

## Die IEC 62443 aus Planer- und Betreibersicht

**Karl-Heinz Niemann**

Suggested citation:

Niemann, Karl-Heinz. 2025. "Die IEC 62443 aus Planer- und Betreibersicht." Hannover: Hochschule Hannover. <https://doi.org/10.25968/opus-3667>.

### Abstract

Die IT-Sicherheit in Produktionsanlagen gewinnt zunehmend an Bedeutung. Statistiken bestätigen eine verschärfende Bedrohungslage auch im Bereich der industriellen Automatisierungstechnik.

Die Europäische Union fordert künftig bestimmte Mindeststandards für Anlagen im Bereich der kritischen Infrastruktur über die NIS-2-Richtlinie. Planer und Betreiber von Produktionsanlagen sind demnach gefordert, die IT-Sicherheit ihrer Produktionsanlagen (im Weiteren OT-Security genannt) zu adressieren und systematisch in ihre Prozesse zu integrieren.

Die Normreihe IEC 62443 wurde speziell auf die Anwendung in Produktionsanlagen konzipiert und berücksichtigt daher die Anforderungen, welche sich aus einer industriellen Echtzeitumgebung ableiten. Die Norm definiert neben Anforderungen an die Hersteller von Automatisierungskomponenten auch Anforderungen an Planer und Betreiber von Automatisierungssystemen. Dieses Dokument widmet sich im Schwerpunkt der Rolle der Planer und Betreiber im OT-Security-Prozess.

Nach einer Abgrenzung der OT-Security und der IT-Security in Kapitel 2 folgt in Kapitel 3 zunächst eine Einführung in die Norm IEC 62443. Kapitel 4 beschreibt dann die Aufgaben des Anlagenplaners. Hier wird unter anderem auf die Aufgaben des Anlagenplaners wie z. B. die Erstellung einer Risiko- und Bedrohungsanalyse sowie die Definition eines Defense-in-Depth-Konzeptes eingegangen. In Kapitel 5 folgen dann die Aufgaben des Anlagenbetreibers (engl. Asset Owner). Zu diesen Aufgaben gehören z. B. der Aufbau eines Information-Security-Management-Systems (ISMS), Erstellung und Wartung eines Asset-Inventories und das Einspielen von Software-Aktualisierungen (Patch-Management).

WHITE PAPER

# Die IEC 62443 aus Planer- und Betreibersicht

Prof. Dr. Karl-Heinz Niemann



Prof. Dr. Karl-Heinz Niemann


ORCID ID  <https://orcid.org/0000-0001-8931-6789>

ABB-Dokumentennummer: 3ADR011430

DOI: <https://doi.org/10.25968/opus-3667>

**Haftungsausschluss:** Die diesem Dokument zu Grunde liegenden Informationen wurden mit größtmöglicher Sorgfalt recherchiert zusammengestellt. Dennoch wird dieses ohne eine Gewährleistung zur Verfügung gestellt. Der Autor lehnt ausdrücklich jede Art von vertraglicher oder gesetzlicher Haftung für dieses Dokument ab. In keinem Fall ist der Autor für Schäden verantwortlich, die durch Fehler oder fehlende Informationen in diesem Dokument entstehen könnten. Logos und Markennamen werden ohne Hinweis auf ggf. bestehende Schutzrechte verwendet.

## Versionsverlauf

Rev.	Beschreibung	Datum
C	Erste veröffentlichte Version	27.07.2025

# Inhalt

<b>1. Einführung</b> .....	<b>5</b>
<b>2. Abgrenzung OT- und IT-Security</b> .....	<b>6</b>
<b>3. Die Normreihe IEC 62443</b> .....	<b>7</b>
3.1. Übersicht über die IEC 62443 .....	7
3.2. Die Rollen im OT-Sicherheitsprozess .....	8
3.3. Zusammenwirken der Stakeholder im OT-Sicherheitsprozess.....	9
3.4. Die Security-Level in der IEC 62443 .....	10
<b>4. Die Aufgaben des Anlagenplaners nach IEC 62443</b> .....	<b>12</b>
4.1. Relevante Normteile der IEC 62443 für Anlagenplaner .....	12
4.2. Die Aufgaben des Anlagenplaners im Detail .....	13
4.2.1. Identifizierung bereits vorhandener Dokumente des Auftraggebers / Anlagenbetreibers .....	14
4.2.2. Definition Betrachtungsgegenstand (System under Consideration) .....	14
4.2.3. Definition des Security-Kontextes.....	14
4.2.4. Risiko- und Bedrohungsanalyse .....	15
4.2.5. Defense in Depth Konzept.....	18
4.2.6. Erstellen der Detailplanung.....	20
4.2.7. Ergebnisse des Planungsprozesses .....	20
4.3. Zusammenwirken des Planers mit den anderen Verantwortlichen im OT- Sicherheitsprozess.....	20
4.4. Vorschlag für die Realisierung der Security Anforderungen .....	21
4.5. Erfolgsfaktoren für den OT-Security-Prozess der Anlagenplaner.....	22
<b>5. Die Aufgaben des Anlagenbetreibers nach IEC 62443</b> .....	<b>23</b>
5.1. Relevante Normteile der IEC 62443 für Anlagenbetreiber .....	23
5.2. Die Aufgaben des Anlagenbetreibers im Detail.....	25
5.3. Zusammenwirken mit den anderen Verantwortlichen im OT-Sicherheitsprozess .....	26
5.4. Vorschlag für ein Vorgehen bei der Realisierung der Anforderungen für Betreiber .....	26
5.5. Erfolgsfaktoren für den Security-Prozess der Anlagenbetreiber .....	27
<b>6. Zusammenfassung</b> .....	<b>29</b>
<b>7. Abbildungsverzeichnis</b> .....	<b>30</b>
<b>8. Tabellenverzeichnis</b> .....	<b>31</b>
<b>9. Stichwortverzeichnis</b> .....	<b>32</b>
<b>10. Literaturverzeichnis</b> .....	<b>34</b>

---

# 1. Einführung

Die IT-Sicherheit in Produktionsanlagen gewinnt zunehmend an Bedeutung. Statistiken bestätigen eine verschärfende Bedrohungslage auch im Bereich der industriellen Automatisierungstechnik [TRE2022]. Die Europäische Union fordert künftig bestimmte Mindeststandards für Anlagen im Bereich der kritischen Infrastruktur über die NIS-2-Richtlinie [NIS-2\_de]. Planer und Betreiber von Produktionsanlagen sind demnach gefordert, die IT-Sicherheit ihrer Produktionsanlagen (im Weiteren OT-Security genannt) zu adressieren und systematisch in ihre Prozesse zu integrieren.

Die Normreihe IEC 62443 [DKE2024] wurde speziell auf die Anwendung in Produktionsanlagen konzipiert und berücksichtigt daher die Anforderungen, welche sich aus einer industriellen Echtzeitumgebung ableiten. Die Norm definiert neben Anforderungen an die Hersteller von Automatisierungskomponenten auch Anforderungen an Planer und Betreiber von Automatisierungssystemen. Dieses Dokument widmet sich im Schwerpunkt der Rolle der Planer und Betreiber im OT-Security-Prozess.

Nach einer Abgrenzung der OT-Security und der IT-Security in Kapitel 2 folgt in Kapitel 3 zunächst eine Einführung in die Norm IEC 62443. Kapitel 4 beschreibt dann die Aufgaben des Anlagenplaners. Hier wird unter anderem auf die Aufgaben des Anlagenplaners wie z. B. die Erstellung einer Risiko- und Bedrohungsanalyse sowie die Definition eines Defense-in-Depth-Konzeptes eingegangen. In Kapitel 5 folgen dann die Aufgaben des Anlagenbetreibers (engl. Asset Owner). Zu diesen Aufgaben gehören z. B. der Aufbau eines Information-Security-Management-Systems (ISMS), Erstellung und Wartung eines Asset-Inventories und das Einspielen von Software-Aktualisierungen (Patch-Management). Das Dokument schließt mit einer Zusammenfassung.

Wo immer möglich wird auf weiterführenden Literaturquellen verwiesen. Die Liste der Quellen findet sich im Literaturverzeichnis in Kapitel 10.

## 2. Abgrenzung OT- und IT-Security

Im Bereich der Informationssicherheit wird zwischen der IT (engl. Information Technology) und der OT (Operational Technology) unterschieden. Die Gartner Group [GAR2021] differenziert die IT und die OT nach den in Tabelle 1 aufgeführten Merkmalen.

Tabelle 1: Unterscheidung zwischen IT und OT nach [GAR2021]

Domäne	Definition gemäß der Gartner-Group	Anwendungsbeispiel
IT	Information-Technology (IT) ist der Sammelbegriff für das gesamte Spektrum der Informationsverarbeitungstechnologien, einschließlich Software, Hardware, Kommunikationstechnologien und damit verbundene Dienstleistungen. Im Allgemeinen umfasst die IT keine eingebetteten Technologien, solange sie keine Daten für den Unternehmensgebrauch erzeugen.	<ul style="list-style-type: none"> <li>• Arbeitsplatzrechner</li> <li>• Laptops</li> <li>• Web-Server</li> <li>• Mail-Server</li> <li>• SAP-Systeme</li> <li>• File-Server</li> <li>• Netzwerke</li> </ul>
OT	Operational Technology (OT) ist Hard- und Software, die durch direkte Überwachung und/oder Kontrolle von industriellen Geräten, Anlagen, Prozessen und Ereignissen eine Veränderung feststellt oder bewirkt.	<ul style="list-style-type: none"> <li>• Speicherprogrammierbare Steuerungen (SPS)</li> <li>• Anzeigesysteme (Operator-Panels)</li> <li>• Server für die Produktionssteuerung</li> <li>• Industrieroboter</li> <li>• Remote-IO Systeme</li> <li>• Echtzeitnetzwerke und sonstige Netzwerke zur Kommunikation mit Automatisierungskomponenten.</li> </ul>

Es ist zu erkennen, dass sich die Operational Technology (OT) im Wesentlichen auf Komponenten der Automatisierungstechnik bezieht. Die besonderen Anforderungen der OT sind:

- Echtzeitkommunikation ist für die Funktionalität eines Automatisierungssystems und damit für die Produktionsanlage essenziell.
- Gerade in der Prozessindustrie muss von einem dauerhaften, unterbrechungsfreien Betrieb der Systeme ausgegangen werden.
- Es besteht eine begrenzte Möglichkeit, Software-Patches während des Betriebs der Anlage zu installieren.
- Ein Integritätsschutz der Kommunikation ist erforderlich.
- Erfüllung der wesentlichen Sicherheitsanforderungen:
  - Verfügbarkeit,
  - Integrität,
  - Authentizität,
  - Vertraulichkeit und
  - Nichtabstreitbarkeit

Diese Anforderungen führen dazu, dass bestimmten Aspekte der OT-Security (z. B. das Patch-Management) anders zu handhaben sind als in der IT. Grundsätzlich bestehen aber auch viele Gemeinsamkeiten, z. B. bei Aufbau und Aufrechterhaltung eines Information Security Management Systems (ISMS).

### 3. Die Normreihe IEC 62443

Das folgende Kapitel widmet sich der Normreihe IEC 62443 [DKE2024]. Im Kapitel 3.1 wird zunächst ein Überblick über die Norm gegeben. Kapitel 3.2 befasst sich dann mit den Rollen im OT-Sicherheitsprozess. Es folgt dann eine Beschreibung des Zusammenwirkens der Stakeholder im OT-Sicherheitsprozess in Kapitel 3.3.

#### 3.1. Übersicht über die IEC 62443

Die IEC-Normenreihe 62443 befasst sich mit der Sicherheit (OT-Security) im Bereich der Automatisierungstechnik (Industrial Automation and Control Systems IACS). Die Normreihe adressiert die Komponente, welche für den Betrieb einer automatisierten Produktionsanlage erforderlich sind. Dazu gehören sowohl Hardware- als auch Softwarekomponenten. Des Weiteren werden auch die organisatorischen Prozesse für die Errichtung und den Betrieb einer Anlage einbezogen.

Allgemeine Grundlagen	Betreiber + Dienstleister	Anforderungen an Automatisierungssysteme	Anforderungen an Automatisierungskomponenten	Profile der IEC 62443	Evaluationsmethodik
IEC/TS 62443-1-1 Concepts and models	IEC 62443-2-1 Sec. Prog. Req. for ass. owners	IEC/TR 62443-3-1 Security technologies f. IACS	IEC/TS 62443-4-1 Lifecycle requirements	IEC/TS 62443-5-1 In Arbeit	IEC/TS 62443-6-1 Evaluation for IEC 62443-2-4
IEC 62443-1-2 Glossary, terms, abbreviations	IEC 62443-2-2 Sec. Protection Rating	IEC 62443-3-2 Security risc assessm. & design	IEC/TS 62443-4-2 Component requirements	IEC/TS 62443-5-2 In Arbeit	IEC/TS 62443-6-2 Evaluation for IEC 62443-4-2
IEC 62443-1-3 System security metrics	IEC/TR 62443-2-3 Patch Management	IEC 62443-3-3 System Security requirements			
IEC 62443-1-4 IACS security life cycle	IEC 62443-2-4 Requirements Service Provid.				
IEC/TS 62443-1-5 Security profiles	IEC 62443-2-5 Implementation Guidance				
			<div style="display: flex; align-items: center;"> <div style="width: 10px; height: 10px; background-color: red; margin-right: 5px;"></div> erschienen         </div> <div style="display: flex; align-items: center;"> <div style="width: 10px; height: 10px; background-color: gray; margin-right: 5px;"></div> in Arbeit         </div>		

Abbildung 1: Übersicht über die Normreihe IEC 62443, In Anlehnung an [DKE2024]

Abbildung 1 gibt einen Überblick über die Normreihe IEC 62443. Die Reihe lässt sich in vier Hauptkategorien unterteilen:

- **Teile 1-1 bis 1-5 – Allgemeine Grundlagen:** In diesen Dokumenten werden die Begriffe und Grundsätze im Zusammenhang mit der OT-Sicherheit definiert. Derzeit sind nur der Teil 1-1 und der Teil 1-5 öffentlich zugänglich.
- **Teile 2-1 bis 2-5 – Betreiber und Dienstleister:** Diese Teile sind für Anlagenbetreiber und Dienstleistungsanbieter relevant. In diesen Teilen werden z. B. der Sicherheitsmanagementprozess, Leitlinien für das Patch-Management und Anforderungen an Dienstleister (z. B. Wartungspersonal) definiert. Weiterhin befasst sich der Teil 2-2 mit der Einstufung der technischen Security Features und dem Reifegrad der Organisation. Die Normteile 2-1 bis 2-5 werden in den Kapiteln 4 und 5 dieses Dokuments, welches sich mit den Aufgaben von Integratoren und Anlagenbetreibern befasst, näher behandelt.

- **Teile 3-1 bis 3-3 – Anforderungen an Automatisierungssysteme:** Diese Teile sind für die Planung eines Automatisierungssystems von Bedeutung. Sie geben Hinweise zum Risikomanagementprozess (Teil 3-2) und zu den Anforderungen an die Systemsicherheit (Teil 3-3). Diese Teile sind für Kapitel 4 dieses Dokuments relevant, das den Prozess des sicheren Entwurfs einer Anlage behandelt.
- **Teile 4-1 bis 4-2 – Anforderungen an Automatisierungskomponenten:** Diese beiden Teile definieren den sicheren Entwicklungslebenszyklus für Automatisierungskomponenten (Teil 4-1) und die technischen Anforderungen an Automatisierungskomponenten (Teil 4-2). Diese beiden Teile sind für Hersteller von Komponenten für Automatisierungssysteme relevant und werden daher hier nicht näher betrachtet.
- **Teile 5-1 und 5-2:** Diese Teile sind noch nicht verfügbar. Es ist geplant, Profile zu beschreiben, die die Anwendung der Norm in verschiedenen Bereichen unterstützen, z.B. Industrieautomation, Prozessindustrie, Medizin- oder Bahntechnik.
- **Teile 6-1 und 6-2 – Evaluationsmethodik:** In diesen beiden Teilen werden Konformitätskriterien und mögliche Konformitätsnachweise beschrieben. Es werden keine neuen Anforderungen aufgestellt, sondern es wird beschrieben, wie die Konformität mit den Anforderungen der Norm IEC 62443 bewertet werden kann. Der Teil [IEC\_62443-6-1] befasst sich mit der Evaluationsmethodik für Dienstleister, der Teil [IEC\_62443-6-2] mit der Evaluation der Anforderungen an Automatisierungskomponenten.

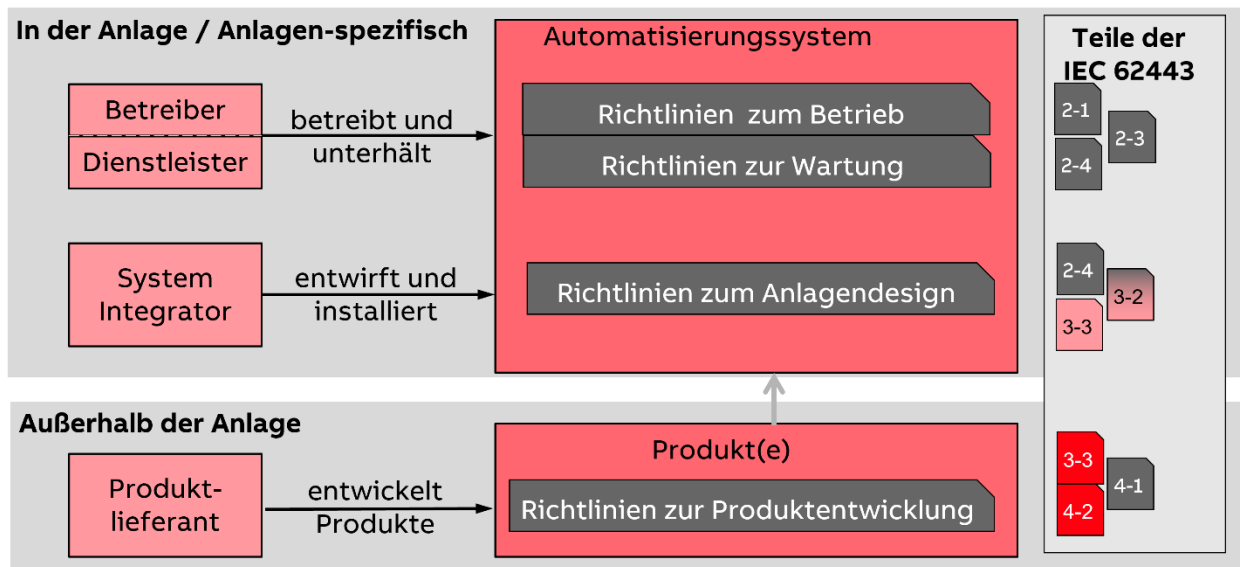
Neben der OT-Sicherheitsnorm IEC 62442 wird auch die ISO 27000-Normenreihe häufig in Bezug auf die Sicherheit herangezogen. Während sich die IEC 62443 auf die OT-Sicherheit konzentriert, behandelt die [DIN\_EN\_ISO/IEC\_27001] allgemeine Aspekte der Informationssicherheit. Wer sich für die Anwendungsbereiche und die Unterschiede interessiert, kann das Whitepaper "Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443" [NIE2021] weiterführende Informationen finden. Zusätzlich zu den beschriebenen Standards sind weitere Dokumentationen zur OT-Sicherheit verfügbar, z.B. im NIST "Guide to Operational Technology (OT) Security" [NIST\_SP\_800-82].

## 3.2. Die Rollen im OT-Sicherheitsprozess

Die [DIN\_EN\_IEC\_62443-4-1] definiert verschiedene Beteiligte am Sicherheitsmanagementprozess. Diese sind:

- **Anlagenbetreiber und Dienstleister**, die den Anlagenbetreiber beim Betrieb der Anlage unterstützen. Das können z. B. Dienstleister sein, die Wartungsaufgaben durchführen.
- **Systemintegratoren und Automatisierungssystemplaner**, die Automatisierungssysteme und Produktionsanlagen entwerfen, installieren und in Betrieb nehmen.
- **Produkt- und Systemlieferanten**, die Komponenten und Automatisierungssysteme entwickeln, vertreiben und die Systeme mit Aktualisierungen (Updates) und die Betreiber mit Security-Advisories versorgen.

Abbildung 2 zeigt die verschiedenen Akteure und deren Rolle im OT-Sicherheitsprozess. Auf der rechten Seite von Abbildung 2 sind die Teile der IEC 62443 aufgeführt, die für die jeweiligen Akteure relevant sind.



Strukturvorgaben Prozesse **Funktionale Anforderungen**

Abbildung 2: Beteiligte am OT-Sicherheitsprozess und zugeordnete Teile der IEC 62443 (abgeleitet aus der [IEC\_62443-4-1])

### 3.3. Zusammenwirken der Stakeholder im OT-Sicherheitsprozess

Es ist in Abbildung 2 zu erkennen, dass verschiedene Teile der IEC 62443 für die unterschiedlichen Stakeholder relevant sind. Es wird davon ausgegangen, dass die betrachtete Produktionsanlage die Anforderungen der IEC 62443 erfüllen soll. Daher wird in dem nachfolgenden Text der Begriff „muss“ verwendet. Nur wenn die Teilleistungen zur Herstellung der Komponenten, zur Planung und Errichtung der Anlage und zum Betrieb der Norm folgen, ist die Gesamtsicherheit gewährleistet.

- **Anlagenbetreiber:** Der Anlagenbetreiber konzentriert sich auf die Einrichtung des industriellen Sicherheitsprogramms nach [DIN\_EN\_IEC\_62443-2-1] in seiner Anlage und nimmt eine Einstufung des erreichten Reifegrades nach [IEC\_62443-2-2] vor. Er muss das Patch-Management planen und überwachen [IEC\_TR\_62443-2-3] und muss die Sicherheitsanforderungen für Dienstleister (z. B. Service-, Wartungs- und Inbetriebnahmepersonal), die in der Anlage arbeiten, gemäß [DIN\_EN\_IEC\_62443-2-4] definieren und überwachen.
- **Systemintegrator:** Der Systemintegrator / Anlagenplaner entwirft, installiert und nimmt Automatisierungssysteme in Betrieb. Wenn der Systemintegrator als Auftragnehmer arbeitet, muss er die Sicherheitsregeln für Dienstleister gemäß [DIN\_EN\_IEC\_62443-2-4] einhalten. Als Teil des Planungsprozesses muss eine Risikobewertung des Automatisierungssystems gemäß [DIN\_EN\_IEC\_62443-3-2] durchgeführt werden. Diese Aufgabe wird in der Regel in Zusammenarbeit / mit Unterstützung des Anlagenbetreibers durchgeführt. Der Systemintegrator muss bei der Planung die in [DIN\_EN\_IEC\_62443-3-3] definierten Anforderungen an die Systemsicherheit beachten.
- **Produktlieferant:** Der Produktlieferant muss die systemweiten Sicherheitsanforderungen nach [DIN\_EN\_IEC\_62443-3-3] kennen, da die Komponentenanforderungen aus dieser Norm abgeleitet wurden. Der Lieferant muss seine F&E- und Produktmanagementorganisation gemäß [DIN\_EN\_IEC\_62443-4-1] qualifizieren. Produktspezifische Anforderungen in Bezug auf die Automatisierungskomponenten sind in [DIN\_EN\_IEC\_62443-4-2] definiert. Für den Produktlieferanten ist es hilfreich, wenn er auch die systemweiten Security-Anforderungen nach

[DIN\_EN\_IEC\_62443-3-3] kenn, da die Security-Komponentenanforderungen aus dieser Norm abgeleitet werden.

•

Die verschiedenen Beteiligten müssen in ihrem Verantwortungsbereich die in der IEC 62443 definierten Prozesse einhalten und die Anforderungen erfüllen, um konforme Komponenten und Systeme innerhalb des Geltungsbereichs der IEC 62443 herzustellen.

Im weiteren Verlauf des Dokumentes wird die Rolle des Produktlieferanten nicht weiter betrachtet.

### 3.4. Die Security-Level in der IEC 62443

Die Security Level werden in der [DIN\_EN\_IEC\_62443-3-3] definiert. Die Norm kennt drei Arten von Security-Leveln (SL): Zu erreichender, erreichter und erreichbarer Security Level. Diese drei Arten beziehen sich auf die verschiedenen Phasen des sicheren Entwicklungslebenszyklus

- Der **Target SL** (SL-T) beschreibt den angestrebten Security-Level eines Systems. Der SL-T wird in der Regel im Rahmen der Risikobewertung definiert. Hierbei spielen der Security-Kontext und die vom System ausgehenden Gefahren eine Rolle.
- Der **Achieved SL** (SL-A) definiert den erreichten Security Level des betrachteten Systems. Dieser kann ermittelt werden, nachdem das System spezifiziert und nachdem das System realisiert wurden. Über die Ermittlung des SL-A kann festgestellt werden, ob ein System die im SL-T definierten Anforderungen erfüllt.
- Der **Capability SL** (SL-C) (erreichbarer SL) ist der Security-Level, den eine Komponente oder ein System bei korrekter Konfiguration liefern kann. Der SL-C gibt an, dass eine bestimmte Komponente oder ein bestimmtes System bei korrekter Konfiguration und Integration in der Lage ist, den Target-SL (SL-T) von sich aus ohne zusätzliche Maßnahmen zu erreichen.

Die vorangehend beschriebenen SL finden in den verschiedenen Phasen des OT-Security-Lebenszyklus Anwendung. Beginnend mit der Zielvorgabe (Target) für ein gegebenes System werden Betreiber und/oder Systemintegrator einen Entwurf des Automatisierungssystems erstellen, der sich an den Anforderungen aus dem zu automatisierenden Prozess und dessen Gefährdungspotenzial für Personal und Umwelt ergibt. Auf dieser Basis entsteht eine Festlegung für den SL-T. Daran anschließend wird das System so entworfen, dass der angestrebte SL-T erreicht werden kann. Dies ist häufig ein iterativer Vorgang, bei dem nach jedem Schritt der erreichte SL (SL-A) des Entwurfs gemessen und mit den SL-T verglichen wird.

Die Norm [DIN\_EN\_IEC\_62443-3-3] definiert auch ein Vektorformat für die gemeinsame Darstellung der drei Security-Level-Typen. Auf dieses Format soll an dieser Stelle nicht näher eingegangen werden. Tabelle 2 zeigt die Definition der Security Level gemäß [DIN\_EN\_IEC\_62443-3-3]. Eine genauere Definition findet sich im Anhang 3.2 der Norm.

Tabelle 2: Definition der Security Level nach [DIN\_EN\_IEC\_62443-3-3] Kapitel 3.3

SL	Beschreibung
1	Verhindern der nicht autorisierten Offenlegung von Informationen durch Abhören oder zufälliges Aufdecken.
2	Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit einfachen Mitteln bei geringem Aufwand, allgemeinen Fertigkeiten und geringer Motivation suchende Einheit.
3	Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit raffinierten Mitteln und moderatem Aufwand, IACS-spezifischen Fertigkeiten und mittlerer Motivation suchende Einheit.
4	Verhindern der nicht autorisierten Offenlegung von Informationen an eine danach aktiv mit raffinierten Mitteln und erheblichem Aufwand, IACS-spezifischen Fertigkeiten und hoher Motivation suchende Einheit.

In der Regel stehen Betreiber und Planer vor der Fragestellung, welcher Security-Level für eine „normale“ Produktionsanlage angemessen ist. Hierzu gibt es verschiedene Veröffentlichungen, die sich mit dieser Fragestellung befassen. Es sei hier auf [EHR2023], [FUH2016], [ISA2024]. Zusammenfassend lässt sich festhalten, dass die Autoren den SL2 für Automatisierungsanwendungen ohne spezielle Security-Anforderungen ansehen.

## 4. Die Aufgaben des Anlagenplaners nach IEC 62443

In der Norm IEC 62443 wird die Rolle des Anlagenplaners auch als Integrationsdienstleister (engl: Integration Service Provider) oder umgangssprachlich auch Systemintegrator (engl. System Integrator) bezeichnet. Der Anlagenplaner plant das Automatisierungssystem nach den Vorgaben des Anlagenbetreibers. Dabei muss der Anlagenplaner die OT-Security-Anforderungen im Planungsprozess berücksichtigen.

### 4.1. Relevante Normteile der IEC 62443 für Anlagenplaner

Für die Arbeit des Anlagenplaners sind gemäß der Darstellung in Abbildung 2 die folgenden Teile der IEC 62443 relevant:

- **[DIN\_EN\_IEC\_62443-2-4]:** Dieser Normteil befasst sich mit Anforderungen an Planungs- und Instandhaltungsdienstleister. Hierzu gehören insbesondere die Beherrschung der Security-Prozesse, eine entsprechende Qualifikation und Unterweisung des Personals in Bezug auf IT-Sicherheitsanforderungen, schützenswerte Daten, Mitarbeiterscreening, Bereitstellung von Werkzeugen zur OT-Security, Kenntnisse im Bereich der Härtung von Automatisierungssystemen, Kenntnisse in Bezug auf die Risikobeurteilung, Kenntnisse in Bezug auf die Netzauslegung, etc. Es geht bei dieser Norm also im Wesentlichen um die erforderliche Qualifikation eines Engineering-Dienstleisters / Anlagenplaners. Sofern ein Betreiber die Anlagenplanung selbst, also inhouse durchführt, sollte auch das eigene Planungspersonal über die entsprechende Qualifikation verfügen.
- **[DIN\_EN\_IEC\_62443-3-2]:** Dieser Teil der IEC 62443 befasst sich u.a. mit dem Risikomanagement und der Risikobewertung von Automatisierungsanlagen und legt die Anforderungen fest für:
  - „Die Festlegung eines zu betrachteten Systems (engl.: System under Consideration, SUC) für ein industrielles Automatisierungssystem (IACS);
  - Die Aufteilung des SUC in Zonen und Conduits; Bei einem Conduit handelt es sich um eine logische Gruppierung von Kommunikationskanälen, um zwei oder mehr Zonen mit gemeinsamen Sicherheitsanforderungen zu verbinden;
  - Die Beurteilung des Risikos für jede Zone und jeden Conduit;
  - Die Festlegung des zu erreichenden Security-Levels (SL-T) für jede Zone und jeden Conduit; und
  - Die Dokumentation der Security-Anforderungen.“

Der Anlagenplaner wird diese Aufgaben im Rahmen des Planungsprozesses bearbeiten.

- **[DIN\_EN\_IEC\_62443-3-3]:** Dieser Teil der Norm definiert die technischen Security-Anforderungen an die zu planende Anlage. Dieser Normteil definiert auf Basis von sieben grundlegenden Anforderungen (engl. Foundational Requirements -FR) detaillierte technische Systemanforderungen (eng. System Requirements -SR) an das Automatisierungssystem. Dies schließt die Festlegung der Anforderungen in Bezug auf den zu erreichenden Security-Level, SL-C (Automatisierungssystem) mit ein. Die grundlegenden Anforderungen sind:
  - Identifizierung und Authentifizierung (IAC)
  - Nutzungskontrolle (UC)
  - Systemintegrität (SI)

- Vertraulichkeit der Daten (DC)
- Eingeschränkter Datenfluss (RDF)
- Rechtzeitige Reaktion auf Ereignisse (TRE)
- Verfügbarkeit der Ressourcen (RA)
- Diese sieben Anforderungen bilden die Grundlage für die erreichbaren SLs eines Automatisierungssystems, die SLC (Automatisierungssystem).

Der Anlagenplaner legt auf Basis der Anforderungen dieses Normteils die Systemstruktur fest und bestimmt die erforderlichen Security-Eigenschaften der verwendeten Komponenten und die erforderlichen Security-Eigenschaften der Umgebung.

## 4.2. Die Aufgaben des Anlagenplaners im Detail

Der Prozess des OT-Security-Designs aus Sicht eines Anlagenplaners (Systemintegrators) umfasst in der Planungsphase die in den folgenden Unterkapiteln beschriebenen Aufgaben. Diese Aufgaben werden in Abstimmung mit dem Anlagenbetreiber, der in der Regel auch Auftraggeber ist, durchgeführt.

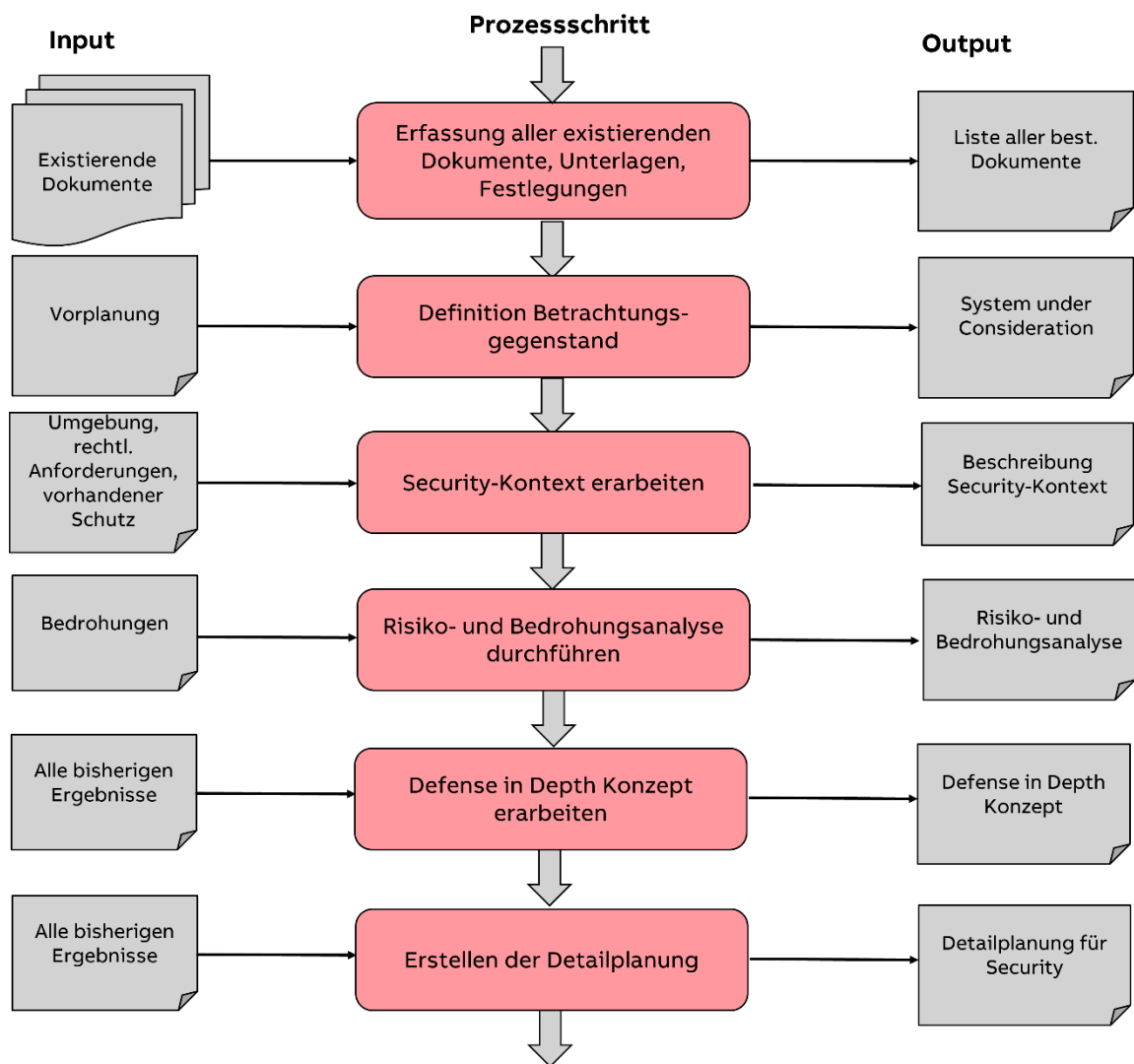


Abbildung 3: Ablaufplan für den Anlagenplaner im Security-Planungsprozess (Bild in Anlehnung an [DIN\_EN\_IEC\_62443-3-2])

Abbildung 3 zeigt die wesentlichen Schritte des Security-Planungsprozesses. In den folgenden Unterkapitel werden die einzelnen Planungsschritte im Detail weiter erläutert.

#### **4.2.1. Identifizierung bereits vorhandener Dokumente des Auftraggebers / Anlagenbetreibers**

Im ersten Schritt des Planungsprozesses ist festzulegen, welche Informationen der Auftraggeber dem Anlagenplaner zur Verfügung stellen kann. Hierbei geht es insbesondere um bereits ausgearbeitete Konzepte, Beschreibung von Schnittstellen zu anderen Anlagenteilen oder um bereits existierende Voruntersuchungen mit Bezug zur OT-Security, z. B. um Festlegungen zum Schutzbedarf oder um bereits durchgeführte Risikoanalysen. Die bereits bestehenden Informationen sollten erfasst und inventarisiert werden. Sie stehen dann als Input für die weiteren Planungsschritte zur Verfügung.

#### **4.2.2. Definition Betrachtungsgegenstand (System under Consideration)**

Die Grundlage für die folgenden Planungsschritte ist zunächst die Definition des Lieferumfangs und der Komponenten/Systemteile, die während des Sicherheitsplanungsprozesses berücksichtigt werden müssen. Die Definition endet mit einer Definition des „System under Consideration“ für die weitere Security-Planung. Wichtig ist hierbei, dass Systemgrenzen und Schnittstellen zu anderen Systemen definiert und dokumentiert werden. Basis für diese Aufgaben, kann zum Beispiel eine Ausschreibung oder eine Vorplanung des Auftraggebers sein, in der die Systemstruktur grundlegend definiert wurde.

#### **4.2.3. Definition des Security-Kontextes**

Der Security Kontext ist nach [IEC\_62443-1-1] wie folgt definiert:

*„Der Security-Kontext bildet die Grundlage für die Interpretation von Terminologie und Konzepten und zeigt auf, wie die verschiedenen Elemente der Security zueinander in Beziehung stehen. Unter dem Begriff Security wird hier die Verhinderung des illegalen oder unerwünschten Eindringens in ein industrielles Automatisierungs- und Steuerungssystem oder die Störung des ordnungsgemäßen und beabsichtigten Betriebs verstanden.“*

Im nächsten Schritt ist der Security-Kontext der Anlage zu definieren. Der Security-Kontext beschreibt dabei sowohl das Risiko als auch die Schutzfaktoren, die durch die Umgebung, in der das System betrieben wird, bedingt sind. Dazu können Standort, Verwendungszweck, Betriebsumgebung, externe Schutzmaßnahmen außerhalb des betrachteten Bereichs sowie bereits bekannte Bedrohungen gehören.

Beispiele für Eigenschaften des Security-Kontextes sind ein existierender Perimeterschutz (Zaun um das Werksgelände), eine Videoüberwachungsanlage-oder die Nutzung abgeschlossener Schaltschränke. In den Security-Kontext gehen aber auch bekannte Bedrohungen, wie z. B. regelmäßiger Zugang zur Anlage z. B. durch Besucher oder Lieferanten, ein. Auch rechtliche und regulatorische Anforderungen gehen in den Security-Kontext ein.

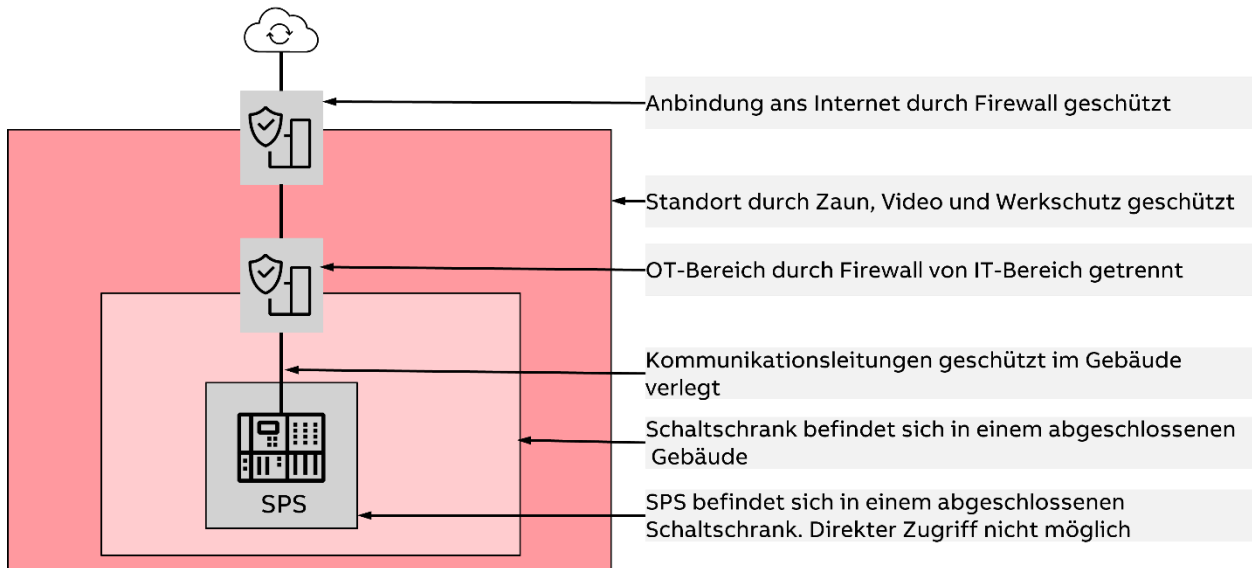


Abbildung 4: Beispiel für den Security Kontext einer SPS

Abbildung 4 zeigt exemplarisch den Security-Kontext einer SPS. Die Umgebung, in der die SPS betrieben wird, bietet bereits einen gewissen Schutz gegen mögliche Angriffe. So ist z. B. ein direkter Angriff auf SPS über das Bedienpanel oder eine Manipulation der Verkabelung nicht mehr möglich, weil die SPS in einem abgeschlossenen Schaltschrank betrieben wird. Weitere Schutzmaßnahmen ergänzen den Schutz der SPS. Es ist zu beachten, dass bei der Betrachtung des Security-Kontextes nicht nur ein möglicher Schutz aus der Umgebung, sondern auch ggf. mögliche Bedrohungen zu betrachten sind.

Das Ergebnis dieses Schrittes ist die Beschreibung des Security-Kontextes. Dieser wird für die in Kapitel 4.2.4 folgende Risiko- und Bedrohungsanalyse benötigt.

#### 4.2.4. Risiko- und Bedrohungsanalyse

Die [IEC\_62443-1-1] sagt zur Risiko- und Bedrohungsanalyse:

*„Im Rahmen des Prozesses der Bedrohungs-Risiko-Bewertung sind die Vermögenswerte Risiken ausgesetzt. Diese Risiken werden wiederum durch den Einsatz von Gegenmaßnahmen minimiert, die zur Behebung von Schwachstellen eingesetzt werden, die von verschiedenen Bedrohungen genutzt oder ausgenutzt werden.“*

Die Risiko- und Bedrohungsanalyse soll ermitteln, welchen Bedrohungen eine Anlage ausgesetzt ist. Die Bedrohungen werden in Bezug auf die Eintrittswahrscheinlichkeit und in Bezug auf das Schadensausmaß bewertet und in Form eines Risikos quantifiziert.

Führen Sie eine Risiko- und Bedrohungsanalyse durch. Diese Analyse soll Bedrohungen für das Automatisierungssystem bzw. die Produktionsanlage aufzeigen. Anhand des Schadensausmaßes und der Schadenswahrscheinlichkeit wird ein Risiko definiert. Bei Bedarf werden risikomindernde Maßnahmen definiert. Basierend auf den identifizierten Risiken werden der erforderliche Target-Security-Level (SL-T) für die betrachtete Zone definiert. Das Vorgehen zur Durchführung einer Risiko- und Bedrohungsanalyse findet sich in [DIN\_EN\_IEC\_62443-3-2]. Die [VDI\_2182\_1] liefert ebenfalls gute Informationen zur Durchführung von Risiko- und Bedrohungsanalysen. Hier finde sich auch Vorschläge für die tabellarische Dokumentation der Ergebnisse. Weitere Normteile beschreiben dann für Hersteller, Planer und Betreiber Beispiele aus der Fertigungs- und Prozessindustrie.

Die Risikoanalyse sollte von einem interdisziplinären Team durchgeführt werden. Typische Rollen in diesem Team sind gemäß [VDI\_2182\_1]:

- **Entscheider:** Initiator und gleichzeitig Entscheidungsträger für den vorliegenden: Der Entscheider legt fest, ob der Prozess angestoßen wird und welche der Gesamtlösungen in seinem Unternehmen implementiert wird. Beispiele: Geschäftsführer, Linienmanager.
- **Security-Experte:** Der Security-Experte stellt sich als Berater für alle IT-Security-relevanten Fragen zur Verfügung. Seine Hauptaufgabe besteht darin, die potenziellen Bedrohungen und Bedrohungsszenarien der Assets besonders in Automatisierungstechnischen Anwendungen aufzuzeigen und mögliche Gegenmaßnahmen vorzuschlagen. Beispiele: IS-Consultant, Security-Administrator.
- **Systemexperte:** IT-Security-relevante Fragen können bei einem Automatisierungssystem nur im Zusammenhang mit technischem Systemwissen beantwortet werden. Daher ist es notwendig, einen Experten auf diesem Gebiet in den Prozess mit einzubeziehen, der als Berater für systemrelevante Fragen fungiert. Gerade die Wirksamkeit und Umsetzbarkeit von Schutzmaßnahmen kann nur mit seiner Hilfe beurteilt werden. Beispiele: System-Administrator, -Entwickler, -Integrator.
- **Anwendungsexperte:** Neben dem technischen Systemwissen ist auch das Wissen über die gesamte Automatisierungsanwendung für die Ausführung dieses Prozesses wichtig. Der Anwendungsexperte hat somit einen Überblick über alle Systeme, die für eine bestimmte Anwendung relevant sind und kennt den Gesamtprozess sowie die Zusammenhänge. Beispiele: Produktmanager, Verfahrenstechniker.
- **Koordinator:** Der Koordinator ist aktiver Treiber des Vorgehens. Somit überwacht, verwaltet, koordiniert und steuert er den Prozessablauf sowie die mitwirkenden Akteure. Diese Rolle ist zuständig für den Gesamtprozess und agiert auch als Moderator und Leiter von Sitzungen, die innerhalb des Prozesses stattfinden. Beispiele: Projektmanager, Projektleiter, Entwicklungsleiter, Linienmanager.
- **Prozessauditor:** Der Prozessauditor prüft alle Schritte des beschriebenen Vorgehensmodells, die zur Sicherheitslösung geführt haben. Beispiele: externer/interner Auditor.“

Die folgende Beschreibung geht davon aus, dass die Risikoanalyse vom Systemintegrator durchgeführt wird. Dennoch müssen Beiträge und Personal des Anlagenbetreibers in den Prozess einbezogen werden.

**Strukturanalyse:** Vor der Verwendung des Verfahrensmodells sollte eine detaillierte Strukturanalyse durchgeführt werden. Diese umfasst eine Beschreibung des zu betrachtenden Systems und seiner Einsatzumgebung. Die Parameter, Funktionen, Schnittstellen und Datenflüsse des Prüfobjekts sollten definiert werden. Außerdem sollten Anwendungsspezifika und die Netzwerkinfrastruktur beschrieben werden. Eine visuelle Darstellung hilft dabei, Kommunikationsverbindungen und Interaktionen mit der Einsatzumgebung darzustellen.

**Identifizierung der Assets:** Der nächste Schritt ist die Identifizierung der Assets. Assets können beispielsweise sein: SPSen, Bedienpanels, Netzwerkkomponenten, Remote-IOs, Aktoren, Sensoren, Panel-PCs, PCs, die als Bedienstationen oder Engineering-Stationen verwendet aber auch Server. Die Liste der Assets kann auch immaterielle Vermögenswerte wie Rechtspositionen, geistiges Eigentum oder andere enthalten.

**Bedrohungsanalyse:** Die Bedrohungsanalyse identifiziert systematisch potenzielle organisatorische, technische und benutzerbezogene Bedrohungsursachen. Das Team muss die potenziellen Schwachstellen und Dienste des Inspektionsziels verstehen. Das Team kann verfügbare Bedrohungskataloge wie z. B. [BSI2023] (siehe Kapitel elementare Gefährdungen) oder [MIT2023] als grundlegende Referenz verwenden. Diese Kataloge bieten typische Bedrohungsszenarien, sollten jedoch durch spezifisches Anwendungswissen und Fachkenntnisse des Analyseteams ergänzt werden. Die Arbeit sollte die Sicherheitsziele der Anlage berücksichtigen. Diese Ziele können für verschiedene Teile der Anlage unterschiedlich sein, da sie möglicherweise unterschiedlich stark geschützt werden müssen.

**Risikoanalyse:** In dieser Phase soll eine übersichtliche Bedrohungsmatrix erstellt werden, aus der hervorgeht, auf welche Sicherheitsziele sich die einzelnen Bedrohungen auswirken. Dabei sollten sowohl typische Bedrohungen als auch deren Quellen, einschließlich der Handlungen von autorisierten und nicht autorisierten Benutzern, Angreifern und Malware, aufgeführt werden. Diese Bewertung muss alle aktuellen Gegenmaßnahmen berücksichtigen. Das identifizierte Risiko wird anhand des potenziellen Schadens und der Eintrittswahrscheinlichkeit analysiert.

**Identifizierung von Schutzmaßnahmen:** In diesem Schritt werden die erforderlichen Gegenmaßnahmen gegen Bedrohungen und deren Umsetzung skizziert. Anhand von Katalogen werden geeignete Maßnahmen für alle erheblichen Risiken ausgewählt, die gemindert werden müssen. Für jedes Risiko stehen eine oder mehrere Maßnahmen zur Verfügung, und es muss festgelegt werden, ob einzelne oder mehrere Maßnahmen erforderlich sind. Das Ziel besteht darin, dass die vorgeschlagenen Maßnahmen das Risiko ausreichend reduzieren, sodass keine weiteren Maßnahmen zur Risikominderung erforderlich sind. Gegenmaßnahmen sollten anhand derselben Klassen wie in der Risikoanalyse bewertet werden (niedrig, mittel, hoch). Oft können mehrere Gegenmaßnahmen auf dasselbe Risiko abzielen. Außerdem sollten die mit einer Gegenmaßnahme verbundenen Kosten, auch wenn sie mehrere Bedrohungen abdeckt, berücksichtigt werden, um die Gesamtkosteneffizienz zu bewerten.

**Auswahl der Schutzmaßnahmen:** In diesem Schritt werden aus einer vorgegebenen Liste Gegenmaßnahmen ausgewählt, die Wirtschaftlichkeit und Wirksamkeit in Einklang bringen. Die optimale Lösung steht im Einklang mit den Zielen und Sicherheitsrichtlinien des Unternehmens. Wenn mehrere kostenvergleichbare Gegenmaßnahmen existieren, sollte die am besten geeignete ausgewählt werden. Lösungen mit gleichen Kosten können unterschiedliche Arten von Ausgaben verursachen, wie z. B. Abschreibungen oder Personal. Bei der Entscheidung sollten Kosteneffizienz, strategische Anforderungen, Machbarkeit und Erweiterung auf potenzielle zukünftige Anforderungen abgewogen werden.

**Planumsetzung:** Die ausgewählten Schutzmaßnahmen sind in den Gesamtplanungsprozess des Automatisierungssystems/Produktionsplans zu integrieren.

**Prozessaudit:** Das Prozessaudit kann während oder nach der Inbetriebnahmephase durchgeführt werden. Siehe Kapitel 10.5.

Parallel zu der oben beschriebenen Risikoanalyse kann eine gleichwertige Analyse gemäß [DIN\_EN\_IEC\_62443-3-2] durchgeführt werden. Der Ablauf ist in Abbildung 5 dargestellt.

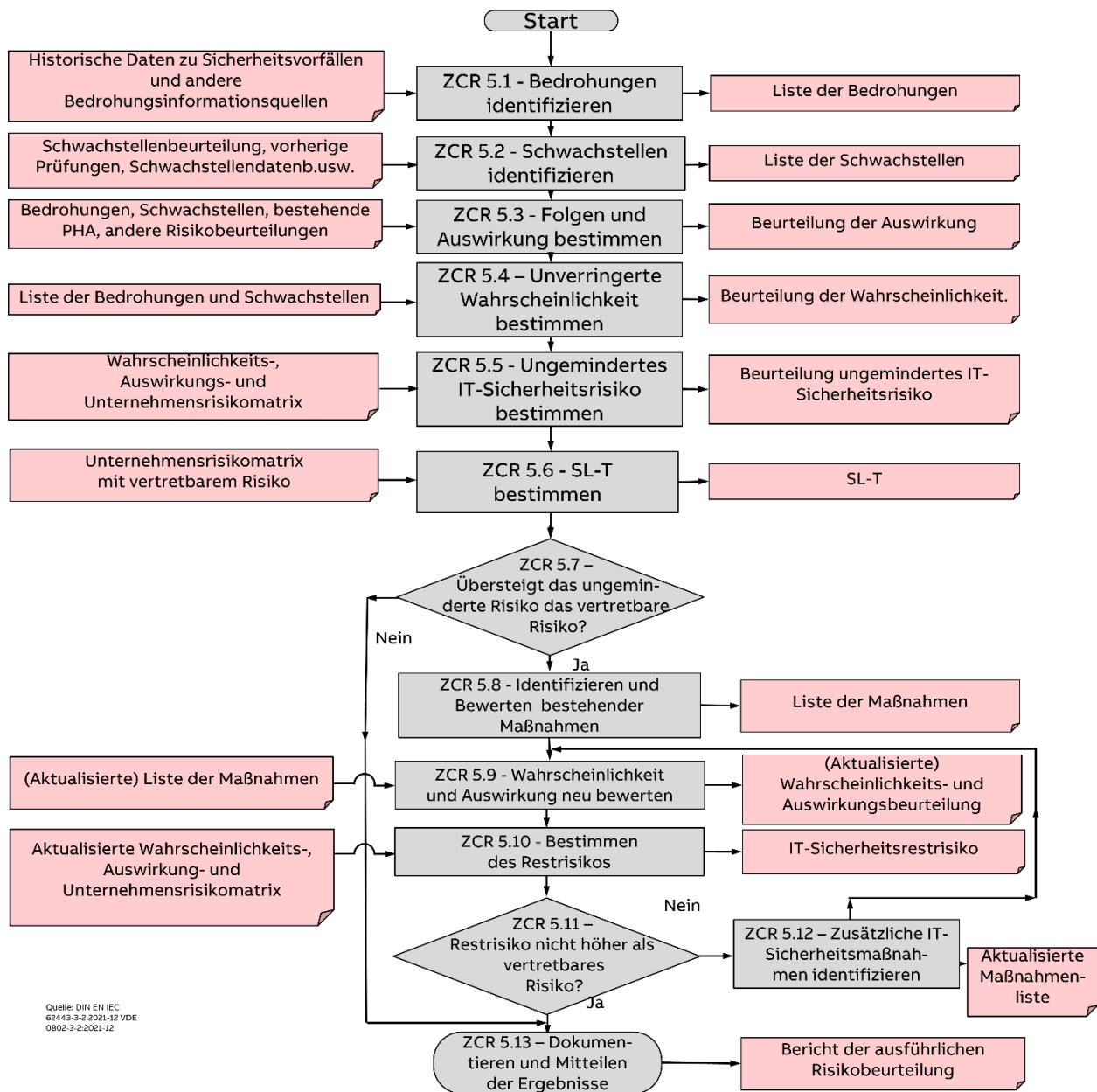


Abbildung 5: Risikoanalyse nach [DIN\_EN\_IEC\_62443-3-2]

Das Flussdiagramm für eine Analyse gemäß dieser Norm ist umfassender, liefert aber im Allgemeinen die gleichen Ergebnisse. Ein zusätzliches Thema, welches die Analyse gemäß [DIN\_EN\_IEC\_62443-3-2] umfasst, ist die Festlegung eines angestrebten Sicherheitsniveaus (SL-T) gemäß 3.4 Tabelle 2. Hierbei ist zu beachten, dass der SL-T für unterschiedliche Zonen der Anlage unterschiedlich hoch sein kann. Anlagenteile mit einem höheren Schutzbedarf können einen höhere SL-T erfordern als Anlagenteile mit einem geringeren Schutzbedarf. Darüber hinaus kann bei Bedarf der SL-T für einzelne Anforderungen unterschiedlich definiert werden. Das ist z. B. dann der Fall, wenn einzelne Anforderungen in diesem Anlagenteil eine besondere Wichtigkeit aufweisen.

#### 4.2.5. Defense in Depth Konzept

Beschreiben Sie den Defense In-Depth-Ansatz: Der Defense-In-Depth-Ansatz [DHS2009] basiert auf der Verwendung mehrerer Sicherheitsschichten, um dem Ausfall einer einzelnen Sicherheitskomponente vorzubeugen. Durch die Kombination der verschiedenen Maßnahmen auf unterschiedlichen Ebenen des

Systems wird das Schutzniveau durch eine entsprechende Zonenbildung für die Gesamtanlage erhöht. Abbildung 6 zeigt exemplarisch die logischen und physischen Vertrauensgrenzen für ein Automatisierungssystem.

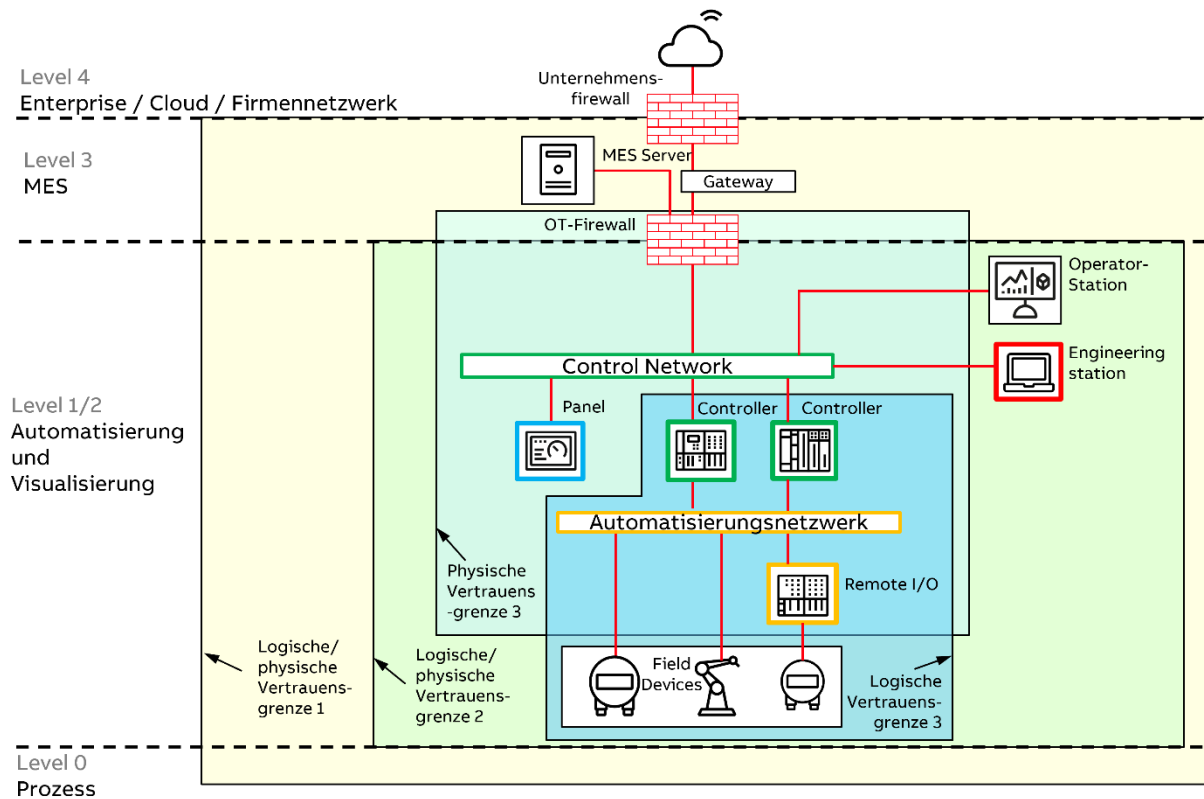


Abbildung 6: Vertrauensgrenzen und Zonenbildung in einem Automatisierungssystem

In Abbildung 6 ist eine gelb dargestellte Zone zu erkennen. Dies wird durch die logische / physische Vertrauensgrenze 1 eingerahmt. Die physische Vertrauensgrenze wird z. B. durch einen Zaun um das Werksgelände in Verbindung mit einem Überwachungssystem und einem zugriffsüberwachten Verwaltungsgebäude gebildet. Die logische Vertrauensgrenze 1 wird durch die Unternehmensfirewall gebildet. Die logische / physische Vertrauensgrenze 2 umrahmt die grün markierte Zone. Diese kann z. B. durch ein Produktionsgebäude mit Zutrittsüberwachung gebildet werden. Die logische Vertrauensgrenze 2 bildet die OT-Firewall. Die physische Vertrauensgrenze 3 könnte z. B. durch einen verschlossenen Schaltschrank oder einen verschlossenen Anlagenraum innerhalb des Produktionsgebäudes gebildet werden, welche die Automatisierungskomponenten gegen physischen Zugriff schützt. Die logische Vertrauensgrenze 3 bildet z. B. die kryptografisch gesicherte Kommunikation innerhalb des Automatisierungsnetzwerkes, z. B. eine PROFINET-Kommunikation in Verbindung mit PROFINET-Security [PNO2019]. Es ist in Abbildung 6 zu erkennen, wie sich die verschiedenen Schutzmaßnahmen im Rahmen des Defense-in-Depth-Konzeptes ergänzen.

Im Rahmen der Planung nach der [DIN\_EN\_IEC\_62443-3-3] wird das Defense-in-Depth-Konzept durch das Zonen-und-Conduit-Konzept ergänzt. Für die Umsetzung des Zonen-und-Conduit-Konzeptes werden die folgenden Schritte empfohlen:

1. Planen Sie das Netz und legen Sie die Zonen und Conduits fest: Die Sicherheit beruht auf der Trennung von Netzen (z. B. durch Firewalls), um das Automatisierungsnetz vor Bedrohungen von außen zu schützen. Die getrennten Teile des Netzes werden als Zonen bezeichnet. Ein Conduit ist eine logische Gruppierung von Kommunikationskanälen zur Verbindung von zwei oder mehr Zonen, die gemeinsame Sicherheitsanforderungen haben.

2. Planen Sie allgemeine Sicherheitsmerkmale für das Automatisierungssystem / die Produktionsanlage auf Basis der Risiko- und Bedrohungsanalyse.
3. Dokumentieren Sie die Ergebnisse des Planungsprozesses.
4. Holen Sie die Genehmigung / Abzeichnung vom Kunden / Anlagenbetreiber ein.

Weitere Aufgaben für den Systemintegrator wie die sichere Inbetriebnahme und die Systemhärtung folgen in späteren Kapiteln dieses Dokuments (siehe Kapitel 11)

#### 4.2.6. Erstellen der Detailplanung

Auf Basis der Vorarbeiten wird dann eine Detailplanung erstellt, welche die Security-Anforderungen der [DIN\_EN\_IEC\_62443-3-3] realisiert. Hierzu gehören z. B. Festlegungen, welche Kommunikationsprotokolle in welcher Ausprägung eingesetzt werden und welche Automatisierungskomponenten mit welchen Eigenschaften verwendet werden sollen.

Weiterhin sollte im Rahmen der Detailplanung auch ein Plan für die Härtung der Anlage im Rahmen der Inbetriebnahme erstellt werden und die hierfür erforderlichen Informationen beschafft werden. Unter Härtung versteht man das Abschalten nicht benötigter Dienste und Funktionen sowie die Auswahl möglichst sicherer Konfigurationseinstellungen, z. B. beim Betriebssystem von PCs. Zur Härtung von Automatisierungssystemen finden sich eine Reihe von Dokumenten, von denen hier einige genannt werden: [BSI2021a], [BSI2021b], [NAM2017], [NIST\_SP\_800-82], [PUL2025], [ZOR2025].

#### 4.2.7. Ergebnisse des Planungsprozesses

Die in den vorangehenden Schritten beschriebenen Planungsarbeiten führen zu den folgenden Ergebnissen:

- Liste aller bereits bestehenden Dokumente
- Beschreibung des betrachteten Systems (engl. System under Consideration)
- Beschreibung Security Kontext
- Risiko- und Bedrohungsanalyse
- Defense in Depth Konzept mit Zoneneinteilung und Target Security Level SL-T
- Security-Detailplanung

Die Ergebnisse sollten dokumentiert und für eine spätere Nutzung archiviert werden. Bei signifikanten Änderungen oder nach Ablauf einer bestimmten Zeit sollte die Risiko- und Bedrohungsanalyse aktualisiert werden.

### 4.3. Zusammenwirken des Planers mit den anderen Verantwortlichen im OT-Sicherheitsprozess

Abbildung 7 zeigt das Zusammenwirken von Betreiber, Planer und Hersteller im OT-Sicherheitsprozess.

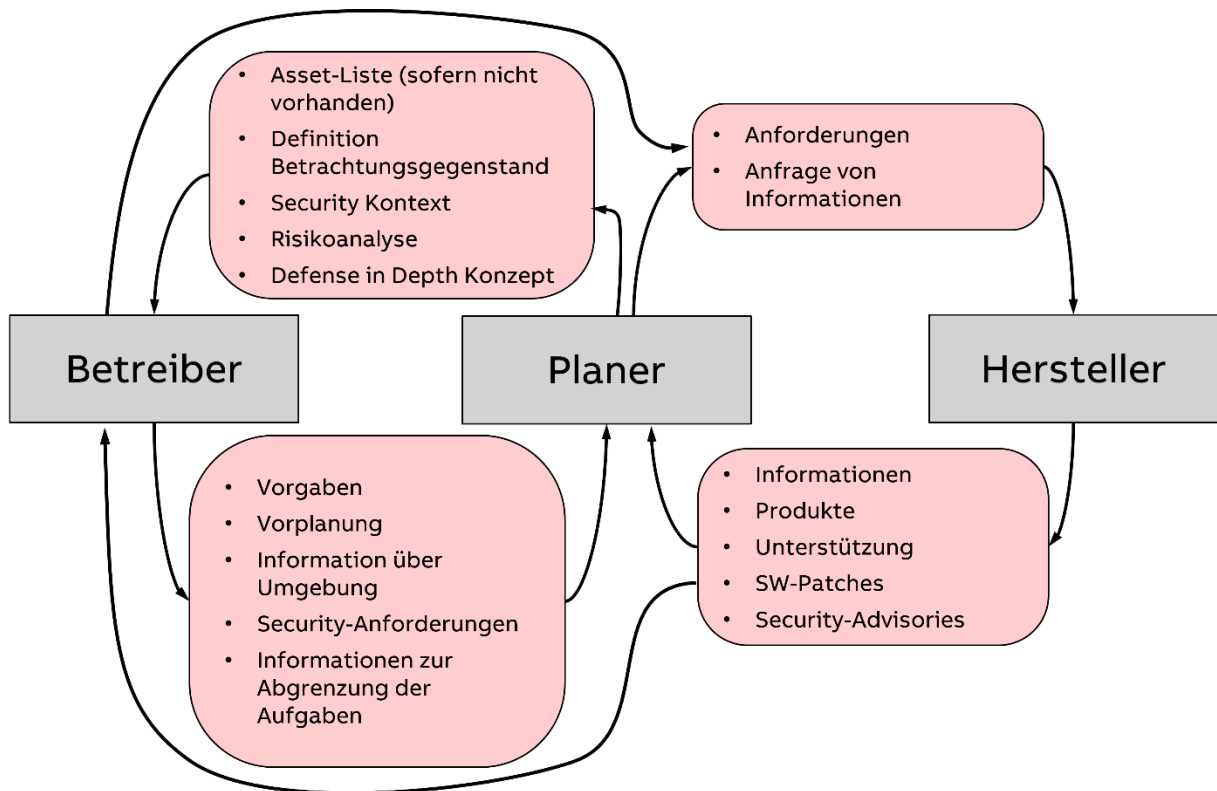


Abbildung 7: Zusammenwirken Planer, Betreiber und Hersteller

Der Betreiber, der in der Regel auch Auftraggeber für den Planer ist, stellt dem Planer existierenden Vorplanungen, Vorüberlegungen bereit und macht Vorgaben für den Planungsprozess. Gleichzeitig liefert er Informationen über die Betriebsumgebung, da der Planer dies für die Risikobetrachtung kennen muss. Weiterhin muss der Planer definieren, welche Aufgaben er selbst und welche Aufgaben der Planer im Security-Prozess übernehmen soll. Sowohl Betreiber als auch Planer stehen in Verbindung mit dem Hersteller, welcher das Automatisierungssystem oder wesentliche Teile davon liefern wird. Im Wesentlichen werden beim Hersteller die Erfüllung von Security-Anforderungen und technische Informationen angefragt, die dieser dann an Betreiber und/oder planer liefert. Darüber hinaus stellt der Hersteller beim Auftreten von Schwachstellen Security-Advisories und die zugehörigen Software-Patches bereit.

## 4.4. Vorschlag für die Realisierung der Security Anforderungen

Es wird vorgeschlagen den Planungsprozess gemäß Abbildung 3 durchzuführen. Die dort beschriebenen Hauptschritte werden in Tabelle 3 in Arbeitspakete heruntergebrochen.

Tabelle 3: Aufgabenpakete für den Security Planungsprozess

Schritt	Aufgabe	Verantwortlich
B1	Definition der Aufgabenstellung für den Planer, Abgrenzung der Aufgaben von Betreiber und Planer, Beauftragung des Planers in dem abgestimmten Umfang.	Betreiber
B2	Erfassung und Inventarisierung aller erforderlichen Unterlage und Weitergabe an den Planer.	Betreiber
B3	Dokumentation der Übergabe	Betreiber, Bestätigung Planer.

<b>P4</b>	Definition Betrachtungsgegenstand, Beschreibung der Schnittstellen	Planer, Bestätigung Betreiber
<b>P5</b>	Beschreibung Security-Kontext, sofern dieser noch nicht vorliegt, auf Basis der vom Betreiber bereitgestellten Information.	Planer, Bestätigung durch Betreiber
<b>P6</b>	Durchführen einer Risiko- und Bedrohungsanalyse	Planer, Bestätigung des Betreibers, dass die Restrisiken zur Kenntnis genommen wurden und akzeptiert werden.
<b>P7</b>	Erarbeiten eines Defense in Depth und des Zonen- und Conduit-Konzeptes	Planer, Abnahme durch Betreiber
<b>P9</b>	Erstellung der Detailplanung	Planer, Abnahme durch Betreiber.
<b>P10</b>	Planung der Härtung der Anlage	Planer, Abnahme des Vorgehens durch Betreiber
<b>P11</b>	Dokumentation und der Ergebnisse. Hier geht es insbesondere um die Erzeugung und Bereitstellung von Asset-Listen, Netzstrukturplänen sowie um die Konfiguration z. B. von Firewalls.	Planer, Abnahme und Prüfung auf Vollständigkeit durch Betreiber.

Es ist zu beachten, dass der in Tabelle 3 beschriebene Arbeitsplan lediglich ein Grundgerüst darstellt, welches an die Gegebenheiten des jeweiligen Projektes anzupassen ist.

## 4.5. Erfolgsfaktoren für den OT-Security-Prozess der Anlagenplaner

Es gibt einige Voraussetzungen, die für einen erfolgreichen und effizienten Planungsprozess gegeben sein müssen. Die wesentlichen sind:

- Klare Beschreibung des Auftragsgegenstandes
- Beschreibung aller anfallenden Security-relevanten Tätigkeiten in einer Aufgabenbeschreibung / in einem Lastenheft und Beauftragung dieser Leistungen.
- Frühe und vollständige Bereitstellung aller Vorarbeiten / Vorüberlegungen durch den Auftraggeber.
- Klare Abgrenzung der Zuständigkeiten zwischen Betreiber und Planer
- Zeitnahe Abnahme der in Tabelle 3 genannten Arbeitspakete.
- Security-Einweisung des Inbetriebnahmepersonals
- Bereitstellung eines PC (vorzugsweise in einer demilitarisierten Zone) zur Entgegennahme der Anlagenprojektierung des Anlagenplaners.

## 5. Die Aufgaben des Anlagenbetreibers nach IEC 62443

Diese Kapitel befasst sich mit den Aufgaben des Anlagenbetreibers. Neben den bereits in Tabelle 3 beschriebenen Aufgaben in Bezug auf die Bereitstellung von Information und die Abnahme von Arbeitsergebnissen, muss der Betreiber insbesondere Aufgaben in der Betriebsphase und bei der Außerbetriebsetzung der Anlage übernehmen.

### 5.1. Relevante Normteile der IEC 62443 für Anlagenbetreiber

Für die Arbeit des Anlagenbetreibers sind gemäß der Darstellung in Abbildung 2 die folgenden Teile der IEC 62443 relevant:

Die **[DIN\_EN\_IEC\_62443-2-1]** beschreibt die Prozesse, die ein Anlagenbetreiber etablieren und aufrechterhalten muss, um den sicheren Betrieb der Anlage zu gewährleisten. Die englischsprachige Version dieser Norm liegt inzwischen in einer neueren Fassung vor **[IEC\_62443-2-1]**. In diese Betrachtung wird auch das Personal einbezogen, welches für die Bedienung der Anlage verantwortlich ist. Die Norm definiert Anforderungen für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung eines IACS-Sicherheitsprogramms. Zweck des Sicherheitsprogramm ist die Minderung von IACS-Sicherheitsrisiken auf ein vertretbares Maß. Diese Anforderungen in der Norm sind so verfasst, dass sie unabhängig von der Umsetzung sind, so dass Betreiber, die für ihre Bedürfnisse am besten geeignete Ansätze auswählen können. Das Dokument verwendet einen risikobasierten Ansatz; Die Anforderungen dienen dazu vorhandene Security-Betriebsrisiken auf ein akzeptables Maß zu reduzieren. Wesentliche Anforderungen der Norm sind z. B:

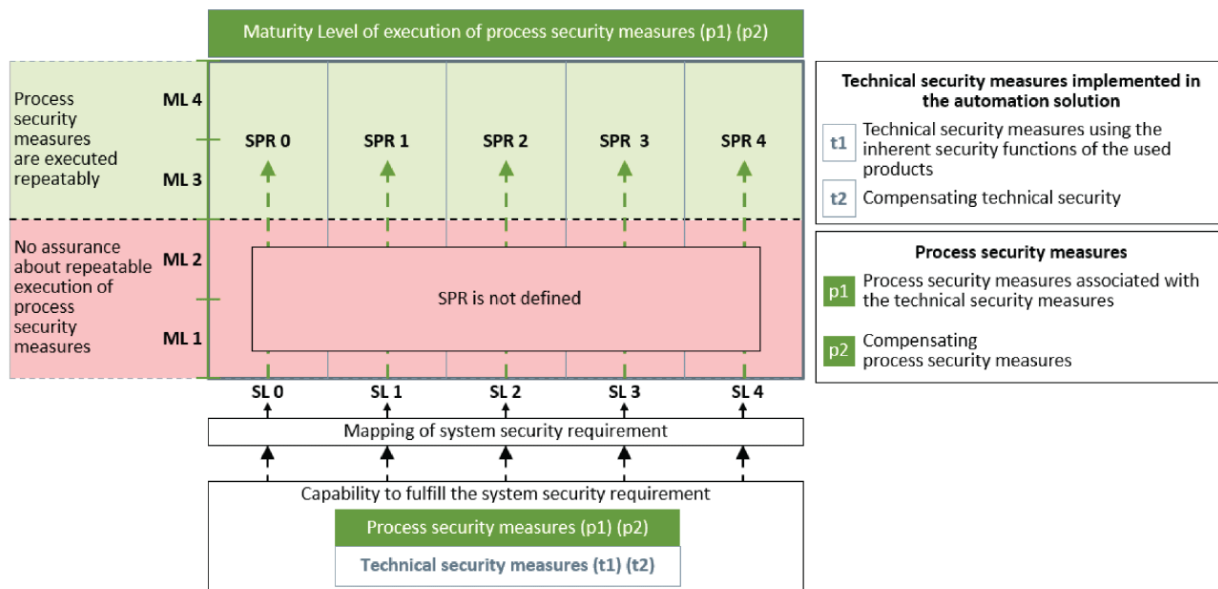
- Qualifikation des Personals.
- Schulung der Mitarbeiter, Auftragnehmer, Unterauftragnehmer, Berater und Lieferanten in Bezug auf die OT-Security.
- Sicherheit der Lieferkette: Definition von Anforderungen an Dienstleister und Lieferanten.
- Identifikation und Reduzierung von IT-Sicherheitsrisiken.
- Etablierung von Prozessen zur Entdeckung von IT-Sicherheitsanomalien.
- Verwendung von Komponenten, die unter Beachtung des sicheren Entwicklungslebenszyklus (siehe **[DIN\_EN\_IEC\_62443-4-1]**) entwickelt wurden.
- Regelmäßige Prüfung und Anpassung des Sicherheitsprogramms.
- Begrenzung und Kontrolle des Zugriffs auf das Automatisierungssysteme.
- Inventarisierung der Hard- und Softwarekomponenten.
- Erstellung und Pflege der Anlagendokumentation (z. B. Asset-Listen und Netzpläne).
- Dokumentation der Konfigurationsinformation für alle Komponenten sowie entsprechende Aktualisierung der Dokumentation.
- Festlegung der Netzwerksegmentierung und Überwachung der Aufrechterhaltung.
- Planung des Systems so, dass es auch bei Trennung vom Rest des Netzwerks (ggf. eingeschränkt) weiterarbeiten kann.
- Identifizierung und Authentifizierung von Geräten, die an das Netzwerk angeschlossen werden.

Diese Aufstellung gibt lediglich einen Auszug aus der Norm wieder. Weitere Punkte sind z. B. Drahtlosnetzwerke, sicherer Fernzugriff, Komponentensicherheit (Schutz von Schnittstellen), Härtung der Geräte, mobile Datenträger, Schutz vor Schadsoftware, Patchmanagement (hierzu gibt es auch einen eigenen Normteil [IEC\_TR\_62443-2-3]), vordefinierte Systemzustände im Fehlerfall, etc..

In Kapitel 3.1 wurde bereits darauf hingewiesen, dass das OT-Security Programm auch mit einem im Unternehmen evtl. bestehendes Sicherheitsprogramm nach ISO 27000 kombiniert werden kann. Details hierzu finden Sie in [NIE2021]

In der [IEC\_62443-2-2] geht es um eine Methodik zur Evaluation des Schutzes industrieller Automatisierungssysteme. Hierbei werden organisatorische und technische Maßnahmen parallel betrachtet und in einem Gesamtwert, dem so genannten „Security Program Rating“ (SPR) bewertet. Die Methodik basiert auf der Erfüllung technischer und organisatorischer Anforderungen, die in den relevanten Dokumenten der Normenreihe IEC 62443 festgelegt sind.

Ziel dieses Vorgehens ist darzustellen, dass die Security-Eigenschaften einer Produktionsanlage nicht nur durch die technischen Anforderungen, sondern auch durch den Reifegrad der Organisation beschrieben werden.



IEC

Abbildung 8: Security Program Rating nach [IEC\_62443-2-2]

Abbildung 8 zeigt einen Auszug aus der [IEC\_62443-2-2]. Auf der Abszisse sind die möglichen Security Level SL1 bis SL4 aufgetragen. Dies definieren die technischen Security-Eigenschaften des realisierten Automatisierungssystems (SL1 ist der geringste Wert, SL4 der höchste). Auf der Ordinate sind die Maturity Level ML1 bis ML4. Diese beschreiben den Reifegrad der Organisation des Anlagenbetreibers (ML1 ist der geringste Level, ML4 der höchste). Aus der Matrix kann nach Auswahl eines Security Levels SL und eines Maturity Levels ML das zugehörige Security Program Rating (SPR) abgelesen werden. Es ist zu erkennen, dass für ein hohe SPR sowohl ein hoher SL als auch ein hoher ML benötigt werden. Dies stärkt die Aussage, dass Security nur durch die Kombination von Technik und Prozessen realisierbar ist.

Der Normteil [IEC\_62443-2-3] betrachtet das Patch-Management für Automatisierungssysteme. Hierbei geht es um die Interaktion zwischen dem Hersteller und Betreiber in Bezug auf Security-Patches. Die Norm definiert ein Zustandsmodell für Hersteller und Betreiber in Bezug auf den Test- und Freigabestatus von Patches. Weiterhin wird ein Datenformat für den standardisierten und maschinenlesbaren Informationsaustausch.

**[DIN\_EN\_IEC\_62443-2-4]:** Dieser Normteil befasst sich mit Anforderungen and Planungs- und Instandhaltungsdienstleistungen und wurde bereits in Kapitel 4.1 beschrieben.

Der Teil IEC 62443-2-5 soll Implementierungshinweise liefern. Dieser Teil ist noch nicht erschienen.

## 5.2. Die Aufgaben des Anlagenbetreibers im Detail

Abbildung 9 gibt einen Überblick über die Aufgaben des Anlagenbetreibers im Security-Prozess. Es wird hier bei unterschieden zwischen Aufgaben, die für eine konkrete Anlage anfallen sowie kontinuierlichen Aufgaben, die für den ganzen Standort anfallen.

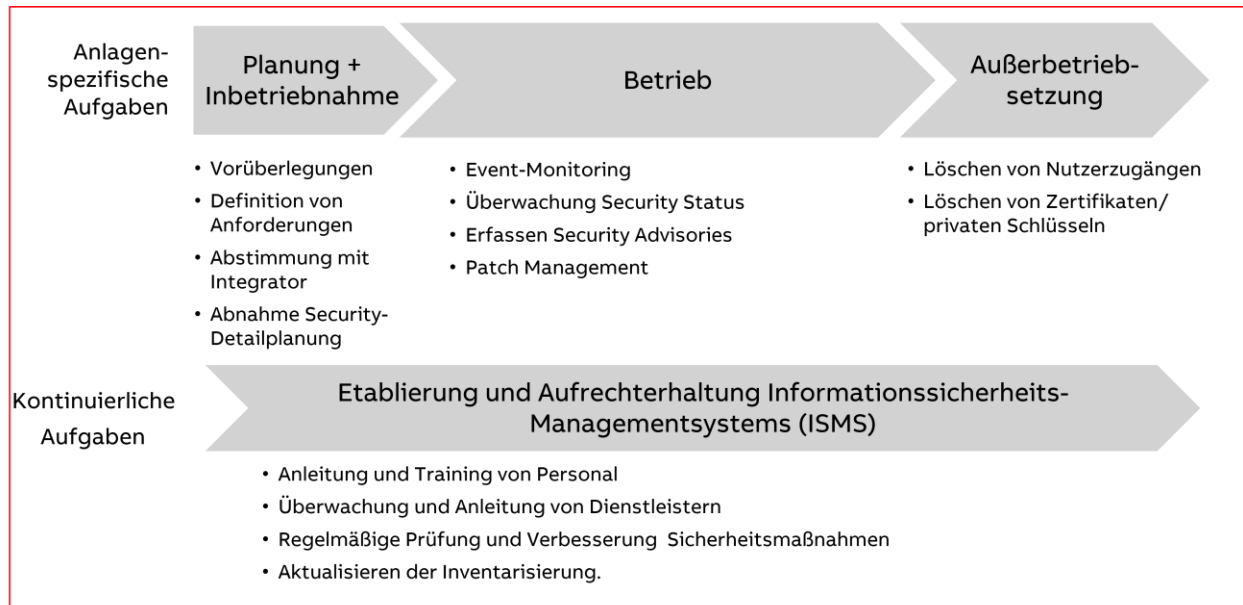


Abbildung 9: Aufgaben des Anlagenbetreibers

Die anlagenspezifischen Aufgaben in **der Planungs- und Inbetriebnahmephase** wurden in Kapitel 4.3 beschrieben. Hier sei insbesondere auf Tabelle 3 verwiesen.

Mit der Übergabe der Anlage durch vom Planer an den Betreiber beginnt die **Betriebsphase**. Es wird davon ausgegangen, dass alle erforderlichen technischen Security-Vorkehrungen geplant und in Betrieb genommen wurden. In diesem Fall hat der Betreiber zum Beispiel die folgenden Aufgaben:

- Überwachung der anfallenden Security Events und Auslösen einer entsprechenden Reaktion. Das kann zum Beispiel im Rahmen eines Security Information and Event Management Systems (SIEM) erfolgen.
- Pflege der Anlagendokumentation bei Veränderungen, z. B. Asset-Listen, Netzpläne.
- Überwachung Security-Status der Anlage und Reaktion auf Ereignisse, z. B. durch automatisierte Auswertung von Log-Informationen.
- Erfassung und Auswertung von Security-Advisories der Leitsystemhersteller. Prüfung, ob Hard- oder Softwareaktualisierungen auf Grund dieser Advisories auf die installierten Assets anzuwenden sind. Durchführen einer Risikoabwägung in Bezug auf den Installationszeitpunkt, ggf. Festlegung von risikominimierenden Ersatzmaßnahmen, falls Patches nicht zeitnah installierbar.
- Test der Softwareupdates in Bezug auf den Einsatz in der eigenen Anlage. Planung der Hard- und/oder SW-Updates.
- Aktualisierung der Risiko- und Bedrohungsanalyse in regelmäßigen Abständen, bei Veränderung der Anlage oder bei bekannten Vorfällen.

In der Phase der **Außerbetriebsetzung** sind im Wesentlichen die in der Anlage verwendeten Nutzerzugänge (Credentials) zu löschen, so dass kein Zugriff mehr auf die Komponenten gegeben ist.

Festplatten von Servern und Rechnern sollten vor Verschrottung gelöscht und die Datenträger mit Zufallsmustern überschrieben werden. Eventuell gespeicherte Zertifikate oder private Schlüssel des Betreibers sind vor Verschrottung zu löschen. Sofern dies nicht möglich ist, sollte eine Vernichtung der Baugruppe erfolgen.

Neben diesen anlagenspezifischen Tätigkeiten muss der Betreiber noch ein Informationssicherheitsmanagementsystem (ISMS) aufbauen und betreiben. Dies ist eine generelle und keine anlagenspezifische Aufgabe. Es sei hier auf die [DIN\_EN\_IEC\_62443-2-1] verwiesen, in der die notwendigen Aktivitäten in Form von Anforderungen dokumentiert sind. In Kapitel 5.1 wurde ein Auszug der erforderlichen Aktivitäten beschrieben.

### 5.3. Zusammenwirken mit den anderen Verantwortlichen im OT-Sicherheitsprozess

Das Zusammenwirken des Betreibers mit den anderen Verantwortlichen im OT-Sicherheitsprozess wurde bereits in Kapitel 4.3 erläutert. Es sein hier auf Abbildung 7 und die zugehörigen Erläuterungen verwiesen.

### 5.4. Vorschlag für ein Vorgehen bei der Realisierung der Anforderungen für Betreiber

Es wird vorgeschlagen, gemäß der Aufteilung in Abbildung 9 vorzugehen und die anlagenspezifischen Teile und die kontinuierlichen Aufgaben in getrennten Arbeitspaketen zu verwalten. Sofern ein Betrieb aus mehreren Anlagen besteht, können hier Synergieeffekte genutzt werden. In jedem Fall ist die Benennung eines/einer OT-Security-Verantwortlichen zu empfehlen. Tabelle 4 gibt einen Überblick über mögliche Arbeitspakete. Es wird hierbei zwischen den kontinuierlichen, zentralen Aufgaben K und den anlagenspezifischen Aufgaben A unterschieden. Die Tabelle nennt grundlegenden Aktivitäten, die an die Erfordernisse des jeweiligen Betreibers anzupassen sind.

Tabelle 4: Arbeitspakete für den Security Prozess für Betreiber

Schritt	Aufgabe	Verantwortlich
K1	Aufbau eines ISMS, vorzugsweise in Abstimmung mit der IT-Abteilung. Sofern schon vorhanden: Anlehnung an ein bestehendes Unternehmens-ISMS	OT-Security-Verantwortliche/r
K2	Training der Mitarbeitenden: Schulung der Mitarbeiter, Auftragnehmer, Unterauftragnehmer, Berater und Lieferanten in Bezug auf die OT-Security.	OT-Security-Verantwortliche/r
K3	Sicherheit der Lieferkette: Definition von generellen Anforderungen an Dienstleister und Lieferanten, die nicht projektspezifisch sind (mitgeltende Unterlagen OT-Security)	OT-Security-Verantwortliche/r
K4	Etablierung von Prozessen zur Entdeckung von IT-Sicherheitsanomalien z. B. durch die zentrale Auswertung von Log-Daten. Bereitstellung eines solchen Systems und Anbindung der Automatisierungssysteme	OT-Security-Verantwortliche/r
K5	Erstellen einer OT-Security-Richtlinie. Unterweisung der Mitarbeitenden und Dienstleister. Überwachung der Einhaltung	OT-Security-Verantwortliche/r
K6	Erstellung eines firmeneinheitlichen Konzeptes für die Fernwartung der Anlagen. Klärung der Anforderungen mit den Anlagenverantwortlichen. Einheitliche Umsetzung für möglichst alle Anlagen.	OT-Security-Verantwortliche/r

<b>K7</b>	Erstellung eines Notfall- und Wiederanlaufplans für das Unternehmen. Ausrollen des Plans. Durchführen von Notfallübungen.	OT-Security-Verantwortliche/r
<b>K8</b>	Bei Anlagen die unter die NIS-2-Direktive fallen: Erstellen eines Meldesystems für die Meldung Security-relevanter Vorfälle.	OT-Security-Verantwortliche/r
<b>K9</b>	Erstellung und Umsetzung eines zentralen Backups-Konzeptes für die OT. Ausrollen des Konzeptes und Durchführen von Restore-Übungen.	OT-Security-Verantwortliche/r
<b>A10</b>	Unterstützung des Planers bei Planung und Inbetriebnahmen in Bezug auf Security-Aspekte	Security-Verantwortliche/r Anlage
<b>A11</b>	Überwachung der Einhaltung der Security-Richtlinien für den Bereich der Anlage.	Security-Verantwortliche/r Anlage
<b>A11</b>	Reaktion auf Security-Ereignisse, die im Rahmen des Monitorings erkannt werden. Bei Anlagen in der kritischen Infrastruktur (KRITIS) oder bei Anlagen die unter die NIS-2-Direktive fallen: Absetzen einer Meldung über den definierten Kanal des Unternehmens.	Security-Verantwortliche/r Anlage
<b>A13</b>	Monitoring der Security Advisories der Leitsystem- und Komponentenhersteller und Ableitung von Maßnahmen für die Anlage.	Security-Verantwortliche/r Anlage
<b>A14</b>	Entgegennahme der SW-Patches der System- oder Komponentenherstellern. Prüfung der Patches auf Eignung und Relevant. Falls erforderlich, Planung und Durchführung der SW-Updates	Security-Verantwortliche/r Anlage
<b>A15</b>	Aktualisierung der Risiko- und Bedrohungsanalyse in regelmäßigen Abständen, bei Veränderung der Anlage oder bei bekannten Vorfällen	Security-Verantwortliche/r Anlage

## 5.5. Erfolgsfaktoren für den Security-Prozess der Anlagenbetreiber

Es gibt einige Voraussetzungen, die für einen erfolgreichen und effizienten Betrieb von Produktionsanlagen gegeben sein müssen. Die wesentlichen sind:

- Management-Kommittent zur Notwendigkeit von IT- und OT-Security im Unternehmen.
- Benennung eines/einer OT-Security-Verantwortlichen.
- Integration des/der OT-Security-Verantwortlichen in den Security-Prozess des Unternehmens.
- Enger Austausch zwischen den Verantwortlichen für IT- und OT-Security.
- Erstellung einer OT-Security-Richtlinie für den Betrieb der Produktionsanlagen.
- Integration der OT-Security-Anforderungen in die Lieferkette (Hersteller und Systemintegratoren).
- Automatisiertes Asset Management.
- Lieferanten auffordern, maschinenlesbare Security-Advisories bereitzustellen.
- Security-Training von Personal und Dienstleistern.
- Kontinuierliche Überwachung und Verbesserung der Security-Prozesse nach einem Plan, Do, Check, Act-Vorgehen.

Die vorangehende Aufzählung stellt nur einen Auszug möglicher Erfolgsfaktoren dar.

## 6. Zusammenfassung

Die Security basiert gemäß [IEC\_62443-1-1] aus den in Abbildung 10 dargestellten Komponenten.

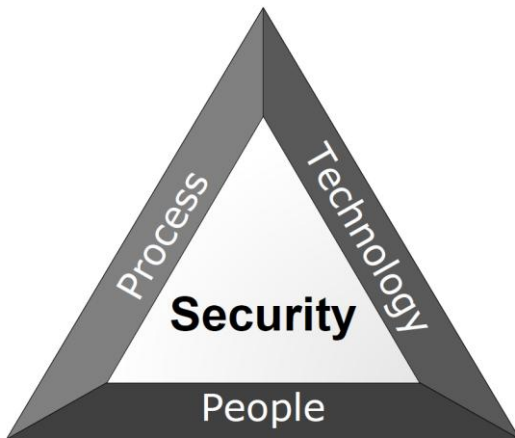


Abbildung 10: Die Komponenten der Security, Quelle [IEC\_62443-1-1]

Die Aussage des Bildes ist, dass die OT-Security nicht nur durch technische Maßnahmen wie Firewalls oder Netzwerkmonitoring, sondern auch durch die zugehörigen Prozesse erreicht wird. Ein Netzwerkmonitoring nützt dem Unternehmen nur dann, wenn die anfallenden Ereignisse ausgewertet und angemessen und zeitnah darauf reagiert wird. Dies ist nur durch die zugehörigen Prozesse möglich die etabliert und stabil betrieben werden müssen. Dabei ist festzuhalten, dass die Security-Prozesse einem risikobasierten Ansatz folgen. Ziel dabei ist eine Risikoreduzierung auf ein akzeptables Niveau, welches einen akzeptablen Kompromiss u. a. aus Security, Kosten, Bedienbarkeit und Anlagenverfügbarkeit ergibt. Der Mensch ist die dritte Komponente zum Erreichen einer guten OT-Security. Nur durch regelmäßiges Training (Notfallübungen, Restore-Übungen eines Backup-System), die Vorgabe klarer Richtlinien (was darf ich, was darf ich nicht) kann ein stabiler Security Prozess erreicht werden.

## 7. Abbildungsverzeichnis

Abbildung 1: Übersicht über die Normreihe IEC 62443, In Anlehnung an [DKE2024] .....	7
Abbildung 2: Beteiligte am OT-Sicherheitsprozess und zugeordnete Teile der IEC 62443 (abgeleitet aus der [IEC_62443-4-1]) .....	9
Abbildung 3: Ablaufplan für den Anlagenplaner im Security-Planungsprozess (Bild in Anlehnung an [DIN_EN_IEC_62443-3-2]) .....	13
Abbildung 4: Beispiel für den Security Kontext einer SPS .....	15
Abbildung 5: Risikoanalyse nach [DIN_EN_IEC_62443-3-2] .....	18
Abbildung 6: Vertrauensgrenzen und Zonenbildung in einem Automatisierungssystem .....	19
Abbildung 7: Zusammenwirken Planer, Betreiber und Hersteller .....	21
Abbildung 8: Security Program Rating nach [IEC_62443-2-2] .....	24
Abbildung 9: Aufgaben des Anlagenbetreibers .....	25
Abbildung 10: Die Komponenten der Security, Quelle [IEC_62443-1-1] .....	29



## 8. Tabellenverzeichnis

Tabelle 1: Unterscheidung zwischen IT und OT nach [GAR2021] .....	6
Tabelle 2: Definition der Security Level nach [DIN_EN_IEC_62443-3-3] Kapitel 3.3 .....	11
Tabelle 3: Aufgabenpakete für den Security Planungsprozess .....	21
Tabelle 4: Arbeitspakete für den Security Prozess für Betreiber .....	26

## 9. Stichwortverzeichnis

Abgrenzung der Zuständigkeiten .....	22	ISO 27000 .....	8, 24
Achieved SL.....	10	IT6	
Anlagenbetreiber .....	5, 8, 9, 23	IT-Sicherheitsrisiken.....	23
Anlagendokumentation.....	23, 25	Kommittent .....	27
Anlagenplaner .....	12	Konfigurationsinformation.....	23
Aufgaben.....	13	KRITIS .....	27
Asset Management.....	27	Lastenheft.....	22
Asset-Owner.....	5	Lieferkette .....	23, 26
Außerbetriebsetzung .....	25	Log-Daten .....	26
Authentifizierung .....	12, 23	Netzwerksegmentierung.....	23
Authentizität .....	6	Nichtabstreitbarkeit.....	6
Automatisierungskomponenten .....	8	NIS-2 .....	27
Automatisierungssystem.....	21	Notfall- und Wiederanlaufplan .....	27
Automatisierungssysteme.....	8	Nutzungskontrolle .....	12
Backup .....	27	Operational Technology .....	6
Begrenzung Zugriff.....	23	OT.....	6
Begriffe.....	7	OT-Security-Richtlinie .....	26, 27
Betreiber .....	7	OT-Security-Verantwortlicher .....	26, 27
Betriebsphase.....	25	Patch-Management .....	6, 24
Betriebsumgebung.....	14	Perimeterschutz .....	14
Capability SL.....	10	Produktlieferant .....	8, 9
Conduits.....	12	Prozessaudit.....	17
Defense in Depth.....	18	Qualifikation.....	23
Defense in Depth Konzept .....	20	Reaktion auf Ereignisse .....	25
Defense-in-Depth-Konzept.....	5	Rechtzeitige Reaktion .....	13
Detailplanung.....	20	Risiko- und Bedrohungsanalyse.....	15
Dienstleister .....	7, 8	Risikoanalysen .....	14
Drahtlosnetzwerke.....	24	Rollen im OT-Sicherheitsprozess.....	8
Eingeschränkter Datenfluss .....	13	Schaden .....	17
Eintrittswahrscheinlichkeit.....	17	Schulung.....	23, 26
Elementare Gefährdungen.....	16	Schutzbedarf .....	14
Erfolgsfaktoren .....	22, 27	Schutzmaßnahmen .....	17
Evaluationsmethodik .....	8	Security Events .....	25
Fernzugriff .....	24	Security Kontext .....	14, 20
Foundational Requirements .....	12	Security Level .....	10, 11
FR .....	12	Security Program Rating .....	24
Grundsätze .....	7	Security-Advisories .....	25
Härtung .....	20, 22	Security-Anforderungen .....	12
IACS .....	7	Security-Detailplanung .....	20
IACS-Sicherheitsprogramm .....	23	Security-Kontext.....	14
IEC 62443 .....	5, 7	Security-Level.....	12
Übersicht.....	7	Security-Prozess.....	12
Information Technology.....	6	Security-Richtlinien.....	27
Information-Security-Management-System.....	5	Security-Status .....	25
Informationssicherheitsmanagementsystem	26	Security-Training.....	27
Instandhaltungsdienstleister .....	24	Service Provider .....	12
Integrationsdienstleister .....	12	Sicherer Entwicklungslebenszyklus .....	23
Integrität.....	6	Sicherheitsanomalien.....	26
Inventarisierung .....	23	SL-A.....	10
ISMS.....	5, 6, 26	SL-C .....	10, 12

SL-T.....	10, 12, 15
SPR.....	24
SR.....	12
SUC.....	12
System Requirements.....	12
System under Consideration.....	12, 14
Systemintegrator.....	8, 9, 12
Systemintegrität.....	12
Systemlieferant.....	8

Target SL.....	10
Trennung.....	23
Überwachung.....	27
Verfügbarkeit.....	6, 13
Vertrauensgrenze.....	19
Vertrauensgrenzen.....	19
Vertraulichkeit.....	6, 13
Zonen.....	12
Zonenbildung.....	19

## 10. Literaturverzeichnis

- [BSI2021a] Bundesamt für Sicherheit in der Informationstechnik (BSI): IND.1: Prozessleit- und Automatisierungstechnik. URL: [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?\\_\\_blob=publicationFile&v=2](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?__blob=publicationFile&v=2).
- [BSI2021b] Bundesamt für Sicherheit in der Informationstechnik (BSI): Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln. URL: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen\\_zur\\_Haertung\\_von\\_Windows\\_10.pdf?\\_\\_blob=publicationFile&v=3](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Konfigurationsempfehlungen_zur_Haertung_von_Windows_10.pdf?__blob=publicationFile&v=3).
- [BSI2023] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium. URL: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT\\_Grundschutz\\_Kompendium\\_Edition2023.pdf?\\_\\_blob=publicationFile&v=4#download=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1).
- [DIN\_EN\_IEC\_62443-2-1] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-2-1:2020-10 - Entwurf VDE 0802-2-1:2020-10: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-1: Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber (IEC 65/756/CDV:2019); Deutsche und Englische Fassung prEN IEC 62443-2-1:2019, 2020. URL: <https://www.dinmedia.de/de/norm-entwurf/din-en-iec-62443-2-1/327919389>.
- [DIN\_EN\_IEC\_62443-2-2] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-2-2 (VDE 0802-2-2): 2021-05: IT-Sicherheit für industrielle Automatisierungssysteme Teil 2-2 IACS-Sicherheitsprogramm-Einstufungen (IEC 65/797/CD:2020); Text Deutsch und Englisch Ausgabedatum: 2021-05, 2021.
- [DIN\_EN\_IEC\_62443-2-4] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-2-4:2024-11 VDE 0802-2-4:2024-11: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern für industrielle Automatisierungssysteme (IEC 62443-2-4:2023); Deutsche Fassung EN IEC 62443-2-4:2024, 2024. URL: <https://www.dinmedia.de/de/norm/din-en-iec-62443-2-4/380674327>.
- [DIN\_EN\_IEC\_62443-3-2] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-3-2:2021-12 VDE 0802-3-2:2021-12: IT-Sicherheit für industrielle Automatisierungssysteme - Teil 3-2: Sicherheitsrisikobeurteilung und Systemgestaltung (IEC 62443-3-2:2020); Deutsche Fassung EN IEC 62443-3-2:2020, 2021.
- [DIN\_EN\_IEC\_62443-3-3] DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, DIN EN IEC 62443-3-3:2020-01 VDE 0802-3-3:2020-01: Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme - Teil 3-3: Systemanforderungen zur IT-Sicherheit und Security-Level (IEC 62443-3-3:2013 + COR1:2014); Deutsche Fassung EN IEC 62443-3-3:2019 + AC:2019, 2020. URL: <https://www.dinmedia.de/de/norm/din-en-iec-62443-3-3/311519620>.
- [DIN\_EN\_IEC\_62443-4-1] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN Deutsches Institut für Normung e. V, DIN EN IEC 62443-4-1 (VDE 0802-4-1): IT -Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung (IEC 62443-4-1 2018);

Deutsche Fassung EN IEC 62443-4-1 2018. Beuth Verlag, Berlin, 2018. URL: <https://www.dinmedia.de/de/norm/din-en-iec-62443-4-1/292194568>.

- [DIN\_EN\_IEC\_62443-4-2] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE, DIN EN IEC 62443-4-2 (VDE 0802-4-2): IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS) (IEC 62443-4-2:2019); Deutsche Fassung EN IEC 62443-4-2:2019, 2019. URL: <https://www.dinmedia.de/de/norm/din-en-iec-62443-4-2/312858287>.
- [DIN\_EN\_ISO/IEC\_27001] DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), DIN EN ISO/IEC 27001:2024: Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023, 2024. URL: <https://www.dinmedia.de/de/norm/din-en-iso-iec-27001/370680635>.
- [DKE2024] DKE-Deutsche Kommission Elektrotechnik, Elektronik Informationstechnik DIN und VDE: IEC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung. URL: <https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung>.
- [EHR2023] Ehrlich, Marco; Bröring, Andre; Diedrich, Christian; Jasperneite, Jürgen; Kastner, Wolfgang; Trsek, Henning: Determining the Target Security Level for Automated Security Risk Assessments: 2023 IEEE 21st International Conference on Industrial Informatics (INDIN). IEEE, 2023 - 2023; S. 1–6.
- [FUH2016] Fuhr, David et al.: Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau. URL: <https://www.plattform-i40.de/IP/Redaktion/DE/Downloads/Publikation/vdma-security-automation.html>.
- [GAR2021] Gartner Inc.: Gartner Glossary Information Technology. URL: <https://www.gartner.com/en/information-technology/glossary>.
- [IEC\_62443-1-1] International Electrotechnical Commission, IEC/TS 62443-1-1:2009: Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, 2009. URL: <https://webstore.iec.ch/publication/7029>.
- [IEC\_62443-2-1] International Electrotechnical Commission, IEC 62443-2-1:2024: Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners, 2024. URL: <https://www.vde-verlag.de/iec-normen/254227/iec-62443-2-1-2024.html>.
- [IEC\_62443-2-2] IEC- International Electrotechnical Commission, IEC 62443-2-2:2025: Security for industrial automation and control systems – Part 2-2: IACS security protection scheme, 2025. URL: <https://www.vde-verlag.de/iec-normen/254909/iec-pas-62443-2-2-2025.html>.
- [IEC\_62443-2-3] IEC- International Electrotechnical Commission, IEC TR 62443-2-3:2015: Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment, 2015. URL: [https://webstore.iec.ch/preview/info\\_iec62443-2-3%7Bed1.0%7Den.pdf](https://webstore.iec.ch/preview/info_iec62443-2-3%7Bed1.0%7Den.pdf).
- [IEC\_62443-6-1] IEC- International Electrotechnical Commission, IEC TS 62443-6-1:2024: Security for industrial automation and control systems - Part 6-1: Security evaluation methodology for IEC 62443-2-4, 2024. URL: <https://www.vde-verlag.de/iec-normen/252700/iec-ts-62443-6-1-2024.html>.
- [IEC\_62443-6-2] IEC- International Electrotechnical Commission, IEC TS 62443-6-2:2025: Security for industrial automation and control systems - Part 6-2: Security evaluation methodology for IEC 62443-4-2, 2025. URL: <https://www.vde-verlag.de/iec-normen/254715/iec-ts-62443-6-2-2025.html>.

- [IEC\_TR\_62443-2-3] IEC- International Electrotechnical Commission, IEC TR 62443-2-3:2015: Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment, 2015. URL: <https://webstore.iec.ch/en/publication/22811>.
- [ISA2024] ISA - The International Society of Automation: The Case for ISA/IEC 62443 Security Level 2 as a Minimum for COTS Components. URL: <https://www.isasecure.org/hubfs/The-Case-for-ISA-IEC-62443-Security-Level-2-as-a-Minimum-FINAL.pdf>.
- [MIT2023] Mitre Corporation: MITRE ATT&C ICS Matrix. URL: <https://attack.mitre.org/matrices/ics/>.
- [NAM2017] NAMUR AK 4.18 Automation Security: Härtung von Computersystemen. URL: [https://www.namur.net/fileadmin/media\\_www/Dokumente/AK-PRAXIS\\_4.18\\_Haertung\\_2017-09-11.pdf](https://www.namur.net/fileadmin/media_www/Dokumente/AK-PRAXIS_4.18_Haertung_2017-09-11.pdf).
- [NIE2021] Niemann, Karl-Heinz: Abgrenzung der IT-Sicherheitsnormenreihen ISO 27000 und IEC 62443 - Eine Sicht auf automatisierungstechnische Anlagen der Fertigungs- und Prozessindustrie. URL: <https://doi.org/10.25968/opus-1973>.
- [NIS-2\_de]: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). NIS-2-Richtlinie: Amtsblatt der Europäischen Union, 2022.
- [NIST\_SP\_800-82] National Institute of Standards and Technology (NIST), SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security, 2023. URL: <https://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-82r3.pdf>.
- [PNO2019] PROFIBUS Nutzerorganisation e.V.: Security Erweiterungen für PROFINET. PI White Paper für PROFINET. URL: <https://www.profinet.com/download/pi-white-paper-security-extensions-for-profinet/>, 07.09.2019.
- [PUL2025] Puls, Jan-Niklas; Niemann, Karl-Heinz: Härtung in der industriellen IT: Schutzmaßnahme gegen Cyberangriffe. In Zukunft.Digital - Zeitschrift des Mittelstand Digitalzentrums Hannover, Ausgabe 01/2025, 2025; S. 20–22. URL: [https://digitalzentrum-hannover.de/wp-content/uploads/2025/06/MDZH\\_Magazin\\_25-01\\_web\\_25-06-16.pdf](https://digitalzentrum-hannover.de/wp-content/uploads/2025/06/MDZH_Magazin_25-01_web_25-06-16.pdf).
- [TRE2022] Trend Micro Inc.: The State of Industrial Cybersecurity. 2022 industrial cybersecurity survey report in manufacturing, electric utilities, oil, and gas. URL: [https://www.trend-micro.com/en\\_us/research/22/f/state-of-ot-security-2022.html](https://www.trend-micro.com/en_us/research/22/f/state-of-ot-security-2022.html).
- [VDI\_2182\_1] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik (GMA), VDI/VDE 2182 Blatt 1: Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Beuth Verlag, Berlin, 2020. URL: <https://www.dinmedia.de/de/technische-regel/vdi-vde-2182-blatt-1/314114388>.
- [ZOR2025] Zorlu, Nurullah: Bestandsaufnahme zur Härtung von Automatisierungssystemen im Sinne der OT-Security. Bachelor Thesis. URL: <https://doi.org/10.25968/opus-3581>.

**ABB AG**

Contact:

<https://access.motion.abb.com/contact/contact>

Homepage:

[www.abb.com/plc](http://www.abb.com/plc)

—

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of ABB AG.  
Copyright© 2025 ABB. All rights reserved.