

Industrie, Robotik und OT-Sicherheit

Leitfaden für Betreiber, Maschinenbauer, Integratoren und Produktionsverantwortliche

Fachlicher Leitfaden zur Cyber-Physical-AI-Security.

Fassung 1.1 · Stand 25. September 2026 · Adressaten: Werk- und Produktionsleitung, OT-Verantwortliche, Automatisierung, funktionale Sicherheit, Robotikintegration, Instandhaltung, Qualität, Informationssicherheit und Einkauf.

Dokumenttyp: Ausgearbeitete Fachfassung; anlagenbezogene Engineering- und Betriebsfreigabe erforderlich

Die Fallstudien in diesem Leitfaden-Paket sind ausdrücklich konstruierte Prüfbeispiele; eine externe wissenschaftliche, klinische, juristische oder sicherheitstechnische Begutachtung des Pakets hat nicht stattgefunden.

Steckbrief

Merkmal	Wert
Dokumenttyp	Ausgearbeitete Fachfassung; anlagenbezogene Engineering- und Betriebsfreigabe erforderlich
Zielgruppe	Werk- und Produktionsleitung, OT-Verantwortliche, Automatisierung, funktionale Sicherheit, Robotikintegration, Instandhaltung, Qualität, Informationssicherheit und Einkauf.
Recherche- und Rechtsstand	25. September 2026
Umfang	3.839 Wörter, 14 Seiten
Belege	0 Literatureinträge, 12 Quellenadressen
Gliederung	20 nummerierte Abschnitte, 0 Tabellen

Inhalt

1. Ausgangspunkt: Welche Wirkung kann Software in dieser Anlage auslösen?	4
2. Drei Verantwortungsbereiche, die zusammenarbeiten müssen	4
3. Das Anlageninventar muss vier Sichten verbinden	4
4. Datenwerte und Angriffsmotive jenseits der Maschinenbewegung	5
5. Sicherheitsanalyse von der Verlustfolge rückwärts	5
6. Zonen und Kommunikationspfade als Entwurfsinstrument	5
7. Handlungsvollmacht von KI und Optimierungssystemen	6
8. Unabhängige Schutzfunktionen und gemeinsame Ursachen	6
9. Mobile Robotik und Flottenkoordination	6
10. Qualität, Chargen und stille Manipulation	7
11. Engineering-Stationen, Fernwartung und Herstellerzugänge	7
12. Änderungen an KI, Software und Parametern	7
13. Brownfield: Umgang mit Altanlagen	8
14. Detektion mit Prozesskontext	8
15. Notbetrieb und kontrollierter Stillstand	8
16. Wiederherstellung umfasst die physische und digitale Realität	9
17. Abnahmetests und Negativproben	9
18. Maschinenrecht, Normen und betriebliche Anforderungen	9
19. Entscheidungsvorlage für Werkleitung und technischen Ausschuss	9
20. Arbeitsunterlagen und Ergebnis	10
Literatur und Quellenstatus	10
12 Rechtliche Hinweise	12
12.1 Keine Beratung	12
12.2 Keine Zusicherung, keine Konformitätsaussage	12
12.3 Rechtsstand	12
12.4 Haftung	12
12.5 Verweise auf fremde Inhalte	12
12.6 Marken und Produktbezeichnungen	12
12.7 Urheberrecht und Nutzung	12
12.8 Keine personenbezogenen Daten	13
12.9 Unabhängigkeit	13
12.10 Anwendbares Recht	13

Impressum und Verantwortlichkeit

Die folgenden Angaben sind wörtlich dem Impressum von fluxlane.eu entnommen, abgerufen am 24. September 2026. Sie wurden nicht ergänzt und nicht umformuliert.

Angabe	Inhalt
Angaben gemäß § 5 DDG	WebTrades GmbH Am Ölberg 2 55459 Grolsheim Deutschland
Vertreten durch	Geschäftsführerin: Laurice Bussmer
Kontakt	Telefon: 0170 890 78 00 E-Mail: info@fluxlane.eu
Registereintrag	Eintragung im Handelsregister Registergericht: Amtsgericht Mainz Registernummer: HRB 54479
Umsatzsteuer-ID	Umsatzsteuer-Identifikationsnummer gemäß § 27 a Umsatzsteuergesetz: DE461650292
Redaktionell verantwortlich	Verantwortlich für den Inhalt nach § 18 Abs. 2 MStV: Laurice Bussmer, Am Ölberg 2, 55459 Grolsheim
Verbraucherstreitbeilegung	Wir sind nicht bereit oder verpflichtet, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen.

Redaktioneller Hinweis des Herausgebers (wörtlich)

„fluxlane ist ein unabhängiges, redaktionelles Fachportal für Robotik, autonome physische Systeme und verkörperte KI. Der redaktionelle Geltungsbereich umfasst Industrie und Produktion, Logistik, Medizin, Pflege und Rehabilitation, Service und Haushalt sowie Forschung, Hersteller, Markt und Regulierung; künstliche Intelligenz gehört dazu, auch ohne physischen Körper. Die Inhalte dienen der allgemeinen Information und stellen keine Rechts-, Kauf- oder Anlageberatung dar. Angaben zu Preisen, Verfügbarkeit und Terminen erfolgen ohne Gewähr und können sich jederzeit ändern.“

Zitierweise

FluxLane (2026): *Industrie, Robotik und OT-Sicherheit – Leitfaden für Betreiber, Maschinenbauer, Integratoren und Produktionsverantwortliche*. Fassung 1.1, Stand 25. September 2026. Herausgegeben von der WebTrades GmbH, Grolsheim, fluxlane.eu.

Herstellung dieses Dokuments

Das vorliegende PDF ist maschinell aus der Markdown-Fassung des Leitfaden-Pakets gesetzt. Inhaltlich ist dieser Satzvorgang keine neue Sachprüfung; die zugrunde liegende Recherche- und Quellenprüfung ist im Lieferpaket dokumentiert. Gesetzt wurde mit IBM Plex Sans und Sora.

Abbildungsnachweis

Dieses Dokument enthält eine schematische Abbildung: Zonen und Kommunikationspfade als Entwurfsinstrument (Abschnitt 6). Die Abbildung ist ein Entwurfsschema, keine reale Netzwerktopologie und keine Bewertung nach einem Security Level. Ergänzt in Fassung 1.1 am 27. September 2026.

1. Ausgangspunkt: Welche Wirkung kann Software in dieser Anlage auslösen?

Eine Fabrik ist nicht allein durch ihre Netzwerkanschlüsse beschrieben. Die relevante Frage ist, welche Befehle, Parameter und Informationen die Produktion verändern können. Dazu zählen Programme und Prozesswerte ebenso wie Auftragsreihenfolge, Qualitätsfreigaben, Materialzuordnung, Wartungsdiagnosen oder die Disposition autonomer Transportmittel. Ein Angreifer muss keinen Robotercontroller direkt übernehmen, wenn eine vorgelagerte Anwendung genügend Wirkung entfalten kann.

Der Leitfaden trennt daher **Verlust von Prozesskontrolle, Verlust der zuverlässigen Prozesssicht, Verlust von Schutzfunktionen, Verlust von Datenvertraulichkeit und Verlust nachweisbarer Produktqualität**. Diese Kategorien können gleichzeitig auftreten, haben aber unterschiedliche Barrieren. MITRE verwendet für industrielle Angriffe unter anderem den Begriff „Loss of Safety“. NIST behandelt die besonderen Sicherheits-, Verfügbarkeits- und Zuverlässigkeitsanforderungen von OT ausdrücklich. [Q27; Q02, §§ 2.4 und 5.3]

Der zu führende Nachweis lautet nicht „Unsere Roboter können nicht gehackt werden“. Er lautet: Die zulässigen Wirkungspfade sind bekannt; missbräuchliche oder fehlerhafte Handlungen werden ausreichend begrenzt; verbleibende Störungen können ohne unvertretbare Gefährdung und mit nachvollziehbarer Produktbewertung beherrscht werden.

2. Drei Verantwortungsbereiche, die zusammenarbeiten müssen

Der Maschinen- oder Komponentenhersteller beschreibt die vorgesehene Verwendung, technische Eigenschaften und Bedingungen des sicheren Einsatzes. Der Integrator gestaltet die konkrete Anwendung, etwa Werkzeug, Zelle, Materialfluss, Mensch-Maschine-Interaktion und Verbindung zu weiteren Systemen. Der Betreiber organisiert den Einsatz im tatsächlichen Betrieb, einschließlich Personal, Änderungen, Instandhaltung und Störungsmanagement. Welche rechtliche Rolle im Einzelfall vorliegt, hängt von Lieferung, Integration und Änderungen ab; sie kann nicht allein aus einer Vertragsüberschrift abgelesen werden.

Die ISO-10218-Reihe unterscheidet entsprechend in ihrer Ausgabe 2025 den Industrieroboter und die Anwendung beziehungsweise Zelle. Die öffentlichen Scopes begrenzen zugleich die Übertragbarkeit auf andere Roboterarten. Eine Industrieroboter-Norm wird nicht dadurch zur vollständigen Grundlage für einen OP-Roboter oder einen öffentlichen Serviceroboter, dass diese ebenfalls einen Arm oder Sensoren besitzen. [Q25; Q26, Scope]

Der Betreiber benötigt außerdem eine betriebliche Gefährdungsbeurteilung. § 3 BetrSichV macht deutlich, dass eine CE-Kennzeichnung diese nicht ersetzt. Das bedeutet für die hier untersuchte Vernetzung: Auch bei ordnungsgemäß beschafften Einzelprodukten sind neue Zugriffe, Betriebsbedingungen und Wechselwirkungen zu beurteilen. [Q31, Abs. 1–3]

3. Das Anlageninventar muss vier Sichten verbinden

Die erste Sicht beschreibt **Anlagen und Funktionen**: Roboter, Steuerungen, Antriebe, Sensoren, Aktoren, lokale Bedienung, Schutzfunktionen und Materialfluss. Die zweite beschreibt **digitale Abhängigkeiten**: Produktionsplanung, Manufacturing Execution System, Qualitätsdatenbank, Identitätsdienste, Engineering-Stationen, Fernwartung, Updateverteilung und gegebenenfalls Cloudfunktionen. Die dritte beschreibt **Handlungsvollmachten**: Wer darf beobachten, auftragen, konfigurieren, freigeben, bewegen oder stoppen? Die vierte beschreibt **Produkt- und Auftragsbezug**: Welche Daten und Parameter gehören zu welchem Produktstand, welcher Charge und welchem Prozessfenster?

Eine Anlage bleibt im Inventar unzureichend beschrieben, wenn ein zentraler Wartungszugang nur als IP-Adresse auftaucht. Erforderlich sind Eigentümer, Zweck, erlaubte Zielsysteme, Berechtigungsdauer, Protokollierung, Abschaltmöglichkeit und Verhalten bei Kommunikationsverlust. Entsprechendes gilt für KI-Dienste: Ihre Rolle wird anhand tatsächlicher Werkzeuge und Rechte erfasst, nicht anhand einer Werbeaussage über „Optimierung“.

Der Leistungsabhängigkeitsgraph zeigt auch versteckte gemeinsame Ursachen. Zwei Produktionslinien können dieselben Engineering-Dateien, denselben Lizenzdienst oder dieselbe zentrale Zertifikatsverwaltung benötigen. Ein als unabhängig betrachteter Backupserver kann über dasselbe Administrationskonto erreichbar sein wie die

produktive Umgebung. Solche Befunde sind vorrangig zu bearbeiten, wenn sie gleichzeitig Betrieb und Wiederherstellung beeinträchtigen können.

4. Datenwerte und Angriffsmotive jenseits der Maschinenbewegung

Industrielle Daten können Kundenbeziehungen, Konstruktionswissen, Rezepturen, Prozessfenster, Ausschussursachen, Produktionsmengen oder Wartungszustände offenlegen. Ein digitaler Zwilling kann einen Teil dieses Wissens zusammenführen. Welche Daten tatsächlich schutzwürdig sind, muss anhand des konkreten Betriebs ermittelt werden; der Begriff „Digital Twin“ allein sagt nichts über Umfang oder Geheimhaltungswert aus.

Ein Datenabfluss kann folgenreich sein, ohne eine sichtbare Störung auszulösen. Deshalb dürfen Detektionskonzepte nicht ausschließlich auf Stillstände und ungewöhnliche Bewegungen reagieren. Ein berechtigter Analysedienst, der plötzlich umfangreiche Konstruktions- oder Bilddaten exportiert, kann eine andere Risikoklasse berühren als ein lokaler Diagnosezugriff. Die Grenze des zulässigen Exports gehört in den Schnittstellen- und Berechtigungsvertrag.

Maschinenkameras und technische Protokolle können außerdem Personen oder personenbezogene Arbeitsabläufe erfassen. Die Sicherheitsverarbeitung benötigt daher einen angemessenen Zweck- und Zugriffsrahmen. Schutz vor Industriespionage rechtfertigt nicht automatisch unbegrenzte Mitarbeiterüberwachung. Die einschlägige Datenschutz- und gegebenenfalls Mitbestimmungsprüfung ist Teil des Einführungsverfahrens. [Q32, § 87 Abs. 1 Nr. 6; Q38, Prüfsuchstellen]

5. Sicherheitsanalyse von der Verlustfolge rückwärts

Für jeden kritischen Prozess wird zunächst benannt, welcher Verlust verhindert werden soll. Beispiele sind Personengefährdung im Bewegungsbereich, unerlaubte Freisetzung eines Mediums, Beschädigung eines Werkstücks, Ausfall einer Kühl- oder Haltefunktion, unerkannter Qualitätsverlust oder Weitergabe eines Fertigungsgeheimnisses. Danach werden mögliche gefährliche Zustände und die zugehörigen digitalen Einflusswege beschrieben.

Ein Roboter könnte beispielsweise einen formal gültigen Auftrag erhalten, dessen Ziel unter dem aktuellen Anlagenzustand unzulässig ist. Die Ursache kann eine manipulierte Planung, eine veraltete Ortsinformation oder ein fehlerhafter Integrationsschritt sein. Die Analyse darf nicht beim Motiv des Angreifers enden. Dieselbe unerwünschte Wirkung kann durch Softwarefehler, falsche Stammdaten oder missverstandene Bedienereingaben entstehen.

Für jede Kette werden präventive, begrenzende und erkennbare Barrieren festgelegt. Eine Zugangsbeschränkung schützt die Konfiguration. Eine unabhängige, geeignete Schutzfunktion begrenzt gefährliche Wirkung. Eine Prozessüberwachung kann Abweichungen anzeigen. Eine Produktprüfung kann betroffene Erzeugnisse zurückhalten. Keine dieser Aufgaben lässt sich vollständig durch eine andere ersetzen. Der historische Triton-Fall verdeutlicht, dass auch Safety-Umgebungen Ziel eines Angriffs werden können; er liefert jedoch keinen Nachweis für die Verwundbarkeit einer beliebigen heutigen Roboterzelle. [Q28]

6. Zonen und Kommunikationspfade als Entwurfsinstrument

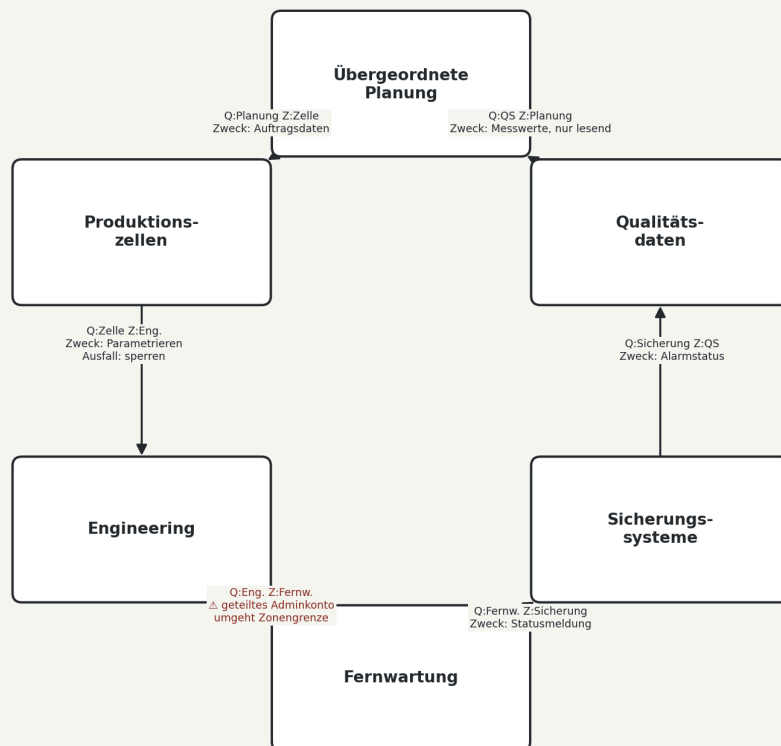
Die öffentlich beschriebene IEC 62443-3-2 ordnet industrielle Sicherheitsbewertung nach dem betrachteten System, Zonen und Kommunikationsverbindungen. In diesem Leitfaden wird diese Grundidee genutzt, um gleichartige Schutzbedarfe und erlaubte Übergänge nachvollziehbar zu machen. Es wird kein Security Level ohne normative Volltextprüfung oder anlagenbezogene Bewertung vergeben. [Q24, Abstract]

Zonen können beispielsweise Produktionszellen, übergeordnete Planung, Engineering, Fernwartung, Qualitätsdaten und Sicherungssysteme trennen. Entscheidend ist nicht die Zahl der VLANs, sondern die tatsächliche Durchsetzung erlaubter Verbindungen und Handlungen. Ein geteiltes Administratorenkonto oder ein uneingeschränkter Engineering-Laptop kann sorgfältig gezeichnete Zonengrenzen faktisch umgehen.

Jeder Kommunikationspfad erhält deshalb einen fachlichen Vertrag: Quelle, Ziel, Zweck, Protokoll, Datenobjekte, erlaubte Änderungen und Verhalten bei Ausfall. Vorhandene Regeln werden gegen beobachteten Betrieb und genehmigte Testfälle geprüft. Die erste Bestandsaufnahme sollte in empfindlichen OT-Umgebungen nicht durch

Zonen und Kommunikationspfade als Entwurfsinstrument

Jeder Pfeil braucht einen fachlichen Vertrag: Quelle, Ziel, Zweck, Protokoll, Datenobjekte, erlaubte Änderungen, Verhalten bei Ausfall



△ markierter Pfad: „Ein geteiltes Administratorenkonto oder ein uneingeschränkter Engineering-Laptop kann sorgfältig gezeichnete Zonengrenzen faktisch umgehen.“

Entscheidend ist nicht die Zahl der Zonen, sondern die tatsächliche Durchsetzung erlaubter Verbindungen. Kein Security Level ohne normative Volltextprüfung oder anlagenbezogene Bewertung.

Abbildung · Zonen und Kommunikationspfade als Entwurfsinstrument (zu Abschnitt 6)

unfreigegebene aktive Scans erfolgen. NIST behandelt die Besonderheiten solcher Systeme und ihrer Betriebsbedingungen; der Betreiber muss die konkrete Prüfmethode mit den Anlagenverantwortlichen abstimmen. [Q02, §§ 5.2 und 6.3]

7. Handlungsvollmacht von KI und Optimierungssystemen

Eine Optimierungs-KI kann Aufträge vorschlagen, Maschinenzustände auswerten oder innerhalb freigegebener Grenzen Prozessvorgaben erzeugen. Daraus folgt keine Berechtigung, Schutzparameter oder Betriebsarten zu verändern. Diese Trennung muss technisch sichtbar sein. Ein Vertrag, in dem „nur Empfehlungen“ steht, schützt nicht, wenn die Integration die Empfehlung automatisch als verbindlichen Auftrag weiterleitet.

Eine geeignete Architektur unterscheidet Vorschlag, fachliche Prüfung, genehmigten Auftrag und Ausführung. Nicht jede Stufe benötigt zwingend einen menschlichen Klick; erforderlich sind aber nach Risiko abgestimmte Grenzen und überprüfbare Zuständigkeiten. Routineaktionen können innerhalb eines festgelegten Rahmens automatisch erfolgen. Änderungen des Rahmens selbst erhalten strengere Freigaben und getrennte Berechtigungen.

Die letzte sicherheitsgerichtete Begrenzung darf nicht allein von dem generativen Modell abhängen, das die operative Aktion erzeugt. Daraus folgt nicht pauschal, dass jede Anwendung dieselbe Safety-SPS benötigt. Es folgt, dass der Sicherheitsnachweis nicht auf der unbelegten Annahme beruhen darf, das Modell werde gefährliche Vorschläge zuverlässig selbst vermeiden. Welche technische Schutzarchitektur notwendig ist, bestimmt die konkrete Risikobeurteilung und das einschlägige Regelwerk.

8. Unabhängige Schutzfunktionen und gemeinsame Ursachen

Die sicherheitsbezogene Funktion muss unter den Bedingungen wirksam bleiben, für die sie vorgesehen ist. Dazu zählt die Prüfung, ob ein kompromittierter Managementzugang ihre Parameter verändern, ihre Signale verfälschen oder ihre Diagnose unterdrücken kann. Getrennte Rollen und Komponenten reichen nicht aus, wenn dieselbe administrative Vertrauensketten alle Ebenen beherrscht.

Ein Prüfer sollte daher Engineering-Zugänge, Updatewege, Schlüsselverwaltung und Sensorquellen gemeinsam betrachten. Wenn ein KI-Dienst seinen eigenen zulässigen Arbeitsraum durch Änderung eines Kartendatensatzes erweitern kann, ist die Begrenzung nicht unabhängig. Wenn eine Schutzfunktion ausschließlich dieselbe ungesicherte Prozessinformation nutzt wie die operative Steuerung, ist ein möglicher gemeinsamer Fehler zu analysieren. Die konkrete technische Lösung kann je nach Anwendung sehr verschieden sein.

Not-Halt, sicherer Stopp, Energieabschaltung und Cyber-Eingrenzung sind keine Synonyme. Ein sofortiger Energieverlust kann bei bestimmten Prozessen zusätzliche Gefahren auslösen. Umgekehrt kann ein geordneter Prozessstopp ungeeignet sein, wenn eine unmittelbare gefährliche Bewegung begrenzt werden muss. Dieser Leitfaden legt deshalb keine universelle Abschaltsequenz fest. Er verlangt eine anlagenbezogen begründete Zuordnung von Ereignis, notwendiger Wirkung und geeigneter Schutzfunktion. [Q02, §§ 2.3.7 und 5.3]

9. Mobile Robotik und Flottenkoordination

Bei autonomen mobilen Robotern besteht ein Unterschied zwischen lokalem Fahrverhalten und Flottenkoordination. Eine lokale Schutzfunktion kann gefährliche Kollisionen begrenzen, während ein kompromittierter Flottenmanager weiterhin Wege blockiert, Aufträge falsch verteilt oder notwendige Transporte verzögert. Der Nachweis kollisionsbezogener Sicherheit ersetzt daher nicht die Betrachtung der betrieblichen Folgen.

Die Flottenanalyse erfasst Auftragserzeugung, Prioritäten, Karten- und Zonenstände, Ladeinfrastruktur, Verkehrsregeln und örtliche Bedienung. Ein nicht autorisierter Wechsel der Betriebsart oder eine massenhafte Änderung von Missionsaufträgen muss technisch begrenzt und nachvollziehbar sein. Die Zulässigkeit eines Befehls hängt auch vom Zustand der Umgebung ab: Ein zuvor freier Übergabepunkt kann inzwischen belegt oder für Menschen reserviert sein.

Kommunikationsverlust ist gesondert zu prüfen. Entscheidend ist nicht allein, ob der Roboter „stoppt“, sondern wo und in welchem Zustand er bleibt, ob Flucht- oder Transportwege betroffen sind, wie lokale Bedienung erfolgt und

welche Informationen bei Wiederverbindung als gültig gelten. Eine alte Missionswarteschlange darf nicht ohne Zustandsabgleich automatisch wieder wirksam werden. Die konkrete Verhaltensdefinition erfolgt mit Hersteller und Integrator in einer genehmigten Testumgebung.

10. Qualität, Chargen und stille Manipulation

Ein Angriff kann das Produkt verändern, ohne eine offensichtliche Anlagenstörung hervorzurufen. Ein verändertes Rezept, ein falscher Werkzeugstand oder eine manipulierte Prüfgrenze kann dazu führen, dass die Produktion weiterläuft, die Qualität aber nicht mehr zuverlässig belegt ist. Das Sicherheitsprogramm muss deshalb mit Qualitätsmanagement und Rückverfolgbarkeit verbunden sein.

Für kritische Produkte werden freigegebene Parameterstände, Rezeptversionen, Messmittelzustände, Softwareversionen und Materialbezüge erfasst. Veränderungen müssen einem Auftrag, einem genehmigten Änderungsvorgang und einer zuständigen Person oder Identität zugeordnet werden können. Ein digitales Signatur- oder Versionsverfahren unterstützt diese Nachvollziehbarkeit, beweist allein aber nicht die fachliche Eignung der Einstellung.

Bei Integritätsverdacht wird der mögliche Betroffenheitszeitraum nicht allein aus dem Zeitpunkt eines Alarms abgeleitet. Zu prüfen sind frühere Änderungen, Datenlücken und die Reichweite gemeinsam genutzter Parameter. Die Qualitätsverantwortlichen entscheiden, welche Chargen zurückgehalten, erneut geprüft oder anderweitig behandelt werden. Der technische Incident Commander gibt keine Produkte frei, deren Qualität nicht beurteilt ist. Eine wieder anlaufende Maschine ist nicht gleichbedeutend mit einem wieder freigegebenen Erzeugnis.

11. Engineering-Stationen, Fernwartung und Herstellerzugänge

Engineering-Systeme besitzen häufig weitreichende Änderungsmöglichkeiten. Für die Risikoanalyse sind sie daher nicht bloß weitere Arbeitsplatzrechner. Zu erheben ist, welche Programme, Konfigurationen und Schutzparameter sie verändern können und wie Änderungen autorisiert werden. Gemeinsame Servicekonten erschweren die Zuordnung von Vorgängen und die gezielte Sperrung bei Verdacht.

Fernwartung wird an konkrete Aufträge und Zielsysteme gebunden. Die zulässige Sitzung, der Zeitpunkt, die verwendete Identität, die mögliche Änderungsart und ein lokaler Ansprechpartner werden dokumentiert. Ein dauerhafter Herstellerzugang ohne Zweckbindung ist nicht durch die bloße Erwartung schnellerer Reparatur ausreichend begründet. Ebenso benötigt der Notzugang eine kontrollierte Ausnahmefunktion, keine geheime Hintertür.

Nach Ende einer Wartung werden nicht nur Sitzungen geschlossen. Es werden verbleibende Tokens, neu eingerichtete Konten, Konfigurationsänderungen und möglicherweise angelegte Dateien geprüft. Die Organisation muss wissen, wie sie den Zugang widerruft, wenn der Dienstleister selbst einen Vorfall meldet. NIST behandelt OT-Fernzugriffe ausdrücklich; die konkreten Freigabe- und Abnahmefelder dieses Pakets sind deren anwendungsbezogene Umsetzung, keine wörtliche Normvorschrift. [Q02, § 6.2.10]

12. Änderungen an KI, Software und Parametern

Ein Modellupdate kann die Interpretation von Eingaben verändern. Ein Werkzeugupdate kann neue Schreibmöglichkeiten eröffnen. Ein geändertes API-Schema kann bislang begrenzte Aktionen erweitern. Deshalb muss das Änderungsmanagement für agentische Systeme über die Versionsnummer des Hauptmodells hinausgehen. Erfasst werden Modell, Systemanweisung, Werkzeuge, Berechtigungen, Datenquellen, Freigaberegeln und gegebenenfalls externe Dienste.

Für jede Änderung wird geprüft, ob die bisherige Sicherheitsargumentation weiter gilt. Ein rein optisches Update benötigt andere Prüfungen als eine neue Fähigkeit zur Parameteränderung. Die Freigabe orientiert sich am veränderten Wirkungspfad. Automatische Updates in kritischen Funktionen sind nicht grundsätzlich ausgeschlossen, aber ihre Bedingungen, Rollbackmöglichkeiten und Nachweisfolgen müssen beherrscht sein.

Ein Rücksetzen auf die vorige Version hilft nur, wenn diese noch verfügbar, kompatibel und unter den aktuellen Bedingungen verwendbar ist. Auch der Rollback muss deshalb geprüft werden. Nach einem Daten- oder Schemawechsel kann die alte Software neue Datensätze möglicherweise nicht korrekt verarbeiten. Der Begriff „Rollback vorhanden“ ist erst aussagekräftig, wenn Reichweite und Grenzen dokumentiert sind.

13. Brownfield: Umgang mit Altanlagen

Bei Bestandsanlagen können technische Eingriffsmöglichkeiten begrenzt sein. Nicht jedes Gerät unterstützt moderne Identitäten, kryptografische Verfahren oder detaillierte Protokollierung. Eine tragfähige Strategie beschreibt diese Grenze offen und setzt geeignete kompensierende Maßnahmen ein, statt Konformität durch Etiketten zu behaupten.

Kompensation kann aus begrenzten Kommunikationspfaden, gesonderten Zugangswegen, lokaler Freigabe, engmaschiger Zustandskontrolle oder vorübergehend eingeschränkter Vernetzung bestehen. Welche Maßnahme ausreichend ist, hängt vom Risiko ab. Eine fehlende Herstellerunterstützung kann auch bedeuten, dass ein geplanter autonomer Zugriff vorläufig nicht eingeführt werden darf. Der wirtschaftliche Wert einer Altanlage begründet keine unbegrenzte neue digitale Erreichbarkeit.

Der Betreiber führt ein Ausnahmeverzeichnis mit Eigentümer, Begründung, kompensierenden Kontrollen, Gültigkeitsende und Ablöseoption. Eine Ausnahme ohne Befristung und Überprüfung wird sonst faktisch zum Dauerzustand. Bei jeder neuen Verbindung ist zu prüfen, ob sie die bereits dokumentierte Grenze verschiebt. Der Umfang der Prüfung richtet sich nach der möglichen Wirkung, nicht allein nach dem Alter des Geräts.

14. Detektion mit Prozesskontext

Ein SOC kann einen ungewöhnlichen Login erkennen. Für die Fertigung muss die Untersuchung zusätzlich klären, ob daraus eine relevante Prozessänderung entstehen kann. Ein Parameterwechsel außerhalb eines genehmigten Produktwechsels kann wichtiger sein als ein hohes Datenvolumen während eines geplanten Backups. Umgekehrt kann ein kleiner, gezielter Export besonders schutzwürdiger Daten relevant sein.

Die Erkennung verbindet deshalb Identitätsereignisse, Wartungsfenster, Aufträge, Konfigurationsstände und ausgewählte Prozessinformationen. Dabei werden nur Informationen verwendet, die für die Entscheidung erforderlich und ausreichend verlässlich sind. Die Überwachung selbst kann neue Abhängigkeiten oder personenbezogene Datenbestände erzeugen; ihr Zweck und ihre Grenzen werden dokumentiert.

Anomalieerkennung ist probabilistisch oder regelbasiert fehleranfällig. Ein Alarm ist eine zu prüfende Beobachtung, nicht automatisch ein bestätigter Angriff. Eine automatisierte Antwort erhält deshalb eine begrenzte Reichweite. Sie kann beispielsweise neue Delegationen sperren oder einen nicht erforderlichen Export blockieren, sofern die Folgen vorher geprüft sind. Eingriffe in sicherheitskritische Bewegungen oder Prozesszustände brauchen die anlagenspezifisch freigegebene Reaktionslogik.

15. Notbetrieb und kontrollierter Stillstand

Für jede kritische Linie wird festgelegt, ob ein lokaler Mindestbetrieb möglich ist oder ein geordneter Stillstand erforderlich wird. Diese Entscheidung hängt von Prozesszustand, Material, Energie, Sicherheit und Qualitätsnachweis ab. Ein Anlagenstopp ist kein einheitlicher Endzustand: Nachlauf, Restenergie, Zwischenprodukte oder notwendige Hilfsmedien können weiterhin Aufmerksamkeit erfordern.

Der Mindestbetrieb benennt die zulässigen Produkte, Aufträge, Parameterstände, Bedienkompetenzen und Prüfmittel. Er darf keine freie improvisierte Produktion unter unsicheren Datenbedingungen sein. Fehlen verlässliche Qualitäts- oder Materialinformationen, kann die zulässige Leistung auf Erhaltung eines sicheren Zustands begrenzt sein. Die Produktionsleitung muss diese Einschränkung kennen, bevor ein wirtschaftlicher Druck im Ereignis entsteht.

Ein kontrollierter Stillstand und die spätere Wiederaufnahme werden getrennt geübt. Die Übung dokumentiert, welche Schritte wirklich lokal möglich sind und welche weiterhin auf zentrale IT angewiesen bleiben. Ein unabhängiger Zugang zur entscheidenden Dokumentation ist Bestandteil des Nachweises. Eine PDF auf dem nicht

erreichbaren Fileserver erfüllt diesen Zweck nicht.

16. Wiederherstellung umfasst die physische und digitale Realität

Die Wiederherstellung benötigt mehr als Datenbanksicherungen. In Betracht kommen Steuerungsprogramme, Roboterprogramme, freigegebene Parameter, Engineering-Projekte, Firmwarestände, Netzkonfigurationen, Zertifikate und die notwendige technische Dokumentation. Welche Dateien und Informationen für eine konkrete Linie erforderlich sind, wird in einer Wiederaufbauliste erfasst. [Q08, OT-Backup-Grundlage]

Anschließend wird der reale Zustand abgeglichen: Welche Teile liegen wo? Welche Chargen wurden bearbeitet? Welche manuelle Änderung wurde vorgenommen? Welche Werkzeuge und Schutzvorrichtungen befinden sich in welchem Zustand? Ein digitaler Zwilling kann diesen Abgleich unterstützen, ist aber keine unabhängige Wahrheit, wenn seine eigenen Eingangsdaten betroffen sind.

Der Wiederanlauf erfolgt nach einem Freigabeverfahren mit getrennten Nachweisen für Cyber-Eingrenzung, technische Funktionsfähigkeit, erforderliche Schutzfunktionen und Produktqualität. Ein neuer Agentenzugang wird nicht deshalb freigegeben, weil die Maschine ohne ihn funktioniert. Seine Handlungsvollmacht ist eine zusätzliche Entscheidung. Offene Integritätsfragen bleiben sichtbar; sie verschwinden nicht durch ein erfolgreiches Einschalten.

17. Abnahmetests und Negativproben

Die Prüfung beginnt mit Modell, Konfiguration und isolierten Testumgebungen. Je nach Anlage können Simulation, Hardware-in-the-Loop oder ein abgesicherter Versuch erforderlich sein. Die Wahl der Methode muss deren Grenzen benennen: Eine Simulation reproduziert nicht automatisch alle Zeit-, Energie- oder Umwelteffekte. Ein bestandener Test in einer leeren Zelle beweist nicht jedes Verhalten bei realer Material- und Personeninteraktion.

Besonders aussagekräftig sind Negativproben: Ein Diagnosekonto versucht eine Konfigurationsänderung; ein abgelaufenes Wartungsmandat versucht einen weiteren Zugriff; ein alter Auftrag wird nach einem Moduswechsel erneut angeboten; ein Agent fordert eine Handlung außerhalb seiner zugelassenen Rolle an. Erwartet wird ein vorher festgelegtes Verhalten mit verwertbarem Nachweis. Es werden keine unkontrollierten Exploits oder echten gefährlichen Bewegungen ausgelöst.

Zusätzlich wird ein gemeinsamer Ursachenfall geprüft. Ein zentraler Dienst wird in der Testumgebung als nicht verfügbar angenommen. Die Beteiligten müssen zeigen, welche Schutz-, Bedien- und Wiederherstellungsfunktionen weiterhin funktionieren. Ein Schutzkonzept, das genau den ausgefallenen Dienst für seine Aktivierung benötigt, besteht diesen Test nicht.

18. Maschinenrecht, Normen und betriebliche Anforderungen

Die Kommissionsübersicht nennt den 20. Januar 2027 als grundsätzlichen Anwendungsbeginn der Maschinenverordnung. Für konkrete Produkte und Übergangsfälle sind die maßgebliche Fassung und die tatsächliche Rolle zu prüfen. Der direkte konsolidierte Normtext war in dieser Recherche technisch nicht durchgängig abrufbar; die angegebenen Suchstellen zu Schutz vor Manipulation und Steuerungen sind deshalb zusätzliche juristisch-technische Prüfaufträge. [Q35; Q40]

Aus einer neuen ISO-Ausgabe folgt nicht automatisch deren harmonisierter Status für einen bestimmten Rechtsakt. Ebenso wird aus einem öffentlichen Normabstract kein Konformitätsnachweis. Die Organisation muss die einschlägigen Volltexte beschaffen, den Anwendungsbereich bestimmen und das Verhältnis zwischen Produktkonformität und betrieblicher Gefährdungsbeurteilung dokumentieren. [Q25; Q26; Q31]

Für Cyberpflichten können zusätzlich BSIG, CRA und Datenschutz relevant sein. Ob ein Unternehmen als Hersteller eines digitalen Produkts oder lediglich als Betreiber handelt, verändert die Pflichtenlage. Ein späterer allgemeiner Produktstichtag ist kein Grund, bereits bestehende Betriebs- oder Sicherheitsanforderungen aufzuschieben. Die Rechtsmatrix in Band 5 trennt diese Ebenen, ohne eine pauschale Einstufung der Fabrik zu behaupten.

19. Entscheidungsvorlage für Werkleitung und technischen Ausschuss

Eine geeignete Entscheidungsvorlage enthält den freizugebenden Funktionsumfang, kritische Verlustszenarien, Handlungsvollmachten, verbleibende gemeinsame Ursachen, durchgeführte Tests und offene Punkte. Sie zeigt ausdrücklich, welche Produkt- und Betriebszustände nicht freigegeben sind. Eine Aussage wie „nur außerhalb der Produktion getestet“ muss erhalten bleiben, wenn sie den Nachweisumfang begrenzt.

Der Ausschuss sollte nach folgenden Zusammenhängen fragen: Kann derselbe Zugang operative und sicherheitsrelevante Grenzen verändern? Welche Qualitätseigenschaft könnte unbemerkt manipuliert werden? Was geschieht mit laufenden und wartenden Aufträgen nach Widerruf? Welche unabhängige Sicht auf den realen Prozess bleibt? Welche Wiederherstellungsdatei ist nur vorhanden, aber noch nie verwendet worden? Welche Herstellerzusage ist nicht vertraglich oder technisch belegt?

Die Freigabe erfolgt für eine konkrete Anlage und Konfiguration. Ein wesentlicher offener Schutzpfad oder ein unbekanntes Verhalten bei Kommunikationsverlust kann die autonome Funktion sperren, auch wenn die bestehende manuelle oder konventionelle Anlage weiter betrieben werden darf. Ziel ist eine begründete Begrenzung, nicht eine undifferenzierte Entscheidung zwischen vollständiger Digitalisierung und vollständigem Stillstand.

20. Arbeitsunterlagen und Ergebnis

Die sektorspezifischen Kontrollen **K19–K28** werden mit den Identitätskontrollen **K29–K38** und den Recovery-Kontrollen **K49–K60** verbunden. Die Formulare **F02 Abhängigkeiten**, **F03 Handlungsvollmachten**, **F04 Gefährdungsfall**, **F07 Änderung**, **F08 Betriebsmodi**, **F10 Wiederanlauf** und **F12 Lieferantennachweise** bilden die Arbeitsakte. Fallstudie **S-INDUSTRIE** führt einen synthetischen Konflikt zwischen Fernwartungsautorität, Flottensteuerung und Qualitätsnachweis durch.

Ergebnis: Sichere Vernetzung bedeutet nicht, dass jede Maschine aus jeder Anwendung erreichbar ist. Sie bedeutet, dass jeder notwendige Wirkungspfad begründet, begrenzt und prüfbar ist – und dass Betrieb, Schutzfunktionen und Qualität auch dann beurteilt werden können, wenn ein Teil der digitalen Umgebung nicht mehr vertrauenswürdig ist.

<!-- GENERATED_LOCAL_BIBLIOGRAPHY -->

Literatur und Quellenstatus

Die folgenden Angaben gehören zu diesem Band. Das vollständige Quellenregister erläutert Verwendungszweck und Zugriff. Quellenstatus und Grenzen sind bei jeder Weiterverwendung zu erhalten. Die Q-Nummern im Text beziehen sich auf diese Einträge; Fundstellen bezeichnen die externe Quelle, nicht eine erfundene PDF-Seite dieses Bandes.

Q02 – Keith Stouffer et al. / NIST. Guide to Operational Technology (OT) Security, SP 800-82 Rev. 3. 2023-09-28. DOI: 10.6028/NIST.SP.800-82r3. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: §§ 2.3.7, 2.4, 3.3, 4.2.2, 5.2, 5.3, 6.2.10–6.2.12, 6.3–6.5; gedruckte S. 25, 28, 38–42, 55, 69–79, 122–138. Zugriff: Landingpage und relevante PDF-Abschnitte gelesen; PDF-Stichprobe visuell geprüft. Grenze: Freiwillige US-Leitlinie, kein deutscher Konformitätsnachweis. Der Leitfaden ergänzt eigene Überlegungen; Kapitelverweise sind keine wörtlichen Normanforderungen.

Q08 – NIST. OT Backup Quick Start Guide, SP 1339. 2026-06-17. DOI: 10.6028/NIST.SP.1339. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; Backup und Recovery für OT. Zugriff: Publikationsseite / Beschreibung gelesen. Grenze: Ein Backup- oder Hashnachweis ist kein Beweis fachlicher Datenrichtigkeit. Konkrete Recovery-Gates sind eigene Ableitungen.

Q24 – IEC. IEC 62443-3-2:2020: Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design. 2020. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract; system under consideration, zones and conduits. Zugriff: Offizielle Metadaten und öffentliches Abstract; Normvolltext nicht zugänglich. Grenze: Kein frei behaupteter Security Level oder Nachweis normgerechter Umsetzung. Funktionale Safety gesondert prüfen.

Q25 – ISO. ISO 10218-1:2025: Robotics — Safety requirements — Part 1: Industrial robots. 2025-02. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract / Scope; edition 3. Zugriff: Offizielle Metadaten / Scope gelesen; Normvolltext nicht geprüft. Grenze: Ausgabestand allein belegt keine EU-Harmonisierung und keinen individuellen Konformitätsstatus.

Q26 – ISO. ISO 10218-2:2025: Robotics — Safety requirements — Part 2: Industrial robot applications and robot cells. 2025-02. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abstract / Scope; edition 2; ausdrückliche Ausschlüsse. Zugriff: Offizielle Metadaten / Scope gelesen; Normvolltext nicht geprüft. Grenze: Nicht pauschal auf OP-Roboter, Pflegerobotik oder öffentliche Servicerobotik übertragbar. Normvolltext und Produktscope prüfen.

Q27 – MITRE. ATT&CK for ICS: Loss of Safety, T0880. abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Description; Mitigations; References. Zugriff: Eintrag gelesen. Grenze: Taxonomie belegt keine Angriffsquote und keine lückenlose Historie.

Q28 – MITRE. Triton Safety Instrumented System Attack, C0030. abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Campaign description; techniques; references. Zugriff: Eintrag und Einordnung gelesen. Grenze: Kontextquelle; keine eigene forensische Verifikation; keine agentische KI-Kampagne.

Q31 – Bundesrepublik Deutschland / Gesetze im Internet. Betriebssicherheitsverordnung § 3 – Gefährdungsbeurteilung. aktuelle Fassung abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abs. 1–3 sowie Aktualisierung / Dokumentation. Zugriff: Paragraph vollständig gelesen. Grenze: Konkrete Prüfpflichten und befähigte Personen aus weiteren Vorschriften und Anlagenscope ableiten, nicht allein aus diesem Paragraphen.

Q32 – Bundesrepublik Deutschland / Gesetze im Internet. Betriebsverfassungsgesetz § 87 – Mitbestimmungsrechte. aktuelle Fassung abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Abs. 1 Nr. 6 und 7. Zugriff: Paragraph gelesen. Grenze: Betriebliche Anwendbarkeit und gesetzliche/tarifliche Vorrangregelungen prüfen; öffentliche und kirchliche Träger können anderen Vertretungsregeln unterliegen.

Q35 – Europäische Kommission, DG GROW. Machinery — Machinery Regulation. abgerufen 2026-09-25. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Machinery Regulation; mandatory application date. Zugriff: Webtext / Anwendungsdatum gelesen. Grenze: Kein individueller Bescheid; Produktscope, Umbau und aktuelle konsolidierte Anhänge Q40 separat prüfen.

Q38 – Europäische Union. Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung. 2016; aktuelle Fassung vor Anwendung prüfen. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Art. 5, 6, 9, 25, 28, 30, 32–35, 38–39, 44 ff.. Zugriff: Direkter Web-Volltextabruf technisch blockiert; nicht als neu volltextverifiziert ausgewiesen. Grenze: Artikelzuordnung dient der rechtlichen Prüfung. Redaktionell bekannte Regelungsinhalte werden nicht als vollständig neu geprüfte konsolidierte Rechtsberatung ausgegeben.

Q40 – Europäische Union. Verordnung (EU) 2023/1230 – Maschinenverordnung. 2023; konsolidierte Fassung vor Anwendung prüfen. [Originalquelle](#). Stand des Abrufs: 2026-09-25.

Fundstelle: Anwendungs-/Übergangsbestimmungen; Anhang III insbesondere 1.1.9 und 1.2.1 als Prüfsuchstellen. Zugriff: Volltextabruf technisch blockiert; Datum/Überblick über Q35 geprüft. Grenze: Fundstellen sind Suchaufträge für die aktuelle Volltextprüfung, kein behaupteter vollständiger Nachweis sämtlicher Anforderungen.

Arbeitsmittel: Kontrollkatalog, Formularbuch, Fallstudien und Claim–Evidence–Matrix.

12 Rechtliche Hinweise

12.1 Keine Beratung

Diese Veröffentlichung ist ein redaktionelles Erzeugnis. Sie stellt keine Rechtsberatung, keine medizinische, pflegerische, arbeitsrechtliche oder datenschutzrechtliche Beratung und keine Beschaffungs- oder Vergabeberatung dar. Sie ersetzt insbesondere nicht die Prüfung durch Rechtsanwaltschaft, Datenschutzaufsicht, Medizinprodukteberatung, Vergabestelle, Ethikkommission nach Medizinprodukterecht oder Arbeitnehmervertretung. Wer auf Grundlage dieses Dokuments entscheidet, entscheidet auf eigene Verantwortung und hat den Sachverhalt vorher eigenständig fachlich prüfen zu lassen.

12.2 Keine Zusicherung, keine Konformitätsaussage

Die beschriebenen Verfahren, Prüfstufen und Checklisten sind redaktionelle Vorschläge. Sie sind keine Zusicherung einer Eigenschaft, kein garantiertes Ergebnis und kein Nachweis der Einhaltung einer Rechtsvorschrift. Wer ein Verfahren aus diesem Dokument anwendet, erfüllt damit keine gesetzliche Anforderung; ob eine Anforderung erfüllt ist, entscheidet die zuständige Stelle am Einzelfall.

12.3 Rechtsstand

Rechtsstände, Fristen und Fundstellen beziehen sich auf den im Dokumentkopf genannten Tag. Der KI-Rechtsrahmen wird laufend geändert; ein älterer Fristenplan darf nicht unverändert weiterverwendet werden. Genannte Gesetze und Verordnungen sind in ihrer jeweils geltenden Fassung heranzuziehen.

12.4 Haftung

Die Inhalte wurden mit Sorgfalt erstellt und, soweit im Methodenteil beschrieben, gegengeprüft. Für Richtigkeit, Vollständigkeit und Aktualität wird gleichwohl keine Gewähr übernommen. Eine Haftung des Herausgebers ist auf Vorsatz und grobe Fahrlässigkeit beschränkt; dies gilt nicht bei der Verletzung des Lebens, des Körpers oder der Gesundheit sowie bei zwingender gesetzlicher Haftung.

12.5 Verweise auf fremde Inhalte

Dieses Dokument verweist auf Inhalte Dritter, insbesondere auf Behörden-, Fachgesellschafts-, Normen- und Fachverlagsseiten. Auf deren Gestaltung und Inhalt hat der Herausgeber keinen Einfluss; für sie ist jeweils der dortige Anbieter verantwortlich. Die Adressen waren zum im Literaturverzeichnis genannten Prüfzeitpunkt erreichbar. Die Nennung eines Produkts, Herstellers oder Dienstes ist weder eine Empfehlung noch eine Bewertung seiner Eignung.

12.6 Marken und Produktbezeichnungen

Genannte Produkt-, Marken- und Unternehmensbezeichnungen sind Kennzeichen ihrer jeweiligen Inhaber und werden ausschließlich zur Beschreibung des Sachverhalts verwendet. Aus der Nennung folgt keine Verbindung zwischen dem Herausgeber und dem jeweiligen Unternehmen und keine Aussage über Zulassungs-, Konformitäts- oder Zertifizierungsstatus.

12.7 Urheberrecht und Nutzung

Dieses Dokument, sein Text, seine Tabellen und seine Abbildungen sind urheberrechtlich geschützt. Rechteinhaberin ist die WebTrades GmbH. Zulässig sind das Lesen, das Speichern und der Ausdruck für den eigenen Gebrauch sowie das Zitieren einzelner Stellen mit vollständiger Quellenangabe nach der im Impressum genannten Zitierweise. Die Vervielfältigung, Bearbeitung, Verbreitung, öffentliche Zugänglichmachung oder kommerzielle Verwertung des Dokuments oder wesentlicher Teile daraus bedarf der vorherigen schriftlichen Zustimmung der Rechteinhaberin. Das gilt ausdrücklich auch für die Übernahme von Tabellen und Abbildungen.

12.8 Keine personenbezogenen Daten

Für dieses Dokument wurden keine personenbezogenen Daten verarbeitet. Es beruht auf veröffentlichter Literatur, amtlichen Rechtsquellen und Veröffentlichungen von Fachgesellschaften; es wurden weder Beschäftigte befragt noch Patientendaten verwendet. Wer die hier beschriebenen Verfahren auf eine reale Einrichtung anwendet, verlässt diesen Rahmen: Die Auswertung von Tätigkeits-, Alarm- oder Quittierungsdaten unterliegt der Datenschutz-Grundverordnung und in der Regel der Mitbestimmung.

12.9 Unabhängigkeit

Dieses Dokument ist ohne Auftrag, ohne Finanzierung und ohne inhaltliche Beteiligung eines Herstellers, Krankenhausträgers, Kostenträgers, Verbands oder Beratungsunternehmens entstanden. Es besteht kein Vergütungs- oder Beteiligungsverhältnis zu einem der genannten Unternehmen oder Institutionen. Genannt werden Systeme, Anbieter und Dokumente, weil sie in den beschriebenen Gegenstand fallen, nicht weil sie beworben werden sollen.

12.10 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Gesetzliche Verbraucherschutzvorschriften bleiben unberührt.