Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

ICS-Security-Kompendium

Version 2.0.0

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0.0	2013	Erste Veröffentlichung
2.0.0	2024	Aktualisierung

Tabelle 1 Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63

53133 Bonn

Tel.: +49 22899 9582-0

E-Mail: ics-sec@bsi.bund.de

Internet: https://www.bsi.bund.de/ics

Inhalt

1 Einleitung

Die Digitalisierung hat in den letzten Jahrzehnten nicht nur die Arbeit in den Büros verändert. Auch Automatisierungslösungen und das Steuern technischer Prozesse wurden zunehmend digitalisiert. Dies betrifft letztlich alle Bereiche von sogenannten Industrial Control Systems (ICS; deutsch: industrielle Steuerungssysteme, Automatisierungssysteme). Dazu zählen neben Produktionsanlagen aller Art beispielhaft auch die Gebäudeautomation, Verkehrsleitsysteme, Energieerzeugung und -verteilung.

Um der großen Einsatzbreite der Komponenten Rechnung zu tragen, wird im weiteren Verlauf allgemein von Operational Technology (OT) gesprochen. Dies dient der Abgrenzung zur klassischen IT mit den Büro- und Rechenzentrumsumgebungen. Gleichzeitig liegt der Fokus nicht nur auf der Fabrikautomation oder Prozesssteuerung, die mit dem Begriff ICS verbunden ist.

1.1 Motivation

OT war in der Vergangenheit physisch von anderen IT-Systemen und Netzen entkoppelt (engl. air gap). Der Grund lag im Wesentlichen darin, dass keine zentralen IT-Systeme vorhanden waren, welche die OT mit der klassischen IT verbunden haben. Damit war die OT weitgehend vor äußeren Einflüssen durch andere Informationstechnik geschützt. Ein rein physischer Zugangsschutz war ausreichend.

Mit der Digitalisierung nahmen die Verbindungen zwischen IT und OT zu. Das Ziel ist die Qualität und Produktivität zu erhöhen. Dies erforderte eine zunehmende Vernetzung der OT und der IT.

Bereits 2013 war die Motivation für das ICS-Security-Kompendium des BSI, auf die zusätzlichen Gefährdungen und damit einhergehenden Risiken hinzuweisen und Lösungswege aufzuzeigen. Die Anzahl erfolgreicher Angriffe steigt stetig. Nicht zuletzt ist Ransomware für eine Vielzahl von Betriebs- und Produktionsunterbrechungen verantwortlich. Dies zeigt, dass Gefährdungen durch Ransomware und Cyberangriffe real sind und Organisationen sich auch mit Cybersicherheit in der OT beschäftigen müssen.

Das vergangene Jahrzehnt ist in Bezug auf Cybersicherheit in der OT von Licht und Schatten geprägt. Erfreulich ist, dass in einer Vielzahl von Organisationen die Cybersicherheit nun fester Bestandteil der Organisationskultur in der IT ist. Im Schatten stehen jedoch viele Organisationen, die sich noch nicht oder nur unzureichend damit beschäftigt haben. Dieser Gruppe soll das Dokument helfen, ihre OT zu schützen.

1.2 Ziele

Vor diesem Hintergrund hat das ICS-Security-Kompendium folgende Ziele:

- Das Kompendium ist ein Grundlagenwerk für die Cybersicherheit in der OT. Es ermöglicht sowohl Cybersicherheits- als auch ICS-Experten den einfachen Zugang zur Cybersicherheit für die OT. Es erläutert das notwendig Basiswissen der Cybersicherheit und der Abläufe und Spezifika in der OT.
- Es werden Grundlagen geschaffen, um definierte Prozesse zu etablieren und erste Maßnahmen umzusetzen. Eine Auswahl von Maßnahmen wird beschrieben.
- Es werden Bezüge zu Standards und Normen zur Cybersicherheit hergestellt, um Anknüpfungspunkte für das vertiefte Bearbeiten der Themen zu ermöglichen.
- Es gibt eine Übersicht relevanter Gesetze, Normen und Standards.
- Eine Methodik zur Auditierung von OT wird beschrieben.

Das ICS-Security-Kompendium bildet einen allgemeinen Rahmen für die verschiedenen Anwendungsbereiche der OT. Ein solches Grundlagenwerk kann natürlich nicht auf alle Spezifika der unterschiedlichen Industriesektoren detailliert eingehen. Es gibt dazu vom BSI mit dem IT-Grundschutz und weiteren Publikationen spezifische Vertiefungen. Gleiches gilt für weiterführende Publikationen von Verbänden.

Die Durchführung einer wiederkehrenden (regelmäßigen bzw. anlassbezogenen) Risikoanalyse wird als notwendig angesehen. Im Rahmen der Risikoanalyse sind dann insbesondere die in Kapitel 3 dargestellten Gefährdungen zu untersuchen und zu bewerten. Anschließend liegt es in der Verantwortung der Organisation, geeignete Sicherheitsmaßnahmen abzuleiten, welche die durch die identifizierten Gefährdungen gegebenen Risiken auf ein akzeptables Restrisiko reduzieren. Eine Hilfestellung können dabei die in Kapitel 6 Good-Practices zum Schutz der OT dargestellten Good-Practices liefern.

Dabei gilt es zusätzlich, die Umsetzbarkeit mit Blick auf die jeweiligen Rahmenbedingungen zu bewerten und ggf. alternative Sicherheitsmaßnahmen zu definieren.

1.3 Adressatenkreis

Das Kompendium richtet sich an Organisationen, die OT-Komponenten herstellen (im folgenden Hersteller), OT-Komponenten zu einer Anlage oder Maschine integrieren (im folgenden Integratoren) und Anlagen und Maschinen betreiben (im folgenden Betreiber). Dabei liegt der Fokus auf Organisationen und deren Mitarbeitenden, die beginnen sich mit der Thematik Cybersicherheit zu befassen. Es werden Grundlagen vermittelt, die den Weg zu etablierten Standards bereiten sollen.

1.4 Inhalte

Kapitel 2 Grundlagen von ICS gibt eine Einführung in die Grundlagen von OT. Es richtet sich an IT-Security-Experten (aus der klassischen Unternehmens-IT), die bisher nicht oder nur wenig mit OT und deren Komponenten in Berührung gekommen sind.

In Kapitel 3 Schwachstellen und Cyberangriffe in der OT werden die cybersicherheitsspezifischen Grundlagen erläutert. Diese bieten einen Zugang zur Cybersicherheit. Neben der allgemeinen Einführung in Schwachstellen und Angriffsvektoren erfolgt eine Erläuterung der Besonderheiten von ICS, die an ICS-Anwender und Cybersicherheitsexperten gleichermaßen gerichtet ist.

Kapitel 4 Organisationen, Verbände und deren Standards gibt einen Überblick über nationale und internationale Organisationen und deren Standards und Quasi-Standards im Bereich der Cybersicherheit in der OT. Es soll alle Leser dabei unterstützen, die vorhandenen Veröffentlichungen einzuordnen.

Kapitel 5 Funktionale Sicherheit vermittelt Grundlagen zur funktionalen Sicherheit und zeigt einen Weg Cybersicherheit und Funktionaler Sicherheit gemeinsam zu betrachten.

Kapitel 6 Good-Practices zum Schutz der OT definiert architektonische, technische und organisatorische Maßnahmen zum Schutz von ICS. Zudem erfolgt eine Gegenüberstellung der Good-Practices zu etablierten Standards. Die Best-Practices adressieren in erster Linie Betreiber von ICS.

Aufbauend auf den zuvor beschriebenen Maßnahmen wird in Kapitel 7 Audits, Assessments und Tests eine Methodik für die Durchführung von Audits in ICS beschrieben.

2 Grundlagen von ICS und OT

Dieses Kapitel gibt eine Einführung in die Grundlagen der ICS. Nach der Erläuterung der Anwendungsgebiete erfolgt eine Beschreibung derzeit typischer Architekturen. Die auf diesen Architekturen aufsetzende Nutzung von ICS-Komponenten sowie die genutzten Kommunikationstechniken werden umrissen. Grundlage der Beschreibungen bildet dabei die herstellerunabhängige, gängige Praxis aus Betreiber-, Integrator- und Komponentenherstellersicht. Mit Rücksicht auf die Vielzahl unterschiedlicher Anwendungen von ICS erfolgt hier eine Betrachtung mit Fokus auf die Cybersicherheit in der OT. Anwendungsspezifische Details werden daher nur generisch angesprochen.

2.1 Glossar

Die Begriffe für Komponenten und Funktionen im Bereich der Automatisierungstechnik werden im Bereich der internationalen Normung umfassend definiert (siehe z. B. (1)). Mit Rücksicht auf die in unterschiedlichen Branchen gebräuchliche Nomenklatur wird im Folgenden eine Gegenüberstellung für die gängigen Begriffe geliefert.

Oft werden deutsche Begriffe synonym mit englischen Begriffen verwendet, die allerdings nicht zwangsweise dieselbe Bedeutung haben. Eine gewisse Bezeichnungsunschärfe ist deshalb leider nicht zu vermeiden.

Aktor

> Ein Aktor, auch Aktuator genannt, wandelt eine Stellgröße in eine elektrische, hydraulische oder pneumatische Aktion um.

Prozessleitsystem (PLS)

> Prozessleitsysteme werden meist für größere verfahrenstechnische Anlagen eingesetzt. Sie können eine Vielzahl von Merkmalen wie Alarmsysteme, Anlagen- und Prozessvisualisierung, Benutzerverwaltung, zentrale Datenhaltung sowie Wartungs- und Entwicklungswerkzeuge aufweisen.

Engineering Workstation (EWS)

> Engineering Workstations, Engineering Stations (ES) sowie Service Rechner ermöglichen die Konfiguration und Programmierung von ICS-Komponenten.

Funktionale Sicherheit

> Funktionale Sicherheit (engl.: functional safety) bezeichnet die Fähigkeit eines elektrischen, elektronischen, programmierbar elektronischen Systems (E/E-System), beim Auftreten systematischer Ausfälle (z. B. fehlerhafte Systemauslegung) sowie zufälliger Hardwareausfälle (z. B. Alterung von Bauteilen) mit gefahrbringender Wirkung, einen wohl definierten sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu verharren.

Factory Acceptance Testing (FAT)

> Werksabnahme einer Anlage

Human Machine Interface (HMI)

> Diese Komponenten stellen Anzeige- und Bedienfunktionen zur Verfügung. Funktional können sie Standard-Bedienbilder, freie Grafiken, Rezepterstellungs- und Beobachtungswerkzeuge, Alarmbehandlung, Datenarchivierung und Auswertung, Systemdiagnosen und -dokumentation (technischer Systeme und Produktionsprozesse) sowie interaktive Betriebsunterstützung beinhalten.

Industrial Control System (ICS)

Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse. Ein industrielles Steuerungssystem ist eine integrierte Hard- und Software-Lösung zur Automatisierung, dazu gehören Sensoren, Aktoren und deren Vernetzung, sowie Verfahren zur Auswertung und Steuerung von vorwiegend industriellen Prozessen. Durch kontinuierliches Messen und Steuern werden Abläufe für den Betrieb von Maschinen automatisiert. (2)

Manufacturing Execution System (MES)

Ein Manufacturing Execution System ist ein Informationssystem, welches komplexe Fertigungssysteme und ihre Datenflüsse verbindet, überwacht und steuert. MES wird typischerweise zur effektiven Steuerung und Optimierung der Produktionsprozesse und Systeme eingesetzt.

Manufacturing Service Bus (MSB)

Eine homogene, dienstbasierte Integrationsschicht, welche eine universelle Schnittstelle für unterschiedliche cyberphysische Produktionssysteme und digitale Werkzeuge zur Verfügung stellt.

Master Terminal Unit (MTU)

Die MTU stellt gesammelte Informationen über ein Human Machine Interface dem Operator zur Verfügung und überträgt Steuersignale zu entfernten Einheiten wie Sub-MTUs, Remote Terminal Units oder direkt zu Speicherprogrammierbaren Steuerungen. Häufig kommen SCADA-Server als MTUs zum Einsatz.

Operation Technology (OT)

Betriebstechnik ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert. (3)

Remote Terminal Unit (RTU)

Automatisierungstechnische Komponente zur Erfassung und ggf. Verarbeitung von Prozessinformationen und Übertragung der Informationen an eine übergeordnete Master Terminal Unit.

Routing

Hier im Kontext der diskreten Fertigung: Individuelle und variable Abfolge einzelner Produktionsschritte und Stationen

Process Analytical Technology (PAT)

Die PAT dient der Optimierung, Analyse und Kontrolle von Herstellungsprozessen hauptsächlich in der chemischen Industrie.

Site Acceptance Testing (SAT)

Prüfung der installierten Anlage vor Ort als Teil der Abnahme.

Safety Instrumented Function (SIF)

Eine SIF ist eine Funktion, welche durch ein System der Funktionalen Sicherheit (siehe SIS) implementiert wird und für den Erhalt oder das Erreichen eines definierten Sicherheitslevels (siehe SIL) verantwortlich ist.

Safety Integrity Level (SIL)

Definieren 4 Stufen (SIL 1 bis SIL 4) von Anforderungen an System der Funktionalen Sicherheit. Je höher der SIL, umso geringer ist die Wahrscheinlichkeit, dass die geforderte Sicherheitsfunktion nicht ausführt wird. Hierbei werden keine Aussagen zur Cybersicherheit getroffen.

Safety Instrumented System (SIS)

System zur Gewährleistung der Funktionalen Sicherheit einer Anlage. Hauptkomponenten sind Sensoren zum Beispiel zur Druckmessung, eine Steuereinheit (siehe PLC oder SPS), welche die Überwachungslogik implementiert, sowie den zu steuernden Aktoren wie zum Beispiel den Ventilen.

Die von SIS-Systemen ausgeführten Sicherheitsfunktionen, die Safety Instrumented Functions (siehe SIF), reduzieren die Risiken unter die Akzeptanzschwelle.

Software Bill of Materials (SBOM)

Eine Software Bill of Materials (deutsch: Software-Stückliste / -Teileliste) ist eine maschinell verarbeitbare Datei, die Details und Lieferkettenverhältnisse der in einer Software genutzten Komponenten enthält. Sie unterstützt die automatisierte Verarbeitung von Informationen zu Software-Komponenten, sowohl der sogenannten „Primärkomponente“ (englisch: Primary Component) als auch der von ihr eingebundenen (Dritt-)Komponenten. Weitere Informationen zum Inhalt und Aufbau einer SBOM sind in der TR-03183 (4) beschrieben.

Supervisory Control and Data Acquisition (SCADA)

SCADA beschreibt das Steuern und Überwachen technischer Prozesse mittels eines Computersystems. Dabei bezieht sich der Terminus gewöhnlich auf Systeme mit dezentraler Datenbasis (im Gegensatz zu PLS). Bei SCADA-Lösungen werden die automatisierten Funktionen durch RTU oder SPS realisiert, während ein Computersystem für Bedienung, Archivierung und Auswertung des Prozessgeschehens verwendet wird.

Sensor

Sensoren nehmen eine Erfassung physikalischer Größen und deren Wandlung in ein Einheitssignal (etwa 4-20mA, 0-10VDC) vor. Es existiert eine Vielzahl von Komponenten, welche zu dieser Klasse gehören: (Grenz-)Taster, (End-)Schalter oder Messwertaufnehmer. Die zum Einsatz kommenden Kommunikationsprotokolle werden als Feldbusse bezeichnet.

Site Integration Testing (SIT)

Integrationstest der installierten Anlage vor Ort.

2.2 Grundcharakteristika

ICS werden überall dort eingesetzt, wo Abläufe automatisiert werden. Sie werden für das Messen, Steuern, Regeln und Bedienen von meist industriellen Abläufen benutzt.

Beispiele hierfür sind

- Verfahrens- und Prozesstechnik, in chemischen Anlagen oder in Ver- und Entsorgungsnetzen (z. B. Strom, Wasser, Gas, Fernwärme),
- diskrete Fertigungsautomatisierung oder
- Betriebstechnik z. B. im Schienen- und Straßenverkehr oder Gebäudeautomation. Die individuellen Anforderungen an ICS werden unmittelbar durch die betrieblichen Anforderungen bestimmt.

Neben typischen IT-Systemen wie Server, Notebooks oder Workstations mit in der IT gebräuchlichen Betriebssystemen, zum Beispiel für die Darstellung von interaktiven Dashboards oder Datenbankanwendungen, existieren eine Vielzahl von spezifischen Gerätetypen für die Steuerung von OT-Prozessen. Einige Beispiele hierfür sind:

- Speicherprogrammierbare Steuerung (SPS)
- HMI wie z. B. berührungssensitiver Bildschirm (Touchscreen) für die Maschinensteuerung

- Remote Sensor- und Schalteinheit bzw. engl. Remote Terminal Units (RTU)
- Protokollwandler (z. B. Seriell zu Ethernet)
- Steuergerät für die Bewegungskontrolle oder engl. Motion Control Unit
- Sensoren und Aktoren im Allgemeinen

Diese Gerätetypen basieren meist auf proprietärer Hard- und Software, welche auf Zuverlässigkeit und Langlebigkeit, in teilweise rauen Produktionsumgebungen, ausgelegt ist. Allerdings ist in diesem Bereich ein Trend zu erkennen, proprietäre Technologie teilweise durch Standard IT-Technik zu ersetzen oder sie zu virtualisieren. Ein Beispiel sind etwa SPS auf Basis des IT-Betriebssystems Linux.

In ICS werden aber in absehbarer Zeit weiterhin die oben erwähnten, nicht-IT Gerätetypen zum Einsatz kommen. Daher ist ein Grundverständnis dieser Technologien für eine erfolgreiche Cyberabwehr notwendig.

ICS werden in der Regel vertikal und horizontal integriert.

2.2.1 Vertikale Integration

Innerhalb der Wertschöpfungskette eines Betriebes gibt es zwischen dem Produktionsauftrag und der materiellen Produktion einen Geschäftsprozess, in dessen Rahmen

- Produktionsführung (in welchem Betrieb wird ein Produktionsauftrag abgewickelt),
- Betriebsführung (sind die für die Abwicklung eines Produktionsauftrages notwendigen Ressourcen verfügbar) und
- Prozessführung (befinden sich die technischen Parameter des Produktionsprozesses im richtigen Bereich)

bearbeitet werden. Nach Abschluss eines Produktionsauftrages wird ein entsprechender Produktionsbericht erstellt und archiviert. Die Details dieses Geschäftsprozesses können sich aufgrund individueller Anforderungen stark unterscheiden.

Die Pfeile in Abbildung 1 stellen die mit dem beschriebenen Vorgängen verbundenen Kommunikationsvorgänge dar.

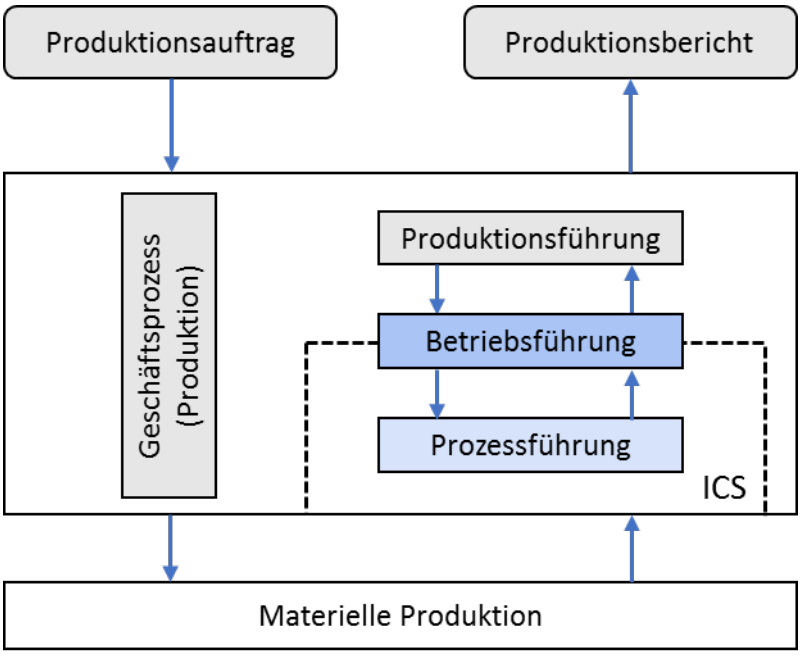

Abbildung 1 Vertikale Integration von Produktionsanlagen

2.2.2 Horizontale Integration

Oft bestehen Produktionsprozesse aus mehrstufig gegliederten Produktionsschritten. In vielen dieser Produktionsschritte sind ICS anzutreffen. Mit Rücksicht auf eine effiziente Produktion und die Einhaltung der qualitätsrelevanten Vorschriften ist zwischen den Produktionseinrichtungen (Anlagen, Lager usw.) ein Informationsaustausch erforderlich. Dieser Informationsaustausch kann in unterschiedlicher Weise erfolgen. Im Folgenden wird der Fokus jedoch auf Kommunikation im Sinne eines elektronischen Datenaustauschs gelegt.

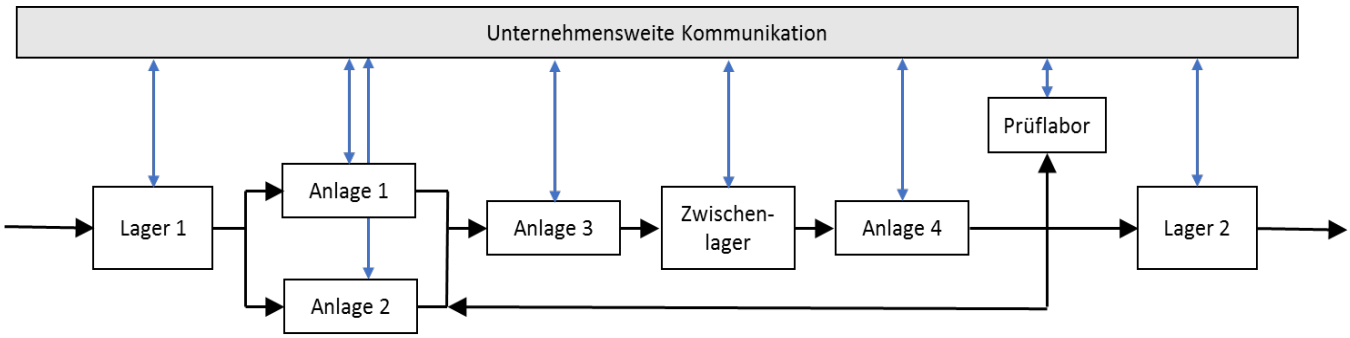

Abbildung 2 Horizontale Integration von Produktionsanlagen

Diese Struktur ist dem unternehmerischen Streben nach Qualität und Effizienz geschuldet. Sie liefert gleichzeitig den Rahmen für die technische Umsetzung des Geschäftsprozesses. Zudem dient die starre, direkte Anbindung an den jeweiligen materiellen Produktionsprozess der direkten Überwachung, Bedienung, Kontrolle von physischen Prozessen, Ereignissen, Geräten (Aktoren, Sensoren).

Dies beeinflusst die Prioritäten der Schutzziele und die Umsetzbarkeit von Maßnahmen. Bei einem Ausfall einer Anlage kann dies weitere Anlagen beeinflussen. Daher ist die Verfügbarkeit entsprechend hoch zu priorisieren. Dies wiederum hat Einfluss auf mögliche Strategien zur Aktualisierung, bei denen ein Stillstand der Anlage erforderlich ist. Deshalb können im Bereich der Office IT gebräuchliche Strategien nicht immer ohne Weiteres umgesetzt werden (vgl. Kap. 2.2.8).

2.2.3 Lebenszyklus

Der Lebenszyklus von ICS wird aus dem der zugehörigen Produktionsanlagen abgeleitet. Dieser ist deutlich länger als die in der Office IT typischerweise anzutreffenden Zeiträume. Die Laufzeit beträgt 10 bis 15 Jahre. Mitunter können es auch deutlich über 20 Jahre sein. In der Office-IT sind es meist nur 3 bis 5 Jahre.

2.2.4 Echtzeitverhalten

Steuerungen in industriellen Anlagen werden im Hinblick auf ihr Zeitverhalten optimiert. Kommt es aufgrund von (temporären) Modifikationen im Bereich der Software zu Änderungen am Zeitverhalten des ICS, führt dies zu Störungen im materiellen Produktionsprozess. Dies kann dazu führen, dass z. B. mehr Ausschuss anfällt.

2.2.5 Funktionale Sicherheit

Ziel der Funktionalen Sicherheit ist es Menschen oder die Umwelt vor Fehlfunktionen zu schützen, die zu Verletzungen oder Umweltschäden führen könnten. Hierzu werden oftmals Sensoren verwendet, wie zum Beispiel Annäherungssensoren oder Laserscanner, die einen abgesteckten Bereich absichern, die die Annäherung einer Person detektieren können. Diese Sicherheitsfunktionen (SIF) werden in der Regel durch spezielle sicherheitsgerichtete Speicherprogrammierbare Steuerungen (SSPS) implementiert, für die besondere Normen (bspw. (5)) gelten und die auf Grund ihrer Funktion, auch im Kontext der Cybersicherheit, besonders schützenwert sind.

Oft ist die Anlagensicherheit an behördliche Auflagen gebunden. In diesen Fällen bedürfen wesentliche Änderungen, worunter auch Softwareänderungen an den eingesetzten ICS fallen können, eines dedizierten

Genehmigungsprozesses. Aufgrund des vorgeschriebenen Prüfprozesses sind hier beispielsweise die Möglichkeiten zum zeitnahen Einspielen von Sicherheitsupdates begrenzt bzw. nicht gegeben.

Das Thema Funktionale Sicherheit wird ausführlich im Kapitel 5 behandelt.

2.2.6 Physikalische Trennung

In einigen Bereichen der ICS bestehen erhöhte Anforderungen an Steuerungskomponenten und ihre Kommunikation bezüglich hoher Verfügbarkeit, deterministischem Antwortverhalten, sehr geringer Latenzen, Validierbarkeit (etwa im pharmazeutischen Bereich). Beispiele hierfür sind die Bewegungssteuerung eines Roboters oder Steuergeräte im Kontext der Funktionalen Sicherheit.

In diesen Bereichen ist es üblich, neben logischer Trennung einzelner Teilbereiche auch eine physikalische Trennung von Funktionseinheiten – speziell im Bereich der Infrastruktur – umzusetzen.

Beispiel: Im Bereich der Office-IT ist es üblich, verschiedene logische Netzwerke auf einem Switch zu betreiben. In der Betriebsleitungsebene wird dies ebenfalls bereits häufiger eingesetzt. Auf Feld-, Prozessteuerungs- und Prozessleitebene ist dies, mit Rücksicht auf mögliche ungewollte Querverbindungen und deren potenzielle Auswirkung, ungebräuchlich. Werden unterschiedliche Netzwerksegmente trotzdem zusammengefasst, so ist dies im Rahmen einer Risikobewertung zu betrachten, welche auch die Cyberrisiken beinhaltet, die durch eine Kopplung von IT- mit OT-Komponenten entstehen können. Die Auswirkungen auf die Systemintegrität und Aspekte wie z. B. die Validierbarkeit eines ICS sind in diesen Fällen zu bewerten und zu dokumentieren.

Als Schutzmaßnahme gegen Cyberangriffe wurden speziell ältere Anlagen eine Zeit lang physikalisch von anderen Netzen getrennt. Dies gilt insbesondere für solche, in denen Systeme mit bekannten Schwachstellen enthalten sind oder eine unzureichende Zugangskontrolle bieten. Diese so genannten „Air-Gaps“ bieten jedoch selten das angestrebte Schutzniveau gegen Cyberangriffe. Denn in vielen Fällen ist weiterhin ein Datenaustausch notwendig oder erwünscht. Die hierfür eingesetzten Daten können von Angreifern genutzt werden, um die Trennung zu überwinden.

2.2.7 Software

Im Gegensatz zur Office IT werden ICS über längere Zeiträume mit quasi gleicher Anwendersoftware betrieben. Änderungen finden im Rahmen von Wartungstätigkeiten wie z. B. Austausch von Komponenten statt.

2.2.8 Updates

Im Bereich der Office IT werden Systeme nach Bekanntwerden von Fehlern oder Schwachstellen im Idealfall schnellstmöglich (durch die Installation von Patches) nachgebessert. Ein kurzzeitiger Ausfall (z. B. aufgrund eines Neustarts) ist vielfach kein Problem, da dies durch Redundanzen ausgeglichen oder der Zeitraum tolerabel ist.

In ICS gibt es Anwendungsbereiche, wie beispielsweise chemische Prozesse oder kontinuierliche Prozesse (z. B. in einem Kraftwerk), bei denen auch kurzzeitige Ausfälle nicht akzeptabel sind. In diesen Fällen ist ein Update nur in langfristig abgestimmten Wartungsfenstern möglich.

Eine weitere Herausforderung ist die Prüfung der Updates. Eine Testinfrastruktur mit einer vollständigen Nachbildung des ICS ist ebenfalls nicht überall vorhanden. Eine komplette Nachbildung eines Automatisierungssystems mit mehreren hundert Sensoren und Aktoren für Tests können sich die wenigsten Organisationen leisten. In diesen Fällen ist ein Test vor dem Update nicht möglich. Anders sieht es im Fall von einzelnen Maschinen aus. Hier kann der Hersteller entsprechende Prüfungen durchführen und mögliche Auswirkungen eines Updates auf beispielsweise Funktion oder Reaktionszeiten austesten.

Zudem können aufgrund regulatorischer Vorgaben (z. B. im Bereich der Pharmaproduktion) anwendungsspezifische Prüfungen existieren, deren Bearbeitung eine Produktionsunterbrechung erzwingt.

2.2.9 Hardware

Im Gegensatz zur Office IT werden ICS über längere Zeiträume mit gleicher Hardware (z. B. Gerätetypen) betrieben. Dies kann über die lange Lebenszeit zu Problemen bei den Ressourcen führen. Ein Beispiel sind kryptografische Funktionen zum Verschlüsseln. Die Migration auf neuere Verfahren bei alten Geräten würde die Verarbeitungs- und Reaktionsgeschwindigkeit verringern, was für die Funktion nicht tragbar wäre.

Bei neu geplant und implementierten Anlagen finden Virtualisierungstechniken vermehrt Anwendung (siehe auch Kapitel 2.3.11).

2.3 Gliederung von ICS

Die hierarchischen Modelle der Gliederung von ICS haben sich von flachen Strukturen über hierarchische Enterprise Architekturmodelle wie das Purdue-Modell (6) hin zu Standards wie ISA-95/ IEC 62264 entwickelt. Die Digitalisierung und Trends rund um Industrie 4.0 verändern die Strukturen von ICS. Mit den Veränderungen in Richtung serviceorientierter Produktion (7) beginnen sich die klassischen Hierarchien aufzulösen. Dies betrifft insbesondere die Kommunikation zwischen und über die unterschiedlichen Ebenen der Hierarchien.

2.3.1 Hierarchische ICS-Strukturen

Die Funktionen der einzelnen Hierarchieebenen werden häufig in Form einer Automatisierungspyramide dargestellt:

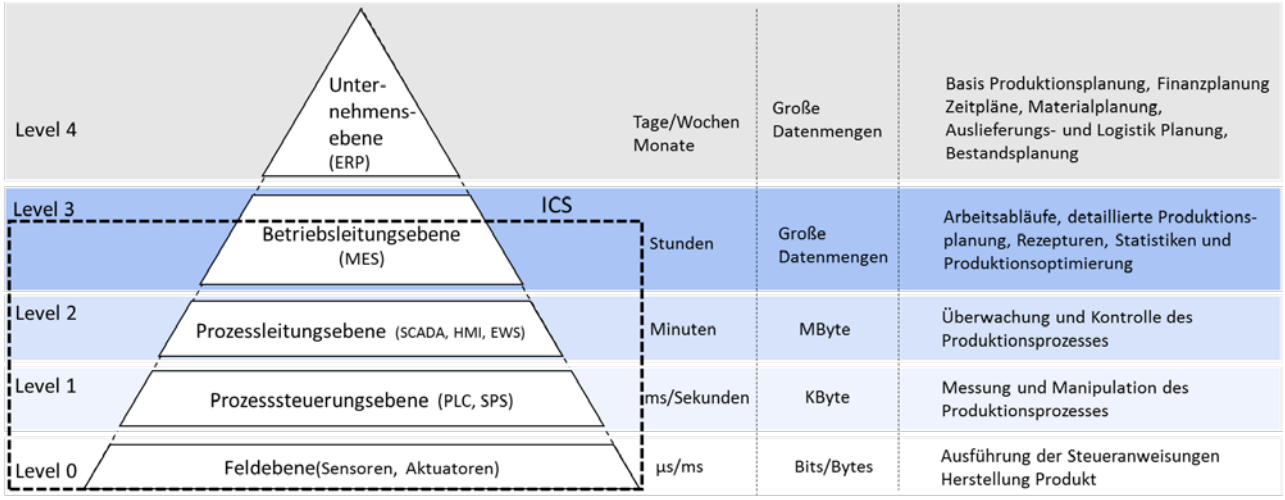

Abbildung 3 Hierarchische Ebenen der Produktionspyramide (8)

Das Modell umfasst 5 Ebenen. Auf der obersten Ebene findet, typischerweise unter Nutzung eines ERP-Systems, die Grobplanung der Produktion statt. Diese unterstützen weitere Organisationsbereiche, wie beispielsweise den Vertrieb bei der Erfassung von Kundenaufträgen und den Einkauf bei der Bestellung von Materialien. Auf der Ebene darunter (Ebene 3) findet eine detailliertere Planung und Steuerung der Produktion statt. Hier kommen vermehrt Manufacturing Execution Systems (MES) an den jeweiligen Produktionsstandorten zum Einsatz. Ebene 3 stellt die Schnittstelle zwischen der betriebswirtschaftlich orientierten Organisationsebene und den operativen Produktionssystemen dar. Die Überwachung findet auf der Prozessleitebene statt. Hier kommen Supervisory Control and Data Acquisition (SCADA)-Systeme und Prozessleitsysteme (PLS) für die Produktionsdatenerfassung und -kontrolle zum Einsatz. Diese ermöglichen zum Beispiel die Anzeige und das Auswerten von Betriebsdaten. Auf der Steuerungsebene übernehmen SPS die Steuerung der Maschinen. Auch wenn die Funktion einer SPS mittlerweile virtualisiert werden kann, benötigt die Steuerung eine Hardwarekomponente, welche mit der Prozessebene verbunden ist und mit Hilfe einer Programmlogik Daten und Signale verarbeitet und ausgibt. Die Feldebene stellt die

Schnittstelle zum Produktionsprozess dar. Die Eingangsdaten der Sensoren werden in Echtzeit verarbeitet und entsprechende Aktuatoren möglichst verzögerungsfrei angesteuert.

Die hieraus resultierende, typischerweise durch den Geschäftsprozess vorgegebene Hierarchie eines ICS, gestaltet sich wie folgt:

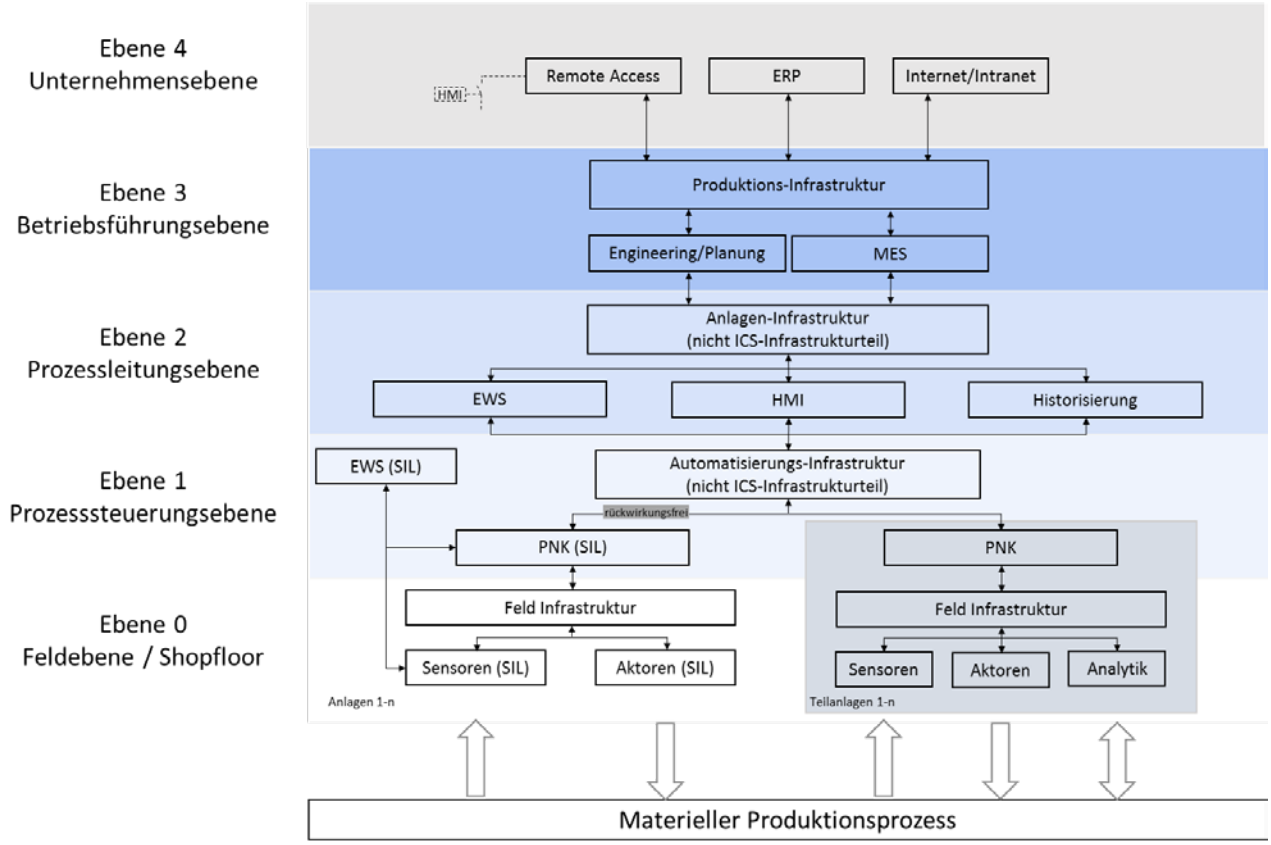

Abbildung 4 Hierarchische Gliederung eines ICS

2.3.2 Ebene 0: Feldebene / Shopfloor

Auf dieser Ebene befinden sich die Komponenten, welche zur Gewinnung von Informationen aus dem Bereich der materiellen Produktion erforderlich sind, bzw. die Einflüsse auf das Geschehen im Bereich der materiellen Produktion nehmen (Endschalter, Messwertaufnehmer, Analysegeräte, Ventile, Stellglieder, Motoren usw.). Diese Komponenten interagieren einerseits direkt mit dem materiellen Produktionsprozess und andererseits, unter Zuhilfenahme ihrer zugehörigen Infrastruktur, mit den zugehörigen informationsverarbeitenden Einheiten oder ggf. auch untereinander (z. B. bei Umsetzung von CIF-Strategien). Die zugehörige Infrastruktur kann je nach Anwendung und eingesetzter Technologie verschiedene Komponenten enthalten. Beispielhaft seien an dieser Stelle genannt:

- Remote Input/Output (ggf. mit Signalvorverarbeitung),
- Interface-Bausteine zur Signalkonditionierung,
- Switches bei Verwendung von Feldbus Lösungen.

Die Prozessdatensignalübertragungen im Ebene 0 erfolgen in Echtzeit. Eine Störung der Signalübertragung führt, sofern keine physikalische (z. B. 2 von 3 Verschaltung bei Messwertaufnehmern) oder logische (z. B. Ersatzwertaufschaltung bei Messwertstörung) Redundanz vorhanden ist, zu einer unmittelbaren Störung im materiellen Produktionsprozess.

Bei der Verwendung von Feldbussen oder Geräten besteht teilweise zusätzlich die Möglichkeit, Diagnose- und Konfigurationsdaten zu übermitteln. Ein Beispiel ist das Protokoll HART (Highway Addressable Remote

Transducer Protocol). Dies ermöglicht zusätzlich zu einem analogen 4-20mA Signal, digitale Daten zu übertragen.

2.3.3 Ebene 1: Steuerungsebene

In dieser Ebene befinden sich die Komponenten, welche zur Signalverarbeitung im Sinne der Darstellung der automatisierten Funktionen erforderlich sind (z. B. Endlage erreicht: Antriebsmotor AUS oder Füllstand HOCH: Pumpe AUS). Diese Komponenten werden typischerweise in Abhängigkeit der zu automatisierenden Teilanlage ausgelegt. Je nach Hersteller und Größe der Anlage unterscheidet sich die Anzahl an Steuerungskomponenten und die Art der Verbindungen untereinander.

Die technische Ausgestaltung ist sehr stark von der gewählten konzeptionellen Lösung abhängig.

Prinzipiell sind 3 Varianten anzutreffen:

1. Die Informationen aus der Feldebene werden ohne Vorverarbeitung eingelesen und verarbeitet; Stellbefehle werden direkt an die Aktoren übermittelt. So erfolgt z. B. die Überwachung der Stellungsrückmeldungen eines Ventils hinsichtlich:
   - des statischen Zustands wie AUF/ZU dürfen nicht gleichzeitig anstehen und
   - des logischen Ablaufs wie innerhalb 1 Sekunde nach Ansteuerung muss die Rückmeldung ZU anstehen.
2. Es erfolgt im Feld eine Signalvorverarbeitung (z. B. die Laufzeitüberwachung eines Ventils), die Ebene 1 Komponente erhält lediglich die resultierenden Informationen wie z. B. das Ventil ist auf und hat eine Laufzeitstörung.
3. Automatisierungsfunktionen, wie z. B. Regelungen, werden in Feldgeräten wie z. B. Stellungsreglern an Regelventilen implementiert. Die zugehörigen Ist-Werte werden von den entsprechenden Messwertaufnehmern direkt (z. B. per Feldbus) an den Stellungsregler gesendet.

Die Verarbeitung dieser Informationen erfolgt deterministisch, d. h. für eine ordnungsgemäße Gesamtfunktion muss eine vordefinierte Reaktionszeit sichergestellt werden. Ein nicht Einhalten dieser Anforderung führt zu einer unmittelbaren Störung im materiellen Produktionsprozess.

Eine Sonderstellung im Bereich der Ebene 0 und Ebene 1 Anwendungen nehmen die Systeme zur funktionalen Sicherheit (siehe auch Kapitel 5) ein. In Abhängigkeit von der branchenspezifischen Anwendung werden an diese Systeme Zusatzanforderungen bis hin zur physikalischen Abtrennung der Systeme (vgl. (9)) gestellt.

Eine besondere Betrachtung ist außerdem für Komponenten erforderlich, bei deren Betrieb spezifische Qualitätsanforderungen zur erfüllen sind, wie beispielsweise GMP (Good Manufacturing Practice) oder GAMP (Good Automation Practice) Anforderungen im Bereich Chemie und Pharma. In diesen Fällen sind ggf. spezifische Risikoanalysen durchzuführen und zu dokumentieren.

2.3.4 Ebene 2: Prozessleitungsebene

In Ebene 2 sind die Einrichtungen angesiedelt, die für die Prozessführung notwendig sind, die jedoch keine Daten in Echtzeit verarbeiten. Beispiele sind HMI, produktbezogene Engineering- und Wartungsstationen, Messwert- und Prozessdatenarchivserver.

Diese Komponenten sind für die Prozessführung wichtig, ihr Verhalten ist jedoch sowohl hinsichtlich des Zeitverhaltens als häufig auch bezüglich ihrer Verfügbarkeit weniger kritisch als dass der Ebene 0 und 1 Komponenten. Ein Ausfall einer Bedienstation beeinträchtigt häufig nicht sofort den Produktionsprozess, da im ersten Moment nur das Überwachen eingeschränkt ist.

Ebene 2 Komponenten werden bzgl. Softwareupdates restriktiv behandelt. Denn die Interaktion der Ebene 2 Komponenten unter einander und den anderen Ebenen ist für eine ordnungsgemäße Führung des

materiellen Produktionsprozesses zwingend erforderlich. Ein potenzieller Fehler beim Aktualisieren der eingesetzten Software alle Ebene 2 Komponenten gleichzeitig betreffen kann.

2.3.5 Ebene 3: Betriebsführungsebene

Die auf Ebene 3 angesiedelten Komponenten übernehmen die Funktionen der Betriebsführung. Diese lassen sich typischerweise in folgende Kategorien gliedern:

- MES
  Die MES bilden in der Betriebsführung den Datentransfer zwischen Automatisierungstechnik einerseits und betriebswirtschaftlicher Datenverarbeitung andererseits ab. Dieser Datentransfer beinhaltet neben den eigentlichen Kommunikationsvorgängen auch ein Aggregieren der Daten. Dies ist notwendig, da die Einrichtungen auf Ebene 2 die Prozessdaten in Sekundenintervallen verarbeiten, während auf Ebene 3 eine Datenverarbeitung in wesentlich größeren Zeitintervallen erfolgt (z. B. tageweise).
- Engineering/Planung
  Auf Ebene 3 sind systemunabhängige Engineering- und Planungswerkzeuge angesiedelt. Diese sind notwendig, um technische Dokumentationen zu erstellen und zu pflegen (z. B. Schaltpläne, Bauzeichnungen, Prozessbeschreibungen).

2.3.6 Ebene 4: Unternehmensebene

Auf Ebene 4 sind die Softwarelösungen angesiedelt, mit deren Hilfe die umfassende Betriebsorganisation unterstützt wird. Typischerweise werden auf Ebene 4 folgende Funktionen angesiedelt:

- ERP-Anbindung
  Über diesen Weg werden Produktionsaufträge und Produktionsberichte übermittelt. Im Normalfall kommuniziert das ERP mit dem MES (Ebene 3).
- Internet/Intranet Zugang
  Kommunikation in das Internet aus der Produktion ist beispielsweise für die kontinuierliche Überwachung oder Übermittlung von Statusinformationen notwendig. Gerade auch, wenn es sich um abgesetzte Standorte handelt. Die Netzübergänge sind entsprechend zu sichern.
- Remote Access Einrichtungen
  Zu Wartungszwecken werden häufig spezifische Zugänge verwendet. Diese benutzen technologisch in der Regel das Internet (wobei auch Telefonverbindungen wie Internetverbindungen anzusehen sind). Diese Verbindungen unterscheiden sich von den vorgenannten Verbindungen dadurch, dass sie normalerweise nicht permanent benötigt werden.

2.3.7 Ausnahmen

Ungeachtet der hier beschriebenen hierarchischen Struktur gibt es Anwendungen, in denen die hier postulierte Hierarchie nicht umgesetzt werden kann (siehe auch 2.3.13).

Beispielhaft seien Geräte genannt, welche Signalverarbeitung, Beobachtung, Bedienung und Anschaltung des materiellen Produktionsprozesses in einem Gerät vereinigen. Projiziert man diese Funktionen auf das hier beschriebene hierarchische Modell, sind diese Geräte somit in den Ebenen 0 bis 2 angesiedelt. In der Praxis werden diese Geräte, sofern sie z. B. Verpackungsmaschinen steuern, üblicherweise auf Ebene 1 in das ICS eingebunden. Steuern sie hingegen autonome Systeme, z. B. im Bereich kleinerer Anwendungen, werden diese Systeme als eigenständige ICS betrieben.

Ein weiteres Beispiel sind spezifische Qualitätsmessungen. Dort werden relevante Sensoren direkt an Systeme auf Ebene 2 angeschaltet und Ebene 1 wird umgangen. Je nach Anforderung werden für diese Anwendungen entweder logisch oder physikalisch separierte Netzwerke aufgebaut (siehe auch Kapitel 2.2.6).

2.3.8 Diskrete Fertigung vs. Prozessfertigung

Die diskrete Fertigung beschreibt den Herstellungsprozess einzelner Artikel, die aus verschiedenen Einzelteilen bestehen und montiert werden müssen. Diskret gefertigte Produkte können meist wieder demontiert werden. Bei der Prozessfertigung werden Stoffe z. B. in einem chemischen Prozess in einen anderen umgewandelt. Eine Umkehrung ist hierbei häufig nicht möglich.

Der diskrete Fertigungsprozess eines Endproduktes kann unter Umständen eine hohe Komplexität erreichen, weil viele Teilkomponenten vor der Endmontage in eigenen, verteilten diskreten Herstellungsprozessen gefertigt werden müssen, einzelne Komponenten kundenindividuell anpassbar sind und bestimmte Herstellungs- und Montage-Reihenfolgen (Routing) voneinander abhängig sind. Bei der diskreten Fertigung spielen daher Stücklisten oder zum Beispiel ERP-Systeme eine zentrale Rolle.

In der Prozessfertigung wird nochmal zwischen Batchprozessen und kontinuierlichen Prozessen unterschieden. In Batchprozessen werden einzelne Chargen nacheinander produziert. Dies beinhaltet Befüllen von Reaktoren, die Reaktion der Ausgangsstoffe zum Produkt, dem Entleeren und Vorbereiten des Reaktors für die nächste Charge. Dem gegenüber laufen in kontinuierlichen Prozessen die Reaktionen ohne Unterbrechung ab.

In der folgenden Tabelle 2 sind einige typische Merkmale der diskreten Fertigung im Vergleich zur Prozessfertigung aufgeführt:

Tabelle 2 Vergleich der diskreten Fertigung zur Prozessfertigung

Diskrete Fertigung	***Prozessfertigung***
Einheiten: Einzelne Artikel, Stückzahlen	Einheiten: Produktchargen, Volumen, kWh
Standardkomponenten	Variable Inhaltsstoffe
Montage „umkehrbar“	Herstellung nicht „umkehrbar“
Stücklisten	Formeln, Rezepte
Variable Abfolge der Montageschritte	Mischen, Generieren
Typischerweise Auftragsfertigung	Typischerweise Lagerfertigung
Typische Branchen: Maschinenbau, Automobilhersteller und -Zulieferer, Werkzeugbau, Geräte, Elektronik, Nutzfahrzeuge, Industrieroboter, Telekommunikationsequipment, Bekleidungsindustrie usw.	Typische Branchen: Chemie, Pharmaka, Öl & Gas, Wasser/Abwasser, Strom, Lebensmittelverarbeitung, Farbe und Beschichtungen, Stahl, Aluminium, Kosmetik, Textilien, Kunststoffe usw.

2.3.9 Prozessleitsystem vs. SCADA

Die in dem voran gegangenen Abschnitt vorgestellten Automatisierungsfunktionen können prinzipiell sowohl mit Prozessleitsystemen (PLS) als auch mit sog. SCADA-Systemen verwirklicht werden.

Mit PLS werden verfahrenstechnische Anlagen automatisiert. Wesentliche Aufgabe eines Prozessleitsystems ist die logische Verknüpfung und die abstrakte Darstellung des Prozesses in einem System, welches den Prozess nach verfahrenstechnischen Vorgaben steuert. (10)

PLS sind dadurch gekennzeichnet, dass sie über eine zentrale Datenhaltung für alle Parameter verfügen. Alle Komponenten eines Prozessleitsystems greifen auf diese Daten zu. Die für den Betrieb des Prozessleitsystems notwendigen Kommunikationsvorgänge werden automatisch nach Maßgabe der individuellen Konfiguration etabliert, ohne dass der Anwender sich darum kümmern muss. Das Engineering für PLS erfolgt von zentraler Stelle unter Verwendung eines integrierten Engineering-Werkzeuges.

SCADA-Systeme sind typischerweise heterogen aufgebaut. Sie bestehen oft aus unterschiedlichen Komponenten, zwischen denen es üblicherweise keine vorkonfigurierten Kommunikationskanäle gibt. Alle

für die Verwirklichung einer Automatisierungsaufgabe notwendigen Kommunikationsvorgänge müssen individuell geplant und konfiguriert werden. Für das Engineering der einzelnen Komponenten sind u. U. verschiedene Engineering-Werkzeuge erforderlich. Bei Automatisierungslösungen kann bezüglich der Komplexität bei der Ausführung grob zwischen 3 Leistungsstufen unterschieden werden:

- Kombinationen aus Speicherprogrammierbaren Steuerungen und SCADA-System zur Visualisierung (Bedienen und Beobachten),
- offene, frei am Markt erhältliche SCADA-Systeme in Kombination mit entsprechenden branchenspezifischen Bibliotheken,
- herstellergebundene, nicht frei am Markt erhältliche SCADA-Systeme mit herstellergebundenen Bibliotheken.

Aus Sicht des Anlagenbetreibers können mit beiden Lösungen gleichwertige Applikationen realisiert werden. Die für die Erstellung einer bestimmten Lösung oder Durchführung einer Prozessanpassung notwendigen Arbeiten können sich unter Umständen deutlich unterscheiden. So sind zum Beispiel für die Generierung eines neuen Alarms durch ein SCADA System typischerweise mehrere einzelne Konfigurationsschritte durchzuführen, während das gleiche Ergebnis über die zentralen Engineering-Werkzeuge eines PLS in wenigen Schritten erreicht werden kann. Diesem Vorteil bzgl. des Bedienungskomforts steht ein bei gleichem Anlagenumfang u.U. deutlich höherer Einstandspreis des PLS gegenüber und ggf. eine Herstellerbindung.

2.3.10 IT-/OT Konvergenz

IT-/OT-Konvergenz bezeichnet die Integration von Systemen der Informationstechnologie (IT) zur Überwachung und Steuerung von Ereignissen, physischen Prozessen und Geräten der Betriebstechnologie (OT, Operational Technology). Dabei findet eine zunehmende Nutzung von Standard IT-Technologien, Plattformen und Konzepten in der Produktion statt, sowie eine zunehmende Vernetzung der Bereiche miteinander.

In „maschinennahen“ Bereichen (Ebene 1 und 0, siehe Kapitel 2.3) wurden in der Vergangenheit meist proprietäre Hard- und Software oder Netzwerkkomponenten eingesetzt. Hier sind mittlerweile Technologien wie Linux basierte SPS, Tablets als HMIs, TCP/IP basierte Netzwerkkommunikation und Virtualisierungssoftware im Einsatz.

Aus Cybersicherheitssicht sind diese Komponenten somit auch den Gefährdungen der jeweiligen IT-Technologie ausgesetzt. Die Verwendung von IT-Technik ermöglicht es aber auch, die etablierten Cybersicherheitsmaßnahmen in diesem Bereich (11) zu nutzen.

Gleichzeitig werden die Bereiche stärker miteinander verbunden. Produktionsplanungssysteme sowie Datensammlung werden integriert. Der verstärkte Datentransfer ermöglicht Optimierungen und neue Produktionsmöglichkeiten. Gleichzeitig steigen Abhängigkeiten zwischen den Systemen, was mögliche Beeinträchtigungen bei einem Ausfall erhöht. Außerdem ermöglicht es Schadsoftware und Angreifern, sich zwischen den Bereichen auszubreiten.

2.3.11 Virtualisierung

Aus Gründen der Flexibilität, Skalierbarkeit, Verfügbarkeit, kosteneffizienter Bereitstellung und zeitnaher Wiederherstellung (etwa im Nachgang eines Cyberangriffs), werden Komponenten von ICS zunehmend virtualisiert oder ehemalige Hardwareelemente wie zum Beispiel SPS-Steuerungssysteme und -Funktionen als Software implementiert. Typische Elemente oder Funktionen sind virtuelle HMIs, SCADA-Server aber auch Steuerungssysteme. Als Virtualisierungstechnik werden neben proprietärer Software auch Hypervisor oder Containersoftware verwendet. Die Virtualisierungssoftware stellt neben ihrem Nutzen einen zusätzlichen Angriffsvektor dar und muss entsprechend abgesichert werden.

2.3.12 Cloud und Edge Integration

Eine verbesserte Transparenz, die Möglichkeit der zeitnahen Datenanalyse zur Optimierung oder Vermeidung von Ausfallzeiten und die resultierende, gesteigerte Effektivität führen unter anderem zu einer zunehmenden Auslagerung von ICS-Funktionen hin zu sogenannten Edge- oder Cloud Plattformen. Hierzu gehören das Speichern oder Laden von SPS-Konfigurationen, das Sammeln von Datenpunkten von Steuerungskomponenten, Digitalen Zwillingen einzelner Komponenten oder ganzer Anlagen, Cloud Management Konsolen, Web-Technologie basierten HMI-Anzeigen bis hin zu Steuerungsaufgaben mit toleranterem Antwortverhalten.

Ein weiterer Treiber für die vermehrte Cloud-Nutzung einiger ICS Funktionen, speziell für Betriebe, bei denen in der Produktion IT-Ressourcen wie Personal und Knowhow knapp sind, ist das Auslagern des Plattformbetriebs (wie z. B. Patchen, Sichern, Wiederherstellung, Leistungsüberwachung, Plattformerweiterungen, usw.) der für ICS notwendigen IT-Komponenten sowie eine im allgemeinen ortsunabhängige Verfügbarkeit (z. B. über webbasierte Anwendungen im Internet) für Personal und Partner.

Das Auslagern von Daten und Funktionen bringt nicht nur die beschriebenen Vorteile. Es ist zu beachten, dass die Daten nicht mehr auf den eigenen Systemen gespeichert sind. Dies ist beim Beurteilen der Cybersicherheit zu berücksichtigen. Zudem gilt es mögliche Abhängigkeiten von den Cloudanbietern zu berücksichtigen. Dies gilt vor dem Hintergrund, dass solche Dienste auch eingestellt werden können.

2.3.13 Service orientierte Produktion

Moderne Produktionsanlagen und -prozesse haben Schlüsselaufgaben in den Bereichen Produktionsplanung bis hin zur Maschinensteuerung digitalisiert. Sie nutzen Technologien wie smarte Sensoren, standardisierte, drahtlose und offene Kommunikation und Protokolle, Big-Data Analysemodelle und -Methoden inklusive maschinellem Lernen und Künstlicher Intelligenz Ansätzen so wie dezentraler Netzwerk- und IT-Infrastruktur inklusive virtualisierter Komponenten wie etwa Steuer- und Kontrollsysteme.

Die Service orientierte Produktion setzt auf einer Architektur auf, die durch Nutzung von Service orientierten Technologien flexible Produktionssysteme implementiert, welche maßgeschneiderte Produkte auch in geringen Losgrößen ermöglicht. Der hierbei entstehende, gesteigerte Bedarf in Bezug auf Interoperabilität und Datenaustausch, so wie die einhergehende vernetzte Kommunikation brechen die klassischen und strikten Schichtmodelle der Produktionspyramide (siehe Kapitel 2.3) auf. Vertikale und horizontale Integration werden, mit Hilfe von zum Teil öffentlich zugänglichen Softwareschnittstellen (APIs), über die Standorts- oder Organisationsgrenze hin erweitert.

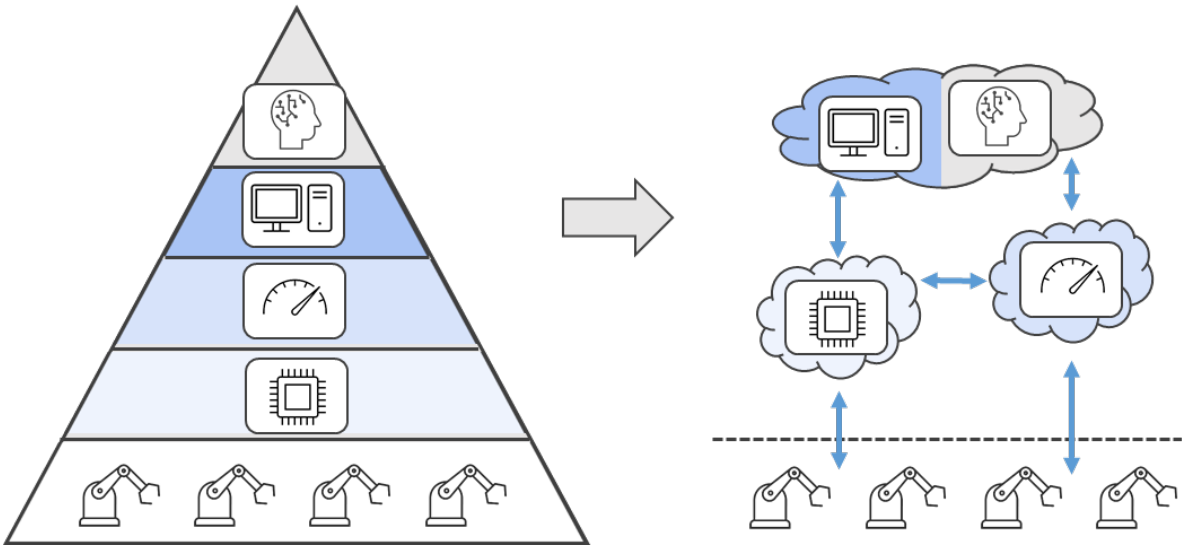

Abbildung 5 Architekturwandel im Kontext der Service orientierten Produktion

Dabei werden Hardwareschnittstellen durch Integrationstechnologien über zum Beispiel einen Manufacturing Service Bus (MSB) an ein in der Cloud betriebenes MES angeschlossen. Dieser Ansatz wurde in verschiedenen Modellen weiterentwickelt, wird aber aufgrund seines Umfangs hier nicht weiter im Detail behandelt. Die Flexibilität und Effizienz einer serviceorientierten Produktion macht zusätzliche Schutzmaßnahmen im Bereich Cloud-, Netzwerk- und Applikationssicherheit erforderlich. Denn sie führt wegen

- externer Kommunikation,
- exponierten APIs,
- ausgelagerten Daten,
- komplexen Vertrauensstellungen,
- sicheren Identitäten oder
- der Verfügbarkeit von Produktionsdaten

zu einer vergrößerten Angriffsfläche. Abbildung 5 visualisiert diesen Wandel von der bisherigen hierarchischen Kommunikationsstruktur hin zu einem mehr oder weniger beliebigem Netz.

2.4 Kommunikationsvorgänge

Die für den Betrieb von ICS erforderlichen Kommunikationsvorgänge können mit vielen verschiedenen technologischen Lösungen realisiert werden. Darüber hinaus sind diese Technologien einem intensiven Entwicklungsprozess unterworfen. Aus diesem Grund werden im Folgenden wesentliche technische Anforderungen und keine individuellen Lösungen betrachtet. Basis der Betrachtung ist die Systemdarstellung gem. Abbildung 3 und Abbildung 4. Als Unterscheidungskriterium wird die Ebene, auf der ein Kommunikationsvorgang stattfindet, verwendet. Zunächst werden Kommunikationsvorgänge innerhalb der individuellen Ebene betrachtet.

2.4.1 Kommunikationsvorgänge auf Ebene 0

Grundsätzlich besteht für die Kommunikation auf Ebene 0 die Notwendigkeit, Daten von Sensoren und Befehle an Aktoren unter Einhaltung deterministischer Bedingungen zu übertragen. Zusätzlich müssen im Anforderungsfall Diagnose- und Konfigurationsdaten übermittelt werden. Die Kommunikation in dieser Ebene ist geprägt von kleinen Datenmengen (einzelne Signalwerte oder Steuerwerte), die in zum Teil mit Verzögerungen im ms/µs-Bereich übertragen werden müssen. Die Einhaltung dieser Parameter ist für die Güte der Steuerung, zum Beispiel für die Bewegungskontrolle eines Roboterarms in der diskreten Fertigung, essenziell. Diese Anforderungen an Verfügbarkeit und Verzögerung erschweren die Implementierung von Standard-Cybersicherheitsmaßnahmen wie Verschlüsselung, Signieren zum Schutz der Integrität von Daten, Filterung über Gateways oder die Verwendung von Zertifikaten zur Authentisierung. Daher ist eine Risikoabwägung in Bezug auf die Schutzmaßnahmen notwendig. So ist es möglich, dass ein Verschlüsseln der Statusdaten für die Bewegungskontrolle nicht möglich ist, da dies die Latenz zu stark erhöhen würde. Aufgrund einer Risikobewertung könnte der Verzicht jedoch gerechtfertigt werden, weil ein Angreifer aus diesen keine relevanten Informationen gewinnen kann.

Grundsätzlich stehen 3 verschiedene Varianten zur Verfügung:

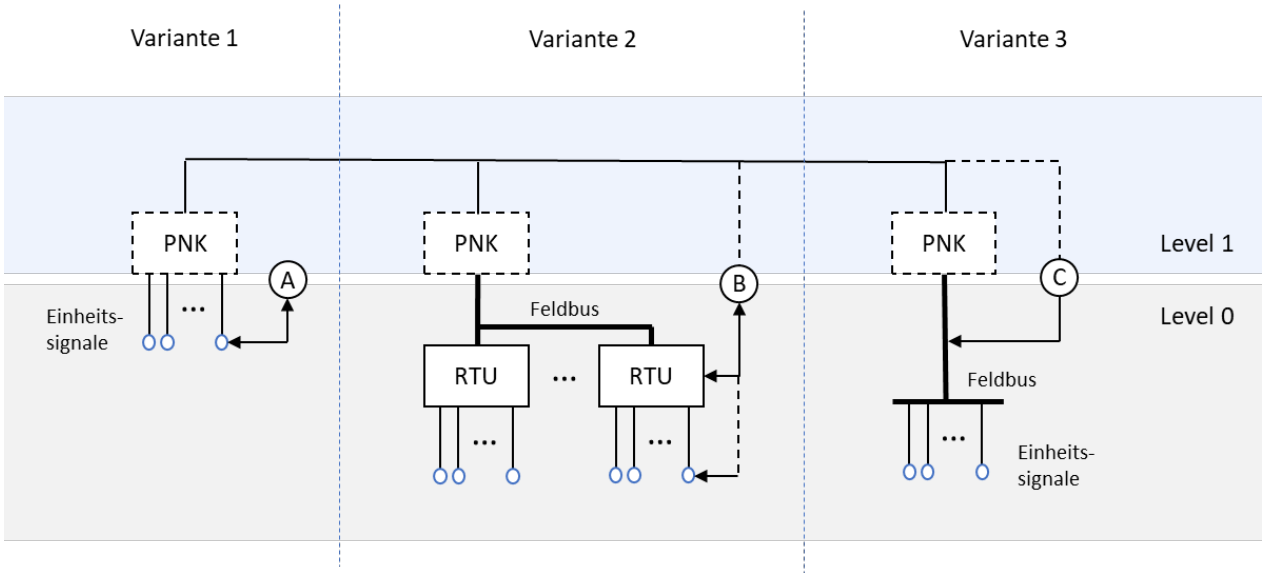

Abbildung 6 Anschaltung von Feldsignalen

Variante 1 (typisch für die diskrete Fertigung)

Die Feldgeräte werden unter Verwendung von Einheitssignalen im Rahmen einer Punkt-zu-Punkt Verdrahtung mit den PNK verbunden. Wartungsgeräte werden typisch gem. A angeschlossen.

Variante 2 (typisch für verteilte Prozessfertigung)

Die Feldgeräte werden unter Verwendung von Einheitssignalen mit den RTU verbunden, diese kommunizieren mittels Feldbus mit den zugehörigen PNK. Wartungsgeräte werden typisch gem. B angeschlossen, wobei der Anschluss der Feldgeräte möglicherweise an der RTU (z. B. bei Anwendungen in explosionsgefährdeten Bereichen) erfolgt.

Variante 3

Die Feldgeräte werden mittels Feldbus mit den PNK verbunden. Wartungsgeräte werden typisch gem. C angeschlossen, wobei der Anschluss möglicherweise an der PNK (z. B. bei Anwendungen in explosionsgefährdeten Bereichen) erfolgt. Im Bereich der Feldbusse existiert eine Vielzahl unterschiedlicher, standardisierter Kommunikationsprotokolle wie IEC 61158, siehe (12).

Beispiele für die diskrete Fertigung sind: Profibus DP, Profinet, ControlNet, SDS, DeviceNet, Ethernet/IP, EtherCat, Interbus, AS-Interface, CANopen. Beispiele für die Prozessautomation sind: Profibus-PA, Foundation Fieldbus H1, FF HSE, Profinet, Profibus DP. Bezüglich der Anforderungen an Feldbusse gibt es zwischen der diskreten Fertigung und der Prozessfertigung, je nach Einsatzgebiet, Unterschiede.

Tabelle 3 Typische Unterschiede zwischen Fertigungs- und Verfahrenstechnik

Diskrete Fertigung	*Prozessfertigung*
Verarbeitung von typischerweise einer Vielzahl von Binärsignalen	Verarbeitung von oftmals Analogsignalen
Kein zeitlicher Einfluss d. Konfigurationsarbeiten auf die Datenübertragung	Explosionsschutz
Schnelle Datenübertragung	Hohe Verfügbarkeit
	Energieübertragung per Buskabel

2.4.2 Kommunikationsvorgänge auf Ebene 1

Auf Ebene 1 eines ICS existieren sowohl Echtzeitverbindungen (z. B. zwischen den PNK) als auch Verbindungen, die nicht übertragungszeitkritisch sind (z. B. Engineering-Zugriffe). Es kommen deshalb

häufig Protokolle mit unterschiedlichen Stacks (z. B.Industrial Ethernet bei neuen Systemen) zum Einsatz. Typischerweise werden die Schichten 1, 2 und 7 des OSI-Schichtenmodells genutzt. Bei Prozessleitsystemen werden die Funktionen der Schicht 7 üblicherweise nicht offengelegt. Als Softwareschnittstellen kommen auch sehr alte und unsichere wie z. B. OPC (OLE for process control) neben neueren wie beispielsweise OPC UA (Unified Architecture) zum Einsatz. Mit Rücksicht auf die Konsequenzen eines Ausfalls der Ebene 2 Kommunikation finden sich hier häufig redundante Strukturen. Für die Kommunikation zwischen PNK, die besonderen Anforderungen genügen müssen, kommen zusätzlich spezifische Sicherungsverfahren zum Einsatz, die es erlauben, zufällige Übertragungsfehler an den Daten zu erkennen (z. B. CRC-Checksummen).

In einigen Fällen werden für die Kommunikation Übertragungsmedien und zugehörige Infrastruktur verwendet, die nicht exklusiver Bestandteil des ICS sind. Dabei werden Switche, Router und Lichtwellenleiter als Bestandteil eines Ebene-4-IT-Werksnetzes für die Ebene-1-Kommunikation (und ICS-Kommunikation im Allgemeinen) genutzt. In diesen Fällen ist eine gesonderte Betrachtung der aus dieser Architektur resultierenden Risiken erforderlich und sollte Bestandteil der Risikoanalyse sein. Beispiele hierfür sind: Change-Management-Abhängigkeiten, Segmentierung der Kommunikation, Patch-Management und tolerierbare Ausfallzeiten, sowie Redundanzen und Verfügbarkeiten.

Zunehmend kommen auch drahtlose Übertragungsprotokolle auf Ebene 1, wie beispielsweise WLAN gem. IEEE 802.11 zum Einsatz (siehe Kap. 2.4.7). Diese Lösungen sind jedoch mit Rücksicht auf die besonderen Anforderungen industrieller Umgebungen (z. B. EMV, Störungen durch Stahlkonstruktionen etc.), ungeachtet möglicher Cybersicherheitsrisiken, für diese Anwendungsbereiche gesondert zu evaluieren.

2.4.3 Kommunikationsvorgänge auf Ebene 2

Über die Ebene 2 einer ICS-Anwendung wird der Datentransfer zwischen dem eigentlichen ICS und den übergeordneten Funktionen bzw. Stationen abgewickelt. Ebene 2 bildet den äußeren Perimeter der eigentlichen ICS-Anwendung (ausgenommen Sonderfälle mit integrierter MES-Funktionalität). Die Datenübertragung erfolgt typischerweise unter Verwendung von Ethernet Technologie. Typischerweise kommen die Schichten 1, 2, 3, 4 und 7 des OSI-Schichtenmodells zur Anwendung.

Drahtlose Übertragungsprotokolle (siehe auch 2.4.7) kommen auf Ebene 2 zur Anwendung. Ein Beispiel sind mobile Wartungsgeräte, die sich mit ICS-Komponenten verbinden.

2.4.4 Kommunikationsvorgänge auf Ebene 3

Auf Ebene 3 kommt eine große Bandbreite an Kommunikationstechnologien zum Einsatz, welche teilweise auch in der IT-/Office Zone anzutreffen ist. Beispiele sind HTTP(S), (S)FTP, IPSec, DNS oder SMB-Kommunikation.

Die Systeme auf Ebene 3 werden bei vielen Anwendern von der IT-Abteilung des jeweiligen Anlagenbetreibers administriert. Hinsichtlich des Schutzbedarfs bestehen Anforderungen, wie im Bereich der Office-IT üblich. Für die Anwendungen auf Ebene 3 sind die typischen Cybersicherheitsstrategien aus dem Bereich der Office-IT anwendbar.

2.4.5 Kommunikationsvorgänge auf Ebene 4

Ebene 4 beinhaltet traditionell keine speziellen ICS-Funktionen. Je nach Implementierung und Anforderung kann aber zum Beispiel die Kommunikation bezüglich Fernzugriffen über Netzwerk- oder Proxy-Systeme in dieser Zone geleitet werden. In diesem Fall können dann ggf. Sicherheitsfunktionen der IT, wie etwa Inhaltsfilter oder eine erste Stufe der Benutzerauthentifizierung, hier implementiert sein.

Mit dem Aufkommen der Service-orientierten Produktion und der zunehmenden Nutzung von Cloudsystemen gewann Ebene 4 an Bedeutung für die OT-Kommunikation. Hier sind typischerweise die Cloud-Edge-Systeme der IT-Infrastruktur beheimatet. Diese übernehmen zunehmend Funktionen zur Analyse größerer Prozessdatenmengen für die Produktion.

2.4.6 Ebenenübergreifende Kommunikation

Die Kommunikation in ICS ist nicht auf die jeweilige Ebene beschränkt. So kann der Wert eines Positionsgebers eines Ventils auf Ebene 0 über eine SPS auf Ebene 1 an eine Software auf Ebene 2 übertragen werden. Kommt es hier zu Abweichungen, generiert die Software (z. B. Intelligent Device Management) auf Ebene 2 einen Alarm an ein Computerized Maintenance Management System (CMMS) auf Ebene 3, welches ein Ticket im ERP-System auf Ebene 4 öffnet.

Für die ebenenübergreifende Kommunikation kommen häufig Gateways zum Einsatz. Das Gateway (Ebene 1) wandelt Daten des I/O-Subsystems auf dem Feldbus (Ebene 0) in ein anderes Protokoll um und leitet diese an ein System auf Ebene 2 weiter.

Von dort wird die Kommunikation zu Ebene 3 und 4 jeweils durch eine Firewall gefiltert und über die DMZ geleitet. So können Daten zwischen "beliebigen" Systemen ausgetauscht werden, aber nicht jedes System muss mit jedem direkt kommunizieren. Das ERP-System benötigt zum Beispiel keine Sensordaten von I/O Systemen auf dem Feldbus.

2.4.7 Drahtlose Kommunikation

Drahtlose Kommunikation wird vermehrt im industriellen Umfeld eingesetzt. Dies gilt sowohl für die Feldebene und ihre Sensorsignale, für WLAN-Netze die von Augmented Reality-Brillen genutzt werden, für „Low-Energy" Weitverkehrsnetze etwa in der Wasserwirtschaft oder 5G Campus Netze, die mit fahrerlosen Transportsystemen kommunizieren. Hierbei ersetzt die Funktechnik einerseits ehemalige, kabelgebundene Kommunikation in ICS-Netzen, andererseits ist sie die Basis für moderne Produktionsmethoden wie mobile Werkzeuge, Assistenzsysteme und Roboter, die ohne drahtlose Kommunikation so nicht möglich wären.

Je nach Anwendung können die Anforderungen an Latenzzeiten, Reichweite, Verfügbarkeit, Fehlertoleranz, Explosionsschutz, Störfelder und nicht zuletzt an die Cybersicherheit sehr unterschiedlich sein (13).

Die verschiedenen drahtlosen Kommunikationsstandards unterstützen unterschiedliche Schutzmechanismen im Sinne der Cybersicherheit. Hierzu zählen Verschlüsselung, Integritätsprüfung oder die Authentisierung der Endpunkte. Die folgende Tabelle 4 gibt eine kurze Übersicht über die wichtigsten Eigenschaften einiger Standards:

Tabelle 4 Eigenschaften drahtloser Kommunikationsstandards

Standard	***Anwendung***	***Cybersicherheitsfunktionen***

WirelessHART
IEC 62591
	Überwachung von:
	• Medizinischen Geräten
	• Umgebungs- und Energie Management
	• Extremen Umweltbedingungen (Korrosion, Flut, etc.)
	• Rotationsgebern
		• 128 Bit AES-Verschlüsselung
		• Neuer Schlüssel für jede Nachricht
		• Authentifizierung von Geräten
		• Daten Integritätsprüfung
		• Rotierende Netzwerkschlüssel
		• Unterschiedliche Sicherheitslevel
		• Automatischer Kanalwechsel (Hopping)
		• Einstellbare Sendestärke
		• Logging für:
		  • Fehlgeschlagene Netzwerkanmeldungen
		  • Korrumpierte Nachrichten
		  • Authentisierungsfehler

Standard	*Anwendung*	*Cybersicherheitsfunktionen*
Trusted Wireless	• Analoge oder digitale Sensordaten • prozesstechnische Applikationen, wie Tanklager, Pipelines, Kläranlagen • als Kabelersatz für große Distanzen • Übertragung serieller Daten (RS232/RS485)	• Authentifizierung nach RFC 36104 • 128 Bit AES Verschlüsselung (Pre Shared Keys)
Bluetooth	• Analoge oder digitale Sensordaten • Übertragung serieller Daten (RS232/RS485) • Wireless Ethernet	• 128 Bit Verschlüsselung • Adaptives Frequenzhopping
ZigBee	• Überwachung Energieverbrauch • Prozessdatenerfassung • Gebäudeautomation und -Leittechnik • Sensoren mit geringer Baugröße	• 128 Bit AES Verschlüsselung • Rotation der Netzwerkschlüssel • „Checked In“ Geräteliste • Daten Integritätschecks • „Refresh Frames“ zur Überprüfung der Sequenz Integrität der Daten-Frames
LoRaWAN (Long Range Wide Area Network)	• Energiesparende IoT Kommunikation über große Distanzen • Geeignet für Batterie betriebene Geräte • Sensoren mit niedrigen Datenraten	• 128 Bit AES Verschlüsselung • Geräteauthentisierung (mittels DevEUI, AppEUI, AppKey) • Join Procedure Security (Beitrittskontrollen) • Message Integrity Checks • Frequenzhopping • Eindeutige Geräte ID (DevAddr) • Zusätzliche Sicherheitsmaßnahmen auf Anwendungsebene
Wifi	• Einsatz in Kontrollzentren und Feldebene für Datenerhebung, -Überwachung und Konfiguration • Datenerhebung, -Überwachung und Konfiguration in der Diskreten Fertigung	• WPA2 (Wi-Fi Protected Access 2) • WPA3 (Wi-Fi Protected Access 3)

Standard	*Anwendung*	*Cybersicherheitsfunktionen*
WiMax	• Breitbandige Weitverkehrsverbindungen • Internetverbindung • VoIP-Kommunikation auf dem Werksgelände	• Open System Authentication • Shared Key Authentication • 128 Bit AES Verschlüsselung
5G	• (Energie)optimierte Konnektivität zu einer sehr großen Anzahl von Endgeräten (Sensoren, Aktuatoren, Maschinen, etc.) mit hoher Bandbreite • Systeme mit hoher Zuverlässigkeit bei gleichzeitig geringer Latenz Grundsätzlich geeignet für Industrie 4.0	• Starke kryptografische Verfahren zur Absicherung der Funkstrecke • Authentisierung und Autorisierung • Sicheres Roaming • Absicherung der Signalisierung • Verschlüsselung der mobilen Identität (IMSI) • Network Slicing • Topology Hiding

Es ist anzumerken, dass die oben beschriebenen Cybersicherheitsfunktionen zwar in den einzelnen Standards spezifiziert werden, dies führt aber in der praktischen Implementierung nicht automatisch dazu, dass sie aktiviert oder vorhanden sind. Oft führen ein erheblich gesteigerter Energieverbrauch oder erhöhte Latenzzeiten zur Deaktivierung der Sicherheitsfunktionen.

2.5 OT-Architekturen

Obwohl das „Purdue Enterprise Reference Architecture“ (PERA) Modell, oder kurz Purdue Modell ursprünglich nicht unter Cybersicherheitsaspekten entworfen wurde und seine Bedeutung durch die in Kapitel 2.3.13 beschriebene „Auflösung“ der Hierarchiestufen diskutiert wird, bildet es derzeit immer noch die Basis vieler Netzwerk-Sicherheitskonzepte bezüglich Segmentierung, Zugriffskontrolle und Kommunikationsflüssen. So wird das Modell unter anderem vom dem für ICS-Sicherheit wichtigem Standard IEC 62443 genutzt.

Das Modell verwendet, in leichter Abwandlung der Produktionspyramide (siehe Abbildung 7), 6 Hierarchie Ebenen (da die DMZ im Pyramidenmodell nicht als eigene Ebene gezählt wird, siehe auch 2.4.5) und soll hier kurz skizziert werden.

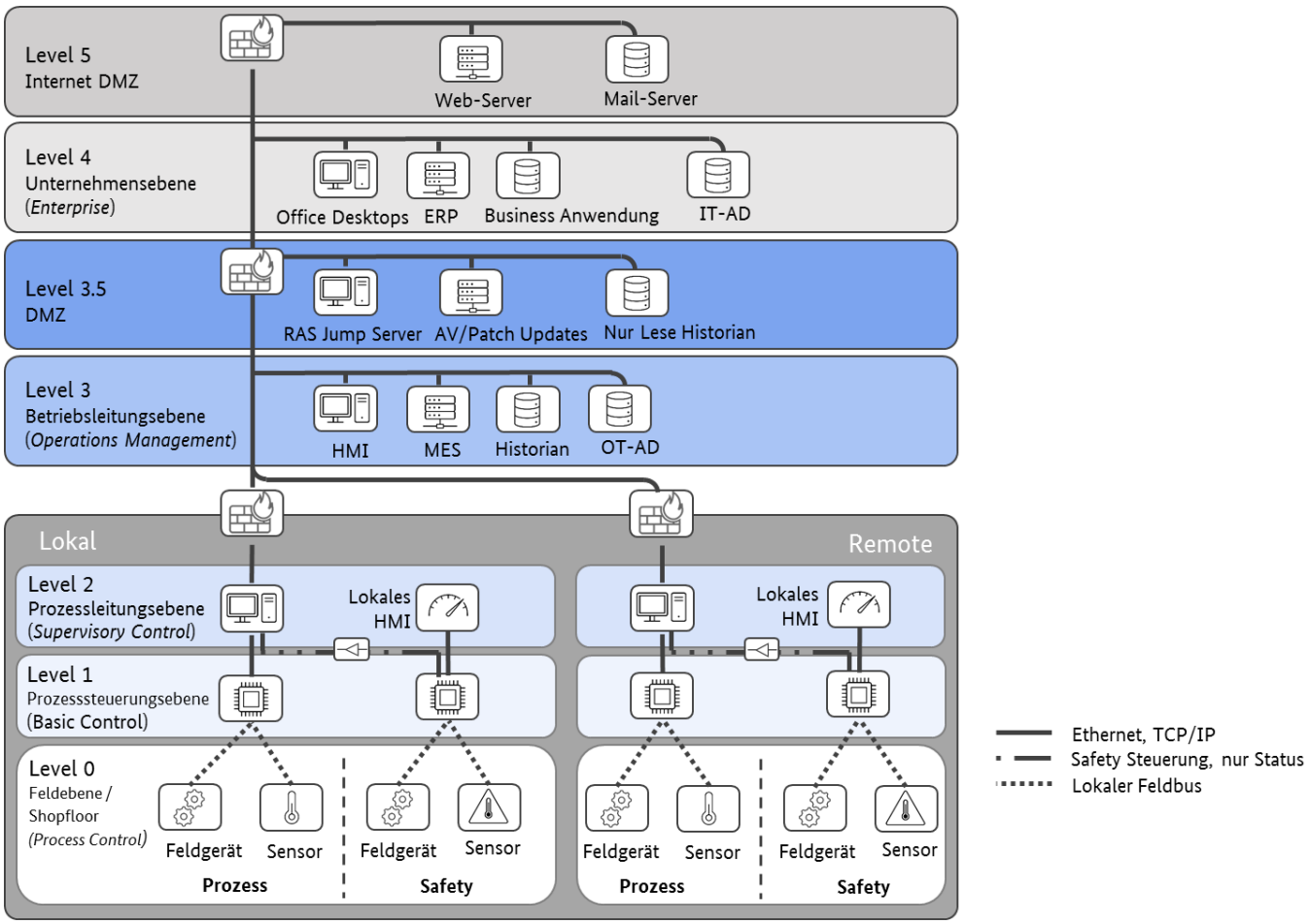

Abbildung 7 Beispiel Netzwerk nach Purdue/IEC 62443

Die einzelnen Ebenen entsprechen weitestgehend den bisher beschriebenen Modellen. Das PERA Modell ergänzt oberhalb der Produktionsführungs- und Unternehmensebene noch eine Internet Ebene, welche die typische Kommunikation mit dem Internet (Web, Mail) repräsentiert. Eine weitere, wichtige Erweiterung ist die Übergangszone Ebene 3.5 (OT-DMZ) zwischen der Office-IT und der Produktion. Als DMZ verhindert diese Zone eine direkte Kommunikation zwischen den beiden Segmenten. Informationen werden über Proxysysteme ausgetauscht. Idealerweise wird die Verbindung hierbei von der Zone mit dem höheren Schutzbedarf (das ICS) aus aufgebaut. So dürfen zum Beispiel ICS-Systeme Daten auf einen Historian in der DMZ schreiben, die Office Systeme hier aber nur lesend zugreifen. Dies zeigt auch den heutigen Fokus des PERA-Modells: Cybersicherheitsaspekte und Anforderungen an OT/ICS Netzwerke und deren Unterteilung in Segmente und definierte Übergänge zur Kontrolle der Kommunikationsflüsse (Zones and Conduits (6)).

2.6 ICS-Lieferkette

Die Lieferkette eines ICS beinhaltet typischerweise die in Abbildung 8 dargestellten Elemente und Akteure.

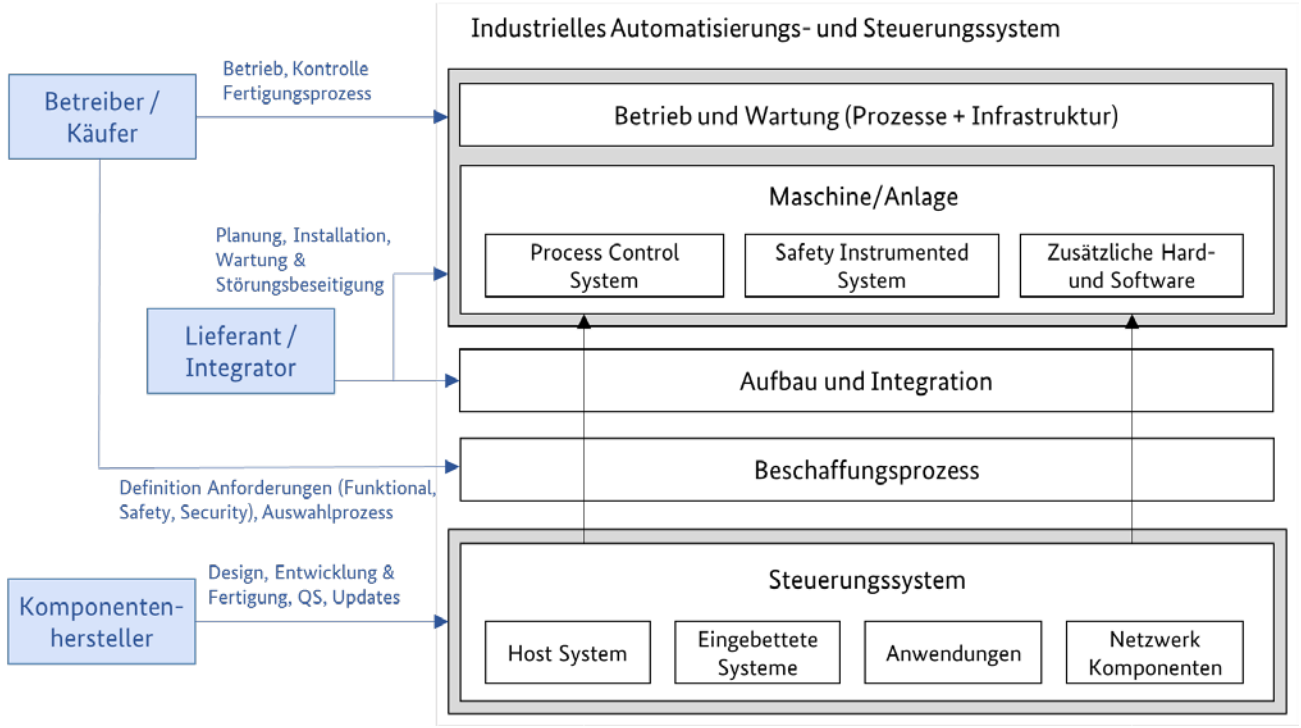

Abbildung 8 Modell der Lieferketten für ICS

Der Komponentenhersteller verantwortet die Entwicklung, Fertigung, Qualitätssicherung und Test, sowie das Bereitstellen und Testen von Updates für Software- und Hardware-Komponenten während des Produktlebenszyklus. Er ist für die grundlegenden Cybersicherheitsanforderungen auf Ebene der Komponenten verantwortlich. Auf diesen kann der Integrator aufbauen und für den Betreiber nutzbar machen.

Der Betreiber definiert vor der Beschaffung Anforderungen an die Anlage (Lastenheft, Funktionspläne, Entwürfe Bedienoberfläche, Grenzwerte, usw.). Dies sind neben den funktionalen Anforderungen auch Cybersicherheitsfunktionen in der OT- und IT wie zum Beispiel Zugriffskontrollen, Benutzerverwaltung, Logging, Härtungsmaßnahmen, Zertifizierungen oder Software-Updateverfügbarkeit. Hierbei müssen auch Rahmenbedingungen für den späteren Betrieb erfasst sein, wie zum Beispiel was bei der Integration in das Netzwerk zu beachten ist, die Anbindung an einen Verzeichnisdienst oder ein zentrales Monitoring.

Im Beschaffungsprozess wählt der Betreiber den Lieferanten und Integrator für den Aufbau und die Integration der spezifischen Anlage. Der Selektionsprozess ist Teil des Lieferantenmanagements. Dabei sollte auch das Thema Cybersicherheit berücksichtigt werden.

Der Integrator führt vor der Auslieferung interne Tests durch und dokumentiert die Ergebnisse in einem Prüfbericht, der zur Werksabnahme (Factory Acceptance Test; FAT) dem Anlageneigner vorzulegen ist. Die anschließende Bereitstellung der Anlage erfolgt in mehreren Phasen (siehe (14) und (15)):

- FAT durch den Integrator: Demonstration der Funktionalität und Abgleich mit den Vorgaben: Lieferumfang, Dokumentation, Anwendungs- und Systemfunktionen kann beim Hersteller/Lieferanten erfolgen.
- Abnahme der installierten Anlage vor Ort (Site Acceptance Test; SAT) durch Betreiber und Integrator: Nachweis der Funktionalität nach der Installation inklusive notwendiger Infrastruktur wie zum Beispiel Spannungsversorgung, Erdung oder Kommunikationsnetzwerke.

- An dieser Stelle sollte auch eine Überprüfung der Vorgaben zur Cybersicherheit stattfinden. Etwa ob ein System gehärtet wurde und sich die Anlage in einer sicheren Konfiguration befindet (z. B. Ändern von Standardpasswörtern, Abschalten unnötiger Services, externe Kommunikationsverbindungen)
- Integrationstest (Site Integration Test; SIT) durch Betreiber: Notwendig falls anlagenübergreifende Funktionen zu prüfen sind. Auch in dieser Phase sollte das Thema Cybersicherheit berücksichtigt werden, z. B. ein Assessment der Cybersicherheit durchgeführt werden, da bei der Integration der Anlage mit externen Systemen durch Nutzung externer Schnittstellen oder zusätzlichen Funktionen neue Schwachstellen entstehen können.

Nach Inbetriebnahme der Anlage sind Integrator und/oder der Hersteller weiterhin bei der Diagnose und Beseitigung von Störungen involviert. Hierzu werden Arbeiten vor Ort oder per Fernzugriff ausgeführt. Hersteller müssen zudem, während der vertraglich vereinbarten Laufzeit der Anlage, Software-Updates zur Fehlerbeseitigung oder Behebung von Schwachstellen zur Verfügung stellen.

Der Betreiber, der Eigner oder ein beauftragter Dienstleister, überwacht die Anlage bezüglich ihrer Funktions- und Systemparameter, führt Änderungen oder Optimierungen an der Anlagenkonfiguration aus, reagiert auf Störungen und führt Wartungsarbeiten durch, welche unter anderem ebenfalls Software-Updates oder Konfigurationsänderungen beinhalten können.

Komplexität von Lieferketten

Die Lieferkette besteht in den seltensten Fällen nur aus den 3 genannten Rollen. Eine ICS-Komponente (zum Beispiel einer SPS) setzt sich typischer Weise aus einer komplexen Kette verschiedener Unterbaugruppen und Software-Komponenten, wie in Abbildung 9 dargestellt, zusammen. Daher stellt das sichere Entwickeln und Betreuen (Bereitstellen und Installieren von Patches) während des Produktlebenszykluses durch Hersteller, Integratoren und Betreiber eine Herausforderung dar.

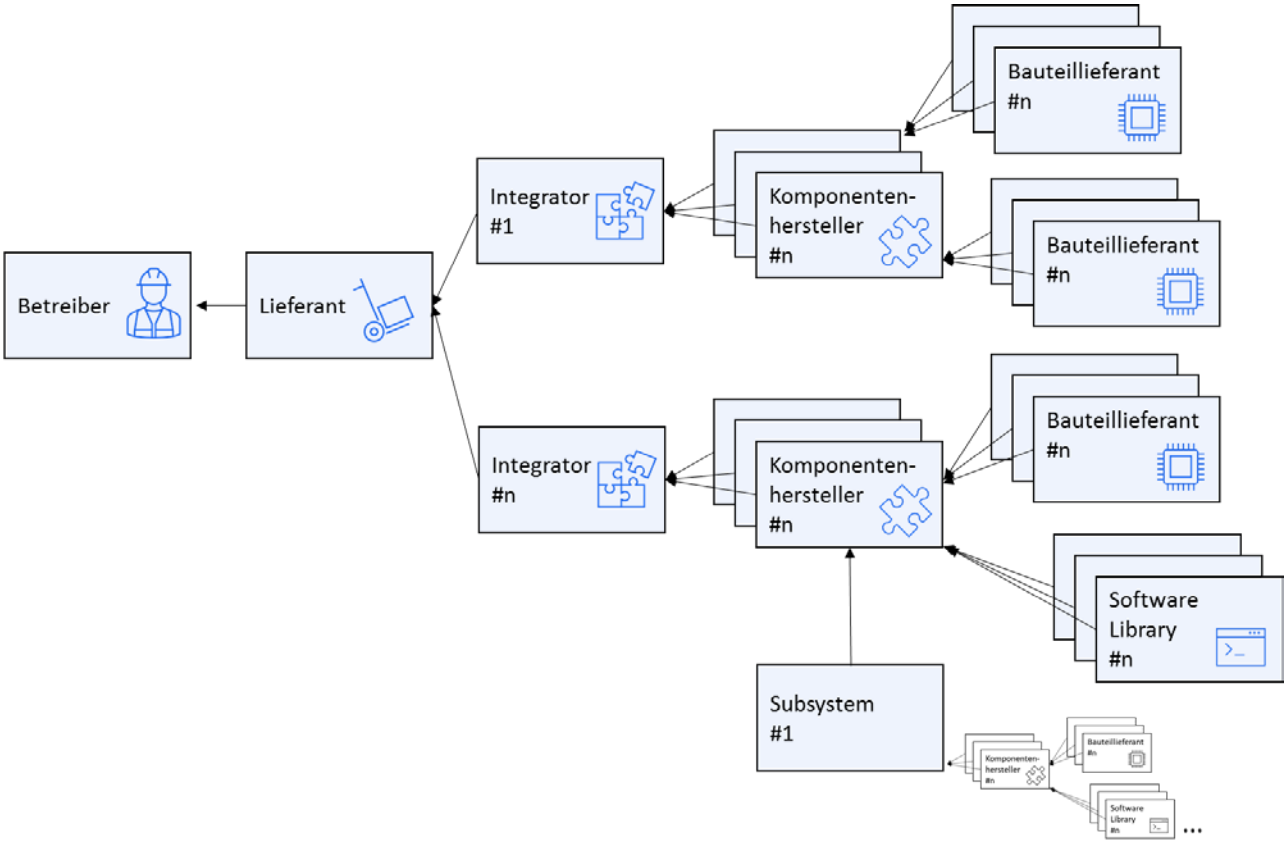

Abbildung 9 Verschachtelte Lieferkette einer ICS Komponente

3 Schwachstellen und Cyberangriffe in der OT

Die fortschreitende Digitalisierung und Vernetzung in der OT hat die Wahrscheinlichkeit von Cyberangriffen und Sicherheitslücken in OT-Umgebungen erhöht. Während Industrieanlagen und Kritische Infrastrukturen früher abgeschottete Systeme waren, die auf proprietären Technologien basierten und keinen Grund zur Vernetzung hatten, werden sie jetzt immer häufiger untereinander oder mit externen Netzen wie dem Internet verbunden.

Aufgrund des vermehrten Einsatzes von Software und Protokollen aus der Office-IT sowie der steigenden Vernetzung und gemeinsamen Nutzung von Ressourcen sind ICS vermehrt ähnlichen Gefahren ausgesetzt wie die Office-IT. Allerdings sind aufgrund von unterschiedlichen Rahmenbedingungen nicht immer die gleichen Schutzmaßnahmen realisierbar oder wirkungsvoll.

Zum Schutz vor Cyberangriffen ist es für Organisationen mit OT unerlässlich, Schwachstellen im OT-Umfeld zu identifizieren und geeignete Schutzmaßnahmen zu ergreifen. Ein erfolgreicher Angriff kann erhebliche Auswirkungen wie Betriebsausfälle, Schäden an Anlagen oder sogar die Gefährdung von Menschenleben haben. Die Beispiele verdeutlichen, weshalb das sorgfältige Vorgehen in der OT umso wichtiger ist.

Dieses Kapitel enthält eine Auflistung der häufigsten organisatorischen und technischen Schwachstellen, die für OT relevant sind. Diese Schwachstellen können von Kriminellen ausgenutzt werden, um Cyberangriffe auf OT durchzuführen. Im weiteren Verlauf werden häufig auftretende Cyberangriffe und deren Auswirkungen auf OT-Anlagen behandelt. Zusätzlich wird ein Überblick über Cyberangriffe und Bedrohungen im Rahmen von Lieferketten gegeben.

Um die Informationen in diesem Kapitel besser zu verstehen, ist es wichtig, die folgenden Begriffe klar zu definieren und voneinander abzugrenzen:

Schwachstelle

> Eine Schwachstelle bezieht sich auf eine Sicherheitslücke, die aufgrund von Architekturentscheidungen, Designfehlern, fehlerhafter Umsetzung oder organisatorischen Unklarheiten entstehen kann.

Bedrohung

> Eine Bedrohung ist allgemein ein Umstand oder Ereignis, durch den oder durch dass ein Schaden entstehen kann. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung (11).
>
> Im OT-Umfeld kann die Bedrohung durch eine Person (unabhängig davon, ob es sich um einen internen oder externen Täter handelt), ein ausgeführtes Script sowie eine OT-Komponente wie SPS, Fertigungsanlage oder ein automatisiertes System wie eine KI oder einen Roboter verursacht werden. Die ausgeführte Handlung wirkt sich hierbei nachteilig auf das System aus und ermöglicht den Zugriff auf sensible Daten oder beeinträchtigt die Verfügbarkeit.

Gefahr

> Eine Gefahr ist eine potenzielle Quelle für ein Risiko, bei der ein Schadensereignis eintreten kann.

Gefährdung

> Eine Gefährdung bezieht sich auf eine spezifische Gefahr, die sich negativ auf Personen, die Umwelt oder Sachwerte wie Anlagen und sensible Daten auswirken kann oder finanzielle Schäden oder Verstöße gegen Auflagen zur Folge hat. Eine Gefährdung tritt auf, wenn eine Schwachstelle eine Bedrohung ermöglicht.

Risiko

Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist (11). Ein Risiko besteht, wenn es durch das Eintreten einer Handlung, eines Ereignisses (plötzlicher Eintritt einer bestimmten Kombination von Umständen) oder einer Entwicklung (allmähliche Veränderung von Umständen) zu einer Zielabweichung kommen kann.

3.1 Schwachstellen im OT-Umfeld

3.1.1 Organisatorische Schwachstellen

3.1.1.1 Unzureichende/ fehlende organisatorische Regelungen und Dokumentation zur Cybersicherheit in der OT

Die Sicherheit der OT hängt wesentlich von der Qualität der organisatorischen Regelungen und der Dokumentation ab. Die aktuellen Regelungen und Dokumentationen bilden die Grundlage für alle Entscheidungen und Aktivitäten. Fehlen jedoch angemessene Regelungen und Dokumentationen, können Schwachstellen entstehen, die die Sicherheit des OT-Umfelds gefährden.

3.1.1.2 Unzureichendes Risikomanagement

Das Risikomanagement im OT-Umfeld ist von entscheidender Bedeutung, da es dabei hilft, potenzielle Gefahren und Bedrohungen, die in der OT auftreten können, zu identifizieren, zu bewerten und zu mindern. Ein unzureichendes Risikomanagement in der OT kann zu einer Reihe von Gefahren wie Systemgefährdungen und Betriebsstörungen führen, da Probleme und deren Folgen falsch oder nicht eingeschätzt werden. In der Folge kann es beim Beheben von Schwachstellen zu falschen Prioritäten kommen oder es werden Ressourcen für Maßnahmen eingesetzt, die einen geringen Beitrag zum Schutzniveau leisten.

3.1.1.3 Mangelnde Kommunikation

Eine der größten Gefahren unzureichender Regelungen und Dokumentationen ist die mangelhafte Kommunikation. Fehlen klare Vorgaben und Anweisungen oder sind diese nicht in geeigneter Form kommuniziert worden, können Missverständnisse entstehen, die zu einer unzureichenden Umsetzung von Sicherheitsmaßnahmen führen. Bei einer unzureichenden Dokumentation kann sich im Schadensfall, beispielsweise durch den Ausfall von Hardware bzw. Fehlfunktionen von Programmen, die Fehlerdiagnose und -behebung erheblich verzögern oder völlig undurchführbar sein.

Wenn das Personal nicht über die Regeln und Anweisungen informiert ist, kann es unwissentlich gegen die Sicherheitsvorgaben verstoßen und damit das System gefährden.

3.1.1.4 Fehlentscheidungen bei der Planung der Sicherheitsarchitektur

Bei der Planung einer Anlage kann bereits viel Einfluss auf die Cybersicherheit einer Anlage genommen werden. Wenn in dieser Phase wichtige Rahmenbedingungen (z. B. Einbindung in das OT-Netzwerk, Anbindung an Verzeichnisdienste oder Auswertung von Logdaten) nicht bekannt sind, kann dies problematisch sein. In diesem Fall müssen ggf. nachträgliche Schutzmaßnahmen getroffen werden.

Ein Beispiel hierfür kann eine unzureichende oder nicht wirksame Segmentierung sein (bezogen auf die durch die Segmentierung zu erreichenden Sicherheitsziele). Ursache für Fehlentscheidungen bei der Planung sind häufig fehlende oder unvollständige Regelungen (z. B. im Änderungsmanagement) oder eine unzureichende Dokumentation (z. B. im Risikomanagement).

3.1.1.5 Unzureichende Regelungen zu den Verantwortlichkeiten

Ein weiteres Problem ist das fehlende Zuweisen von Verantwortlichkeiten für das Erstellen, Überprüfen und Aktualisieren von Regeln und Dokumentationen. Ohne klare Verantwortlichkeiten ist es schwierig sicherzustellen, dass die Dokumentation und die Regeln aktuell und korrekt umgesetzt sind.

Ist nicht festgelegt ob oder in welcher Form das Einhalten der Regeln überwacht wird, kann sich daraus eine geduldete Missachtung der getroffenen Regelungen ergeben.

3.1.1.6 Übertragung von ungeeigneten IT-Regelungen auf das OT-Umfeld

Das Übertragen ungeeigneter IT-Regeln auf das OT-Umfeld kann ebenfalls ein Problem darstellen, da die Anforderungen von IT und OT unterschiedlich sind. So kann beispielsweise eine Vorgabe zum Patchen aus der IT oder Maßnahmen zum Erkennen von Schwachstellen (Schwachstellenscan) in der Regel nicht oder nur eingeschränkt im OT-Umfeld umgesetzt werden.

3.1.1.7 Unzureichende Incident Response Fähigkeit

Ist eine Organisation nicht auf die Abwehr bzw. Mitigation von Sicherheitsvorfällen vorbereitet, kann dies zu einer höheren Tragweite eines Cybervorfalls beitragen. Das Personal, insbesondere Verantwortliche für den Betrieb von IT und OT, ist bei einem Cybervorfall stark unter Druck. Es gilt (weitere) Schäden abzuwenden, schnellstmöglich Einschränkungen zu beheben und alle Systeme wieder in einen einwandfreien Zustand zu versetzen. Wenn für eine solche Situation keine vorbereiteten Pläne beispielsweise zum Abschalten von Systemen oder später zum Wiederanlaufen vorhanden sind, verzögert dies mögliche Handlungen und es vergeht wertvolle Zeit. Hierbei spielt die Dokumentation der Systeme eine wichtige Rolle (siehe auch 3.1.1.1).

3.1.1.8 Einsatz von Standard IT-Komponenten mit bereits identifizierten Schwachstellen

Neben OT-spezifischen Komponenten werden im OT-Umfeld zunehmend Komponenten, Technologien und Software aus der Office-IT eingesetzt. Diese Komponenten, sogenannte commercial-off-the-shelf (COTS) Produkte, weisen (wie fast jede Software) Schwachstellen auf. Diese sind oftmals dokumentiert und öffentlich bekannt.

Darüber hinaus sind häufig entsprechende Angriffswerkzeuge frei verfügbar, die auch von nicht versierten Angreifern benutzt werden können. Da COTS-Produkte weitverbreitet sind, besteht für Angreifer auch ein großes Interesse daran, weitere Schwachstellen in diesen Produkten ausfindig zu machen und speziell zugeschnittene Software für die Ausnutzung dieser Schwachstellen zu entwickeln. Somit werden durch den Einsatz von COTS-Produkten alte und neue Schwachstellen aus der Office-IT in die OT-Umgebung überführt.

3.1.1.9 Mangelnde Awareness und unzureichende Trainings

Fehlende Awareness in Bezug auf Cybersicherheit in der OT bei internem sowie externem Personal (z. B. von externem Dienstleister) stellt eine signifikante Schwachstelle für Betreiber von Industrieanlagen dar.

Eine der Hauptursachen für diesen Mangel an Awareness ist die Tatsache, dass Cybersicherheit in der OT oft als getrenntes Thema von der allgemeinen IT-Sicherheit, beziehungsweise vom Betrieb der Anlage, betrachtet wird. OT-Systeme haben jedoch oft spezifische Eigenschaften, die spezielle Kenntnisse erfordern, um sie effektiv vor Cyberangriffen zu schützen. Weiterhin betrachten viele Organisationen ihre OT-Systeme als geschlossene Systeme, die nicht von außen bedroht werden können. Dies führt oft zu einem trügerischen Sicherheitsgefühl und zu einem mangelnden Verständnis für die Notwendigkeit von Sicherheitsmaßnahmen.

Ein weiteres Problem ist, dass viele Organisationen es vernachlässigen, ihr Personal in Cybersicherheit in der OT zu schulen. Es ist jedoch wichtig, dass das gesamte Personal, das im OT-Umfeld arbeitet, die

notwendigen Kenntnisse und Fähigkeiten hat, die Systeme sicher zu betreiben. Dies umfasst nicht nur IT-Personal, sondern auch Personal aus anderen Abteilungen wie Ingenieure, die oft mit der Wartung von OT-Systemen betraut sind.

Mangelnde bzw. fehlende Awareness und Trainings in der Cybersicherheit in der OT können schwerwiegende Folgen haben. Unbewusste und unsichere Handlungen des Personals, wie z. B. die Auswahl von schwachen Passwörtern, der unsichere Umgang mit Zugangsdaten oder das Öffnen von E-Mail-Anhängen können Cyberangriffe auf das OT-Umfeld ermöglichen. Eine erfolgreiche Attacke auf ein OT-System kann zu Betriebsausfällen, Produktionsverlusten und sogar zu Verletzungen oder Todesfällen führen.

3.1.1.10 Verwendung von initialen Anmeldedaten

Initiale Anmeldedaten sind Standard-Anmeldedaten, die häufig bei der Auslieferung und Integration von Anlagenkomponenten konfiguriert sind und bei der Erstinstallation eines Systems verwendet werden, um einen schnellen und einfachen Zugang zu ermöglichen. Diese Anmeldedaten können jedoch allgemein bekannt und leicht zu erraten sein. Die Verwendung von initialen Anmeldedaten stellt innerhalb der Cybersicherheit in der OT eine Schwachstelle dar. Diese kann von Angreifern ausgenutzt werden, um Zugang zu Systemen und Daten zu erhalten und damit zu erheblichen Folgen für die Sicherheit im OT-Umfeld führen.

Festkodierte Anmeldedaten beziehen sich auf Benutzeranmeldeinformationen, die direkt in den Quellcode eines Programms oder einer Anwendung eingebettet sind, anstatt vom Benutzer bei der Anmeldung eingegeben werden zu müssen. Findet der Angreifer die Anmeldeinformationen im Quellcode, kann er sich leicht mit diesen Informationen anmelden und unautorisierten Zugriff auf das System oder die Anwendung erlangen.

3.1.1.11 Nicht benötigte Zugriffsrechte

Die Vergabe von unnötigen Zugriffsrechten kann zu erheblichen Gefahren für die Sicherheit des OT-Umfelds führen. Durch den nicht benötigten Zugriff auf Funktionen oder Systeme durch Benutzer und Systeme werden Sicherheitsverletzungen ermöglicht. Die damit erhöhte Angriffsfläche kann missbraucht werden, um in OT-Umgebungen einzudringen und Schäden zu verursachen.

Darüber hinaus können nicht benötigte Zugriffsrechte die Einhaltung von Gesetzen und Vorschriften erschweren. Wenn zu viele Benutzer unnötigen Zugriff auf vertrauliche Informationen oder Systeme haben, die bestimmten Datenschutzrichtlinien oder Branchenvorschriften unterliegen, kann dies zu Verstößen führen. Solche Verstöße können hohe Geldstrafen und Haftungsansprüche nach sich ziehen.

3.1.1.12 Unsachgemäße Außerbetriebnahme von Assets

Die ordnungsgemäße Außerbetriebnahme von OT-Systemen ist ein wichtiger Aspekt der Cybersicherheit in der OT. Assets, die unsachgemäß außer Betrieb genommen oder aus dem Netz entfernt wurden, können eine Gefährdung in der Cybersicherheit in der OT verursachen. Darüber hinaus kann eine mangelhafte Außerbetriebnahme von Assets dazu führen, dass kritische bzw. vertrauliche Daten nicht ordnungsgemäß z. B. durch kryptographische Bereinigung gelöscht oder nicht ordnungsgemäß physisch aus dem Gebäude bzw. Anlage entfernt werden. Dies kann zum Offenlegen von sensiblen Informationen führen.

3.1.1.13 Innentäter

Ein Innentäter ist jede Person, die autorisierten Zugang zu IT- und OT-Ressourcen hat oder hatte und die die Sicherheit einer Organisation gefährden könnte. Die Täter sind für gewöhnlich aktuelles oder ehemaliges Personal oder Geschäftspartner, die beabsichtigt oder unbeabsichtigt zu einer Bedrohung werden können.

Unwissende Mitarbeitende können auch als Innentäter betrachtet werden, da sie ohne Vorsatz oder kriminelle Absicht handeln. Sie werden zu einem Sicherheitsrisiko, weil sie fahrlässig und unbeabsichtigt handeln und zum Beispiel vertrauliche Geschäftsdaten „ausplaudern“. Von ihnen geht die größte Gefahr aus, da ihr mangelndes Wissen über den Umgang mit Daten und Assets ein Sicherheitsrisiko darstellt.

Böswilliges Personal hingegen handelt in krimineller Absicht und missbraucht Zugangsberechtigungen innerhalb einer Organisation, um dieser zu schaden. Die Handlungen umfassen unter anderem die Weitergabe sensibler Informationen, die Sabotage von Geräten und den Diebstahl geschützter Daten oder geistigen Eigentums.

3.1.2 Technische Schwachstellen

3.1.2.1 Unvollständige Absicherung von Fernzugängen

Fernzugänge ermöglichen autorisierten Personen auf Systeme und Geräte von entfernten Standorten aus zuzugreifen, um Wartungsarbeiten durchzuführen oder Störungen zu beheben. Die Bedeutung von Fernzugängen hat insbesondere mit der vermehrten Anwendung aus dem Homeoffice oder von unterwegs an Relevanz gewonnen. Wenn die Zugänge jedoch nicht ausreichend abgesichert sind oder sich in unzureichend geschützten Netzwerken befinden, können sie von Angreifern missbraucht werden, um unerlaubten Zugriff auf Systeme und Geräte zu erlangen. Dies kann zu schwerwiegenden Sicherheitsproblemen führen, wie z. B. Datenlecks, Ausfallzeiten, Manipulation von Produktionsprozessen oder gar zur Gefährdung von Menschenleben in einigen kritischen Anwendungen.

Fernzugänge können insbesondere missbraucht werden, wenn sie falsch konfiguriert oder geplant sind. Ein Missbrauch kann auch stattfinden, wenn nicht genügend Kontrollen und Überprüfungen vorhanden sind, um unautorisierte Zugriffe zu verhindern oder ungewöhnliche Aktivitäten zu erkennen. Hierzu zählt auch eine unzureichende Verschlüsselung der Verbindung, indem beispielsweise veraltete kryptografische Verfahren zum Einsatz kommen.

Die Zugangspunkte aus dem Internet sind zudem der Gefahr von Denial-of-Service-Angriffen ausgesetzt. Diese werden dabei durch sehr viele Anfragen überlastet, was den Zugangspunkt für legitime Verbindungsanfragen unerreichbar macht oder verlangsamt.

Nachdem ein Angreifer durch unsichere Fernzugangsverbindungen ein OT-System kompromittiert hat, kann er diesen Zugang nutzen, um den unerlaubten Zugriff auf weitere OT-Systeme zu erlangen.

3.1.2.2 Fehlende Überwachung der Infrastruktur

Das Überwachen von Zuständen in der Produktion ist eine wesentliche Funktion von OT-Lösungen, um mögliche Probleme rechtzeitig zu erkennen und zu beheben. So werden für gewöhnlich die Produktion betreffende Warnungen (z. B. bei unterschrittenen Füllständen) und technische Parameter (z. B. Temperaturen, Ventilstellungen) abgebildet. Diese Überwachung deckt aber meist keine cybersicherheitsrelevanten Ereignisse, wie zum Beispiel das Alarmieren bei unberechtigten Zugriffsversuchen, ab.

Es ist immens wichtig, dass der Betreiber einer OT-Umgebung einen Überblick über das Netzwerk, dessen Assets und die stattfindenden Aktivitäten hat.

Werden ungewöhnliche oder sicherheitsrelevante Ereignisse von OT nicht oder unzureichend überwacht, entsteht ein Sicherheitsrisiko. Engpässe in der Netzarchitektur oder absehbare Ausfälle können zu Systemausfällen und Produktionsunterbrechungen führen.

Eine fehlende Überwachung auf auftretende Schwachstellen in der eingesetzten OT kann dazu führen, dass Gefährdungen der Infrastruktur unentdeckt bleiben und von Angreifern ausgenutzt werden können.

Wenn sicherheitsrelevante Protokollierungsdaten nicht vorhanden sind oder nicht analysiert werden, gehen der Organisation Informationen zum sicheren Betrieb der OT-Umgebung verloren. Dies kann

wiederum bedeuten, dass Aktivitäten vor und bei Cyberangriffen unentdeckt bleiben und Angreifer sich weiter ausbreiten können. Darüber hinaus kann auch eine mangelhafte, unübersichtliche Darstellung der Ereignisse dazu führen, dass Warnungen und Fehler verspätet erkannt werden.

3.1.2.3 Abhängigkeiten des OT-Netzes von IT-Netzen

OT-Netze werden mittlerweile nicht mehr durchgängig als autarke Netzwerke betrieben. Bestehen Abhängigkeiten zu anderen Systemen, Netzen oder Diensten, so wirken sich Ausfälle oder Sicherheitsvorfälle außerhalb des OT-Netzes u. U. auch auf die OT-Umgebung aus. Dies kann dazu genutzt werden, um gezielt die OT-Umgebung zu stören oder zu kompromittieren. Wird zum Beispiel der in der IT vorhandene Verzeichnisdienst zur Authentifizierung von Nutzern im OT-Netzwerk genutzt, so führt ein erfolgreicher Angriff im IT-Netz zur Kompromittierung oder Ausfällen in der OT-Infrastruktur.

Eine Störung der IT-Infrastruktur kann zu einer Unterbrechung der Kommunikation zwischen den OT-Systemen führen. Dies kann schwerwiegende Folgen wie Produktionsausfälle oder sogar Industrieunfälle nach sich ziehen.

Beispiele für Abhängigkeiten zu anderen Systemen und Netzen sind Internetanbindungen (sowohl drahtgebunden als auch über WLAN oder Mobilfunk), gemeinsam genutzte Infrastrukturkomponenten oder auch die zunehmende Nutzung von Cloud-Diensten. Eine weitere Abhängigkeit entsteht durch die zunehmende Nutzung von Datensets zur OT-Prozessoptimierung (z. B. für Digitale Zwillinge). Die Verarbeitung dieser Daten erfolgt aufgrund ihrer Größe und der Komplexität der Verarbeitung (Big Data Analytics) typischerweise in Rechensystemen außerhalb der OT-Umgebung (Edge/Cloud). Eine Manipulation oder das Blockieren dieser Daten kann weitreichende Folgen in der Produktion haben.

3.1.2.4 Unzureichende Absicherung oder zu weitreichende Vernetzung

Werden nicht benötigte Kommunikationskanäle in das OT-Netz eingerichtet, kann ein Angreifer diese ggf. unzureichend gesicherten Zugriffswege nutzen, um auf die OT zuzugreifen und Systeme zu kompromittieren. Wenn z. B. eine Person zur Überwachung eines ICS eine Datenverbindung von seinem Büro-/Arbeitsplatzrechner in das OT-Netz einrichtet, so wird damit das Office-Netz (z. B. mit Verbindung zum Internet) mit dem OT-Netz gekoppelt. Somit ist das OT-Netz denselben Bedrohungen ausgesetzt wie das Office-Netz (z. B. Angriffe oder Schadprogramme aus dem Internet).

Darüber hinaus können OT-Komponenten beispielsweise über Verbindungen in unterschiedliche Ebenen der Beispielarchitektur (vgl. Abbildung 3) verfügen. So kann es einem Angreifer möglich sein, mittels dieser Verbindungen von einem der Netzsegmente, unbefugt auf ein anderes zuzugreifen (z. B. bei aktivierter Bridge- oder Routing-Funktionalität).

Ein weiterer Faktor sind unzureichende Regeln auf Paketfiltern und Firewalls. Firewall-Regeln sollen den Datenverkehr zwischen verschiedenen Teilen des Netzwerks kontrollieren und schützen. Wenn diese Regeln jedoch nicht korrekt konfiguriert sind oder zu weitreichend sind, können sie von Angreifern genutzt werden, um unberechtigt auf Systeme zuzugreifen oder sich im Netzwerk auszubreiten.

Darüber hinaus können Verbindungen zu MES und Cloudbasierten Diensten wie IoT-Plattformen das Risiko von Angriffen auf OT-Netzwerke erhöhen. Diese Verbindungen müssen sorgfältig geprüft und konfiguriert werden.

3.1.2.5 Fehlerhafte Konfigurationen und Verwendung von Standardkonfigurationen

Die fehlerhafte Konfiguration von OT-Systemen und die Verwendung von Standardkonfigurationen stellen eine erhebliche Schwachstelle in der Cybersicherheit in der OT dar. Dies liegt daran, dass viele OT-Systeme ursprünglich für den Einsatz in geschlossenen Netzwerken entwickelt wurden und daher nicht für die Verwendung in offenen Netzwerken ausgelegt sind.

Viele OT-Systeme werden in ihren Standardkonfigurationen betrieben. Diese Konfigurationen sind oftmals öffentlich bekannt und können von Angreifern leicht durchsucht werden, um Schwachstellen zu

identifizieren und auszunutzen. Wenn die Konfigurationen nicht geändert werden, kann dies zu einem erheblichen Sicherheitsrisiko führen.

Ein weiteres Problem besteht darin, dass unnötige Dienste nicht deaktiviert werden. Diese können Schwachstellen aufweisen und von Angreifern ausgenutzt werden, um unbefugten Zugriff auf das OT-System zu erlangen oder Schaden zu verursachen. Ein Beispiel dafür wäre ein veralteter Webserver, der auf einem OT-System ausgeführt wird und eine Schwachstelle aufweist, die von Angreifern ausgenutzt werden kann.

Viele OT-Systeme nutzen proprietäre Betriebssysteme oder Plattformen, die nicht so häufig aktualisiert werden wie allgemeine Betriebssysteme. Dies kann bedeuten, dass Schwachstellen in diesen Systemen länger unentdeckt bleiben können, was das Risiko von Angriffen erhöht.

3.1.2.6 Unsichere oder unbekannte Benutzerschnittstellen

Ein wichtiger Faktor bei der Absicherung von OT-Systemen ist die Überwachung und Sicherung von Benutzerschnittstellen, die häufig als Einfallstor für Cyberangriffe dienen. Im OT-Umfeld ist es üblich, dass die Steuerung und Konfiguration von Komponenten über Webschnittstellen erfolgen kann, die eine Schnittstelle zwischen Benutzer und Software darstellen. Webschnittstellen ermöglichen den einfachen Zugang von jedem Computer und Betriebssystem, weshalb sie umso mehr eine Gefahr für die OT darstellen. Anbieter in der Softwareindustrie haben viele Lösungen eingeführt, um den Zugang zu kritischen Steuerungen zu schützen und den Zugriff auf Webschnittstellen sicher zu gestalten. Unterschiedlich komplexe Plattformen und Technologien bieten sowohl einfache Authentifizierungsmethoden als auch mehrschichtige Zugangskontrollen an.

Unsichere Webschnittstellen können es einem Angreifer ermöglichen, auf sensible Systeminformationen zuzugreifen oder böswillige Aktionen wie die Änderung von Systemeinstellungen durchzuführen. Eine Schwachstelle in einer Webschnittstelle kann es einem Angreifer ermöglichen, eine Vielzahl von Angriffen durchzuführen, einschließlich Denial-of-Service-Angriffen, Cross-Site-Scripting-Angriffen (XSS) und SQL-Injection-Angriffen.

Unbekannte Benutzerschnittstellen können ebenfalls ein Risiko darstellen, wenn sie beispielsweise durch die Installation von Fremdsoftware oder durch nicht autorisierte Änderungen am System eingeführt werden. Diese Schnittstellen können unentdeckt bleiben und es Angreifern ermöglichen, unerkannt auf das System zuzugreifen oder Daten zu stehlen.

3.1.2.7 Fehlende Backups

Fehlende Backups stellen eine ernsthafte Schwachstelle in der Cybersicherheit in der OT dar, da hierdurch die Folgen eines Angriffs auf ein OT-System erheblich verschärft werden.

Ohne Backups gibt es keine Möglichkeit, beschädigte oder verlorene Daten wiederherzustellen.

Das Fehlen von Backups kann auch die Wiederherstellung von Systemen nach einem Angriff oder Ausfall erschweren. Unter Umständen kann dies zu einem langfristigen Betriebsausfall führen.

Wenn eine Sicherung für ein OT-System fehlt, dauert die Wiederherstellung für gewöhnlich länger. Um bspw. den Produktionsablauf nicht zu behindern, werden ausgefallene Systeme oftmals mit unsicheren Konfigurationen wiederhergestellt und keine Härtung oder Abnahmetests durchgeführt. Obwohl MTO- (Maximum Tolerable Outage) und RTO- (Recovery Time Objective) Vorgaben erfüllt werden, kann dies schwerwiegende Folgen haben und Schwachstellen verursachen.

Ein weiterer Grund, für die hohe Relevanz von Backups, ist die Tatsache, dass OT-Systeme oft über einen längeren Zeitraum betrieben werden. Im Laufe der Zeit können sich Konfigurationen ändern, und es kann schwierig sein, den ursprünglichen Zustand des Systems wiederherzustellen, wenn es keine aktuellen Backups gibt. Informationen dazu gibt es in Abschnitt 6.4.5.1 Datensicherung.

3.1.2.8 Fehlende Ersatzhardware

Ersatzhardware in OT-Systemen spielt eine entscheidende Rolle für die Ausfallsicherheit und kontinuierliche Verfügbarkeit kritischer Infrastrukturen und industrieller Prozesse. Vor allem in Krisenzeiten wie der Corona-Pandemie war das Vorhalten von Ersatzhardware von großer Bedeutung, da Lieferengpässe die zeitnahe Ersatzbeschaffung verhinderten.

Wird durch den Betreiber keine Ersatzhardware vorgehalten oder keine entsprechenden Verträge zum Hardwareaustausch abgeschlossen, so kann es zu langfristigen Ausfällen der OT kommen.

Um einen langfristigen Ausfall der Komponenten zu verhindern, sollten für besonders kritische Komponenten Ersatzhardware vorgehalten oder eine zeitnahe Ersatzbeschaffung organisiert werden.

3.1.2.9 Mobile Datenträger und Laptops (BYOD usw.)

Mobile Datenträger und Laptops sind heute allgegenwärtig und werden oft im Rahmen des BYOD-Konzepts (Bring Your Own Device) auch im OT-Umfeld eingesetzt. Einige administrative Tätigkeiten können nicht über Fernwartungszugänge (vgl. Kap. 3.1.2.1) durchgeführt werden, sodass ein Wartungstechniker vor Ort erscheinen muss. Hierzu nutzt ein Wartungstechniker meist mobile Datenträger (z. B. USB-Sticks) oder eigene Laptops, die mit dem OT-Netz oder der betroffenen OT-Komponente verbunden werden. Hier besteht die Gefahr, dass sich auf diesen Geräten Schadprogramme befinden und diese sich im Netzwerk ausbreiten oder die Komponente infizieren, vgl. (16) G 0.39).

Wartungslaptops weisen darüber hinaus unterschiedliche Kommunikationsschnittstellen auf (z. B. Ethernet, WLAN, Bluetooth, Infrarot, Mobilfunknetze). Besteht beispielsweise bereits eine Internetverbindung über Mobilfunk und wird der Laptop gleichzeitig mit dem OT-Netz verbunden, stellt dies eine Netzkopplung dar. Auf diesem Wege sind direkte Zugriffe aus dem Internet in das OT-Netz denkbar.

3.1.2.10 Unzureichende Validierung von Eingaben und Ausgaben

Unzureichende Validierung von Eingaben und Ausgaben kann beispielsweise in SCADA- oder in industriellen Steuerungssystemen auftreten. Das Problem liegt darin, dass die Bedienoberflächen oder nachgelagerten Programme nicht ausreichend prüfen, ob Daten, die sie erhalten oder senden, tatsächlich korrekt und vertrauenswürdig sind. Fehlerhafte oder manipulierte Eingaben können zu falschen Ergebnissen oder sogar zu schwerwiegenden Fehlfunktionen führen. Beispielsweise könnte ein Angreifer Pufferüberläufe ausnutzen, um falsche Befehle einzuschleusen. Dies kann zum Ausfall von OT-Systemen oder zur unkontrollierten Auslösung von Abläufen führen.

Zum anderen können unzureichend validierte Ausgaben vertrauliche Informationen preisgeben oder dazu führen, dass unautorisierte Personen Zugriff auf das System erlangen. Ein Beispiel dafür wäre die Einschleusung von Schadcode in die Ausgabe eines SCADA-Systems, der dann auf einem Client ausgeführt wird, der diese Daten empfängt.

3.1.2.11 Unzureichende Authentifizierung und Autorisierung

Robuste Authentifizierung und Autorisierung spielen im OT-Umfeld eine entscheidende Rolle, um sicherzustellen, dass nur autorisierte Personen Zugriff auf die Systeme und die darin gespeicherten Daten haben und dass nur autorisierte Systeme im OT-Netzwerk kommunizieren können.

Allerdings gibt es auch in der Cybersicherheit in der OT Schwachstellen bei der Authentifizierung und Autorisierung, die von Angreifern ausgenutzt werden können.

Eine Schwachstelle ist die Verwendung unsicherer Authentifizierungs- und Autorisierungsprotokolle. Einige dieser Protokolle sind veraltet und weisen bekannte Sicherheitslücken auf, die von Angreifern ausgenutzt werden können.

3.1.2.12 Unverschlüsselter Transport von Daten

Die Hauptpriorität der Sicherheit von OT wird oftmals in der Verfügbarkeit und Zuverlässigkeit der Systeme gesehen. Aspekte der Vertraulichkeit und Integrität werden unter Umständen nachrangig berücksichtigt. Bspw. wird häufig auf eine Verschlüsselung der Daten oder Transportwege verzichtet. Hieraus entsteht die Gefahr das Daten von Angreifern abgefangen sogar manipuliert werden können. In einem solchen Fall ist die Integrität und die Vertraulichkeit der Daten nicht mehr sichergestellt. Das so entstandene Risiko kann sich auf verschiedene Bereiche der Organisation auswirken und beispielsweise finanzielle Verluste, Image-Schäden oder rechtliche Konsequenzen zur Folge haben.

3.1.2.13 Einsatz von Legacy-Systemen

Legacy-Systeme sind ältere Technologien, die aufgrund ihrer eingeschränkten Funktionalität und mangelnder Unterstützung und Wartung durch die Hersteller häufig anfällig für Cyberangriffe sind. Sie wurden oft entwickelt, bevor Cybersicherheitsgefährdungen so ausgeprägt waren wie heute, und sind daher oft nicht in der Lage, moderne Angriffsmethoden abzuwehren. Der Einsatz von Legacy-Systemen ist im OT-Umfeld durchaus noch verbreitet, insbesondere bei Anlagen mit langen Laufzeiten (mehrere Jahrzehnte).

Eine Herausforderung im Zusammenhang mit dem Einsatz von Legacy-Systemen besteht darin, dass sie in der Regel nicht mehr von den Herstellern unterstützt werden (End of Life – EoL, End of Support – EoS). Dadurch bleiben Schwachstellen offen, welche von Angreifern ausgenutzt werden können. Zudem sind diese Systeme oft nicht in der Lage, Sicherheitsmechanismen wie Authentifizierung oder Verschlüsselung zu unterstützen.

Ein weiteres Problem bei der Verwendung von Legacy-Systemen ist die mangelnde Transparenz. Teilweise gibt es nur wenig Dokumentation zu dem Legacy-System. Entweder besitzt das Personal nicht die erforderlichen technischen Kenntnisse oder die ursprünglichen Anwender bzw. Entwickler haben die Organisation bereits verlassen. Die Systeme sind oft sehr komplex und verwenden veraltete und proprietäre Kommunikationsprotokolle, weshalb Aussagen zur Cybersicherheit of schwer oder gar nicht möglich sind. Das erschwert zusätzlich auch das Erkennen von Anomalien oder verdächtigen Aktivitäten.

3.1.2.14 Unzureichender Schutz vor Schadsoftware

Während der Schutz vor Schadsoftware der Office-IT oftmals durch Software oder Endpoint-Protection-Lösungen gewährleistet ist, erweist sich diese im OT-Umfeld als deutlich komplexer, da hier spezielle Herausforderungen bestehen, die sich von der Absicherung im IT-Umfeld unterscheiden.

Teilweise steht für ältere ICS (und die dort verwendeten Betriebssysteme) auch keine aktuelle Schutzsoftware mehr zu Verfügung.

Ein weiteres Problem ist der Ressourcenbedarf der Schutzsoftware. Diese können die Leistung der Systeme beeinträchtigen. Die Leistungsreduzierung kann während eines erkannten Schadsoftwarebefalls oder möglicherweise sogar durch einen Fehlalarm zu unerwünschten Unterbrechungen in der Produktion führen. Einige Hersteller von OT-Komponenten haben daher keine Freigabe für den Betrieb von Endpoint-Protection-Lösungen auf ihren OT-Komponenten erteilt.

Für ein regelmäßiges Update der Signaturen ist eine Internetverbindung meist zwingend erforderlich. In der OT-Umgebung könnte eine aktive Internetverbindung zur Installation von Updates die Cybersicherheit in der OT gefährden und das Risiko eines Cyberangriffs erhöhen.

Bei Endpoint-Protection-Lösungen die nicht auf Signaturen basieren (bspw. Application Allow Listing oder einer Verhaltensanalyse mit maschinellem Lernen) kann die Gefahr bestehen das selten genutzte Funktionen (z. B. Aktoren der Funktionalen Sicherheit) unterdrückt bzw. unterbunden werden.

Endpoint-Protection-Lösungen sind meist an die in der Office-IT verwendete Kommunikation angepasst und für diese optimiert. Die in der OT verwendeten Protokolle werden teilweise nicht OT spezifisch betrachtet, sodass die Erkennungsrate in den OT-typischen Protokollen nicht sehr ausgeprägt ist.

3.1.2.15 Unbekannte Schwachstellen in Software und Kommunikationsprotokollen

Schwachstellen in Software und Kommunikationsprotokollen, die von Geräten im OT-Umfeld verwendet werden, können ein erhöhtes Risiko darstellen, wenn diese über einen längeren Zeitraum unentdeckt bleiben. Eine unbekannte Schwachstelle kann dazu führen, dass ein Angreifer diese ausnutzt, um sich unbemerkt Zugang und Kontrolle über das System zu verschaffen. Solche Schwachstellen können beispielsweise Zero-Day-Exploits oder verwundbare Bibliotheken sein.

Zero-Day-Exploits stellen eine besondere Bedrohung dar, da es sich um Sicherheitslücken handelt, die von Hackern oder Sicherheitsforschenden entdeckt wurden, bevor der Hersteller sie identifizieren und beheben konnte. Diese Art von Schwachstellen ist besonders gefährlich, da sie von Sicherheitssoftware und -lösungen nicht erkannt werden können. Dies ermöglicht es einem Angreifer, die Schwachstelle auszunutzen und Schaden anzurichten, ohne dass das Opfer dies bemerkt.

Eine weitere potenzielle Schwachstelle in OT-Systemen sind anfällige Bibliotheken. Bibliotheken sind Sammlungen von Code, die von Entwicklern wiederverwendet werden können, um Zeit und Aufwand zu sparen. Wenn jedoch eine Bibliothek verwundbar ist und von vielen Entwicklern verwendet wird, kann ein Angreifer diese Bibliothek ausnutzen, um Zugriff auf alle Systeme zu erhalten, die diese Bibliothek verwenden.

Ein bekanntes Beispiel für eine verwundbare Bibliothek ist die OpenSSL-Bibliothek, die in vielen OT-Systemen zur Verschlüsselung von Daten verwendet wird. Im Jahr 2014 wurde eine Sicherheitslücke in der Bibliothek entdeckt, die als "Heartbleed" bekannt wurde. Diese Schwachstelle ermöglichte es Angreifern, sensible Daten wie Passwörter und private Schlüssel zu stehlen.

3.1.3 Schwachstelle Lieferkette

Cyberangriffe auf Lieferketten industrieller Steuerungssysteme haben in den letzten Jahren zugenommen und stellen eine erhebliche Bedrohung für Organisationen dar. Es wird hier nur die Lieferkette für die OT-Komponenten selbst, deren Bauteile und die Softwarebestandteile betrachtet. Nicht betrachtet werden die Versorgungssicherheit für Rohstoffe oder andere Bestandteile für die herzustellenden Endprodukte. Angreifer nutzen Schwachstellen in der Lieferkette aus, um Schadsoftware oder sonstige bösartige Komponenten in die Produkte der Lieferanten einzuschleusen, die dann in der Infrastruktur der Endkunden zum Einsatz kommen. Im Folgenden sind typische Beispiele für Schwachstellen im Kontext der Lieferkette aufgeführt.

3.1.3.1 Unzureichende Regelungen

Wenn Verantwortlichen in der Lieferkette oder mit Dienstleistern nicht eindeutig geregelt sind, kann dies ähnlich wie in einigen in 3.1.1 Organisatorische Schwachstellen genannten Punkten zur Gefährdungen führen. Dies kann beispielsweise der Fall sein, wenn unklar ist, wer sich um die Cybersicherheit von Komponenten kümmert. In der Folge wird sich niemand darum kümmern.

3.1.3.2 Hardware-Hintertüren

Eine Hintertür (Backdoor) ist eine Funktion oder ein Mechanismus, die/der von einem Hersteller oder einem Dritten in ein elektronisches System eingebaut wird, um einen verdeckten Zugriff auf das System oder auf Daten im System zu ermöglichen. In einer OT-Komponente verhelfen Angreifern solche Hardware-Hintertüren zu unautorisierten Zugriffen auf Steuerungssysteme kritischer Infrastrukturen wie Stromnetze, Wasserversorgung oder Verkehrssteuerung zu ermöglichen.

Hintertüren können auf verschiedene Weise implementiert werden, z. B.:

- Hinzufügen versteckter Schnittstellen oder Komponenten
- Einfügen spezieller Codes oder Befehle in die Firmware oder das BIOS der OT-Komponente.

Hardware-Hintertüren können auch unbeabsichtigt oder aufgrund von Fehlern in der Entwurfs- oder Herstellungsphase der OT-Komponente entstehen.

3.1.3.3 Schwachstellen in der Firmware

Die Betriebssoftware von Steuergeräten, auch als Firmware bezeichnet, ist ein entscheidendes Element für die korrekte Funktion des Gerätes. Allerdings kann die Firmware auch verschiedene Schwachstellen aufweisen, die für potenzielle Angreifer ein Einfallstor bieten können.

Eine mögliche Schwachstelle in der Firmware sind fest einprogrammierte Zugangsdaten. Da diese nicht geändert werden können, findet keine wirkliche Authentisierung statt, da davon auszugehen ist, dass die Informationen auch einem Angreifer bekannt sind.

Schwachstellen in der Firmware können auch unbeabsichtigt durch Fehler in der Softwareentwicklung entstehen.

Zusätzlich besteht die Gefahr, dass modifizierte Firmware eingespielt wird. Dies kann auf verschiedene Weise geschehen, zum Beispiel durch das Einspielen modifizierter Firmware auf dem Transportweg vor der Auslieferung oder durch ein reguläres Update, das von einem Angreifer kompromittiert wurde. Durch modifizierte Firmware können Angreifer das Steuergerät fernsteuern, Daten auslesen oder sogar das Gerät komplett übernehmen.

3.1.3.4 Schwache Kryptographie

Die Wirksamkeit von kryptografischen Verfahren kann sich durch Schwachstellen in den Verfahren, mehr Rechenleistung oder neue Technologien (z. B. Quantencomputer) verringern. Daher ist es notwendig, die eingesetzten Parameter und Verfahren zu prüfen und notwendige Änderungen bereits bei Entwurf und Design zu berücksichtigen.

Dies betrifft auch die Implementierungen der Verfahren. Es gab in der Vergangenheit wiederholt Beispiele für Fehler in entsprechenden Softwarebibliotheken oder auch entsprechender Hardware.

Neben den Verfahren selbst sind auch die entsprechenden Daten, wie private und öffentliche Schlüssel, sowie zugehörige Zertifikate entsprechend zu generieren, aufzubewahren und das Vertrauen zu verwalten.

3.1.3.5 Unsichere Anwendungssoftware

Neben der Firmware einzelner Anlagenkomponenten wird zum Betrieb von Anlagen und Steuerungen des OT-Prozesses zusätzliche Anwendungssoftware (SCADA Anwendungen, Engineering Workstation, Historians, Software-HMIs, etc.) benötigt. Diese setzt oft auf Standard IT-Betriebssystemen wie Windows oder Linux und deren Anwendungen auf, die wiederum weiter in die IT-Umgebung und Anwendungen des Betreibers integriert sind (z. B. für Authentifizierung, Autorisierung, Zeitgeber, Namensauflösung, Backup und weitere). Jede dieser Softwarekomponenten birgt das Risiko von Schwachstellen, die im Rahmen des Schwachstellen-Managements adressiert werden müssen (siehe auch 3.1.1.2).

3.1.3.6 Unsicherer Beschaffungsprozess

Mangelt es an Spezifikationen und Anforderungen zur Cybersicherheit bei der Beschaffung und Auswahl von Komponenten und Dienstleistern, kann keine sichere Implementierung, Integration oder sicherer Betrieb der Steuerungssysteme gewährleistet werden. Die Steuerung der betreffenden Prozesse kann durch Ausnutzen von Schwachstellen gefährdet und somit die Geschäftskontinuität beeinflusst werden.

3.1.3.7 Unsichere Implementierung und Integration

Industrieanlagen werden in der Regel aus einer Vielzahl von Komponenten unterschiedlicher Hersteller aufgebaut. Dieser Aufbau erfolgt typischerweise durch einen Integrator, der die Anlage anschließend an den Betreiber übergibt. Während dieses Prozesses kann es jedoch zu Mängeln und Schwachstellen kommen,

insbesondere, wenn angemessene Sicherheitsmaßnahmen nicht ergriffen oder keine Vorgaben dazu gemacht werden.

Ein häufiges Problem besteht darin, dass die Netzwerke nicht ausreichend sicher segmentiert werden. (siehe auch 3.1.2.4 Unzureichende Absicherung oder zu weitreichende Vernetzung)

3.1.3.8 Unsicherer Betrieb durch externe Dienstleister

Externe Dienstleister können zu einem unzureichend geschützten Betrieb betragen. Ein Beispiel ist das Durchführen von Wartungsarbeiten an der Anlage mit ungeprüften Laptops oder Wechseldatenträgern. Wenn diese Geräte mit einer Schadsoftware infiziert sind, kann dies zu einer Infektion der Anlage führen und ein Sicherheitsrisiko für die Anlage darstellen.

Ein weiteres Beispiel sind unzureichend geschützte Systeme bei einem Dienstleister, die über Fernzugänge, auf Anlagen zugreifen können.

3.1.3.9 Externe Plattformen und Infrastruktur

Heutzutage nutzen immer mehr Organisationen externe Plattformen, um Funktionen im Bereich der Produktionsplanung und -optimierung auszulagern. Dabei kommen häufig aktuelle Technologien wie MES-Systeme oder Funktionen zur Analyse von Maschinendaten in der Cloud zum Einsatz. Aber nicht nur solche Funktionen werden ausgelagert, sondern auch wichtige Cybersicherheitsfunktionen wie die Authentifizierung über einen OAuth-Provider, DDoS-Filter gegen Netzwerküberlastung oder sichere Datenräume für den Austausch sensibler Daten.

In diesem Kontext gibt es auch einige Herausforderungen zu beachten. Der Anlagenbetreiber hat oft nur wenig Kontrolle über die Schutzmaßnahmen des Cloud-Betreibers. Dies bedeutet, dass er sich auf die Sicherheitsmaßnahmen des Cloud-Anbieters verlassen muss, um seine Daten und Systeme vor Bedrohungen zu schützen. Eine weitere Herausforderung besteht darin, dass die Übertragung von Daten zwischen verschiedenen Systemen und Plattformen häufig mit potenziellen Gefährdungen verbunden ist. Wenn diese ausgenutzt werden, kann es zu Datenverlusten oder unberechtigtem Zugriff auf vertrauliche Informationen kommen.

3.2 Cyberangriffe auf die OT

3.2.1 Cyberangriffe und vorsätzliche Handlungen

3.2.1.1 Denial of Service Angriffe (DoS)

DoS-Angriffe verfolgen das Ziel, die Verfügbarkeit von Systemen oder angebotenen Diensten einzuschränken. Werden beispielsweise von einem Angreifer gezielt Ressourcen durch eine Vielzahl von gleichzeitigen Anfragen gebunden, so ist die Komponente aufgrund der Last ggf. nicht mehr für andere Nutzer erreichbar.

Im OT-Umfeld können die Auswirkungen eines DoS-Angriffs besonders verheerend sein. Ein erfolgreicher Angriff kann dazu führen, dass wichtige industrielle Steuerungssysteme wie SCADA-Systeme oder Prozessleitsysteme ausfallen oder falsche Steuerbefehle senden, was zu Produktionsausfällen, Sicherheitsproblemen oder sogar Unfällen führen kann.

Ein Angriff kann auf Netzwerkebene erfolgen (z. B. Überlastung der Übertragungskapazität) oder auch auf Anwendungsebene durch das gehäufte Ausführen ressourcenintensiver Operationen. Darüber hinaus kann auch das Ausnutzen von softwarebasierten Schwachstellen (z. B. Pufferüberlauf) zum Ausfall des Systems oder Dienstes führen (vgl. (17)). Wenn die Kommunikation drahtlos erfolgt, kann ein Angreifer die Funksignale gezielt stören und ggf. unterbrechen. Der Angriff kann auch über eine verteilte Infrastruktur, beispielsweise ein Bot-Netz, erfolgen. In diesem Fall wird dies als Distributed-DoS (DDoS) bezeichnet.

3.2.1.2 Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen (Angriffe gegen Zugangsdaten)

Erfordert der Zugang zu Systemen eine Authentisierung mittels Zugangsdaten, so kann ein Angreifer versuchen, diese zu erraten. In der Regel werden hierzu automatisierte Angriffswerkzeuge verwendet, die auf unterschiedlicher Datenbasis versuchen, Kennwörter herauszufinden. Bei einem Brute-Force-Angriff werden alle denkbaren Kombinationen an Zeichen für das Passwort durchgetestet (z. B. Alphabet mit Zahlen und Sonderzeichen). Hierbei steigt der Aufwand exponentiell mit der Passwort-Länge. Daher ist ein Brute-Force-Angriff oftmals sehr zeitintensiv und von zahlreichen, nicht erfolgreichen Anmeldeversuchen gekennzeichnet. Aufgrund des ineffizienten Vorgehens bei einem Brute-Force-Angriff mit allen denkbaren Kombinationen für ein Passwort wird häufig die Datenbasis zur Ermittlung der Passwörter auf ein definiertes Wörterbuch eingeschränkt. In diesem Fall spricht man von einem Wörterbuch-Angriff (engl. dictionary attack). Hierbei handelt es sich somit um eine Variante eines Brute-Force-Angriffs. Entgegen dem oben beschriebenen Brute-Force-Angriff ist der Erfolg bei einem Wörterbuch-Angriff jedoch stark abhängig von der Qualität des Wörterbuchs. Solche Wörterbücher mit häufig genutzten Passwörtern werden daher rege im Internet ausgetauscht. Insbesondere Standardzugangsdaten (vgl. Kap. 3.1.2.5) und nicht ausreichend komplexe, triviale und zu kurze Passwörter können mittels dieser Angriffstechniken effizient und in kurzer Zeit ermittelt werden.

3.2.1.3 Systematische Schwachstellensuche über das Netzwerk

Sind ICS für einen Angreifer über das Netzwerk erreichbar, so kann er verfügbare Dienste identifizieren und ggf. bekannte, vorhandene Schwachstellen mittels unterschiedlicher Techniken über das Netzwerk ermitteln. Ein Angreifer, der Schwachstellen in der Netzwerkarchitektur ermittelt, kann diese ausnutzen, um in das Netzwerk einzudringen und Schaden anzurichten, wie z. B. Datendiebstahl, das Lahmlegen von Systemen oder sogar die Übernahme der Kontrolle über kritische industrielle Prozesse.

Hierfür können frei verfügbare Programme verwendet werden, die den Prozess automatisieren. Mittels eines sogenannten Port-Scans lassen sich die verfügbaren Ports und erreichbaren Dienste über das Netz ermitteln (z. B. TCP- und UDP-Scan).

Sind die verfügbaren Ports ermittelt, wird anschließend ein sogenannter Schwachstellenscanner eingesetzt, um die identifizierten Dienste auf Schwachstellen zu prüfen. Der Scanner kann beispielsweise versuchen, veraltete Software- oder Betriebssystemversionen zu erkennen, die für bekannte Exploits anfällig sind. Der Scanner kann auch bekannte Standardpasswörter oder Schwachstellen in Netzwerkkonfigurationen testen. Hierfür sind in Schwachstellenscannern Tests hinterlegt, welche die Dienste auf spezifische, bekannte Schwachstellen überprüfen (z. B. Pufferüberläufe, SQL-Injection, Broken Authentication oder fehlerhaftes Sitzungsmanagement (vgl. (18)).

3.2.1.4 Man-in-the-Middle-Angriffe (MitM) - unverschlüsselte Kommunikationen

Die Kommunikation von Mess- und Steuerdaten ist ein wichtiger Aspekt in vielen industriellen Prozessen und erfolgt meist über Netzwerke oder drahtlose Verbindungen wie z. B. Ethernet, TCP/ IP, WLAN, GSM oder auch ICS-spezifische Protokolle.

ICS-spezifische Daten werden häufig im Klartext übertragen und unterliegen daher keinen oder nur eingeschränkten IT-Sicherheitsmaßnahmen. Ein Angreifer mit physischem Zugriff auf das OT-Netz kann diese Werte somit auslesen, verändern oder neue einspielen (z. B. zur Steuerung einer Maschine oder zur Fälschung von Sensordaten).

Bei einem MitM-Angriff nimmt der Angreifer eine Position zwischen zwei Kommunikationspartnern ein, um beispielsweise die übertragenen Daten mitzulesen oder zu manipulieren. Dies kann physikalisch z. B. durch das Auftrennen einer Leitung und/oder der direkten Verbindung zu den beiden Kommunikationspartnern geschehen. Alternativ kann dies durch Manipulationen auf Netzwerkebene erfolgen, wodurch die Datenpakete an den Angreifer gesendet werden. Dieser kann die Daten dann lesen,

ggf. manipulieren und an das eigentliche Ziel weiterleiten. Manipulation von Mess- und Steuerdaten durch einen MitM-Angriff kann verheerende Auswirkungen haben, da fehlerhafte oder falsche Daten an wichtige Steuerungsprozesse gesendet werden können.

Die Manipulation von Sensordaten kann zu Fehlfunktionen in automatisierten Steuerungssystemen führen. Werden beispielsweise falsche Sensordaten von einem Angreifer vorgetäuscht, können die Systembediener keine zuverlässigen Sensordaten mehr ablesen und können sich u. U. in einem schwerwiegenden Irrtum über den tatsächlichen Systemzustand befinden. Die Manipulation von Sensordaten, auf denen vollautomatische Steuerungen (closed loop control) basieren, kann zu falschen Steuerbefehlen führen und damit direkte Auswirkungen auf den Prozess haben. Insbesondere bei ungesicherten Funkverbindungen ist ein einfacher Zugriff auf die übertragenen Daten möglich. Durch gezielte Überlagerung ist es möglich, Daten einzuspeisen oder zu verändern sowie die Kommunikation insgesamt zu stören. Derartige Angriffe können zu folgenden Problemen (siehe auch Kap. 3.2.1.1) führen:

- Verlust der Anzeige (loss of view),
- Manipulation der Anzeige (manipulation of view) und
- Störung oder Verlust der Kontrolle (loss of control)

So können beispielsweise Sensordaten (z. B. Füllstand, Temperatur, Druck) verfälscht werden, um Abschaltungen oder Regelbefehle zu verhindern und damit den Produktionsprozess zu beeinflussen. Denkbar ist auch die Verfälschung von Produktionsparametern (z. B. Frequenzen, Drehzahlen, Dauer eines Schweißvorgangs), um gezielt Fehlproduktionen herbeizuführen. Darüber hinaus können ggf. Mechanismen der Funktionalen Sicherheit ausgelöst oder gestört werden (z. B. Selbstabschaltung bei Drucküberschreitung, Unter- oder Überschreitung eines definierten Füllstands oder Unterdrückung der automatischen Selbstabschaltung).

3.2.1.5 Replay Angriffe

Gelingt es einem Angreifer den Netzwerkverkehr mitzuschneiden (z. B. SPS STOP-Befehl), so kann er durch das Wiedereinspielen dieser Daten in das Netzwerk die mitgeschnittene Aktion unter Umständen ohne Befugnis erneut auszuführen. Dies setzt voraus, dass das zur Datenübertragung verwendete Protokoll nicht in der Lage ist, mehrfach versendete Daten zu unterscheiden. In diesem Fall können erstmalig legitim übertragene Daten von einer Kopie der zuvor übertragenen Daten nicht abgegrenzt und ggf. verworfen werden. Diese Technik wird als Replay-Angriff bezeichnet. Auf diese Weise kann der Angreifer korrekt formatierte und auch verschlüsselte oder signierte Daten in den Verkehr bringen, die der Empfänger als authentische Information weiterverarbeitet, ohne z. B. die Verschlüsselung brechen oder zuvor ein Passwort herausfinden zu müssen. Beispielsweise kann ein Schaltbefehl (z. B. Einschalten einer Pumpe) oder die Parameterübermittlung (z. B. Vorgabe einer Solltemperatur für einen Ofen) an eine OT-Komponente von einem Angreifer aufgezeichnet und zu einem späteren Zeitpunkt, zu dem ein Schaden zu erwarten ist, wiederholt werden.

3.2.1.6 Phishing und Social Engineering

Bei einem Phishing-Angriff gibt sich der Angreifer gegenüber dem Benutzer als vertrauenswürdige Person oder Stelle aus (z. B. Administrationspersonal, Hersteller). Er nutzt meist menschliche Eigenschaften wie Neugier, Angst und Hilfsbereitschaft aus und versucht so, an Informationen wie Zugangsdaten zu gelangen oder den Benutzer dazu zu bringen, bestimmte Handlungen auszuführen (z. B. Änderung einer sicherheitsrelevanten Konfiguration, Installation eines Schadprogramms im E-Mail-Anhang). Der Angreifer versucht dabei, Vertrauensverhältnisse des Benutzers auszunutzen. In der Regel werden solche Phishing-Angriffe über gefälschte Internetauftritte und den Versand von E-Mails oder Nachrichten in sozialen Medien durchgeführt. Durch den Massenversand solcher E-Mails können Phishing-Angriffe auf eine Vielzahl von Benutzern ausgeweitet werden. Neben dem Massenversand von Nachrichten gibt es einen Trend zu zielgerichteten Attacken. Hierbei werden z. B. Informationen aus öffentlichen Quellen oder sozialen Netzwerken genutzt, um eine möglichst persönliche Ansprache zu erreichen. Dadurch wird die

Wahrscheinlichkeit erhöht, dass das Opfer einen Anhang öffnet oder einen Link anklickt, der auf eine mit einem Schadprogramm infizierte Seite verweist.

Oft verweisen Phishing E-Mails auf mit Schadcode präparierte Webseiten. Aufgrund von Schwachstellen in Browsern oder deren Erweiterungen kann das bloße Aufrufen dieser Seiten zur Infektion des Rechners mit Schadsoftware führen. Dies wird als Drive-By-Download (auch Drive-By-Exploit) bezeichnet. Dazu ist keine weitere Interaktion durch den Benutzer erforderlich.

Zusätzlich kann sich ein Angreifer auch durch eine nicht-technische Handlung wie z. B. durch die Ausgabe als Techniker unberechtigten Zugang zu einem Gebäude verschaffen.

3.2.1.7 Cyberangriffe auf Webapplikationen

Cyberangriffe auf Webapplikationen erfolgen in der Regel mittels Injection oder Cross-Site-Scripting. Bei einem Injection-Angriff übergibt ein Angreifer einer Anwendung präparierte Eingabedaten und versucht damit Befehle auszuführen. Dies betrifft vor allem verarbeitende Dienste und beruht auf einer mangelhaften Validierung von Eingabedaten (vgl. Kap. 3.1.2.10). Ein Beispiel sind SQL-Injection-Angriffe, bei denen einer Web-Anwendung speziell konstruierte Daten übermittelt werden, um einen Befehl auf der Datenbank auszuführen. Werden die Daten nicht ausreichend auf Plausibilität geprüft, ist eine Manipulation der Datenbankinhalte möglich, weil diese als Befehl interpretiert werden. Weitere Beispiele sind LDAP3-Injection, Mail-Command-Injection, OS-Command-Injection oder Code-Injection.

XSS-Angriffe richten sich gegen die Benutzer einer Webanwendung. Hierbei versucht ein Angreifer, Schadcode (in der Regel browserseitig ausführbare Skripte, wie z. B. JavaScript) indirekt an den Client des Benutzers einer Webanwendung zu senden. Sind die Ein- und Ausgaben von einer Webanwendung nicht ausreichend validiert, so kann ein Angreifer schadhaften Code in die Webanwendung einschleusen (z. B. innerhalb eines Kommentars zu einem Artikel) und so verbreiten. Wird eine infizierte Webseite von einem Benutzer aufgerufen, führt der Client (z. B. Browser) den eingeschleusten Schadcode aus. Aus Sicht des Benutzers stammt der Schadcode von der Webanwendung und wird somit als vertrauenswürdig eingestuft. Daher wird der Schadcode im Sicherheitskontext der Webanwendung interpretiert und es ist dem Angreifer möglich, Befehle im Kontext einer eventuell bestehenden Sitzung des betroffenen Benutzers auszuführen.

3.2.1.8 Schadprogramme und Schadsoftware

Engineering Workstations (EWS) werden zur Konfiguration und Programmierung von OT-Komponenten verwendet. Zusammen mit OT-Servern und Bediengeräten wie HMI sind sie dem größten Risiko ausgesetzt, mit einem Schadprogramm infiziert zu werden. Wenn diese Komponenten der OT mit einem Schadprogramm infiziert sind, können hierüber:

- Die Programme auf der SPS verändert werden. Dies kann sich in veränderten Darstellungen, zusätzlichen Steuerbefehlen oder Ähnlichem auswirken. Somit kann der Angreifer auf diesem Weg Veränderungen am Produktions- bzw. Automatisierungsablauf vornehmen. Dies kann zu Produktionsausfällen oder anderen Betriebsstörungen führen.
- Die Programme und Abläufe auf der SPS entwendet und an den Angreifer übertragen werden. Dies kann zu erheblichen Schäden führen, insbesondere wenn es sich um wichtige Organisationsdaten oder sensible Kundendaten handelt.

Für Angreifer ist dieser Angriffsvektor besonders wertvoll, da hierdurch nicht nur die SPS kompromittiert und die Produktion gestört werden kann. Es wird gleichzeitig die Visualisierung des Steuerungszustands im Sinne des Angreifers beeinflusst. In der Folge bemerkt das Bedienpersonal die Auswirkungen des Angriffs unter Umständen nicht, schöpft keinen Verdacht und setzt die bereits gestörte Produktion unvermindert fort. Beeinträchtigte Systeme können dann über einen längeren Zeitraum unbemerkt sabotiert werden.

Ein neuer Trend ist Industrial Ransomware-as-a-Service (RaaS), der speziell auf industrielle Umgebungen und OT-Netzwerke abzielt. Bei diesem Modell bieten Kriminelle ihre Ransomware-Dienste als Service an, der es anderen Angreifern ermöglicht, gezielt industrielle Systeme zu attackieren. Industrial RaaS

ermöglicht es Angreifern, ohne umfangreiche technische Kenntnisse oder Ressourcen an Ransomware-Angriffen auf OT-Netzwerke teilzunehmen. Die Anbieter stellen die notwendige Ransomware-Infrastruktur, die Angriffs-Tools und die Support-Dienste bereit, während die Kunden (Angreifer) die gewünschten Ziele und Lösegeldforderungen festlegen können.

Neben der gezielten Infektion mit Schadprogrammen können auch Schadprogramme, die eigentlich auf die Organisations-IT abzielen, Schäden im ICS verursachen (Kollateralschäden). Dies kann zu Abstürzen, veränderten Laufzeiten oder einem erhöhten Netzwerkverkehr und damit zu Ausfällen führen. Mögliche Infektionswege wurden bereits in Kapitel 3.2.1.6 und 3.2.1.7 beschrieben.

3.2.2 Cyberangriffe im Rahmen von 5G und Mobilfunk

Im Kontext von 5G-Netzwerken und älteren Mobilfunknetzwerken sind gezielte Cyberangriffe möglich, die auf eine Störung oder die Übernahme der Kommunikation abzielen. Dazu gehören unter anderem, Angriffe auf das GPRS Tunneling Protocol oder SIM-Swapping.

3.2.3 MitM-Angriffe in OT-Netzwerken

MitM-Angriffe in OT-Netzwerken können dazu führen, dass ein Angreifer den Datenverkehr zwischen den Steuerungssystemen und anderen OT-Geräten abfängt, manipuliert oder sogar blockiert. Dadurch kann der Angreifer kritische Befehle oder Informationen ändern, Geräte falsch steuern oder die Kommunikation zwischen verschiedenen Komponenten der industriellen Infrastruktur unterbrechen.

3.2.4 Machine-to-Machine-Angriffe in OT-Netzwerken

M2M-Angriffe in OT-Netzwerken zielen darauf ab, die Kommunikation zwischen vernetzten Geräten in industriellen Umgebungen zu stören oder zu manipulieren. Durch die Kompromittierung von Geräten oder die Manipulation von M2M-Kommunikationsprotokollen kann ein Angreifer schädlichen Code in das OT-Netzwerk einschleusen oder gefälschte Befehle an die industrielle Steuerung senden.

3.2.5 Cyberangriffe im Rahmen von Lieferketten

In Kapitel 3.1.3 wurden Schwachstellen in der Lieferkette beschrieben. Diese sind für Angreifer besonders interessant, weil der erfolgreiche Angriff auf ein Ziel (z. B. Beispiel eine häufig eingesetzte Fernwartungssoftware), den Zugang zu einer großen Zahl an Opfern ermöglicht und diese Art von Angriffen häufig lange nicht entdeckt werden, weil der Lieferant eine Vertrauensstellung zum Opfer hat. Die Erkennung ist schwierig, da zum Beispiel keine „Malware“ oder verdächtige, externe Verbindungen oder Anmeldeversuche gefunden werden.

Die Ausnutzung dieser Schwachstellen kann auf unterschiedliche Weise erfolgen:

Beispiel: Modifikation von Fernwartungssoftware oder Plattformen – SolarWinds-Angriff

Der SolarWinds-Angriff wurde Ende 2020 bekannt und sorgte für große Verunsicherung. Die Auswirkungen des Angriffs sind noch nicht vollständig absehbar, er zeigt jedoch, wie wichtig es für Organisationen ist, ihre IT- und OT-Systeme kontinuierlich zu überwachen und abzusichern, um solche Angriffe zu verhindern oder zumindest schnell erkennen zu können.

Bei dem genannten Angriff auf den Hersteller von Fernwartungssoftware gelang es den Angreifern zunächst, in das Netzwerk der Organisation einzudringen und sich Zugang zu den Rechnersystemen für die Softwareentwicklung zu verschaffen. Auf diesen Systemen modifizierten die Angreifer den Prozess der Softwareentwicklung, indem sie die einzelnen Softwaremodule so manipulierten, dass diese zu einem ausführbaren Programm zusammengefügt wurden.

Durch diese Manipulation wurde eine "Hintertür" in zukünftige Software-Updates der Plattform eingebaut, die den Angreifern einen unberechtigten Zugriff auf die Systeme der Endkunden ermöglichte. Entscheidend war dabei, dass diese Hintertür auch durch eine Inspektion des Quellcodes nicht entdeckt werden konnte.

Dadurch konnte der Angriff lange Zeit unentdeckt bleiben und die Angreifer hatten Zeit, sich Zugriff auf weitere Systeme und Daten zu verschaffen. (19)

Beispiel: Manipulation der Betriebssoftware einer Steuerkomponente

In diesem Szenario gelingt es einem Angreifer, sich Zugang zur Website des Herstellers von Anlagen oder Komponenten zu verschaffen. Dort gelingt es ihm, die zum Download bereitgestellte Firmware und die zugehörige Prüfsumme so zu manipulieren, dass er auf den betroffenen Systemen Schadfunktionen ausführen kann.

Ein erfolgreicher Angriff dieser Art kann gravierende Auswirkungen haben, insbesondere wenn es sich um kritische Infrastruktursysteme handelt. In diesem Fall könnte der Angreifer nicht nur die Kontrolle über die betroffenen Systeme erlangen, sondern auch Schäden verursachen, die die Sicherheit und das Wohlergehen von Menschen gefährden könnten.

Beispiel: Verwundbare Automationssoftware

Durch das Eindringen in eine infizierte Engineering-Station kann ein Angreifer bösartigen Script-Code an eine Projektdatei einer Steuerungskomponente anhängen. Wenn eine Person während eines Wartungsvorgangs über die cloudbasierte Administrationsplattform auf diese SPS zugreift, wird der angehängte Script-Code im Kontext der Person ausgeführt. Dadurch wird im Hintergrund über den Browser der Person ein neues Administrationskonto erstellt. Zu diesem Zeitpunkt hat der Angreifer über die Cloudplattform Zugriff auf alle Steuerungskomponenten, die von diesem neuen Administrationskonto verwaltet werden.

Dieses Szenario zeigt, wie gefährlich ein Angriff auf ein Steuerungssystem sein kann, da es dem Angreifer eine weitreichende Kontrolle über das System ermöglicht. Es unterstreicht auch die Bedeutung der Sicherheit von Engineering-Stationen und anderen Geräten, die zur Verwaltung von Steuerungskomponenten verwendet werden.

3.2.6 Auswirkungen von Cyberangriffen auf Anlagen

Cyberangriffe können schwerwiegende Auswirkungen auf OT haben, da diese oft direkt mit der Produktion und der Infrastruktur einer Organisation verbunden sind. OT-Systeme, die z. B. in der Fertigung, im Energiesektor oder im Transportwesen eingesetzt werden, steuern wichtige Prozesse und sind daher für die Aufrechterhaltung der Produktion und des Betriebs von entscheidender Bedeutung.

Ein erfolgreicher Cyberangriff auf ein OT-System kann daher verheerende Folgen haben. Beispielsweise kann ein Angriff dazu führen, dass ein OT-System gestört oder manipuliert wird, wodurch die Produktion unterbrochen oder die Qualität der hergestellten Produkte beeinträchtigt wird. Im schlimmsten Fall kann ein Angriff sogar zu einem Totalausfall des OT-Systems führen, was erhebliche finanzielle Verluste und Reputationsschäden nach sich ziehen kann.

Darüber hinaus kann ein Cyberangriff auf ein OT-System auch die Sicherheit des Personals gefährden. Beispielsweise kann ein Hacker, der Zugang zu einem OT-System hat, die Kontrolle über Maschinen oder Geräte übernehmen, die gefährliche oder lebensbedrohliche Aufgaben ausführen. Eine solche Manipulation kann zu Unfällen führen und das Risiko von Verletzungen oder Todesfällen erhöhen.

Ein weiteres potenzielles Risiko von Cyberangriffen auf OT-Systeme ist die Umweltverschmutzung. Wenn Anlagen manipuliert werden, um Abfälle oder Chemikalien freizusetzen, können diese in die Umwelt gelangen und zu einer Verschmutzung von Boden, Wasser und Luft führen. In einigen Fällen kann dies zu einer dauerhaften Schädigung der Umwelt und der Tierwelt führen.

Zusammenfassend lässt sich sagen, dass ein erfolgreicher Cyberangriff auf OT-Systeme schwerwiegende Auswirkungen auf die Produktivität, das Personal und die Umwelt haben kann. Organisationen müssen sich darüber im Klaren sein, dass Cybersicherheit nicht nur eine Frage der Compliance ist, sondern auch ein wichtiges Element des Risikomanagements. Es ist wichtig, regelmäßig Sicherheitsaudits durchzuführen, um

Schwachstellen zu identifizieren und zu beheben. Zudem ist sicherzustellen, dass Personal geschult und sensibilisiert wird, um die Risiken von Cyberangriffen zu minimieren.

4 Organisationen, Verbände und deren Standards

Dieses Kapitel gibt einen Überblick über nationale und internationale Organisationen sowie deren Standards und Handreichungen im Bereich Cybersicherheit für die OT. Die Zielsetzung, Adressaten, Inhalte und Anwendungsbereiche der Standards und Quasi-Standards sind im Überblick dargestellt.

4.1 International

Die Internationale Organisation für Normung (ISO; http://www.iso.org) erarbeitet international gültige Normen in allen Bereichen. Zusammen mit der Internationalen Elektrotechnischen Kommission (IEC; http://www.iec.ch), die für den Bereich der Elektrik und der Elektronik zuständig ist und der Internationalen Fernmeldeunion (ITU), die für den Bereich der Telekommunikation zuständig ist, bilden diese 3 Organisationen die World Standards Cooperation (WSC).

4.1.1 IT-/Cybersicherheit

4.1.1.1 ISO/IEC 27000-Serie

Die ISO/IEC 27000-Serie ist eine Sammlung von international anerkannten Normen und Richtlinien, die sich mit Informationssicherheitsmanagement befassen. Sie bietet einen Rahmen für die Implementierung, Überwachung und Verbesserung von Informationssicherheitsmaßnahmen in Organisationen.

Im Folgenden sind die wichtigen Normen der ISO/IEC 27000-Serie tabellarisch zusammengefasst:

Tabelle 5 Relevante Normen der ISO/IEC 27000-Serie (auszugsweise)

ISO/IEC 27000-Serie	*Beschreibung*
ISO/IEC 27000	Diese Norm dient als Einführung und Überblick über die gesamte ISO/IEC 27000-Serie. Sie stellt grundlegende Begriffe, Definitionen und Konzepte bereit und bietet eine allgemeine Orientierung für Organisationen, die ein Informationssicherheitsmanagementsystem (ISMS) implementieren möchten.
ISO/IEC 27001	Diese Norm definiert die Anforderungen für ein ISMS. Sie legt den Rahmen fest, wie Organisationen Risiken bewerten und behandeln, Sicherheitsziele festlegen, Sicherheitskontrollen implementieren und kontinuierlich verbessern sollten.
ISO/IEC 27002	Diese Norm enthält umfangreiche Leitlinien und Best Practices für Informationssicherheitskontrollen. Sie gibt Empfehlungen für verschiedene Sicherheitsbereiche wie Organisation der Informationssicherheit, Zugangssteuerung, Verschlüsselung, Netzwerksicherheit, Incident Management und Compliance.
ISO/IEC 27003	Diese Norm bietet detaillierte Leitlinien für die Planung, Implementierung, Überwachung und Verbesserung eines ISMS. Sie beschreibt den Prozess der Einführung eines ISMS und bietet praktische Anleitungen und Empfehlungen für jede Phase des Projekts.
ISO/IEC 27004	Diese Norm konzentriert sich auf die Messung und Bewertung der Effektivität eines ISMS. Sie bietet Leitlinien für die Auswahl und Umsetzung von Sicherheitsmaßnahmen sowie für die Durchführung von Messungen, Überwachung und Überprüfung, um die Effektivität des ISMS zu bewerten. Ziel ist es, eine kontinuierliche Verbesserung der Informationssicherheit zu erreichen.
ISO/IEC 27005	Diese Norm behandelt den risikobasierten Ansatz für Informationssicherheit. Sie stellt einen Rahmen bereit, wie Organisationen Risiken identifizieren, bewerten und behandeln können. Sie unterstützt bei der Entwicklung eines effektiven Risikomanagements für Informationssicherheit.

Diese Normen ergänzen sich gegenseitig und bieten einen ganzheitlichen Ansatz für Informationssicherheit in Organisationen. Die ISO/IEC 27001 dient als Basis für die Implementierung eines ISMS, während die ISO/IEC 27002 konkrete Empfehlungen für Sicherheitskontrollen bietet. Die ISO/IEC 27005 hilft bei der Bewertung und Behandlung von Risiken im Bereich der Informationssicherheit.

Neben der ISO/IEC 27000-Serie gibt es weitere Normen, die speziell für den Schutz kritischer Infrastrukturen relevant sind. Beispielsweise die ISO/IEC 27019 für den Energiesektor.

4.1.1.2 IEC 62443

Die Normenreihe IEC 62443 Industrial communication networks – Network and system security stellt Anforderungen zur Herstellung von IT-Sicherheit für industrielle Automatisierungs- und Kontrollsysteme (IACS: Industrial automation and control systems). Sie umfasst funktionale Anforderungen an Automatisierungslösungen, -systeme und -komponenten sowie prozessorientierte Vorgehensmodelle für den Betrieb, die Systemintegration und die Produktentwicklung. Die Norm richtet sich an Hersteller (H), Integratoren (I), Betreiber (B) und besteht aus mehreren Teilnormen.

In der folgenden Tabelle sind alle aktuell (Stand März 2024) veröffentlichten Teile aufgeführt. In der ersten Spalte steht das grundsätzliche Thema, dass die Teilenormen (zweite Spalte) behandeln. In der letzten Spalte wird die Rolle für den diese Teile relevant sind angegeben. Beispielsweise richtet sich der Teil IEC 62443-2-1 mit Anforderungen an ein IT-Sicherheitsprogramm an einen Betreiber. Dabei orientiert sich dieser Teil an der ISO/IEC 27001.

Tabelle 6 Gliederung der Norm IEC 62443 in Teilnormen

Thema	*Teilnorm*	*Rolle*
Grundlegende Konzepte, Modelle und Begriffe für die Security industrieller Automatisierungssysteme	IEC 62443-1-1 bis IEC 62443-1-4	H, I, B
Anforderungen an ein IT-Sicherheitsprogramm für IACS-Betreiber	IEC 62443-2-1	B
Methodik zur Beurteilung des Schutzes in Betrieb befindlicher industrieller Automatisierungssysteme	IEC 62443-2-2	B
Patch Management in IACS-Umgebungen	IEC 62443-2-3	B, H
Anforderungen an die Security von Dienstleistern für industrielle Automatisierungssysteme	IEC 62443-2-4	I
Security-Anforderungen auf Netzwerkebene	IEC 62443-3-1	I, B
Security-Risk assessment für System Design	IEC 62443-3-2	B
Security-Anforderungen auf Systemebene	IEC 62443-3-3	H, B
Entwicklungsprozess	IEC 62443-4-1	H
Produkt-Fähigkeiten	IEC 62443-4-2	H

> *Begriffe: IEC 62443, Security, Anforderungen - Link: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards*

4.1.1.3 NIST Cybersecurity Framework

Das NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) ist ein umfassender Leitfaden, der Organisationen dabei unterstützt, ihre Cybersicherheit zu verbessern und Risiken zu minimieren. Es besteht aus 5 Kategorien.

Tabelle 7 Kategorien des NIST Cybersecurity Framework (CSF)

Kategorie	*Beschreibung*
Identifizierung	In der Identifizierung analysiert eine Organisation ihre Daten, Systeme und Infrastruktur, um Schwachstellen und potenzielle Bedrohungen zu identifizieren.
Schutz	Im Schutzbereich werden geeignete Sicherheitsmaßnahmen implementiert, um potenzielle Risiken zu minimieren.
Erkennung	Die Erkennung beinhaltet die Einrichtung von Überwachungs- und Frühwarnsystemen, um Sicherheitsvorfälle schnell zu erkennen.
Reaktion	Bei der Reaktion entwickelt die Organisation einen Notfallplan und stellt sicher, dass sie angemessen auf Sicherheitsvorfälle reagieren kann.
Wiederherstellung	Die Wiederherstellung umfasst Aktivitäten zur Wiederherstellung von Daten und Systemen nach einem Sicherheitsvorfall, um den Geschäftsbetrieb so schnell wie möglich wieder aufzunehmen.

Das NIST CSF basiert auf bewährten Praktiken und Standards und kann an die spezifischen Bedürfnisse einer Organisation angepasst werden. Es dient als Referenzrahmen, um ein robustes Cybersicherheitsprogramm zu entwickeln und kontinuierlich zu verbessern.

Begriffe: Anforderungen, Security, Organisation, Risikomanagement, Maßnahmen - Link: https://www.nist.gov/cyberframework

4.1.1.4 NIST Special Publication 800-82 Rev. 3 – Guide to Operational Technology (OT) Security

Die NIST Special Publication 800-82 Rev. 3 bietet Leitlinien zur Cybersicherheit der Operational Technology (OT) und berücksichtigt dabei deren einzigartige Anforderungen hinsichtlich Leistungsfähigkeit, Zuverlässigkeit und Cybersicherheit. OT umfasst eine breite Palette von programmierbaren Systemen und Geräten, die mit der physischen Umgebung interagieren (oder Geräte steuern, die mit der physischen Umgebung interagieren). Diese Systeme und Geräte erfassen oder verursachen direkte Veränderungen durch die Überwachung und/oder Steuerung von Geräten, Prozessen und Ereignissen. Beispiele hierfür sind industrielle Steuerungssysteme, Gebäudeautomatisierungssysteme, Transportsysteme, Systeme zur physischen Zugangskontrolle, Systeme zur Überwachung der physischen Umgebung und Systeme zur Messung der physischen Umgebung. NIST Special Publication 800-82 Rev. 3 bietet einen Überblick über OT und typische Systemtopologien, identifiziert gemeinsame Bedrohungen und Schwachstellen dieser Systeme und empfiehlt Sicherheitsmaßnahmen zur Minimierung der damit verbundenen Risiken.

Begriffe: Maßnahmen, Konzepte - Link: https://csrc.nist.gov/pubs/sp/800/82/r3/ipd

4.1.1.5 NIST IR 8219 Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection

Industrial Control Systems werden in vielen Branchen eingesetzt, um physische Prozesse zu überwachen und zu steuern. Da ICS zunehmend kommerziell verfügbare Informationstechnologie (IT) übernehmen, um die Konnektivität von Unternehmensgeschäftssystemen und die Fernzugriffsfähigkeiten zu fördern, werden sie anfälliger für Cybersicherheitsbedrohungen. Das National Institute of Standards and Technology's National Cybersecurity Center of Excellence (NCCoE) hat in Zusammenarbeit mit NIST's Engineering Laboratory eine Reihe von Behavioral Anomaly Detection (BAD) demonstriert, um die Cybersicherheit in Fertigungsunternehmen zu unterstützen. Diese Funktionen ermöglichen es Herstellern, abweichende Bedingungen in ihrer Betriebsumgebung zu erkennen, um Malware-Angriffe und andere Bedrohungen für die Integrität kritischer Betriebsdaten zu minimieren. NIST's NCCoE und EL haben diese nachgewiesenen Fähigkeiten dem Cybersicherheitsframework zugeordnet und dokumentiert, wie dieser

Satz von standardbasierten Kontrollen viele der Sicherheitsanforderungen von Herstellern unterstützen kann. NIST IR 8219 dokumentiert die Verwendung von BAD in zwei verschiedenen, aber verwandten Demonstrationsumgebungen: einem auf Robotern basierenden Fertigungssystem und einem Prozesssteuerungssystem, das dem ähnelt, was in der chemischen Fertigungsindustrie verwendet wird.

Begriffe: Erkennung von Cyberangriffen, Security Monitoring, IDS, SIEM - Link: https://csrc.nist.gov/publications/detail/nistir/8219/final

4.1.2 Funktionale Sicherheit

4.1.2.1 IEC TR 63069 - Industrial-process measurement, control and automation - Framework for functional safety and security

Dieser technische Bericht enthält Leitlinien für die Bewertung und das Management von Risiken der funktionalen Sicherheit und der Cybersicherheit in industriellen Automatisierungs- und Steuerungssystemen. Er unterstützt Organisationen bei der Identifizierung und Bewertung potenzieller Gefahren und Bedrohungen, die sich aus dem Zusammenspiel von Funktionaler Sicherheit und Cybersicherheit ergeben. IEC TR 63069 unterstützt Organisationen bei der Implementierung von Risikomanagementprozessen, um sowohl Funktionale Sicherheit als auch Cybersicherheit auf koordinierte und integrierte Weise anzugehen.

Im Bereich Sicherheit und Gefahrenabwehr wurden zahlreiche sektorspezifische Leitfäden, Normen und technische Spezifikationen entwickelt. Ein allgemeines Rahmendokument für Sicherheit und Gefahrenabwehr wird jedoch von den Akteuren des Sektors erwartet.

Selbst die Begriffe "funktionale Sicherheit" und "Security" werden in der IEC TR 63069 teilweise mit unterschiedlicher Bedeutung verwendet. Daher kann es schwierig sein, sie gleichzeitig und umfassend auf ein Fertigungssystem anzuwenden.

Begriffe: Risiko, Security, Safety - Link: https://webstore.iec.ch/publication/31421

4.1.2.2 IEC TS 63074 - Safety of machinery - Security aspects related to functional safety of safety-related control systems

Dieser technische Bericht enthält Leitlinien zu den Lebenszyklusaspekten der Integration von Funktionaler Sicherheit und Cybersicherheit in industriellen Automatisierungs- und Steuerungssystemen. Er behandelt die Beziehungen zwischen dem Lebenszyklus aus IEC 61511 (funktionale Sicherheit für die Prozessindustrie) und IEC 62443 (Cybersicherheit für industrielle Automatisierungs- und Steuerungssysteme). IEC TR 63074 soll Organisationen dabei helfen, potenzielle Konflikte zwischen Anforderungen der Funktionalen und Cybersicherheit zu identifizieren und zu managen, um sicherzustellen, dass beide Aspekte effektiv und koordiniert behandelt werden.

IEC TR 63074:2021 gibt eine Anleitung zur Anwendung von IEC 62443 in Bezug auf Aspekte von Sicherheitsbedrohungen und Schwachstellen, die die durch Safety-Systeme implementierte und realisierte funktionale Sicherheit beeinflussen und zum Verlust der Fähigkeit führen können, den sicheren Betrieb einer Maschine aufrechtzuerhalten.

Die betrachteten Sicherheitsaspekte der Maschine mit potenziellem Bezug zu Systemen der Funktionalen Sicherheit sind

- Schwachstellen im System der Funktionalen Sicherheit, die entweder direkt oder indirekt über andere Teile der Maschine ausgenutzt werden können, was zu einer Beeinträchtigung der Funktionalen Sicherheit führen kann;
- Auswirkungen auf die Sicherheitseigenschaften und die Fähigkeit des Systems der Funktionalen Sicherheit, seine Funktion(en) ordnungsgemäß zu erfüllen;

- Definition eines typischen Anwendungsfalls und Anwendung eines entsprechenden Bedrohungsmodells.

Begriffe: Safety, Anforderungen, IEC 62443 - Link: https://webstore.iec.ch/publication/69228

4.1.2.3 IEC TS 63208 - Low-voltage switchgear and control gear - Security aspects

Diese Technische Spezifikation befasst sich mit der Anwendung von IEC 62443 im Kontext von Systemen der Funktionalen Sicherheit, insbesondere mit den Wechselwirkungen zwischen Funktionaler Sicherheit und IACS. Sie bietet eine Anleitung für die Anwendung der Konzepte und Prinzipien der IEC 62443 zur Absicherung von Sicherheitssystemen unter Beibehaltung ihrer funktionalen Sicherheit. IEC TS 63208:2020 trägt dazu bei, dass Systeme der Funktionalen Sicherheit vor Cybersicherheitsbedrohungen geschützt werden, ohne ihre Fähigkeit zur Ausführung von Sicherheitsfunktionen zu beeinträchtigen.

IEC TS 63208:2020 gilt für die sicherheitsbezogenen Hauptfunktionen von Schaltgeräten während ihres gesamten Lebenszyklus. Sie gilt für die drahtgebundene und drahtlose Datenkommunikation und die physische Zugänglichkeit der Geräte innerhalb der Grenzen der Umgebungsbedingungen.

Das Dokument soll das Bewusstsein für Sicherheitsaspekte schärfen und enthält Empfehlungen und Anforderungen für geeignete Gegenmaßnahmen gegen die Verwundbarkeit gegenüber Bedrohungen.

Begriffe: Security, Safety, IEC 62443 - Link: https://webstore.iec.ch/publication/62912

4.1.2.4 IEC 61508 - Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme

Die IEC 61508 mit dem Titel "Funktionale Sicherheit elektrischer/elektronischer/programmierbarer elektronischer sicherheitsbezogener Systeme" ist eine von der IEC entwickelte internationale Norm. Sie bietet einen umfassenden Rahmen für den Entwurf, die Implementierung, den Betrieb und die Wartung sicherheitsbezogener Systeme in verschiedenen Branchen, einschließlich der Prozess-, Transport- und Maschinenbranche. Die Norm zielt darauf ab, die funktionale Sicherheit von Geräten und Systemen zu gewährleisten, d. h. die Fähigkeit, gefährliche Ereignisse zu verhindern oder abzuschwächen und Menschen, Eigentum und die Umwelt vor Schäden zu schützen.

Begriffe: Implementierung, Betrieb, Wartung - Link: https://www.beuth.de/de/norm/din-en-61508-1/135302584

4.1.2.5 ISO/TR 22100-4:2018 - Sicherheit von Maschinen - Zusammenhang mit ISO 12100 - Teil 4: Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits- (Cybersicherheits-) Aspekte

ISO/TR 22100-4:2018 mit dem Titel " Sicherheit von Maschinen - Zusammenhang mit ISO 12100 - Teil 4: Leitlinie für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits-(Cybersicherheit-)Aspekte“ ist ein technischer Bericht, der von der ISO veröffentlicht wurde. Ziel dieses Berichts ist es, Maschinenherstellern eine Anleitung zu geben, wie sie Aspekte der Cybersicherheit im Zusammenhang mit der Maschinensicherheit berücksichtigen und dabei die Anforderungen der ISO 12100, der internationalen Norm für Maschinensicherheit, erfüllen können.

Begriffe: Safety, Security - Link: https://www.beuth.de/de/technische-regel/iso-tr-22100-4/300424281

4.1.2.6 ISA TR 84.00.9-2017 - Cybersecurity Related to the Functional Safety Lifecycle

ISA TR 84.00.9 mit dem Titel "Cybersecurity Related to the Functional Safety Lifecycle" ist ein technischer Bericht, der von der ISA veröffentlicht wurde. Dieser Bericht enthält Leitlinien für die Einbeziehung von

Überlegungen zur Cybersicherheit in den Lebenszyklus der funktionalen Sicherheit von SIS, die in industriellen Prozessbereichen eingesetzt werden.

Das Hauptziel von ISA TR 84.00.9 ist es, sicherzustellen, dass die Integrität und Zuverlässigkeit von sicherheitsgerichteten Systemen nicht durch Cybersicherheitsbedrohungen beeinträchtigt wird. Die Norm trägt der zunehmenden Vernetzung und Digitalisierung industrieller Steuerungssysteme Rechnung, die neue Risiken für die Cybersicherheit mit sich bringen, welche die funktionale Sicherheit dieser Systeme beeinträchtigen können.

ISA TR 84.00.9 steht in engem Zusammenhang mit den Normen IEC 61508 und IEC 61511, die die Anforderungen an die funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer sicherheitsrelevanter Systeme definieren. Der Bericht bietet praktische Anleitungen zur Integration von Cybersicherheitsmaßnahmen in den Lebenszyklus der funktionalen Sicherheit von sicherheitsgerichteten Systemen unter Einhaltung dieser Normen.

Begriffe: Security, Safety, Bedrohungen, Maßnahmen - Link: https://www.isa.org/products/isa-tr84-00-09-2017-cybersecurity-related-to-the-f

4.2 National

4.2.1 Cybersicherheit in der OT

4.2.1.1 BSI - Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen

Systeme zur Fertigungs- und Prozessautomatisierung werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse steuern. Dies reicht von der Energieerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zur Fabrikautomation, Verkehrsleittechnik und modernem Gebäudemanagement. Solche ICS sind zunehmend denselben Cyberangriffen ausgesetzt, wie dies in der konventionellen IT der Fall ist. Betreiber müssen sich angesichts einer zunehmenden Häufigkeit von Vorfällen und neu entdeckten Schwachstellen dringend dieser Thematik annehmen. Das Risiko und Schadenspotenzial von sowohl nicht-zielgerichteter Schadsoftware als auch von gezielten, qualitativ hochwertigen und mit signifikantem Aufwand durchgeführten spezifischen Angriffen gegen ICS muss berücksichtigt werden. Dies gilt sowohl für Systeme, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyberangriffe attackiert werden können. Im Rahmen seiner Analysen und Industriekooperationen zur Cybersicherheit hat das BSI die aktuellen Bedrohungen mit der höchsten Kritikalität zusammengestellt, denen ICS derzeit ausgesetzt sind.

Begriffe: Bedrohungen, Maßnahmen - Link: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html

4.2.1.2 Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz

Die Verordnung unterstützt Betreiber von Anlagen, Systemen oder Dienstleistungen sowie Behörden bei der Feststellung, ob ein Betrieb als Teil der kritischen Infrastruktur anzusehen ist und besondere Anforderungen erfüllen muss. Kritische Infrastrukturen sind von wesentlicher Bedeutung für die Aufrechterhaltung der Gesundheit, Sicherheit, dem wirtschaftlichen und sozialen Wohlergehen der Bevölkerungen.

Die Verordnung wurde aufgrund der Änderungen des BSI-Gesetzes durch das IT-Sicherheitsgesetz erlassen und umfasst Kriterien zur Einstufung von Anlagen der Sektoren für kritische Infrastrukturen. Regelungen zur Verbesserung der Verfügbarkeit und Sicherheit der IT-Systeme, speziell im Bereich der Kritischen Infrastrukturen, sind im IT-Sicherheitsgesetz für die betreffenden Sektoren referenziert.

4.2.2 Funktionalen Sicherheit

4.2.2.1 Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (12. BImschV)

Betriebsbereiche, in denen bestimmte gefährliche Stoffe ab festgelegten Mengenschwellen vorhanden oder vorgesehen sind, unterliegen in Deutschland der 12. BImschV. Das gilt auch für Anlagen, bei denen davon auszugehen ist, dass solche Stoffe bei einem außer Kontrolle geratenen Prozess, auch bei Lagerung, anfallen. Das BImSchG und die 12. BImSchV formulieren gegenüber dem Betreiber von genehmigungspflichtigen Anlagen bzw. Betriebsbereichen bestimmte Betreiberpflichten und dienen der Verhinderung von Störfällen und der Begrenzung von Störfallauswirkungen.

Betreiber von Betriebsbereichen haben nach § 3 der 12. BImschV die Pflicht, Vorkehrungen zu treffen, um Störfälle zu verhindern. Dabei sind als Gefahrenquelle auch „Eingriffe Unbefugter“ zu berücksichtigen. Durch Eingriffe Unbefugter in IT-/OT-Systeme können Störfälle herbeigeführt werden.

In der 12. BImschV sind jedoch nur Grundsätze für die Verhinderung und die Begrenzung von Störfällen integriert. Weiterhin sind danach bei den Gefährdungen die Eingriffe Unbefugter zu betrachten.

Der Schutz vor Eingriffen Unbefugter hatte in den 1990er und 2000er Jahren nichts mit Angriffen auf die Cybersicherheit in OT und IT zu tun, da zu diesem Zeitpunkt das Internet noch in den Anfängen steckte. Insoweit sind die Methoden auch nicht in der 12. BImschV beschrieben. Allerdings wurde schon in der ersten Fassung der 12. BImschV die Durchführung einer sicherheitstechnischen Gefahrenanalyse nach dem PAAG-Verfahren vorgesehen. Das Thema Cybersicherheit in OT und IT ist dabei nicht explizit adressiert.

> *Begriffe: Störfall, Anlagen, Prozesse - Link: https://www.gesetze-im-internet.de/bimschv_12_2000/*

4.2.2.2 Leitfaden Maßnahmen gegen Eingriffe Unbefugter KAS-51

Der Leitfaden unterstützt Betreiber von Betriebsbereichen dabei, sich gegen Eingriffe Unbefugter, durch die ernste Gefahren hervorgerufen werden können, zu schützen. Somit gibt er Leitlinien zur Erfüllung der in § 3 Abs. 2 Nr. 3 der 12. BImschV enthaltenen Betreiberpflicht zur Berücksichtigung von Eingriffen Unbefugter als Gefährdung.

Die Kommission für Anlagensicherheit (KAS) ist das Nachfolgegremium der Störfall-Kommission (SFK) und des Technischen Ausschusses für Anlagensicherheit (TAA). Ihre Aufgaben richten sich nach dem § 51a BImSchG. Sie schlägt unter anderem technische Regeln vor, die im Rahmen von Genehmigungsverfahren und sicherheitstechnischen Prüfungen Berücksichtigung finden.

Im Leitfaden KAS 44 vom November 2017 waren erstmals Leitsätze für die Abwehr von cyber-physischen Angriffen im Hinblick auf die Eingriffe Unbefugter nach 12. BImschV genannt. Der Leitfaden KAS-51 -Maßnahmen gegen Eingriffe Unbefugter- ist das jüngste Dokument in dieser Reihe. Er löst den Leitfaden SFK-GS-38 ab und integriert den KAS 41 zum Schutz vor Eingriffen Unbefugter. Hiernach ist eine Sicherungsanalyse vorgesehen und die Maßnahmen werden in organisatorische Maßnahmen (Sicherungsmanagementsystem) und anlagentechnische Maßnahmen unterschieden.

Der Leitfaden beschreibt Methoden und Maßnahmen zum Schutz vor Eingriffen Unbefugter. Dazu gehören vor allem auch Gefährdungen durch Eingriffe Unbefugter auf IT-/OT-Systeme (Cyber-Angriffe).

4.2.2.3 Technische Regel für Betriebssicherheit 1115 Teil 1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen

Die Technische Regel für Betriebssicherheit (TRBS) 1115 Teil 1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) konkretisiert Anforderungen der Betriebssicherheitsverordnung. Sie richtet sich an die sichere Verwendung von Arbeitsmitteln inklusive überwachungsbedürftiger Anlagen. Die TRBS beschreibt eine Vorgehensweise

zur Festlegung, Umsetzung und Prüfung von Cybersicherheitsmaßnahmen für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen (MSR-Einrichtungen).

Begriffe, Betriebssicherheitsverordnung, Security, Risiken, Link: https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html

4.2.2.4 Produktsicherheitsgesetz (ProdSG)

Das ProdSG und die auf der Grundlage des § 8 ProdSG erlassenen Produktsicherheitsverordnungen (ProdSV) setzen insgesamt 9 europäische Binnenmarktrichtlinien sowie die Richtlinie 2001/95/EG über die allgemeine Produktsicherheit in deutsches Recht um. Dabei enthält das ProdSG selbst Regelungen, die in allen Richtlinien gleichermaßen enthalten sind, wie z. B. allgemeine Begriffsbestimmungen (§ 1) oder die Regelungen zu den benannten Stellen (§§ 3 und 4). Diese Regelungen sind daher vor die Klammer gezogen. Die produktspezifischen Regelungen der Richtlinien (z. B. wesentliche Sicherheitsanforderungen und anzuwendende Konformitätsbewertungsverfahren) finden sich in den nachgeordneten Produktsicherheitsverordnungen (1. bis 14. ProdSV).

Begriffe - Produktionssicherheit - Link: https://www.gesetze-im-internet.de/prodsg_2021

4.2.2.5 Maschinenverordnung / Maschinenrichtlinie

Maschinen müssen in Europa den formalen sowie den grundlegenden Sicherheits- und Gesundheitsanforderungen entsprechen.

Bis 19.01.2027 ist die derzeit geltenden Maschinenrichtlinie (2006/42/EG) gültig. Danach ist die Maschinenverordnung ((EU) 2023/1230) für das Inverkehrbringen von Maschinen anzuwenden.

Beide Dokumente beschreiben wie eine Maschine auf dem Binnenmarkt bereitzustellen ist und wie mit Maschinen umgegangen wird, die nicht mit der Verordnung konform sind. Dies beinhaltet grundlegende Sicherheits- und Gesundheitsschutzanforderungen denen Maschinen entsprechen müssen.

In Anhang III der Maschinenverordnung werden grundlegende Anforderungen zur Sicherheit und zudem Gesundheitsschutz beschrieben. Diese sind von Herstellern bei Konstruktion und Bau von Maschinen zu berücksichtigen. Der Teil wurde aufgrund zunehmenden Vernetzung von Maschinen sowie dem Einsatz von künstlicher Intelligenz (KI) erweitert. In der Risikobeurteilung und bei der Risikominderung müssen Gefährdungen berücksichtigt werden, die sich durch den Einsatz von künstlicher Intelligenz und der Vernetzung heraus ergeben.

Zudem müssen Maschinen nun angemessen gegen unbeabsichtigte oder vorsätzliche Korrumpierung geschützt sein und gegen vernünftigerweise vorhersehbaren böswilligen Versuchen Dritter, die zu einer Gefährdungssituation führen, standhalten. (20)

Link: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:de:PDF & https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32023R1230

4.2.2.6 DIN EN ISO 12100

Name: DIN EN ISO 12100 Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung[1]

Die ISO 12100 spezifiziert grundlegende Anforderungen an die funktionale Sicherheit von Maschinen (z. B. Turbinen, Pumpen, Armaturenantriebe, Notstromaggregate, Rührwerke, etc.) gem. den Anforderungen der EU-Richtlinien. Wer dergleichen Anlagen oder Teile dieser Maschinen vertreibt oder ändert, wird zum

[1] https://www.beuth.de/de/norm/din-en-iso-12100/128264334

Inverkehrbringer und ist an die Anforderungen gebunden. Grundlegende IT-Security Anforderungen an die Steuerungen von Maschinen sind ebenfalls definiert.

Die ISO 12100 beschreibt ein einfaches und systematisches Verfahren, um Gefahren, die von einer Maschine ausgehen, zu identifizieren und bzgl. des Risikos abzuschätzen. Zudem erfolgt eine Gegenüberstellung zu den Maßnahmen, mit denen das Risiko minimiert werden kann. Das Kapitel 6.2.11 befasst sich mit der inhärent sicheren Konstruktion von Steuerungen und kann auch auf IT-Risiken sinngemäß angewendet werden. Z. B. sind Sicherheitssteuerungen auf Grundlage der IEC 61508 auszulegen, in der u.a. eine IT-Risikoanalyse verbindlich gefordert wird. Konkret fordert die ISO 12100 die Software einer Maschine durch geeigneten Schutz unveränderlich zu halten oder den Zugriff durch Schlösser oder Passwörter zu begrenzen.

4.2.2.7 VDI/VDE 2180 Funktionale Sicherheit in der Prozessindustrie

Diese Richtlinie basiert auf der IEC 61511 und gilt für Anlagen der Prozessindustrie, z. B. der chemischen und petrochemischen Industrie. Sie stellt eine bewährte Möglichkeit dar, die Anforderungen der 12. BlmSchV an PLT-Sicherheitseinrichtungen umzusetzen. Die Richtlinie besteht aus 3 Teilen:

- Blatt 1: Einführung, Begriffe, Konzeption
- Blatt 2: Planung, Errichtung und Betrieb von PLT-Sicherheitsfunktionen
- Blatt 3: Nachweis der Ausfallwahrscheinlichkeit im Anforderungsfall (PFD)

PLT-Sicherheitseinrichtungen kommen üblicherweise dann zum Einsatz, wenn andere Maßnahmen nicht anwendbar, nicht ausreichend oder bei vergleichbarer Risikoreduzierung nicht wirtschaftlich sind. Die Anwendung möglichst einfacher, überschaubarer und unmittelbar wirkender Maßnahmen (z. B. Sicherheitsventile, druckfeste Absicherung) führt in der Regel zu sicheren und gleichzeitig wirtschaftlichen Lösungen.

In dieser Richtlinie werden die allgemeinen Grundsätze für die Sicherung von Anlagen der Prozessindustrie mit Mitteln der PLT für den typischen Fall, dass eine PLT-Sicherheitsfunktion maximal einmal im Jahr angefordert bzw. benötigt wird, beschrieben.

Die VDI/VDE 2180 beschreibt einen möglichen Umgang mit PLT-Sicherheitseinrichtungen auf Basis der internationalen Normen und vereinfacht die diversen Möglichkeiten der entsprechenden Regelwerke.

Die Richtlinie verweist in ihrem Teil 1 auf die Notwendigkeit der Betrachtung von Risiken der IT-Security. Im Management der funktionalen Sicherheit müssen Aspekte der IT-Security in der Planung, der Beschaffung, der Validierung, im Betrieb, bei Änderungen und bei der Außerbetriebnahme berücksichtigt werden. Für die Komponenten und Schnittstellen zwischen Systemen ist zwingend eine IT-Risikobeurteilung erforderlich.

4.2.2.8 DIN EN IEC 61511

Die IEC 61511-Reihe behandelt die Anwendung von PLT-Sicherheitseinrichtungen in der Prozessindustrie. Sie thematisiert außerdem die Gefahren- und Risikoanalyse des Prozesses, die durchzuführen ist, um die Spezifikation der PLT-Sicherheitseinrichtungen daraus abzuleiten. Die Beiträge anderer Sicherheitseinrichtungen werden nur im Hinblick auf die Anforderungen an die PLT-Sicherheitseinrichtung betrachtet. Die PLT-Sicherheitseinrichtung umfasst dabei alle zur Ausführung einer PLT-Sicherheitsfunktion erforderlichen Geräte vom Sensor bis zum Aktor.

Diese Norm stellt Anforderungen zur Erreichung der erforderlichen funktionalen Sicherheit auf, legt jedoch nicht fest, wer für die Erfüllung dieser Anforderungen verantwortlich ist (beispielsweise Planung, Lieferfirmen, Betreiber, Kontraktoren). Diese Verantwortlichkeit wird den Beteiligten im Rahmen der Sicherheitsplanung, der Projektplanung, des Projektmanagements oder nationaler Vorschriften zugewiesen.

Sie ist anwendbar, wenn Geräte, die den Anforderungen der IEC 61508 Serie 2010 oder IEC 61511-1:2016 [11.5] entsprechen, in ein Gesamtsystem integriert werden, das in der Prozessindustrie eingesetzt werden soll. Sie ist nicht anwendbar, wenn Hersteller die Eignung von Geräten als PLT-Sicherheitseinrichtungen in der Prozessindustrie erklären wollen (siehe IEC 61508-2:2010 und IEC 61508-3:2010).

Die IEC verweist darauf, dass eine Risikobeurteilung hinsichtlich der IT-Security durchgeführt werden muss. Es werden einige Rahmenbedingungen zur Durchführung der Risikoanalyse definiert, im Grundsatz verweist die Norm aber auf die Anwendung der ISO/IEC 27001 und IEC 62443-2-1.

4.2.2.9 NAMUR Arbeitsblatt Nr. 163

Betriebsbereiche werden nach der 12. BImschV zunehmend intern und nach außen informationstechnisch vernetzt. Diese Netze und Systeme sind grundsätzlich als Angriffspunkte nach § 3 Absatz 2 Nummer 3 der 12. BImschV zu betrachten. Die NA 163 beschreibt ein Vorgehen, mit dem eine IT-Risikobeurteilung in nur einem Tag durchgeführt werden kann.

Wie auch die KAS-51 betrachtet die NA 163 ausschließlich potentielle Angriffe auf IT-Systeme, die sicherheitstechnische Relevanz (Funktionale Sicherheit) haben. Sie besteht aus einem beschreibenden Teil und einer Checkliste. In dem beschreibenden Teil sind Referenzarchitekturen von im OT-Netzwerk eingesetzten Sicherheitssteuerungen beschrieben, für die die Methode anwendbar ist. Mit der Checkliste kann zu je einer PLT-Sicherheitssteuerung eine IT-Risikobeurteilung durchgeführt und dokumentiert werden. Bei der Durchführung der IT-Risikoanalyse festgestellte Abweichungen zu den in der Checkliste empfohlenen Maßnahmen geben direkt Aufschluss zu konkreten Verbesserungsmaßnahmen. Bei Anwendung der NA 163 kann somit ein einheitlicher Stand der IT-Security durchgesetzt werden. Berichten von Nutzenden der NA 163 zufolge hat sich die Moderation durch mit der Methodik bereits vertrauten Personen bewährt.

https://www.namur.net/de/empfehlungen-und-arbeitsblaetter/aktuelle-nena.html

5 Funktionale Sicherheit

Funktionale Sicherheit bezeichnet die Fähigkeit eines elektrischen, elektronischen, programmierbar elektronischen Systems (E/E-System), beim Auftreten systematischer Ausfälle (z. B. fehlerhafte Systemauslegung) sowie zufälliger Hardwareausfälle (z. B. Alterung von Bauteilen) mit gefahrbringender Wirkung, einen wohl definierten sicheren Zustand einzunehmen bzw. in einem sicheren Zustand zu verharren.[2]

In diesem Kapitel wird auf die Beziehung zwischen Funktionaler Sicherheit und Cybersicherheit in der OT eingegangen. Hierbei wird erläutert, welche Auswirkungen Cyberangriffe auf Systeme der Funktionalen Sicherheit haben können und wodurch die Cyberangriffe ermöglicht werden. Auf technischer und organisatorischer Ebene wird betrachtet, inwiefern sich Funktionalen Sicherheit und Cybersicherheit in der OT grundlegend voneinander unterscheiden und inwiefern Fachexperten zur Cybersicherheit aus der OT und IT sowie der Funktionalen Sicherheit zusammenarbeiten müssen.

5.1 Unterschiede zwischen Funktionaler Sicherheit und Cybersicherheit in der OT

Funktionale Sicherheit und Cybersicherheit in der OT sind eigene umfangreiche Fachdisziplinen, die jeweils eigene Sichtweise auf die eingesetzten Systeme im ICS-Netzwerk haben.

Die Funktionale Sicherheit ist Teil der Gesamtsicherheit eines OT-Systems und sorgt dafür, dass Mensch und Umwelt vor Schaden durch OT-Systeme geschützt sind. Die Begriffe Funktionale Sicherheit und Safety werden im Dokument synonym verwendet.

Cybersicherheit dagegen schützt OT-Systeme gegen mutwillige Manipulationen, die deren bestimmungsgemäßen Gebrauch gefährden. Der Schutz zielt auf das Aufrechterhalten der Funktion des OT-Systems. Dazu gehört im Besonderen auch der Schutz der Funktionalen Sicherheit, neben der eigentlichen Funktion des OT-Systems.

In Tabelle 8 werden Funktionale Sicherheit und Cybersicherheit in der OT betrachtet und deren Unterschiede dargestellt.

Tabelle 8 Vergleich Safety und Cybersicherheit in der OT

Bereich	*Funktionale Sicherheit*	*Cybersicherheit in der OT*
Fokus	Schutz von Menschen, Umwelt und Anlagen vor Gefahren durch die OT	Schutz der OT (Infrastrukturen, Prozesse, Daten und Know-how) durch Manipulationen von außen
Ziel	Vermeidung von Unfällen	Verhinderung von unbefugtem Zugang/Zugriff, Manipulation oder Ausfall von OT-Systemen
Risikobeurteilung	Identifikation und Bewertung von Gefahren	Identifikation und Bewertung von Schwachstellen und Bedrohungen
Schutzmechanismen	Redundanz, Notabschaltung, Sicherheitsfunktionen etc.	Firewalls, Intrusion Detection Systems, Verschlüsselung, Zugriffskontrolle etc.
Standards und Normen	IEC 61508, ISO 12100 etc.	IEC 62443, NIST SP 800-82 etc.
Auswirkung von Fehlern	Gefahr für Leben, Gesundheit und Umwelt	Betriebsstörungen, Datenverlust etc.
Verantwortliche	Sicherheitsexperten, Ingenieure, Hersteller	Cybersicherheitsexperten für IT oder OT, Hersteller, Integrator, Betreiber

[2] Angelehnt an ISO 26262-Teil 1

Somit sind Funktionale Sicherheit und Cybersicherheit in der OT zwei kritische Aspekte moderner industrieller Systeme, die gemeinsam eine zentrale Rolle für den reibungslosen Betrieb und den Schutz von Mensch und Umwelt spielen.

5.2 Auswirkung von Cyberbedrohungen auf Funktionale Sicherheit

Cyberangriffe können einen Einfluss auf die Funktionale Sicherheit nehmen und zu einem Schaden für Leib und Leben führen. Ein bemerkenswertes Beispiel, das zeigt, wie wichtig es ist, Funktionalen Sicherheit und Cybersicherheit in der OT gemeinsam anzugehen, ist die TRITON-Malware[3] . Im Jahr 2017 wurde eine petrochemische Anlage in Saudi-Arabien von einer hochentwickelten Malware namens TRITON angegriffen. Diese Malware wurde speziell entwickelt, um die Schwachstellen in den SIS der Anlage auszunutzen, wodurch deren Fähigkeit, Unfälle zu verhindern, beeinträchtigt wurde und es zu schwerwiegende Folgen hätte kommen können.

In Anlehnung an NA163 kann zur Kategorisierung von Auswirkungen kompromittierter PLT-S genutzt werden.

Tabelle 9 Kategorien für Auswirkungen bei Angriffen auf Systeme der Funktionalen Sicherheit

Kategorie	*Beschreibung*	*Auswirkung*
A1	SIF löst ohne Anforderung bzw. durch vorsätzliche Herbeiführung des Anforderungsfalls aus.	Nicht gefährlich im Sinne der Funktionalen Sicherheit, aber Betriebsunterbrechung
A2	SIF deaktiviert. Auslösung findet nicht statt. Allerdings: Das gleichzeitige Eintreten des Anforderungsfalls ist ein von der Manipulation unabhängiges Zufallsereignis.	gefährlich
A3	SIF deaktiviert und vorsätzliches Herbeiführen des Anforderungsfalles durch Manipulation von einer oder mehrerer Komponenten.	gefährlich

Die Auswirkung A1 hat die Überführung des Produktionsprozesses in einen sicheren Zustand zur Folge obwohl die Prozessbedingungen dies nicht notwendig machen. Die PLT-S löst damit fälschlicherweise aus (False Positive). Dies kann beispielsweise durch eine Verschiebung der Grenzwerte in der SSPS Logik „zur sicheren Seite“, nicht Verfügbarkeit von Messwerten des Sensors oder einem DoS Angriff gegen die SSPS erreicht werden. Diese Auswirkung kann je nach Häufigkeit und Art des Produktionsprozesses finanziell beträchtliche oder gar existenzbedrohende Ausmaße annehmen. Die Wirksamkeit der Sicherheitsfunktion bleibt jedoch davon unberührt. Zudem gilt zu beachten, dass diese Auswirkung auch durch Manipulation des Produktionsprozesses erreicht werden kann. Sollte der Betreiber sich gegen diese Auswirkung schützen wollen ist der Geltungsbereich entsprechend zu fassen und Maßnahmen nicht nur für die PLT-S zu treffen.

Die Auswirkung A2 führt dazu, dass die PLT-S bei einem Anforderungsfall nicht auslöst (False Negative). Ein schadenswirksamer Erfolg einer solchen Manipulation ist von einem Zufallsereignis, welches den Anforderungsfall auslöst, abhängig. Aufgrund der niedrigen Ansprechrate (low demand) der Sicherheitsfunktion findet für gewöhnlich in vergleichsweise kurzen Zeitabständen eine Funktionsprüfung statt bei der die Manipulation mit hoher Wahrscheinlichkeit erkannt würde. Daher stellt diese Auswirkung kein zu unterstellendes abschließendes Ziel eines Cyberangriffs dar.

Bei Auswirkung A3 kann ein Angreifer sowohl den Anforderungsfall auslösen als auch das Auslösen der PLT-S verhindern. Der Angreifer ist damit in der Lage ein Schadensereignis gezielt herbeizuführen.

[3] https://scadahacker.com/library/Documents/Cyber_Events/Nozomi%20-%20TRITON%20-%20The%20First%20SIS%20Cyberattack.pdf

5.3 Einheitliche Risikoanalyse Funktionale Sicherheit und Cybersicherheit in der OT

Für die Funktionalen Sicherheit und die Cybersicherheit existieren getrennte Normen, die sich beide mit Risikomanagement befassen.

Für die Cybersicherheit in der OT wird in der IEC 62443 das Thema Risikomanagement in der Teilnorm IEC 62443-3-2 behandelt. Diese Teilnorm befasst sich mit der Identifizierung von Sicherheitsrisiken, der Bewertung von Risiken sowie der Entwicklung und Umsetzung von Sicherheitsmaßnahmen für industrielle Automatisierungssysteme. Die Teilnorm legt fest, wie das Risikomanagement im Kontext der Cybersicherheit für industrielle Automatisierungssysteme durchgeführt werden soll, um eine angemessene Sicherheitsstrategie zu entwickeln.

Für die Funktionalen Sicherheit existiert die Norm ISO 12100 mit dem Titel "Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung". Die Norm wurde entwickelt, um Organisationen dabei zu unterstützen, sicherheitsrelevante Aspekte bei der Gestaltung und Konstruktion von Maschinen zu berücksichtigen. Die Norm legt einen allgemeinen Rahmen für die Risikobeurteilung und Risikominderung fest, um potenzielle Gefahren im Zusammenhang mit Maschinen zu identifizieren und geeignete Maßnahmen zur Risikominderung zu ergreifen.

Der technische Report CLC IEC/TR 63069:2021 befasst sich mit einer einheitlichen Risikoanalyse für Funktionalen Sicherheit und Cybersicherheit in der OT. In einer derartigen Risikoanalyse wird das Gesamtrisiko beider Fachdisziplinen ermittelt.

Abbildung 10 stellt eine Vorgehensweise bei der Risikoanalyse dar, bei der Risiken für Mensch, Umfeld oder Betriebsmittel und Cybersicherheitsrisiken gemeinsame betrachtet werden. Dabei wird gezeigt, dass die Sicherheitsrisikobeurteilung in die Beurteilung der Cybersicherheit mit einfließt. Damit wird dem Schutz der Systeme der Funktionalen Sicherheit vor Cyberangriffen Rechnung getragen. Gleichzeitig werden die Anforderungen aus der Funktionalen Sicherheit kommuniziert. Dies betrifft beispielsweise Anforderungen für den Betrieb, dass eine Nothaltfunktion nicht erst eine Authentisierung erfordern darf.

Am Ende stehen entsprechende Leitlinien für die Umsetzung und den Betrieb. Auf dieser Basis letztlich auch die identifizierten Risiken beider Bereiche behandelt werden und entsprechend reduziert werden.

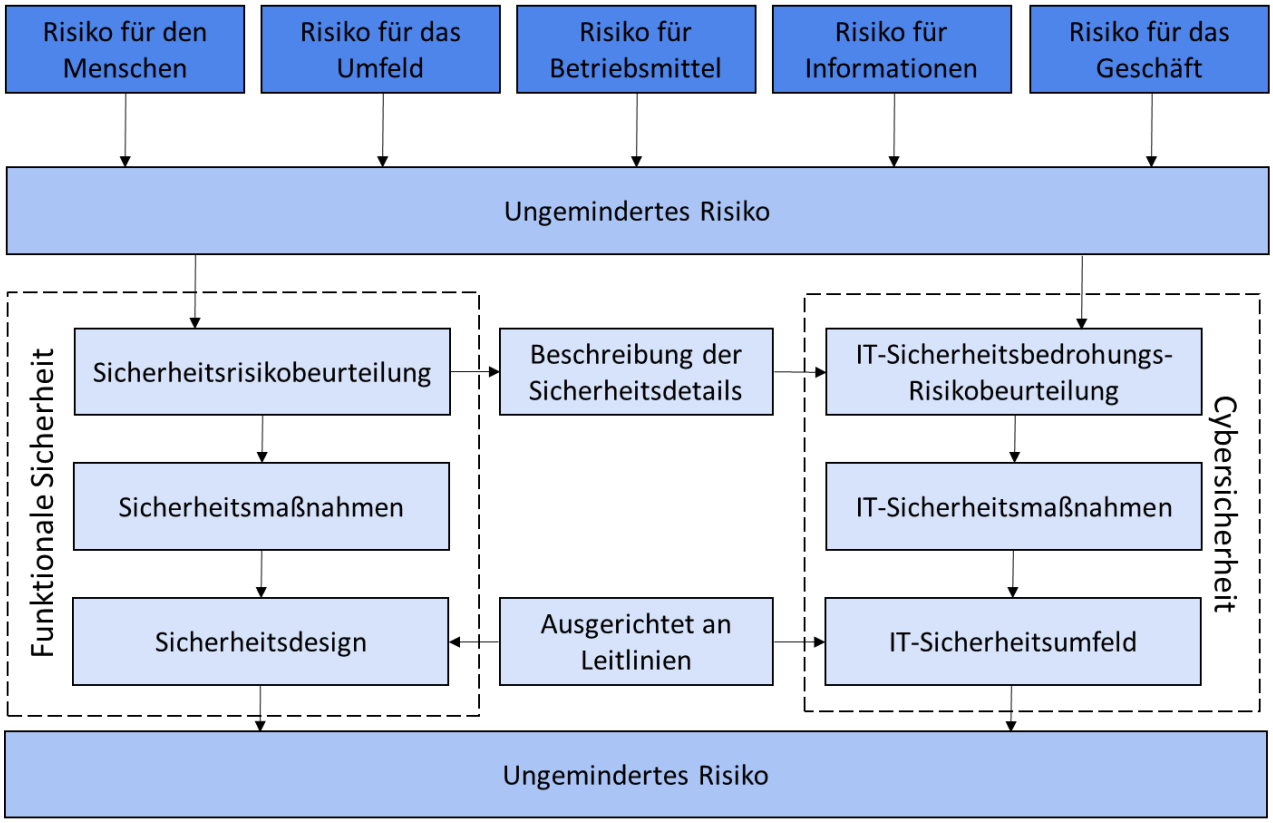

Abbildung 10 Gemeinsame Risikobetrachtung von Funktionaler Sicherheit und Cybersicherheit

5.4 Zusammenarbeit unterschiedlicher Fachexperten

Eine wichtige Voraussetzung für den erfolgreichen Umgang mit Funktionaler Sicherheit und Cybersicherheit in der OT liegt in der verstärkten interdisziplinären Zusammenarbeit von Fachexperten. In der Vergangenheit arbeiteten Teams für Cybersicherheit in der IT und OT sowie Funktionaler Sicherheit isoliert voneinander und konzentrierten sich ausschließlich auf ihre jeweiligen Bereiche, wobei es kaum bis gar keine Interaktion zwischen ihnen gab. Angesichts der sich verändernden Bedrohungslandschaft ist es jedoch erforderlich, dass diese Teams zusammenarbeiten. Im Rahmen der OT-/IT-Konvergenz streben Betreiber verstärkt eine Zusammenarbeit zwischen den Cybersicherheitsteams für IT und OT an. Die effektive Zusammenarbeit der Teams ermöglicht es den Betreibern, eine ganzheitliche Herangehensweise an die Sicherheit zu gewährleisten und potenzielle Bedrohungen proaktiv anzugehen. Nur die gemeinsame Analyse und Abstimmung können Risiken umfassend identifiziert und angemessene Maßnahmen ergriffen werden, um die Systeme widerstandsfähiger gegenüber Sicherheitsvorfällen und potenziellen Gefahren zu machen.

Um ein umfassenderes Verständnis für potenzielle Risiken und Schwachstellen in ihren Systemen zu entwickeln und robustere sowie widerstandsfähigere Sicherheitsstrategien zu implementieren, müssen Betreiber eine Kultur der Zusammenarbeit fördern. Die Zusammenarbeit sollte insbesondere in den folgenden Themenbereichen stattfinden:

- Risikomanagement
- Netzwerksegmentierung
- Monitoring der Cybersicherheit
- Incident Response Prozess

Eine erfolgreiche Zusammenarbeit bei der Betrachtung von Funktionaler Sicherheit und Cybersicherheit erfordert nicht nur die Einbeziehung der Teams zu Cybersicherheit und Funktionaler Sicherheit, sondern auch der Hersteller und Integratoren. Diese Akteure spielen eine wichtige Rolle bei der Gewährleistung der Sicherheit und Zuverlässigkeit von Systemen. Um sicherzustellen, dass Sicherheitsaspekte bereits in der Design- und Implementierungsphase berücksichtigt werden, müssen Hersteller und Integratoren mit den Betreibern und deren Fachexperten zusammenarbeiten.

6 Good-Practices zum Schutz der OT

Dieses Kapitel gibt einen Überblick über einige organisatorische, personelle und technische Good Practices für die Absicherung von OT. Diese Good Practices stellen eine Sammlung von sinnvollen Maßnahmen dar, welche sich zum einen in der Praxis bewährt haben und sich zum anderen aus den vorhandenen Standards ISO/IEC 27001, BSI IT-Grundschutz und IEC 62443 ableiten.

Die Ausführungen in diesem Kapitel adressieren die Aspekte möglichst breit. Aufgrund des Umfangs und Gegebenheiten in den jeweiligen Institutionen ist es nicht möglich, alle Maßnahmen umfänglich zu beschreiben. Daher wird auf detaillierte technische Darstellungen verzichtet.

Die Texte liefern einen ersten Anstoß und helfen bei den ersten Schritten. Für weitergehende Informationen erfolgen Verweise auf Standards und Normen, sowie Literatur.

An dieser Stelle soll daher betont werden, dass die hier beschriebenen Good Practices nur den Einstieg in einen geordneten IT- und OT- Sicherheitsprozess ermöglichen sollen. Ziel sollte es sein, ein gelebtes Informationssicherheitsmanagement auf Basis von ISO/IEC 27000-Serie, IT-Grundschutz oder IEC 62443 aufzubauen.

Eine Umsetzung aller im folgenden beschriebenen Maßnahmen ohne Betrachtung der bestehenden Risiken sollte nicht im Fokus stehen. Ein möglichst vollständiges Abarbeiten in Form von Checklisten ohne Betrachtung des Risikos und Aufwands für die jeweilige Umsetzung wird nicht durchführbar sein und ist auch nicht empfehlenswert. Vor allem im Bereich der technischen Maßnahmen ist davon auszugehen, dass Maßnahmen umgesetzt werden, die in manchen Situationen nicht praktikabel sind, evtl. über das notwendige Maß hinausschießen oder in manchen Fällen auch nicht ausreichend sind.

Bei der Umsetzung der Maßnahmen kann es aufgrund der Betriebsgröße und der Organisationsform zu gewissen Abweichungen kommen oder zu der Entscheidung, dass eine Maßnahme nicht umgesetzt wird. Hier müssen auf Aufwand, Nutzen und das verbleibende Risiko in Relation gesetzt werden. Es sollte sich hierbei jedoch um eine bewusste Entscheidung handeln, bei der man die verbleibenden Risiken ausdrücklich eingeht.

Bei den einzelnen Maßnahmen werden Verweise auf relevante Standards vorgenommen. Diese Verweise geben ggf. weitere Informationen für die Umsetzung. Alternativ kann dies genutzt werden, bei einer späteren Umsetzung auf Basis eines Standards zu erkennen, was bereits umgesetzt ist. In der Spalte „VDMA-Mindestanforderungen“ wird auf

6.1 Organisation

In diesem Abschnitt werden allgemeine organisatorische Maßnahmen beschrieben. Dies beinhaltet das Erstellen von Konzepten und Dokumentation, sowie unterstützender Prozesse.

6.1.1 Aufbau einer Cybersicherheitsorganisation

6.1.1.1 Verantwortung der Leitungsebene

Die Leitungsebene sollte sich zu einem Cybersicherheitsprogramm allgemein und für die OT bekennen.

Relevante Themen für die Leitungsebene sind allgemein:

- Sicherheitsrisiken für die Institution und deren Informationen
- Auswirkungen und Kosten im Schadensfall
- Auswirkungen von Sicherheitsvorfällen auf kritische Geschäftsprozesse
- Sicherheitsanforderungen, die sich aus gesetzlichen und vertraglichen Vorgaben ergeben
- die für eine Branche typischen Vorgehensweisen zur Informationssicherheit

- der aktuelle Stand der Cybersicherheit in der Institution mit abgeleiteten Handlungsempfehlungen (21).

Relevante Themen für die Leitungsebene in Bezug auf OT sind

- Auswirkungen von Angriffen auf die Verfügbarkeit der OT. Dies reicht von Manipulationen der Produktion über einen eingeschränkten Betrieb bis hin zum Unterbrechen der Produktion.
- Auswirkungen auf die Funktionale Sicherheit und dem Verletzen von Vorgaben aus dem Arbeitsschutz, der Arbeitssicherheit oder dem Immissionsschutz.

Tabelle 10 Weiterführende rollenspezifische Informationen aus dem Abschnitt Verantwortung der Leitungsebene

Rolle	*Hinweise*
Betreiber	Es sind Folgen durch Angriffe auf die OT (z. B. Betriebsunterbrechungen) und den Schutz von Mensch und Umwelt berücksichtigen.
Integrator/ Hersteller	Es sind Folgen durch Angriffe auf Qualität und Verfügbarkeit von Dienstleistungen und Pflichten hinsichtlich Cybersicherheit, die von den Kunden gefordert werden und zu erfüllen sind, zu berücksichtigen.

Tabelle 11 Verweise auf relevante Standards aus dem Abschnitt Verantwortung der Leitungsebene

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
1	A.5.4	01	GV.OC-01 GV.OC-02 GV.OC-03 GV.OC-04 GV.OC-04 GV.RM GV.RR-02	GOV-1 GOV-2

Weiterführende Informationen:

- Wege in die Basisabsicherung
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/WIBA/Weg_in_die_Basis_Absicherung_WiBA_node.html
- Leitfaden Basisabsicherung
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/Leitfaden-Basis-Absicherung/leitfaden-basis-absicherung_node.html

6.1.1.2 Rollen und Aufgaben

Rollen und Verantwortlichkeiten für die Cybersicherheit der OT müssen geregelt werden. Dazu sind alle an Entwicklung und Betrieb der OT beteiligten Rollen in der Organisation zu berücksichtigen. Dazu gehören beispielsweise IT-Abteilung, Produktionsleitung und Instandhaltung.

Es muss eine enge Kooperation zwischen Personen der Cybersicherheit für OT und IT stattfinden. Es wird ein gemeinsames Ziel verfolgt. Der Austausch dient dem gegenseitigen Lernen und Vermeiden von Fehlplanungen.

Schnittstellen und Aufgaben zwischen unterschiedlichen Bereichen bzw. Abteilungen müssen klar definiert werden. Ein Beispiel ist die Aufgabenverteilung zwischen klassischer IT-Abteilung und Betriebsverantwortlichen in der OT.

Tabelle 12 Weiterführende rollenspezifische Informationen aus dem Abschnitt Rollen und Aufgaben

Rolle	*Hinweise*
Betreiber	Für alle OT-Systeme (und deren Bestandteile) müssen eindeutige Verantwortliche bestimmt und deren Aufgaben beschrieben werden. Es hat sich als sinnvoll erwiesen, Rollen für bestimmte Systemgruppen oder Netzbereiche zu bestimmen, beispielsweise aufgeteilt nach den einzelnen Bereichen, sowie die Instandhaltung einzubinden.
Integrator	Bereiche in denen Rollen zur Cybersicherheit benannt werden müssen, sind beispielsweise die Entwicklung, Integration der OT-Systeme für Kunden, Dienstleistungen für Wartung und Instandhaltung (zusätzlich zur IT im allgemeinen).
Hersteller	Bereiche in denen Rollen zur Cybersicherheit benannt werden müssen, sind beispielsweise Entwicklung und Support für die OT-Komponenten (zusätzlich zur IT im allgemeinen).

Tabelle 13 Verweise auf relevante Standards aus dem Abschnitt Rollen und Aufgaben

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
1	A.5.2	02-1	GV.RR-02	-

6.1.1.3 Ressourcen

Verantwortlichen Personen müssen ausreichend Ressourcen für das Erfüllen der Aufgaben zur Cybersicherheit in der OT zur Verfügung stehen. Dies gilt, je nach Zuständigkeit, für Zeit- und Sachressourcen.

Tabelle 14 Weiterführende rollenspezifische Informationen aus dem Abschnitt Ressourcen

Rolle	*Hinweise*
Betreiber	Zu berücksichtigende Aufwände sind beispielsweise einmalig: • Erheben der Assets und Erstellen der Risikobewertung laufend/wiederholend beispielsweise • Aktualisieren der Dokumentation • Bewerten von Änderungen • Bewerten und Installieren von Sicherheitspatches
Integrator/ Hersteller	Zu berücksichtigende Aufwände sind beispielsweise • Planungs- und Entwicklungsphase um Architekturen hinsichtlich Cybersicherheit zu ergänzen und zu prüfen • Abnahmen und Sicherheitstests • Bewertung von neuen Schwachstellen in eingesetzten Teilkomponenten über den Lebenszyklus der Komponente • Information der Kunden

Tabelle 15 Verweise auf relevante Standards aus dem Abschnitt Ressourcen

ICS-Security-Kompendium (2013)	*ISO/IEC ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
1	-	02-2	GV.RR-03	-

6.1.1.4 Betrachtungsgegenstand

In den Cybersicherheitskonzepten sollten die OT-Systeme mit allen Abhängigkeiten betrachtet werden. Durch die zunehmenden Verbindungen oder Zugriffsmöglichkeiten der Systeme untereinander und den Datenaustausch kann der Ausfall eines Subsystems schnell auch andere Systeme innerhalb der OT betreffen.

Beispielsweise kann durch den alleinigen Fokus auf Safety-Systeme der Blick auf die Abhängigkeiten der entsprechenden Engineeringsysteme verloren gehen.

Tabelle 16 Weiterführende rollenspezifische Informationen aus dem Abschnitt Betrachtungsgegenstand

Rolle	*Hinweise*
Betreiber	Cybersicherheitskonzepte und -maßnahmen sind nicht nur auf einzelne Teilbereiche der OT (z. B. Funktionale Sicherheit) zu beschränken. Es sind auch abhängige und verbundene Systeme betrachten.
Integrator Hersteller	Integratoren sollten eine gründliche Bewertung und Risikoanalyse der Cybersicherheitsrisiken durchführen, um potenzielle Schwachstellen in den integrierten Systemen zu identifizieren. Dies umfasst eine Bewertung der Cybersicherheitsanforderungen, die Identifizierung möglicher Angriffsvektoren und die Entwicklung geeigneter Cybersicherheitsmaßnahmen zur Minimierung dieser Risiken. Abhängigkeiten innerhalb eines OT-Systems und von Drittsystemen sollten dokumentiert werden.

Tabelle 17 Verweise auf relevante Standards aus dem Abschnitt Betrachtungsgegenstand

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.5.1	-	-	GOV-2

6.1.2 Dokumentation

6.1.2.1 Liste der OT-Systeme und installierten Anwendungen

Die eingesetzten Systeme und Komponenten in der OT müssen erfasst werden. Dazu zählen alle Systeme, Geräte und Software, die zur Steuerung notwendig sind. Dies umfasst auch die Safety-Systeme. Zudem sollten auch weitere Abhängigkeiten erfasst werden (z. B. Verzeichnisdienste oder ERP-Systeme), die nicht direkt in der OT betrieben werden.

Die Liste ist die Grundlage für viele weitere Prozesse. Die Liste muss im gesamten Lebenszyklus aktualisiert und gepflegt werden (beginnend bei den Vorgaben an Lieferanten und Hersteller bis zur Aussonderung).

Die Liste sollte beispielsweise folgende Eigenschaften dokumentieren:

- Name & Bezeichnungen der OT-Komponente / des OT-Systems,
- Funktionaler Name, Gerätename,
- Hersteller und Gerätetyp (z. B. eindeutiger Produktidentifikator),
- Versionen von Hardware, Firmware, Betriebssystem oder Software,
- Netzwerkinformationen (z. B. FQDN, (Fully Qualified Domain Name), DNS-Bezeichnung, MAC-Adresse(n), IP-Adresse(n)),
- Zuständiges Personal mit hinterlegten Kontaktdaten (ggf. auch Servicezeiten),
- Physischer Aufstellungsort (kann auch im Netzplan dokumentiert werden),
- Konfiguration,
- Datum der letzten Prüfung auf Schadsoftware (z. B. täglich automatisiert, manuell am Datum),
- Backupintervall (vollständig und inkrementell), Umfang der Datensicherung und die zuletzt durchgeführte Datensicherung,
- Lebenszyklusstatus,

- Datum für End-of-Support und End-of-Life oder
- Informationsquelle für Security-Advisories und Updates.

Tabelle 18 Weiterführende rollenspezifische Informationen aus dem Abschnitt Liste der OT-Systeme und installierten Anwendungen

Rolle	*Hinweise*
Betreiber	Informationen zu im Einsatz befindlichen Anlagen und Maschinen müssen erfasst werden. Auch deren Komponenten sollten erfasst werden, sofern der Betreiber Zugriff und Einfluss auf diese hat. Gerade zu Beginn kann ein schrittweises Erfassen helfen den Aufwand zu begrenzen.
Integrator	In einer komplexeren Anlage müssen die verwendeten Komponenten, deren Konfiguration und Zusammenwirken erfasst werden.
Hersteller	Da Softwareanteile von OT-Komponenten in der Regel aus weiteren Unterkomponenten (z. B. Bibliotheken) unterschiedlichster Quellen besteht, muss durch den Hersteller eine Liste der eingesetzten Softwarekomponenten (SBOM) geführt werden.

Tabelle 19 Verweise auf relevante Standards aus dem Abschnitt Liste der OT-Systeme und installierten Anwendungen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
5	A.5.9	-	ID.AM-01 ID.AM-02 ID.AM-07	AMS-1 AMS-2

Weiterführende Informationen:

- TR SBOM
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html

6.1.2.2 Netzplan

Die Netzstruktur in der OT muss in einem physischen und einem logischen Netzplan dokumentiert werden.

Der physische Plan zeigt die Orte und Infrastruktur der OT, z. B. Kabel, Gebäude, Funkverbindungen. Insbesondere wird die tatsächliche, physikalische Beziehung zwischen den Geräten/Komponenten, aus denen das Netzwerk besteht, skizziert. Er enthält u.a.

- Gerätename bzw. Verknüpfung zur Liste der OT-Systeme,
- Gebäude, Raum, Schrank,
- Ports an Switchen/Routern.

Der logische Netzplan stellt die physischen Gegebenheiten nicht dar, sondern fokussiert auf die strukturelle Sicht und die Sicherheitszonen. Er stellt die Kommunikationsverbindungen zwischen den Systemen dar.

Er enthält u.a.

- Gerätename bzw. Verknüpfung zur Liste der OT-Systeme und
- IP-Netzadressen, Netzmasken, VLAN (z. B. 192.168.1.0/24),
- Schnittstellen zwischen den Segmenten und am Perimeter.

Da die Pläne sehr umfangreich werden können, hat sich es bewährt nicht jedes System einzutragen, sondern gleichartige Systeme zu gruppieren. Im IT-Grundschutz (BSI-Standard 200-2) nennt sich das Ergebnis dann

„Bereinigter Netzplan“. Vorteil ist, dass dieser einen schnellen Überblick über die Infrastruktur (Scope) und dessen Schnittstellen (Perimeter) bietet.

Die technische Dokumentation muss im gesamten Lebenszyklus aktualisiert und gepflegt werden (beginnend bei den Vorgaben an Lieferanten und Hersteller).

Tabelle 20 Weiterführende rollenspezifische Informationen aus dem Abschnitt Netzplan

Rolle	*Hinweise*
Betreiber	Der Netzplan umfasst das Netzwerk in der OT und die dort angeschlossenen Komponenten, Anlagen und Maschinen, sowie die Verbindungen zur IT und anderen Netzen (z. B. Internet).
Integrator	Die Verbindungen innerhalb einer Anlage/Maschine sind zu erfassen. Bei der Weitergabe an den Betreiber ist zu prüfen, welche Informationen von diesem relevant sind.
Hersteller	-

Tabelle 21 Verweise auf relevante Standards aus dem Abschnitt Netzplan

ICS-Security-Kompendium (2013)	*2023*	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
4	12	A.8.21		ID.AM-03	-

Weiterführende Informationen:

- BSI Standard 200-2, Abschnitt 8.1 Strukturanalyse https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf

6.1.2.3 Kommunikationsverbindungen

Neben dem Netzplan müssen auch die Kommunikationsverbindungen erfasst werden. Der Netzplan erfasst die Netzwerkstruktur und beschreibt die grundsätzlich möglichen Kommunikationswege. Die Kommunikationsverbindungen beschreiben die tatsächlichen Kommunikationsvorgänge.

Für alle Kommunikationsverbindungen sollte erfasst werden,

- welche Komponenten miteinander kommunizieren,
- welches Protokoll zum Einsatz kommt und
- welchen Zweck diese Verbindung hat.

Diese Informationen dienen als Grundlage für das Segmentieren der Netze und zur Konfiguration der Firewalls. Auf diese Weise kann nachvollzogen werden, welche Verbindungen notwendig sind und die Kommunikation kann auf das notwendige Minimum beschränkt und überwacht werden.

Die Dokumentation sollte im gesamten Lebenszyklus aktualisiert und gepflegt werden (beginnend bei den Vorgaben an Lieferanten und Hersteller).

Tabelle 22 Weiterführende rollenspezifische Informationen aus dem Abschnitt Kommunikationsverbindungen

Rolle	*Hinweise*
Betreiber	Die Kommunikationsverbindungen zwischen allen Systemen in der OT, sowie zur IT und auch zu Dienstleistern sind zu erfassen.
Integrator	Der Integrator muss dokumentieren, welche Verbindungen zur Anlage bzw. von der Anlage aufgebaut werden und diese Informationen an den Betreiber weitergeben.
Hersteller	Es müssen alle standardmäßig aktivierten Verbindungen dokumentiert sein.

Tabelle 23 Verweise auf relevante Standards aus dem Abschnitt Kommunikationsverbindungen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
4	A.8.21	-	ID.AM-03	-

6.1.2.4 Risikoanalyse

Auf Basis der Liste der OT-Systeme und installierten Anwendungen, des Netzplans, der Kommunikationsverbindungen und deren Funktion sollte eine Bewertung der möglichen Risiken erfolgen. Dabei sollte in einem ersten Schritt betrachtet werden, welche Folgen ein Ausfall und eine Manipulation haben kann. In einem zweiten Schritt sollte betrachtet werden, auf welchen Wegen der Ausfall oder eine Manipulation herbeigeführt werden kann und welche Voraussetzungen hierzu erfüllt sein müssen.

Die Risikoanalyse kann ebenfalls schrittweise erweitert und verfeinert werden. Ähnlich wie dies mit den Assetlisten erfolgt, um den initialen Aufwand gering zu halten und auf eine kontinuierliche Verbesserung zu setzen. Es kann daher damit begonnen werden, auch wenn die Liste der OT-Systeme noch nicht vollständig vorhanden ist. Werden neue Systeme hinzugefügt, ist die Risikoanalyse entsprechend zu erweitern.

Mögliche Risiken sind an die verantwortlichen Personen zu kommunizieren. Dort hat eine Abwägung zu erfolgen, ob die Risiken tragbar sind oder mitigierende Maßnahmen ergriffen werden müssen.

Tabelle 24 Weiterführende rollenspezifische Informationen aus dem Abschnitt Risikoanalyse

Rolle	*Hinweise*
Betreiber	Im Ergebnis sollten die Auswirkungen von Ausfall und Manipulationen von einzelnen Systemen auf das Gesamtsystem bekannt sein. Auswirkungen können ein Stillstand der Produktion oder eine Beeinträchtigung der Safety sein. Entsprechend dieser Ergebnisse erfolgt eine Priorisierung der Systeme, welche zuerst geschützt werden sollten.
Integrator	Ergebnisse der Risikoanalyse sollten in das Design der Anlagen, Maschinen und Dienstleistungen einfließen. Mögliche Risiken sind bei Maschinen und Anlagen ein Ausfall oder eine beeinträchtigte Safety. Bei Dienstleistungen kann es der Ausfall dieser Leistung sein oder mögliche Angriffe auf Kunden über die Systeme des Integrators.
Hersteller	Ergebnisse der Risikoanalyse sollten in das Design und die angebotenen Sicherheitsfunktionen eingehen. Diese hängen stark von der angedachten Einsatzumgebung ab. Es sollte realistisch geplant werden und nicht von einer idealisierten Umgebung ausgegangen werden und in einem gewissen Maß (wie auch in der Funktionalen Sicherheit) von einer vorhersehbaren Fehlanwendung durch die Kunden ausgegangen werden. Hinweise zu relevanten Risiken für die Kunden sind entsprechend in den Handbüchern zu dokumentieren.

Tabelle 25 Verweise auf relevante Standards aus dem Abschnitt Risikoanalyse

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	-	-	GV.RM-01 GV.RM-02 GV.RM-03 GV.RM-04 GV.RM-05 GV.RM-06 GV.RM-07 ID.RA-04 ID.RA-05	SRM-1 SRM-2 SIK-1 SIK-2 SIK-3 SCS-1

6.1.2.5 Administrations- und Benutzerhandbücher

Für einen sicheren Einsatz und Betrieb muss eine ausreichende Dokumentation zu den Komponenten und Systemen vorhanden sein. Die Dokumente sollten dabei folgende Punkte zur Cybersicherheit abdecken:

- Anweisungen zur Härtung spezifischer Anwendungen,
- Anweisungen zur (sicheren) Konfiguration,
- spezifische Risiken (z. B. bei der Aktivierung einer bestimmten Konfiguration),
- Systemwiederherstellung (zur Notfallvorsorge).

Integratoren und Hersteller sollten zwischen interner und externer Dokumentation unterscheiden. Interne Dokumentation umfasst Entwicklungs- und Designentscheidungen und Risikobewertungen. Externe Dokumentation sind Benutzerhandbücher, die an Kunden herausgegeben werden. Diese Dokumente enthalten Anweisungen für den sicheren Einsatz. Dazu gehören beispielsweise:

- die verfügbaren Schnittstellen und Dienste (unterteilt in inaktiv und aktiv),
- Auflistung der Anforderungen an alle zum ordnungsgemäßen Funktionieren des Gesamtsystems notwendigen Ressourcen / Systeme,
- für die Cybersicherheit notwendige organisatorische und technische Maßnahmen,
- Dokumentation sämtlicher Produktfunktionen (insbesondere mit Bezug zur Cybersicherheit)
- Anleitungen für eine sichere Inbetriebnahme (z. B. Konfiguration von Diensten, Vergabe von Rechten, Authentisierungsmaßnahmen),
- potentielle Risiken bei verschiedenen Konfigurationen
- sowie Hinweise zu weiteren Cybersicherheitsmaßnahmen und -informationen.

Tabelle 26 Weiterführende rollenspezifische Informationen aus dem Abschnitt Administrations- und Benutzerhandbücher

Rolle	*Hinweise*
Betreiber	Es sind alle Informationen für das Aufrechterhalten des laufenden Betriebs sowie zur Reaktion auf Probleme und Angriffe zu erfassen. Kommt es zu Ausfällen beim Personal (z. B. krankheitsbedingt oder aufgrund eines Weggangs), muss sichergestellt sein, dass die benötigten Informationen weiterhin im Unternehmen verfügbar und für das Personal zugänglich sind. Weitere vertrauliche Dokumente sind u.a. Auditberichte.
Integrator	Entwicklungsdokumentation und relevante Informationen für den Betreiber.
Hersteller	Entwicklungsdokumentation und relevante Informationen für Integratoren & Betreiber.

Tabelle 27 Verweise auf relevante Standards aus dem Abschnitt Administrations- und Benutzerhandbücher

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
6	A.5.10 A.5.37	-	-	SCS-7

Weiterführende Informationen:

- Traffic Light Protocol zur Einstufung von Dokumenten
  https://www.first.org/tlp/

6.1.2.6 Kontaktstelle für Cybersicherheit

Es sollte eine Kontaktstelle zur Cybersicherheit (allgemein und für die OT) innerhalb der Institution vorhanden sein. An diese Stelle können Cybersicherheitsvorfälle und -auffälligkeiten gemeldet werden

Das Personal sollte über diese Stelle informiert sein.

Zusätzlich sollte auch für Externe eine Möglichkeit zum Kontakt vorhanden sein, um Meldungen zur Cybersicherheit abgeben zu können. Auf diese Weise kann diese Meldungen schnell reagiert werden.

Tabelle 28 Weiterführende rollenspezifische Informationen aus dem Abschnitt Kontaktstelle für Cybersicherheit

Rolle	*Hinweise*
Betreiber	Kontaktstelle dient primär dem eigenen Personal als Ansprechstelle oder Externen um Auffälligkeiten mit dem Betrieb zu melden.
Integrator/ Hersteller	Kontaktstelle dient dem eigenen Personal als Ansprechstelle oder Externen um Auffälligkeiten mit dem Betrieb zu melden. Zusätzlich können externe Personen auch Meldungen zu Schwachstellen in Diensten, OT-Systemen und OT-Komponenten melden. Die im Rahmen des Schwachstellenmanagement behandelt werden sollten.

Tabelle 29 Verweise auf relevante Standards aus dem Abschnitt Kontaktstelle für Cybersicherheit

ICS-Security-Kompendium (2013)	*27001*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	-	03	-	-

Weitere Informationen:

- Empfehlung zum Veröffentlichen von Ansprechkontakten zur Cybersicher mittels security.txt https://securitytxt.org/

6.1.2.7 Kontakte zu Behörden & Dienstleistern

Bei Störungen in der OT kann es sich um meldepflichtige Sicherheitsvorfälle handeln. Es sollte daher im Vorfeld geprüft werden, ob es im Kontext des Betriebes der OT zu meldepflichtigen Ereignissen kommen kann. Ist dies der Fall, so sind die Kriterien für ein meldepflichtiges Ereignis zu dokumentieren und in den Incident Response Plan aufzunehmen.

Zudem sollten Kontaktdaten zu den Strafverfolgungsbehörden erfasst werden, da diese Hinweise beim Bewältigen eines Angriffs liefern können.

Gleiches gilt für Kontakte zu Dienstleistern, die bei einem Vorfall unterstützen können. Hierbei sollte bereits über entsprechende Verträge nachgedacht werden.

Die Informationen sollten in aktueller Form auch in Papier vorliegen, um auch bei einem Angriff und ggf. damit verbundenen Abschaltung der IT verfügbar zu sein.

Tabelle 30 Verweise auf relevante Standards aus dem Abschnitt Kontakte zu Behörden & Dienstleistern

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.5.5 A.5.6	-	-	-

Weiterführende Informationen:

- Zusammenarbeit mit der Polizei https://www.allianz-fuer-cybersicherheit.de/dok/6643392

6.1.3 Beschaffung

6.1.3.1 Cybersicherheitsanforderungen an Lieferanten & Dienstleister

Bei der Beschaffung von Komponenten, Systemen und Dienstleistungen für die OT sollte Cybersicherheit ein Teil der Anforderungen sein, die an den Lieferanten bzw. Dienstleister gestellt werden. Sie enthalten unter anderem:

- Rahmenbedingungen für den späteren Einsatz:
  - Einsatzumgebung der Komponente oder Systeme (z. B. räumliche Gegebenheiten, physikalische Aspekte, Klima)
  - Beschreibung des geplanten Nutzungsprofils
- Vorgaben für Funktionsumfang
  - Anforderungen an Schnittstellen zu Verzeichnisdiensten, Zeitsynchronisation, Log-Servern, Netzwerkanbindung, Fernwartung oder Steuerung, drahtlose Kommunikationsanforderungen, usw.
  - Vorgaben für Authentifizierung / Autorisierung
  - Vorgaben bezüglich Datensicherheit und Verschlüsselung
  - Datenschutzanforderungen
  - Vorgaben bezüglich zu Fähigkeiten zur Detektion und Reaktion wie zum Beispiel
    - die Verwendung von Mirrorports zum Ausleiten von Daten,
    - Komponenten mit aussagekräftiger und dokumentierter Protokollierung und
    - standardisierte Schnittstellen für die Protokollierung (z. B. Syslog, REST)
  - Mindestvorgaben für das zu erreichende Cybersicherheitsniveau
  - Anforderungen und Umfang des erlaubten Fernzugriffs oder der Kommunikation mit externen Dienstleister- oder Herstellersystemen
- Anforderungen für den Betrieb
  - Bereitstellungszeitraum für Aktualisierungen (Patches) und Reaktionszeiten bezüglich Schwachstellenbehebung.
  - Bereitstellen von Security-Advisories mittels Common Security Advisory Framework
- Bewertung der Kritikalität des Lieferanten bzw. Dienstleisters, sowie bestehender Risiken

Tabelle 31 Weiterführende rollenspezifische Informationen aus dem Abschnitt Cybersicherheitsanforderungen an Lieferanten & Dienstleister

Rolle	*Hinweise*
Betreiber	Die Kommunikationsverbindungen zwischen allen Systemen in der OT, sowie zur IT und auch Dienstleistern sind zu erfassen.
Integrator	Der Integrator muss dokumentieren, welche Verbindungen zur Anlage bzw. von der Anlage aufgebaut werden und diese Informationen an den Betreiber weitergeben.
Hersteller	Es müssen alle standardmäßig aktivierten Verbindungen dokumentiert sein.

Tabelle 32 Verweise auf relevante Standards aus dem Abschnitt Cybersicherheitsanforderungen an Lieferanten & Dienstleister

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
20	A.5.19 A.5.20 A.5.21	-	GV.SC-01 GV.SC-02 GV.SC-03 GV.SC-04 GV.SC-05 GV.SC-09	SCS-2 SCS-3 SCS-4

Weiterführende Informationen:

- VDMA Position: Cybersecurity - Betreiber- und Arbeitgeberpflichten (https://www.vdma.org/documents/34570/0/VDMA%20Position%20Cybersecurity%20-%20Betreiber-%20und%20Arbeitgeberpflichten.pdf/0e25e796-a169-1d79-29fa-6278c03d9058?filename=VDMA%20Position%20Cybersecurity%20-%20Betreiber-%20und%20Arbeitgeberpflichten.pdf)
- Mindestempfehlungen zur Cybersicherheit in der Supply Chain (https://www.vdma.org/documents/34570/12205854/VDMA_Mindestempfehlungen_Security_Supply_Chain.pdf/585ae9fc-0ab9-a8e5-1ee8-79dac978f286?filename=VDMA_Mindestempfehlungen_Security_Supply_Chain.pdf)
- CSAF - Common Security Advisory Framework
  https://bsi.bund.de/csaf

6.1.3.2 Qualitäts- und Sicherheitstests im Rahmen der Beschaffung und Entwicklung

Im Rahmen von Abnahme- und Qualitätstests sollte auch die Cybersicherheit berücksichtigt werden. Eine solche Überprüfung ist in der Regel sehr aufwändig und benötigt spezielles ausgebildetes Personal und u.U. spezielle Hardware.

Der Umfang der Tests kann dabei variieren. Es können zudem auch Testergebnisse der Lieferanten als Nachweise dienen. Wenn ein Hersteller beispielsweise einen zertifizierten Entwicklungsprozess hat und bereits entwicklungsbegleitende Tests durchführt, kann prinzipiell davon ausgegangen werden, dass bereits eine gewisse Qualität vorhanden ist.

Tabelle 33 Weiterführende rollenspezifische Informationen aus dem Abschnitt Qualitäts- und Sicherheitstests im Rahmen der Beschaffung und Entwicklung

Rolle	*Hinweise*
Betreiber	Dies kann für Maschinen/Anlagen beispielsweise im Rahmen des SAT erfolgen. Des Weiteren kann dies dazu dienen, die umgesetzten Maßnahmen auf Wirksamkeit zu prüfen. Für Betreiber ist dies eine fortgeschrittene Maßnahme.
Integrator	Dies kann im Rahmen des FAT erfolgen, um dem Betreiber bereits Nachweise bezüglich Cybersicherheit vorzulegen.
Hersteller	Dies kann im Rahmen des Entwicklungs- und Freigabeprozess erfolgen und als Nachweis dienen.

Tabelle 34 Verweise auf relevante Standards aus dem Abschnitt Qualitäts- und Sicherheitstests im Rahmen der Beschaffung und Entwicklung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.5.20 A.5.21 A.8.29	-	ID.IM-02	SCS-5

6.1.3.3 Auswahl und Integration von Systemen, Komponenten und Dienstleistern

Es sollte ein Prozess implementiert werden, der sicherstellt, dass Systeme, Komponenten und Dienstleister die erforderlichen Maßnahmen zur Cybersicherheit umsetzen. Ziel ist sich vor Angriffen über die Lieferkette oder Dienstleister zu schützen. Die Bandbreite reicht hier von einfachen vertraglichen Regelungen über das Einfordern von Auditberichten bis hin zu eigenen Audits bei den Lieferanten.

Ergebnisse interner Audits und Zertifizierungen von Integratoren und Hersteller können als Nachweise dienen. Auf diese Weise können Aufwände auf beiden Seiten (Beschaffender und Lieferant) reduziert werden. Bei den Nachweisen ist zu prüfen, dass Audits bzw. Zertifizierungen die relevanten Bereiche erfasst haben. Beispielsweise, dass bei einem Zertifikat nach ISO/IEC 27001 eines Integrators, der Geltungsbereich auch den Servicebereich umfasst und nicht nur die Bürosysteme von Verwaltung und Vertrieb.

Dies hängt stark mit den Anforderungen zur

- Mitteilung der Cybersicherheitsanforderungen an den Lieferanten
- Entwicklung von Komponenten

zusammen.

Tabelle 35 Weiterführende rollenspezifische Informationen aus dem Abschnitt Auswahl und Integration von Systemen, Komponenten und Dienstleistern

Rolle	*Hinweise*
Betreiber/Integrator/Hersteller	Es sollten Nachweise und Informationen zur Umsetzung von Prozessen zur Cybersicherheit von Integratoren und Herstellern eingefordert werden.

Tabelle 36 Verweise auf relevante Standards aus dem Abschnitt Auswahl und Integration von Systemen, Komponenten und Dienstleistern

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.5.22 A.5.23	-	GV.SC-05 GV.SC-10	SCS-4

Weitere Informationen:

- VDMA Position: Cybersecurity - Betreiber- und Arbeitgeberpflichten https://www.vdma.org/documents/34570/0/VDMA%20Position%20Cybersecurity%20-%20Betreiber-%20und%20Arbeitgeberpflichten.pdf/0e25e796-a169-1d79-29fa-6278c03d9058?filename=VDMA%20Position%20Cybersecurity%20-%20Betreiber-%20und%20Arbeitgeberpflichten.pdf
- Mindestempfehlungen zu Security in der Supply Chain (https://www.vdma.org/documents/34570/12205854/VDMA_Mindestempfehlungen_Security_Supply_Chain.pdf/585ae9fc-0ab9-a8e5-1ee8-79dac978f286?filename=VDMA_Mindestempfehlungen_Security_Supply_Chain.pdf)

6.1.4 Produktentwicklung

6.1.4.1 Entwicklung von Komponenten

Die OT ist ein Verbund verschiedener Komponenten und Systeme. Die Anpassung auf die individuellen Gegebenheiten und Bedürfnisse wird durch deren Konfiguration realisiert.

Bei der Entwicklung von Software oder Tools sollte sowohl die sichere Erstellung der Programme als auch die sichere Integration in die bestehende Umgebung durch eine Softwareentwicklungsrichtlinie (Secure Development Life Cycle) geregelt werden.

Die Entwicklungsumgebung und der Quellcode sollten vor Manipulationen geschützt werden und der Abfluss von Daten verhindert werden. Dies kann beispielsweise dadurch erfolgen, dass sich die Entwicklungsbereiche in einem getrennten Netzwerkbereich befinden.

Der Entwicklungsprozess sollte auch entsprechende Arbeiten zur Dokumentation des bestimmungsgemäßen Gebrauchs, einer sicheren Konfiguration und eines sicheren Betriebes beinhalten.

Zudem sind Schnittstellen zum Schwachstellenmanagement vorzusehen. Dies ist erforderlich um auf identifizierte Probleme in verwendeten Teilkomponenten (z. B. Softwarebibliotheken) oder eigener Software zu reagieren.

Tabelle 37 Weiterführende rollenspezifische Informationen aus dem Abschnitt Entwicklung von Komponenten

Rolle	*Hinweise*
Betreiber	-
Integrator	Entwicklungsprozess muss eine sichere Auswahl und Integration der Komponenten festlegen. Bei der Integration sind die Hinweise der Hersteller zu berücksichtigen. Vor Auslieferung sollten die Komponenten auf Schadsoftware geprüft werden.
Hersteller	Entwicklungsprozess muss einen sicheren Entwicklungszyklus beschreiben. Cyberbedrohungen und Maßnahmen sind direkt zu berücksichtigen. Vor Auslieferung sollten die Komponenten auf Schadsoftware geprüft werden.

Tabelle 38 Verweise auf relevante Standards aus dem Abschnitt Entwicklung von Komponenten

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
7	A.5.8 A.8.25 A.8.26 A.8.27 A.8.28	-	PR.PS-06	VUL-3

Weiterführende Informationen:

- Top 20 PLC Coding Practices: https://www.plc-security.com/

6.1.5 Betriebsprozesse

6.1.5.1 Kontrolle & Abstimmung der Lieferkette

Beim Betrieb von OT kann es dazu kommen, dass unterschiedliche Organisationen beteiligt sind. Es gibt beispielsweise einen Betreiber bei dem das OT-System steht. Die gesamte Wartung wird jedoch durch einen Dienstleister übernommen. Es sind hier auch komplexere Varianten möglich, bei denen mehrere OT-Systeme zusammenarbeiten und deren Betreuung von unterschiedlichen Organisationen erfolgt. Damit

hier keine Schwachstellen entstehen, sollten die Aufgaben, Verantwortung und Reaktionszeiten der jeweiligen Organisation klar definiert sein. Dies gilt auch für Meldewege.

Zudem sollten Risiken in und durch die Lieferkette betrachtet und regelmäßig bewertet werden.

Dieser Punkt grenzt sich gegenüber Rollen und Aufgaben ab, dass an dieser Stelle externe Organisationen adressiert werden.

Tabelle 39 Verweise auf relevante Standards aus dem Abschnitt Kontrolle & Abstimmung der Lieferkette

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
10	A.5.21 A.5.22 A.5.23	-	GV.SC-07	-

6.1.5.2 Änderungsmanagement

Für Änderungen an Systemen oder Komponenten sollte ein Änderungsmanagement (alternative Begriffe: Changemanagement, Management of change) etabliert werden. Der Prozess dient dem Koordinieren von allen Veränderungen in Systemen und Komponenten. In vielen Fällen ist ein solcher Prozess vorhanden, um auf funktionale Änderungen zu reagieren. Funktionale Änderungen und Erweiterungen an der OT sollten vor dem Umsetzen aus dem Blickwinkel Cybersicherheit betrachtet werden. Damit sollen Schwachstellen vermieden werden. Zu Änderungen gehören neben dem Austausch von Hardware auch Veränderungen an der Konfiguration oder an Steuerungsprogrammen. Alle Konfigurationsdaten sollten entsprechend gesichert werden.

Zudem gibt es auch Änderungen, die aufgrund der Cybersicherheit angestoßen werden. Dazu gehören das Beheben von entdeckten Schwachstellen, beispielsweise durch die Installation von Sicherheitsupdates. Langfristig sollten so auch Änderungen geplant werden, wenn für Geräte kein Support mehr verfügbar ist.

Alle geplanten Änderungen sollten daher von geeigneten Personen dahingehend geprüft werden, ob sie relevante Auswirkungen auf die Cybersicherheit der OT haben.

Tabelle 40 Verweise auf relevante Standards aus dem Abschnitt Änderungsmanagement

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
11	A.8.9 A.8.32	-	ID.AM-08 PR.PS-01	-

6.1.5.3 Schwachstellenmanagement

Schwachstellen in Systemen stellen ein Risiko dar, da diese von Angreifern ausgenutzt werden können. Sie sind daher ein Einstiegspunkt oder stellen eine Möglichkeit zur Ausbreitung dar. Dies gilt insbesondere für besonders exponierte Systeme, die mit Systemen in nicht oder weniger vertrauenswürdigen Netzwerken kommunizieren. Daher sollten diese so schnell wie möglich geschlossen werden. Beim Schließen der Schwachstellen spielen alle Beteiligten der Lieferkette eine Rolle.

Wenn eine Schwachstelle in einer Komponente auftritt, muss der Hersteller diese analysieren, einen Patch oder Workaround bereitstellen und seine Kunden informieren. Der Integrator muss Schwachstellen in den verbauten Komponenten berücksichtigen und Schwachstellen, die durch die Kombination in einem OT-System entstehen. Auch er muss diese analysieren, verfügbare Patches oder Workaround prüfen und installieren sowie seine Kunden informieren. Für den Betreiber gilt letztlich, dass die die Patches, Workarounds und Informationen der Hersteller und Lieferanten umsetzen muss. Er ist dabei aber auf die Informationen der Hersteller und Integratoren angewiesen.

Tabelle 41 Weiterführende rollenspezifische Informationen aus dem Abschnitt Schwachstellenmanagement

Rolle	*Hinweise*
Betreiber	Auf Basis der Liste der eingesetzten Komponenten erfolgt die Kontrolle nach veröffentlichten Security-Advisories bei den Integratoren und Herstellern. Anhand der Bewertung sind die beschriebenen Maßnahmen im Rahmen des Changemanagement einzuplanen und in der OT umzusetzen.
Integrator	Auf Basis der eingesetzten Komponenten erfolgt die Kontrolle nach Informationen zu Schwachstellen bei den entsprechenden Herstellern. Auf Basis der Konfiguration erfolgt bei bekanntgewordenen Schwachstellen eine Bewertung und es werden Handlungsempfehlungen erstellt und kommuniziert. Ggf. werden Anpassungen für die Kunden im Rahmen des Service angeboten.
Hersteller	Es sollte ein Product Security Incident Response Team (PSIRT) aufgebaut werden, dass sich um die Behandlung von Schwachstellenmeldungen in eigenen und integrierten Komponenten kümmert. Dieses ist mit dem gesamten Prozess zur Überwachung der Komponenten auf Schwachstellen, Behebung und Kommunikation an die Kunden befasst.

Tabelle 42 Verweise auf relevante Standards aus dem Abschnitt Schwachstellenmanagement

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.8.8	15-1 15-2 16 17-1 17-2	ID.RA-01 ID.RA-08	VUL-1 VUL-2

Weitergehende Informationen:

- CS 019: Handhabung von Schwachstellen https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf
- CS 027: Lebenszyklus einer Schwachstelle https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_027.html

6.1.5.4 Auditierung

Die Cybersicherheit in der OT sollte regelmäßig auditiert werden. In den Audits sollten die korrekte Umsetzung der Prozesse und Maßnahmen für Netze und Komponenten geprüft werden. Das Ziel ist mögliche Schwachstellen in den eigenen Systemen und Prozessen zu entdecken und zu beheben.

Die Ergebnisse sollten dokumentiert werden. Die Dokumentation (insbesondere wenn die Audits durch eine unabhängige Stelle durchgeführt wurden) kann auch als Nachweis in der Lieferkette verwendet werden.

In komplexen Systemen ist die Etablierung von spezialisierten Teams zur Identifikation und Bewertung möglicher Angriffsszenarien unabdingbar.

Tabelle 43 Weiterführende rollenspezifische Informationen aus dem Abschnitt Auditierung

Rolle	*Hinweise*
Betreiber	Im Fokus sollten die Betriebsprozesse stehen. Ziel ist das Umsetzen und Einhalten der Vorgaben, sowie das Identifizieren von Lücken. Eine Methodik für die Durchführung von Audits in der OT ist in Kapitel 7 Audits, Assessments und Tests beschrieben.

Rolle	*Hinweise*
Integrator	Im Fokus sollten Integrationsprozesse und Serviceprozesse stehen. Bei den Integrationsprozessen sollte die sichere Einrichtung der Anlagen betrachtet werden. Bei den Serviceprozessen sollte die Sicherheit der Kundendaten und der Services betrachtet werden. (Unabhängige) Prüfung der Anlage vor oder bei Auslieferung.
Hersteller	Im Fokus sollten Entwicklungsprozesse und Serviceprozesse stehen. Bei den Entwicklungsprozessen sollte die sichere Entwicklung von Komponenten betrachtet werden. Serviceprozesse sollten die Reaktion auf Schwachstellenmeldungen sowie das Beheben von Schwachstellen und die Information der Kunden beinhalten. (Unabhängige) Prüfung der Komponenten während oder am Ende der Entwicklung.

Tabelle 44 Verweise auf relevante Standards aus dem Abschnitt Auditierung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
17 18	A.5.35	-	-	-

6.1.5.5 Berechtigungsmanagement

Es sollte ein Prozess zum Berechtigungsmanagement für

- Zutritt (Betreten von abgegrenzten Bereichen),
- Zugang (Nutzen von Systemen und Netzen) und
- Zugriff (Nutzen von Informationen oder Daten)

umgesetzt werden.

Für Zutritt zur OT gibt es vielfach bereits Vorgaben. Beispielsweise ist der Zutritt zu Räumen mit Schaltanlagen nur einem bestimmten Personenkreis zugänglich.

Für den Zugang und Zugriff gibt teilweise auch schon Regeln. Die Umsetzung hängt jedoch stark von den gegebenen Möglichkeiten der Systeme ab. Wenn ein System keine personalisierten Benutzerkonten unterstützt und daher nur ein Gruppenkonto zur Verfügung steht, ist hier eine Einschränkung auf technischer Ebene nicht möglich. In einem solchen Fall sollte der Kreis der Berechtigten möglichst begrenzt gehalten werden.

Insbesondere bei Safety-Systemen sollte der Zugang und Zugriff eingeschränkt werden, damit Änderungen und Zugriffe nur unter bestimmten Voraussetzungen erfolgen können.

Das Berechtigungsmanagement knüpft an folgende Maßnahmen an:

- Prozesse für Einstellung, Wechsel und Ausscheiden von Personal
- Authentisierung

Tabelle 45 Verweise auf relevante Standards aus dem Abschnitt Berechtigungsmanagement

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.5.15 A.5.16 A.5.17 A.5.18	08-1 08-2	PR.AA-01 PR.AA-02 PR.AA-04 PR.AA-05	UAC-1 UAC-3

6.1.6 Notfallmanagement

6.1.6.1 Security Incident Response Plan

Fehler und Sicherheitsvorfälle (wie bspw. Cyberangriffe) können zu einer Störung des Produktionsprozesses führen und Gefährdungen von Leib, Leben und Umwelt nach sich ziehen. Eine Störung stellt dabei eine Beeinträchtigung (bis hin zur Unterbrechung) oder Qualitätsminderung des Produktionsprozesses dar. Unter Sicherheitsvorfall wird ein negatives Ereignis, das die Informationssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) beeinträchtigt, verstanden. Ein frühzeitiges Erkennen von sicherheitsrelevanten Ereignissen ist für eine rechtzeitige Reaktion erforderlich. Nur so kann ein möglicher Schaden abgewendet werden. Daher sollte im Vorfeld in einem Security Incident Response Plan eine Strategie entwickelt werden, wie sicherheitsrelevante Ereignisse erfasst und erkannt werden, welche Reaktionen erforderlich sind und wie ein sicherer Zustand wiederhergestellt werden kann.

Die wichtigsten Phasen sind

- Eindämmung und Begrenzung
- Wiederanlauf und Wiederherstellung (werden im Wiederherstellungsplan adressiert)

Cybersicherheitsvorfälle können auf Grund der Komplexität der OT den Einsatz von interdisziplinären Störungsbehebungsteams erforderlich machen. So können sich Cybersicherheitsvorfälle anfangs auch nur als scheinbar funktionale Störungen zeigen. Daher ist ein enges Verzahnen mit Instandhaltung und Wartung sinnvoll, da in diesen Bereichen Wissen zur Störungseingrenzung und -behebung vorhanden ist.

Innerhalb des Incident Response Plan ist das weitere Vorgehen möglichst detailliert aufzuführen. Für Störungsszenarien sollen für Störungsszenarien detaillierte Ablaufpläne für die Umsetzung von Sofortmaßnahmen und die Überführung der OT in einen Notbetrieb erstellen. Die notwendigen Handlungsanweisungen sollten dokumentiert sein. Dabei sollten sie so einfach wie möglich gehalten sein, damit sie auch in stressigen Situationen angewendet werden können.

Es sollten Prozeduren vorliegen, wie die OT bei Infektion (und damit verbundenem Ausfall) der IT reagiert. Dies beinhaltet mögliche Isolierung der OT von der IT bzw. die Abschaltung um Infektionen in der OT zu verhindern.

Der Plan sollte in regelmäßigen Abständen erprobt, auf Aktualität geprüft und bei Bedarf überarbeitet und angepasst werden.

Tabelle 46 Weiterführende rollenspezifische Informationen aus dem Abschnitt Security Incident Response Plan

Rolle	*Hinweise*
Betreiber	Es sind Prozesse zur Prüfung vorzusehen, entsprechende Unterlagen bereitzuhalten und auch die notwendigen Werkzeuge und Daten zur Wiederherstellung. Betreiber sollten prüfen, ob entsprechende Servicedienste mit dem Integrator vereinbart werden.
Integrator/Hersteller	Dokumentationen zum Prüfen der Integrität der OT-Systeme sind zu erstellen und ggf. zu übergeben. Informationen zum Erkennen von abweichendem Verhalten von OT-Systemen und Angebot von unterstützenden Diensten zur Reaktion können angeboten werden. Kunden (in Form von anderen Herstellern, Integratoren und Betreibern) sollten über Cybersicherheitsvorfälle oder Schwachstellen geeignet informiert werden.

Tabelle 47 Verweise auf relevante Standards aus dem Abschnitt Security Incident Response Plan

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
12	A.5.24 A.5.28 A.5.29	-	RS.MA-01 RS.MA-02 RS.MA-03 RS.MA-04 RS.MA-05 RS.AN-03 RS.CO-02	-

6.1.6.2 Wiederherstellungsplan &Business Continuity Plan

Es sollte festgelegt werden, wie grundlegende Funktionen nach einer signifikanten Störung oder einem Cybersicherheitsvorfall wiederaufgenommen werden können. Dazu sind Aktionen zu erarbeiten, die nach Eintritt einer Störung oder eines Cybersicherheitsvorfalls den Wiederanlauf in einer angemessenen Zeit sicherstellen. Dazu zählen beispielsweise Prozesse zur Datensicherung, Wiederherstellung und dem Überprüfen der Integrität von Komponenten. Weitere Aktionen können sich mit Prozeduren zur Systemeinrichtung, Reparatur defekter Komponenten und Vorhalten von Ersatzteilen als auch alternativen Kommunikations- und Steuerungsmöglichkeiten bei Ausfällen befassen.

Der Plan sollte in regelmäßigen Abständen und mindestens jährlich auf Aktualität geprüft und bei Bedarf überarbeitet werden.

Tabelle 48 Weiterführende rollenspezifische Informationen aus dem Abschnitt Wiederherstellungsplan &Business Continuity Plan

Rolle	*Hinweise*
Betreiber	Die Aufgaben überschneiden sich stark mit den klassischen Tätigkeiten der Instandhaltung in der OT. Daher kann es sinnvoll sein, die Instandhaltung zu berücksichtigen bzw. zu beteiligen.
Integrator/ Hersteller	Es sollten dabei insbesondere die Bereiche für Entwicklung, Verkauf und Servicedienste betrachtet werden. Ziel ist insbesondere wieder Kunden eine sichere Dienstleistung anbieten zu können.

Tabelle 49 Verweise auf relevante Standards aus dem Abschnitt Wiederherstellungsplan &Business Continuity Plan

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
13	A.5.26 A.5.30	-	RC.RP-02 RC.RP-03 RC.RP-04 RC.RP-05 RC.RP-06	IIM-1 AVA-1

6.2 Personal

6.2.1 Training des Personals

Das Personal (intern als auch extern) muss regelmäßig in Qualifizierungs- und Fortbildungsprogrammen das Wissen zur Cybersicherheit auffrischen und erweitern. Die Inhalte sollten sich an den fachlichen Qualifikationen und den zugeordneten Tätigkeiten orientieren. Damit sichergestellt wird, dass das Personal keine Fehlentscheidung z. B. aus Unwissenheit oder mangelnder Qualifikation trifft.

Es kann sich dabei beispielsweise um Sensibilisierungsschulungen handeln, die über relevante Bedrohungen und Schwachstellen informieren und hierfür sensibilisieren.

Das Service- und Wartungspersonal sowie Administratoren sollten durch Schulungen in die Lage versetzt werden, mögliche Schwachstellen zu identifizieren und zu bewerten sowie diesen durch angemessene Gegenmaßnahmen zu begegnen.

Tabelle 50 Weiterführende rollenspezifische Informationen aus dem Abschnitt Training des Personals

Rolle	*Hinweise*
Betreiber	Themenfelder sind der sichere Betrieb und die Administration der Anlage sowie zugehöriger Systeme. Es gilt das Personal auf die Richtlinien und Pflichten hinzuweisen und über Hintergründe aufzuklären
Integrator	Themenfelder sind der sichere Betrieb und die Administration von Servicegeräten und die sichere Entwicklung, um Fehler frühzeitig zu vermeiden. Es gilt das Personal auf die Richtlinien und Pflichten hinzuweisen und über Hintergründe aufzuklären
Hersteller	Themenfelder sind der sichere Betrieb und die Administration von Servicegeräten und die sichere Entwicklung, um Fehler frühzeitig zu vermeiden. Es gilt das Personal auf die Richtlinien und Pflichten hinzuweisen und über Hintergründe aufzuklären

Tabelle 51 Verweise auf relevante Standards aus dem Abschnitt Training des Personals

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*ISA-62443-2-1-FDIS-D04E03*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
14	A.6.3	02-3 04-1 04-2 05-1 05-2	ORG 1.4 ORG 1.5	PR.AT-01 PR.AT-02	TRA-1 TRA-2 TRA-3

6.2.2 Prozesse für Einstellung, Wechsel und Ausscheiden von Personal

Es sollten Prozesse etabliert sein, die sicherstellen, dass bei Neueinstellungen, Wechsel innerhalb des Unternehmens und bei Abgängen von Mitarbeitern das Thema Cybersicherheit behandelt wird.

Dies betrifft unter Anderem:

- das Anpassen der Berechtigungen
- Erteilung und Entzug von Berechtigungen
- Informationen zu Cybersicherheitsrichtlinien und Sensibilisierungen.

Tabelle 52 Verweise auf relevante Standards aus dem Abschnitt Prozesse für Einstellung, Wechsel und Ausscheiden von Personal

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*ISA-62443-2-1-FDIS-D04E03*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
15	A.6.1 A.6.2 A.6.4 A.6.5	-	ORG 1.2	GV.RR-04	-

6.3 Physische Sicherheit

6.3.1 Physische Absicherung

Es müssen Absicherungen der OT gegen unberechtigten physischen Zutritt und Zugang getroffen werden. Dies gilt für Gebäude, Bereiche und Räume sowie Schränke.

Grundsätzlich gilt, dass Zugang und Zutritt auf das Minimum an Personen beschränkt werden sollte. Je nach Kritikalität sollten zusätzliche Kontrollen und eine Überwachung erfolgen, um unbefugten Zutritt und Zugang zu verhindern bzw. zu erkennen und reagieren zu können. Zugang und Zutritt sollten protokolliert werden können. Es sollte das Prinzip "Zugang nur, wenn erforderlich" gelten.

Die physische Absicherung stellt bei OT-Systemen, die sich nicht auf dem Gelände der Organisation befinden und für die kein Personal vor Ort ist, eine besondere Herausforderung dar. Hier sollten zusätzliche Maßnahmen ergriffen werden.

Tabelle 53 Weiterführende rollenspezifische Informationen aus dem Abschnitt Physische Absicherung

Rolle	*Hinweise*
Betreiber	Der Fokus liegt auf dem Umsetzen des Berechtigungskonzepts und dem Überwachen der Schutzmaßnahmen.
Integrator	Die Aufgabe ist geeignete Schutzmaßnahmen zu unterstützen, ggf. bereits vorzusehen und entsprechend Hinweise für das Umsetzen zu liefern.
Hersteller	Die Aufgabe ist geeignete Schutzmaßnahmen zu unterstützen, ggf. bereits vorzusehen und entsprechend Hinweise für das Umsetzen zu liefern.

Tabelle 54 Verweise auf relevante Standards aus dem Abschnitt Physische Absicherung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
31	A.7.1 A.7.2 A.7.3 A.7.9	-	PR.AA-06 DE.CM-02	INF-1

6.3.2 Umgang mit Wechseldatenträgern

Wechseldatenträger in Form von beispielsweise USB-Sticks, mobilen Festplatten oder Speicherkarten werden häufig zum Transport von Updates, Konfigurationen oder anderen Daten genutzt. Dabei werden diese an unterschiedliche Systeme angeschlossen. Teilweise handelt es sich auch um OT-Komponenten in unterschiedlichen Unternehmen, wenn ein Servicetechniker diese einsetzt.

Für die Nutzung von Wechseldatenträgern sollten daher Regelungen für den Umgang aufgestellt und bekannt gemacht werden. Dazu gehören unter anderem:

- An welche OT-Komponenten darf ein Wechseldatenträger angeschlossen werden?
- Welche Wechseldatenträger dürfen verwendet werden?
- Welche Daten werden mit den Wechseldatenträgern transportiert?
- Wie erfolgt eine Prüfung auf mögliche Schadsoftware? Ist der Einsatz einer Wechseldatenträgerschleuse vorgesehen?

Auf den Komponenten sollte die Nutzung auf bestimmte Geräte eingeschränkt werden (sogenannte Device Control, wenn technisch möglich). Die Umsetzung ist meist mit Funktionen des Betriebssystems oder über zusätzliche Software möglich.

Tabelle 55 Verweise auf relevante Standards aus dem Abschnitt Umgang mit Wechseldatenträgern

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
66, 67	A.7.10	-	-	-

6.3.3 Entsorgung von Hardware

Es sollte ein Prozess für die Aussonderung und Entsorgung von Komponenten definiert und dokumentiert werden. Wichtig in diesem Zusammenhang ist, dass alle vertraulichen Informationen oder Konfigurationen auf dem Gerät gelöscht oder gegebenenfalls zerstört werden (z. B. mechanische Zerstörung von Festplatte oder internem Speicher), bevor dieses ausgemustert und entsorgt wird. Auch im Reparatur- bzw. Wartungsfall sollten beispielsweise Speichermedien mit vertraulichen Informationen vorher entfernt oder sicher gelöscht werden.

Mit der Entsorgung von Hardware sollten vertrauenswürdige Dienstleister beauftragt werden. Hierbei sollten die defekten Geräte bis zur Abholung so gelagert werden, dass sie vor unbefugten Zugriffen geschützt sind (z. B. durch abgeschlossene Schränke).

Tabelle 56 Verweise auf relevante Standards aus dem Abschnitt Entsorgung von Hardware

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
8	A.7.14	-	-	-

6.3.4 Einsatz von mobilen Systemen zu Wartungszwecken

Neben Wechseldatenträgern kommen häufig mobile Wartungsgeräte (wie z. B. Notebook oder Tablets) zum Einsatz.

Vor dem Einsatz eines externen Wartungsgerätes ist eine Bestandsaufnahme der mobilen Systeme erforderlich. Zu klären ist in diesem Zusammenhang:

- Welche Software ist installiert (inkl. Betriebssystem und Patches)?
- Welche Schnittstellen sind vorhanden und aktiv (insb. Mobilfunk)?
- Welcher Schutz für Schadprogramme ist installiert (sind aktuelle Signaturen vorhanden)?

Es sind geeignete Maßnahmen zum Schutz vor Schadsoftware zu treffen. Dies soll verhindern, dass eine Schadsoftware von einem OT-System zum nächsten getragen wird.

Es sind geeignete Maßnahmen zum Schutz der Vertraulichkeit und Integrität von auf dem mobilen System gespeicherten Daten zu gewährleisten. Dies soll verhindern, dass die Daten unbemerkt verändert oder in unberechtigte Hände gelangen.

Diese beiden Punkte sind insbesondere bei Arbeiten an OT-Systemen mit besonderem Schutzbedarf wichtig, um unberechtigte Änderungen zu verhindern.

Tabelle 57 Weiterführende rollenspezifische Informationen aus dem Abschnitt Einsatz von mobilen Systemen zu Wartungszwecken

Rolle	*Hinweise*
Betreiber	Unterscheiden zwischen internen und externen Geräten: • Interne Geräte: Über organisatorische Maßnahmen ist sicherzustellen, dass auf diesen Wartungsgeräten ausschließlich Software enthalten ist, die für Wartungszwecke erforderlich ist. Es sollte eine Systemhärtung durchgeführt werden. Darüber hinaus sollten diese Geräte regelmäßig mit Sicherheitsupdates versorgt und auf Schadsoftware untersucht werden. • Externe Geräte: Es empfiehlt sich zunächst der Abschluss eines entsprechenden Vertrages mit dem Serviceanbieter, in welchem das Thema Cybersicherheit vertraglich geregelt ist. Insbesondere gilt dies für Schutzmaßnahmen bzgl. der mobilen Systeme und des Verhaltens des Personals damit.
Integrator	Auf den Wartungsgeräten sollte ausschließlich Software enthalten sein, die für Wartungszwecke erforderlich ist. Es sollte eine Systemhärtung durchgeführt werden. Darüber hinaus sollten diese Geräte regelmäßig mit Sicherheitsupdates versorgt und auf Schadsoftware untersucht werden. Entsprechende Maßnahmen und Überprüfungen sollten dokumentiert werden.
Hersteller	-

Tabelle 58 Verweise auf relevante Standards aus dem Abschnitt Einsatz von mobilen Systemen zu Wartungszwecken

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
68	-	-	-	-

6.4 Technische Maßnahmen

6.4.1 Komponenteneigenschaften & Härtung

Die Absicherung von OT-Komponenten (z. B. Sensoren und Aktoren) ist wichtig, um Angreifern mit physischem Zugriff auf diese entgegenzuwirken. Sofern diese OT-Komponenten über Cybersicherheitsmechanismen, z. B. Authentisierung, Verschlüsselung, Zugriffskontrolle oder Protokollierung verfügen, sollten diese verwendet werden. Insbesondere ältere Komponenten sind aber häufig rein funktional ausgelegt und verfügen daher nicht über integrierte Cybersicherheitsmechanismen. In diesem Fall sollten flankierende physikalische, organisatorische oder zusätzliche technische Maßnahmen eingesetzt werden.

6.4.1.1 Produkteigenschaften & -umfang

Bei Entwurf und Beschaffung sollte auf ein Mindestmaß an Cybersicherheitsfunktionen geachtet werden. Grundlegende Funktionen sind

- Authentisieren von Benutzern und Diensten für den Zugriff auf die Komponente
- Sichern und Wiederherstellen von Konfigurationen
- Möglichkeiten für Updates
- je nach Anwendungsfall Möglichkeiten zur Verschlüsselung und / oder Integritätsschutz für Programme, Konfigurationen und übertragene Daten.

Tabelle 59 Weiterführende rollenspezifische Informationen aus dem Abschnitt Produkteigenschaften & -umfang

Rolle	*Hinweise*
Betreiber	-
Integrator / Hersteller	Integratoren und Hersteller sollten anhand einer Risikoanalyse ermitteln, welche Bedrohungen für das Gerät bestehen. Cybersicherheitsfunktionen sollten Teil der Anforderungen beim Beschaffen von OT-Systemen und Komponenten sein.

Tabelle 60 Verweise auf relevante Standards aus dem Abschnitt Produkteigenschaften & -umfang

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
18	A.8.26	-	-	CHA-2

6.4.1.2 Standard-Benutzerkonten und -Passwörter

OT-Systeme und Komponenten werden von Herstellern und Integratoren teilweise mit Standard-Benutzern und -Passwörtern ausgeliefert. Da diese in den Handbüchern beschrieben sind, sind sie auch Angreifern bekannt. Daher sollten Standard-Passworte oder andere Authentisierungsmerkmale bei der Ersteinrichtung geändert werden. Die neuen Daten sind entsprechend zu dokumentieren.

Tabelle 61 Weiterführende rollenspezifische Informationen aus dem Abschnitt Standard-Benutzerkonten und -Passwörter

Rolle	*Hinweise*
Betreiber	Standardpassworte in den OT-Systemen und Komponenten müssen bei der Ersteinrichtung geändert werden
Integrator/Hersteller	Es sind alle Standardbenutzer und -Passwörter zu dokumentieren. Diese müssen bei der Ersteinrichtung geändert werden.
Hersteller	Standardbenutzer sollten geändert werden können. Auf feste Benutzer (fest codierte Zugangsdaten) sollte möglichst verzichtet werden.

Tabelle 62 Verweise auf relevante Standards aus dem Abschnitt Standard-Benutzerkonten und -Passwörter

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
46	-	-	-	UAC-2

6.4.1.3 Individuelle Benutzerkonten

Das Personal sollte jeweils über individuelle Benutzerkonten verfügen und sich ausschließlich mit dem eigenen Konto am Betriebssystem und an den Anwendungen anmelden. Dies erleichtert den Schutz der Systeme beim Wechsel oder Ausscheiden von Personal. Kommen in diesem Fall Gruppenkonten zum Einsatz, müssen neue Authentisierungsdaten (wie z. B. Passworte) für diese ausgerollt werden. Nur auf diese Weise können unberechtigte Zugriffe verhindert werden. Zudem wird auch bei einem Vorfall die Aufklärungsarbeit erleichtert, da nachvollzogen werden kann, mit welchen Benutzerkonto ggf. Änderungen durchgeführt wurden. Dementsprechend kann bei einer Kompromittierung eines Benutzerkontos nachvollzogen werden, was geändert wurde. An- und Abmeldungen sollten daher protokolliert werden.

Besonders in älteren OT-Systemen ist es häufig nicht möglich, entsprechende Benutzerkonten einzurichten. In diesem Fall sollte durch eine Risikoanalyse geprüft werden, wie ein Missbrauch eingeschränkt werden kann (z. B. abgeschlossene Türen). Darüber hinaus sollten die Passwörter für Gruppenkonten mindestens in jedem Netzsegment unterschiedlich sein.

Das Ändern von Passworten nach Ausscheiden von Mitarbeitern oder Wartungsfirmen ist anzuraten, auch wenn der Aufwand bei nicht vernetzten Feldgeräten oft sehr hoch ist. Es wird in dem Fall eine Risikobetrachtung empfohlen.

Tabelle 63 Weiterführende rollenspezifische Informationen aus dem Abschnitt Individuelle Benutzerkonten

Rolle	*Hinweise*
Betreiber	Protokollierung der An- und Abmeldungen für alle Benutzerkonten
Integrator/Hersteller	Unterstützung von individuellen Benutzerkonten in OT-Systemen und Komponenten

Tabelle 64 Verweise auf relevante Standards aus dem Abschnitt Individuelle Benutzerkonten

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
47	-	-	-	UAC-2 UAC-3

6.4.1.4 Verzicht auf unnötige Software und Dienste

Der Funktionsumfang und die Dienste von OT-Komponenten sollten auf das für den Betrieb benötigte beschränkt werden. Alle Softwarepakete, die nicht benötigt werden, sollten entfernt und nicht benötigte Dienste deaktiviert werden.

In der Vergangenheit wurden bei OT-Komponenten im Auslieferungszustand bei der Inbetriebnahme eine Vielzahl von Diensten automatisch gestartet und bei der Einrichtung nicht deaktiviert. Dies erleichtert Angreifern das System zu kompromittieren.

Tabelle 65 Weiterführende rollenspezifische Informationen aus dem Abschnitt Verzicht auf unnötige Software und Dienste

Rolle	*Hinweise*
Betreiber	Die Dienste sollten auf das wesentliche funktional notwendigste beschränkt werden. Es sollte in regelmäßigen Abständen kontrolliert werden, ob aktivierte Dienste weiterhin benötigt werden.
Integrator / Hersteller	Standardmäßig installierte Software und aktivierte Dienste sind zu dokumentieren. Bei Zusatzfunktionen sind die Auswirkungen auf den Betrieb und ggf. vorhandene Abhängigkeiten ebenfalls zu dokumentieren.

Tabelle 66 Verweise auf relevante Standards aus dem Abschnitt Verzicht auf unnötige Software und Dienste

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
24, 48	-	-	-	CHA-2

6.4.1.5 Sichere Standardeinstellungen

Die Standardeinstellungen bei der Auslieferung von OT-Systemen und Komponenten sollten bereits einen sicheren Einsatz unterstützen bzw. gewährleisten. Dies wird häufig als Security by Default bezeichnet.

Die folgenden Beispiele sollen mögliche Umsetzungen verdeutlichen:

- eine vorhandene Firewall beschränkt den möglichen Datenverkehr auf das für die Inbetriebnahme notwendige Minimum.
- bei unterstützten Protokollen sind Verschlüsselung und Signaturen aktiviert.
- Es sind die Hinweise des Integrators und Herstellers für die Einrichtung zu berücksichtigen.

- es sind nur die für die Inbetriebnahme oder einen typischen Betrieb der Komponente notwendigen Dienste aktiviert.

Der letzte Punkt zeigt auch den Zusammenhang mit anderen Punkten wie "Entfernen von unnötiger Software und Diensten".

Zudem gilt insbesondere bei der Inbetriebnahme von OT-Systemen und Komponenten, dass die aktuellsten Sicherheitsupdates installiert sind.

Tabelle 67 Weiterführende rollenspezifische Informationen aus dem Abschnitt Sichere Standardeinstellungen

Rolle	*Hinweise*
Betreiber	-
Integrator / Hersteller	Ausliefern der OT-Systeme und Komponenten in einer sicheren Grundkonfiguration

Tabelle 68 Verweise auf relevante Standards aus dem Abschnitt Sichere Standardeinstellungen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
49, 26	-	-	-	CHA-3

6.4.1.6 Reduktion/Deaktivieren von Hardwareschnittstellen

Nicht für den produktiven Betrieb benötigte Hardware sollte entfernt, deaktiviert oder unzugänglich gemacht werden. Dies beinhaltet lokale Schnittstellen wie USB-Ports, CD/ DVD-Laufwerke und andere Speichermedien-Geräte.

Eine Deaktivierung kann beispielsweise durch eine mechanische Sperrvorrichtung, softwaregesteuert oder durch Siegel z. B. an USB-Ports erfolgen. Werden diese Geräte trotz der Absicherung unbefugt genutzt, sollte dies für den Administrator des Systems nachvollziehbar sein (z. B. durch gebrochene Schlösser, Siegel oder Protokolleinträge im System).

Im Fall einer Software-Lösung sollte der Administrator zu Wartungszwecken den Sperrmechanismus kurzzeitig deaktivieren und aufheben können, sodass Zugriffe auf die Hardware möglich sind.

Tabelle 69 Weiterführende rollenspezifische Informationen aus dem Abschnitt Reduktion/Deaktivieren von Hardwareschnittstellen

Rolle	*Hinweise*
Betreiber	-
Integrator/Hersteller	Die Deaktivierung von Schnittstellen sollte Teil der Produkteigenschaften sein

Tabelle 70 Verweise auf relevante Standards aus dem Abschnitt Reduktion/Deaktivieren von Hardwareschnittstellen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
50	-	-	-	-

6.4.1.7 Langfristige Gewährleistung der Cybersicherheit

Bereits bei der Planung sollte die lange Lebenszeit und Nutzungsdauer der OT-Komponenten und Systeme berücksichtigt werden. Daher sollte eine Strategie für den kompletten Lebenszyklus vorhanden sein und eine klare Kommunikation innerhalb der Lieferkette dazu erfolgen.

Dazu müssen beispielsweise folgende Fragen beantwortet werden:

- Für welchen Zeitraum wird die Versorgung mit Sicherheitsupdates sichergestellt? Dies ist ggf. relevant nach Produktionsende der Komponente.
- Wie wird auf das Ende der Versorgung mit Sicherheitsupdates reagiert? Dies kann ggf. auch frühzeitig der Fall sein, wenn ein Lieferant in der Lieferkette insolvent geht oder aus anderen Gründen den Support einstellt.

Tabelle 71 Weiterführende rollenspezifische Informationen aus dem Abschnitt Langfristige Gewährleistung der Cybersicherheit

Rolle	*Hinweise*
Betreiber	Dieser Aspekt sollte Teil der Beschaffung und Planung sein.
Integrator	Dieser Aspekt sollte Teil der Planung, Entwicklung und des Service sein.
Hersteller	Dieser Aspekt sollte Teil der Planung, Entwicklung und des Service sein.

Tabelle 72 Verweise auf relevante Standards aus dem Abschnitt Langfristige Gewährleistung der Cybersicherheit

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
27	-	17-1 17-2	-	SCS-6 SSM-1 LCS-1 CHA-1

6.4.2 Entwicklung / Konfiguration

6.4.2.1 Berücksichtigung der Cybersicherheitsvorgaben der Lieferanten

Beim Betrieb und der Integration von Komponenten sind durch den Lieferanten erstellte Vorgaben zum sicheren Einsatz zu berücksichtigen. Dies betrifft die in der Dokumentation hinterlegten Hinweise zum Einsatz und Betrieb der Komponenten und Systeme. Hierdurch sollen Schwachstellen beim Einsatz vermieden werden, die von der konkreten Einsatzumgebung abhängen.

Tabelle 73 Weiterführende rollenspezifische Informationen aus dem Abschnitt Berücksichtigung der Cybersicherheitsvorgaben der Lieferanten

Rolle	*Hinweise*
Betreiber	Berücksichtigen der Vorgaben im Rahmen des Einsatzes.
Integrator/Hersteller	Cybersicherheitshinweise und -empfehlungen sollten in der Produktdokumentation enthalten sein

Tabelle 74 Verweise auf relevante Standards aus dem Abschnitt Berücksichtigung der Cybersicherheitsvorgaben der Lieferanten

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
21	A.8.19	-	-	-

6.4.2.2 Robustheit der Produkte

Bei der Entwicklung von Hardware wird üblicherweise berücksichtigt, dass die Hardware unter widrigen Umgebungsbedingungen betrieben wird. Dies sollte auch bei der Entwicklung von Soft- und Firmware etabliert werden. Diese sollten robust gegenüber zu verarbeitenden Daten und Systemzuständen reagieren. Mit robust ist gemeint, dass sich keine undefinierten Systemzustände herbeiführen lassen.

So sollten beispielsweise bei Protokollstacks ungültige Netzpakete nicht zum Absturz oder zu Fehlern der Software führen, sondern von dem Protokollstack ignoriert und bei Bedarf protokolliert werden.

Hierzu zählt auch das Validieren von Eingabedaten. Bei der Validierung werden beispielsweise Längenbegrenzungen von Feldern und die Kodierung von Werten auf ihre Korrektheit geprüft. Wenn eine solche Prüfung unterbleibt, kann es bei der Verarbeitung unter Umständen zu Pufferüberläufen oder zu einer fehlerhaften Interpretation der Daten kommen. Pufferüberläufe gehören zu den größten Gefahren, da die Möglichkeit besteht, Schadcode einzuschleusen und zur Ausführung zu bringen.

Tabelle 75 Weiterführende rollenspezifische Informationen aus dem Abschnitt Robustheit der Produkte

Rolle	*Hinweise*
Betreiber	Diese Anforderung sollte bereits bei der Anschaffung neuer Komponenten gefordert werden
Integrator	Die Robustheit der Komponenten sollte bereits durch den Integrator sichergestellt werden. Diese Anforderung sollte bereits bei der Anschaffung neuer Komponenten gefordert werden.
Hersteller	Die Robustheit der Komponenten sollte bereits durch die Hersteller sichergestellt werden.

Tabelle 76 Verweise auf relevante Standards aus dem Abschnitt Robustheit der Produkte

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
22	-	-	-	-

6.4.2.3 Kompatibilität mit Cybersicherheitssystemen

Die OT besteht häufig aus einer Vielzahl unterschiedlicher Systeme und Komponenten verschiedener Hersteller. Im Bereich der Cybersicherheit sollten die unterschiedlichen Lösungen kompatibel zu etablierten Standards sein. Beispiele hierfür sind die Anbindung

- an Verzeichnisdienste zur Authentisierung oder
- an zentrale Monitoring- und Protokollierungssysteme zur zentralen Auswertung.

Tabelle 77 Verweise auf relevante Standards aus dem Abschnitt Kompatibilität mit Cybersicherheitssystemen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
23	-	-	-	-

6.4.2.4 Schutz von Daten beim Übertragen (Data-in-transit)

Ein Angreifer, der sich in einem Netzwerk befindet, kann dort ungeschützt übertragene Daten abgreifen oder manipulieren. Daher sollte geprüft werden, ob sensible Daten übertragen werden. Die Schutzmaßnahmen hängen dabei von den angestrebten Schutzzielen ab. Zur Sicherstellung der Integrität ist eine Signierung der Daten ausreichend. Soll die Vertraulichkeit der Daten sichergestellt werden, müssen die Daten verschlüsselt werden.

Bei administrativen Tätigkeiten sollte die Vertraulichkeit (insbesondere der Authentisierungsdaten) gewahrt bleiben. Bei Echtzeitdaten kann ggf. auf die Verschlüsselung verzichtet werden, wenn die Vertraulichkeit der Informationen als nachrangig einzustufen ist.

Grundsätzlich ist zu empfehlen, dass soweit möglich (z. B. in neuen Anlagen) Protokollvarianten zum Einsatz kommen, die einen Schutz der zu übertragenden Daten enthalten.

Falls Schutzmaßnahmen erforderlich sind und schwache Protokolle nicht abgesichert oder durch sichere Alternativen ersetzt werden können (z. B. im Fall von proprietären, ICS-spezifischen Protokollen), sollten zusätzliche Schutzmaßnahmen ergriffen werden.

Tabelle 78 Weiterführende rollenspezifische Informationen aus dem Abschnitt Schutz von Daten beim Übertragen (Data-in-transit)

Rolle	*Hinweise*
Betreiber	Sichere Protokolle als Teil der Anforderungen
Integrator	Sichere Protokolle den unsicheren vorziehen
Hersteller	Neue Komponenten sollten für sichere Protokolle geeignet sein

Tabelle 79 Verweise auf relevante Standards aus dem Abschnitt Schutz von Daten beim Übertragen (Data-in-transit)

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
43	-	-	PR.DS-02	-

Weitere Informationen:

- BSI TR-02101-1:
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

6.4.2.5 Schutz von gespeicherten Daten (data-at-rest)

Für gespeicherte Daten sollten geeignete und notwendige Maßnahmen ergriffen werden, um Integrität, Vertraulichkeit und Verfügbarkeit zu gewährleisten. Dies kann beispielsweise durch Signaturen von wichtigen Daten erfolgen oder den Einsatz von Datenträgerverschlüsselung. Der Einsatz sollte auf Basis der Risikoanalyse erfolgen.

Dabei sind Maßnahmen zur Datensicherung und -wiederherstellung zu berücksichtigen.

Tabelle 80 Weiterführende rollenspezifische Informationen aus dem Abschnitt Schutz von gespeicherten Daten (data-at-rest)

Rolle	*Hinweise*
Betreiber	Auswahl und Nutzen entsprechender Lösungen zum Schutz der gespeicherten Daten.
Integrator	Bei Design und Umsetzen sollten entsprechende Technologien berücksichtigt werden.
Hersteller	Bei Design und Umsetzen sollten entsprechende Technologien berücksichtigt werden.

Tabelle 81 Verweise auf relevante Standards aus dem Abschnitt Schutz von gespeicherten Daten (data-at-rest)

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
43	-	-	PR.DS-01	-

6.4.2.6 Aktuelle Protokoll-Versionen

Ähnlich wie beim Sicherheitsupdate für Soft- und Firmware sollten auch für eingesetzte Protokolle aktuelle Versionen zum Einsatz kommen.

Ein Wechsel ist insbesondere dann erforderlich, wenn Schwachstellen in der bisherigen Version entdeckt wurden. Ein Beispiel ist Transport Layer Security (TLS), das im Wesentlichen für Webverbindungen genutzt wird. Dort wurden in den letzten Jahren immer wieder Schwachstellen entdeckt, die durch neuere Versionen behoben wurden.

Eine Abwägung kann erfolgen, wenn ein Protokoll lediglich funktional erweitert wurde.

Werden aus Gründen der Kompatibilität ältere Protokollversionen unterstützt, sollten diese erst nach expliziter Aktivierung durch den Betreiber genutzt werden können bzw. sollten deaktivierbar sein.

Tabelle 82 Verweise auf relevante Standards aus dem Abschnitt Aktuelle Protokoll-Versionen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
	A.8.8	-	-	-

6.4.2.7 Einsatz geeigneter kryptographischer Verfahren

Wenn kryptographische Verfahren (z. B. Hashfunktionen, symmetrische und asymmetrische Verschlüsselung) zum Einsatz kommen, sollten diese für den Anwendungszweck geeignet sein und dem Stand der Technik entsprechen. Empfehlungen für kryptografische Verfahren werden in (23) gegeben.

Auf Basis der Schutzanforderungen und unter Berücksichtigung der in den OT-Systemen und Komponenten zur Verfügung stehenden Ressourcen (z. B. eingeschränkte Rechenleistung) sind geeignete kryptografische Verfahren auszuwählen.

Es sollte auf etablierte Bibliotheken zurückgegriffen werden. Auf eigene Implementierung sollte wegen der Komplexität verzichtet werden.

Zertifizierte Hard- oder Software mit kryptografischen Funktionen, deren Zertifizierung die jeweils relevanten Aspekte der Kryptografie umfasst, sollten bevorzugt ausgewählt werden.

Bei der Auswahl von geeigneten kryptografischen Verfahren sind auch die Auflagen der nationalen Außenwirtschaftsgesetze (Stichwort: Exportkontrolle) zu beachten. Hersteller sollten dieses Thema bereits in der Entwicklung entsprechend berücksichtigen

Neben der initialen Auswahl gilt es auch während des ganzen Lebenszyklus der Komponenten die Entwicklungen in diesem Bereich zu verfolgen. Es kann durchaus möglich sein, dass Schwächen in einem Verfahren bekannt werden und dieses daraufhin ausgetauscht werden sollte/muss. Das Stichwort ist Kryptoagilität um einen Umstieg einfach zu ermöglichen. Der Umgang mit auftretenden Schwachstellen im eingesetzten kryptografischen Verfahren sollte daher beschrieben werden.

Bei der Verwaltung kryptografischer Geheimnisse sollten u.a. nachfolgende Punkte beachtet werden:

- die Speicherung der kryptografischen Geheimnisse erfolgt in vor unberechtigtem Zugriff geschützter Weise (ein Auslesen darf nicht möglich sein),
- ein Wechsel der Geheimnisse durch berechtigte Personen sollte möglich sein,
- ein Wechsel der Geräte sollte möglich sein, z. B. im Rahmen von automatisierten/ autarken Parametrier- und Konfigurationsvorgängen (wenn eine sichere Authentisierung und Autorisierung stattgefunden hat) und
- eine Generierung erfolgt in einer geschützten und vertrauenswürdigen Umgebung.

Tabelle 83 Weiterführende rollenspezifische Informationen aus dem Abschnitt Einsatz geeigneter kryptographischer Verfahren

Rolle	*Hinweise*
Betreiber	-
Integrator	Entsprechend dem Einsatzzweck Komponenten auswählen, die kryptografische Verfahren unterstützen
Hersteller	Kryptografische Verfahren als Produkteigenschaft bei der Produktentwicklung berücksichtigen

Tabelle 84 Verweise auf relevante Standards aus dem Abschnitt Einsatz geeigneter kryptographischer Verfahren

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
58	A.8.24	-	-	-

6.4.2.8 Schutz der Safety

OT-Systeme und Komponenten für die Safety sollten beim Schutz priorisiert behandelt werden. Dabei sollte der Schutz der Safety-Systeme in das gesamte Cybersicherheitsmanagement eingebettet werden.

Für diese Systeme sollten die Risiken durch Manipulation und Ausfall bewertet und mögliche Auswirkungen betrachtet werden.

Bei der Risikoidentifikation sollten die beteiligten Parteien die auf die funktionale Sicherheit einwirkenden Gefährdungen bewerten. Gefährdungen sind dabei gefährliche Vorfälle und Gefährdungssituationen im Kontext der OT-Komponente(n). Diese müssen unter allen vernünftigerweise vorhersehbaren Umständen festgelegt werden. Sie müssen alle relevanten menschlichen Faktoren (einschließlich Fehlerbedingungen und böswilliger oder nicht autorisierter Handlung) einschließen und ungewöhnlichen und selten genutzten Betriebsarten der OT besondere Aufmerksamkeit schenken.

Es sollten spezielle Prozesse für Safety-Systeme und -Komponenten etabliert werden, um die Integrität bei der Wiederherstellung nach einem Vorfall zu gewährleisten.

Tabelle 85 Weiterführende rollenspezifische Informationen aus dem Abschnitt Schutz der Safety

Rolle	*Hinweise*
Betreiber	Umsetzung der Vorgaben von Herstellern und Integratoren, sowie Aktualisierung der Risikobetrachtungen bei Anpassungen.
Integrator	Entsprechende Betrachtungen und Schutzkonzepte sollten bereits bei Planung und Umsetzung erarbeitet und dokumentiert werden.
Hersteller	Entsprechende Betrachtungen und Schutzkonzepte sollten bereits bei Planung und Entwicklung erarbeitet und dokumentiert werden.

Tabelle 86 Verweise auf relevante Standards aus dem Abschnitt Schutz der Safety

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	-	-	RC.RP-05	-

6.4.2.9 Validierung der Integrität und Authentizität von Komponenten, Systemen, Firm- und Software

Software, Steuerungsprogramme, Konfigurationen, Updates oder vergleichbares, die in die OT eingebracht werden, sollten auf Authentizität und Integrität geprüft und bei Abweichungen nicht eingespielt werden. Für die Prüfung können Prüfsummen oder Signaturen, die durch den Hersteller an der Software angebracht wurden, genutzt werden.

Tabelle 87 Weiterführende rollenspezifische Informationen aus dem Abschnitt Validierung der Integrität und Authentizität von Komponenten, Systemen, Firm- und Software

Rolle	*Hinweise*
Betreiber	Prüfung der Daten vor dem Einspielen.
Integrator	Notwendige Informationen und Funktionen sollten durch die Hersteller und Integratoren bereitgestellt werden. Prüfung der Daten vor dem Einspielen.

Rolle	*Hinweise*
Hersteller	Notwendige Informationen und Funktionen sollten durch die Hersteller bereitgestellt werden.

Tabelle 88 Verweise auf relevante Standards aus dem Abschnitt Validierung der Integrität und Authentizität von Komponenten, Systemen, Firm- und Software

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.8.19	19-1	-	-

6.4.3 Absichern der OT-Netze

6.4.3.1 Netzsegmentierung

Das OT-Netz sollte in unterschiedliche Bereiche getrennt (segmentiert) werden. Damit sollen unberechtigte Zugriffe auf das OT-Netz erschwert oder ganz verhindert werden. Gleiches gilt für Zugriffe zwischen OT und IT-Netzen.

Das Segmentieren sollte nach den erforderlichen Sicherheitsbedarfen des OT-Netzes bzw. der OT-Systeme geplant und umgesetzt werden. Die Grundlage bildet der Netzplan und die Kommunikationsverbindungen. Dabei sind u.a. nachfolgende Aspekte zu berücksichtigen:

- VLANs sollten zur logischen Trennung von Netzsegmenten eingesetzt werden. Zur Trennung von Netzsegmenten mit erhöhtem Schutzbedarf kann eine physikalische Trennung erfolgen. Kommt eine logische Trennung zum Einsatz so sind die damit verbundenen Risiken über eine Risikobewertung zu betrachten.
- Bei der Verwendung von VLANs sollte das Default-VLAN deaktiviert sein. Ungenutzte Ports an dem Switch sollten einem eigenen VLAN zugeordnet werden.
- Die Komponenten in einem Segment / Sub-Segment sollten alle über ein gleiches bzw. sehr ähnliches Sicherheitsniveau verfügen.
- Der Verbindungsaufbau sollte immer aus dem Netzsegment mit dem höheren Schutzbedarf in das Netzsegment mit dem niedrigeren Schutzbedarf stattfinden.
- Eine Umgehung der Netztrennung durch nicht dokumentierte Verbindungen darf nicht stattfinden. Insbesondere sollten keine unkontrollierten Verbindungen zu Netzsegmenten mit unterschiedlichem Schutzbedarf zugelassen werden.
- Falls die Verbindung zwischen zwei Netzsegmenten im OT-Netz abbricht, sollte dies nicht oder nur in geringem Maße die Produktion beeinträchtigen. Daher sollten Abhängigkeiten zwischen Netzen vermieden werden. Somit werden mögliche Auswirkungen eines Netzsegmentausfalls weitestgehend reduziert.
- Eine Abtrennung (Isolierung) von Sub-Netzen im Falle eines Cybersicherheitsereignisses sollte bei der Planung des Segmentierungskonzeptes mitberücksichtigt werden.
- Vertikale Segmentierung
  Betriebsführungs- und Produktionsbetriebssysteme, Geschäftslogiksysteme und Büronetzwerk sollten von den ICS-Komponenten der Produktionsanlage getrennt werden. Dies wird als vertikale Segmentierung bezeichnet.
  Die Unterteilung des Netzwerks in vertikale Ebenen kann gemäß den Ebenen des Purdue Model erfolgen. Perimeter sollten zwischen den Ebenen implementiert werden.
  Um eine direkte Kommunikation zwischen den Ebenen der Produktionsführung (Ebene 4) und der Betriebsführung-Ebene (Ebene 3) zu vermeiden, sollte eine DMZ-Ebene (Ebene 3.5 OT-DMZ) zur

Entkopplung des Datenverkehrs zwischen IT und OT etabliert werden. Dieses verfügt über ein reduziertes Sicherheitsniveau da Zugriffe aus beiden Bereichen (OT und IT) möglich sind.

- Horizontale Segmentierung
  Die Produktionsanlage bzw. Maschinen sollten in Subnetze unterteilt werden. Die Subnetze sollten in Segmente eingeteilt und mit geeigneten technischen Isolationsmaßnahmen (logische oder physikalische Trennung¸ Firewall, Access Listen, Datendioden) voneinander getrennt werden. Dabei darf keine Kommunikation zwischen den Anlagenkomponenten funktionsbeeinträchtigend eingeschränkt werden. Die Aufteilung von Anlagen und Maschinen in Teilbereiche wird als horizontale Segmentierung bezeichnet. Die horizontale Segmentierung soll Angriffe oder die Ausbreitung von Fehlfunktionen auf weitere Teilbereiche der Produktionsanlage verhindern bzw. erschweren.
  Bei der horizontalen Segmentierung des Netzes sollte darauf geachtet werden, dass die einzelnen Segmente so weit wie möglich im Betrieb voneinander unabhängig sind. Insbesondere die Segmente, in denen der technische Prozess gesteuert wird, sollten bei einem Ausfall der anderen Segmente für einen gewissen Zeitraum weiter funktionstüchtig sein. Auch sollten die Segmente bei einer notwendig gewordenen Isolierung (z. B. nach einem Angriff) weiter funktionieren.
- Zur Trennung der IT und OT muss eine OT-DMZ umgesetzt werden. Diese regelt die Zugriffe von der IT in die OT und aus der OT in die IT bzw. das Internet. Die OT-DMZ kann aus zwei physisch getrennten Firewall-Systemen aufgebaut werden, wenn ein erhöhter Schutzbedarf besteht. Ein Application Level Gateway oder Proxy-Dienste mit Filtermöglichkeiten bis hin zum Layer 7 sollten den Datenverkehr steuern und kontrollieren.
- Segmentierung von Safety-Systemen
  Safety-Systeme sollten ggf. zusätzlich vor Zugriffen geschützt werden. Ziel ist es eine Beeinflussung und Ausnutzung von Schwachstellen zu erschweren.

Tabelle 89 Weiterführende rollenspezifische Informationen aus dem Abschnitt Netzsegmentierung

Rolle	*Hinweise*
Betreiber	Planen, Umsetzen und Aufrechterhalten der Segmentierung.
Integrator	Unterstützen von Strategien zum Segmentieren der OT-Netze und Bereitstellen der notwendigen Informationen zur Umsetzung (z. B. Kommunikationsprotokolle und -endpunkte).
Hersteller	Unterstützen von Strategien zum Segmentieren der OT-Netze und Bereitstellen der notwendigen Informationen zur Umsetzung

Tabelle 90 Verweise auf relevante Standards aus dem Abschnitt Netzsegmentierung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
31	A.8.22	-	PR.IR-01	INF-3 NCC-1 NCC-2

6.4.3.2 Absichern der Kommunikationsschnittstellen

Alle externen Kommunikationsschnittstellen zum OT-Netz sollten identifiziert und dokumentiert werden (z. B. in einem Netzplan). Hierzu zählen neben offensichtlichen Schnittstellen wie die Verbindung zum IT-Netz über eine DMZ auch weniger offensichtliche, externe Kommunikationsschnittstellen wie Mobilfunk, andere drahtlose Netze und serielle Verbindungen.

Es sollte ein Prozess definiert sein, der eine regelmäßige Prüfung der Dokumentation und im Fall von Änderungen eine zeitnahe Aktualisierung vorsieht.

Direkte Zugriffe aus externen Netzen auf das OT-Netz über die erfassten Kommunikationsschnittstellen sollten vermieden werden (z. B. direkte Verbindungen an ein OT-System (z B. über ein Modem oder Router) oder Administration über eine direkte Verbindung aus dem Internet (z. B. mittels Port-Forwarding)). Diese Verbindungen sollten nach Möglichkeit über einen Proxy-Dienst in einer DMZ in das OT-Netz erfolgen. Auf diese Weise sind alle Zugriffe auf das OT-Netz an einer Stelle gebündelt und lassen sich einfacher kontrollieren.

Bei externen Schnittstellen sollten insbesondere folgende IT-Sicherheitsmaßnahmen berücksichtigt werden, um unbefugte Zugriffe von außen in das OT-Netz zu verhindern:

- Zugriffe über externe Schnittstellen sollten eine starke Authentisierung erfordern
- bedarfsweise Freischaltung des Zugangs von Intern
- Verbindungsversuche und Zugriffe sollten protokolliert und überwacht werden
- Für einen längeren Zeitraum nicht benötigte, externe Schnittstellen (z. B. Fernzugänge) müssen abgeschaltet werden. Nur bei Bedarf sollten die Geräte wieder (elektrisch) eingeschaltet werden.
- IT-Sicherheitsrelevante Daten sollten nicht übertragen werden (z. B. Zugangsdaten, kritische und privilegierte Befehle).
- Die Speicherung von Daten (Engineering Daten, Produktionsdaten) sollte nur in der OT, nicht jedoch auf externen Systemen (außerhalb der Institution) erfolgen.
- Soweit möglich sollten Fernwartungszugänge ausschließlich lesenden Zugriff ermöglichen.

Tabelle 91 Weiterführende rollenspezifische Informationen aus dem Abschnitt Absichern der Kommunikationsschnittstellen

Rolle	*Hinweise*
Betreiber	Erfassen und konsolidieren aller Kommunikationsschnittstellen
Integrator	Dokumentation der verwendeten Kommunikationsschnittstellen
Hersteller	Dokumentation aller an den Komponenten vorhandenen Schnittstellen

Tabelle 92 Verweise auf relevante Standards aus dem Abschnitt Absichern der Kommunikationsschnittstellen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
3	A.8.22	-	PR.IR-01	-

6.4.3.3 Statische Netz-Konfiguration

Die Netzwerkadressen in einem OT-Netz sollten statisch vergeben werden, sofern dies möglich ist. Dazu zählt beispielsweise die statische Vergabe von IP-Adressen, Subnetzmasken und Routen innerhalb des ICS-Netzes. Auch die Konfiguration von DNS-Servern kann erforderlich sein, falls über diese Namen aufgelöst werden sollen.

Das Zuordnen der Adressen zu den OT-Systemen und Komponenten muss dokumentiert werden. Darüber hinaus sollte darauf geachtet werden, dass eine IP-Adresse nicht mehrfach vergeben wird.

Wenn eine statische Netz-Konfiguration in der OT durchgeführt wird, sollte DHCP-Client-Software deinstalliert oder zumindest deaktiviert werden.

Tabelle 93 Verweise auf relevante Standards aus dem Abschnitt Statische Netz-Konfiguration

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
34	-	-	-	

6.4.3.4 Unabhängiger Betrieb der OT

Durch das Vernetzen von IT und OT entstehen Abhängigkeiten zwischen den Bereichen. So ist es in einigen Branchen notwendig, dass die OT Informationen für die Produktion aus Systemen der IT erhält. Beispiele sind Auftragsverwaltung oder auch zentrale Lagerverwaltung. Fallen diese aus, kann die Produktion nur noch kurze Zeit aufrechterhalten werden.

Daher sollten alle Abhängigkeiten der OT von der IT dokumentiert werden. Dazu gehören beispielsweise Informationen zum Verwendungszweck und den Folgen eines Ausfalls. Auf Basis dieser Informationen sollte abgewogen werden, ob eine mögliche Doppelung sinnvoll ist. Dabei sollte der Mehraufwand für den Betrieb und dem möglichen Sicherheitsgewinn gegenübergestellt werden. Daneben sollten andere Alternativen, wie ein zusätzliches Absichern oder Redundanzen geprüft werden.

Tabelle 94 Verweise auf relevante Standards aus dem Abschnitt Unabhängiger Betrieb der OT

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
36	A.8.21	-	PR.IR-02	-

6.4.3.5 Absichern der Funktechnologien

Der Einsatz von Funktechnologie erfordert sorgfältige Planung. Da es sich hierbei um ein sogenanntes Shared Medium handelt, ist der Zugriff auf das Übertragungsmedium für Angreifer in der Regel auch aus großen Distanzen und außerhalb des Betriebsgeländes möglich und nur schwierig einzuschränken.

Die Reichweite von Funknetzen sollte daher soweit wie möglich eingeschränkt werden. IT-Sicherheitsfunktionen (z. B. Passwörter, PIN-Eingabe) sollten aktiviert sein und in der Konfiguration von den vorgegebenen Einstellungen bei der Erstinstallation abweichen.

Funktechnologien sollten nicht für Einsatzzwecke verwendet werden, die hohe Anforderungen an die Verfügbarkeit voraussetzen (z. B. kann durch Störsignale eine Funkverbindung immer unterbrochen oder stark eingeschränkt werden). Darüber hinaus sollten die verwendeten Technologien über hinreichende IT-Sicherheitsmechanismen gemäß dem Stand der Technik verfügen, sodass kein unbefugter Zugriff auf die übertragenen Daten möglich ist (z. B. Verschlüsselung des Datenverkehrs).

Die IT-Sicherheit bei Funknetzen sollte nicht ausschließlich auf den IT-Sicherheitsmerkmalen der eingesetzten Technologie basieren, sondern es sollten zusätzliche IT-Sicherheitsmechanismen auf Netzebene umgesetzt werden. Dabei sollte darauf geachtet werden, dass nicht nur eine Schutzmauer errichtet wird, sondern mehrere Hürden errichtet werden. Dazu gehören z. B. Netzsegmentierung und der zusätzliche Einsatz von kryptographischen Algorithmen bei der Datenübertragung.

Verfügbare Protokolldaten der Geräte sollten regelmäßig auf Auffälligkeiten geprüft werden (z. B. Kommunikation mit unbekannten Geräten).

Tabelle 95 Verweise auf relevante Standards aus dem Abschnitt Absichern der Funktechnologien

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
37	A.8.21	25-1 25-2	-	-

6.4.3.6 Einsatz von Firewalls

Zur logischen Trennung von Netzsegmenten sollte eine Firewall eingesetzt werden, die als Filterkomponente den Datenfluss zwischen den Segmenten reglementiert.

Hierbei kann nach den folgenden Kategorien von Firewalls auf Netzebene unterschieden werden:

- Paketfilter (Filterung nach IP-Adresse und Port),
- Stateful Inspection Firewall (Filterung nach IP-Adresse, Port und Verbindungsstatus),
- Application Level Gateway (zusätzliche Filterung bis auf Anwendungsebene).

Firewalls sollten möglichst als dedizierte Hardware eingesetzt werden. Hierbei sollte geschultes Personal für die Konfiguration und den Betrieb der Firewalls zuständig sein. Die folgenden Punkte sollten bei der Konfiguration einer Firewall beachtet werden:

- Die Firewall sollte restriktiv konfiguriert sein und daher gemäß dem Allow-List-Ansatz grundsätzlich alles verbieten, sodass explizit Verbindungen und Zugriffe freigeschaltet werden müssen.
- Nur Verbindungen, die zwingend notwendig für den Betrieb der OT sind, sollten freigegeben werden.
- Verbindungen vom OT-Netz zu externen Netzen (z. B. Office-Netz) sollten ausschließlich über Proxy-Dienste in der DMZ erfolgen. Direkte Verbindungen zwischen den Netzen sollten auf das funktional notwendige Maß beschränkt werden. Die Kommunikation mit anderen Netzen sollte komplett unterbunden werden.
- Vorzugsweise sollten eingehende Verbindungen von externen Netzen in das OT-Netzwerk vollständig unterbunden werden. Wenn dies nicht möglich ist, sollten die Inhalte der Verbindungen gefiltert und auf Konformität geprüft werden.
- Die Filterung sollte so feingranular wie möglich erfolgen. Nach Möglichkeit sollte daher der Zugriff auf einzelne IP-Adressen oder kleine definierte Adressbereiche beschränkt werden.
- Es sollten lediglich die zwingend notwendigen Ports für TCP oder UDP freigegeben werden.
- Es sollte eingehender und ausgehender Datenverkehr gefiltert werden.
- Der Platzhalter ANY sollte vermieden werden.
- Die letzte Filterregel sollte immer alles verbieten (DENY ALL, PERMIT NONE).

Die Einstellungen sollten auf ihre Wirksamkeit überprüft werden. Manche Einstellungen der Firewall wirken nur auf IPv4 während IPv6 getrennt konfiguriert werden muss.

Darüber hinaus sollten die Protokolldaten der Firewall regelmäßig hinsichtlich Auffälligkeiten überprüft werden. Hierbei ist hervorzuheben, dass die reine Installation einer Firewall keinen zusätzlichen Schutz bietet, wenn keine sorgfältige und restriktive Konfiguration der Regeln und eine Überwachung vorgenommen werden.

Die Beschaffungskriterien unterscheiden sich dabei von Fall zu Fall. Je nach Einsatzart können Funktionen zur Filterung und Überwachung der Protokolle eingesetzt werden. Es ist zu empfehlen, dass nicht nur eine Filterung auf IP-Adressen und Ports stattfindet, sondern auch der Protokolle selbst.

Tabelle 96 Verweise auf relevante Standards aus dem Abschnitt Einsatz von Firewalls

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
38	A.8.20 A.8.22 A.8.23	22-1 22-2	PR.IR-01	-

6.4.3.7 Host-based Firewalls

Eine Host-basierte Firewall ist eine Software zur Filterung des Netzverkehrs von und zu einem OT-System bzw. Komponente. Entgegen einer Netz-Firewall ist eine Host-basierte Firewall auf dem zu schützenden System installiert. Häufig sind diese Firewalls Bestandteil des Betriebssystems.

Soweit möglich sollte auf allen OT-Systemen und Komponenten eine Host-basierte Firewall installiert sein und genutzt werden.

Tabelle 97 Weiterführende rollenspezifische Informationen aus dem Abschnitt Host-based Firewalls

Rolle	*Hinweise*
Betreiber	Funktion sollte aktiviert sein/werden
Integrator	Funktion sollte ggf. in den Komponenten / Systemen vorhanden sein und aktiviert sein
Hersteller	Funktion sollte ggf. in den Komponenten / Systemen vorhanden sein

Tabelle 98 Verweise auf relevante Standards aus dem Abschnitt Host-based Firewalls

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
39	-	-	PR.IR-01	-

6.4.3.8 Datendiode (One-Way-Gateway)

Eine Datendiode ermöglicht es, dass die Datenübertragung nur in eine Richtung erfolgt. Ein Rückkanal ist nicht vorhanden, was zu gewissen Einschränkungen führt. Falls ein Rückkanal für Quittungen notwendig ist, sollten die einzelnen Verbindungen in dem Gateway terminiert werden, eine Prüfung des Protokolls durchgeführt werden und erst danach die Weiterleitung erfolgen.

Je nach Ausrichtung der Datendiode können unterschiedliche Schutzziele verfolgt werden. So kann verhindert werden, dass beispielsweise Steuerbefehle von einem Netz mit niedrigem Schutzbedarf (z. B. Office-Netz) in ein Netzwerk mit hohem Schutzbedarf (z. B. OT-Netz) übertragen werden. Auf der anderen Seite kann bei umgekehrter Positionierung der Abfluss von vertraulichen Informationen aus einem Netzwerk mit hohem Schutzbedarf verhindert werden.

Die Einschränkungen gelten in diesem Fall auch für den Bezug von Updates und die Konfiguration der Komponenten über das Netzwerk. Die Einrichtung von Verbindungen an der Datendiode vorbei für diesen Zweck hebelt die Funktion aus und muss vermieden werden.

Wenn Kommunikation in beide Richtungen stattfinden muss, gibt es andere Lösungen, die Filter und Kontrollmöglichkeiten bieten.

Tabelle 99 Weiterführende rollenspezifische Informationen aus dem Abschnitt Datendiode (One-Way-Gateway)

Rolle	*Hinweise*
Betreiber	Funktion sollte geprüft und ggf. umgesetzt werden
Integrator	Funktion sollte geprüft und ggf. berücksichtigt werden
Hersteller	-

Tabelle 100 Verweise auf relevante Standards aus dem Abschnitt Datendiode (One-Way-Gateway)

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
40	A.8.22	-	PR.IR-01	-

6.4.3.9 Zeitsynchronisierung

Eine Vielzahl an Prozessen, aber auch administrative Tätigkeiten, beruhen in der OT auf einer genauen und abgestimmten Zeit (z. B. Nachvollziehbarkeit verteilter Protokolldaten, Beigabe von Zusatzstoffen in der Produktion zum richtigen Zeitpunkt). Es muss aufgrund der Applikationsanforderungen abgewogen werden, wie die Zeitsynchronisation erfolgt.

Für die Synchronisation kann Network Time Protocol (NTP) bzw. NTPSec oder Precision Time Protocol (PTP; IEEE 1588; IEC 61588) genutzt werden.

Das Zeitsignal für den Server sollte aus einer vertrauenswürdigen Quelle stammen. OT-Komponenten und Systeme sollten die Zeit in einem einheitlichen, standardisierten Format interpretieren (z. B. unter Berücksichtigung von Zeitzonen, Winter- und Sommerzeit).

Tabelle 101 Verweise auf relevante Standards aus dem Abschnitt Zeitsynchronisierung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
45	A.8.17	-	-	-

6.4.3.10 Fernwartung

Die Systeme, die den Fernzugang bereitstellen, müssen besonders geschützt sein. Der Verbindungsaufbau sollte mindestens eine Zwei-Faktor-Authentisierung verlangen (z. B. Token und Passwort) und die Daten müssen in verschlüsselter Form übertragen werden.

Soll der Verbindungsaufbau für die Fernwartung von extern erfolgen, so sollte keine direkte Verbindung in die OT etabliert werden. Die Verbindung in das OT-Netz sollte vielmehr über einen sog. Sprungserver/Proxyserver in einer DMZ erfolgen. Dieser besitzt die Möglichkeit, eine entsprechende Verbindung in die OT aufbauen. Gleichzeitig kann er alle Aktivitäten aufzeichnen.

Client-Systeme, die für die Fernwartung genutzt werden, müssen vor Manipulation, unberechtigtem Zugriff und Schadsoftware geschützt werden. Dies gilt sowohl für Systeme bei Dienstleistern (wie Integratoren und Herstellern) als auch Sprungserver in der OT-DMZ.

Als Alternative zum Sprungserver kann der Verbindungsaufbau anstatt von extern von intern aus dem OT-Netz heraus erfolgen. Das OT-System oder Komponente verbindet sich somit zum Hersteller. Auf diese Weise werden eingehende Verbindungen vermieden und nach extern keine zusätzlichen Dienste angeboten. Auch hier ist auf die Sicherheit der Systeme beim Dienstleister zu achten.

Die Fernwartungs-Zugangsmöglichkeit für den Hersteller sollte nur bei Bedarf aktiviert werden und sonst vom Betreiber deaktiviert sein. Dies reduziert die Gefahr für mögliche Angriffe. Darüber hinaus sollte ein Verbindungsaufbau durch die Bediener bestätigt werden, bevor ein Zugriff auf OT-Systeme oder Komponenten möglich ist.

Tabelle 102 Verweise auf relevante Standards aus dem Abschnitt Fernwartung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
29	-	26-1 26-2 26-3	-	NRA-1 NRA-2 NRA-3 NRA-4 NRA-5

6.4.3.11 Zugriff auf das Internet aus dem OT-Netz

Durch das Surfen im Internet besteht die Gefahr der Infektion mit Schadsoftware durch Drive-By-Downloads. Zudem wird aus dem Internet häufig Schadcode nachgeladen, die Schadsoftware nimmt Befehle entgegen oder es werden Daten exfiltriert. Daher sollte der freie Zugriff auf das Internet aus dem OT-Netz unterbunden werden.

Wenn dennoch ein Zugriff auf das Internet benötigt wird, sollte dieser mittels eines Proxy-Server überwacht und auf die notwendigen Endpunkte beschränkt werden.

Tabelle 103 Weiterführende rollenspezifische Informationen aus dem Abschnitt Zugriff auf das Internet aus dem OT-Netz

Rolle	*Hinweise*
Betreiber	Dokumentation der Verbindungen und Einschränken des Datenverkehrs.
Integrator	Dokumentation der Endpunkte und Adressen im Internet auf die zugriffen werden muss und deren Zweck.
Hersteller	Dokumentation der Endpunkte und Adressen im Internet auf die zugriffen werden muss und deren Zweck.

Tabelle 104 Verweise auf relevante Standards aus dem Abschnitt Zugriff auf das Internet aus dem OT-Netz

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
51	A.8.23	-	-	-

6.4.4 Betrieb

6.4.4.1 Administration

Nur berechtige Personen sollten administrative Veränderungen an den OT-Systemen und Komponenten vornehmen dürfen. Zu den Veränderungen zählen beispielsweise:

- Installation von Software
- Austausch von Steuerungsprogrammen

Tabelle 105 Verweise auf relevante Standards aus dem Abschnitt Administration

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
	-	19-2	PR.PS-05	UAC-3

6.4.4.2 Umgang mit Sicherheitsupdates

Fehler in Software können bei aller Sorgfalt auftreten und stellen ein Problem dar. Durch Schwachstellen kann ein Angreifer Zugriff auf das System erlangen oder den Ablauf der Software stören. Daher gilt grundsätzlich, dass diese Fehler behoben werden sollten. Der Schwachstellenmanagementprozess regelt allgemein den Vorgang um über neue Schwachstellen informiert zu werden und die Sicherheitsupdates einzuplanen.

Bei einer Meldung der Schwachstelle und jeder Information zu einem Sicherheitsupdate gilt es zu prüfen:

- Bewerten der Relevanz von Schwachstellen
  - Ist die Schwachstelle in der Komponente und dem jeweiligen Einsatz ausnutzbar oder wird die Funktion nicht benutzt?
- Bewerten der Kritikalität von Schwachstellen

    - Wie schwer sind die möglichen Auswirkungen?
    - Wie einfach kann die Schwachstelle im jeweiligen Umfeld ausgenutzt werden?
- Testen & Freigabe
    - Nach Möglichkeit sollten Sicherheitsupdates vor der Installation getestet werden. Alternativ sollte für die Installation beim Betreiber eine Freigabe durch den Integrator erfolgen oder eine Bestätigung durch den Hersteller, dass sich das Systemverhalten nicht verändert.
- Einplanen der Installation des Sicherheitsupdates oder eines Workarounds im Changemanagement.
    - Dabei sollte unter anderem berücksichtigt werden:
        - Ist ein Neustart der Komponente notwendig?
        - Kann bis zum nächsten geplanten Wartungsfenster gewartet werden? Kann ein Workaround umgesetzt werden, um die Installation des Sicherheitsupdates auf einen späteren Zeitpunkt zu verschieben?
        - Wie kann bei einem Fehler der alte Zustand wiederhergestellt werden?

Tabelle 106 Weiterführende rollenspezifische Informationen aus dem Abschnitt Umgang mit Sicherheitsupdates

Rolle	*Hinweise*
Betreiber	Der Betreiber sollte mit Hersteller oder Integratoren vertraglich Zeiträume zur Freigabe und Bereitstellung von Patches und Updates oder alternativen Workarounds für Schwachstellen festlegen.

Tabelle 107 Verweise auf relevante Standards aus dem Abschnitt Umgang mit Sicherheitsupdates

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
52	A.8.8	15-1 15-2 16	PR.PS-02 PR.PS-03	SCS-7

6.4.4.3 Umgang mit End Of Support

Falls für OT-Komponenten oder Systeme der End of Support erreicht wird, können diese Komponenten aus Cybersicherheitssicht ein erhöhtes Risiko sein. Dies gilt im speziellen für Software aus dem IT-Umfeld (z. B. Betriebssysteme). In diesem Fällen ist es durchaus möglich, dass weiterhin Schwachstellen entdeckt werden, diese jedoch nicht mehr geschlossen werden. In diesem Fall sind ggf. zusätzliche Schutzmaßnahmen notwendig, z. B. die Migration auf eine neue Softwareversion.

Hierfür sollte eine Risikoanalyse durchgeführt werden und darauf aufbauend sollten in Abhängigkeit der Funktion der OT und Bedeutung für die Produktion angemessene Cybersicherheitsmaßnahmen identifiziert werden. So kann beispielsweise eine Separierung von OT-Systemen oder Komponenten mit ungepatchten Schwachstellen in ein eigenes Netzsegment und einer restriktiven Firewall zur Filterung des Datenverkehrs die Systeme schützen.

Langfristiges Ziel sollte der Austausch der vulnerablen OT-Komponenten und Systemen durch vom Hersteller unterstützte Komponenten sein. Ohne Support durch den Hersteller können zukünftig auftretende Fehler und Ausfälle die Produktion stark beeinträchtigen, da die Erarbeitung von Lösungen ohne Unterstützung durch den Hersteller aufwendiger ist.

Es sollte insbesondere bei der Anschaffung darauf geachtet werden, dass keine Komponenten zum Einsatz kommen, die bereits durch den Hersteller abgekündigt wurden.

Tabelle 108 Verweise auf relevante Standards aus dem Abschnitt Umgang mit End Of Support

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
53	-	17-1 17-2	PR.PS-02 PR.PS-03	-

Weiterführende Informationen:

- BSI-CS 145: Umgang mit End of Support in industriellen Steuerungs- und Automatisierungssystemen https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_145.pdf

6.4.5 Notfallmanagement

6.4.5.1 Datensicherung

Um das Risiko und die Folgen eines Datenverlusts zu reduzieren (z. B. durch unbeabsichtigte Änderungen der Daten, Hardwaredefekte), sollten von allen Systemen Datensicherungen durchgeführt werden.

Hierzu sollte für jedes System und den darauf ausgeführten Anwendungen die Rahmenbedingungen der Datensicherung erhoben werden. Es sollten dabei mindestens die nachfolgenden Informationen berücksichtigt werden:

- zu sichernde Daten,
- Speichervolumen,
- Änderungsvolumen,
- Änderungszeitpunkte,
- Verfügbarkeitsanforderungen,
- Vertraulichkeitsanforderungen,
- Integritätsbedarf,
- rechtliche Anforderungen,
- Anforderungen an das Löschen und Vernichten der Daten sowie
- Zuständigkeiten für die Datensicherung.

Das Datensicherungskonzept sollte die verschiedenen Ebenen der Datensicherung umsetzen. Daher sollte für den schnellen Zugriff eine Datensicherung lokal auf den IT-Systemen vorgehalten werden und zusätzlich eine Datensicherung auf einem zentralen System erfolgen.

Abhängig von Aspekten wie den Verfügbarkeitsanforderungen oder Änderungen der Daten bei Systemen kann das Intervall und der Umfang der Datensicherung variieren. So ändert sich beispielsweise die Konfiguration von Switches nur selten. Daher kann in solchen Fällen die Datensicherung auf das entsprechende Anwendungsszenario abgestimmt werden, sodass Datensicherungen z. B. ereignisbasiert durchgeführt werden können.

Die folgenden Punkte sollten beim Entwurf eines Datensicherungskonzepts beachtet werden:

- Definitionen zu wesentlichen Aspekten der Datensicherung (z. B. unterschiedliche Verfahrensweisen zur Datensicherung),
- Gefährdungslage,
- Einflussfaktoren je System oder Gruppe von Systemen,
- Datensicherungspläne je System oder Gruppe von Systemen sowie
- relevante Ergebnisse des Notfallmanagements/BCM

Die Datensicherung sollte generell alle Daten auf den Medien des OT-Systems miteinschließen. Dazu zählen beispielsweise:

- Betriebssystem und Firmware,
- Konfigurationen (z. B. Router, Switches, Anwendungen, Firewall Regelwerk),
- Anwendungen,
- Datenbanken,
- Produktionsdaten,
- sonstige Daten (z. B. Protokolldaten).

Die Datensicherung sollte sowohl inkrementelle als auch vollständige Backups umfassen. Falls möglich sollte die lokale Datensicherung täglich erfolgen. Für diesen Zweck kann beispielsweise eine zweite Festplatte verbaut werden.

Es sollten Daten zur Sicherstellung der Integrität in der Datensicherung enthalten sein, sodass unbefugte Änderungen oder Defekte erkannt werden.

Der Umfang der Datensicherung (z. B. inkrementell, vollständig) sollte für jedes OT-System mit dem Datum der zuletzt durchgeführten Datensicherung dokumentiert werden.

Wird die Datensicherung automatisiert durchgeführt, sollten Überwachungsfunktionen etabliert werden, die aufzeigen können, ob eine Datensicherung erfolgreich durchgeführt wurde.

Datensicherungen sollten sequenziell bei den IT-Systemen durchgeführt werden. Es ist darauf zu achten, dass die zur Verfügung stehenden Kommunikationswege, über die die Datensicherung durchgeführt wird, nicht überlastet werden und es dadurch zu funktionellen Fehlern im Prozess kommt.

Tabelle 109 Weiterführende rollenspezifische Informationen aus dem Abschnitt Datensicherung

Rolle	*Hinweise*
Betreiber	Planen und Umsetzen der Datensicherungen.
Integrator	Bereitstellen von Funktionen und Anleitungen zur Datensicherungen
Hersteller	Bereitstellen von Funktionen und Anleitungen zur Datensicherungen

Tabelle 110 Verweise auf relevante Standards aus dem Abschnitt Datensicherung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A.8.13	11-1 12 13-1 13-2 14-1 14-2 14-3	PR.DS-11	-

6.4.5.2 Wiederherstellung & Wiederanlauf

Der Wiederherstellungsplan beschreibt den Ablauf um nach einem Cybersicherheitsvorfall wieder in den Normalbetrieb zu gelangen und den Zustand, in dem die OT wieder einsatzbereit ist.

Folgend Punkte sollten unter anderem in einem Wiederherstellungsplan beinhaltet sein:

- Für welche ICS-Komponente der Wiederherstellungsplan angewendet werden kann (Geltungsbereich)
- Der Prozess für die Aktivierung des Wiederherstellungsplanes

- Die Zuständigkeiten und involvierten personellen Ressourcen (intern wie extern).
- Die für die Wiederherstellung des Systems benötigten Ressourcen und die dafür erforderlichen Dokumentationen
- Die Voraussetzungen für die Wiederherstellung des Systems
- Detaillierte Ablaufplan der Wiederherstellung der Komponente
- Test- bzw. Prüfmaßnahmen am Ende der Wiederherstellung und vor dem Wiederanlauf der OT
- Auflistung und Kontakte von unterstützenden Dienstleistern

Der Wiederherstellungsplan sollten regelmäßig, mindestens jährlich und in jedem Fall bei relevanten Änderungen in der OT überprüft und ggf. angepasst werden.

Die beschriebenen Abläufe sollten regelmäßig geübt werden. Erkenntnisse aus den durchgeführten Übungen sollten eingearbeitet werden.

Tabelle 111 Weiterführende rollenspezifische Informationen aus dem Abschnitt Wiederherstellung & Wiederanlauf

Rolle	*Hinweise*
Betreiber	Eine regelmäßige Prüfung der Wiederherstellungs-Pläne sowie eine Anpassung bei Veränderungen innerhalb der Systeme (OT, ICS, Komponenten) sollte sichergestellt werden.
Integrator	Die Abhängigkeiten des Wiederanlaufes von Systemkomponenten sollten in der Dokumentation des jeweiligen Systems mit aufgenommen werden. Dem Betreiber sollten Empfehlungen zum Ablauf einer Wiederherstellung zur Verfügung gestellt werden.
Hersteller	Bereits bei der Entwicklung von Systemen und Komponenten sollten die Möglichkeiten einer zügigen Wiederherstellung mitberücksichtigt werden. So sollte der Austausch von Teilkomponenten möglich sein. Die Übernahme von Konfigurationen z. B. durch einen wechselbaren Speicher-Chip oder das Wiedereinspielen von vorhandenen Konfigurationsdaten sollte unkompliziert möglich sein.

Tabelle 112 Verweise auf relevante Standards aus dem Abschnitt Wiederherstellung & Wiederanlauf

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
-	A8.13	-	PR.DS-11 RC.RP-02 RC.RP-03 RC.RP-04 RC.RP-05 RC.RP-06	AVA-1 AVA-2

6.4.6 Authentisierung

6.4.6.1 Technische Authentisierungsmaßnahmen

Soweit möglich, sollte die Nutzung aller OT-Systeme und Komponenten eine Authentisierung der Benutzer und Dienste erfordern, sodass eine Bedienung der Systeme nur im authentisierten Zustand möglich ist. Ein unbefugter Zugriff auf Systeme sollte verhindert werden. Es sollte erkennbar und dokumentiert sein, welcher Benutzer aktiv war. Eine reine Anzeige von Zustandsinformationen ohne Bedienmöglichkeit kann auch ohne Authentisierung möglich sein.

Zur Authentisierung können unterschiedliche Verfahren und Merkmale eingesetzt werden. Es wird zwischen den Authentisierungsmerkmalen Wissen (z. B. Passwort, PIN), Besitz (z. B. Token, Smartcard, Zertifikat) und biometrische (körperliche) Merkmale (z. B. Fingerabdruck, Iriserkennung) unterschieden. Zur

Authentisierung können bspw. technische Lösungen wie kontaktbehaftete oder kontaktlose Chipkarten genutzt werden, um die Eingabe von Passworten zu vermeiden.

Zusätzlich zu einem Merkmal können auch weitere Merkmale zur Authentisierung herangezogen werden und so ein höheres IT-Sicherheitsniveau etablieren (z. B. Zwei-Faktor-Authentisierung mittels Token und Passwort). Hierbei sollten Merkmale aus unterschiedlichen Klassen (Wissen, Besitz, Biometrie) kombiniert werden.

Bei bzw. vor der Auswahl der Authentisierungsmethoden ist eine Risikoanalyse durchzuführen. Diese Analyse muss mit weiteren Anforderungen (z. B. 12. BImschV) und organisatorischen Rahmenbedingungen (z. B. Zugangsrestriktionen) abgeglichen werden, um zu einer geeigneten Auswahl zu kommen.

Tabelle 113 Verweise auf relevante Standards aus dem Abschnitt Technische Authentisierungsmaßnahmen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
54	A.8.3 A.8.5	08-2 10 23	PR.AA-03	-

6.4.6.2 Passwortverteilung und -management, Passwort-Richtlinie

Es sollte eine Passwort-Richtlinie erstellt und umgesetzt werden, welche die folgenden Punkte berücksichtigt. Dabei können technische Lösungen als auch organisatorische Maßnahmen festgelegt werden.

- Der Benutzer sollte durch Komplexitätsanforderungen daran gehindert werden, schwache Passwörter zu wählen (z. B. Länge, Alphabet mit Zahlen und Sonderzeichen).
- Die Anzahl fehlgeschlagener Anmeldeversuche sollte begrenzt werden (z. B. temporäre Sperrung des Benutzerkontos).

Die Verwaltung der genannten Anforderungen sollte vorzugsweise über eine zentrale Management-Lösung realisiert werden (z. B. in einem Verzeichnisdienst innerhalb der OT).

Nicht alle Maßnahmen sind vollumfassend auf alle OT-Systeme und Komponenten anwendbar. So kann beispielsweise ein Angreifer durch provozierte, fehlgeschlagene Anmeldeversuche das Benutzerkonto sperren. Somit wäre ein Zugriff auf das betroffene System durch den legitimen Benutzer nicht mehr möglich. Daher muss der Sicherheitszugewinn durch die jeweilige Maßnahme und mögliche Einschränkungen sonstiger Anforderungen an die OT (z. B. erforderlicher, unmittelbarer Zugriff) gegeneinander abgewogen werden.

Tabelle 114 Verweise auf relevante Standards aus dem Abschnitt Passwortverteilung und -management, Passwort-Richtlinie

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
55	A.8.5	09-1 09-1	PR.AA-05	-

6.4.6.3 Autorisierung

Soweit möglich sollten auf allen OT-Systemen und Komponenten in Abhängigkeit von dem angemeldeten Benutzer nur die jeweils erforderlichen Zugriffsrechte vergeben sein. Dementsprechend sollte die Berechtigungsvergabe z. B. auf das Dateisystem dem Prinzip der geringsten Privilegien folgen (engl. principle of least privilege*)*. Einem Benutzer oder Dienst sollten somit nur solche Rechte zugewiesen werden, die zur Durchführung seiner Tätigkeiten erforderlich sind.

Gewöhnlich werden Zugriffsrechte auf Dateisystem-Ebene (Lesen, Schreiben, Ausführen und Löschen von Dateien) und auf Netzebene (Zugriff auf Netze und Netzdienste) vergeben.

Privilegierte Nutzerrechte sollten auf das notwendige Minimum im jeweiligen Bereich reduziert werden.

Bei der Verwaltung von Benutzern, Gruppen und Berechtigungen (z. B. in Windows-Netzen) ist es zu empfehlen, Benutzerkonten Gruppen zuzuordnen und auf diese Gruppen Berechtigungen zu vergeben. Somit wird ein sogenanntes rollenbasiertes Berechtigungskonzept umgesetzt (engl. Role Based Access Control; *RBAC)*.

Tabelle 115 Verweise auf relevante Standards aus dem Abschnitt Autorisierung

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
57	A.8.3 A.8.5 A.8.18	08-2	PR.PS-05	-

6.4.7 Schutz vor Schadprogrammen

6.4.7.1 Unterstützung von Lösungen zum Schutz vor Schadsoftware

Es sollte geprüft werden, ob OT-Systeme und Komponenten mit einem Schutz vor Schadsoftware sinnvoll ausgestattet werden können. Einschränkende Faktoren können sein:

- begrenzte Systemressourcen
- mögliche Beeinflussung von Produktionsparametern (z. B. Zeitverhalten)
- keine Möglichkeit für die zeitnahe Versorgung mit aktuellen Daten und Signaturen zur Erkennung.

Wenn dies nicht der Fall ist, sollte der Betrieb von Anwendungen zum Schutz vor Schadsoftware unterstützt werden. Ansonsten sollten alternative Maßnahmen ergriffen werden. Dazu gehören beispielsweise Application-Allow-Listing (siehe 6.4.7.4 Application Allow Listing) und entsprechende Protokollierungswerkzeuge (siehe 6.4.8 Monitoring).

Tabelle 116 Weiterführende rollenspezifische Informationen aus dem Abschnitt Unterstützung von Lösungen zum Schutz vor Schadsoftware

Rolle	*Hinweise*
Betreiber	Planen und Umsetzen von Konzepten zum Schutz vor Schadsoftware auf Basis der gegebenen Rahmenbedingungen.
Integrator	Bei der Entwicklung von neuen Anlagen und Maschinen sollten bereits Konzepte und Maßnahmen zum Schutz vor Schadsoftware berücksichtigt werden.
Hersteller	Bei der Entwicklung von neuen Komponenten sollten bereits Konzepte und Maßnahmen zum Schutz vor Schadsoftware berücksichtigt werden.

Tabelle 117 Verweise auf relevante Standards aus dem Abschnitt Unterstützung von Lösungen zum Schutz vor Schadsoftware

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
28	A.8.7	-	-	-

6.4.7.2 Installation und Betrieb von Programmen zum Schutz vor Schadsoftware

Ist die Installation und der uneingeschränkte Betrieb von Programmen zum Schutz vor Schadsoftware auf einem OT-System oder Komponente möglich und durch den Hersteller freigegeben, sollten diese Systeme automatisiert mit aktuellen Signaturen versorgt werden.

Gewöhnlich werden vom Hersteller die folgenden ICS-Komponenten für die uneingeschränkte Installation und den Betrieb von Software zum Schutz vor Schadsoftware freigegeben:

- EWS,
- Systeme für die Prozessdatenverarbeitung und -darstellung,
- Bedien- und Beobachtungssysteme,
- Asset Management Systeme und

- Systeme für Konfiguration der Feldgeräte.

Grundsätzlich sollten folgende Einstellungen bei der Konfiguration der Software zum Schutz vor Schadsoftware berücksichtigt werden:

- Manuelle Scans sollten ausschließlich bei Stillstand der Produktion durchgeführt und dokumentiert werden.
- Ausschließlich lokale Medien sollten geprüft werden. Netzlaufwerke sollten nicht gescannt werden, um parallele Scans durch mehrere Rechner zu vermeiden.
- Nur der jeweils verantwortliche Administrator sollte die Befugnisse haben, Programme zum Schutz vor Schadsoftware zu konfigurieren oder zu deaktivieren.
- Verdachtsfälle oder gefundene Schadsoftware sollten automatisch an einer zentralen Stelle gemeldet und bewertet werden.

Das Aktualisieren der Signaturen zum Erkennen von Schadsoftware sollte bei der Planung mitberücksichtigt werden. Dabei sollte der eingeschränkte Zugriff auf das Internet berücksichtigt werden. Ebenfalls sollten die Zeitpunkte für das Aktualisieren betrachtet und geeignet gewählt werden.

Der Installationsprozess sowie die Konfiguration sollten für jedes OT-System und Komponente dokumentiert werden.

Tabelle 118 Weiterführende rollenspezifische Informationen aus dem Abschnitt Installation und Betrieb von Programmen zum Schutz vor Schadsoftware

Rolle	*Hinweise*
Betreiber	Aktivieren der Schutzprogramme unter Berücksichtigung der Empfehlungen der Integratoren und Hersteller.
Integrator	Empfehlung / Freigabe für den Einsatz erteilen. Hinweise zum Betrieb dokumentieren
Hersteller	Empfehlung / Freigabe für den Einsatz erteilen. Hinweise zum Betrieb dokumentieren

Tabelle 119 Verweise auf relevante Standards aus dem Abschnitt Installation und Betrieb von Programmen zum Schutz vor Schadsoftware

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
59, 61, 62, 63	A.8.7	18 19-1	-	-

6.4.7.3 Einsatz von Alternativen zu Programmen zum Schutz vor Schadsoftware

Es gibt Fälle, bei denen keine oder nur eine eingeschränkte Installation eines Programms zum Schutz vor Schadsoftware auf einem OT-System oder Komponente möglich ist (z. B. es steht kein Programm zum Schutz vor Schadsoftware für das Betriebssystem oder die Hardware zur Verfügung). Davon betroffen sind üblicherweise Steuerungssysteme, SPS und Feldgeräte. In diesem Fall müssen zusätzliche, kompensierende Sicherheitsmaßnahmen umgesetzt werden, um die Systeme ausreichend vor Schadprogrammen zu schützen. Die folgende Liste führt einige beispielhafte Kriterien zur Identifikation solcher Systeme auf:

- Der Hersteller hat keine Programme zum Schutz vor Schadsoftware freigegeben.
- Es ist nur ein eingeschränkter Betrieb der Software zum Schutz vor Schadprogrammen möglich, sodass kein hinreichender Sicherheitsgewinn besteht.
- Die Signaturen können nicht zeitnah aktualisiert werden (z. B. tägliche Updates).
- Es besteht ein zu hohes Risiko, dass die Verfügbarkeit beeinträchtigt wird.

Ausgehend von individuellen Risikoanalysen für jede OT-Komponente sollte eine angemessene Kombination an kompensierenden Schutzmaßnahmen identifiziert werden. Dazu zählen unter anderem folgende Sicherheitsmaßnahmen:

- Einsatz einer Wechseldatenträgerschleuse, wenn Wechseldatenträger an das Gerät angeschlossen werden
- falls möglich, regelmäßiges Scannen des ICS von einem Boot-Medium oder USB-Device mit aktueller Software zum Schutz vor Schadprogrammen und Signaturen, beispielsweise während eines geplanten Wartungsfensters (auf diese Weise kann, wenn auch verspätet, eine Infektion erkannt und dann beseitigt werden),
- Ausgliederung der betroffenen ICS in ein eigenes Netzsegment mit einer Filterkomponente
- Application Allow Listing
- Deaktivierung von Dateifreigaben im Netzwerk.

Tabelle 120 Verweise auf relevante Standards aus dem Abschnitt Einsatz von Alternativen zu Programmen zum Schutz vor Schadsoftware

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*
60	A.8.7	-	-

6.4.7.4 Application Allow Listing

Es besteht die Möglichkeit, mittels spezieller Software zur Applikationskontrolle das Ausführen von Programmen zu überwachen und einzuschränken. Anders als bei Programmen zum Schutz vor Schadprogrammen wird nicht versucht unerwünschte Software zu blockieren, sondern es wird der Ansatz verfolgt, ausschließlich erwünschten Programmen die Ausführung zu erlauben.

Beim Application-Allow-Listing werden nur solche Anwendungen und solches Verhalten erlaubt, welches explizit freigegeben wurde. Alles andere ist verboten. Im Gegensatz zu Programmen zum Schutz vor Schadprogrammen gibt es keine Signaturen für potentielle Schadsoftware. Insbesondere bei Systemen wie in der OT, die nur geringfügigen Änderungen durch Updates unterliegen, eignet sich dieses Verfahren.

Um das Ausführen von unerlaubter Software zu verhindern, kann eine solche Schutzsoftware beispielsweise auf folgende unterschiedliche Attribute zurückgreifen:

- Zertifikate (Signieren von vertrauenswürdiger Software z. B. durch eine zentrale Stelle),
- Dateisystempfad (Bestimmte Bereiche werden als vertrauenswürdig deklariert),
- Hashwert (Die Anwendungen und möglicherweise unbefugte Änderungen werden anhand eines Hashwertes der Dateien identifiziert),
- System- und Benutzerverhalten (z. B. Nutzung gewisser TCP-Ports, Bedienung nur zu bestimmten Zeiten).

Tabelle 121 Verweise auf relevante Standards aus dem Abschnitt Application Allow Listing

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
65	A.8.7	-	PR.PS-05	-

6.4.8 Monitoring

6.4.8.1 Protokollierungs- und Detektionskonzept

Durch ein zeitnahes Erkennen von sicherheitsrelevanten Ereignissen kann frühzeitig auf diese reagiert und ggf. ein möglicher Schaden abgewendet werden.

Es sollte ein Konzept für die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen erstellt werden. Dabei sollten zum einen die Anforderungen und Vorgaben beschrieben werden, zum anderen ist zu planen wie die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen umgesetzt und sicher betrieben werden kann.

Das Sicherheitskonzept zur Protokollierung und Detektion von Sicherheitsereignissen soll u.a. nachfolgende Aspekte betrachten:

- Definition der zu detektierenden Ereignisse
- die Kritikalität des zu detektierenden Ereignisses
- die hierfür notwendigen Informationen und Daten
- die Sensoren (Quellen) über die die notwendigen Daten erlangt werden
- die einzusetzenden Systeme zur Korrelation und Analyse der Protokollierungsdaten
- die Korrelations-Logik von Daten unterschiedlicher Quellen
- die Speicherung (Ort, Vorhaltezeitraum, etc.)
- die Zugriffsberechtigungen auf die erhobenen Daten
- die Zeitsynchronisation

Die Protokollierungsdaten sollten auf einem zentralen Server gespeichert werden. So können die Protokollierungsdaten von verteilten Systemen und Komponenten zentral gesammelt, analysiert und in Zusammenhang gebracht werden. In den Protokollierungsdaten sollten keine sensiblen und vertraulichen Daten, wie z. B. Passwörter, enthalten sein.

Innerhalb des spezifische Sicherheitskonzepts zur Detektion von Sicherheitsereignissen müssen die Anforderungen des Datenschutzes mitberücksichtigt werden.

In der OT sollten folgenden Ereignisse protokolliert und zentral gesammelt werden, soweit diese verfügbar sind:

- lokale Ereignisse, z. B. der Betriebssysteme,
- Ereignisse von Domänen-Controllern,
- Firewall-/Router-/Switch-/Server-Ereignisse,
- Ereignisse der Software zum Schutz vor Schadsoftware,
- Ereignisse des Netzwerk- bzw. Host-basierte IDS/IPS.

Zusätzlich sollten zu den vorher genannten Ereignissen folgende Daten aufgezeichnet werden:

- Datum und Zeit,
- Beschreibung des Ereignisses,
- Kritikalität,
- Quelle des Ereignisses, z. B. Anwendung, Betriebssystem.
- Betroffenes OT-System/-Prozess

Über das Sicherheitskonzept zur Detektion von Sicherheitsereignissen sollte definiert werden, wie eine kontinuierliche Überwachung der Protokolldaten erfolgt, welche Systeme hierfür eingesetzt und wie diese betrieben werden.

Das spezifische Sicherheitskonzept zur Detektion von Sicherheitsereignissen sollte allen im Bereich Detektion zuständigen Mitarbeitenden bekannt, Aspekten des Datenschutzes Rechnung tragen und grundlegend für ihre Arbeit sein.

Tabelle 122 Weiterführende rollenspezifische Informationen aus dem Abschnitt Protokollierungs- und Detektionskonzept

Rolle	*Hinweise*
Betreiber	Der Betreiber passt, auf Basis der gemachten Betriebserfahrung sowie der Entwicklung der Risiko-Lage dem das ICS ausgesetzt ist, das Protokollierungs- und Überwachungs-Konzept regelmäßig an. Insbesondere werden Erkenntnisse aus dem Schwachstellenmanagement zeitnah in das Sicherheitskonzept zur Detektion von Sicherheitsereignissen aufgenommen.
Integrator	Die zentrale Speicherung und Auswertung von Protokollierungsdaten sind bei der Integration von OT-Systemen und Komponenten mit zu berücksichtigen. Die OT-Systeme und Komponenten sollten die Systemuhr synchronisieren können. Gemeinsam mit dem Betreiber sind die sicherheitsrelevanten Ereignisse zu definieren und zu dokumentieren.
Hersteller	Eine Anbindung an ein zentrales Protokollierungs-System sollte bereits bei der Entwicklung der OT-Systeme und Komponente berücksichtigt werden. Die OT-Systeme und Komponente sollte dabei über eine Protokollierung verfügen, die alle relevanten Ereignisse dokumentiert. Die relevanten Ereignisse sowie der Umfang der Protokollierung sind in der Systemdokumentation zu beschreiben.

Tabelle 123 Verweise auf relevante Standards aus dem Abschnitt Protokollierungs- und Detektionskonzept

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
42	A.8.15 A.8.16	-	PR.PS-04 DE.CM-03 DE.CM-06 DE.CM-09 DE.AE-02 DE.AE-03 DE.AE-04 DE.AE-06 DE.AE-08	NRA-4

6.4.8.2 Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen

Mithilfe von Intrusion-Detection-Systemen (IDS) und Intrusion-Prevention-Systemen (IPS) lassen sich Angriffsversuche in einer frühen Phase erkennen, sodass verantwortliche Personen rechtzeitig alarmiert wird (z. B. durch ein IDS) oder bereits eine automatisierte Reaktion auf den Angriff eingeleitet wird (z. B. durch ein IPS).

Typische Vorfälle und Ereignisse, die durch ein solches System erkannt werden können, sind z. B. unbefugte Zugriffe auf Systeme und die unbefugte Installation von Software oder Manipulationen von Daten. Zudem können hierdurch auch unbeabsichtigte und versehentliche Änderungen (z. B. in Konfigurationsdateien) bemerkt werden.

Ein IDS/IPS kann einzelne Server oder Clients überwachen (Hostbasierte IDS/IPS: HIDS/HIPS) oder durch Sensoren im Netz den Datenverkehr prüfen (Netzbasiertes IDS/IPS: NIDS/NIPS).

Wird ein NIDS/NIPS verwendet, so sollten die Sensoren im Netz zur Überwachung des Datenverkehrs insbesondere bei externen Schnittstellen platziert werden (z. B. als Teil der DMZ). Von externen Schnittstellen geht gewöhnlich eine höhere Bedrohung durch Angriffe aus (z. B. Internet). Ebenso sollte ein HIDS auf allen OT-Systemen installiert werden. Die Protokolldaten des HIDS sollten in ein zentrales Logging integriert werden.

IDS/IPS sind Teil des Monitorings und sollten als zusätzliche Informationsquelle angesehen werden. Sie ersetzen kein Monitoring der Systeme und des Netzes (z. B. mittels eines Security Information Event Management (SIEM) Systems).

Für den Einsatz und der Betrieb eines IDS sollten ausreichend Ressourcen verfügbar sein. Die Einrichtung, die Pflege und die Sichtung der Meldungen (insbesondere in der Anfangsphase) sind mit einem nicht unerheblichen Aufwand verbunden. Daher müssen erst die grundlegenden Schutzmaßnahmen umgesetzt sein, bevor ein IDS zum Einsatz kommt.

Bei der Umsetzung eines IPS ist zudem zu beachten, dass bei der Planung auch sehr spezielle Situationen berücksichtigt werden, damit diese legitimen Übertragungen nicht verhindert werden. Vor einer Aktivierung dieser Funktionen ist daher eine sehr sorgfältige Probephase zu absolvieren. Insbesondere IPS sollten mit Bedacht eingesetzt werden. Vorrangig ist hier der laufende Betrieb, der ggf. durch ein fehlerhaftes Eingreifen des IPS gestört werden könnte.

Die Effektivität eines IDS/IPS ist stark abhängig von einer angepassten und individuellen Konfiguration. So kann die Effektivität beispielsweise durch eine hohe Anzahl an immer wiederkehrenden False Positives beeinträchtigt werden.

Daher erfordert nicht nur die initiale Konfiguration des IDS/IPS ein geschultes Fachpersonal, sondern auch im Betrieb muss das Personal im Notfall einen gemeldeten Angriffsversuch von einem False Positive unterscheiden können. Das Personal sollte zeitnah erreichbar sein, sodass nach der Klassifizierung der Meldung ggf. entsprechende Gegenmaßnahmen eingeleitet werden können.

Erstellung von Ablaufplänen, sogenannten Playbooks, können bei der Bewertung und Behandlung von Meldungen unterstützen.

Tabelle 124 Weiterführende rollenspezifische Informationen aus dem Abschnitt Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen

Rolle	*Hinweise*
Betreiber	Prüfung, ob Ressourcen für Betrieb vorhanden sind, Planung des Einsatzes und Berücksichtigen der Hinweise der Integratoren und Hersteller
Integratoren/ Hersteller	Bereitstellen der notwendigen Informationen zum Einsatz von IDS wie z. B. Protokolle und Kommunikationspartner Bereitstellen der notwendigen Informationen zum Einsatz von IDS wie z. B. Protokolle

Tabelle 125 Verweise auf relevante Standards aus dem Abschnitt Implementierung von Intrusion-Detection- bzw. Intrusion-Prevention-Systemen

ICS-Security-Kompendium (2013)	*ISO/IEC 27001:2021*	*DIN SPEC 27076:2023*	*NIST CSF 2.0 Draft 2023*	*VDMA-Mindestanforderungen (22)*
42	A.8.15 A.8.16	-	PR.PS-04 DE.CM-01	-

7 Audits, Assessments und Tests

7.1 Prüfung von OT-Netzwerken und -Systemen

In dem genannten Kapitel wird eine Darstellung verschiedener Arten von Audits für OT-Netzwerke und -Systeme gegeben sowie deren Vorgehensweise erläutert. Es wird auch darauf hingewiesen, dass die verschiedenen Arten von Audits bei Bedarf miteinander kombiniert werden können.

7.1.1 Initiales Assessment

Das initiale Assessment zur Identifizierung von technischen und organisatorischen Schwachstellen in OT-Netzwerken und zur Feststellung des aktuellen Zustands umfasst eine Reihe von Schritten. Der Zweck dieses Assessments besteht darin, die Sicherheitsstandards zu evaluieren, um den gegenwärtigen Zustand zu ermitteln und Abweichungen zu erkennen. Im Folgenden wird die Vorgehensweise beschrieben:

1 Physische Begehung

Im Rahmen des initialen Assessments wird eine physische Begehung der OT durch einen Fachexperten durchgeführt. An den Standorten, an denen sich die OT-Systeme befinden, erfolgt eine detaillierte Erfassung der Infrastruktur, Geräte und Komponenten vor Ort. Hierdurch wird eine visuelle Inspektion der physischen Sicherheitsmaßnahmen ermöglicht, wie beispielsweise Zutrittskontrollen, Überwachungskameras und Schutzvorrichtungen.

2 Interviews mit Wartungspersonal

Während der physischen Begehung werden Gespräche mit dem verantwortlichen Personal der OT-Systeme geführt. Dabei werden Fragen zur aktuellen Konfiguration, den Wartungsverfahren, den Zugriffsrechten, den Sicherheitsrichtlinien und möglichen Schwachstellen gestellt. Das Wartungspersonal sind häufig diejenigen, die über das umfassendste Wissen bezüglich der Systeme verfügen und somit wertvolle Einblicke in den Betrieb sowie die Sicherheitsmaßnahmen bieten können.

3 Bewertung der Cybersicherheitsstandards

Im anschließenden Schritt werden die aktuellen Sicherheitsstandards und bewährten Verfahren für OT-Netzwerke konsultiert. Diese können Industriestandards wie IEC 62443 oder branchenspezifische Leitlinien umfassen. Die existierenden Sicherheitsrichtlinien und -verfahren werden mit den Anforderungen dieser Standards abgeglichen, um Abweichungen zu erkennen.

4 IST-Zustand ermitteln

Basierend auf den Erkenntnissen aus den physischen Begehungen und den Gesprächen sowie dem Abgleich mit den Sicherheitsstandards wird der gegenwärtige IST-Zustand des OT-Netzwerks ermittelt. Hierbei werden sowohl technische als auch organisatorische Schwachstellen herausgearbeitet. Dies kann Defizite in den Sicherheitsmaßnahmen, veraltete Systeme, unangemessene Zugangskontrollen, fehlende Schulungsmaßnahmen oder andere Schwachstellen einschließen.

5 Abweichungen feststellen

Mittels des Abgleichs mit den Sicherheitsstandards werden Abweichungen und mögliche Risiken identifiziert. Es wird festgestellt, an welchen Stellen das OT-Netzwerk von den empfohlenen Sicherheitsstandards abweicht und welche potenziellen Auswirkungen dies haben könnte. Diese Abweichungen bilden die Grundlage für die Ausarbeitung von Vorschlägen zur Verbesserung sowie für die Formulierung von Maßnahmen zur Stärkung der Sicherheit des OT-Netzwerks.

Das initiale Assessment legt den Grundstein für nachfolgende Schritte, wie die Ausarbeitung eines Sicherheitskonzepts, die Umsetzung von Sicherheitsmaßnahmen und periodische Überprüfungen. Diese Schritte gewährleisten, dass das OT-Netzwerk zukünftig optimal gegen Bedrohungen abgesichert ist.

7.1.2 Physische Begehung

Bei einer physischen Begehung sollten regelmäßig die folgenden Prüfmethoden angewandt werden:

- Inaugenscheinnahme von ICS-Komponenten und Räumlichkeiten: Untersuchung der physischen Aspekte von ICS-Komponenten und Räumen.
- Übereinstimmung der Komponenten mit der Inventarliste und der dokumentierten Funktion: Prüfung, ob die Komponenten den Angaben in der Inventarliste und den dokumentierten Funktionen entsprechen.
- Identifizierung nicht vorgesehener bzw. nicht dokumentierter Schnittstellen (z. B. Netzverkabelung): Erkennen von nicht beabsichtigten oder nicht dokumentierten Verbindungen oder Schnittstellen.
- Zutrittsbeschränkung und Abweichungen von der Raumplandokumentation: Überprüfung, ob Räume entsprechend den Dokumenten zugangsbeschränkt sind und ob es ungeplante Änderungen oder Abweichungen von der Raumplanung gibt.
- Eindeutige Bezeichnung und Zuordnung der Systeme zu Produktionsbereichen: Sicherstellen, dass Systeme klar gekennzeichnet sind und den jeweiligen Produktionsbereichen zugeordnet werden können (z. B. Schild mit Anlagenkennzeichen (AKZ) auf Gerät, Schaltunterlagen, Geräteliste).
- Beobachtung von relevanten Ereignissen durch das Auditteam: Beobachtung von wichtigen Vorgängen oder Auffälligkeiten durch das Auditteam.
- Verständnis für Besonderheiten des Produktionsprozesses: Verstehen der spezifischen Abläufe und Besonderheiten des Produktionsprozesses.
- Überprüfung des Clear-Desk- und Clear-Screen-Status: Feststellen, ob Schreibtische und Bildschirme frei von sensiblen Informationen sind.
- Technische Prüfung von Sicherheitseinrichtungen und -funktionen: Überprüfung von Sicherheitsaspekten wie Alarmanlagen, Zutrittskontrollen und Schließzuständen.
- Bedienung von Anlagen und HMI durch sachkundiges Personal: Test der Anlagenbedienung durch qualifiziertes Personal.
- Überprüfung von automatisierten Abschaltvorgängen: Test der automatisierten Abschaltmechanismen.
- Testweises Auslösen von Sensoren (z. B. Lichtschranken, Vibration, Hitze, Wasser, Rauch): Durchführen von Tests, um Sensoren auf ihre Funktionalität zu prüfen.
- Einsichtnahme in Daten (z. B. Logdateien, HMI-Zugang, gedruckte Protokolle): Überprüfung von Aufzeichnungen und Daten, wie z. B. Logdateien und HMI-Zugriffe.
- Identifizierung sicherheitsrelevanter Ereignisse in den Aufzeichnungen: Erkennen von sicherheitsrelevanten Vorfällen oder Ereignissen in den Aufzeichnungen.
- Überprüfung von ergriffenen Maßnahmen (Angemessenheit, Vollständigkeit, Wirksamkeit): Bewertung der Wirksamkeit und Angemessenheit der ergriffenen Sicherheitsmaßnahmen.
- Überprüfung der Einhaltung von Dokumentationspflichten: Kontrolle der ordnungsgemäßen Dokumentation.
- Durchführung von Checklisten: Abhaken von Checklisten und Vergleich mit den vorgegebenen Kriterien.

Diese Prüfmethoden dienen dazu, die Sicherheit und Integrität von ICS-Netzwerken zu gewährleisten und potenzielle Schwachstellen aufzudecken.

7.1.3 Gap-Analyse

Eine Gap-Analyse ist ein Instrument, das dazu dient, Unterschiede oder Abweichungen (sogenannte Gaps) zwischen den aktuellen Gegebenheiten und den angestrebten Zielen oder Anforderungen aufzudecken. Bei der Einhaltung von Normen wie beispielsweise der IEC 62443 oder anderen relevanten Standards bezieht sich eine Gap-Analyse auf die Prüfung der Konformität eines Betreibers mit den Vorgaben dieser Normen. Hier ist eine Schritt-für-Schritt-Anleitung für eine Gap-Analyse:

1 **Bestimmung des aktuellen Zustands**

   Analyse der bestehenden Prozesse, Richtlinien, Systeme und Sicherheitskontrollen, um festzustellen, inwiefern sie den Anforderungen der Norm entsprechen.

2 **Identifizierung der Anforderungen**

   Die Anforderungen der Norm genau durchgehen und mit den vorhandenen Sicherheitsmaßnahmen und -praktiken vergleichen, um Gaps zu erkennen.

3 **Bewertung der Auswirkungen**

   Die Auswirkungen der identifizierten Gaps bewerten, diese nach Dringlichkeit und Relevanz klassifizieren.

4. **Erstellung eines Maßnahmenplans**

   Basierend auf der Bewertung der Auswirkungen sollte ein Maßnahmenplan entwickelt werden, um die festgestellten Gaps zu schließen. Der Plan sollte klare Ziele, Maßnahmen und Zeitpläne enthalten, um die Konformität mit den Normen zu erreichen.

4 **Umsetzung des Maßnahmenplans**

   Die festgelegten Maßnahmen unter Einbeziehung aller relevanten Stakeholder implementieren, um eine effektive Umsetzung sicherzustellen.

5 **Überprüfung und Wirksamkeit**

   Den Fortschritt bei der Schließung der Gaps überwachen und die Wirksamkeit der implementierten Maßnahmen organisatorisch und technisch bewerten.

6 **Erstellung eines Abschlussberichts**

   Einen Abschlussbericht erstellen, der den Status der Gap-Analyse, die identifizierten Gaps, den Maßnahmenplan und den erreichten Fortschritt zusammenfasst. Der Bericht sollte auch Empfehlungen für zukünftige Maßnahmen enthalten, um die Sicherheit von OT-Systemen weiter zu verbessern.

7.1.4 Vulnerability Assessments

Ein Vulnerability Assessment ist ein Prüfverfahren, bei dem Schwachstellen und Sicherheitslücken in einer Netzwerkinfrastruktur identifiziert und bewertet werden. Die Nutzung von Netzwerkanalysetools stellt eine gängige Methode dar, um den Netzwerkverkehr zu überwachen und potenzielle Anomalien oder Sicherheitsrisiken aufzuspüren. Bei der Einbeziehung industrieller Netzwerkswitche in das Assessment sind jedoch einige zusätzliche Überlegungen zu berücksichtigen:

1. **Netzwerkinfrastrukturbewertung**

   Vor der Durchführung des Vulnerability Assessments ist es von Bedeutung, die Netzwerkinfrastruktur zu analysieren. Hierbei geht es um die Identifikation der relevanten Netzwerkswitche, die für das Überwachen des Netzwerkverkehrs eingesetzt werden sollen.

Industrielle Umgebungen können komplexe Netzwerke aufweisen, daher ist es essenziell, die Netzwerkarchitektur zu verstehen, um die passenden Switche auszuwählen.

2. **Auswahl von Netzwerkanalysetool**

   Netzwerkanalysetools sind Werkzeuge zur Überwachung und Analyse des Netzwerkverkehrs. Bei der Wahl von Netzwerkanalysetools für industrielle Netzwerkswitche ist sicherzustellen, dass sie mit den spezifischen Protokollen und Schnittstellen der Switche kompatibel sind. Empfehlenswert ist die Auswahl von Netzwerkanalysetools, die in der Lage sind, industrielle Protokolle zu verstehen und zu analysieren, um eine effiziente Überwachung durchzuführen.

3. **Konnektivität mit den Netzwerkswitchen**

   Die Verbindung von Netzwerkanalysetools mit industriellen Netzwerkswitchen kann herausfordernd sein. In einigen Fällen sind industrielle Netzwerkswitche nicht "managebar", das bedeutet, dass sie möglicherweise keine standardmäßige Schnittstelle oder Funktionen für das Monitoring bieten. In solchen Szenarien könnte es notwendig sein, spezielle Lösungen oder zusätzliche Hardware einzusetzen, um den Netzwerkverkehr zu überwachen.

4. **Anomalieüberwachung**

   Nachdem die Netzwerkanalysetools mit den entsprechenden Netzwerkswitchen verbunden sind, kann der Netzwerkverkehr überwacht und auf Anomalien untersucht werden. Das Netzwerkanalysetool erfasst den Datenverkehr und analysiert ihn, um potenzielle Schwachstellen oder verdächtige Aktivitäten auszumachen. Dies kann auf untypische Datenströme, unbefugten Zugriff oder andere Sicherheitsbedrohungen hinweisen.

Es ist wichtig zu betonen, dass industrielle Netzwerkswitche eventuell nicht über dieselben Überwachungsfunktionen verfügen wie herkömmliche Netzwerkgeräte. Daher könnte es notwendig sein, alternative Methoden oder spezialisierte Tools zu nutzen, um eine umfassende Überwachung und Bewertung der Sicherheit in industriellen Umgebungen sicherzustellen.

7.1.5 OT-Penetrationstests

Ein OT-Penetrationstest ist ein spezieller Sicherheitstest, der darauf abzielt, Schwachstellen und Sicherheitslücken in OT-Netzwerken und OT-Systemen aufzudecken.

Bei Tests an Produktivsystemen sind mögliche Konsequenzen vorher zu prüfen. Auch im Stillstand befindliche Anlagen können immer noch gewisse Risiken aufweisen (z. B. Tanklager), welche eine funktionierende Automatisierung notwendig machen. Es besteht ein erhebliches Risiko, dass Angriffsversuche oder Schwachstellenscans zu unbemerkten Änderungen führen können, welche sich als neue Vulnerabilitäten manifestieren können. Aus diesen Gründen sollten OT-Penetrationstests nur mit Bedacht ggf. unter Nutzung von Labor-Ausrüstung oder im Rahmen von FAT ausgeführt werden.

Die Schritte eines solchen Tests könnten wie folgt aussehen:

1. **Zieldefinition**

   Festlegung des Umfangs und der Ziele des Penetrationstests. Identifizierung der zu überprüfenden OT-Netzwerke und -Systeme sowie der spezifischen Komponenten oder Protokolle, die untersucht werden sollen.

2. **Planung und Vorbereitung**

   Erstellung eines detaillierten Testplans, der die verwendeten Werkzeuge, Techniken und Methoden beschreibt. Sicherstellen, dass der Penetrationstester über die notwendigen Genehmigungen und Berechtigungen verfügt, um den Test durchzuführen. Dokumentation des Umfangs des Tests, um die möglichen Auswirkungen auf den Produktionsbetrieb zu minimieren.

3. **Scannen**

Durch Scannen werden aktive Netzwerkressourcen, offene Ports, verwendete Protokolle und andere relevante Informationen gesammelt, um die Sicherheit eines Systems oder Netzwerks zu bewerten. Hierbei werden verschiedene Tools und Techniken eingesetzt, um diese Informationen zu sammeln.

4. **Auswertung der Ergebnisse**

   Analyse der Scan-Ergebnisse, um offene Ports, verwendete Protokolle und potenzielle Schwachstellen zu identifizieren. Bewertung der Ergebnisse, um mögliche Sicherheitslücken oder Angriffspunkte zu erkennen.

5. **Prüfen der Schwachstellen**

   Basierend auf den identifizierten Schwachstellen können weitere Tests durchgeführt werden, um die Auswirkungen auf die OT-Systeme zu überprüfen. Beispiele für Tests könnten das Überprüfen von Standardpasswörtern, das Ausnutzen von Protokoll-Schwachstellen oder das Durchführen von Denial-of-Service-Angriffen sein. Fachliche Kenntnisse und Erfahrung sind hierbei wichtig, um den Produktionsbetrieb nicht zu beeinträchtigen.

6. **Dokumentation und Berichterstattung**

   Alle Schritte, Ergebnisse und verwendeten Werkzeuge werden in einem Bericht festgehalten. Identifizierte Schwachstellen, ihre Auswirkungen und mögliche Lösungsansätze werden beschrieben. Empfehlungen zur Behebung der Schwachstellen und zur Verbesserung der Sicherheit in OT-Netzwerken und -Systemen werden abgeleitet.

Beispiele für Tests in OT-Netzwerken und -Systemen könnten die Überprüfung von Schwachstellen in SCADA-Systemen, die Bewertung der Sicherheit von industriellen Protokollen, die Analyse von Firewall-Regeln und Zugriffskontrollen, Tests der Sicherheit von Remote-Zugriffslösungen sowie die Überprüfung der physischen Sicherheit von Anlagen sein.

7.2 Prüfung der OT-Komponenten

Die Prüfung von OT-Komponenten durch den Hersteller ist ein wesentlicher Schritt, um sicherzustellen, dass die Komponenten den erforderlichen Sicherheitsstandards genügen. Hier ist eine schrittweise Vorgehensweise für die Prüfung von OT-Komponenten wie einer SPS (Speicherprogrammierbare Steuerung) oder einem Leitsystem, die von Herstellern von OT-Systemen und Komponenten durchgeführt werden kann:

1. **Festlegung von Normen und Standards**

   Als Basis für die Prüfung können Standards wie IEC 62443-4-2 und Common Criteria (allgemeine Kriterien für die Sicherheit von IT-Produkten) verwendet werden. Diese Normen definieren Sicherheitsanforderungen für OT-Systeme und bieten Leitlinien für Sicherheitstests.

2. **Anforderungsanalyse**

   Die Anforderungen der genannten Normen werden analysiert, und die relevanten Sicherheitsaspekte für die zu testende Komponente werden identifiziert. Dies kann Authentifizierung, Zugriffskontrolle, Kommunikationssicherheit und andere sicherheitsrelevante Aspekte umfassen.

3. **Erstellung eines Testplans**

   Basierend auf den ermittelten Anforderungen wird ein detaillierter Testplan entwickelt. Dieser Plan sollte die spezifischen Tests, Methoden und Tools beschreiben, die zur Überprüfung der Sicherheit der OT-Komponente eingesetzt werden sollen.

4. **Durchführung von Funktionstests**

Funktionalitätstests werden durchgeführt, um sicherzustellen, dass die OT-Komponente ordnungsgemäß funktioniert. Hierbei wird überprüft, ob die Funktionen korrekt implementiert sind und keine unerwarteten Verhaltensweisen auftreten.

5. **Durchführung von Sicherheitstests**

   Sicherheitstests werden ausgeführt, um potenzielle Schwachstellen und Sicherheitslücken aufzudecken. Dies kann Authentifizierungs- und Zugriffskontrollmechanismen, Kommunikationssicherheitsprotokolle, Penetrationstests und die Reaktion auf Sicherheitsvorfälle einschließen.

6. **Bewertung der Ergebnisse**

   Die Ergebnisse der Tests werden analysiert und bewertet, um festzustellen, ob die Sicherheit der OT-Komponente im Einklang mit den definierten Anforderungen steht. Identifizierte Schwachstellen, Sicherheitslücken oder potenzielle Verbesserungsbereiche werden ermittelt.

7. **Dokumentation und Berichterstattung**

   Alle Schritte, Ergebnisse und verwendeten Werkzeuge werden sorgfältig in einem Bericht festgehalten. Dies umfasst eine Beschreibung der durchgeführten Tests, der identifizierten Schwachstellen sowie möglicher Lösungsansätze. Die ergriffenen Sicherheitsmaßnahmen und die Konformität der OT-Komponente mit den Normen werden ebenfalls dokumentiert.

Durch die Durchführung einer solchen Prüfung können Hersteller sicherstellen, dass ihre OT-Komponenten den erforderlichen Sicherheitsstandards entsprechen und somit die Sicherheit von OT-Netzwerken und -Systemen gewährleistet ist.

7.3 Prüfung der SPS-Programmierung

Die Überprüfung der SPS-Programmierung auf Fehler, die bei Cyberangriffen ausgenutzt werden können, ist ein wesentlicher Schritt, um die Sicherheit von industriellen Steuerungssystemen zu gewährleisten. Hier ist eine Vorgehensweise zur Durchführung dieser Überprüfung:

- Es wird darauf hingewiesen, dass sicherzustellen ist, dass bewährte Standards und Good Practices bei der SPS-Programmierung befolgt werden sollten. Dies beinhaltet die Anwendung sicherer Codierungsmethoden, die Implementierung von Zugriffssteuerungsmechanismen, die Vermeidung unsicherer Kommunikationsprotokolle sowie die Durchsicht der Programmierlogik auf mögliche Schwachstellen.
- Es wird vorgeschlagen, einen umfassenden Code-Review des SPS-Programms durchzuführen, um potenzielle Fehler zu erkennen, die von Cyberangreifern ausgenutzt werden könnten. Hierbei könnten Aspekte wie Variablenmanipulationen, fehlerhafte Berechtigungsprüfungen, unzureichende Fehlerbehandlungen, unsichere Kommunikation und andere verbreitete Sicherheitslücken überprüft werden.

8 Abkürzungsverzeichnis

Abkürzung	*Langtitel*
API	Application Programming Interfaces
BAD	Behavioral Anomaly Detection
BAuA	Bundesanstalt für Arbeitsschutz und Arbeitsmedizin
BetrSichV	Betriebssicherheitsverordnung
BYOD	Bring Your Own Device
COTS	Commercial of the Shelf
CSF	Cyber Security Framework
DDE	Dynamic Data Exchange
DIN	Deutsche Institut für Normung
DKE	Verband der Elektrotechnik, Elektronik und Informationstechnik
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed-DoS
EoS	End of Support
EoL	End of Life
ERP	Enterprise Resource Planning
ES	Engineering Station
EWS	Engineering Workstation
FAT	Factory Acceptance Testing
GAMP	Good Automation Practice
GMP	Good Manufacturing Practice
HART	Highway Addressable Remote Transducer Protocol
HMI	Human Machine Interface
IACS	Industrial automation and control systems
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISA	International Society of Automation
ISMS	Information security management system
ISO	International Organization for Standardization
MES	Manufacturing Execution System
MitM	Man-in-the-Middle
MSB	Manufacturing Service Bus
MSR	Mess-, Steuer- und Regeleinrichtungen
MTO	Maximum Tolerable Outage
MTU	Master Terminal Unit
NIST	National Institute of Standards and Technology

Abkürzung	*Langtitel*
NOA	Namur Open Architecture
NTP	Network Time Protocol
OLE	Open Linking and Embedding
OPC	Open Platform Communications
OPC UA	OPC Unified Architecture
OT	Operational Technology
PAT	Process Analytical Technology
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controller (dt. Speicherprogrammierbare Steuerung)
PLS	Prozessleitsystem
PNK	Prozessnahe Komponente
ProdSG	Produktsicherheitsgesetz
ProdSV	Produktsicherheitsverordnungen
PSIRT	Product Security Incident Response Team
RAMI	Reference Architecture Model Industrie
RaaS	Ransomware-as-a-Service
RBAC	Role Based Access Control
REST-API	Representational State Transfer - Application-Program-Interface
RFID	Radio Frequency Identification
RTO	Recovery Time Objective
RTU	Remote Terminal Unit
SAT	Site Acceptance Testing
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information Event Management
SIF	Satefy Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SIT	Site Integration Testing
SPS	Speicherprogrammierbare Steuerung

9 Literaturverzeichnis

1. **Internationale Elektrotechnische Kommission (IEC).** *IEC 60050: International Electrotechnical Vocabulary.*

2. **Bundesamt für Sicherheit in der Informationstechnik.** IT-Grundschutz-Kompendium (Edition 2023). [Online] 2023. [Zitat vom: 22. 11 2023.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html.

3. —. IT-Grundschutz-Bausteine - IND.1 Prozessleit- und Automatisierungstechnik. [Online] 2023. [Zitat vom: 23. 11 2023.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html.

4. —. Technische Richtlinie TR-03183-2: Cyber-Resilienz-Anforderungen an Hersteller und Produkte: Software Bill of Materials (SBOM). [Online] 2023. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03183/BSI-TR-03183-2.pdf.

5. **(IEC), International Elektrotechical Commission.** *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.* 2011.

6. **Institute for Interdisciplinary Engineering Studies Purdue University West Lafayette.** Purdue Enterprise Reference Architecture (PERA): A Handbook on Master planning and implementation for enterprise integration programs. [Online] Februar 2001. [Zitat vom: 10. Oktober 2023.] http://www.pera.net/Pera/Report160%281996%29Handbook/PERA_Handbook.pdf.

7. **Bundesministerium für Wirtschaft und Klimaschutz.** Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0). [Online] April 2016. [Zitat vom: 10. Oktober 2023.] http://www.pera.net/Pera/Report160%281996%29Handbook/PERA_Handbook.pdf.

8. **International Society of Automation (ISA).** ISA95: Enterprise-Control System Integration. [Online] [Zitat vom: 10. Oktober 2023.] https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95.

9. **(IEC), International Elektrotechnical Commission.** *IEC/EN 61511-1 Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming Requirements - Abs. 9.5.1.* 2019.

10. **VGB PowerTech e.V.** *VGB-S-175-00-2ß14-DE Richtlinie: IT-Sicherheit für Erzeugungsanlagen.* Essen : VGB PowerTech e.V, 2014.

11. **Bundesamt für Sicherheit in der Informationstechnik.** *IT-Grundschutz-Kataloge.* 2023, Bonn : s.n.

12. **Internationale Elektrotechnische Kommission (IEC).** *IEC 61158: Industrial communication networks - Fieldbus specifications.* 2023.

13. **VDE Verband der Elektrotechnik Elektrik Informationstechnik e.V.** *VDE-Positionspapier Funktechnologien für Industrie 4.0.* Juni 2017.

14. **Internationale Elektrotechnische Kommission (IEC).** *DIN EN 62381: Automatisierungssysteme in der Prozessindustrie - Werksabnahme (FAT), Abnahme der installierten Anlage (SAT) und Integrationstest (SIT).*

15. **Verband Deutscher Maschinen- und Anlagenbau e.V.** VDMA Einhaltsblatt Standard für die Beauftragung und Abnahme formgebender Werkzeuge. [Online] August 2023. [Zitat vom: 10. Oktober 2023.] https://www.vdma.org/documents/34570/4887800/Entwurf+VDMA+34195_2023-08+%28de%29.pdf/8243fbf1-d44a-ad89-bc02-131947f9b5f3?t=1686317703064 .

16. **Bundesamt für Sicherheit in der Informationstechnik.** IT-Grundschutz: Elementare Gefährdungen. [Online] 2020. [Zitat vom: 22. 11 2023.] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html.

17. **Waibel, Stefan.** Wie man sich vor Denial-of-Service-Angriffen schützt. iX Nr.5. Hannover : Heise Zeitschriften Verlag GmbH & Co. KG, 2013, S. 64-67.

18. **OWASP.** Top Ten Project. [Online] 2021, Open Web Application Security Project. [Zitat vom: 14. April 2023.] https://owasp.org/Top10/.

19. **MANDIANT.** FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor. [Online] Dezember 2020. [Zitat vom: 17. August 2023.] https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.

20. **M.Kittelmann, T. Mössner.** Die neue Europäische Maschinenverordnung. *Arbeitsschutz in Recht und Praxis.* 2023, Bd. 4, 11.

21. **Bundesamt für Sicherheit in der Informationstechnik.** Leitfaden zur Basis-Absicherung nach IT-Grundschutz. [Online] 2017. [Zitat vom: 12. 12 2023.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf.

22. **VDMA - Competence Center Industrial Security.** Industrial Security: Mindestempfehlungen. [Online] 01 2022. [Zitat vom: 26. 03 2024.] https://www.vdma.org/documents/34570/12205854/VDMA_Mindestempfehlungen_Security_Supply_Chain.pdf/585ae9fc-0ab9-a8e5-1ee8-79dac978f286?filename=VDMA_Mindestempfehlungen_Security_Supply_Chain.pdf.

23. **Bundesamt für Sicherheit in der Informationstechnik.** *Technische Richtlinie 02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* Bonn : s.n., 2023.