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

Österreichs E-Wirtschaft
Brahmsplatz 3
1040 Wien
Österreich

Verband Schweizerischer Elektrizitätsunternehmen
Hintere Bahnhofstrasse 10
5000 Aarau
Schweiz

Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme

Vollständig überarbeitete Version 3.0 09/2024:

Aarau/Berlin/Wien, 30. September 2024

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
2.0	Mai 2018	Grundlegende Aktualisierung und Überarbeitung (Projektteam Oesterreichs Energie / BDEW)
3.0	September 2024	Grundlegende Aktualisierung und Überarbeitung Version 3.0 (Projektteam Oesterreichs Energie / VSE / BDEW)

Gemeinsame Herausgeber

Österreichs E-Wirtschaft

Brahmsplatz 3, 1040 Wien, Österreich

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32, 10117 Berlin, Deutschland

Verband Schweizerischer Elektrizitätsunternehmen

Hintere Bahnhofstrasse 10, 5000 Aarau, Schweiz

Ansprechpartner

Armin Selhofer (Österreichs E-Wirtschaft)

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

Markus Riner (Verband Schweizerischer Elektrizitätsunternehmen)

Fachliche Beratung und Unterstützung

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

Inhalt

1 Einleitung und Geltungsbereich

Das vorliegende Dokument definiert grundsätzliche Sicherheitsanforderungen für OT- und Telekommunikationssysteme für die Prozesssteuerung in der Energieversorgung und gibt Ausführungshinweise zu deren Umsetzung. Hierzu werden von Fachexperten zusammengestellte, aktuelle und branchenspezifische Empfehlungen zur Sicherstellung der Informationssicherheit aufgeführt.

Das Whitepaper definiert Anforderungen an Einzelkomponenten und für aus diesen Komponenten zusammengesetzte Systeme und Anwendungen. Ergänzend werden auch Sicherheitsanforderungen an Wartungsprozesse, Projektorganisation und Entwicklungsprozesse behandelt.

Fokus dieses Dokuments sind die im Rahmen der Beschaffung zu berücksichtigenden Anforderungen an technische Komponenten und Systeme und für die Projektabwicklung und Wartung relevanten Prozesse. Ebenso wichtig sind organisatorische, Personal- und physische Sicherheitsmaßnahmen im Unternehmen, wie der Aufbau einer Sicherheitsorganisation, ein angemessenes Risikomanagement oder die Schaffung eines umfassenden Sicherheitsbewusstseins bei den Mitarbeitern (Security Awareness). Diese organisatorischen Anforderungen stehen nicht im Fokus des Whitepapers, hierzu sei insbesondere auf die Normen ISO/IEC 27001 und ISO/IEC 27019 verwiesen.

Das vorliegende Dokument ist eine vollständig überarbeitete Neuauflage des BDEW-Whitepapers, in der die Inhalte gemäß aktuellen Technologieentwicklungen umfassend aktualisiert und ergänzt wurden.

In diesem Dokument werden unter dem Begriff *Operational Technology* (Abk. *OT*) alle in Tabelle 1 definierten und beschriebenen Technologiekategorien verstanden. Es wird darauf hingewiesen, dass keine allgemein anerkannte Definition des Begriffs OT existiert und diese sich abhängig von der Organisation unterscheiden kann. In Anhang B „Abkürzungsverzeichnis und Glossar“ sind weitere alternative Begriffsdefinitionen enthalten.

2 Gliederung und Aufbau

In diesem Dokument werden OT- und Telekommunikationssysteme für die Prozesssteuerung in der Energieversorgung als „Systeme“ bzw. als „Gesamtsystem“ bezeichnet. Diese Systeme sind in der Regel aus Einzelkomponenten zusammengesetzt. Einzelkomponenten können auch eigenständige Geräte sein, die (Teil-) Aufgaben in der Prozesssteuerung und Telekommunikation für die Energieversorgung übernehmen.

Die Anforderungen an das Gesamtsystem und die Einzelkomponenten sind in den Kapiteln 4.1 bis 4.8 thematisch gegliedert. In deren Unterkapiteln werden in der ersten Tabelle zunächst die konkreten Sicherheitsanforderungen definiert. Zu Beginn der Tabelle wird dabei auf die sogenannten Controls des Internationalen Standards ISO/IEC 27002:2022 *Information security controls* und dessen Erweiterung für den Energiesektor ISO/IEC 27019:2017 *Information security controls for the energy utility industry* verwiesen. Diese Referenzen dienen lediglich als Hinweis auf die in den Standards aufgeführte „Guidance“, die bei der Umsetzung der Whitepaper-Anforderungen zurate gezogen werden kann. Dabei ist zu beachten, dass sich die Systematik des

Whitepapers von der Normenreihe ISO/IEC 27000 unterscheidet. Die referenzierten Norm-Controls decken deshalb unter Umständen nur Teile der jeweiligen Anforderung des Whitepapers ab.

In der folgenden Tabelle werden dann im Abschnitt „Ergänzungen und Anmerkungen“ allgemeine Hinweise und Beispiele zur Umsetzung der Anforderungen gegeben, die alle Technologiebereiche im Bereich der OT in der Energieversorgung betreffen. Anschließend werden bei Bedarf 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 Energieversorgung dienen sowie die hierzu notwendigen unterstützenden zentralen IT/OT-Systeme, Anwendungen und die zugehörige zentrale Infrastruktur. Beispiele: • Zentrale Netzleit- und Netzführungssysteme • Kraftwerks-Leitsysteme • Zentrale Systeme zur Überwachung und Steuerung von verteilten Erzeugern und Lasten, z. B. virtuelle Kraftwerke, Speichermanagement, zentrale Leitwartensysteme für Wasserkraftwerke oder Photovoltaik-/Windenergieanlagen • Systeme zur Störungsannahme und zur Einsatzplanung • Zentrale Zähler- und Messwertverarbeitungssysteme • Datenarchivierungssysteme • Zentrale Parametrier-, Konfigurations- und Programmiersysteme • die für den Betrieb der o.g. Systeme notwendigen unterstützenden Systeme, wie z. B. Programmier- und Parametriergeräte
Übertragungstechnik / Sprachkommunikation:	Die in der OT zur Sprach- und Datenkommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik. Beispiele: • Router, Switches und Firewalls • Übertragungstechnische Netzelemente • Endgeräte der Sprachkommunikation • Telefonanlagen, 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 Safety-Systeme und fernwirktechnischen Komponenten. Hierzu gehören insbesondere die Technik in den dezentralen Stationen und Anlagen sowie die Automatisierungstechnik in Erzeugungs- und Speicheranlagen. Beispiele: • Steuerungs- und Automatisierungskomponenten • Leit- und Feldgeräte • Fernwirkgeräte • Controller und SPSen inklusive digitaler Sensor- und Aktorelemente • Schutzgeräte • Safety-Komponenten • Digitale Mess- und Zählvorrichtungen • Synchronisiergeräte • Erregungssysteme

Tabelle 1: Technologiekategorien

Hinweis: In diesem Papier werden mit dem Begriff „Auftragnehmer“ Akteure bezeichnet, an die nach Auftragsvergabe mittel- oder unmittelbar Sicherheitsanforderungen gerichtet sein können. Dazu gehören z. B. Hersteller, Lieferanten, Systemintegratoren oder externe Planer.

3 Anwendungshinweise

3.1 Systemplanung und Ausschreibung

Das vorliegende Whitepaper richtet sich sowohl an Hersteller, Lieferanten, Systemintegratoren und externe Planer auf Auftragnehmerseite als auch an unternehmensinterne Planer, Realisierer und Betreiber auf der Auftraggeberseite.

Beim Auftragnehmer sind die Anforderungen und Ausführungshinweise bereits für die Produkt- und Systementwicklung hilfreich und sollten deshalb entsprechend frühzeitig berücksichtigt werden. Dies betrifft insbesondere auch die Weiterentwicklung von Systemen und Komponenten über deren gesamten Lebenszyklus.

Auf der Auftraggeberseite wird empfohlen, in der Planungsphase eine frühzeitige Auswahl der notwendigen Sicherheitsanforderungen auf Basis einer individuellen Risikoanalyse durchzuführen. Aufbauend auf den Ergebnissen der Risikoanalyse ist dann für das geplante System detailliert zu spezifizieren, wie die einzelnen Anforderungen erfüllt werden sollen. Insbesondere in die-

ser Phase sollen die in den Kapiteln aufgeführten ergänzenden Umsetzungshinweise unterstützend wirken. Sofern IT-Umsysteme (z. B. Verzeichnisdienste, File-Server, Backupsysteme etc.) zum Liefer- und Leistungsumfang des Auftragnehmers gehören, sollten die damit verbundenen Sicherheitsanforderungen dieses Dokumentes ebenfalls erfüllt werden.

Ist das geplante Projekt zur Ausschreibung vorgesehen, werden nach Ende der planerischen Phase die ermittelten Sicherheitsanforderungen in das Lastenheft integriert. In der Ausschreibung sollten dann eine Kopie des Whitepapers, konkretisierte Anforderungen und zusätzliche Maßnahmen sowie Umsetzungsvorgaben und 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. Die Nicht-Anwendung von Maßnahmen ist durch die Planer, Realisierer bzw. Betreiber auf Auftraggeberseite im Rahmen einer Risikoanalyse zu bewerten und zu dokumentieren bzw. im Risikobehandlungsprozess zu bearbeiten.

Auftraggeber sollten berücksichtigen, dass derzeit keine durch die Herausgeber des Whitepapers anerkannten Verfahren zur Zertifizierung oder Konformitätsprüfung von Komponenten oder Systemen existieren und daher Angaben zur Whitepaper-Konformität durch den Auftraggeber kritisch geprüft werden müssen.

Es wird empfohlen, das Sicherheitskonzept des Gesamtsystems in der Konzeptions- und Pflichtenheftphase und bei wesentlichen Änderungen durch einen unabhängigen Experten zu prüfen.

3.2 Anwendung für Bestandssysteme

Die in diesem Whitepaper beschriebenen Sicherheitsmaßnahmen werden für alle neuen Steuerungs- oder Telekommunikationssysteme empfohlen. Eine Anwendung für Bestandssysteme ist aufgrund technologischer Beschränkungen häufig nur mit Einschränkungen möglich. Insbesondere bei Upgrades oder Erweiterungen sollten aber im Rahmen einer Risikoanalyse alle Umsetzungsoptionen geprüft, bewertet und ggf. ergänzende Sicherheitsmaßnahmen eingeplant werden. Das Whitepaper kann auch genutzt werden, um eine Gap-Analyse durchzuführen, um mögliche Risiken der Bestandssysteme zu identifizieren.

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 und Produkte. 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 Patch-Management, Schadsoftwareschutz oder Systemupgrades und Migrationen regeln. Hierfür sind in der Regel Wartungsverträge abzuschließen und verbindliche Vorgehensweise zur Migration festzulegen.

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

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 OT. Diese neuen und vielversprechenden Technologien können zu Kosteneinsparungen und zu Verbesserungen der Funktionalität führen. Allerdings müssen vor dem Einsatz neuer Technologien relevante Informationssicherheits-Aspekte hinreichend berücksichtigt, getestet und einer Risikobewertung unterzogen werden. Hierbei sollten verschiedene Themenpunkte betrachtet werden:

- Identifikation und Bewertung bekannter Sicherheitslücken und Schwachstellen
- Sicherstellung von Zuverlässigkeit und Stabilität im betrieblichen Einsatz
- Prüfung der Verfügbarkeit des Produkts bzw. zugehöriger Ersatzteile sowie ggf. Software-Patches über den Lebenszyklus der Systeme
- Bewertung der Abhängigkeiten von Fremdprodukten wie Open Source Bibliotheken oder proprietärer Software
- Patch-Politik des Auftraggebers über den Produktlebenszyklus
- Prüfung der Anpassungsfähigkeit im Lebenszyklus, z. B. an zukünftige kryptografische Algorithmen und Schlüssellängen
- Klärung der Komplexität im Sinne einer raschen Wiederherstellung des Normalbetriebes bei Störungen und Ausfällen
- Erfüllung der Vorgaben für den Echtzeitbetrieb
- Erfüllung der Safety-Vorgaben für Mensch und Umwelt auch bei hohen Security-Einstellungen am System
- Erwartungshaltung des Herstellers an die Anbindung des Produktes an öffentliche Netze o.ä. (Internetverfügbarkeit oder Cloud-Anbindung)
- Erfüllung der Erfordernisse im Sinne der Kritischen Infrastruktur bzw. Betreiber wesentlicher Dienste.

4 Sicherheitsanforderungen

4.1 Allgemeine Anforderungen

Dieses Kapitel definiert allgemeine und übergreifende Sicherheitsanforderungen, die für das Gesamtprojekt und alle Technologiebereiche anwendbar sind.

4.1.1 Sichere Systemarchitektur

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.3, 8.14, 8.22, 8.27, 8.30 ISO/IEC 27019:2017 13.1.3, 17.2.1 Die Einzelkomponenten und das Gesamtsystem müssen auf einen sicheren Betrieb hin entworfen und entwickelt werden. Zu den Prinzipen eines sicheren Systemdesigns gehören: **Security-By-Design:** Das Gesamtsystem und seine Einzelkomponenten werden von Grund auf im Hinblick auf Sicherheit entwickelt. Vorsätzliche Angriffe und unberechtigte Handlungen werden explizit betrachtet, die Auswirkungen von Sicherheitsvorfällen werden durch das Systemdesign minimiert. **Minimal-Need-To-Know-Prinzip**: Jede Komponente und jeder Benutzer erhält nur die Rechte, die für die Ausführung einer Aktion notwendig 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 Gesamtsystem 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).

Ergänzungen und Anmerkungen:	Sicherheitsanforderung 4.1.1 richtet sich in erster Linie an Systemdesigner und Entwickler und soll eine Leitlinie für das gesamte Systemdesign und den Entwicklungsprozess darstellen. Neben den genannten grundlegenden Sicherheitsprinzipien existieren weitere sinnvolle und ergänzende Designprinzipien, die ebenfalls berücksichtigt werden sollten, wie z. B. Access Control, Input Sanitization und -Validation, 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 Sicherheitsmechanismen kommen darf. In Hinblick auf Sicherheitsfunktionen ist hier insbesondere eine logische Redundanz im Sinne des Defence-in-Depth-Prinzips gemeint, nach dem das Gesamtsystem über mehrere, gestaffelte Sicherheitsfunktionen verfügen muss. Hieraus ist aber nicht zwingend abzuleiten, dass alle Komponenten im Sinne einer Hardware-Redundanz doppelt ausgelegt werden müssen. Beispiele für Maßnahmen zur Realisierung des Redundanz- und Defence-in-Depth-Prinzips: • Implementierung von Laufzeitüberwachungs-Mechanismen, z. B. Watch-Dogs, Exception-Handling etc. • Echtzeit-Schadsoftwareschutz auf den Systemkomponenten bei gleichzeitiger Prüfung aller Datenschnittstellen und Blockierung der nicht benötigten Datenträgerschnittstellen wie USB-Ports und Wechseldatenträgern • Deaktivierung oder besser Deinstallation von nicht benötigten Diensten, wie z. B. DHCP • Konsistenzprüfung von Daten sowohl an der Außenschnittstelle einer Anwendung als auch bei der Übergabe zwischen den verschiedenen Systemmodulen innerhalb der Applikation • Kommunikations-Gateways mit Prüffunktionen auf Applikations-Ebene, z. B. zur Filterung nach erlaubten bzw. nicht freigegebenen Telegrammtypen • Redundante Übertragungswege und Vermeidung von Verbindungen über das öffentliche Internet • 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 Systemdokumentation beschrieben werden.
	Betriebsführungs-/ Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.1.2 Patchfähigkeit und Patch-Management

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.8 Alle Systemkomponenten müssen patchfähig sein. Der Auftragnehmer muss einen Patch-Managementprozess für die Einzelkomponenten und das Gesamtsystem unterstützen, anhand dessen das Testen, Installieren und Dokumentieren von Sicherheits-Patches und Updates gesteuert und verwaltet werden kann. Sicherheits-Patches und Updates müssen durch den Betreiber selbst bzw. durch von ihm beauftragte Dienstleister installiert werden können. Das Installieren bzw. Deinstallieren von Patches muss vom Betreiber autorisiert werden und darf nicht automatisch geschehen. Die Installation bzw. Deinstallation ist im System nachvollziehbar und manipulationsgeschützt zu protokollieren. Die Integrität von Sicherheits-Patches und Updates muss durch einen kryptographischen Mechanismus prüfbar sein. Die Vorgehensweise zur Installation von Sicherheits-Patches sowie für Deinstallation und Rollback muss für alle Systemkomponenten detailliert dokumentiert werden. Die Patches müssen durch den Auftragnehmer eindeutig versioniert werden. Erfordert das Gesamtsystem bzw. seine Komponenten nach einem Update die Durchführung von Funktionstests, müssen diese nach technischer Möglichkeit automatisiert werden und die hierfür notwendigen Mechanismen im System vorgesehen sein. Der Auftragnehmer muss die notwendigen Testfälle und die bei einem erfolgreichen Testdurchlauf zu erwartenden Ergebnisse dokumentieren (Testbuch). Die im Rahmen des Patch-Managements durchgeführten Prozesse müssen sich an anerkannten Betriebs- und Servicemanagement-Standards orientieren. Der Auftragnehmer muss ein Patch-Management während der Projektlaufzeit über den Projektvertrag im Zuge der Vergabe implementieren. Das Patch-Management während der Betriebsphase wird typischerweise in einem separaten Wartungsvertrag vereinbart, siehe Abschnitt 4.7.5 „Wartungsvertrag / Service-Level-Agreement“.

Ergänzungen und Anmerkungen:	Unter Patchen wird das Implementieren von sicherheitsrelevanten und funktionalen Softwareupdates verstanden. Dies umfasst sowohl die reine Fehlerbeseitigung als auch die Erweiterung, Ergänzung und Optimierung von Funktionalitäten und betrifft sowohl die Anwendungsebene als auch alle unterlagerten Systemkomponenten (z. B. Basis- und Betriebssysteme, Datenbanken, Programmbibliotheken und Komponenten von Drittherstellern, Firmware, BIOS und Management-Schnittstellen usw.).

		Werden keine Komplettsysteme geliefert, sollten vom Auftragnehmer die notwendigen Prozesse und Voraussetzungen zur Installation von Sicherheits-Patches und sonstigen Updates für die im System genutzten Drittkomponenten genannt werden. 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. Daher sollten die Patches wenn möglich zuerst auf den inaktiven Redundanz-Komponenten eingespielt und nach einem Switch-Over-Prozess (Wechsel der aktiven Komponente im Redundanzsystem) und einem darauffolgenden Basis-Funktionstest bzw. Probelauf auf den restlichen Komponenten installiert werden. Insbesondere übergeordnete Systeme ohne direkte Prozess-Anbindung sollten dabei so ausgeführt werden, dass eine Außerbetriebnahme der Anlage zur Patch-Installation i. d. R. nicht notwendig ist. Das Gesamtsystem sollte so aufgebaut sein, dass die Anzahl der notwendigen Sicherheits-Patches bzw. der zu patchenden Komponenten sowie ggf. notwendiger Betriebsunterbrechungen auf ein Minimum reduziert werden kann. Eine umfassende Härtung kann hierbei unterstützend wirken (vgl. 4.3.1). Zur Durchführung von Funktionstests kann in Abhängigkeit von der Kritikalität der Systeme ein kundenspezifisches Testsystem beim Auftragnehmer und ggf. ein zusätzliches Testsystem beim Kunden notwendig sein. 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 Patch-Management sind auch Embedded-Komponenten, Parametrier- und Managementsysteme sowie Management-Schnittstellen zu berücksichtigen. Sollten Patches bestimmte Firmware-Stände erfordern, ist dies gesondert zu überprüfen und sicherzustellen. Zu den anerkannten Betriebs- und Servicemanagement-Standards gehören z. B. COBIT oder ITIL. In der Regel sind für das Patch-Management Administrationswerkzeuge und Systeme zum System- und Versionsmanagement notwendig (z. B. zentrale Update-Server, Versionierungs- und Konfigurationsmanagement-Datenbanken etc.). Hierfür sollte eine von der Business-IT getrennte Infrastruktur betrieben werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Bei hohen Verfügbarkeitsanforderungen sollten zur Sicherstellung eines kontinuierlichen Betriebs Redundanzkomponenten genutzt werden.

	Übertragungs-technik / Sprach-kommunikation:	Berücksichtigt werden sollten sowohl Netzwerkkomponenten und Netzelemente, Endgeräte und zentrale Kommunikations-, Management- und Überwachungssysteme.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	Die Installation von Sicherheits- und Firmware-Updates in prozessnahen Komponenten (z. B. Steuerungen, SPSen, Feldeinheiten, Schutzgeräten) ist unter Umständen nur während einer Anlagenaußerbetriebnahme, wie z. B. während einer Revision, möglich. Die Komponenten sollten beim Auftraggeber möglichst so ausgeführt sein, dass in diesen Fällen 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 Soft-/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.

4.1.3 Bereitstellung von Sicherheits-Patches für alle Systemkomponenten

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.8, 8.19 ISO/IEC 27019:2017 12.5.1, 12.6.1 Der Auftragnehmer muss gewährleisten, dass Sicherheitsupdates für alle Systemkomponenten während des gesamten, vertraglich geregelten Betriebszeitraums durch ihn im Rahmen des Patch-Managementprozesses bereitgestellt und ggf. installiert werden. Updates von Basiskomponenten, die nicht vom Auftragnehmer entwickelt wurden, wie z. B. Betriebssystem, Bibliotheken oder Datenbank-Managementsystem, muss der Auftragnehmer von den jeweiligen Herstellern beziehen, diese testen und sie gegebenenfalls an den Auftraggeber weiterleiten. Test, Freigabe und Bereitstellung der Updates müssen innerhalb eines angemessenen, vertraglich geregelten Zeitrahmens erfolgen.

Ergänzungen und Anmerkungen:	Der Bereitstellungsprozess sollte alle zum Lieferumfang gehörenden Software- und Systemkomponenten umfassen, z. B. Basis- und Betriebssysteme, Datenbanken, Programmbibliotheken und Komponenten von Drittherstellern, Firmware, BIOS und Management-Schnittstellen usw. Hierfür sollte der Auftragnehmer eine Inventarliste bereitstellen, in der die im Bereitstellungsprozess umfassten Softwarekomponenten für mindestens alle vernetzten Systemkomponenten ausgewiesen sind.

		Die Installation von Sicherheits-Patches und Updates erfordert i. d. R. eine individuelle Prüfung und Freigabe der einzelnen Patches und Updates durch den Auftragnehmer. Hierfür kann in Abhängigkeit von der Kritikalität der Systeme ein kundenspezifisches Testsystem beim Lieferanten und ggf. ein zusätzliches Testsystem beim Kunden notwendig sein. Für weniger kritische Anwendungen ist ggf. eine generische Freigabe bestimmter Patch- und Updatekategorien durch den Auftragnehmer möglich. Informationen über zu installierende Updates sollten dem Auftraggeber regelmäßig und zeitnah zur Verfügung gestellt werden (siehe 4.7.4 Schwachstellen-Management und Patchinformationsdienst). 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 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 Vorgehensweise zur Migration grob skizziert und vertraglich festgeschrieben werden. Für verbindliche Vereinbarungen zu diesem Thema, welche im Rahmen eines Wartungsvertrages abgeschlossen werden, siehe 4.7.5. „Wartungsvertrag / Service-Level-Agreement“. Es ist zu beachten, dass Redundanzkomponenten keine dedizierten Testsysteme ersetzen.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.1.4 Support für eingesetzte Systemkomponenten

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.8, 8.30 ISO/IEC 27019:2017 12.6.1 Der Auftragnehmer muss sicherstellen, dass sowohl für von ihm eigenentwickelte als auch für fremdentwickelte Systemkomponenten (z. B. Betriebssystem, Datenbank-Managementsystem, etc.) innerhalb des

	geplanten und vertraglich festgeschriebenen Betriebszeitraums Herstellersupport und Sicherheitsupdates zur Verfügung stehen. Das Abkündigungsverfahren und alle relevanten Mindestlaufzeiten wie z. B. Last-Customer-Shipping und End-Of-Support müssen verbindlich festgeschrieben werden. Der Securitysupport muss auch die für den Betrieb notwendigen Parametrier- und Konfigurationstools umfassen. Eine Konfiguration und Parametrierung muss für die definierte Laufzeit mit einem supporteten Parametrier- und Konfigurationstools möglich sein.

Ergänzungen und Anmerkungen:		Betriebszeiträume, die den Lebenszyklus von System- oder Softwarekomponenten überschreiten, erhöhen das sicherheitstechnische Risiko und sollten daher unbedingt vermieden werden. Die Auftragnehmer sollten den entsprechenden Support sowohl für selbst entwickelte als auch für 3rd-Party-Produkte bieten und bei Produkten mit langen Lebenszyklen bei Vertragsabschluss Vorgehensweisen zur Migration definieren. Es sollten zunächst nur Drittkomponenten (z. B. Betriebssystem, Protokoll-Stacks, etc.) genutzt werden, die aktuell und während der geplanten Laufzeit noch unterstützt werden. Aufgrund der üblicherweise langfristigen Betriebszeiträume in den betrachteten Bereichen kann der Auftragnehmer dies allerdings häufig nicht garantieren. Deshalb sollten an dieser Stelle Grobkonzepte und Kostenschätzungen für eine Migration auf neuere Versionen vorgelegt werden. Es sollte zusätzlich gefordert werden, dass bei Inbetriebnahme möglichst die zu diesem Zeitpunkt aktuellen System- und Komponentenversionen eingesetzt werden, falls dem keine betrieblichen Gründe des Betreibers entgegenstehen. Eine besondere Herausforderung stellen die stark unterschiedlichen Lebenszeiten der genutzten Drittsoftwarekomponenten und des gewünschten Lebenszyklus eines Systems 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.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.1.5 Verschlüsselung vertraulicher Daten

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.33, 5.34, 8.15, 8.21, 8.24 ISO/IEC 27019:2017 10.1.1, 12.4.2, 13.1.2, 18.1.3, 18.1.4 Vertrauliche Daten dürfen nur verschlüsselt gespeichert bzw. übertragen werden. Dort, wo der Schutzbedarf offensichtlich ist (z. B. bei Authentisierungsinformationen wie Passwörtern), müssen entsprechende Maßnahmen durch den Auftragnehmer bereits in der Standardkonfiguration umgesetzt sein.

Ergänzungen und Anmerkungen:		Beim Schutz vertraulicher Daten sollten sowohl Informationssicherheitsaspekte als auch Datenschutzanforderungen berücksichtigt werden. Eine Auflistung der vom System standardmäßig verarbeiteten Informationen sollte vom Auftragnehmer vorgelegt werden. Welche Daten als vertraulich anzusehen sind, ist durch den Auftraggeber festzulegen. Zu den zu schützenden Daten können beispielsweise Protokolldateien, Passwörter, Parametrierdaten, personenbezogene Daten oder vertrauliche Daten nach behördlichen Vorgaben oder den relevanten Gesetzen, wie z. B. dem Bundesdatenschutzgesetz oder Datenschutzgrundverordnung, gehören. Gegebenenfalls sollte das System auch die sichere, selektive Löschung bestimmter Daten, beispielsweise durch Überschreiben mit Zufallsdaten und die Anonymisierung bestimmter Daten, ermöglichen.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.1.6 Kryptographische Verfahren

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.33, 8.24 ISO/IEC 27019:2017 10.1.2, 13.1.4 ENR Bei der Auswahl von kryptographischen Verfahren sind nationale Gesetzgebungen zu berücksichtigen. Es dürfen nur anerkannte Verfahren und Schlüsselmindestlängen benutzt werden, die nach aktuellem Stand der Technik auch in Zukunft als sicher gelten. Die Nutzung von selbstentwickelten kryptographischen Algorithmen ist nicht erlaubt. Abweichungen hiervon dürfen nur nach expliziter Freigabe durch den Auftraggeber eingesetzt werden. Das gewählte kryptographische Verfahren muss, wo technisch möglich, durch ein neueres Verfahren im Rahmen eines Updates austauschbar sein bzw. es müssen veraltete Verfahren deaktiviert oder deinstalliert werden können. Bei der Implementierung der kryptographischen Verfahren muss, wo technisch möglich, auf anerkannte Bibliotheken zurückgegriffen werden, um Implementierungsfehler zu vermeiden.

Ergänzungen und Anmerkungen:	Als Stand der Technik von Verfahren für Hashbildung, Signaturen und Verschlüsselung und die zugehörigen Schlüssellängen werden insbesondere die BSI-Empfehlungen der TR-02102-Reihe „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (Bundesamt für Sicherheit in der Informationstechnik, Deutschland) angesehen. Insbesondere im Embedded-Bereich müssen bei der Spezifikation von Algorithmen und Schlüssellängen allerdings die teilweise beschränkten Ressourcen der Komponenten berücksichtigt werden. Die Normenreihe IEC 62351 definiert für ihren Anwendungsbereich Mindestanforderungen an die zu unterstützenden kryptographischen Verfahren. Bei der Auswahl der im Projekt aktivierten und genutzten Verfahren sollte diese zusammen mit den o.g. BSI-Empfehlungen berücksichtigt werden. Für Schlüsselverwaltung, Erzeugung von Zufallszahlen etc. kann der Einsatz von kryptographischen Hardware-Modulen wie eines Trusted Platform Module (TPM) sinnvoll sein. Bei der Auswahl der kryptographischen Verfahren sollten Entwicklungen der Post-Quanten-Kryptographie berücksichtigt werden, siehe hierzu z. B. die BSI-Veröffentlichung *Kryptografie quantensicher gestalten*.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungs-technik / Sprach-kommunikation:	-

	Sekundär-, Automatisierungs- und Fernwirktechnik:	

4.1.7 Public Key Infrastructure

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.24 ISO/IEC 27019:2017 10.1.2 Sofern im System digitale Zertifikate eingesetzt werden, muss eine PKI etabliert sein. Die Nutzung von nicht-vertrauenswürdigen, selbst-signierten Zertifikaten (s.u.) ist nicht erlaubt. Alle kryptographischen Schlüssel und Zertifikate müssen durch den Betreiber ersetzbar sein. Zudem muss auch die Integration einer vom Betreiber bereitgestellten PKI möglich sein. Die für den Zertifikatsaustausch notwendigen Prozesse sind in der Systemdokumentation vollständig zu dokumentieren. Für das AutoEnrollment von X.509-Zertifikaten müssen sichere Verfahren wie z. B. SCEP oder EST genutzt werden. Vor der Nutzung von Zertifikaten ist deren Gültigkeit und Authentizität zu prüfen, beim Aufbau verschlüsselter Verbindungen ist dies durch beide Kommunikationspartner beidseitig zu prüfen. Als ungültig oder fehlerhaft erkannte Zertifikate und Zertifikatsketten dürfen nicht akzeptiert werden. Beim Einsatz einer PKI bzw. von digitalen Zertifikaten müssen potenzielle Ausfall- und Notfallszenarien berücksichtigt werden, wie u. a. der Ausfall von PKI-Systemen oder die Ungültigkeit von digitalen Zertifikaten. Für diese Szenarien sollten Kernprozesse (bspw. Anmeldeprozesse von Nutzern oder von Diensten) weiterhin möglich sein. Wenn eine vom Lieferanten oder Dritten betriebene PKI genutzt wird, müssen folgende Punkte vertraglich geregelt werden: • Sichere Erzeugung von Schlüsselmaterial • Sichere Speicherung / Archivierung von Schlüsselmaterial • Sichere Löschung / Vernichtung von Schlüsselmaterial • Zugriffsschutz und physische Sicherheit für die o. g. Prozesse • Definition und Dokumentation einer Sicherheitsrichtlinie für den Einsatz kryptografischer Verfahren und Produkte

Ergänzungen und Anmerkungen:		Selbst-signierte Zertifikate sind nicht von einer vertrauenswürdigen CA, sondern mit dem zum Zertifikat gehörigen privaten Schlüssel signiert. Sie können somit nicht einfach verifiziert werden. Wenn eine vom Lieferanten oder Dritten betriebene PKI genutzt wird und erhöhte Sicherheitsanforderungen bzw. erhöhter Schutzbedarf bestehen, kann eine Verpflichtung auf Umsetzung der BSI TR-03145-1 sinnvoll sein. Für die Zertifikatsprüfung sollen automatisch im System verteilte CRLs oder OCSP / OCSP-Stapling genutzt werden. Alternativ kann eine sehr kurze Zertifikatslebenszeit (wenige Stunden bis Tage) und ein kurzzyklischer, automatisierter Roll-Out-Prozess vorgesehen werden. Die System-Komponenten sollten eine Warnmeldung erzeugen, wenn ein Zertifikat in weniger als 180 Tagen ausläuft. Anwendungsfälle für digitale Zertifikate umfassen z. B. die Absicherung von Netzwerkkommunikation (TLS), Code-Signing, E-Mail-Verschlüsselung und -signierung per S/MIME oder Server- und Client-Authentisierung.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.1.8 Sichere Standard-Konfiguration

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.9, 8.18, 8.19, 8.33 ISO/IEC 27019:2017 12.5.1 Das Gesamtsystem 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 und Accounts, 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. Sind in der Systemumgebung des Betreibers gegenüber der Standard-Installation noch weitere Sicherheitseinstellungen, Konfigurationen, etc. notwendig, müssen diese explizit dokumentiert werden.

Ergänzungen und Anmerkungen:		
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.1.9 Integritäts-Prüfung

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.19, 8.25, 8.32 Systemdateien, Anwendungen, Konfigurationsdateien und Anwendungs-Parameter müssen auf Integrität überprüft werden können, beispielsweise durch kryptographische Prüfsummen.

Ergänzungen und Anmerkungen:	Neben den Systemdateien des Betriebssystems sollten insbesondere Konfigurationsdaten, Anwendungsparameter sowie Firmware-Parameter und Firmware-Versionen sicher auf Integrität geprüft werden können. Um gezielte Manipulationen verhindern bzw. erkennen zu können, sind hierzu i. d. R. kryptographisch berechnete Prüfsummen notwendig. Durch den Auftraggeber definierte Komponentenparameter sollten automatisiert auslesbar sein (z. B. durch standardisierte Schnittstellen für Asset-Management-Werkzeuge oder durch das Engineering-Tool). Dabei darf kein Rücklesen der Firmware oder der Parametrierungs-/Engineering-Daten möglich sein, welches Reverse-Engineering ermöglicht. Nach Möglichkeit sollten die Prüfungen für Patches und Updates die gleichen Mechanismen nutzen (vgl. 4.1.2). Die Möglichkeit zur Integritätsprüfung auf der Ebene übergeordneter Systeme sollte eine Mindestanforderung sein. Mittelfristig sollte die Möglichkeit zur Integritätsprüfung auf allen Komponenten angestrebt werden. Die Integritätsprüfungen sollten insbesondere auch im Rahmen der Change-Management-Prozesse berücksichtigt 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 Firmware-Versionen vorhanden sein. Eine Vergleichbarkeit von Parametrierständen insbesondere von Offline- und Onlineversionen und archivierten Parametrierungen sollte angestrebt werden. Dabei sollte erkennbar sein, an welchen Datenbereichen Änderungen vorgenommen wurden.

4.1.10 Nutzung von Cloud-Diensten

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 5.22, 5.23 ISO/IEC 27019:2017 15.1.2 Bei der Nutzung von Cloud-Diensten sind die folgenden Anforderungen zu berücksichtigen: a) Mit dem Cloud-Dienstleister müssen Vereinbarungen getroffen werden, welche sicherheitsrelevante Prozesse für den Betrieb der Cloud-Infrastruktur regeln. b) Funktionen zur Steuerung kritischer Infrastrukturen, deren Manipulation/Veränderung die Energieversorgung gefährden kann, dürfen nicht in Cloud-Diensten realisiert werden, die nicht unter Kontrolle des Betreibers liegen (die Kontrolle des Betreibers muss dabei die Datenhoheit und die Kontrolle über Administration und Verfügbarkeit umfassen). c) Der Ausfall eines Cloud-Dienstes bzw. des Zugriffs auf diesen Dienst darf zu keinen wesentlichen Einschränkungen der definierten Grundfunktion des Systems führen. Störungen und Ausfälle des Cloud-Dienstes müssen auch in der Notfallkonzeption und Wiederanlaufplanung berücksichtigt werden (siehe 4.8.2).

Ergänzungen und Anmerkungen:	Cloud-Dienste im hier verwendeten Sinn umfassen die dynamische Nutzung von geteilten IT-Ressourcen und IT-Dienstleistungen wie Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen (z. B. Applikationsserver, Datenbanken), Software und Anwendungen über ein Netzwerk. Die Nutzung von Cloud-Diensten im Bereich der OT in der Energieversorgung ist nicht grundsätzlich abzulehnen, muss aber im Rahmen

	einer Risikobewertung kritisch hinterfragt werden. Dies gilt insbesondere bei der Nutzung von öffentlichen Cloud-Diensten (Public Cloud). Zur Risikobewertung sollte eine Cloud-Referenzarchitektur herangezogen werden, um sicherstellen zu können, dass alle relevanten Aspekte der Cloud-Nutzung und deren Risiken berücksichtigt werden. Bei der Nutzung von Cloud-Diensten gibt der Eigentümer der Daten die eigentliche Datenhoheit an den Cloud-Dienstleister ab. Er muss sich in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit auf die sichere Umsetzung des Dienstes verlassen können. Bei einer Verarbeitung oder Speicherung von Daten mit erhöhten Sicherheitsanforderungen bezüglich Verfügbarkeit, Integrität und Vertraulichkeit ist dabei besondere Sorgfalt geboten. Die konkrete Umsetzung von sicherheitsrelevanten Prozessen für einen sicheren Betrieb aufseiten des Cloud-Dienstleisters ist nicht immer transparent. Das betrifft unter anderem das Patch-Management, das Backup, den Infrastrukturschutz, die sichere Datenübertragung und die Mandantentrennung in der Cloud-Infrastruktur. Bei der Speicherung im Ausland sind sich ändernde lokale rechtliche Regelungen nicht einschätzbar bzw. vorhersehbar. Hier besteht unter Umständen die Gefahr, dass Daten für Dritte zugänglich werden. Es sollte geprüft werden, ob Daten, die in einem Cloud-Dienst verarbeitet oder gespeichert werden, in die Backup-Konzeption des Betreibers aufgenommen werden müssen. zu a) Es sollten insbesondere die folgenden Themen verbindlich geregelt werden: • Authentisierung/Autorisierung der Zugriffe • Mandantenfähigkeit / Trennung der Kundendaten • Festlegung zur Datenübertragung (Verschlüsselung / Integritätsschutz) und zur Kommunikationsanbindung zwischen Kunden und Cloud-Dienstleister • Datensicherung und -wiederherstellung • Schutz der Dienstleister-Infrastruktur • Sichere Speicherung der Daten • Schwachstellen- und Patch-Management der Cloud-Infrastruktur • Personalsicherheit • Physische Sicherheit der Rechenzentren und Zutrittsschutz • Ort der Leistungserbringung durch den Cloud-Dienstleister • Vorgaben zum Incident Handling • Schadsoftwareschutz • Sicherstellung der Datenlöschung • Notfallvorsorge • Möglichkeit der Dienstleisterauditierung • Protokollierung und Überwachung

		Empfehlungen zur Absicherung von Cloud-Diensten sind in den internationalen Standards ISO/IEC 27017:2015 *Code of practice for information security controls based on ISO/IEC 27002 for cloud services* und ISO/IEC 27018:2019 *Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* definiert. Anforderungen an Cloud-Dienstleister sind auch in der *Checkliste zur Auswahl eines Cloud-Dienstes* und im *Kriterienkatalog Cloud Computing C5* des Bundesamts für Sicherheit in der Informationstechnik definiert. Dabei ist zu beachten, dass eine Zertifizierung des Cloud-Dienstleisters gemäß diesen Normen in der Regel nicht hinreichend ist, sondern ergänzende verbindliche Vereinbarungen zu den o.g. Themen notwendig sind. zu c) Cloud-Dienste können beispielsweise durch Störungen der Internet- bzw. Cloud-Anbindung ausfallen. Das entsprechende Risiko kann durch eine direkte RZ-Anbindung an den Cloud-Anbieter reduziert werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	

4.1.11 Anforderungen an die Dokumentation

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.8, 5.37, 6.3, 8.27 ISO/IEC 27019:2017 12.1.1, 14.1.1 Eine Design-Dokumentation muss bereits in der Engineering-/Pflichtenheftphase erstellt, durch den Auftraggeber abgenommen und diesem übergeben werden. Die Design-Dokumentation muss nachvollziehbar beschreiben, wie die vertraglich vereinbarten Sicherheitsanforderungen umgesetzt werden. Dabei muss eine Rückverfolgbarkeit zwischen den einzelnen im Projekt definierten Sicherheitsanforderungen und den Kapiteln bzw. den Inhalten der Design-Dokumentation hergestellt werden. Für Einzelkomponenten und Gesamtsysteme muss in der Design-Dokumentation eine Beschreibung aller sicherheitsrelevanten Systemeinstellungen und Parameter sowie ihrer Standardwerte und ggf. projekt-

	spezifischer Einstellungen enthalten sein. Außerdem werden sicherheitsspezifische Implementierungsdetails aufgelistet und kurz beschrieben (z. B. verwendete kryptographische Verfahren). Für ein Gesamtsystem sind zusätzlich Informationen über die Systemarchitektur in der Design-Dokumentation zu dokumentieren. Dies umfasst den grundsätzlichen 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. Dem Auftraggeber muss spätestens zur Abnahme eine projektspezifische Betriebs-Dokumentation übergeben werden. Die Dokumentation von potenziell vertraulichen Informationen, z. B. Zugangsdaten wie Passwörter oder Portfreigaben, darf nicht in der allgemeinen System- oder Sicherheitsdokumentation erfolgen, sondern muss dem Auftraggeber separat in gesicherter Form übergeben werden. Außerdem muss die Dokumentation auf Konsequenzen von grob unsicheren Konfigurationseinstellungen hinweisen. Die Dokumentation muss eine Beschreibung der Voraussetzungen für einen sicheren Systembetrieb enthalten.

Ergänzungen und Anmerkungen:	Der Auftragnehmer sollte eine Sicherheitsdokumentation erstellen, in der alle für den Betrieb relevanten Informationen zusammengefasst sind. Neben der konkreten Sicherheitskonfiguration und der zugehörigen Parameter sollten z. B. auch System- und Kommunikationseinstellungen wie maximale Anzahl gleichzeitig angemeldeter Nutzer, maximale Anzahl von Netzwerkverbindungen, minimale Netzwerkbandbreiten usw. dokumentiert werden. Die Dokumentation sollte über den gesamten Projektverlauf aktuell gehalten werden. Typischerweise wird zwischen Design-Dokumentation und Betriebsdokumentation unterschieden. Die Design-Dokumentation beschreibt dabei grundlegende Architektur- und Sicherheitsaspekte, während die Betriebsdokumentation betriebliche Details (z. B. durch Bedienanleitungen) beschreibt. Dabei wird davon ausgegangen, dass in der Betriebsdokumentation keine Festlegungen getroffen werden, die den Sicherheitsanforderungen widersprechen. Es sollten getrennte Dokumentationen für den Administrator und die System-Benutzer existieren. Beide Dokumentationen sollten für die jeweiligen Gruppen unter anderem eine Auflistung der sicherheitsrelevanten Einstellungen und Funktionen enthalten und Hinweise für sicherheitsverantwortliches Handeln nennen. Außerdem sollten alle sicherheitsspezifischen Log- und Audit-Meldungen erläutert und mögliche Ursachen sowie gegebenenfalls passende Gegenmaßnahmen genannt werden.

		Zur Beschreibung der Voraussetzungen für einen sicheren Systembetrieb gehören unter anderem Anforderungen an den Benutzerkreis, Netzwerkumgebung sowie Interaktion und Kommunikation mit anderen Systemen und Netzwerken. Ebenfalls kann dies Anforderungen an die physische Sicherheit und Umgebungsparameter wie Klimatisierung, Energieversorgung, EMV-Schutz, Brand- und Havarieschutz, etc. umfassen. Die aktuelle Dokumentation sollte verfügbar sein, z. B. für den Bereitschaftsdienst. Die Prüfung der Dokumentation sollte Teil der Abnahmeprüfung sein. Die Design- und Betriebsdokumentation sollte die folgenden Themen umfassen: • Systemarchitektur (z. B. Leittechnik-Konfigurator, System-Konfigurator etc.) • Netzwerk-Diagramme und Listen (Übersicht als Topologie bis hin zum Detailplan inkl. Netzwerklisten z. B. VLAN-Übersicht, je nach Projektphase unterschiedliche Detailtiefen notwendig) • Kommunikationsmatrix • Firewall-Regelwerk • Asset-Inventar (Hardware, Software) • physische sowie logische Schnittstellen, • Systembeschreibungen (Funktionale High-Level-Beschreibung der Systeme) • Software Bill of Materials (Software-Stücklisten), z. B. nach BSI TR-03183-2 • Beschreibung der Sicherheitsmaßnahmen (von Pflichtenheft bis hin zur Übergabedokumentation) • Security-Risikoanalysen aus Sicht des Integrators
	Betriebsführungs-/ Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	In der Regel sind sicherheitsrelevante Parameter und Meldungen projektspezifisch und im Zuge der Anlagenplanung zu dokumentieren.

4.1.12 Physische Sicherheit

Sicherheitsanforderungen	ISO/IEC 27002:2022 7.8, 7.9 ISO/IEC 27019:2017 11.1.7 ENR, 11.1.8 ENR, 11.1.9 ENR, 11.3.1 ENR

	Sofern schützenswerte Systemkomponenten an Orten platziert werden, bei denen der Zutritt von nicht befugten Personen nicht ausgeschlossen ist, müssen Maßnahmen ergriffen werden, die den unbemerkten physischen Zugang zu den Systemkomponenten verhindern.

Ergänzungen und Anmerkungen:		Solche Maßnahmen können bspw. umfassen: • Verschlossene und öffnungsüberwachte Schränke • Manipulationsgeschütze Gehäuse mit Öffnungsüberwachung • Gehärtete Konfiguration lokaler Schnittstellen Die Öffnungsüberwachung sollte Alarme an eine dauerhaft besetzte Stelle melden, z. B. Leitstelle oder SOC.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.1.13 Integration in Systeme zur Erkennung von Anomalien und Angriffen

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.15, 8.16 ISO/IEC 27019:2017 12.4.1 Das Systemdesign muss für die Integration in Systeme zur Erkennung von Anomalien und Angriffen ausgelegt sein. a) Sofern die Netzwerkhardware zum Liefer- und Leistungsumfang des Auftragnehmers gehört, muss es möglich sein, den gesamten Netzwerkverkehr rückwirkungsfrei an einen bzw. mehrere Sensoren(en) auszuleiten, z. B. per Mirror-Port oder Netzwerk-TAP. b) Bei der Nutzung von Mirror-Ports darf sich eine Überbuchung nicht negativ auf die Systemfunktion und -performance auswirken. c) Auf Server- / PC-basierten Komponenten muss es möglich sein, hostbasierte Sensoren zu installieren. d) Es muss möglich sein, die Meldungen der Schadsoftwareschutzlösung in ein Angriffserkennungssystem bzw. SIEM zu integrieren (siehe 4.3.2 Schadsoftware-Schutz). Die Datenübertragung muss kryptographisch gesichert (verschlüsselt, authentisiert und integritätsgesichert) erfolgen.

	e) Es muss möglich sein, die Log- und Protokollierungs-Meldungen der Systemkomponenten und des Gesamtsystems in ein Angriffserkennungssystem bzw. SIEM zu integrieren (siehe 4.5.6 Logging). Die Datenübertragung muss kryptographisch gesichert (verschlüsselt, authentisiert und integritätsgesichert) erfolgen. f) Alle für die Angriffserkennung maßgeblichen Sicherheitsrelevanten Ereignisse (SRE) und betrieblichen Ereignisse müssen dokumentiert sein. Sofern keine systemspezifischen SRE definiert sind, ist ein Verweis auf die Dokumentation der Vorlieferanten, z. B. der Betriebssystemhersteller hinreichend. g) Es muss ein Baselining etabliert werden, um festzustellen, welche SRE im Normalzustand auftreten.

Ergänzungen und Anmerkungen:		Es sollte möglich sein, dass Gesamtsystem bzw. seine Einzelkomponenten technisch aktiv ohne Verfügbarkeitseinschränkungen nach Hinweisen für Kompromittierung (Indicators of Compromise) und auf Integrität analysieren zu können. Dazu gehören Portscans, Schwachstellenscans und Inventarisierungsscans. Der Einsatz von Intrusion-Prevention-Systemen wird nur nach Durchführung einer Risikoanalyse empfohlen. Sicherheitsrelevante Ereignisse (SRE) sollten in einem standardisierten Format ausgetauscht werden. Sofern bei Patches, Upgrades oder anderen Änderungen Logmeldungen angepasst werden, sollte dies kommuniziert werden (z. B. im Changelog). Zu c) Der Lieferant soll die einzusetzenden hostbasierten Sensoren auf Kompatibilität mit seinem System testen und diese bestätigen.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.2 Projektorganisation

Dieses Kapitel definiert Anforderungen an die Projektorganisation und den Projektablauf, insbesondere an die in Form von Projekten durchgeführten Aktivitäten für die Planung, Realisierung und Inbetriebnahme von Systemen und Komponenten. Das Kapitel umfasst Grundanforderungen an die Benennung von Ansprechpartnern und die operativen Mindestmaßnahmen, die in der Umsetzung von Projekten durchgeführt werden sollten. Die Vorgabe einer Projekt-Management-Methodik ist nicht Gegenstand dieser Unterlage.

4.2.1 Ansprechpartner

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.2, 5.8, 5.20, 5.22 Der Auftragnehmer muss einen Ansprechpartner definieren, der während der Angebotsphase, der System-Entwicklung und während des geplanten Betriebs- und Wartungszeitraumes für den Bereich der IT/OT-Sicherheit verantwortlich ist. Für den Fall der Abwesenheit muss eine Vertretung vorgesehen werden.

Ergänzungen und Anmerkungen:		Bei entsprechender Unternehmensgröße sollten die Aufgaben in den verschiedenen Bereichen und Projektphasen von mehreren Mitarbeitern wahrgenommen werden. Auf Projektebene ist für diesen Fall ein einzelner Verantwortlicher zu benennen, der dem Auftraggeber als primärer Ansprechpartner dient.
	Betriebsführungs-/ Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.2.2 Sicherheits- und Abnahmetests

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.22, 8.29, 8.30 Vor der Abnahme bzw. Übergabe müssen die einzelnen Systemkomponenten und wesentlichen Funktionen des Gesamtsystems einem umfangreichen Sicherheits- und Stresstest unterzogen werden. Diese internen Sicherheitstests müssen nachweislich vom Auftragnehmer an einer repräsentativen Konfiguration durchgeführt werden. Zusätzlich zu den internen Sicherheitstests müssen zur Sicherheitsfreigabe des Gesamtsystems eine vom Entwicklungsteam unabhängige Organisationseinheit Security-Abnahmetests durchführen. Die Ergebnisse sowie die dazugehörige Dokumentation (Softwarestände, Prüfkonfiguration, etc.) der internen Tests und der Security-Abnahmetests müssen dem Auftraggeber zur Verfügung gestellt werden. Im Rahmen beider Testarten muss die effektive und vollständige Umsetzung der vorgesehenen Sicherheitsmaßnahmen geprüft werden und ggf. vorhandene oder in der aktuellen Konzeption nicht angemessen berücksichtigte Schwachstellen identifiziert werden. Der Auftraggeber hat das Recht, die Security-Abnahmetests auch selbst vorzunehmen oder durch einen externen Dienstleister durchführen zu lassen. Art und Umfang der Abnahmetests werden durch den Auftraggeber festgelegt. Dem Auftraggeber bzw. dem von ihm Beauftragten ist für die Prüfungen ein Systemzugriff mit den technisch maximal möglichen Zugriffsrechten einzuräumen. Zwischen Auftraggeber und Auftragnehmer muss vor der Test-Durchführung das Vorgehen zur Behebung von festgestellten Abweichungen (einschließlich Zeitplan) für beide Testarten festgelegt werden. Ebenfalls sind die Eckpunkte der durchzuführenden Tests sowie die Erfüllungskriterien abzustimmen.

Ergänzungen und Anmerkungen:	In der Auslieferungsdokumentation sollte die Dokumentation der Sicherheitstests in einer für eine Bewertung hinreichenden Detailtiefe enthalten sein. Der Umfang und die Testtiefe sollten je nach Systemkomplexität und -kritikalität von einfachen Stichproben bis hin zu einer vollständigen Auditierung reichen. Entsprechende Sicherheitsprüfungen sollten auch während des Betriebszeitraums regelmäßig wiederholt werden. Bei Standardkomponenten ist im Regelfall eine Typprüfung pro Produkt-Release 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 übereinstimmt. Hierzu sollten bei der Inbetriebnahme die Einstellungen entsprechend einem Typprüfungsprotokoll überprüft werden.

		Die Sicherheits- und Anforderungsprüfungen aufseiten der Auftraggeber und Auftragnehmer sollten auch Last- und Stresstests beinhalten. Im Rahmen der Sicherheits- und Abnahmetests sollte die Integrität des zu prüfenden Systems gegen ungewünschte Veränderungen sichergestellt werden. Gegebenenfalls ist eine Neuinstallation nach dem Test vorzusehen. Die Anzahl und die Abstufung von Security-Abnahmetests („Pre-FAT“, „FAT“, „SAT“, „SAT Stufe II“) sollte sich am projektweiten Vorgehen zu den Abnahmetests orientieren. Ziel der Abnahmetests ist die Sicherheitsfreigabe durch den Auftraggeber, sie sind daher nicht als Qualitätssicherungsmaßnahmen mit anschließendem Verbesserungsprozess anzusehen – dies muss der Auftragnehmer durch die vorab durchgeführten internen Sicherheitstests gewährleisten.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Leitsysteme und zentrale Betriebsführungssysteme sind häufig angepasste Individualentwicklungen und sollten i. d. R. bei der Abnahme explizit durch eine vollständige Auditierung überprüft werden.
	Übertragungstechnik / Sprachkommunikation:	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.

4.2.3 Sichere Datenspeicherung und Übertragung

Sicherheitsanforderungen	ISO/IEC 27002:2022 5.14, 6.6, 7.10, 8.1, 8.24, 8.33 ISO/IEC 27019:2017 6.2.1 Vertrauliche Daten des Auftraggebers, die im Entwicklungs- und Wartungsprozess benötigt werden oder anfallen, dürfen über ungeschützte Verbindungen nur verschlüsselt übertragen werden. Bei einer Speicherung auf mobilen Datenträgern oder Systemen dürfen solche Daten nur verschlüsselt gespeichert werden. Die Menge und die Dauer der Aufbewahrung der gespeicherten Daten müssen auf ein vertraglich festzulegendes Minimum beschränkt sein.

	Alle Informationen und Daten des Auftraggebers, die dem Auftragnehmer im Rahmen seiner Tätigkeit bekannt werden bzw. anfallen, müssen zunächst als vertraulich bzw. projektintern behandelt werden, bis sie vom Auftraggeber anderweitig klassifiziert worden sind. Es müssen vertragliche Regelungen getroffen werden, nach denen der Verlust von Daten oder Datenträgern bzw. die missbräuchliche Verwendung oder der missbräuchliche Zugriff umgehend dem Auftraggeber/Betreiber zu melden ist.

Ergänzungen und Anmerkungen:	Hiervon sollten nur offensichtlich nicht vertrauliche Informationen ausgenommen sein. In Zweifelsfällen sollte der Auftragnehmer eine Klassifizierung durch den Auftraggeber anfordern. Das betrifft z. B. interne Informationen und Dokumente des Auftraggebers, aber auch Protokolldateien, Fehleranalysen und relevante Systemdokumentation. Die als vertraulich bzw. projektintern anzusehenden Daten, das „notwendige Minimum“ der Datenspeicherung sowie die Art der Datenhaltung und Übertragung sollte in einer Vereinbarung zwischen Auftraggeber/Betreiber und Auftragnehmer geregelt werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.2.4 Übergabe projektspezifischer Anpassungen

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.30 Bei Individualprojekten und bei projekt- bzw. kundenspezifischen Erweiterungen, Anpassungen und Engineering-Dienstleistungen müssen alle projektspezifischen Parametrierungen, Änderungen und Anpassungen dem Auftraggeber vollständig und umfassend dokumentiert ausgehändigt werden.

Ergänzungen und Anmerkungen:		Gegebenenfalls sollte die Hinterlegung des Quellcodes und der entsprechenden Dokumentation bei einem Treuhänder vereinbart werden, um beispielsweise im Falle einer Insolvenz des Auftragnehmers sicherheitskritische Updates zu ermöglichen. Wird hierbei seitens des Auftragnehmers einer Sourcecode-Hinterlegung nicht zugestimmt, sollte ein Service-Vertrag abgeschlossen werden, der zum Inhalt hat, dass ein separates Referenzsystem mit dem gesamten Sourcecode beim Auftragnehmer vorgehalten wird. Die entsprechenden Regelungen sollten in den Liefer- bzw. Service- und Wartungsverträgen berücksichtigt werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	

4.3 Basissystem

Dieses Kapitel beschreibt Anforderungen, die auf Ebene von Firmware, Betriebssystem und Middleware-Systemen, wie z. B. Datenbank- und Serverdiensten, umgesetzt werden sollten.

4.3.1 Grundsicherung und Systemhärtung

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.9, 8.18, 8.19, 8.21, 8.27, 8.32 ISO/IEC 27019:2017 14.2.10 ENR Alle Standard-Komponenten (Betriebssystem, Firmware und ggf. eingesetzte Datenbanksysteme und Serverdienste) müssen anhand anerkannter Best-Practice-Guides dauerhaft gehärtet und mit aktuellen Service-Packs und Sicherheits-Patches versehen sein. Unnötige Benutzer, Default User, Programme, Netzwerkprotokolle, Dienste und Services müssen deinstalliert, oder – falls eine Deinstallation nicht möglich ist – dauerhaft deaktiviert und gegen versehentliches Reaktivieren geschützt werden. Die sichere Grundkonfiguration des Gesamtsystems muss überprüft und dokumentiert sein. Wird vom Auftragnehmer nur ein Teil der Komponenten des Gesamtsystems geliefert, muss von ihm beschrieben werden, wie die weiteren Teilkomponenten auf Basis anerkannter Best-Practice-Guides gehärtet werden können, ohne dass die Funktion der vom Auftragnehmer gelieferten Systemkomponenten und des Gesamtsystems beeinträchtigt wird. Können gewisse Standardhärtungsmaßnahmen aus technischen Gründen nicht angewandt werden, muss dies durch den Auftragnehmer explizit begründet werden, z. B. im Rahmen der Pflichtenheftphase. Benötigen die Anwendungsnutzer keinen Zugriff auf das Betriebssystem, muss ein solcher Zugriff wirksam verhindert werden. Ist ein Betriebssystemzugriff notwendig, darf 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. Die Grundkonfiguration und die Härtungsmaßnahmen müssen geprüft und in der Sicherheitsdokumentation aufgeführt werden (z. B. installierte Programme und Anwendungen, aktive bzw. deaktivierte Dienste und Ports, Dateifreigaben, Einstellungen zur Systemkonfiguration etc.).

Ergänzungen und Anmerkungen:		Zu den anzuwenden Härtungsmaßnahmen zählen u.a.: • Deinstallation oder Deaktivierung nicht benötigter Softwarekomponenten und Funktionen • Deaktivierung unsicherer bzw. nicht benötigter System- und Kommunikationsdienste (z. B. Parametrierung und Engineering-Zugänge) • Aktivierung lokaler Firewall-Funktionen • Deaktivierung bzw. Löschung nicht benötigter Standardnutzer • Änderung aller Standardpassworte • Löschung von Installations- und temporären Dateien • Aktivierung sicherheitserhöhender Konfigurationsoptionen • Einschränkung der Rechte von Nutzern und Programmen auf das notwendige Minimum • Deaktivierung nicht benötigter Kommunikations- und Datenträgerschnittstellen (CD/DVD, USB, Bluetooth, WLAN, usw.) • Deaktivierung nicht benutzter Switch-Ports • Aktivierung von Application-Whitelisting Eine Sammlung von Best-Practice Härtungs-Guides 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. Sofern Standardhärtungsmaßnahmen nicht angewendet werden könnten, sollten Alternativmaßnahmen benannt und implementiert werden. Bei der Implementierung eines Zugriffsschutzes auf das Betriebssystem ist insbesondere darauf zu achten, dass dieser nicht durch das Starten von Hilfsanwendungen wie Web- und Hilfebrowsern, Dateibetrachtern o.ä. umgangen werden kann. Die sichere Grundkonfiguration sollte nach Möglichkeit automatisiert verifizierbar sein. Die Systemhärtung sollte entsprechend einer Risikobewertung im Rahmen regelmäßig durchzuführender Sicherheitstests überprüft und bei Bedarf in Abstimmung mit dem Auftragnehmer angepasst werden. Die Überprüfung sollte dabei im Regelfall von vom Auftragnehmer unabhängigen Prüfern durchgeführt werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Für relevante Systeme der Betriebsführung sind Sicherheitstest i. d. R. jährlich durchzuführen.
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.3.2 Schadsoftware-Schutz

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.7 ISO/IEC 27019:2017 12.2.1 Alle vernetzten Systeme müssen an geeigneter Stelle mit einem Schadsoftware-Schutz (z. B. durch signatur-basierte oder Allowlisting-Lösungen) versehen sein. Alternativ zum Einsatz eines Schadsoftware-Schutzes auf allen Systemkomponenten ist vom Auftragnehmer ein umfassendes Schadsoftware-Schutzkonzept vorzulegen, das einen gleichwertigen Schutz bietet. Sofern eine signatur-basierte Lösung eingesetzt werden soll, muss eine automatische und zeitnahe Aktualisierung der Signatur-Dateien möglich sein. Dabei darf keine direkte Verbindung mit Updateservern in externen Netzen wie dem Internet benutzt werden. Der Zeitpunkt der Aktualisierung auf den Endsystemen muss konfigurierbar sein. Alle vom Auftragnehmer gelieferten Systeme und Datenträger sollten vor der Auslieferung bzw. Übergabe einer Untersuchung auf Schadsoftwarebefall unterzogen werden. Sofern keine technischen Gründe entgegenstehen, muss der Auftragnehmer den Einsatz von durch den Auftraggeber präferierten Schadsoftwareschutz-Lösungen gewährleisten.

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 Business-IT, Schnittstellen für Fernzugriff, Fernwartung und Prozessankopplung sowie alle stationären und mobilen Arbeitsplätze, Parametriernotebooks und Programmiergeräte. Die Möglichkeit zur Installation und zum Betrieb eines Schadsoftwareschutzes 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, welche die Gefahr eines Schadsoftwarebefalls oder von durch Schadsoftware induzierten Störungen reduzieren, oder gleichwertige Alternativmaßnahmen vorgesehen werden.

		Der Einsatz von bereits im Unternehmen vorhandenen Schadsoftwareschutz-Produkten ist häufig sinnvoll. Allerdings kann bei erhöhtem Schutzbedarf der Einsatz anderer oder ergänzender Produkte notwendig sein. Der Schadsoftwareschutz sollte nicht nur Datenträgerzugriffe, sondern auch den Arbeitsspeicher überwachen. Für pattern-basierte Schutzsoftware sollte das vorgesehene Konzept für Pattern-Updates 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, prozessnetz-interner Update-Server sollte angestrebt werden. Die Verwendung von sogenannten Allowlisting-Lösungen sollte geprüft werden. Dort, wo diese zum Einsatz kommen sollen, ist sicherzustellen, dass mit der vorgesehenen 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 Allowlisting-Anwendungen. Bei der Inbetriebnahme des Basissystems sollte seitens des Auftragnehmers die Kompatibilität der Schutzsoftware mit dem Gesamtsystem explizit geprüft werden. Alle vom Auftragnehmer 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. In der Notfallkonzeption sollten auch Szenarien berücksichtigt werden, bei denen es aufgrund von Fehl-Erkennungen oder Fehlkonfigurationen des Schadsoftwareschutzes zu Systemausfällen kommt.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	
	Übertragungstechnik / Sprachkommunikation:	Derzeit ist der Einsatz von Schadsoftwareschutz-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 Schadsoftwareschutz-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.

4.3.3 Autonome Benutzerauthentifizierung

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.16, 5.18, 8.5 ISO/IEC 27019:2017 9.2.1, 9.4.2 Die zur Nutzeridentifizierung und -authentifizierung notwendigen Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden.

Ergänzungen und Anmerkungen:		Die Anforderung umfasst alle Arten der Nutzeridentifizierung und -authentifizierung, z. B. auf Betriebssystem- und Anwendungsebene. Die Integration der Basissystemkomponenten in einen zentralen Benutzer-Verzeichnisdienst ist anzustreben, wobei dies mit prozessnetz-internen Servern realisiert werden sollte. Dabei kann ein eigener Verzeichnisdienst aufgebaut werden oder die Integration in einen bestehenden Dienst erfolgen. Bei Neu-Projekten sollten anlagenspezifische Verzeichnisdienste in bestehende Verzeichnisdienst-Strukturen des Auftraggebers integrierbar sein. 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. System-Accounts sollten nicht für die normale, nicht-administrative Anwendungsnutzung verwendet werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	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 Verzeichnisdienste sollte bei Bedarf realisierbar

		sein. Hierbei sollte insbesondere für dezentrale Systeme, wie z. B. verteilte Stationen und Anlagen, die Verfügbarkeitsproblematik zentraler Verzeichnisdienste hinreichend berücksichtigt werden.

4.3.4 Virtualisierungstechnologien

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.6, 8.8, 8.13, 8.14, 8.22 ISO/IEC 27019:2017 12.6.1, 13.1.3, 17.2.1 Bei der Nutzung von Virtualisierungstechnologien sind die folgenden Anforderungen zu berücksichtigen: a) Die Netzwerksegmentierung von separierten Sicherheitszonen darf nicht über die virtualisierten Komponenten bzw. die Virtualisierungsumgebung umgangen werden können. b) Die für Verwaltungs- und Administrationsdienste sowie die für die Datenspeicherung der Virtualisierungsinfrastruktur genutzten Netzwerke müssen von weiteren Netzwerken durch Firewalls segmentiert werden, an denen nur die minimal benötigten Netzwerkdienste restriktiv freigeschaltet werden. Der Zugriff auf die Verwaltungs- und Administrationsdienste und die o.g. Netzwerke muss auf Administratoren beschränkt werden. c) Die Virtualisierungsschicht, die Verwaltungs- und Administrationsschnittstellen und die zugehörige Infrastruktur müssen gemäß Hersteller-Empfehlungen einheitlich konfiguriert, gesichert und gehärtet sowie im Patch-Management und im Datensicherungskonzept berücksichtigt werden. d) Die Virtualisierungsserver müssen über hinreichende Ressourcen für den Betrieb aller auf ihnen betriebenen virtualisierten Komponenten verfügen. Dies gilt insbesondere auch für Betriebssituationen unter erhöhter Last. e) Der Ausfall von Virtualisierungsservern oder sonstigen Komponenten der Virtualisierungsinfrastruktur darf keine negativen Auswirkungen auf die definierten Verfügbarkeitsanforderungen haben. Störungen und Ausfälle der Virtualisierungsumgebung müssen auch in der Notfallkonzeption und Wiederanlaufplanung berücksichtigt werden (siehe 4.8.2)

Ergänzungen und Anmerkungen:		Das Testsystem sollte auch die wesentlichen Komponenten und Funktionen der Virtualisierungsinfrastruktur umfassen, um gewährleisten zu können, dass das Verhalten der virtuellen Komponenten in der Testumgebung nicht von der Produktivumgebung abweicht. Die Vorteile der Virtualisierung sollen insbesondere im Rahmen des Backups, des Patch-Managements sowie bei der Notfallplanung und Wiederanlaufplanung genutzt werden, z. B. durch das Einfrieren und Speichern von Betriebszuständen virtueller Komponenten (sog. Snapshots). zu a) Virtualisierte Komponenten, die unterschiedlichen Sicherheits- oder Vertrauenszonen zugeordnet sind (z. B. interne Komponenten und DMZ-Komponenten), sollten nicht auf denselben Virtualisierungsservern betrieben werden. Virtualisierte Komponenten der OT und der Business-IT sollten auf getrennten Virtualisierungsservern betrieben werden. Entwicklungs- bzw. Test- und Produktivumgebungen sollten ebenfalls auf verschiedenen Virtualisierungsservern betrieben werden. zu c) Hierzu sollte insbesondere auch die Vermeidung oder Einschränkung des Einsatzes von Gast-Werkzeugen der Virtualisierungslösung berücksichtigt werden, da diese bei unzureichender Konfiguration Schwachstellen einführen können. zu d) Die Überbuchung von Ressourcen wie Hauptspeicher oder Massenspeicherplatz sollte vermieden werden. Es sollte jederzeit sichergestellt sein, dass eine Ressourcen-Überbuchung keine negativen Einflüsse auf die Verfügbarkeit, Funktionsfähigkeit und Performance des Produktivsystems haben kann.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	

4.3.5 Containervirtualisierung

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.6, 8.8, 8.13, 8.14, 8.22 ISO/IEC 27019:2017 12.6.1, 13.1.3, 17.2.1 Bei der Nutzung von Container-Virtualisierungstechnologien sind die folgenden Anforderungen zu berücksichtigen: a) Die verschiedenen Workloads müssen voneinander isoliert werden, z. B. durch Netzwerkrichtlinien und Namespaces b) Container, die unterschiedlichen Sicherheits- oder Vertrauenszonen zugeordnet sind (z. B. interne Komponenten und DMZ-Komponenten), dürfen nicht auf denselben Hostsystemen betrieben werden. Die Netzwerksegmentierung von separierten Sicherheitszonen darf nicht über die Container- oder Hostsysteme umgangen werden können. c) Die Kommunikation der Containerinstanzen untereinander und mit externen Systemen und der Ressourcenzugriff muss durch entsprechend restriktive Netzwerk- und Zugriffsrichtlinien auf das betriebsnotwendige Minimum beschränkt werden d) Die für Verwaltungs- und Administrationsdienste wie z. B. Orchestrierung oder Deployment sowie die für die Datenspeicherung der Containerinfrastruktur genutzten Netzwerke müssen von weiteren Netzwerken durch Firewalls segmentiert werden, an denen nur die minimal benötigten Netzwerkdienste restriktiv freigeschaltet werden. Der Zugriff auf die Verwaltungs- und Administrationsdienste und die o. g. Netzwerke muss gemäß einem abgestuftem Rollenmodell beschränkt werden. e) Die Containerimages, die Runtime-, Verwaltungs- und Administrationsschnittstellen und die zugehörige Infrastruktur müssen gemäß Hersteller-Empfehlungen einheitlich konfiguriert, gesichert und gehärtet sowie im Patch-Management und im Datensicherungskonzept abgedeckt werden. f) Container dürfen nicht im privilegierten Modus betrieben werden. g) Container-Images dürfen nur aus vertrauenswürdigen Quellen bezogen werden (Basis-Images bzw. Registries). h) Container-Images müssen durch kryptographische Signaturen vor unberechtigten Veränderungen geschützt werden, die Signatur muss vor dem Deployment oder der Erzeugung abgeleiteter Images geprüft werden. i) Container-Images müssen im Rahmen des Buildprozesses und vor dem Deployment mit automatisierten Tools auf bekannte Schwachstellen wie z. B. fehlenden Sicherheitspatches oder Fehlkonfigurationen überprüft werden. Ggf. vorhandene Schwachstellen müssen durch den Lieferanten auf Relevanz/Ausnutzbarkeit bewertet werden. Die Ergebnisse der Prüfung/Buildprozesses müssen dem Betreiber zur Verfügung gestellt werden. j) Die Hostsysteme müssen über hinreichende Ressourcen für den Betrieb aller auf ihnen betriebenen Container-Komponenten verfügen. Dies gilt insbesondere auch für Betriebssituationen unter erhöhter Last.

	k) Der Ausfall von Hostsysteme oder sonstigen Komponenten der Container-Infrastruktur darf keine negativen Auswirkungen auf die definierten Verfügbarkeitsanforderungen haben. Störungen und Ausfälle der Container-Laufzeitumgebung müssen auch in der Notfallkonzeption und Wiederanlaufplanung berücksichtigt werden (siehe 4.8.2 Notfallkonzeption und Wiederanlaufplanung).

Ergänzungen und Anmerkungen:		Für detaillierte Anforderungen und Empfehlungen können folgende Standards herangezogen werden: • „SYS.1.6 Containerisierung“, in: „IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit. Edition 2023“. Bundesamt für Sicherheit in der Informationstechnik. • NIST SP 800-190: „Application Container Security Guide“. • Security standard SS-011: Containerisation. Department for Work & Pensions. Vereinigtes Königreich.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.3.6 Industrial IoT

Sicherheitsanforderungen	ISO/IEC 27002:2022 5.17, 7.9, 8.5, 8.9, 8.20, 8.32 ISO/IEC 27019:2017 9.4.2 Bei der Integration von Industrial-IoT- und OT-Technologien sind die folgenden Anforderungen zu berücksichtigen: a) Die Anbindung der IIoT-Komponenten an die OT-Umgebung muss über gesicherte Gateway-Komponenten mit Proxyfunktion erfolgen. b) Die Kommunikation der IIoT-Komponenten muss mit kryptographisch gesicherten Protokollen erfolgen (siehe 4.1.6 Kryptographische Verfahren). c) Die IIoT-Komponenten müssen gehärtet sein (siehe 4.3.1 Grundsicherung und Systemhärtung)

	d) Die IIoT-Komponenten müssen über sichere Updatemechanismen verfügen und in das Schwachstellen- und Patchmanagement integriert sein (siehe 4.1.2 Patchfähigkeit und Patch-Management) e) Vertrauliche bzw. sicherheitskritische Daten (wie z. B. Authentisierungsinformationen/Credentials) müssen auf den IIoT-Komponenten gegen unbefugte Zugriffe geschützt bzw. verschlüsselt gespeichert werden. f) Die IIoT-Komponenten müssen in ein Geräte-Management integriert sein, über das Komponenten-Verwaltung, -Update, -Monitoring etc. gesteuert werden kann. g) Öffentlich zugängliche IIoT-Komponenten müssen gegen physische Manipulation geschützt sein.

Ergänzungen und Anmerkungen:		Siehe hierzu auch Industrial Internet of Things, Volume G4: Security Framework (Hrsg. Industrial Internet Consortium)
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.3.7 Rollenkonzepte Basissystem

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.3, 5.16, 5.18, 8.2, 8.3 ISO/IEC 27019:2017 9.2.1 Alle Standard-Komponenten (Betriebssystem, Firmware und ggf. eingesetzte Datenbanksysteme und Serverdienste) müssen eine granulare Zugriffskontrolle auf Daten und Ressourcen erlauben und müssen hierzu 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. • Bediener: Benutzer, der das System im Rahmen der vorgesehenen Nutzung bedient. Dies beinhaltet auch das Recht zur Änderung von betriebsrelevanten Einstellungen. Die Standard-Zugriffsrechte müssen einer sicheren Systemkonfiguration entsprechen. Sicherheitsrelevante Systemeinstellungen und Konfigurationswerte dürfen nur von der Administrator-Rolle gelesen und geändert werden können. Zur normalen Systemnutzung sind nur Bediener- oder Read-Only-Nutzerrechte notwendig. Benutzer-Accounts müssen einzeln deaktiviert werden können, ohne sie vom System entfernen zu müssen. Eine Festlegung der den Rollen zugewiesenen Rechte muss durch den Auftraggeber erfolgen.

Ergänzungen und Anmerkungen:	Sofern praktikabel bzw. technisch möglich sollten Read-Only-Nutzer angelegt werden. Dies sind Benutzer, die den Status des Systems abrufen und definierte Betriebsdaten lesen dürfen, aber nicht berechtigt sind, Änderungen durchzuführen. Benutzerrollen ermöglichen eine einheitliche und leichtere Zuordnung von Berechtigungen für die einzelnen Benutzer. Rollenkonzepte dienen auch dazu, unabsichtliche Fehlhandlungen zu verhindern.
Betriebsführungs- / Leitsysteme und Systembetrieb:	
Übertragungs-technik / Sprach-kommunikation:	
Sekundär-, Automatisierungs- und Fernwirktechnik:	

4.4 Netzwerk und Kommunikation

Dieses Kapitel beschreibt Sicherheitsanforderungen an die Netzwerktechnik, Netzarchitektur sowie an Kommunikationsprotokolle und -technologien.

4.4.1 Eingesetzte Protokolle und Technologien

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.3, 8.5, 8.20, 8.21, 8.22, 8.24 ISO/IEC 27019:2017 10.1.2, 13.1.1, 13.1.3, 13.1.4 ENR a) Wo technisch möglich, dürfen generell nur sichere Kommunikationsstandards und Protokolle benutzt werden, die Integritätsüberprüfung, Authentifizierung und ggf. Verschlüsselung bieten. Für Protokolle zur Remote-Administration und Parametrierung ist dies zwingend umzusetzen. Bei nicht standardkonformen bzw. proprietären Protokollen sind die genannten Punkte ebenfalls zu berücksichtigen. 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 verwaltet werden können. Zur Administration und zum Monitoring werden sichere Protokolle verwendet, die Integritätsschutz, Authentifizierung und Verschlüsselung gewährleisten. 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 Patch-Management 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 TLS-Verschlüsselung oder durch verschlüsselte VPN-Technologie). e) 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. f) Insbesondere die Datenkopplung mit weiteren Leitsystemen und mit Automatisierungs-/Fernwirkkomponenten muss über genormte Protokolle über kontrollierende Elemente wie z. B. Firewalls (siehe 4.4.2) erfolgen.

Ergänzungen und Anmerkungen:	Bieten die genutzten Netzwerkprotokolle sicherheitserhöhende Optionen, sollten diese aktiviert werden. Protokolle, die UDP als Transportprotokoll nutzen, sollten generell vermieden werden. Dies gilt insbesondere beim Einsatz über die Grenzen von Sicherheitszonen hinweg. 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, mindestens in der Version 3) • RADIUS (Remote Authentication Dial In User Service) • Syslog Die Nutzung von Protokollen mit dynamischer Portvergabe (z. B. RPC/DCOM) sollte über Firewalls hinweg prinzipiell vermieden werden. Falls dies nicht verhindert werden kann, sollte eine Firewall eingesetzt werden, welche mit dynamischer Portvergabe umgehen kann und diese nur bei Bedarf (related connection) öffnet. Aus der häufig zur Systemkopplung eingesetzten OPC-Protokollfamilie sollte ausschließlich die im Hinblick auf Sicherheitsaspekte entwickelte Protokollversion OPC-UA genutzt werden. Dabei sollten die folgenden Einstellungen aktiviert werden: • Der securityMode sollte 'Sign' (Signieren von Nachrichten) oder 'SignAndEncrypt' (Signieren und Verschlüsseln von Nachrichten) sein. Damit wird unter anderem eine Authentifizierung auf Applikationsebene erzwungen. Der securityMode 'SignAndEncrypt' sollte dann genutzt werden, wenn über Integrität hinaus vertrauliche Daten zu schützen sind. Der securityMode 'None' bietet keinerlei Schutz. • Bei der Wahl der kryptographischen Verfahren sollte die SecurityPolicy 'Basic256SHA256' gewählt werden. • Benutzerauthentifizierung: Die Möglichkeit der Anmeldung mit der Kennung 'anonymous' sollte unterbunden werden. Entsprechend den technischen Möglichkeiten sollten in allen Bereichen standardisierte IEC-Protokolle angewendet werden. Der private Bereich dieser Kommunikationsprotokolle sollte nur bei technischer Notwendigkeit verwendet werden. Die Standard-Protokolle IEC 60870-5-101/104 und IEC 61850 bieten ohne zusätzliche Maßnahmen keine sichere Integritätsüberprüfung, Authentifizierung und Verschlüsselung. Hier sollten die verfügbaren Erweiterungen gemäß IEC 62351 eingesetzt werden. Mögliche Einschränkungen wie z. B. in Bezug auf Performance und bei der Fehlerdiagnose sowie die notwendige Infrastruktur und Prozesse zur Schlüsselverwaltung sollten berücksichtigt werden. Bei der Kommunikation über Zonengrenzen sollten Protokollbrüche, z. B. durch Application Layer Gateways oder durch Umwandlung in ein

		anderes Protokoll vorgesehen werden, damit potenzielle Verwundbarkeiten und Schwachstellen vermindert werden können. zu a) Zur Fernadministration sollten bevorzugt SSH (Secure Shell), SCP (Secure Copy), SFTP (SSH File Transfer Protocol), HTTPS (Hypertext Transfer Protocol Secure) bzw. RDP (Remote Desktop Protocol) in den aktuellen Versionen und mit aktivierten Sicherheitseinstellungen verwendet werden. Schalthandlungen und 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, kaufmännischen und VoIP-Netze und der Aufbau eines zentralen Netzwerkmanagementsystems für die Prozessnetze.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Die Kommunikation innerhalb des Leitsystems ist i. d. R. herstellerabhängig. Hier sollten gleichwertige Sicherungsmechanismen vorgesehen werden.
	Übertragungstechnik / Sprachkommunikation:	Insbesondere für Voice-over-IP-Kommunikation sollten Sicherheitsmechanismen eingesetzt werden, die die Vertraulichkeit der Kommunikation sicherstellen und eine sichere Authentisierung der Kommunikationspartner und -komponenten gewährleisten.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	Die Kommunikation zwischen einzelnen Automatisierungskomponenten erfolgt vielfach über Industriestandards oder proprietäre Herstellerprotokolle (z. B. Industrial Ethernet, Profinet, Profibus, etc.). Die Anbindung an die Stationsebene und an das Leitsystem sollte über die angeführten Standardprotokolle erfolgen. zu d) Bei physisch exponierten bzw. nicht hinreichend geschützten Komponenten sollte die VPN-Terminierung direkt auf den Steuerungseinheiten erfolgen können. zu e) Beim Einsatz einer gemeinsamen Netzwerk-Infrastruktur in Automatisierungsnetzen 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/R-GOOSE und Sampled Values (SV / R-SV), VLAN-Nutzung in der Stationsautomatisierung).

4.4.2 Sichere Netzwerkstruktur

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.3, 8.20, 8.21, 8.22 ISO/IEC 27019:2017 12.9.1 ENR, 13.1.1, 13.1.3, 13.1.4 ENR, 13.1.5 ENR a) 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, filternde 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) Das Gesamtsystem und seine Einzelkomponenten muss in die Zonenstruktur des Auftraggebers eingebettet werden. d) Netzübergänge sind so zu planen, dass sie in die Angriffs- / Anomalieerkennung des Betreibers eingebunden werden können (siehe 4.1.13 Integration in Systeme zur Erkennung von Anomalien und Angriffen).

Ergänzungen und Anmerkungen:	Die Anforderungen sind in der Regel projektspezifisch umzusetzen. Netzwerke der OT sollten von Business-IT Netzwerken durch eine Firewall mit restriktivem Regelsatz segmentiert werden. 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 physischem 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. Der initiale Aufbau der Kommunikationsverbindung sollte immer vom hohen Sicherheitslevel zum geringeren gerichtet sein. Ausgenommen hiervon ist der interaktive Fernzugriff aus einer DMZ über gesicherte Protokolle (vgl. 4.4.1). 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 vermieden werden. Werden diese zwingend benötigt, sollten sie nur über die o.g. abgeschlossenen Netzwerksegmente zugänglich sein. Der Auftraggeber sollte prüfen, ob Netzwerk- und Security-Komponenten wie Firewalls oder VPN-Konzentratoren selbst beigestellt werden oder gegebenenfalls zum Lieferumfang des Auftragnehmers gehören. zu a) Eine physische Trennung funktionaler Ebenen sollte einer logischen Trennung vorgezogen werden. Wenn eine physische 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. Für detailliertere Anforderungen zur Netzwerksegmentierung können Anforderungen der IEC-62443-Normreihe herangezogen werden, insbesondere: • IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-3 (2013-08): System security requirements and security levels; Abschnitt 9.3 „SR 5.1 – Network segmentation“ • IEC 62443-4-2 (2019-02): Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components; Abschnitt 9.3 „CR 5.1 – Network segmentation“ In Anhang A "Netzwerkzonen-Diagramme“ sind Beispiele zur Veranschaulichung möglicher Netzwerkzonenkonzepte enthalten.
	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 Firewall-Funktionalitäten vorgesehen werden.
	Übertragungstechnik / Sprachkommunikation:	Wo möglich, sollte betriebseigene Infrastruktur verwendet werden. Bei der Nutzung von fremdbetriebener Kommunikations-Infrastruktur 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 Gateways mit Firewall-Funktionalitäten auf Netzwerk- und Applikationsebene (Telegramm-/Profilfilterung) vorgesehen werden.

		Es sollte eine physische oder logische Trennung zwischen den Netzwerken für Produktivdaten (Prozessdaten) und Managementdaten (Monitoring, Logging, Engineering, Administration etc.) 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. 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 Gateway-Komponenten realisiert werden.

4.4.3 Dokumentation der Netzwerkstruktur und -konfiguration

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.9 ISO/IEC 27019:2017 8.1.1 Die Netzwerkkonzeption und -konfiguration, alle physischen, virtuellen und logischen Netzwerkverbindungen und die verwendeten Protokolle, IP-Adressen und Ports sowie die Netzwerk-Perimeter, die Bestandteil des Systems sind bzw. mit ihm interagieren, müssen dokumentiert sein. Änderungen, z. B. durch Updates, werden innerhalb des Change-Managements 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. Sofern die entsprechende Netzwerkarchitektur/ -konfiguration Projekt- bzw. Lieferbestandteil sind, müssen die folgenden Netzwerkschichten dokumentiert werden: • Netzzugangs- / Bitübertragungsschicht / Data Link Layer (Verkabelung, Layer 2 / VLAN Konfiguration) • Vermittlungs- / Transportschicht (IP- und Routing-Konfiguration) • Anwendungsschicht (genutzte Protokolle und deren Konfiguration)

Ergänzungen und Anmerkungen:		Die Dokumentation sollte sowohl eine grafische Netzwerkdarstellung als auch eine nachvollziehbare Beschreibung des Netzwerkes umfassen. Neben Kabellaufplänen sollten auch die logische Segmentierung in Sicherheitszonen und die Informationsflüsse in der Netzwerkdokumentation enthalten sein. Die Dokumentation sollte Port-genau sein, Kabel sollten mit Kabelnummer und Ziel 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. Es sollte die maximal zulässige Netzwerkbelastung angeben werden, unterhalb der eine zuverlässige Funktion des Gesamtsystems und der Einzelkomponenten gewährleistet ist. Die aktuelle Dokumentation sollte jederzeit (insbesondere auch bei Ausfall des betroffenen Netzwerks) verfügbar sein, z. B. für den Bereitschaftsdienst.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	Zur korrekten Umsetzung der Sicherheitsanforderung sollte auch die Kommunikation zwischen den Komponenten in der Station und mit dem Feld dokumentiert werden. Unter dem Begriff „Perimeter“ ist im Stations-Umfeld die „Außenschnittstelle“ zwischen der einzelnen Station und anderen Netzwerken zu verstehen (Leitstelle, Ferndiagnose, etc.).

4.4.4 Sichere Fern-Zugänge

Sicherheitsanforderungen	ISO/IEC 27002:2022 5.15, 6.7, 8.3, 8.5 ISO/IEC 27019:2017 6.2.2, 9.1.2 a) Administration, Wartung und Konfiguration aller Komponenten muss auch über ein Out-of-Band-Netz, zum Beispiel über lokalen Zugriff, via serielle Schnittstelle, Netzwerk oder direkter Steuerung der Eingabegeräte (KVM), möglich sein. b) Fern-Zugriff muss über zentral verwaltete Zugangsserver (Jumpserver) unter der Kontrolle des Systembetreibers durchgeführt werden. Die Zugangsserver müssen in einer DMZ betrieben werden und eine Isolation des Prozessnetzes sicherstellen. Es muss

	ein 2-Faktor-Authentifizierungsverfahren benutzt werden. Wenn der AG die Fernwartung zur Verfügung stellt, ist ausschließlich diese zu verwenden. c) Direkte Einwahl-Zugänge in Endgeräte sind grundsätzlich nicht erlaubt. d) Der Zugriff auf einen Fernzugang muss zentral geloggt werden, wiederholte Fehlversuche werden gemeldet. e) Alle Fern-Zugangs-Möglichkeiten müssen dokumentiert werden.

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 sollten immer 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. Die Zugangsserver sollten gehärtet und mit Schadsoftwareschutz versehen sein und immer auf aktuellem Softwarestand gehalten werden. Des Weiteren sollte eine Überwachung und Protokollierung der Fernwartung möglich sein. Zusätzlich zu empfehlen sind separat aktivierbare Zugangspunkte (manuelle Freischaltung bzw. Trennung sowie zeitgesteuerte Trennung) in das jeweilige technische Netz bzw. Netzsegment. Für jede Netzwerkzone und jeden Dienstleister sollte nach Möglichkeit ein eigener, logisch separierter Fernwartungszugang und Server geschaffen werden. Für alle Fernzugriffe müssen mindestens die gleichen Sicherheitsanforderungen 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. Es sollten für alle Dienstleister standardisierte und je nach Anwendungsumfeld zentralisierte Fernwartungsinfrastrukturen und -prozesse genutzt werden. Bei einem Fernzugriff auf von Anwendern direkt genutzte Komponenten sind die entsprechenden gesetzlichen Rahmenbedingungen wie z. B. Datenschutzgesetze oder Betriebsverfassungsgesetz zu berücksichtigen. In der Regel ist dem Anwender der Fernzugriff eindeutig zu signalisieren. Zu e)

		Wenn die Komponenten integrierte Fern-Zugangs-Möglichkeiten (z. B. Modems) besitzen, sind diese zu dokumentieren, auch wenn diese deaktiviert sind.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.4.5 Funktechnologien

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.20, 8.21, 8.22, 8.24 ISO/IEC 27019:2017 13.1.1, 13.1.3 Der Einsatz von Nahbereichs-Funktechnologien (z. B. WLAN, Bluetooth, ZigBee, RFID etc.) ist nur nach Analyse der damit verbundenen Risiken und unter Beachtung der nachfolgend beschriebenen Mindestsicherungsmaßnahmen in Abstimmung mit dem Auftraggeber und nach Genehmigung zulässig: • Drahtlose Übertragungstechnik muss nach dem Stand der Technik abgesichert werden. • WLANs dürfen nur in dedizierten und durch Firewalls und Applikations-Proxies abgetrennten Netzwerksegmenten betrieben werden. • WLANs sind so einzurichten, dass bestehende WLANs nicht gestört oder beeinträchtigt werden.

Ergänzungen und Anmerkungen:	Alle Funktechnologien sollten generell nur bei zwingendem Bedarf und nach expliziter Freigabe durch den Auftraggeber eingesetzt werden. Generell sollte 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, Bluetooth und RFID siehe die NIST-Dokumente „NIST Special Publication 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)“, „NIST Special Publication 800-121 - Guide to Bluetooth Security“ und „NIST Special Publication 800-98 - Guidelines for Securing Radio Frequency Identification (RFID) Systems”.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	Im Umfeld der Sprachkommunikation sollte insbesondere auch die Absicherung von draht-/schnurlosen Telefonen berücksichtigt werden.
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.4.6 Netzwerkauthentifizierung

Sicherheitsanforderungen	ISO/IEC 27002:2022 5.17, 8.5, 8.20, 8.24 ISO/IEC 27019:2017 9.3.1, 10.1.2 Vernetzte Systemkomponenten müssen netzwerkseitig authentisiert sein. Wird keine IEEE 802.1X-basierte Netzwerkauthentifizierung implementiert, muss eine MAC-basierte Authentifizierung implementiert sein. Können aus technischen Gründen keine Netzwerkauthentifizierungsmaßnahmen implementiert werden, müssen Netzwerkschnittstellen deaktiviert werden oder dürfen nur durch berechtigtes Personal zugänglich sein. Bei der Nutzung von Netzwerkauthentifizierung müssen potenzielle Ausfall- und Notfallszenarien berücksichtigt werden, während derer die Netzwerkauthentifizierung nicht zur Verfügung steht oder digitale Zertifikate für ungültig erklärt wurden (siehe hierzu auch 4.8.2 „Notfallkonzeption und Wiederanlaufplanung“ sowie 4.1.7 „Public Key Infrastructure“).

Ergänzungen und Anmerkungen:	Es sollte eine IEEE 802.1X-basierte Netzwerkauthentifizierung angestrebt werden. Abhängig von den Verfügbarkeitsanforderungen von Systemkomponenten können sowohl IEEE 802.1X als auch MAC-basierte Authentisierungsverfahren im Gesamtsystem eingesetzt werden, wobei nicht beide Verfahren gleichzeitig für eine Komponente eingesetzt werden sollten.

		Beim Einsatz von IEEE 802.1X sollte bevorzugt das Authentifizierungsprotokoll EAP-TLS genutzt werden und für Supplicants, die nicht IEEE 802.1x fähig sind, auf MacAuthenticationBypass ausgewichen werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.5 Anwendung

Dieses Kapitel beschreibt Sicherheitsanforderungen auf Ebene der Anwendungen und Fachapplikationen.

4.5.1 Rollenkonzepte

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.3, 5.16, 5.18, 8.2, 8.3 ISO/IEC 27019:2017 9.2.1 Das Gesamtsystem muss eine granulare Zugriffskontrolle auf Daten und Ressourcen erlauben und muss hierzu 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. • Bediener: Benutzer, der das System im Rahmen der vorgesehenen Nutzung bedient. Dies beinhaltet auch das Recht zur Änderung von betriebsrelevanten Einstellungen. • Read-Only-Nutzer: Benutzer, der den Status des Systems abrufen und definierte Betriebsdaten lesen darf, aber nicht berechtigt ist, Änderungen durchzuführen. Die Standard-Zugriffsrechte müssen einer sicheren Systemkonfiguration entsprechen. Sicherheitsrelevante Systemeinstellungen und Konfigurationswerte dürfen nur von der Administrator-Rolle gelesen und geändert werden können. Zur normalen Systemnutzung sind nur Bediener- oder Read-Only-Nutzerrechte notwendig. Benutzer-Accounts müssen einzeln deaktiviert werden können, ohne sie vom System entfernen zu müssen. Die Berechtigungen dürfen nicht nur auf Ebene der Bedien- und Benutzeroberfläche realisiert werden, sondern müssen durchgehend in der gesamten Applikation und – sofern vorhanden – auch auf Betriebssystem- und Datenbankebene umgesetzt werden.

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, etc.) 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 Möglichkeit zur zeitlichen Befristung von Rollen und/oder Rechtevergaben sollte bei Bedarf vorgesehen werden. Die Normen IEC 62351-8 und 62351-90-1 behandeln rollenbasierte Zugriffssteuerung für Steuerungssysteme der Energieversorgung und können zur Umsetzung eines Rollenkonzepts herangezogen werden. Die im System hinterlegten Rollen sollten mit der Organisationsstruktur abgeglichen werden und sich bei Änderungen anpassen lassen.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Beispiele für Nutzerrollen im Umfeld von Betriebsführungs- und Leitsystemen sind z. B.: • Administrator • Parametrierung/Datenaufbereitung • Bedien-/Schaltberechtigung • Beobachtung/Überwachung • 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 (in Klammern ist ein beispielhaftes Mapping zu den in IEC 62351-8 definierten Rollen angegeben): • Administrator (INSTALLER / SECADM) • Bedien-/Schaltberechtigung (OPERATOR) • Beobachtung/Überwachung (VIEWER) • Parametrierung (ENGINEER) • Änderung von Betriebsparametern • Diagnose (ohne Parametrier- und Schaltmöglichkeit) • Datentest/Qualitätssicherung

4.5.2 Benutzer-Authentifizierung und Anmeldung

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.16, 5.17, 5.18, 8.5, 8.15 ISO/IEC 27019:2017 9.2.1, 9.3.1, 9.4.2, 12.4.1 Die Anwendung muss eine personenspezifische Identifizierung und Authentifizierung vornehmen, Gruppen-Accounts werden von Auftraggeber nur in genau spezifizierten Ausnahmefällen erlaubt. a) Ohne erfolgreiche Benutzer-Authentifizierung darf das System nur genau definierte Aktionen erlauben. b) Das System muss eine Passwort-Policy unterstützen, welche dem Stand der Technik entspricht. c) Wo technisch möglich, wird eine starke 2-Faktor-Authentifizierung verwendet, z. B. durch die Verwendung von Tokens oder SmartCards. d) Die zur Nutzeridentifizierung und Authentifizierung benötigten Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden (siehe auch 4.3.3). e) Erfolgreiche und fehlgeschlagene Anmeldeversuche müssen zentral geloggt werden, fehlgeschlagene Anmeldeversuche müssen zentral alarmiert werden können.

Ergänzungen und Anmerkungen:	Passworte und andere Authentisierungsinformationen dürfen nur kryptographisch gesichert übertragen und im System gespeichert werden (vgl. 4.1.5 und 4.4.1). Der Betreiber sollte sicherstellen, dass eine Passwort-Policy festgelegt ist und umgesetzt wird. Die Standardbenutzer-Accounts aller Applikationen und Systeme sollten bei Übernahme des Systems geändert oder deaktiviert werden, siehe auch 4.3.1. 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 Überschreitung einer konfigurierbaren Anzahl von fehlgeschlagenen Anmeldeversuchen soll eine Alarmmeldung ausgelöst und das Konto ggf. gesperrt werden.

		zu a) Der Betreiber und der Auftragnehmer sollen gemeinsam konkret festlegen, welche Aktionen das System ohne erfolgreiche Benutzer-Authentifizierung zulässt. zu b) Im Rahmen der Anwendungskonfiguration sollte die erforderliche Passwortkomplexität durch den Anwendungsadministrator möglichst umfassend konfigurierbar sein (gemäß der Password-Policy des Unternehmens). 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 c) Insbesondere bei Fernarbeitsplätzen sollte eine 2-Faktor-Authentifizierung vorgesehen werden. zu d) Eine kryptographisch gesicherte Anbindung an einen zentralen, prozessnetzinternen Verzeichnisdienste sollte in Betracht gezogen 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) Insbesondere im dezentralen Stationsumfeld ist auch für HMI-Systeme die Nutzung zentraler Verzeichnisdienste aus Verfügbarkeitsgründen u.U. mit aktueller Technik derzeit nicht zu realisieren. Zukünftig sollte auch hier eine Einbindung in Verzeichnisdienste möglich sein.

4.5.3 Autorisierung von Aktionen auf Benutzer- und Systemebene

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.3, 8.18 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.

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:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.5.4 Web-Applikationen und Web-Services

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.27 Für Web-Applikationen, Web-Schnittstellen und Web-Services sind die Empfehlungen der OWASP TOP 10 und des OWASP Application Security Verification Standard Projekte sowie des BSI-Leitfadens zur Entwicklung sicherer Webanwendungen zu berücksichtigen.

	Abweichungen sind zu begründen und vom Auftraggeber vorab zu genehmigen. Sofern die eingesetzten Systemkomponenten über Browserschnittstellen (z. B. zur Parametrierung) verfügen, muss auch hier eine sichere Implementierung gewährleistet sein. Andernfalls müssen die Schnittstellen deaktiviert werden. Von den Anforderungen des OWASP Application Security Verification Standard Projekts (ASVS) muss im Bereich der Prozessteuerung der Energieversorgung mindestens Level L2 (Standard) umgesetzt werden.

Ergänzungen und Anmerkungen:	Die Einführung von Webanwendungen sollte generell nur in Abstimmung und nach einer expliziten Freigabe durch den Auftraggeber/Betreiber erlaubt werden. Im Bereich kritischer Infrastrukturen sollte das Level L3 (Advanced) des ASVS umgesetzt werden.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.5.5 Integritätsprüfung

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.27 ISO/IEC 27019:2017 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).

Ergänzungen und Anmerkungen:	Die Konsistenz der verarbeiteten Daten sollte jederzeit sichergestellt sein. Ein konsistenter Eingangsdatensatz sollte immer 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 Programm-Modulen. 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:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.5.6 Logging

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.33, 8.15, 8.17 ISO/IEC 27019:2017 12.4.1, 12.4.4 a) Das Gesamtsystem muss über eine einheitliche Systemzeit verfügen und die Möglichkeit zur Synchronisation dieser Systemzeit mit einer externen, gesicherten 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) Die zentrale Speicherung der Logdateien erfolgt an einem frei konfigurierbaren Ort. Ein Mechanismus zur automatisierten Übertragung des Logfiles auf zentrale Komponenten muss zur Verfügung stehen. d) Das Logfile muss gegen spätere Modifikation geschützt sein.

	e) Bei Überlauf des Logfiles werden die älteren Einträge überschrieben, das System muss bei knapp werdendem Logging-Speicherplatz warnen. f) Es muss möglich sein, sicherheitsrelevante Meldungen in ein vorhandenes Alarm-Management aufzunehmen.

Ergänzungen und Anmerkungen:	Eine Pflicht zur Protokollierung kann aufgrund von betrieblichen, behördlichen oder rechtlichen Anforderungen bestehen. Um eine zielgerichtete Verwaltung der Logfiles zu gewährleisten, sollten die Kriterien dafür in einem Logging-Betriebskonzept festgelegt werden. Der Auftraggeber sollte Vorgaben für den Mindestzeitraum bzw. die Mindestanzahl der zu speichernden Meldungen für die lokale und zentrale Speicherung festlegen. Das Logging von Events sollte möglichst einfach konfigurierbar und modifizierbar sein. Sicherheitsrelevante Events sollen in den Systemlogs als solche markiert werden und in der Dokumentation mit entsprechenden Standard-Anwendungsfällen des Systems verknüpft werden, um eine automatische Auswertung zu erleichtern. Beispiele: abgewiesener Befehl wegen Zeitdifferenz/Befehlsalter, Anmeldeversuche mit falschem Passwort. Die Kritikalität eines Ereignisses sollte systemspezifisch klassifiziert werden. 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. Bei der Nutzung des NTP-Protokolls sollte eine kryptographische Authentisierung gemäß RFC 2030 / RFC 1305 vorgesehen werden. Ausfälle der Verfügbarkeit des Zeitsignals bzw. der externen Zeitsynchronisierung sollten keine bzw. nur wohldefinierte Auswirkungen auf leittechnische Funktionen haben. Gegebenenfalls sollte eine redundante Zeitquelle vorgesehen werden. zu e) Sofern ein Ringspeicher-Mechanismus eingesetzt wird, ist die Anforderung nicht direkt anwendbar. In diesem Fall sollte die Mindestgröße des Ringspeichers festgelegt und eine Speicherung auf einem zentralen Logserver (siehe c)) vorgesehen werden.
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 c) 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 d) siehe c)

4.6 Entwicklung

Dieses Kapitel beschreibt Anforderungen, die in der Hard- und Software-Entwicklung umgesetzt werden sollten. Sofern Standard-Komponenten wie z. B. Betriebssysteme oder Datenbank-Systeme zum Einsatz kommen, bezieht sich dieses Kapitel auch auf die Integration der Standard-Komponenten in das Gesamtsystem und/oder die jeweilige Komponente.

4.6.1 Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.20, 5.21, 8.32, 8.27, 8.31, 8.30, 8.29, 8.33, 8.28 ISO/IEC 27019:2017 9.4.5 a) 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. Im Rahmen des Entwicklungsprozesses müssen insbesondere die folgenden sicherheitsrelevanten Entwicklungsschritte berücksichtigt werden: • Definition der Sicherheitsanforderungen • Bedrohungsmodellierung und Risikoanalyse • Ableitung von Anforderungen an Systemdesign und Implementierung • Sichere Programmierung • Anforderungstests • Sicherheitsprüfungen vor der Inbetriebnahme Die angewandten Prozesse und Aktivitäten müssen nachvollziehbar dokumentiert werden. Die Dokumentation kann bei Bedarf vom Auftraggeber eingesehen werden. c) Das Testen erfolgt nach dem 4-Augen-Prinzip: Entwicklung und Tests werden von verschiedenen Personen durchgeführt. Die Testpläne und -prozeduren sowie erwartete und tatsächliche Testergebnisse müssen dokumentiert und nachvollziehbar sein. Sie können bei Bedarf vom Auftraggeber eingesehen werden. d) Der Auftragnehmer muss über einen dokumentierten Entwicklungs-Sicherheitsprozess verfügen, der die physische, organisatorische und personelle Sicherheit abdeckt und die Integrität und Vertraulichkeit des Systems schützt. Die Effektivität des o.g. Prozesses kann durch eine externe Auditierung überprüft werden. e) 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. f) Die Freigabe des Systems bzw. von Updates/Sicherheits-Patches muss anhand eines spezifizierten und dokumentierten Freigabe-Prozesses stattfinden.

Ergänzungen und Anmerkungen:	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. Der Standard *IEC 62443-4-1:2018* kann zum Beispiel als Grundlage für Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung herangezogen 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.
Betriebsführungs- / Leitsysteme und Systembetrieb:	-
Übertragungstechnik / Sprachkommunikation:	-
Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.6.2 Sichere Entwicklungs- und Test-Systeme, Integritäts-Prüfung

Sicherheits-anforderungen	ISO/IEC 27002:2022 8.30, 8.31, 8.33 ISO/IEC 27019:2017 9.4.5, 12.1.4 a) Die Entwicklung muss auf sicheren Systemen erfolgen, die Entwicklungsumgebung, Quellcode und Binärdateien müssen gegen fremde Zugriffe gesichert sein. Alle Entwicklungssysteme müssen anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet sein und über einen aktuellen Schadsoftwareschutz verfügen sowie mit allen aktuellen Sicherheits-Patches versehen sein. b) Entwicklung und Test des Systems sowie von Updates, Erweiterungen und Sicherheits-Patches muss in einer vom Produktivsystem getrennten Test-Umgebung erfolgen. c) Auf Produktiv-Systemen darf mit Ausnahme von interpretierten Skriptsprachen 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.

Ergänzungen und Anmerkungen:	Die Entwicklungssysteme und -umgebungen sowie die Testsysteme sollten immer nach Stand der Technik gesichert und vom allgemeinen Unternehmensnetz getrennt sein. Ein Zugriff auf unsichere Netze, z. B. zur Internet- oder Mail-Nutzung, 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 Virtualisierungs- oder Proxylösungen. Es sollte sichergestellt sein, dass Risiken durch Verbindungen zum Internet (z. B. durch Web- oder Mailnutzung) größtmöglich minimiert werden. Die Entwicklungssysteme und -umgebungen sowie die Testsysteme sollten mit einem sicheren logischen Zugangsschutz versehen sowie vor unberechtigtem physischem Zugriff geschützt sein. zu c) Ein ausreichender Schutz gegen unerlaubte Veränderung sollte vorgesehen werden, z. B. Code-Signing. Ein 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 nachzustellen, 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 auf dem Produktivsystem 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 dem 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 Auftragnehmer 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.

4.7 Wartung

Dieses Kapitel beschreibt Sicherheitsanforderungen, die im Rahmen von Wartungsprozessen berücksichtigt werden sollten. Der Ausdruck „Wartung“ bezieht sich in diesem Dokument allgemein auf alle vom Auftraggeber/Betreiber zu beauftragenden Service-Maßnahmen wie Instandhaltungsarbeiten, Störungsanalysen, Fehler- und Störungsbehebung, Verbesserungen, Anpassungen, usw[1].

4.7.1 Anforderung an die Wartungsprozesse

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.15, 5.16, 5.18, 5.19, 5.20 ISO/IEC 27019:2017 9.1.2, 9.2.1, 15.1.2 a) Der Fern- und Vor-Ort-Zugriff darf nur durch einen definierten und geschulten Personenkreis und nur von abgesicherten Systemen aus erfolgen. Die für den Fern- und Vor-Ort-Zugriff genutzten Zugangs-Systeme und IT-Infrastrukturen müssen anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet sein und über einen aktuellen Schadsoftwareschutz verfügen sowie mit allen aktuellen Sicherheits-Patches versehen sein. b) Durch einen definierten Wartungsprozess muss sichergestellt sein, dass das Wartungspersonal im Rahmen seiner Tätigkeiten nur Zugriff auf die benötigten Systeme, Dienste und Daten und Zutritt zu den entsprechenden Räumlichkeiten erhält. c) Der interaktive Fern-Zugang muss über personalisierte Accounts und unter Nutzung von 2-Faktor-Authentifizierung erfolgen. Für automatisierte Abläufe sind spezielle Kennungen einzurichten, die nur bestimmte Funktionen ausführen können und die keinen interaktiven Zugang ermöglichen. d) Es muss technisch sichergestellt sein, dass ein Fern-Zugriff nur erfolgen kann, wenn dieser vom verantwortlichen Betreiber freigegeben wird. Bei externen Dienstleistern müssen die Freigabe und die Trennung für jede Fernzugriffs-Sitzung einzeln erfolgen. Eine Sitzung ist nach Ablauf einer angemessenen Zeit automatisch zu trennen. Insbesondere sind die für den Fernzugriff genutzten Zugangs-Systeme während des Fern-Zugriffs von anderen Netzen logisch oder physisch zu entkoppeln. Eine physische Entkopplung ist der logischen vorzuziehen. e) Die Absicherung der für Fern- und Vor-Ort-Wartung genutzten Systeme muss insbesondere die folgenden Punkte umfassen: • Die Wartungssysteme müssen mit einem sicheren logischen Zugangsschutz versehen sowie vor unberechtigten physischen Zugriff geschützt sein. • Die Wartungssysteme müssen anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet sein.

[1] Hinweis: Die in diesem Whitepaper verwendete Definition von Wartung und Instandhaltung weicht von der in der DIN 31051 benutzten Definition ab.

	• Fernwartungszugriffe dürfen nur aus einer abgesicherten und gegen unberechtigte Zugriffe geschützten DMZ-Umgebung erfolgen. • Mobile Systeme zur Vor-Ort-Wartung müssen mit einer restriktiv konfigurierten Firewall-Software geschützt werden. • Die Wartungssysteme müssen beim Wartungszugriff über einen aktuellen Schadsoftwareschutz verfügen und mit allen aktuellen Sicherheits-Patches versehen sein.

Ergänzungen und Anmerkungen:	Die hier genannten Anforderungen sollten bereits bei Projektplanungen und bei Wartungsvereinbarungen in Zusammenarbeit zwischen Auftraggeber und Auftragnehmer bzw. Dienstleister berücksichtigt werden. Ebenso sollten Datenschutz- und Geheimhaltungsvereinbarungen schriftlich vereinbart werden. Ein Ziel der Anforderung ist u.a., dass kein unbemerkter und unbefugter 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 Authentifizierungstokens in der Warte erreicht werden. Die Vorortwartung durch Servicetechniker stellt ein ernst zu nehmendes Sicherheitsrisiko dar. Es sollte vermieden werden, dass der Auftragnehmer eigene Hardware an das Prozessnetz anschließt (z. B. Wartungs-Notebooks, aber auch Speichergeräte wie USB-Sticks). Stattdessen sollte eine Bereitstellung von Auftraggeber-eigener Hardware erfolgen. Falls die Nutzung von Hardware des Auftragnehmers doch notwendig sein sollte, sollte dies vom Auftraggeber explizit genehmigt werden. Der Auftragnehmer sollte verpflichtet werden, die Durchsetzung einer angemessenen internen Sicherheitsrichtlinie für diese Dienstleistung nachzuweisen. Die Sicherheitsrichtlinie sollten mindestens die folgenden Punkte behandeln: • Zugriffs- und Zugangsschutz • Sichere Authentisierung am Gerät • Sichere Speicherung von Kundendaten • Datenträgerverschlüsselung • Festlegung zur Datenübertragung (Verschlüsselung / Integritätsschutz) • Datensicherung und -wiederherstellung • Patch-Management • Schadsoftwareschutz • Sichere Mechanismen zur Löschung von Kundendaten

		Das Wartungspersonal muss den jeweils anwendbaren gesetzlichen Vorgaben, z. B. bezüglich einer Sicherheitsüberprüfung, bei Tätigkeiten im Bereich Kritischer Infrastrukturen genügen. Für Wartungszugriffe auf kritische Systeme sollte das Wartungspersonal des Auftragnehmers bzw. Dienstleisters namentlich benannt werden. 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. Vergleiche hierzu auch 4.4.4
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.7.2 Sichere Updateprozesse

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.19, 8.29, 8.30, 8.32 ISO/IEC 27019:2017 12.5.1 Die Bereitstellung und Installation von Updates, Erweiterungen und Patches muss nach einem definierten Prozess und nach Rücksprache mit dem Auftraggeber erfolgen. Updates und Patches müssen vom Auftragnehmer auf korrekte Funktionalität und Kompatibilität überprüft und freigegeben sein.

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. Updates und Patches sollten vorab auf einem Testsystem getestet werden. Insbesondere bei Individualentwicklungen bietet sich hierfür ein mehrstufiges Vorgehen an: 1. Der Auftragnehmer prüft auf Basis des zugrundeliegenden Standardprodukts.

		2. Test und Freigabe durch den Auftragnehmer erfolgen auf einer Testumgebung, die dem System des Betreibers möglichst entspricht. 3. Gegebenenfalls prüft der Betreiber bzw. der Auftragnehmer 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 aufrechtzuerhalten (vgl. 4.1.2). 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.
	Betriebsführungs-/ Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

4.7.3 Konfigurations- und Change-Management, Rollbackmöglichkeiten

Sicherheitsanforderungen	ISO/IEC 27002:2022 8.9, 8.19, 8.29, 8.32 ISO/IEC 27019:2017 12.1.2, 12.5.1, 12.9.1 ENR a) Das System muss mit einem Konfigurations- und Change-Management entwickelt und betrieben werden. b) Das System muss ein Rollback auf eine festgelegte Anzahl von Konfigurationszuständen unterstützen.

Ergänzungen und Anmerkungen:		Sind im Laufe des Systembetriebs nicht-triviale Konfigurations- oder Parametrierungsänderungen zu erwarten, sollte das System ein ausreichendes Konfigurations- und Change-Management unterstützen. Insbesondere sollte ein Rollback auf eine festzulegende Anzahl von vorhergehenden Konfigurationszuständen möglich sein. Die Anforderung gilt sowohl für den Auftragnehmer als auch für den Auftraggeber/Betreiber. Auf Betreiberseite sollten die für eine Konfigurations- und Change-Management notwendigen Prozesse definiert und realisiert werden. Das System soll eine Protokollierung der Änderungen von Konfigurationszuständen unterstützen. zu b) Eine Sicherung von mindestens einem älteren Datenstand (Parametrier- und Firmware-Stand, Datenmodell, etc.), sowie eine Rollbackmöglichkeit sollten vorgesehen werden. Alle Änderungen sollten dokumentiert werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Eine Rollback-Möglichkeit sollte auf Anwendungsebene für dynamische und statische Daten vorgesehen werden. Für Software- und Systemänderungen 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 Firmware-Ständen sollte aber über die Bedien- und Wartungsprogrammen der Geräte möglich sein.

4.7.4 Schwachstellen-Management und Patchinformationsdienst

Sicherheitsanforderungen	ISO/IEC 27002:2022 5.20, 8.8 ISO/IEC 27019:2017 12.6.1 Der Auftragnehmer muss während des gesamten, vertraglich geregelten Betriebszeitraums einen dokumentierten Prozess für das Management von Schwachstellen und Security-Patches für alle Einzelkomponenten und das Gesamtsystem implementieren, der die systematische Behandlung von Schwachstellen und Security-Patches sicherstellt. Der Prozess muss dabei folgende Anforderungen unterstützen: a) Identifikation und Meldung von Schwachstellen und Security-Patches: Der Auftragnehmer muss für alle Einzelkomponenten nachvollziehbar erklären, wie und in welchen Abständen Schwachstel-

	len und Security-Patches identifiziert werden bzw. wie diese beschafft werden. Außerdem muss es allen Beteiligten, aber auch Außenstehenden möglich sein, tatsächliche oder potenzielle Schwachstellen zu melden. b) Bewertung von Schwachstellen und Security-Patches: Die Kritikalität und Relevanz der Schwachstelle bzw. des Security-Patches im Kontext des bereitgestellten Gesamtsystems muss bewertet werden. Die Bewertungsmethodik für Schwachstellen muss mit dem Auftraggeber abgestimmt und nachvollziehbar dokumentiert werden. c) Bereitstellung von Sicherheitsinformationen: Der Auftragnehmer muss den Auftraggeber unter der Maßgabe der Vertraulichkeit regelmäßig über bekannt gewordene Schwachstellen und neu erschienene Security-Patches und deren Kritikalität und Relevanz informieren. Dies gilt auch für den Fall, dass noch kein Patch zur Behebung des Problems zur Verfügung steht. Dabei muss berücksichtigt werden, dass als besonders kritische bewertete Schwachstellen oder Security-Patches unverzüglich mitgeteilt werden müssen. d) Behandlung von Schwachstellen: Der Auftragnehmer muss nachvollziehbar erklären, wie und in welchem Zeitrahmen Schwachstellen behandelt werden bzw. die Security-Patches installiert werden. e) Verwaltung von Schwachstellen: Der Auftragnehmer muss ein Register über die aktuell bekannten und noch nicht abschließend behandelten Schwachstellen führen. f) Der konkrete Zeitrahmen für die Identifikation, Information und Behandlung von Schwachstellen muss vertraglich geregelt werden.

Ergänzungen und 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, siehe auch 4.7.5. Informationen zu Schwachstellen und Security-Patches (nachfolgend Sicherheitsinformation genannt) können typischerweise direkt vom Hersteller der Einzelkomponenten und/oder von amtlichen Quellen (z. B. CERT-Bund oder CISA) bezogen werden. Bereits bekannte Schwachstellen können mittels selbst durch den Lieferanten durchgeführte Schwachstellenscans identifiziert werden. In bestimmten Fällen kann es bei bekannt gewordenen Schwachstellen sinnvoll sein, den Hersteller proaktiv zu kontaktieren, um die Betroffenheit zu prüfen. Die Bewertungsmethodik für Sicherheitsinformationen sollten den Anforderungen des Auftraggebers entsprechen. Für die Bewertung von Sicherheitsinformationen kann das Common Vulnerability Scoring System[2] (CVSS) in der mit dem Auftragnehmer abgestimmten Version verwendet werden. Bei der Bewertung sollen die Gegebenheiten des

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

	Gesamtsystems berücksichtigt werden, um die tatsächlichen Risiken besser einschätzen zu können. Für die Bereitstellung von Sicherheitsinformationen kann ein monatlicher Informationsdienst vereinbart werden, indem Informationen zu bekannt gewordenen Schwachstellen bzw. Security-Patches inklusive der Bewertung und der vorgeschlagenen Vorgehensweise zur Behandlung bereitgestellt werden. Es sollte ein Schwellenwert (z. B. CVSS-Score ≥ 7) für die zeitnahe (z. B. innerhalb einer Woche) Bereitstellung von besonders kritischen Informationen vereinbart werden. 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 Sicherheits-Patches beziehen und den notwendigen Freigabe- und Qualifizierungstests unterziehen. • Informationen über freigegebene Sicherheits-Patches sollten dem Auftraggeber zeitnah nach deren Veröffentlichung zur Verfügung gestellt werden, z. B. per E-Mail, über eine Webseite oder ein Supportforum. • Wenn ein Sicherheits-Patch im gegebenen Systemumfeld als nicht relevant eingestuft wird, sollte dies dokumentiert und dem Auftraggeber mitgeteilt werden. • Wird für einen Sicherheits-Patch 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 aufgrund von Neustarts von Diensten oder Komponenten. • Zu jedem Patch sollte dokumentiert sein, welche Sicherheitslücken adressiert und welche Änderungen vorgenommen werden. Es sollte geprüft werden, ob im regelmäßigen Informationsdienst auch Threat-Intelligence-Informationen enthalten sein sollen. Die Behandlung von Schwachstellen kann auf verschiedene Weise erfolgen. Neben der Akzeptanz von als unkritisch bewerteten Schwachstellen bis zum nächstgeplanten Patch-Zyklus oder die Behandlung durch Konfigurationsänderungen (Workarounds, Mitigations) werden Schwachstellen üblicherweise durch die Installation von Patches im Rahmen des Patch-Managements behoben (siehe 4.1.2 und 4.1.3). Die Verwaltung der Schwachstellen dient zur Überwachung existierender Schwachstellen und insbesondere auch der Verhinderung der Anhäufung von als unkritisch bewerteten Schwachstellen, aus der sich selbst Sicherheitsrisken ergeben können. Die Integration des Prozesses in das betreiber-eigene SOC/CSIRT, sofern vorhanden, sollte berücksichtigt werden.

	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Auto-matisierungs- und Fernwirktechnik:	-

4.7.5 Wartungsvertrag / Service-Level-Agreement

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.19, 5.20, 5.21, 5.22 ISO/IEC 27019:2017 15.1.2 Zur Sicherstellung eines durchgehenden Security-Supports muss ein Wartungsvertrag bzw. ein Service-Level-Agreement mit dem/den Systemlieferanten abgeschlossen werden.

Ergänzungen und Anmerkungen:	Die Vereinbarung sollte die folgenden Themen abdecken, sofern für das Projekt relevant:
	• Laufzeit
	  ○ Der Security-Support sollte spätestens ab der Einbringung des Systems in eine produktive OT-Umgebung gewährleistet sein
	• Festlegungen zum Support-Modell
	  ○ Zuordnung der Support-Level zwischen Auftragnehmer und Auftraggeber
	  ○ Support-Zeiten
	  ○ Fehlerklassen und zugehörige Reaktionszeiten
	  ○ Kontaktinformationen Auftragnehmer und Auftraggeber
	  ○ Rahmenbedingungen für Supportanfrage und -abwicklung, z. B. zu Telefonsupport, Fernzugriff oder durch Vorort-Einsatz
	  ○ Ggf. notwendige Support-Werkzeuge und Infrastruktur, z. B. Ticketing-Tools, Komponenten zur Remote-Wartung
	  ○ Anforderungen zum Wiederanlauf und Notbetrieb
	• Informationspflicht des Auftragnehmers zu ihm bekannten Sicherheitslücken bzw. verfügbaren Security-Patches inklusive angemessener Fristen, inklusive 3rd-Party-Software
	  ○ Unverzügliche Information bei kritischen Schwachstellen
	• Schwachstellen- und Patchmanagement
	  ○ Abdeckung aller notwendigen Hard- und Softwarekomponenten, ggf. inklusive 3rd-Party-Software (Applikationen, Bibliotheken, Softwaremodule, Frameworks, Pakete etc.)
	  ○ Einstufungskriterien für Schwachstellen gemäß der Methodik des Auftraggebers

	○ Proaktive Schwachstellenanalyse und komponenten- bzw. anlagenspezifische, dokumentierte Relevanzbewertung von Schwachstellen/Security-Patches ○ Prüf- und Informationspflichten, Testmethodik und Vorgehen für die Freigabe von Security-Patches inklusive angemessener Fristen, Alternativmaßnahmen bei Nicht-Freigabe ○ Vorgehen für die Bereitstellung von Security-Patches und/oder deren Installation durch den Auftragnehmer inklusive angemessener Fristen ○ Dokumentations-/Mitteilungspflicht und Vorgehensweise bei Betriebsunterbrechungen (z. B. aufgrund von Neustarts) ○ Zyklische Patchfenster und Vorgehen bei kritischen unterzyklischen Patches ○ Zu jedem Patch sollte dokumentiert sein, welche Sicherheitslücken adressiert und welche Änderungen vorgenommen werden • Obsoleszenz-Management ○ Frühzeitige Informationspflicht des Auftragnehmers zur Abkündigung von Produkten und Hardware- und Softwarekomponenten ○ Rahmenbedingungen für notwendige Hard- und Softwareupgrades bzw. entsprechende Upgrade-Projekte • Ersatzteilvorhaltung bei Auftragnehmer oder Auftraggeber • Sichere Entsorgung von Assets durch den Auftragnehmer • Regelmäßig notwendige Pflegearbeiten des Auftragnehmers • Sofern erforderlich, Vorhaltung eines Testsystems beim Auftragnehmer ○ Umfang und Aufbau des Testsystems ○ Notwendige Pflegearbeiten am Testsystem • Vorgaben an das Personal des Auftragnehmers, z. B. Ausbildung/Kompetenzen, namentliche Benennung, Sicherheitsüberprüfung etc. • Schulungspflichten des Auftragnehmers, u. a. zu den Security-Vorgaben des Auftraggebers • Dokumentationspflichten • Pflicht zur Meldung von Security-Incidents, die in Zusammenhang mit dem Auftraggeber stehen bzw. eine Auswirkung auf diesen oder die Dienstleistungserbringung haben können • Festlegung von wesentlichen Key-Performance-Indikatoren • Reporting durch den Auftragnehmer (Umfang und Zyklus) • Auditrecht des Auftraggebers, z. B. Fristen, Vorgehen und Kostenübernahme • Anforderungen an das Konfigurationsmanagement • Anforderungen an sichere Wartungsprozesse (siehe 4.7.1)

	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungs-technik / Sprach-kommunikation:	-
	Sekundär-, Auto-matisierungs- und Fernwirktechnik:	-

4.8 Datensicherung und Notfallplanung

Dieses Kapitel beschreibt Anforderungen, die im Bereich der Datensicherung und Notfallplanung berücksichtigt werden sollten.

4.8.1 Backup: Konzept, Verfahren, Dokumentation, Tests

Sicherheits-anforderungen	ISO/IEC 27002:2022 5.37, 8.13 ISO/IEC 27019:2017 12.1.1 Es müssen dokumentierte und getestete Verfahren zur Datensicherung und -wiederherstellung der Einzelkomponenten bzw. des Gesamtsystems und der jeweiligen Konfigurationen existieren. Die Konfigurationsparameter von dezentralen Komponenten müssen zentral gesichert werden können. Die Dokumentation und die Verfahren müssen bei relevanten System-Updates angepasst und erneut getestet werden.

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. Der maximal zulässige Datenverlust (Recovery Point Objective, RPO) und die Wiederherstellungszeit-Vorgabe (Recovery Time Objective, RTO) sollten zwischen Auftragnehmer und Auftraggeber abgestimmt und dokumentiert 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. Das Sicherungs-/Rücksicherungsverfahren sollte jederzeit für das Gesamtsystem konsistente Datenstände gewährleisten können. Es sollten Mechanismen vorgesehen werden, mit denen die Vollständigkeit und Korrektheit einer Datensicherung gegen den aktuellen Datenbestand geprüft werden kann. Das Sicherungsverfahren sollte den Schutzbedarf der zu sichernden Daten berücksichtigen, z. B. durch Verwendung von Verschlüsselung. Die Datensicherungs- und Rücksicherungsverfahren sollten ausführlich dokumentiert werden. Im Rahmen des Abnahmetests sollte eine vollständige Sicherung und Rücksicherung mit realistischen Datenmengen geprüft werden. Die

		Tests sollten durch den Systembetreiber regelmäßig wiederholt werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	Es sollte insbesondere auch eine zyklische Sicherung aller manuell eingegebenen Daten (Verfügungserlaubnis, Meldesperre, usw.) vorgesehen werden.
	Übertragungstechnik / Sprachkommunikation:	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:	

4.8.2 Notfallkonzeption und Wiederanlaufplanung

Sicherheitsanforderungen	ISO/IEC 27002:2022 5.29, 5.30, 8.14 ISO/IEC 27019:2017 17.2.1 Für relevante Notfall- und Krisenszenarien müssen vom Auftragnehmer dokumentierte und getestete Vorgehensweisen und Wiederanlaufpläne inklusive Angabe der Wiederherstellungszeiten zur Verfügung gestellt werden. Die Dokumentation und Verfahren müssen bei relevanten System-Updates angepasst und im Rahmen des Abnahmeverfahrens für Release-Wechsel erneut getestet werden.

Ergänzungen und Anmerkungen:	Die Notfallkonzeption und die Wiederanlaufplanung sollte mit den Vorgaben des Auftraggebers zum maximal zulässigen Datenverlust (Recovery Point Objective, RPO) und zur Wiederherstellungszeit (Recovery Time Objective, RTO) konform sein. Relevante Notfall- und Krisenszenarien sollten aufseiten des Betreibers bzw. Auftraggebers im Rahmen eines bereichsübergreifenden 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. Werden Dienstleistungen des Auftragnehmers für Wiederanlauf und Notbetrieb benötigt, sollten diese vertraglich vereinbart werden. 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. Auf Betreiberseite sollten Wiederanlaufplanung und die Notfallkonzepte zyklisch geprüft und ggf. angepasst werden.
	Betriebsführungs- / Leitsysteme und Systembetrieb:	-
	Übertragungstechnik / Sprachkommunikation:	-
	Sekundär-, Automatisierungs- und Fernwirktechnik:	-

Anhang

A Netzwerkzonen-Diagramme

Netzwerkzonen-Diagramm 1

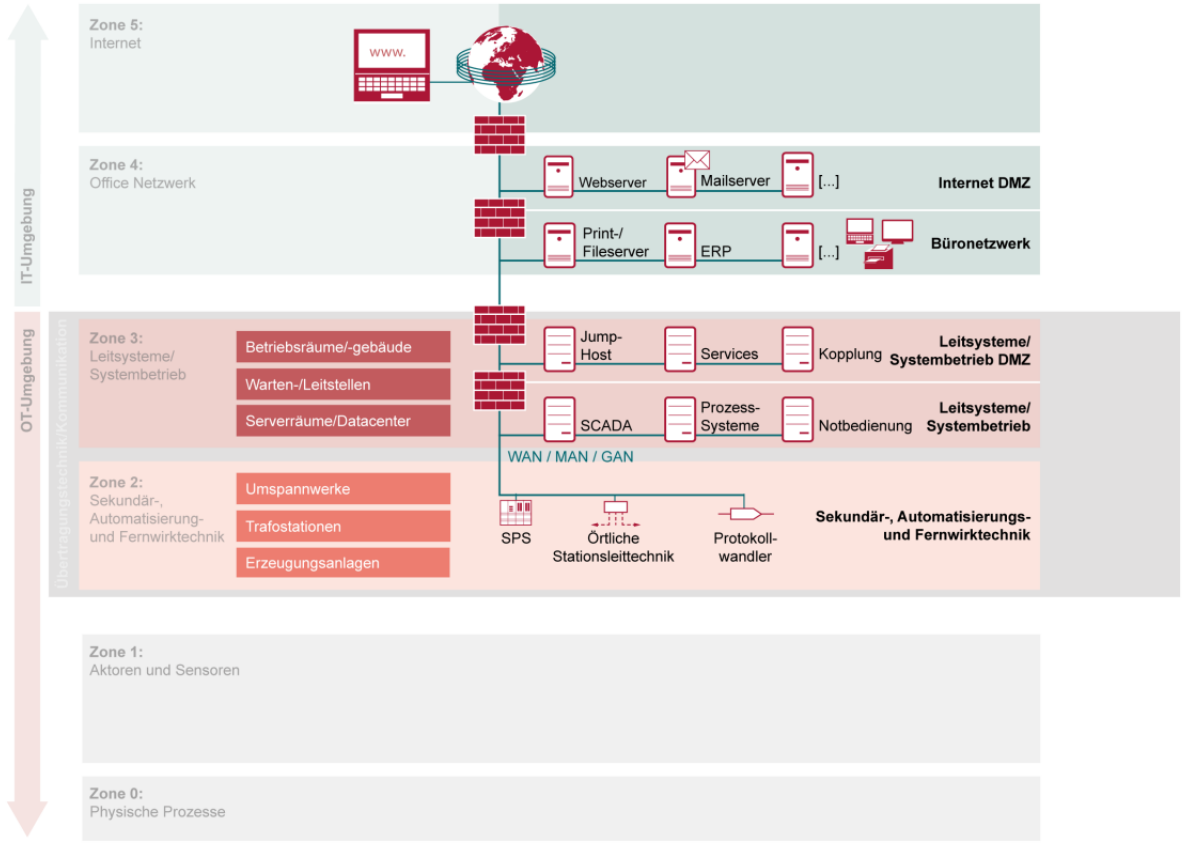

Abbildung 1: Generischer Strukturplan mit Zonen und Technologiekategorien

Netzwerkzonen-Diagramm 2

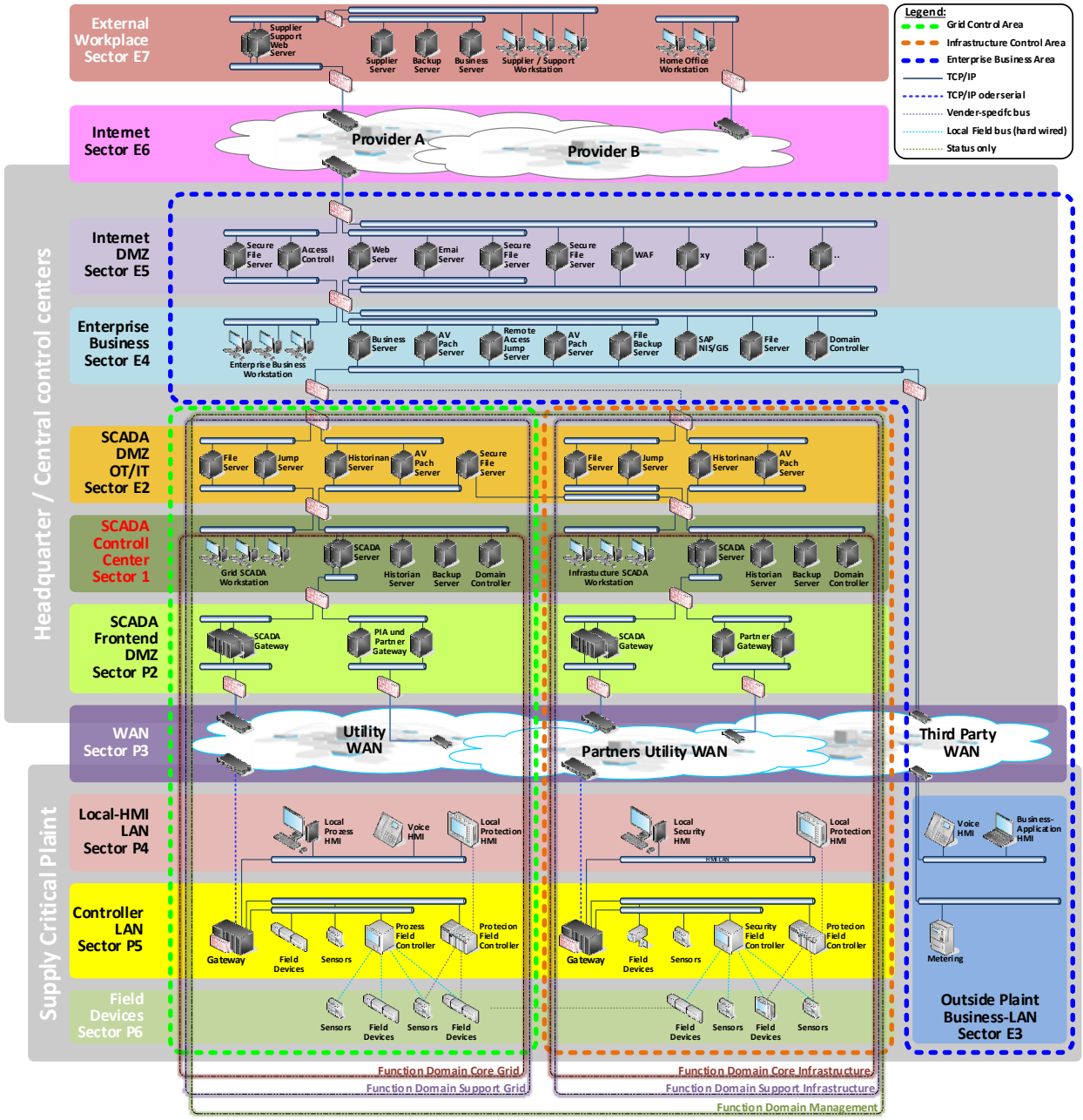

Abbildung 2: Beispiel einer Netzwerkarchitektur

B Abkürzungsverzeichnis und Glossar

2-Faktor-Authentifizierung	Authentifizierung unter Verwendung zweier verschiedener Authentifizierungsmechanismen, z. B. Passwort und Chipkarte
3rd-Party-Produkte	Standard-Software bzw. -Hardware, die vom Systemlieferanten zugekauft wird, z. B. Datenbank, Compiler, Rechner, Netzwerkkomponenten, usw.
ACL	Access Control List
Applikation	Anwendungsprogramm
Applikations-Proxy bzw. Application Level Gateway	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 und Middleware inklusive Grundkomponenten wie z. B. X11 oder Datenbanksysteme, 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.
BIOS	Basic Input/Output System, Firmware eines x86-Systems
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
Change-Management	Managementprozess, mit dem das Testen, Anwenden und Dokumentieren von Hard- und Softwareupdates, Konfigurationsanpassungen und sonstiger Änderungen gesteuert und verwaltet wird
CET	Central European Time, mitteleuropäische Zeit
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency
COBIT	Control Objectives for Information and Related Technologies, international anerkanntes Framework zur IT-Governance
CRL	Certificate Revocation List
CSIRT	Computer Security Incident Response Team
DCOM	Distributed Component Object Model
DHCP	Dynamic Host Configuration Protocol

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 ein System oder eine Systemkomponente mit der Absicht, das Angriffsziel arbeitsunfähig zu machen, z. B. durch Beanspruchung der gesamten verfügbaren Rechenleistung oder Netzwerkkapazität
EAP	Extensible Authentication Protocol
ENR	Präfix der sektor-spezifischen Anforderungen in ISO/IEC 27019
EMV	Elektromagnetische Verträglichkeit
EST	Enrollment over Secure Transport
EVU	Energieversorgungsunternehmen
FAT	Factory Acceptance Test
Gateway	Ein Gateway ermöglicht die Verbindung von Komponenten oder Netzwerken, die auf unterschiedlichen Protokollen basieren
Gesamtsystem	Im vorliegenden Dokument alle vom Auftragnehmer gelieferten Hard- und Software-Komponenten, z. B. Applikationen, Betriebssysteme, Firmware, Rechnersysteme und die Netzwerk-Infrastruktur
GOOSE	Generic Object Oriented Substation Events
HMI	Human-Machine-Interface
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISO/IEC 27002	ISO/IEC-Standard für Informationssicherheit
ISO/IEC 27019	Sektor-spezifischer ISO/IEC-Informationssicherheitsstandard für die Energieversorgung
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

KVM	Keyboard Video Mouse
LAN	Local Area Network
Lifecycle / Lebens-zyklus	Lebenszyklus eines Systems beginnend mit der Planung, über die Ausschreibung, die Implementierung, Inbetriebnahme, den eigentlichen Betrieb, bis hin zur Demontage und Entsorgung
MAC	Media access control
MPLS	Multiprotocol Label Switching
NIST	National Institute of Standards and Technology
Netzwerk-Perime-ter	Netzwerksystem, das den Übergang zu einem externen Netzwerk bildet, z. B. ein Router, eine Firewall oder ein Remote-Access-System
Netzwerk-TAP	Netzwerkgerät für den Abgriff (*wiretapping*) von Datenverkehr (TAP: Test Access Point)
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OPC	Open Platform Communications, in der Automatisierungstechnik häufig genutzte Kommunikationsschnittstelle
OPC-UA	OPC Unified Architecture
OT	Operational Technology Die in diesem Dokument verwendete OT-Definition wird in Kapitel 1 “Einleitung und Geltungsbereich“ erläutert. Es existieren verschiedene alternative Begriffsdefinitionen, wie z. B.: • *„Operational technology (OT) encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.“* Quelle: https://csrc.nist.gov/Projects/operational-technology-security • *„Prozessleit- und Automatisierungstechnik (Operational Technology, OT) ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert.“* Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/08_IND_Industrielle_IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2021.pdf • *„Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.“* Quelle: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

- *„Der Begriff ‚OT' bezeichnet die Technologie, welche unter Einsatz von Hard- und Software physische Geräte, Prozesse und Ereignisse überwacht und / oder steuert. OT umfasst dabei unter anderem spezialisierte industrielle Systeme wie die Stationsleit-, Fernwirk- und Schutztechnik. Ebenso zählen im OT-Umfeld eingebundene Netzwerkkomponenten, die Automatisierungstechnik, die Regelungstechnik sowie technische Gebäudeausrüstung, die Objektsicherheitstechnik und ggf. safety-relevante Komponenten zur OT."*
  Quelle: Eigendefinition

Out-Of-Band-Kommunikation	Kommunikation, die nicht die primäre, zur Nutzdatenkommunikation vorgesehene Kommunikationsanbindung nutzt
OWASP	Open Web Application Security Project
Patch-Management	Managementprozess, mit dem das Testen, Installieren, Verteilen und Dokumentieren von Sicherheits-Patches und Software-Updates gesteuert und verwaltet wird
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
PKI	Public Key Infrastructure
R-GOOSE	Routed GOOSE, siehe GOOSE
R-SV	Routed SV, siehe SV
RDP	Remote Desktop Protocol
RFC	Request for Comments
RFID	Radio-frequency identification
Rollback	Das vollständige Zurücksetzen eines IT-Systems in einen definierten Ausgangszustand, z. B. vor Durchführung eines Softwareupdates oder nach einer fehlerhaften Änderung
Rolle	siehe Benutzerrolle
RPC	Remote Procedure Call
Safety	Freiheit von untragbaren Risiken
SAT	Site Acceptance Test
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SFTP	SSH File Transfer Protocol
SIEM	Security Information and Event Management

S/MIME	Secure / Multipurpose Internet Mail Extensions
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOC	Security Operations Center
SPS	Speicherprogrammierbare Steuerung
SSH	Secure Shell Protocol, verschlüsseltes Terminalprotokoll
Stresstest	Test, bei dem das Verhalten einer Soft- oder Hardwarekomponente unter hoher Last bzw. bei Verarbeitung von außerhalb der Spezifikation liegenden Daten überprüft wird
SV	Sampled Values
System	siehe Gesamtsystem
TAP	siehe Netzwerk-TAP
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technische Richtlinie
UDP	User Datagram Protocol
USB	Universal Serial Bus
UTC	Universal Time Coordinated, koordinierte Weltzeit
ÜT	Übertragungstechnik
Verzeichnisdienst	Netzwerkdienst, der eine zentrale Sammlung an bestimmten Daten zur Verfügung stellt, z. B. Usernamen, Berechtigungen, u. ä.
VLAN	Virtual Local Area Network, Methode um auf einem physischen Netzwerk verschiedene logische Netze einzurichten
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless LAN
X.509	Standard des International Telecommunication Union (ITU) für das Format von digitalen Zertifikaten

C Referenzen und Verweise

Internationale Normen

ISO/IEC 27000 Reihe „Information security, cybersecurity and privacy protection“:

ISO/IEC 27001: Information security management systems — Requirements

ISO/IEC 27002: Information security controls

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

IEC 62351 Reihe „Power systems management and associated information exchange — Data and communications security“:

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

IEC 62351-4: Profiles including MMS and derivatives

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

IEC 62351-6: Security for IEC 61850

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

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

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

IEC TR 62351-10: Security architecture guidelines

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

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

Frameworks und Handlungsempfehlungen

BSI - Bundesamt für Sicherheit in der Informationstechnik (Deutschland)

ICS-Security-Kompendium

ICS-Security-Kompendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten

NIST - National Institute of Standards and Technology (USA)

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

NIST Special Publication 800-121 — Guide to Bluetooth Security

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