponenten wie z.B. 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 Konfigurati-onsänderungen gesteuert und verwaltet wird
CET	Central European Time, mitteleuropäische Zeit
COBIT	Control Objectives for Information and Related Technologies, international anerkanntes Framework zur IT-Governance
DCOM	Distributed Component Object Model
Directory Service	Ein Verzeichnisdienst, der einem Netzwerk eine zentrale Sammlung an bestimmten Daten zur Verfügung stellt, z.B. User-namen, Berechtigungen, u.ä.
DSG	Datenschutzgesetz

DL	Dienstleister
DMZ	Demilitarized Zone, isolierte Netzwerkzone zwischen Sicherheitszonen unterschiedlichen Schutzniveaus, in der die Sicherheitssysteme angesiedelt sind, die die Kommunikation zwischen den Zonen 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 (Deutschland)
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 gewährleistet sind
Gateway	Ein Gateway ermöglicht die Verbindung von Komponenten oder Netzwerken, die auf unterschiedlichen Protokollen basieren
Gesamtsystem	Im vorliegenden Dokument alle vom Hersteller gelieferten Hard- und Software-Komponenten, z. B. Applikationen, Betriebssysteme, Firmware, Rechnersysteme und die Netzwerk-Infrastruktur
GOOSE	Generic Object Oriented Substation Events
HW	Hardware
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
ISO 27002	ISO-Standard für Informationssicherheit
IT	Informationstechnologie
ITIL	IT Infrastructure Library, eine Sammlung von Best Practices bzw. Good Practices in einer Reihe von Publikationen, die eine mögliche Umsetzung eines IT-Service-Managements beschreiben und inzwischen international einen de-facto-Standard darstellen
LAN	Local Area Network

Lifecycle	Lebenszyklus eines Systems beginnend mit der Planung, über die Ausschreibung, die Implementierung, Inbetriebnahme, den eigentlichen Betrieb, bis hin zur Demontage
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
Netzwerk-Perimeter	Netzwerksystem, das den Übergang zu einem externen Netzwerk bildet, z. B. ein Router, eine Firewall oder ein RAS-System
NTP	Network Time Protocol
Out-Of-Band-Kommunikation	Kommunikation, die nicht die primäre, zur Nutzdatenkommunikation vorgesehene Kommunikationsanbindung nutzt
OPC	In der Automatisierungstechnik häufig genutzte Kommunikationsschnittstelle
Patchmanagement	Managementprozess, mit dem das Testen, Installieren, Verteilen und Dokumentieren von Sicherheitspatches und Software-Updates gesteuert und verwaltet wird
PKI	Public Key Infrastructure
Port	Kommunikationsendpunkt, der Datenströme eines Netzwerkprotokolls bestimmten Applikationen oder Diensten zuordnet
Profibus	Process Field Bus, Standard für die Feldbuskommunikation in der Automatisierungstechnik
Profinet	Industrieller Ethernet-Standard, u.a. zur Echtzeit-Kommunikation
Proxy	Computersystem, das den Datenverkehr zwischen zwei getrennten Datennetzen vermittelt und ggf. auch überwacht und filtert
RDP	Remote Desktop Protocol
RAS	Remote Access Service
Rollback	Das vollständige Zurücksetzen eines IT-Systems in einen definierten Ausgangszustand, z.B. vor Durchführung eines Softwareupdates
Rolle	siehe Benutzerrolle
SCP	Secure Copy,
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell Protocol, verschlüsseltes Terminalprotokoll

SSL	Secure Socket Layer
Staging	Dedizierte Testumgebung, an der System- und Software-Änderungen geprüft werden, bevor sie produktiv umgesetzt werden.
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	Transmission Control Protocol
Telnet	Nicht verschlüsseltes Netzwerkprotokoll zum zeichenorientierten Datenaustausch über eine TCP-Verbindung, häufig für interaktiven Zugriff auf Betriebssystemebene genutzt
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTC	Universal Time Coordinated, koordinierte Weltzeit
V-Model	Vorgehensmodell für die Planung und Durchführung von Systementwicklungsprojekten
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
XML	Extensible Markup Language
XSS	Cross Site Scripting, in Umfeld von Webapplikationen häufig vorkommender Schwachstellentyp, der zum Angriff auf Clientsysteme genutzt werden kann

C Referenzen und Verweise

C.1 Normen

ISO/IEC 27000 Reihe “Information technology — Security techniques — Information security management systems”:

ISO/IEC 27000:2009(E): “Information technology — Security techniques — Information security management systems — Overview and vocabulary”

ISO IEC 27001:2005: "Information technology — Security techniques — Information security management systems – Requirements”

ISO IEC 27002:2005: "Information technology — Security techniques — Code of practice for information security management”

ISO/IEC 27003:2010 “Information technology — Security techniques — Information security management system implementation guidance”

ISO/IEC 27004:2009 “Information technology — Security techniques — Information security management – Measurement”

ISO/IEC 27011:2008 “Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002”

ISO/IEC 27031:2011 “Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity”

ISO/IEC 27033 Part 1 “Information technology — Security techniques — Network security”

ISO/IEC 27035:2011 “Information technology — Security techniques — Information security incident management”

DIN ISO/IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2005)“

DIN ISO/IEC 27002 “Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2005)“

IEC 62351 Reihe “Power systems management and associated information exchange - Data and communications security”:

IEC/TS 62351-1 “Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues “

IEC/TS 62351-2: "Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms"

IEC TS 62351-3: "Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP”

IEC TS 62351-4: "Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS"

IEC/TS 62351-5: "Power systems management and associated information exchange – Data and communications security – Part 5: Security for IEC 60870-5 and derivatives”

IEC TS 62351-6: "Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850"

IEC TS 62351-7: “Power systems management and associated information exchange – Data and communication security – Part 7: Network and system management (NSM) data object models"

IEC 61850-7-2 “Communication networks and systems for power utility automation - Part 7-2: Basic information and communication structure - Abstract communication service interface (ACSI)”

ISO/IEC 62443 / ANSI/ISA-99 Reihe "Industrial communication networks - Network and system security”:

IEC/TS 62443-1-1 “Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models”

IEC 62443-2-1 “Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program”

IEC/PAS 62443-3 “Security for industrial process measurement and control - Network and system security“

IEC/TR 62443-3-1 “Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems”

C.2 Frameworks und Handlungsempfehlungen

COBIT (Control Objectives for Information and Related Technology):

Cobit ist ein international anerkanntes Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives (oft mit Kontrollziel übersetzt, eigentlich Steuerungsvorgaben, in der aktuellen deutschsprachigen Version wird der Begriff nicht mehr übersetzt). CobiT definiert hierbei nicht vorrangig, wie die Anforderungen umzusetzen sind, sondern primär darauf, was umzusetzen ist.

ITIL (IT Infrastructure Library):

Die IT Infrastructure Library (ITIL) ist eine Sammlung von Best Practices bzw. Good Practices in einer Reihe von Publikationen, die eine mögliche Umsetzung eines IT-Service-Managements (ITSM) beschreiben und inzwischen international als De-facto-Standard hierfür gelten. In dem Regel- und Definitionswerk werden die für den Betrieb einer IT-Infrastruktur notwendigen Prozesse, die Aufbauorganisation und die Werkzeuge beschrieben. Die ITIL orientiert sich an dem durch den IT-Betrieb zu erbringenden wirtschaftlichen Mehrwert für den Kunden. Dabei werden die Planung, Erbringung, Unterstützung und Effizienz-Optimierung von IT-Serviceleistungen im Hinblick auf ihren Nutzen als relevante Faktoren zur Erreichung der Geschäftsziele eines Unternehmens betrachtet. Aus deutscher Sicht werden die Inhalte vom itSMF Deutschland e.V. weiterentwickelt und verbessert, der zugleich eine Plattform zum Wissens- und Erfahrungsaustausch bietet und damit die IT-Industrialisierung vorantreibt.

NERC North American Electric Reliability Corporation:

Standard CIP-001-1 — Sabotage Reporting

Standard CIP-002-1 — Cyber Security — Critical Cyber Asset Identification

Standard CIP-003-1 — Cyber Security — Security Management Controls

Standard CIP-004-1 — Cyber Security — Personnel and Training

Standard CIP-005-1 — Cyber Security — Electronic Security Perimeter(s)

Standard CIP-006-1 — Cyber Security — Physical Security

Standard CIP-007-1 — Cyber Security — Systems Security Management

Standard CIP-008-1 — Cyber Security — Incident Reporting and Response Planning

Standard CIP-009-1 — Cyber Security — Recovery Plans for Critical Cyber Assets

NIST National Institute of Standards and Technology:

NIST Special Publication 800-53: “Recommended Security Controls for Federal Information Systems and Organization”

NIST Special Publication 800-40 Version 2.0: "Creating a Patch and Vulnerability Management Program”

NIST Special Publication 800-82: "Guide to Industrial Control Systems (ICS) Security”

DHS Department of Homeland Security:

Cyber Security Procurement Language for Control Systems

CPNI Centre for the Protection of National Infrastructure:

Process Control and SCADA Security Guide 1-7