OT-Security-Kompetenzen – Rollenprofile, Kompetenzniveaus und Entwicklung

Auswertung und Weiterentwicklung der Ergebnisse aus den I2M-Workshops 2026

NETZWERK SMART INDUSTRIES · FORSCHUNG & TRANSFER

Herausgeber	Netzwerk Smart Industries · Technische Hochschule Mannheim · Digital Hub Rhein-Neckar
Autor:innen	Dr. Sachar Paulus (TH Mannheim), Jonathan Marin Franco (Daimler Truck) et. al.
Informationsgrundlage	I2M-Workshops am 03. Juli 2026 und am 25. September 2026
Version / Datum	Arbeitsfassung 1.0 · 03. November 2026

Präambel

Dieses Werk steht unter der Creative-Commons-Lizenz Namensnennung 4.0 International[1] (“CC BY 4.0”). Sie dürfen das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten sowie Teile verwenden, verändern und darauf aufbauen – auch kommerziell –, sofern Sie angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und kenntlich machen, ob Änderungen vorgenommen wurden.

Autoren

Die folgenden Personen haben an der Erstellung dieser Studie mitgewirkt:

- Dr. Sachar Paulus (Technische Hochschule Mannheim, Editor)
- Jonathan Marin Franco (Daimler Truck, Moderator)
- Sandra Link (Stadt Mannheim)
- Sandra Steinert-Ramirez (Stadt Mannheim)
- Erwin Kruschitz (Anapur)
- Richard Biala (ABB)
- Robin Jaus
- Christopher Jeuthe (Heidelberg Materials)
- Rudolf Preuss (Actemium)
- Jochen Sessig (John Deere)
- Maximilian Bardon (Daimler Truck)
- Nicholas Jones (Pepperl & Fuchs)

Zitierempfehlung

Netzwerk Smart Industries / Technische Hochschule Mannheim / Digital Hub Rhein-Neckar (Hrsg.) (2026): OT-Security-Kompetenzen – Rollenprofile, Kompetenzniveaus und Entwicklung. Studienergebnisse.

Hinweis zur Verwendung

Die in diesem Bericht enthaltenen Kompetenzprofile und Entwicklungsmaßnahmen sind als praxisorientiertes Orientierungs- und Entwicklungsmodell zu verstehen. Sie ersetzen weder eine organisationsspezifische Risikoanalyse noch eine formale Zertifizierungs- oder Eignungsprüfung.

Kontakt

Anfragen zur Studie stellen Sie bitte an Sandra Link, Sandra.Link@mannheim.de.

[1] Lizenztext: https://creativecommons.org/licenses/by/4.0/deed.de

Kurzfassung / Executive Summary

Dieser Forschungsbericht überführt die Ergebnisse zweier I2M-Workshops vom 03. Juli und 25. September 2026 in ein praxisorientiertes Rollen- und Kompetenzmodell für OT-Security-Tätigkeiten. Betrachtet werden zwölf Rollen entlang der vier Kompetenzfelder OT & Technik, Security, Prozesse & Organisation sowie Kommunikation & Übersetzung. Für jede Rolle werden Soll-Kompetenzen, ein Ist-/Soll-Abgleich, eine typische Aufgabenbeschreibung und Vorschläge zur Personalentwicklung beschrieben.

Die Ergebnisse verdeutlichen, dass OT-Security-Kompetenz nicht allein aus klassischer IT-Security-Expertise besteht. Erforderlich ist vielmehr die Verbindung von Anlagen- und Prozessverständnis, technischer Sicherheitskompetenz, organisatorischer Einbettung und adressatengerechter Kommunikation. Besonders ausgeprägte Entwicklungsbedarfe zeigen sich unter anderem in der Produktions-IT im Aufbau von OT-Grundverständnis sowie bei Anlagenbetreibern, insbesondere bei OT-Security-Koordinatoren und -Engineers in der Vertiefung sicherheitsbezogener Fähigkeiten.

Das Modell ist als Grundlage für Personalentwicklung und Organisationsgestaltung gedacht. Die Einstufungen sind ordinale, workshopbasierte Einschätzungen; es erfolgt keine quantitative Kompetenzmessung. Die vorgeschlagenen Entwicklungsmaßnahmen sind in der Folge von Experten identifizierte, fachlich abgeleitete Empfehlungen.

Schlagwörter

Operational Technology · OT-Security · Kompetenzmodell · Rollenprofile · Personalentwicklung · industrielle Automatisierung

Inhaltsverzeichnis

Präambel 2
Autoren 2
Zitierempfehlung 2
Hinweis zur Verwendung 2
Kontakt 2
Kurzfassung / Executive Summary 3
Schlagwörter 3
Inhaltsverzeichnis 4
1. Einleitung 6
2. Stand der Forschung und fachliche Grundlagen 8
2.1. Normen, Leitlinien und regulatorische Anforderungen für die OT-Security 8
2.2. Forschung zu Kompetenzen und Qualifikationsanforderungen in der OT-Security 11
2.3. Einordnung und Beitrag des vorliegenden Kompetenzmodells 11
3. Methodik und Vorgehensweise der Kompetenzanalyse 13
3.1. Untersuchungsansatz und Datengrundlage 13
3.2. Rollenbezogene Analyse und Ist-/Soll-Abgleich 13
3.3. Operationalisierung der Kompetenzniveaus 15
3.4. Ableitung von Entwicklungsmaßnahmen 16
3.5. Methodische Einordnung und Grenzen der Aussagekraft 17
4. Ergebnisse des Kompetenzmappings und Rollenprofile 18
4.1. Rollen-Kompetenzprofile 18
4.1.1. Rollenprofil: Instandhaltung 18
4.1.2. Rollenprofil: Engineering 20
4.1.3. Rollenprofil: Automatisierung / Digitalisierung 21
4.1.4. Rollenprofil: Anlagenbetreiber 23
4.1.5. Rollenprofil: Produktions-IT 25
4.1.6. Rollenprofil: Qualitätsmanagement 27
4.1.7. Rollenprofil: Safety, Health & Environment (SHE) 28
4.1.8. Rollenprofil: CISO 30
4.1.9. Rollenprofil: Head OT Security 32
4.1.10. Rollenprofil: BISO (Business Information Security Officer) 34
4.1.11. Rollenprofil: OT Security Expert / Architect 35
4.1.12. Rollenprofil: OT Security Coordinator / Engineer 37

4.2. Ist-/Soll-Mapping der Rollen ... 39
4.3. Entwicklungsempfehlungen ... 40
4.3.1. Großes Kompetenzdelta: zwei Niveaustufen ... 40
4.3.2. Mittleres Kompetenzdelta: eine Niveaustufe ... 41
4.3.3. Kein Kompetenzdelta ... 42
4.4. Detaillierte Entwicklungsempfehlungen ... 42
4.4.1. Rollenprofil Instandhaltung ... 43
4.4.2. Rollenprofil Engineering ... 44
4.4.3. Rollenprofil Automatisierung / Digitalisierung ... 45
4.4.4. Rollenprofil Anlagenbetreiber ... 46
4.4.5. Rollenprofil Produktions-IT ... 47
4.4.6. Rollenprofil Qualitätsmanagement ... 48
4.4.7. Rollenprofil SHE ... 49
4.4.8. Rollenprofil CISO ... 50
4.4.9. Rollenprofil Head OT-Security ... 51
4.4.10. Rollenprofil BISO ... 52
4.4.11. Rollenprofil OT-Security Expert / Architect ... 53
4.4.12. Rollenprofil OT-Security Coordinator / Engineer ... 54
5. Diskussion, Handlungsempfehlungen und Grenzen ... 56
5.1. Empfehlungen ... 56
5.1.1. Zwei komplementäre Entwicklungspfade etablieren ... 56
5.1.2. Rollenbezogene Lernpfade statt Einheitscurriculum ... 56
5.1.3. Lernen am realen Betrieb ausrichten ... 56
5.1.4. Kompetenznachweise definieren ... 56
5.1.5. Verantwortung und Zeitbudget sichern ... 57
5.1.6. Matrix regelmäßig aktualisieren ... 57
5.2. Grenzen, Annahmen und Übertragbarkeit ... 57
5.3. Weitere Schritte ... 57
6. Literaturverzeichnis ... 59

1. Einleitung

Operational Technology (OT) umfasst Systeme und Komponenten, die physische Prozesse überwachen oder steuern. Ihre Absicherung unterscheidet sich in wesentlichen Punkten von klassischer IT-Sicherheit: Verfügbarkeit, Echtzeitverhalten, Safety, lange Lebenszyklen, Legacy-Komponenten und eingeschränkte Wartungsfenster beeinflussen die Auswahl und Umsetzung von Schutzmaßnahmen. Diese Besonderheiten werden unter anderem in der NIST-Leitlinie SP 800-82 beschrieben [1].

Vor diesem Hintergrund benötigt OT-Security ein organisationsübergreifendes Kompetenzverständnis. Rollen in Produktion, Instandhaltung, Engineering, IT, Management und Security müssen jeweils unterschiedliche Beiträge leisten und zugleich an Schnittstellen zusammenarbeiten. Die erforderlichen Kompetenzen gehen dabei über rein technische Sicherheitskenntnisse hinaus. Neben dem Verständnis von OT-Systemen und Security-Verfahren sind insbesondere Kenntnisse betrieblicher Prozesse, organisatorischer Verantwortlichkeiten sowie die Fähigkeit zur Kommunikation und Übersetzung zwischen unterschiedlichen Fachbereichen erforderlich.

Aus dieser Ausgangslage ergibt sich die zentrale Forschungsfrage dieses Berichts:

Welche Kompetenzen benötigen die unterschiedlichen Rollen in einer Organisation, um OT-Security wirksam und nachhaltig umzusetzen, wie lassen sich die erforderlichen Kompetenzniveaus beschreiben, wie ist der aktuelle Stand der Kompetenzen und welche Entwicklungsmaßnahmen können aus bestehenden Kompetenzlücken abgeleitet werden?

Die Forschungsfrage wird durch drei miteinander verbundene Betrachtungsschwerpunkte konkretisiert: Erstens ist zu bestimmen, welche Kompetenzfelder für die verschiedenen Rollen relevant sind und wie sich deren jeweilige Anforderungen unterscheiden. Zweitens ist zu beschreiben, welche Kompetenzniveaus für eine wirksame Wahrnehmung der jeweiligen Rolle erforderlich sind und wie diese den im Workshop ermittelten Ist-Ständen gegenübergestellt werden können. Drittens ist zu untersuchen, welche Qualifizierungs- und Personalentwicklungsmaßnahmen geeignet erscheinen, um identifizierte Kompetenzlücken zu schließen.

Zur Beantwortung dieser Frage werden die Ergebnisse zweier I2M-Workshops vom 3. Juli 2026 und 25. September 2026 ausgewertet und systematisch zusammengeführt. I2M ist eine von der Stadt Mannheim moderierte Gruppe von OT-Security-Experten in Industrieunternehmen der Region Rhein-Neckar; an den Workshops haben zudem Gäste aus der Cybersecurity Community Rhein-Neckar teilgenommen, welche Security-Dienstleister der Region zusammenbringt.

Die Untersuchungsmethodik besteht aus einer strukturierten, workshopbasierten Anforderungsanalyse mit anschließender konzeptioneller Auswertung. Im ersten Workshop wurden die fachlichen Inhalte in vier Kompetenzfelder gegliedert: OT & Technik, Security, Prozesse & Organisation sowie Kommunikation & Übersetzung. Im zweiten Workshop erfolgte ein rollenbezogenes Ist-/Soll-Mapping, in dem die vorhandenen und angestrebten Kompetenzniveaus gegenübergestellt wurden. Die Kompetenzniveaus werden anhand einer vierstufigen, an der Bloom'schen Lernzieltaxonomie orientierten Skala beschrieben. Im Rahmen der anschließenden Auswertung wurden die Workshop-Ergebnisse zu Rollenprofilen verdichtet, Kompetenzdifferenzen identifiziert und daraus Vorschläge für Personalentwicklungs- und Qualifizierungsmaßnahmen abgeleitet. Die Entwicklungsmaßnahmen und Priorisierungen sind somit analytische Ableitungen aus den Workshop-Ergebnissen.

Ziel ist es, die Workshop-Ergebnisse so aufzubereiten, dass Unternehmen daraus Rollenprofile, Qualifizierungsbedarfe und konkrete Entwicklungsmaßnahmen ableiten können. Der Bericht dokumentiert keine repräsentative empirische Studie und beansprucht keine statistische Generalisierbarkeit. Insbesondere stellt das entwickelte Kompetenzmodell kein standardisiertes oder zertifiziertes Verfahren zur individuellen Kompetenzmessung dar. Die Einstufung einzelner Personen muss vielmehr anhand konkreter Arbeitsproben, Interviews, Projektbeiträge und Beobachtungen in der jeweiligen Organisation validiert werden. Der Bericht ist daher als wissenschaftlich fundierter Praxisbericht zu verstehen, dessen empirische Grundlage die genannten I2M-Workshops bilden. Gleichwohl ist der Anspruch, einen Strukturierungsansatz zu vermitteln und erste Impulse für eine Weiterentwicklung der OT-Security-Kompetenzlandschaft zu setzen.

Der Bericht ist wie folgt aufgebaut: Kapitel 2 erläutert den fachlichen Bezugsrahmen und den Forschungsstand. Kapitel 3 beschreibt Untersuchungsansatz, Datengrundlage und Auswertungsmethodik. Kapitel 4 stellt die Ergebnisse des Kompetenzmappings vor: die zwölf Rollenprofile, den Ist-/Soll-Abgleich sowie die daraus abgeleiteten Entwicklungsempfehlungen. Kapitel 5 priorisiert die wesentlichen Entwicklungsbedarfe. Kapitel 6 führt die Diskussion und übergreifenden Handlungsempfehlungen mit der methodischen Einordnung, den Grenzen und einem Ausblick zusammen. Kapitel 7 enthält das Literaturverzeichnis.

2. Stand der Forschung und fachliche Grundlagen

Die Entwicklung eines organisationsübergreifenden Kompetenzmodells für OT-Security bewegt sich im Spannungsfeld zwischen technischen Sicherheitsanforderungen, betrieblichen Prozessen und den Kompetenzen der beteiligten Akteure. Während sich die fachlichen und normativen Grundlagen zur Absicherung industrieller Automatisierungs- und Steuerungssysteme in den vergangenen Jahren deutlich weiterentwickelt haben, ist die systematische Beschreibung der dafür erforderlichen rollenbezogenen Kompetenzen weniger weit fortgeschritten. Für die Einordnung des vorliegenden Modells werden deshalb sowohl etablierte Normen und Leitlinien als auch einschlägige Forschung zur Kompetenzentwicklung und zur menschlichen Dimension industrieller Cybersicherheit herangezogen.

2.1. Normen, Leitlinien und regulatorische Anforderungen für die OT-Security

Einen zentralen fachlichen Referenzpunkt bildet die Leitlinie NIST SP 800-82 Rev. 3 – Guide to Operational Technology (OT) Security. Sie beschreibt die besonderen Anforderungen an die Absicherung von Operational Technology und berücksichtigt dabei insbesondere die spezifischen Anforderungen an Verfügbarkeit, Zuverlässigkeit, Performance und Safety. Neben einer Beschreibung typischer OT-Systemarchitekturen behandelt die Leitlinie Bedrohungen, Schwachstellen, Risikomanagement und geeignete Sicherheitsmaßnahmen. Sie verdeutlicht damit, dass OT-Security nicht als isolierte technische Aufgabe verstanden werden kann, sondern die Abstimmung zwischen technischen Schutzmaßnahmen, betrieblichen Anforderungen und organisatorischen Verantwortlichkeiten voraussetzt [1].

Zum Zeitpunkt der Erstellung dieses Berichts liegt bereits ein Entwurf für die vierte Revision der NIST SP 800-82 vor. Der am 21. September 2026 veröffentlichte Initial Public Draft erweitert unter anderem die Betrachtung auf weitere OT-Anwendungsbereiche wie Wasser- und Abwassersysteme, maritime Systeme und industrielle IoT-Umgebungen. Zudem wird die Struktur stärker am NIST Cybersecurity Framework 2.0 ausgerichtet. Da es sich noch um einen Entwurf handelt, wird für die fachliche Referenzierung in diesem Bericht weiterhin die verabschiedete Revision 3 verwendet. Die Entwicklungen der Revision 4 sind gleichwohl ein Hinweis auf die zunehmende Bedeutung einer integrierten Betrachtung von OT, IT, Cloud-Umgebungen und übergreifendem Risikomanagement [1a].

Eine besondere Bedeutung für die industrielle Automatisierung besitzt die Normenreihe IEC 62443 – Security for Industrial Automation and Control Systems. Sie stellt einen umfassenden normativen Rahmen für die Cybersicherheit industrieller Automatisierungs- und Steuerungssysteme bereit und betrachtet dabei ausdrücklich unterschiedliche Akteursgruppen entlang des gesamten Lebenszyklus. Dazu gehören insbesondere Anlagenbetreiber (Asset Owner), Integratoren, Hersteller von Automatisierungskomponenten sowie Dienstleister und Service Provider. Die Normenreihe adressiert damit nicht nur technische Anforderungen an Systeme und Komponenten, sondern auch Anforderungen an Sicherheitsmanagement, Entwicklungsprozesse, Integration und Betrieb [2].

Die einzelnen Teile der IEC-62443-Reihe setzen dabei unterschiedliche Schwerpunkte. IEC 62443-2-1 behandelt Anforderungen an das Security-Programm von Anlagenbetreibern, während IEC 62443-2-4 Anforderungen an Dienstleister formuliert. IEC 62443-3-2 beschreibt die Sicherheitsrisikobeurteilung und die Ableitung von Sicherheitsanforderungen für industrielle Systeme. IEC 62443-3-3 konkretisiert technische Anforderungen an die Systemsicherheit und definiert Security Levels. Die Teile IEC 62443-4-1 und IEC 62443-4-2 adressieren schließlich sichere Produktentwicklungsprozesse und technische Sicherheitsanforderungen an Komponenten. In ihrer Gesamtheit macht die Normenreihe deutlich, dass OT-Security eine gemeinsame Verantwortung verschiedener Akteure ist und nur durch das Zusammenwirken von Menschen, Prozessen und Technologie wirksam umgesetzt werden kann.

Für die Entwicklung von Rollenprofilen ist insbesondere das zugrunde liegende Prinzip der geteilten Verantwortung relevant. Die Anforderungen an einen Anlagenbetreiber unterscheiden sich beispielsweise von denen eines Systemintegrators oder eines Komponentenherstellers. Gleichzeitig müssen die beteiligten Akteure an den jeweiligen Schnittstellen zusammenarbeiten. Daraus ergibt sich unmittelbar die Notwendigkeit, Verantwortlichkeiten, Aufgaben und Kompetenzanforderungen rollenbezogen zu beschreiben.

Eine weitere wichtige Grundlage bildet ISO/IEC 27001:2022. Die Norm definiert Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) und bietet damit einen organisationsweiten Rahmen für die systematische Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken. Sie ist nicht spezifisch auf OT ausgerichtet, lässt sich jedoch auf die Informationssicherheitsorganisation eines Unternehmens einschließlich der Schnittstellen zur Produktion und zu industriellen Steuerungssystemen anwenden [3].

Ergänzend konkretisiert ISO/IEC 27002:2022 Maßnahmen und Umsetzungshinweise für die Informationssicherheit. Für OT-Umgebungen ist dabei insbesondere die organisatorische Einbettung von Sicherheitsmaßnahmen relevant: Verantwortlichkeiten, Kompetenzaufbau, Sensibilisierung, Zugriffssteuerung, Lieferantenbeziehungen und der Umgang mit Sicherheitsvorfällen müssen sowohl in der IT als auch in den produktionsnahen Bereichen berücksichtigt werden.

Das NIST Cybersecurity Framework 2.0 (CSF 2.0) bietet einen weiteren übergreifenden Orientierungsrahmen für das Management von Cybersecurity-Risiken. Es strukturiert die erforderlichen Aktivitäten in sechs Funktionen: Govern, Identify, Protect, Detect, Respond und Recover. Besonders hervorzuheben ist die mit Version 2.0 neu eingeführte Funktion Govern, die die Steuerung von Cybersecurity-Risiken, die Festlegung von Verantwortlichkeiten, Richtlinien und strategischen Vorgaben stärker in den Mittelpunkt rückt. Damit wird die Bedeutung von Management, Governance und organisationsübergreifender Zusammenarbeit ausdrücklich betont [4].

Für die Kompetenzentwicklung ist diese Perspektive besonders relevant: Die Funktionen des CSF 2.0 lassen sich nicht ausschließlich einer zentralen IT- oder Security-Abteilung zuordnen. Vielmehr erfordern sie Beiträge unterschiedlicher Organisationseinheiten, beispielsweise bei der Identifikation von Anlagen und Risiken, der Umsetzung von Schutzmaßnahmen, der Erkennung von Sicherheitsereignissen oder der Wiederherstellung des Betriebs. Die erforderlichen Kompetenzen verteilen sich somit auf verschiedene Rollen und Verantwortungsbereiche.

Für den deutschsprachigen Anwendungskontext ist darüber hinaus das ICS-Security-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) relevant. Die 2024 veröffentlichte Version 2.0 bietet eine praxisorientierte Grundlage zur Informationssicherheit industrieller Steuerungs- und Automatisierungssysteme. Sie unterstützt insbesondere die gemeinsame fachliche Einordnung durch IT-Sicherheitsexperten und Fachleute aus Automatisierung und Betrieb [5].

Über die genannten technischen Normen und Leitlinien hinaus prägen rechtliche Anforderungen den organisatorischen Rahmen der OT-Security. Ihre Anwendbarkeit hängt von Branche, Größe, Tätigkeit, Anlagenart und konkreter Betreiberrolle ab. Die folgenden Regelwerke werden deshalb nicht als pauschal für jedes Unternehmen geltende Pflichten verstanden, sondern als relevante Bezugspunkte, deren Anwendbarkeit im Einzelfall zu prüfen ist.

Mit dem NIS-2-Umsetzungsgesetz ist die europäische NIS-2-Richtlinie in Deutschland seit dem 6. Dezember 2025 insbesondere durch das novellierte BSI-Gesetz umgesetzt. Betroffene besonders wichtige und wichtige Einrichtungen müssen angemessene technische, operative und organisatorische Risikomanagementmaßnahmen umsetzen; dazu gehören unter anderem Risikoanalyse, Umgang mit Sicherheitsvorfällen, Business Continuity, Lieferkettensicherheit, Zugriffskontrolle und Wirksamkeitsprüfung. Hinzu kommen Registrierungs- und Meldepflichten. Für OT-Security ist entscheidend, dass Produktions- und Steuerungssysteme in die organisationsweite Risikobetrachtung einbezogen werden und Verantwortlichkeiten, Eskalations- und Meldewege auch für OT-Vorfälle funktionieren. Die konkrete Betroffenheit ist anhand der gesetzlichen Kriterien zu bestimmen [12].

Arbeitsschutzrechtliche Anforderungen bilden eine eigenständige, mit OT-Security eng verbundene Perspektive. Das Arbeitsschutzgesetz verpflichtet Arbeitgeber zu einer tätigkeitsbezogenen Beurteilung der Gefährdungen; die Betriebssicherheitsverordnung konkretisiert dies für die Verwendung von Arbeitsmitteln einschließlich Maschinen und Anlagen. Zu berücksichtigen sind auch vorhersehbare Betriebsstörungen, Änderungen, Instandhaltungsarbeiten sowie Qualifikation und Unterweisung der Beschäftigten. Cyberbedingte Fehlfunktionen oder Manipulationen von Steuerungs- und Sicherheitseinrichtungen können daher Gegenstand einer integrierten Gefährdungsbeurteilung sein. Die Vorschriften begründen nicht automatisch eine allgemeine Cybersecurity-Pflicht für jede Anlage, verlangen aber, relevante Gefährdungen für Beschäftigte zu erkennen und geeignete Schutzmaßnahmen festzulegen [13].

Für Konstruktion, Inverkehrbringen und Inbetriebnahme von Maschinen ist außerdem die Maschinenverordnung (EU) 2023/1230 zu berücksichtigen, die grundsätzlich ab dem 20. Januar 2027 anzuwenden ist. Sie enthält Anforderungen an die Sicherheit und den Gesundheitsschutz bei Maschinen und adressiert unter anderem Risiken durch mögliche Manipulation oder Korrumpierung sicherheitsrelevanter Software und Daten. Für Engineering, Automatisierung und Anlagenverantwortliche gewinnt damit die Fähigkeit an Bedeutung, Security-Aspekte bereits bei Spezifikation, Beschaffung, Integration und Änderungen von Maschinen zu berücksichtigen. Die Verordnung ist von den Betreiberpflichten im laufenden Betrieb zu unterscheiden; hierfür bleiben insbesondere die jeweils einschlägigen Arbeitsschutz- und Betriebssicherheitsvorschriften relevant [14].

Bei Betriebsbereichen im Anwendungsbereich der Störfall-Verordnung (12. BImSchV) kommt eine weitere sicherheitsrechtliche Dimension hinzu. Betreiber müssen erforderliche Vorkehrungen zur Verhinderung von Störfällen treffen, Eingriffe Unbefugter berücksichtigen und die Auswirkungen möglicher Störfälle begrenzen. Die Verordnung verlangt unter anderem zuverlässige Mess-, Steuer- und Regeleinrichtungen sowie den Schutz sicherheitsrelevanter Anlagenteile; das Sicherheitsmanagementsystem umfasst auch Organisation, Verantwortlichkeiten und Schulungsbedarf. Cybervorfälle sind dabei nicht automatisch Störfälle im Rechtssinn, können aber als Ursache oder Verstärker eines Szenarios relevant sein, wenn sie sicherheitsrelevante Funktionen beeinträchtigen oder gefährliche Stofffreisetzungen ermöglichen [15].

Für das Kompetenzmodell folgt daraus: Regulatorische Anforderungen sind keine fünfte Kompetenzdimension, sondern konkretisieren – abhängig von der jeweiligen Organisation – die Inhalte der vier Kompetenzfelder. Besonders wichtig sind die Fähigkeit zur Einordnung der Anwendbarkeit, die Übersetzung rechtlicher Pflichten in betriebliche Prozesse sowie die Zusammenarbeit von OT-Security, Betrieb, Engineering, Arbeitsschutz, Qualitätsmanagement und Unternehmensleitung.

Zusammenfassend beschreiben die genannten Normen und Leitlinien ein breites Anforderungsbild: OT-Security erfordert technische Schutzmaßnahmen, ein systematisches Risikomanagement, klare organisatorische Verantwortlichkeiten sowie die Zusammenarbeit unterschiedlicher Akteure über den gesamten Lebenszyklus industrieller Systeme. Die Normen definieren jedoch nicht in einer einheitlichen, unmittelbar übertragbaren Form, welche konkreten Kompetenzen jede einzelne betriebliche Rolle auf welchem Niveau besitzen sollte. Diese Konkretisierung bildet einen wesentlichen Ansatzpunkt des vorliegenden Kompetenzmodells.

2.2. Forschung zu Kompetenzen und Qualifikationsanforderungen in der OT-Security

Die wissenschaftliche Literatur zur Kompetenzentwicklung in der industriellen Cybersicherheit ist vorhanden, aber im Vergleich zur technischen OT-Security-Forschung weniger umfangreich und bislang nur teilweise konsolidiert. Chowdhury und Gkioulos identifizieren in einer systematischen Literaturübersicht vier Kompetenzbereiche für die Cybersicherheit kritischer Infrastrukturen: technische, Management-, Umsetzungs- und soziale Kompetenzen. Zugleich stellen sie fest, dass bislang kein einheitlicher Konsens darüber besteht, welche Kompetenzen für die verschiedenen Rollen besonders kritisch sind [8]. Ani et al. untersuchen die menschliche Dimension der industriellen Cybersicherheit und entwickeln einen Ansatz, mit dem sich Sicherheitswissen und praktische Fähigkeiten von Beschäftigten bewerten lassen [9]. Eine stärker arbeitsmarktbezogene Perspektive liefern Ramezan et al., die 100 Stellenanzeigen für OT-Cybersecurity-Positionen analysieren. Neben technischen Kenntnissen werden darin insbesondere Berufserfahrung, Kenntnisse relevanter Standards und Frameworks sowie Kommunikationsfähigkeiten nachgefragt [10]. Ergänzend bietet das NIST NICE Framework eine strukturierte Beschreibung von Cybersecurity-Aufgaben, Wissen und Fähigkeiten, ist jedoch nicht speziell auf die betrieblichen Rollen in OT-Umgebungen zugeschnitten [11]. Insgesamt zeigt die Literatur damit die Bedeutung technischer, organisatorischer und sozialer Kompetenzen, liefert aber bislang kein umfassendes, branchenübergreifend etabliertes Rollenmodell mit abgestuften Kompetenzniveaus für die OT-Security.

2.3. Einordnung und Beitrag des vorliegenden Kompetenzmodells

Aus der Zusammenschau der Normenlandschaft und des Forschungsstands ergibt sich eine erkennbare Lücke zwischen den allgemeinen Anforderungen an die Absicherung industrieller Systeme und ihrer konkreten Umsetzung in den betrieblichen Rollen. Während die IEC-62443-Reihe unterschiedliche Verantwortungsbereiche und Anforderungen entlang des Lebenszyklus beschreibt, bleiben die daraus abzuleitenden individuellen Kompetenzprofile in der konkreten betrieblichen Anwendung vielfach organisationsspezifisch zu bestimmen. Auch die vorhandenen Forschungsarbeiten liefern wichtige Hinweise auf erforderliche Kompetenzbereiche, bieten jedoch keine unmittelbar übertragbare Systematik für sämtliche an OT-Security beteiligten Funktionen eines Unternehmens.

Das vorliegende Modell setzt an dieser Schnittstelle an. Es überführt die fachlichen und organisatorischen Anforderungen in eine rollenbezogene Kompetenzstruktur. Hierzu werden vier Kompetenzfelder unterschieden:

- OT & Technik: Verständnis industrieller Anlagen, Automatisierungs- und Steuerungssysteme sowie ihrer technischen Zusammenhänge.
- Security: Kenntnisse und Fähigkeiten zur Identifikation, Bewertung und Behandlung von Cybersecurity-Risiken und zur Umsetzung geeigneter Schutzmaßnahmen.
- Prozesse & Organisation: Verständnis betrieblicher Abläufe, Verantwortlichkeiten, Governance-Strukturen und organisatorischer Sicherheitsprozesse.
- Kommunikation & Übersetzung: Fähigkeit, zwischen unterschiedlichen Fachdisziplinen zu vermitteln, Risiken verständlich zu kommunizieren und technische sowie organisatorische Anforderungen miteinander zu verbinden.

Die Kompetenzfelder werden durch vier beobachtungsorientierte Kompetenzniveaus ergänzt. Damit soll nicht nur beschrieben werden, welche Kompetenzen für eine Rolle relevant sind, sondern auch, in welcher Ausprägung diese Kompetenzen zur wirksamen Wahrnehmung der jeweiligen Aufgaben erforderlich sind. Die Gegenüberstellung von Ist- und Soll-Kompetenzen ermöglicht anschließend die Identifikation von Entwicklungsbedarfen und die Ableitung geeigneter Qualifizierungsmaßnahmen.

Das Modell versteht sich ausdrücklich nicht als Ersatz für die genannten Normen, Standards oder etablierten Kompetenzrahmen. Es stellt eine praxisorientierte Konkretisierung dar, die deren Anforderungen auf betriebliche Rollen und Entwicklungsbedarfe überträgt. Die konkrete Anwendung muss dabei an die jeweilige Anlagenlandschaft, Organisationsstruktur, Aufgabenverteilung und regulatorischen Rahmenbedingungen angepasst werden.

3. Methodik und Vorgehensweise der Kompetenzanalyse

3.1. Untersuchungsansatz und Datengrundlage

Die Entwicklung des vorliegenden Rollen- und Kompetenzmodells basiert auf einer strukturierten, workshopgestützten Anforderungsanalyse. Ziel des Vorgehens war es, die für eine wirksame Umsetzung von OT-Security erforderlichen Kompetenzen aus unterschiedlichen betrieblichen Perspektiven zu erfassen, systematisch zu ordnen und den relevanten Organisationsrollen zuzuordnen. Im Mittelpunkt stand dabei nicht die Bewertung individueller Beschäftigter, sondern die Beschreibung rollenbezogener Kompetenzanforderungen und die Identifikation daraus resultierender Entwicklungsbedarfe.

Die Datengrundlage bilden die Ergebnisse zweier I2M-Workshops. Die Workshops verfolgten unterschiedliche, aufeinander aufbauende Zielsetzungen: Während im ersten Workshop die fachliche Strukturierung der relevanten Kompetenzbereiche im Vordergrund stand, diente der zweite Workshop der rollenbezogenen Konkretisierung und Bewertung dieser Kompetenzen.

Die im ersten Workshop erarbeiteten fachlichen Inhalte wurden zu vier übergeordneten Kompetenzfeldern zusammengefasst:

- **OT & Technik:** Kompetenzen im Verständnis und Umgang mit industriellen Anlagen, Automatisierungs- und Steuerungssystemen sowie deren technischen Zusammenhängen.
- **Security:** Kompetenzen zur Identifikation, Bewertung und Behandlung von Cybersecurity-Risiken sowie zur Umsetzung geeigneter Sicherheitsmaßnahmen.
- **Prozesse & Organisation:** Kompetenzen im Hinblick auf betriebliche Abläufe, organisatorische Verantwortlichkeiten, Governance und die Integration von Sicherheitsanforderungen in bestehende Prozesse.
- **Kommunikation & Übersetzung:** Kompetenzen zur fachbereichsübergreifenden Kommunikation und zur Vermittlung zwischen technischen, organisatorischen und sicherheitsbezogenen Anforderungen.

Diese vier Kompetenzfelder bilden die inhaltliche Struktur des Modells. Sie dienen dazu, die unterschiedlichen Anforderungen an die betrachteten Rollen in einer einheitlichen Systematik abzubilden, ohne deren jeweilige fachliche Ausprägung gleichzusetzen.

Der zweite Workshop baute auf dieser Struktur auf. Im Rahmen eines Rollen-Kompetenz-Mappings wurden die Kompetenzanforderungen den betrachteten Rollen zugeordnet und hinsichtlich ihres jeweiligen Ausprägungsgrades eingeschätzt. Die daraus hervorgegangenen Ist-/Soll-Bewertungen bilden die Grundlage für die im Bericht dargestellten Kompetenzprofile und Kompetenzdifferenzen.

3.2. Rollenbezogene Analyse und Ist-/Soll-Abgleich

Die Analyse erfolgt rollenbezogen. Ausgangspunkt sind die im Rahmen der Workshops betrachteten OT-Security-bezogenen Funktionen und Verantwortungsbereiche innerhalb einer Organisation. Für jede Rolle wird untersucht, welche Beiträge sie zur Umsetzung von OT-Security leistet und welche Kompetenzen dafür erforderlich sind.

Die folgenden Rollen werden betrachtet:

- **Instandhaltung**: Stellt die technische Verfügbarkeit und Funktionsfähigkeit der Anlagen sicher. Im OT-Security-Kontext geht es insbesondere darum, Wartungs- und Reparaturarbeiten unter Berücksichtigung von Sicherheitsanforderungen durchzuführen und sicherheitsrelevante Auffälligkeiten zu erkennen.
- **Engineering**: Plant und realisiert technische Anlagen und Systeme sowie deren Änderungen. Die Rolle berücksichtigt OT-Security-Anforderungen bereits bei der Konzeption, Auswahl und Integration von Komponenten und Systemen.
- **Automatisierung / Digitalisierung**: Entwickelt und betreibt Automatisierungs- und Digitalisierungslösungen für Produktionsprozesse. Sie integriert Sicherheitsanforderungen in Steuerungs-, Kommunikations- und Datenverarbeitungssysteme und berücksichtigt dabei die Auswirkungen auf den laufenden Betrieb.
- **Anlagenbetreiber**: Trägt die operative Verantwortung für den sicheren und zuverlässigen Betrieb der Anlagen. Dazu gehört, Verfügbarkeit, Produktionsanforderungen und Safety mit den Anforderungen der OT-Security in Einklang zu bringen und sicherheitsrelevante Betriebsentscheidungen zu treffen.
- **Produktions-IT**: Stellt die IT-Infrastruktur und die IT-Services für die Produktion bereit. Im Mittelpunkt stehen die sichere Vernetzung von IT und OT, der Betrieb produktionsnaher IT-Systeme sowie die Umsetzung geeigneter Schutzmaßnahmen an den Schnittstellen.
- **Qualitätsmanagement**: Sichert die Einhaltung und kontinuierliche Verbesserung definierter Qualitätsanforderungen und Prozesse. Im OT-Security-Kontext unterstützt die Rolle dabei, Sicherheitsanforderungen in bestehende Management-, Audit- und Verbesserungsprozesse einzubetten.
- **Safety, Health & Environment (SHE)**: Verantwortet Aspekte der Arbeits-, Anlagen- und Umweltsicherheit. Die Rolle betrachtet insbesondere die möglichen physischen Auswirkungen von Cybervorfällen auf Menschen, Anlagen und Umwelt und unterstützt die Abstimmung zwischen Safety und Security.
- **CISO (Chief Information Security Officer)**: Verantwortet die Informationssicherheit auf strategischer und organisationsweiter Ebene. Im OT-Kontext stellt die Rolle sicher, dass OT-spezifische Risiken und Schutzanforderungen in die übergreifende Sicherheitsstrategie und das Informationssicherheitsmanagement einbezogen werden.
- **Head OT Security**: Trägt die übergreifende fachliche und organisatorische Verantwortung für die OT-Security. Dazu gehören die Entwicklung der OT-Security-Strategie, die Steuerung entsprechender Programme und Maßnahmen sowie der Aufbau geeigneter Strukturen und Kompetenzen.
- **BISO (Business Information Security Officer)**: Vermittelt zwischen den Sicherheitsanforderungen der Organisation und den fachlichen Anforderungen eines Geschäfts- bzw. Produktionsbereichs. Die Rolle übersetzt Security-Vorgaben in bereichsspezifische Anforderungen und unterstützt deren Umsetzung.
- **OT Security Expert / Architect**: Entwickelt und bewertet technische OT-Security-Architekturen und Schutzkonzepte. Die Rolle definiert technische Sicherheitslösungen, bewertet Risiken und stellt sicher, dass Schutzmaßnahmen mit den technischen und betrieblichen Randbedingungen der Anlagen vereinbar sind.
- **OT Security Coordinator / Engineer**: Koordiniert und realisiert konkrete OT-Security-Maßnahmen im operativen Umfeld. Dazu zählen beispielsweise die Umsetzung von Sicherheitsvorgaben, die Koordination von Schwachstellen- und Incident-Management sowie die Abstimmung mit Betrieb, Engineering und IT.

Regulatorische Anforderungen werden in der vorliegenden Analyse als Querschnittsbedingungen berücksichtigt. Sie wurden in den Workshops jedoch nicht als eigenständiges fünftes Kompetenzfeld und auch nicht für jede Rolle separat anhand einer Rechtskonformitätsprüfung bewertet. Die Rollenprofile beschreiben daher erforderliche Fähigkeiten, regulatorische Anforderungen in den jeweiligen Verantwortungsbereich zu übersetzen und mit den zuständigen Fachfunktionen zusammenzuarbeiten. Ob und in welchem Umfang NIS-2/BSIG, Arbeitsschutz- und Betriebssicherheitsrecht, Maschinenverordnung oder Störfall-Verordnung auf eine konkrete Organisation oder Anlage Anwendung finden, ist standort- und organisationsspezifisch zu prüfen.

Die Rollen sind als funktionale Perspektiven auf OT-Security zu verstehen. Sie müssen nicht zwingend jeweils eigenständigen Stellen oder Personen entsprechen. Insbesondere in kleineren Organisationen können mehrere Rollen durch dieselbe Person wahrgenommen werden; umgekehrt können einzelne Rollen auf mehrere Personen verteilt sein.

Die Zuordnung der Kompetenzen erfolgt entlang der vier zuvor beschriebenen Kompetenzfelder. Dabei wird zwischen dem im Rollen-Kompetenz-Mapping erfassten Ist-Zustand und dem angestrebten Soll-Zustand unterschieden. Der Ist-Zustand beschreibt das im Workshop eingeschätzte Kompetenzniveau, während der Soll-Zustand die für eine angemessene Wahrnehmung der jeweiligen Rolle als erforderlich angesehene Ausprägung abbildet.

Der Vergleich beider Einschätzungen ermöglicht es, rollenbezogene Kompetenzdifferenzen sichtbar zu machen. Diese Differenzen werden im Bericht als Entwicklungsbedarfe interpretiert. Sie geben Hinweise darauf, in welchen Kompetenzfeldern eine Rolle gestärkt werden sollte und wo gegebenenfalls bereits ein ausreichendes Kompetenzniveau angenommen wird.

Die Ist-/Soll-Bewertungen werden aus dem im zweiten Workshop erstellten Rollen-Kompetenz-Mapping übernommen. Sie stellen somit keine nachträglich durchgeführte individuelle Kompetenzmessung dar. Vielmehr dokumentieren sie die im Workshop erarbeiteten Einschätzungen auf der Ebene der Rollen. Die Ergebnisse sind daher als strukturierte fachliche Einschätzung und nicht als objektiv gemessene Kompetenzwerte zu verstehen.

Insbesondere ist zwischen Kompetenzanforderungen und rechtlicher Pflichtenverteilung zu unterscheiden: Das Modell ordnet Rollen fachliche Beiträge zu, begründet aber keine neue Betreiber-, Arbeitgeber-, Hersteller- oder Leitungsverantwortung und ersetzt keine rechtliche Prüfung. Gesetzliche Pflichten verbleiben bei den jeweils normativ verpflichteten Rechtsträgern bzw. verantwortlichen Personen; die interne Aufgabenübertragung und Delegation muss organisationsspezifisch geregelt werden.

3.3. Operationalisierung der Kompetenzniveaus

Um die unterschiedlichen Kompetenzanforderungen vergleichbar beschreiben zu können, wird eine vierstufige Skala verwendet. Die Beschreibung der Niveaus orientiert sich an der revidierten Bloom'schen Lernzieltaxonomie, die unterschiedliche kognitive Anforderungsstufen von Erinnern und Verstehen über Anwenden und Analysieren bis hin zu Bewerten und Gestalten unterscheidet.

Die Bloom-Orientierung wird dabei nicht als unmittelbares Messinstrument verwendet. Vielmehr dient sie als konzeptionelle Grundlage, um Kompetenzniveaus anhand des erwarteten Handelns und der Selbstständigkeit bei der Aufgabenwahrnehmung zu beschreiben. Die Einstufung bezieht sich ausdrücklich nicht auf das Dienstalter, die Dauer der Berufserfahrung oder das Vorliegen einer bestimmten formalen Qualifikation. Entscheidend ist vielmehr, welche Aufgaben eine Person im

jeweiligen Kompetenzfeld bewältigen kann und in welchem Umfang sie dabei Anleitung oder Unterstützung benötigt.

Die vier Kompetenzniveaus werden wie folgt operationalisiert:

Niveau	Bloom-orientierte, beobachtbare Beschreibung
Sehr niedrig	**Erinnern / erste Orientierung:** Die Person kann einzelne Begriffe mit Unterstützung benennen, erkennt typische Situationen jedoch noch nicht zuverlässig und benötigt eine kleinschrittige Anleitung.
Niedrig	**Verstehen:** Die Person kann grundlegende Zusammenhänge erläutern und typische Situationen erkennen. Einfache Aufgaben werden mit Anleitung und anhand vorgegebener Verfahren bearbeitet.
Mittel	**Anwenden / Analysieren:** Die Person wendet Methoden in bekannten Situationen selbstständig an, analysiert Abweichungen und kann Maßnahmen im eigenen Verantwortungsbereich begründen.
Hoch	**Bewerten / Gestalten:** Die Person bewertet komplexe Zielkonflikte selbstständig, entwickelt tragfähige Lösungen, priorisiert Maßnahmen und steuert deren Umsetzung auch über Bereichsgrenzen hinweg.

Die Skala bildet damit eine qualitative Entwicklungsperspektive ab: Von einer ersten Orientierung und angeleiteten Aufgabenbearbeitung über die selbstständige Anwendung bis hin zur eigenständigen Gestaltung und bereichsübergreifenden Steuerung. Die Niveaus sind als allgemeine Beschreibungslogik zu verstehen. Ihre konkrete Ausprägung muss jeweils im Kontext des betrachteten Kompetenzfeldes und der jeweiligen Rolle interpretiert werden.

3.4. Ableitung von Entwicklungsmaßnahmen

Auf Grundlage der Ist-/Soll-Gegenüberstellung werden für die einzelnen Rollen Entwicklungsempfehlungen formuliert. Ausgangspunkt ist dabei die Frage, welche Kompetenzdifferenzen für die wirksame Wahrnehmung der jeweiligen Rolle besonders relevant sind und durch welche Qualifizierungs- oder Entwicklungsmaßnahmen diese adressiert werden können.

Die Entwicklungsmaßnahmen stellen analytische Ableitungen aus den Workshop-Ergebnissen dar. Sie wurden aus den identifizierten Kompetenzanforderungen und den erkennbaren Differenzen zwischen Ist- und Soll-Niveau entwickelt. Sie sind ausdrücklich nicht mit Beschlüssen oder verbindlichen Maßnahmenfestlegungen der Workshop-Teilnehmenden gleichzusetzen.

Bei der Formulierung der Empfehlungen wird angestrebt, die Maßnahmen möglichst eng mit den jeweiligen Aufgaben und Verantwortlichkeiten der Rollen zu verknüpfen. Je nach Kompetenzfeld können dies beispielsweise fachliche Schulungen, praktische Übungen, die Mitarbeit in Projekten, die Einbindung in bereichsübergreifende Arbeitsgruppen oder die Übernahme spezifischer Verantwortlichkeiten sein. Die konkrete Auswahl und Ausgestaltung geeigneter Maßnahmen bleibt den jeweiligen Organisationen vorbehalten.

Die rollenbezogenen Empfehlungen werden anschließend zu übergreifenden Entwicklungsbedarfen zusammengeführt. Dadurch lassen sich sowohl spezifische Qualifizierungsanforderungen einzelner Rollen als auch gemeinsame Entwicklungsfelder identifizieren, die mehrere Rollen oder Organisationseinheiten betreffen.

3.5. Methodische Einordnung und Grenzen der Aussagekraft

Das entwickelte Kompetenzmodell ist als Instrument zur strukturierten Beschreibung von Rollenanforderungen und zur Unterstützung der Personalentwicklung konzipiert. Die verwendete Kompetenzmatrix stellt eine Operationalisierung dar, mit der Kompetenzanforderungen und Entwicklungsbedarfe systematisch beschrieben und diskutiert werden können.

Die zugrunde liegenden Workshop-Unterlagen enthalten jedoch keine formalisierten Prüfverfahren, standardisierten Bewertungsinstrumente oder empirisch validierten Kriterien für eine zertifizierte Kompetenzmessung. Insbesondere ist nicht dokumentiert, dass die Kompetenzniveaus durch standardisierte Tests oder systematische Beobachtungsverfahren bei einzelnen Beschäftigten erhoben wurden. Die im Rollen-Kompetenz-Mapping enthaltenen Ist-Einschätzungen sind daher als workshopbasierte Einschätzungen zu interpretieren.

Für die Übertragung des Modells auf konkrete Personen und Organisationen ist deshalb eine zusätzliche Validierung erforderlich. Eine individuelle Einstufung sollte nicht allein aus der Stellenbezeichnung oder der Zuordnung zu einer Rolle abgeleitet werden. Vielmehr empfiehlt sich eine Kombination unterschiedlicher Beobachtungs- und Bewertungsformen, beispielsweise:

- strukturierte Interviews zu Aufgaben, Erfahrungen und Handlungssituationen,
- Arbeitsproben und praktische Übungen,
- Beobachtung der Aufgabenwahrnehmung im betrieblichen Kontext,
- Bewertung konkreter Projektbeiträge und Problemlösungen,
- fachliche Einschätzung durch Vorgesetzte und relevante Schnittstellenpartner.

Darüber hinaus sind die Ergebnisse im Kontext der jeweiligen Organisation zu interpretieren. Aufgabenverteilung, Anlagenlandschaft, Automatisierungsgrad, regulatorische Anforderungen und bestehende Sicherheitsorganisation können dazu führen, dass sich Kompetenzanforderungen zwischen Unternehmen unterscheiden, auch wenn die Rollenbezeichnungen vergleichbar sind.

Schließlich ist zu berücksichtigen, dass die Ergebnisse auf den beiden zugrunde liegenden Workshops beruhen und keine repräsentative Erhebung über Unternehmen oder Branchen hinweg darstellen. Eine statistische Generalisierbarkeit wird daher nicht beansprucht. Das Modell ist vielmehr als wissenschaftlich fundierte, praxisorientierte Strukturierungshilfe zu verstehen, deren Übertragbarkeit und Wirksamkeit in weiteren betrieblichen Anwendungen überprüft und gegebenenfalls angepasst werden sollte.

4. Ergebnisse des Kompetenzmappings und Rollenprofile

4.1. Rollen-Kompetenzprofile

Die folgenden Rollenprofile bilden den Kern des entwickelten Kompetenzmodells. Sie beschreiben für jede der zwölf betrachteten Rollen die relevanten Anforderungen in den vier Kompetenzfeldern und konkretisieren diese durch beobachtbare Kompetenzniveaus sowie typische Aufgaben. Die Profile sind als rollenbezogene Orientierungsrahmen zu verstehen; sie ersetzen keine organisationsspezifischen Stellenbeschreibungen. Ihre konkrete Ausgestaltung hängt insbesondere von Anlagenstruktur, Betriebsmodell, Verantwortungsverteilung und regulatorischem Umfeld ab.

4.1.1. Rollenprofil: Instandhaltung

4.1.1.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu Anlagenzustände, Steuerungen, Wartung, Legacy und Verfügbarkeit, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Anlagenzustände, Steuerungen, Wartung, Legacy und Verfügbarkeit und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Anlagenzustände, Steuerungen, Wartung, Legacy und Verfügbarkeit in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Anlagenzustände, Steuerungen, Wartung, Legacy und Verfügbarkeit unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.1.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu sichere Wartung, Auffälligkeiten, Schwachstellen und Meldewege, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu sichere Wartung, Auffälligkeiten, Schwachstellen und Meldewege und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu sichere Wartung, Auffälligkeiten, Schwachstellen und Meldewege in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu sichere Wartung, Auffälligkeiten, Schwachstellen und Meldewege unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.1.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Wartungs- und Change-Prozesse, Dokumentation und Eskalation, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Wartungs- und Change-Prozesse, Dokumentation und Eskalation und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Wartungs- und Change-Prozesse, Dokumentation und Eskalation in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Wartungs- und Change-Prozesse, Dokumentation und Eskalation unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.1.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu Meldungen, Übergaben und Abstimmung mit Produktion, IT und Security, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Meldungen, Übergaben und Abstimmung mit Produktion, IT und Security und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Meldungen, Übergaben und Abstimmung mit Produktion, IT und Security in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Meldungen, Übergaben und Abstimmung mit Produktion, IT und Security unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.1.5. Typische Stellenbeschreibung

Sichere und verfügbare Anlagen im laufenden Betrieb erhalten; OT-Sicherheitsanforderungen in Wartung, Störungsbehebung und Instandhaltungsplanung integrieren.

1. Anlagen- und Steuerungskomponenten im Betrieb verstehen und Änderungen nachvollziehbar durchführen.
2. Sicherheitsrelevante Auffälligkeiten, Schwachstellen und unsichere Fernzugriffe erkennen und über definierte Meldewege eskalieren.
3. Wartungs-, Patch- und Ersatzmaßnahmen mit Produktion, Engineering und OT-Security abstimmen.
4. Verfügbarkeit und Safety bei Security-Maßnahmen berücksichtigen; Änderungen dokumentieren.

Bei Wartungs-, Prüf- und Reparaturarbeiten sind die Gefährdungsbeurteilung, sichere Arbeitsverfahren, Freischalt- und Wiederanlaufprozesse sowie die erforderliche Qualifikation und

Unterweisung nach Arbeitsschutz- und Betriebssicherheitsrecht zu beachten. In störfallrelevanten Betriebsbereichen müssen sicherheitsrelevante Wartungen, Prüfungen und Eingriffe nachvollziehbar dokumentiert und gegen unbefugte Veränderungen geschützt werden.

4.1.2. Rollenprofil: Engineering

4.1.2.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu Anlagenarchitekturen, technische Änderungen, Safety und Lifecycle, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Anlagenarchitekturen, technische Änderungen, Safety und Lifecycle und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Anlagenarchitekturen, technische Änderungen, Safety und Lifecycle in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Anlagenarchitekturen, technische Änderungen, Safety und Lifecycle unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.2.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Security-by-Design, Bedrohungen und Sicherheitsanforderungen in Projekten, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Security-by-Design, Bedrohungen und Sicherheitsanforderungen in Projekten und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Security-by-Design, Bedrohungen und Sicherheitsanforderungen in Projekten in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Security-by-Design, Bedrohungen und Sicherheitsanforderungen in Projekten unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.2.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Projekt-, Design-Review-, Beschaffungs- und Änderungsprozesse, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Projekt-, Design-Review-, Beschaffungs- und Änderungsprozesse und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Projekt-, Design-Review-, Beschaffungs- und Änderungsprozesse in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.

4. Hoch: Bewertet komplexe Fragestellungen zu Projekt-, Design-Review-, Beschaffungs- und Änderungsprozesse unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.2.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu technische Security-Anforderungen für Projektbeteiligte und Lieferanten, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu technische Security-Anforderungen für Projektbeteiligte und Lieferanten und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu technische Security-Anforderungen für Projektbeteiligte und Lieferanten in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu technische Security-Anforderungen für Projektbeteiligte und Lieferanten unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.2.5. Typische Stellenbeschreibung

Anlagen, Maschinen und technische Lösungen planen, ändern und industrialisieren und Security-Anforderungen in Engineering- und Änderungsprozesse integrieren.

1. Technische Anlagenarchitekturen und ihre Betriebs- und Safety-Abhängigkeiten bewerten.
2. Security-Anforderungen in Spezifikationen, Beschaffung, Design Reviews und Änderungen berücksichtigen.
3. Risiken und Auswirkungen auf Produktion, Qualität und Lifecycle in Projektentscheidungen einbringen.
4. Mit IT, OT-Security, Automatisierung, Lieferanten und Betrieb technische Lösungen abstimmen.

Bei Neu- und Umbauprojekten sind die Anforderungen der Maschinenverordnung (EU) 2023/1230 – soweit einschlägig ab ihrem Anwendungsbeginn am 20. Januar 2027 – bereits in Spezifikation, Risikobeurteilung, Auswahl und Integration von Maschinen und Steuerungen einzubeziehen. Änderungen an bestehenden Anlagen sind zugleich auf Auswirkungen auf Safety, Gefährdungsbeurteilung, Konformität und gegebenenfalls störfallrelevante Sicherheitsfunktionen zu prüfen.

4.1.3. Rollenprofil: Automatisierung / Digitalisierung

4.1.3.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu SPS, Automatisierung, OT-Protokolle und IT/OT-Schnittstellen, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu SPS, Automatisierung, OT-Protokolle und IT/OT-Schnittstellen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.

3. Mittel: Wendet passende Verfahren zu SPS, Automatisierung, OT-Protokolle und IT/OT-Schnittstellen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu SPS, Automatisierung, OT-Protokolle und IT/OT-Schnittstellen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.3.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Hardening, Segmentierung, Zugriffsschutz und Bedrohungsanalyse, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Hardening, Segmentierung, Zugriffsschutz und Bedrohungsanalyse und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Hardening, Segmentierung, Zugriffsschutz und Bedrohungsanalyse in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Hardening, Segmentierung, Zugriffsschutz und Bedrohungsanalyse unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.3.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Projektintegration, Change, Verantwortlichkeiten und Lifecycle, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Projektintegration, Change, Verantwortlichkeiten und Lifecycle und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Projektintegration, Change, Verantwortlichkeiten und Lifecycle in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Projektintegration, Change, Verantwortlichkeiten und Lifecycle unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.3.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu Abstimmung zwischen Automatisierung, Betrieb, IT und Security, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Abstimmung zwischen Automatisierung, Betrieb, IT und Security und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.

3. Mittel: Wendet passende Verfahren zu Abstimmung zwischen Automatisierung, Betrieb, IT und Security in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Abstimmung zwischen Automatisierung, Betrieb, IT und Security unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.3.5. Typische Stellenbeschreibung

Automatisierungs- und Digitalisierungsplattformen technisch gestalten und betreiben und ihre sichere Einbindung in industrielle Produktionsumgebungen gewährleisten.

1. SPS, Steuerungsarchitekturen, OT-Protokolle und Schnittstellen zu IT-Systemen verstehen und beurteilen.
2. Grundlegende Security-Maßnahmen wie Segmentierung, sichere Konfiguration und kontrollierten Fernzugriff umsetzen.
3. Security-Anforderungen in Automatisierungs- und Digitalisierungsprojekte integrieren.
4. Mit Produktion, Engineering, IT und Security Änderungen und Betriebsrisiken koordinieren.

Die Gestaltung und Änderung von Steuerungs-, Leitsystem- und Digitalisierungsfunktionen muss mögliche Wechselwirkungen zwischen Cybersecurity und funktionaler Sicherheit berücksichtigen. Sicherheitsrelevante Software, Daten und Konfigurationen sind gegen unbeabsichtigte oder unbefugte Veränderung zu schützen; Änderungen müssen nachvollziehbar bewertet, getestet und freigegeben werden.

4.1.4. Rollenprofil: Anlagenbetreiber

4.1.4.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu Anlagenfunktion, Produktionsabhängigkeiten, Verfügbarkeit und sichere Betriebszustände, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Anlagenfunktion, Produktionsabhängigkeiten, Verfügbarkeit und sichere Betriebszustände und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Anlagenfunktion, Produktionsabhängigkeiten, Verfügbarkeit und sichere Betriebszustände in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Anlagenfunktion, Produktionsabhängigkeiten, Verfügbarkeit und sichere Betriebszustände unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.4.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Cyberrisiken, Risikoabwägung, Eskalation und Notfallverhalten, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Cyberrisiken, Risikoabwägung, Eskalation und Notfallverhalten und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Cyberrisiken, Risikoabwägung, Eskalation und Notfallverhalten in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Cyberrisiken, Risikoabwägung, Eskalation und Notfallverhalten unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.4.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Betriebsentscheidungen, Verantwortlichkeiten, Business Continuity und Risikoakzeptanz, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Betriebsentscheidungen, Verantwortlichkeiten, Business Continuity und Risikoakzeptanz und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Betriebsentscheidungen, Verantwortlichkeiten, Business Continuity und Risikoakzeptanz in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Betriebsentscheidungen, Verantwortlichkeiten, Business Continuity und Risikoakzeptanz unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.4.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu betriebliche Risiken, Maßnahmen und Entscheidungen an Teams und Management vermitteln, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu betriebliche Risiken, Maßnahmen und Entscheidungen an Teams und Management vermitteln und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu betriebliche Risiken, Maßnahmen und Entscheidungen an Teams und Management vermitteln in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.

4. Hoch: Bewertet komplexe Fragestellungen zu betriebliche Risiken, Maßnahmen und Entscheidungen an Teams und Management vermitteln unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.4.5. Typische Stellenbeschreibung

Den sicheren und wirtschaftlichen Betrieb einer Anlage verantworten und Produktionsziele, Anlagenverfügbarkeit, Safety und OT-Security in Betriebsentscheidungen zusammenführen.

1. Produktionsabläufe, kritische Abhängigkeiten und Folgen von Anlagenstörungen benennen.
2. Security-relevante Risiken und Betriebsabweichungen erkennen, priorisieren und an zuständige Stellen melden.
3. Security-Maßnahmen mit Produktionsplanung, Instandhaltung, Engineering und OT-Security abstimmen.
4. Betriebliche Entscheidungen und Ausnahmegenehmigungen unter Berücksichtigung von Risiko, Verfügbarkeit und Safety treffen.

Der Betreiber muss – soweit die jeweiligen Regelwerke anwendbar sind – OT-Risiken in die Betreiberpflichten nach BSIG/NIS-2, in Gefährdungsbeurteilungen und in das Sicherheitsmanagement nach Störfall-Verordnung einordnen. Dazu gehören klare Zuständigkeiten, belastbare Notfall- und Wiederanlaufverfahren sowie die Bewertung, ob Cybereignisse sicherheitsrelevante Anlagenfunktionen oder Störfallszenarien beeinflussen können.

4.1.5. Rollenprofil: Produktions-IT

4.1.5.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu Produktionssysteme, OT-Netze, Legacy und Auswirkungen von IT-Änderungen, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Produktionssysteme, OT-Netze, Legacy und Auswirkungen von IT-Änderungen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Produktionssysteme, OT-Netze, Legacy und Auswirkungen von IT-Änderungen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Produktionssysteme, OT-Netze, Legacy und Auswirkungen von IT-Änderungen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.5.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu OT-Security-Architektur, Monitoring, Schwachstellen- und Incident-Management, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu OT-Security-Architektur, Monitoring, Schwachstellen- und Incident-Management und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.

3. Mittel: Wendet passende Verfahren zu OT-Security-Architektur, Monitoring, Schwachstellen- und Incident-Management in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu OT-Security-Architektur, Monitoring, Schwachstellen- und Incident-Management unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.5.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu IT/OT-Prozesse, Asset-/Schwachstellenmanagement und Maßnahmensteuerung, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu IT/OT-Prozesse, Asset-/Schwachstellenmanagement und Maßnahmensteuerung und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu IT/OT-Prozesse, Asset-/Schwachstellenmanagement und Maßnahmensteuerung in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu IT/OT-Prozesse, Asset-/Schwachstellenmanagement und Maßnahmensteuerung unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.5.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu IT/OT-Schnittstellen, Eskalation und Erklärung von Produktionsrisiken, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu IT/OT-Schnittstellen, Eskalation und Erklärung von Produktionsrisiken und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu IT/OT-Schnittstellen, Eskalation und Erklärung von Produktionsrisiken in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu IT/OT-Schnittstellen, Eskalation und Erklärung von Produktionsrisiken unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.5.5. Typische Stellenbeschreibung

IT-nahe Infrastruktur und Services für die Produktion bereitstellen und den sicheren, verfügbaren Betrieb an der IT/OT-Schnittstelle unterstützen.

1. Produktionsnahe IT-Systeme, OT-Abhängigkeiten und Auswirkungen von Änderungen auf den Betrieb nachvollziehen.

2. Security-Maßnahmen wie Segmentierung, Monitoring, Zugriffsschutz und Schwachstellenbehandlung für Produktionsumgebungen planen oder umsetzen.
3. IT- und OT-Risiken gemeinsam mit Anlagenverantwortlichen bewerten.
4. Security-Vorfälle und Änderungen entlang definierter Schnittstellen koordinieren und verständlich kommunizieren.

4.1.6. Rollenprofil: Qualitätsmanagement

4.1.6.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu technische Anlagenabhängigkeiten und OT-spezifische Randbedingungen, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu technische Anlagenabhängigkeiten und OT-spezifische Randbedingungen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu technische Anlagenabhängigkeiten und OT-spezifische Randbedingungen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu technische Anlagenabhängigkeiten und OT-spezifische Randbedingungen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.6.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Security-Risiken, Kontrollziele, Nachweise und Maßnahmenwirksamkeit, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Security-Risiken, Kontrollziele, Nachweise und Maßnahmenwirksamkeit und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Security-Risiken, Kontrollziele, Nachweise und Maßnahmenwirksamkeit in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Security-Risiken, Kontrollziele, Nachweise und Maßnahmenwirksamkeit unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.6.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Audits, Qualitätsprozesse, Maßnahmenverfolgung und Wirksamkeitsprüfung, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Audits, Qualitätsprozesse, Maßnahmenverfolgung und Wirksamkeitsprüfung und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.

3. Mittel: Wendet passende Verfahren zu Audits, Qualitätsprozesse, Maßnahmenverfolgung und Wirksamkeitsprüfung in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Audits, Qualitätsprozesse, Maßnahmenverfolgung und Wirksamkeitsprüfung unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.6.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu Security-Anforderungen verständlich in Prozesse und Audits übersetzen, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Security-Anforderungen verständlich in Prozesse und Audits übersetzen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Security-Anforderungen verständlich in Prozesse und Audits übersetzen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Security-Anforderungen verständlich in Prozesse und Audits übersetzen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.6.5. Typische Stellenbeschreibung

Qualitätsmanagementsysteme und Nachweise steuern und OT-Security-Anforderungen in etablierte Qualitäts-, Audit-, Änderungs- und Verbesserungsprozesse integrieren.

1. Bestehende Qualitätsprozesse, Audits, Dokumentation und Korrekturmaßnahmen auf Anschlussfähigkeit für OT-Security prüfen.
2. Security-Risiken, Maßnahmen und Nachweise in Prozess- und Auditstrukturen integrieren.
3. Abweichungen, Verantwortlichkeiten und Wirksamkeit von Maßnahmen nachvollziehbar verfolgen.
4. Security-Anforderungen für Fachbereiche verständlich aufbereiten und Verbesserungsmaßnahmen moderieren.

4.1.7. Rollenprofil: Safety, Health & Environment (SHE)

4.1.7.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu Safety-Systeme, Cyber-physische Auswirkungen und sichere Betriebszustände, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Safety-Systeme, Cyber-physische Auswirkungen und sichere Betriebszustände und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.

3. Mittel: Wendet passende Verfahren zu Safety-Systeme, Cyber-physische Auswirkungen und sichere Betriebszustände in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Safety-Systeme, Cyber-physische Auswirkungen und sichere Betriebszustände unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.7.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Cyberrisiken mit Safety-/Umweltwirkung und Notfallvorsorge, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Cyberrisiken mit Safety-/Umweltwirkung und Notfallvorsorge und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Cyberrisiken mit Safety-/Umweltwirkung und Notfallvorsorge in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Cyberrisiken mit Safety-/Umweltwirkung und Notfallvorsorge unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.7.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Risikomanagement, Audits, Notfallplanung und Verantwortlichkeiten, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Risikomanagement, Audits, Notfallplanung und Verantwortlichkeiten und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Risikomanagement, Audits, Notfallplanung und Verantwortlichkeiten in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Risikomanagement, Audits, Notfallplanung und Verantwortlichkeiten unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.7.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu Cyber-/Safety-Wechselwirkungen und Maßnahmen bereichsübergreifend vermitteln, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Cyber-/Safety-Wechselwirkungen und Maßnahmen bereichsübergreifend vermitteln und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.

3. Mittel: Wendet passende Verfahren zu Cyber-/Safety-Wechselwirkungen und Maßnahmen bereichsübergreifend vermitteln in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Cyber-/Safety-Wechselwirkungen und Maßnahmen bereichsübergreifend vermitteln unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.7.5. Typische Stellenbeschreibung

Safety-, Gesundheits- und Umweltanforderungen verantworten und Wechselwirkungen zwischen funktionaler Sicherheit, Cybersecurity und Anlagenbetrieb frühzeitig sichtbar machen.

1. Safety- und Umweltfolgen möglicher Cybervorfälle und Security-Änderungen identifizieren.
2. Security-Grundlagen so weit verstehen, dass Risiken für Schutzsysteme, Verfügbarkeit und sichere Betriebszustände erkannt werden.
3. Bestehende Risiko-, Audit- und Managementprozesse mit OT-Security abstimmen.
4. Sicherheitsrelevante Informationen zielgruppengerecht vermitteln und bereichsübergreifende Maßnahmen unterstützen.

SHE sollte Cyberbedrohungen dort in Gefährdungsbeurteilungen und Sicherheitsmanagementprozesse einbringen, wo sie die Sicherheit und Gesundheit von Beschäftigten oder die Beherrschung von Anlagengefahren beeinflussen können. Bei Betriebsbereichen nach Störfall-Verordnung ist insbesondere die Schnittstelle zwischen Cybervorfall, sicherheitsrelevanten Anlagenteilen, Alarm- und Gefahrenabwehrplanung sowie den zuständigen Einsatz- und Fachstellen zu berücksichtigen.

4.1.8. Rollenprofil: CISO

4.1.8.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu OT-Architektur, Legacy, Safety und Produktionsabhängigkeiten, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu OT-Architektur, Legacy, Safety und Produktionsabhängigkeiten und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu OT-Architektur, Legacy, Safety und Produktionsabhängigkeiten in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu OT-Architektur, Legacy, Safety und Produktionsabhängigkeiten unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.8.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu OT-Risikosteuerung, Schutzmaßnahmen und Wirksamkeit der Security-Governance, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.

2. Niedrig: Erläutert grundlegende Zusammenhänge zu OT-Risikosteuerung, Schutzmaßnahmen und Wirksamkeit der Security-Governance und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu OT-Risikosteuerung, Schutzmaßnahmen und Wirksamkeit der Security-Governance in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu OT-Risikosteuerung, Schutzmaßnahmen und Wirksamkeit der Security-Governance unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.8.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Governance, Risikomanagement, Priorisierung und unternehmensweite Verantwortlichkeiten, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Governance, Risikomanagement, Priorisierung und unternehmensweite Verantwortlichkeiten und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Governance, Risikomanagement, Priorisierung und unternehmensweite Verantwortlichkeiten in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Governance, Risikomanagement, Priorisierung und unternehmensweite Verantwortlichkeiten unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.8.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu OT-Risiken und Investitionsentscheidungen gegenüber Management und Fachbereichen vermitteln, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu OT-Risiken und Investitionsentscheidungen gegenüber Management und Fachbereichen vermitteln und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu OT-Risiken und Investitionsentscheidungen gegenüber Management und Fachbereichen vermitteln in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu OT-Risiken und Investitionsentscheidungen gegenüber Management und Fachbereichen vermitteln unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.8.5. Typische Stellenbeschreibung

Die unternehmensweite Informationssicherheitsstrategie und Governance verantworten und OT-Security angemessen in Risikosteuerung, Priorisierung und Managemententscheidungen integrieren.

1. OT-spezifische Risiken, Produktionsabhängigkeiten und Safety-/Verfügbarkeitsanforderungen in die unternehmensweite Risikosicht aufnehmen.
2. Strategie, Governance, Verantwortlichkeiten und Eskalationswege für OT-Security festlegen.
3. Ressourcen und Maßnahmen risikobasiert priorisieren und Restrisiken transparent entscheiden lassen.
4. Management und Fachbereiche zu OT-Risiken, regulatorischen Erwartungen und Handlungsoptionen beraten.

Der CISO muss die Anwendbarkeit des BSIG/NIS-2 gemeinsam mit den zuständigen Rechts-, Compliance- und Fachfunktionen einordnen und sicherstellen, dass OT-Systeme in Risikomanagement, Vorfallbehandlung, Business Continuity, Lieferkettensicherheit und Meldeprozesse einbezogen werden. Die operative Umsetzung und die gesetzlichen Verantwortlichkeiten sind dabei eindeutig zuzuordnen.

4.1.9. Rollenprofil: Head OT Security

4.1.9.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu industrielle Architekturen, Betriebsrealität und technische Schutzanforderungen, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu industrielle Architekturen, Betriebsrealität und technische Schutzanforderungen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu industrielle Architekturen, Betriebsrealität und technische Schutzanforderungen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu industrielle Architekturen, Betriebsrealität und technische Schutzanforderungen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.9.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Architektur, Risikoanalyse, Detection, Incident-Resilienz und Lieferkettensicherheit, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Architektur, Risikoanalyse, Detection, Incident-Resilienz und Lieferkettensicherheit und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Architektur, Risikoanalyse, Detection, Incident-Resilienz und Lieferkettensicherheit in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.

4. Hoch: Bewertet komplexe Fragestellungen zu Architektur, Risikoanalyse, Detection, Incident-Resilienz und Lieferkettensicherheit unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.9.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Strategie, Governance, Roadmap, Ressourcen und kontinuierliche Verbesserung, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Strategie, Governance, Roadmap, Ressourcen und kontinuierliche Verbesserung und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Strategie, Governance, Roadmap, Ressourcen und kontinuierliche Verbesserung in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Strategie, Governance, Roadmap, Ressourcen und kontinuierliche Verbesserung unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.9.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu gemeinsames Zielbild, Stakeholder, Konfliktlösung und Befähigung, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu gemeinsames Zielbild, Stakeholder, Konfliktlösung und Befähigung und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu gemeinsames Zielbild, Stakeholder, Konfliktlösung und Befähigung in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu gemeinsames Zielbild, Stakeholder, Konfliktlösung und Befähigung unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.9.5. Typische Stellenbeschreibung

OT-Security-Funktion, Zielbild und Umsetzung unternehmensweit steuern und technische, organisatorische und kommunikative Fähigkeiten zu einem wirksamen Programm verbinden.

1. OT-Security-Strategie, Architekturprinzipien, Standards und Roadmap verantworten.
2. Risiken und Maßnahmen über Standorte, Anlagen, Projekte und Lieferanten hinweg priorisieren.
3. Rollen, Verantwortlichkeiten, Kennzahlen, Governance und Incident-Bereitschaft etablieren.
4. Fachbereiche, Management und externe Partner führen, befähigen und bei Zielkonflikten vermitteln.

Die OT-Security-Funktion sollte regulatorische Anforderungen in ein abgestimmtes OT-Security-Programm übersetzen und Schnittstellen zu CISO, Anlagenbetrieb, Engineering, SHE und Qualitätsmanagement verbindlich gestalten. Dazu gehören insbesondere OT-relevante Nachweise, Melde- und Eskalationswege sowie die Berücksichtigung von Safety- und Störfallauswirkungen in Risiko- und Incident-Prozessen.

4.1.10. Rollenprofil: BISO (Business Information Security Officer)

4.1.10.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu geschäftsrelevante OT-Abhängigkeiten und technische Grundzusammenhänge, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu geschäftsrelevante OT-Abhängigkeiten und technische Grundzusammenhänge und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu geschäftsrelevante OT-Abhängigkeiten und technische Grundzusammenhänge in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu geschäftsrelevante OT-Abhängigkeiten und technische Grundzusammenhänge unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.10.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Risikoanalyse, Security-Anforderungen und Maßnahmenpriorisierung, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Risikoanalyse, Security-Anforderungen und Maßnahmenpriorisierung und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Risikoanalyse, Security-Anforderungen und Maßnahmenpriorisierung in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Risikoanalyse, Security-Anforderungen und Maßnahmenpriorisierung unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.10.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Governance, Rollen, Risiko- und Maßnahmenmanagement im Geschäftsbereich, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.

2. Niedrig: Erläutert grundlegende Zusammenhänge zu Governance, Rollen, Risiko- und Maßnahmenmanagement im Geschäftsbereich und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Governance, Rollen, Risiko- und Maßnahmenmanagement im Geschäftsbereich in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Governance, Rollen, Risiko- und Maßnahmenmanagement im Geschäftsbereich unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.10.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu Business-Risiken und Security-Anforderungen zwischen Stakeholdern übersetzen, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Business-Risiken und Security-Anforderungen zwischen Stakeholdern übersetzen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Business-Risiken und Security-Anforderungen zwischen Stakeholdern übersetzen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Business-Risiken und Security-Anforderungen zwischen Stakeholdern übersetzen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.10.5. Typische Stellenbeschreibung

Security-Anforderungen und -Risiken in einem Geschäftsbereich vertreten und zwischen Business, zentraler Security, IT und operativen Bereichen vermitteln.

1. Geschäftsbereichsrisiken und betriebliche Auswirkungen von OT-Security-Themen strukturieren.
2. Security-Grundlagen und Anforderungen in umsetzbare Maßnahmen für den Bereich übersetzen.
3. Governance, Verantwortlichkeiten, Maßnahmenverfolgung und Eskalation im Geschäftsbereich unterstützen.
4. Vertrauen aufbauen, Zielkonflikte moderieren und Managemententscheidungen verständlich vorbereiten.

4.1.11. Rollenprofil: OT Security Expert / Architect

4.1.11.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu industrielle Architekturen, Zonen/Conduits, Protokolle und technische Schutzmaßnahmen, kann deren Bedeutung für die eigene Rolle

aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.

2. Niedrig: Erläutert grundlegende Zusammenhänge zu industrielle Architekturen, Zonen/Conduits, Protokolle und technische Schutzmaßnahmen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu industrielle Architekturen, Zonen/Conduits, Protokolle und technische Schutzmaßnahmen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu industrielle Architekturen, Zonen/Conduits, Protokolle und technische Schutzmaßnahmen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.11.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu Threat Modelling, Architektur, Segmentierung, Hardening und Detection, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Threat Modelling, Architektur, Segmentierung, Hardening und Detection und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Threat Modelling, Architektur, Segmentierung, Hardening und Detection in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Threat Modelling, Architektur, Segmentierung, Hardening und Detection unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.11.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Lifecycle, Governance, Projektintegration und Architekturentscheidungen, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Lifecycle, Governance, Projektintegration und Architekturentscheidungen und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Lifecycle, Governance, Projektintegration und Architekturentscheidungen in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Lifecycle, Governance, Projektintegration und Architekturentscheidungen unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.11.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu Architektur- und Risikoentscheidungen zielgruppengerecht erklären, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Architektur- und Risikoentscheidungen zielgruppengerecht erklären und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Architektur- und Risikoentscheidungen zielgruppengerecht erklären in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Architektur- und Risikoentscheidungen zielgruppengerecht erklären unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.11.5. Typische Stellenbeschreibung

OT-Security-Architekturen und technische Schutzmaßnahmen entwerfen, Risiken bewerten und die sichere Gestaltung industrieller Systeme über ihren Lebenszyklus begleiten.

1. OT-Architekturen, Zonen und Kommunikationsbeziehungen analysieren und sichere Zielarchitekturen entwerfen.
2. Threat Modelling, Risikoanalyse, Segmentierung, Hardening, Monitoring und Zugriffsschutz fachlich verantworten.
3. Security-Anforderungen in Projekte, Betrieb, Lieferantenbeziehungen und Incident-Vorbereitung übersetzen.
4. Architekturentscheidungen, Risiken und notwendige Maßnahmen für unterschiedliche Zielgruppen verständlich erläutern.

Bei Architekturentscheidungen sind neben Cybersecurity-Anforderungen auch die Anforderungen an Maschinen- und Anlagensicherheit sowie – sofern einschlägig – störfallrelevante Schutzfunktionen zu berücksichtigen. Sicherheitsmaßnahmen dürfen Schutz- oder Steuerungsfunktionen nicht unbeabsichtigt beeinträchtigen; technische Änderungen sind mit Engineering, Betrieb und Safety abzustimmen.

4.1.12. Rollenprofil: OT Security Coordinator / Engineer

4.1.12.1. OT & Technik

1. Sehr niedrig: Benennt einzelne Begriffe zu Anlagen, OT-Netze, Steuerungen und operative technische Abhängigkeiten, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Anlagen, OT-Netze, Steuerungen und operative technische Abhängigkeiten und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Anlagen, OT-Netze, Steuerungen und operative technische Abhängigkeiten in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.

4. Hoch: Bewertet komplexe Fragestellungen zu Anlagen, OT-Netze, Steuerungen und operative technische Abhängigkeiten unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.12.2. Security

1. Sehr niedrig: Benennt einzelne Begriffe zu operative Schutzmaßnahmen, Schwachstellen, Monitoring und Incident-Abläufe, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu operative Schutzmaßnahmen, Schwachstellen, Monitoring und Incident-Abläufe und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu operative Schutzmaßnahmen, Schwachstellen, Monitoring und Incident-Abläufe in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu operative Schutzmaßnahmen, Schwachstellen, Monitoring und Incident-Abläufe unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.12.3. Prozesse & Organisation

1. Sehr niedrig: Benennt einzelne Begriffe zu Maßnahmenplanung, Dokumentation, Change und operative Koordination, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Maßnahmenplanung, Dokumentation, Change und operative Koordination und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Maßnahmenplanung, Dokumentation, Change und operative Koordination in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.
4. Hoch: Bewertet komplexe Fragestellungen zu Maßnahmenplanung, Dokumentation, Change und operative Koordination unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.12.4. Kommunikation & Übersetzung

1. Sehr niedrig: Benennt einzelne Begriffe zu Status, Blockaden, Risiken und Vorfälle verständlich kommunizieren, kann deren Bedeutung für die eigene Rolle aber noch nicht zuverlässig erklären und benötigt Anleitung, um relevante Situationen zu erkennen.
2. Niedrig: Erläutert grundlegende Zusammenhänge zu Status, Blockaden, Risiken und Vorfälle verständlich kommunizieren und erkennt typische Beispiele; bearbeitet einfache Aufgaben mit Checklisten oder Unterstützung erfahrener Kolleginnen und Kollegen.
3. Mittel: Wendet passende Verfahren zu Status, Blockaden, Risiken und Vorfälle verständlich kommunizieren in bekannten Situationen selbstständig an, analysiert Abweichungen und begründet geeignete Maßnahmen innerhalb der eigenen Zuständigkeit.

4. Hoch: Bewertet komplexe Fragestellungen zu Status, Blockaden, Risiken und Vorfälle verständlich kommunizieren unter Abwägung von Risiko, Verfügbarkeit, Safety und Geschäftswirkung; gestaltet Lösungen, setzt Prioritäten und stimmt die Umsetzung mit relevanten Bereichen ab.

4.1.12.5. Typische Stellenbeschreibung

OT-Security-Maßnahmen operativ koordinieren und umsetzen, technische Risiken in konkrete Arbeitspakete übersetzen und lokale Ansprechpartner verbinden.

1. OT-Anlagen, Netzwerke und Produktionsabhängigkeiten ausreichend tief verstehen, um Maßnahmen korrekt einzuordnen.
2. Security-Maßnahmen wie Asset-Erfassung, Schwachstellenmanagement, sichere Fernzugriffe und Segmentierung koordinieren oder umsetzen.
3. Risiken, Abweichungen und Maßnahmen dokumentieren und die Zusammenarbeit zwischen Betrieb, IT und Security organisieren.
4. Fortschritt, Blockaden und Vorfälle zielgruppengerecht kommunizieren und eskalieren.

4.2. Ist-/Soll-Mapping der Rollen

Das Rollen-Kompetenz-Mapping konzentriert die Workshop-Einschätzungen zu einer vergleichenden Übersicht. Für jedes Kompetenzfeld werden das eingeschätzte Ist-Niveau und das angestrebte Soll-Niveau gegenübergestellt. Die resultierenden Differenzen machen sichtbar, wo Entwicklungsbedarf besteht und wo vorhandene Kompetenzen zunächst gesichert und weitergegeben werden sollten. Die Werte sind ordinal zu interpretieren; sie bilden weder eine quantitative Gesamtpunktzahl noch eine Rangfolge der Rollen.

Rolle	OT Ist	OT Soll	Security Ist	Security Soll	Prozesse Ist	Prozesse Soll	Komm. Ist	Komm. Soll
Instandhaltung	Hoch	Hoch	Niedrig	Mittel	Niedrig	Mittel	Niedrig	Mittel
Engineering	Mittel	Mittel	Niedrig	Mittel	Hoch	Hoch	Hoch	Hoch
Automatisierung / Digitalisierung	Mittel	Hoch	Niedrig	Mittel	Hoch	Hoch	Mittel	Mittel
Produktions-IT	Sehr niedrig	Mittel	Mittel	Hoch	Niedrig	Mittel	Niedrig	Mittel
Qualitätsmanagement	Niedrig	Niedrig	Niedrig	Mittel	Hoch	Hoch	Niedrig	Mittel
Anlagenbetreiber	Sehr niedrig	Mittel	Niedrig	Mittel	Hoch	Hoch	Hoch	Hoch
Safety, Health & Environment (SHE)	Niedrig	Niedrig	Niedrig	Mittel	Hoch	Hoch	Niedrig	Mittel
CISO	Niedrig	Mittel	Hoch	Hoch	Hoch	Hoch	Hoch	Hoch
Head OT Security	Hoch	Hoch	Hoch	Hoch	Hoch	Hoch	Hoch	Hoch

BISO (Business Information Security Officer)	Mittel	Mittel	Niedrig	Mittel	Niedrig	Mittel	Hoch	Hoch
OT Security Expert / Architect	Hoch	Hoch	Hoch	Hoch	Niedrig	Mittel	Mittel	Hoch
OT Security Coordinator / Engineer	Mittel	Hoch	Mittel	Hoch	Niedrig	Mittel	Mittel	Mittel

Die Werte sind ordinal und nicht additiv zu interpretieren. Ein „hoher“ Wert in Kommunikation kompensiert beispielsweise keinen kritischen Mangel in OT-Technik oder Security, wenn diese Kompetenz für die jeweilige Aufgabe erforderlich ist.

4.3. Entwicklungsempfehlungen

Aus dem Ist-/Soll-Abgleich lassen sich Entwicklungsbedarfe unterschiedlicher Größenordnung ableiten. Die nachfolgende Übersicht fasst zunächst die Kompetenzdifferenzen nach ihrer Ausprägung zusammen und benennt die betroffenen Rollen und Kompetenzfelder. Sie dient der übergreifenden Orientierung; die konkrete Umsetzung muss anschließend an den jeweiligen betrieblichen Kontext angepasst werden.

Die folgende Priorisierung richtet sich nach der Distanz zwischen Ist- und Sollniveau in der Workshop-Matrix. Ein Delta von zwei Niveaustufen wird vor einem Delta von einer Niveaustufe priorisiert. Die Einstufung beschreibt die Größe des Entwicklungsbedarfs, nicht automatisch Aufwand, Dauer oder Kritikalität einer konkreten Maßnahme. Die ausführlichen Maßnahmen stehen jeweils im Abschnitt der betreffenden Rolle.

In der operativen Umsetzung sind regulatorisch relevante Prozesse praktisch zu unterstützen: dokumentierte Changes, Schwachstellen- und Patchbewertungen, sichere Fernwartung, Incident-Eskalation und Wiederanlauf. Bei möglichen Auswirkungen auf Beschäftigte oder störfallrelevante Funktionen ist frühzeitig SHE bzw. die zuständige Störfallorganisation einzubeziehen.

4.3.1. Großes Kompetenzdelta: zwei Niveaustufen

4.3.1.1. Produktions-IT

1. OT & Technik (Sehr niedrig → Mittel): OT-Grundlagen gezielt aufbauen, insbesondere Anlagen- und Prozessverständnis, OT-Architekturen und die besonderen Verfügbarkeits- und Sicherheitsanforderungen industrieller Umgebungen. Dafür ein intensives Format „OT für IT-Experten“ mit Praxisanteilen und begleitetem Einsatz an einer Anlage vorsehen.

4.3.1.2. Anlagenbetreiber

2. OT & Technik (Sehr niedrig → Mittel): Ein arbeitsplatznahes OT-Basisprogramm aufbauen, damit Anlagenbetreiber Architektur, kritische Komponenten, Betriebsabhängigkeiten und typische Auswirkungen von Cybervorfällen verstehen. Die Inhalte anhand der eigenen Anlage und konkreter Störungsszenarien üben.

4.3.2. Mittleres Kompetenzdelta: eine Niveaustufe

4.3.2.1. Instandhaltung

5. Security (Niedrig → Mittel): Sicherheitsanforderungen in Wartung, Diagnose und Instandsetzung sicher anwenden; Checklisten, sichere Fernwartung und Meldewege anhand realer Arbeitsabläufe trainieren.
6. Prozesse & Organisation (Niedrig → Mittel): Security-Prüfpunkte in Wartungs- und Freigabeprozesse integrieren und Abweichungen nachvollziehbar dokumentieren.
7. Kommunikation & Übersetzung (Niedrig → Mittel): Verdächtige Beobachtungen und Sicherheitsvorfälle strukturiert, zeitnah und mit den für IT/OT-Security erforderlichen Informationen melden.

4.3.2.2. Engineering

3. Security (Niedrig → Mittel): Security-by-Design, IEC 62443, Zonen und Conduits sowie OT-Risikobewertungen in Engineering-Aufgaben anwenden.

4.3.2.3. Automatisierung / Digitalisierung

4. OT & Technik (Mittel → Hoch): OT-Protokolle, Steuerungs- und Leitsysteme sowie deren Abhängigkeiten vertiefen; Härtung und sichere Konfiguration an repräsentativen Systemen praktisch umsetzen.
5. Security (Niedrig → Mittel): Sicherheitsmaßnahmen für Automatisierungs- und Digitalisierungslösungen systematisch anwenden und Risiken bereits bei Konzeption und Änderung berücksichtigen.

4.3.2.4. Produktions-IT

6. Security (Mittel → Hoch): Sicherheitskompetenz auf ein selbstständiges Bewertungs- und Gestaltungsniveau entwickeln. Schwerpunkte sind OT-Risikobewertung, sichere Segmentierung, Fernzugriffe, Schwachstellen- und Patchmanagement unter Betriebsbedingungen sowie die begründete Abwägung von Security-Maßnahmen gegen Verfügbarkeit und Safety.
7. Prozesse & Organisation (Niedrig → Mittel): Training zu OT-spezifischem Prozess- und Change-Management; eine Änderung von der Risikoanalyse bis zur Betriebsfreigabe als Fallstudie bearbeiten.
8. Kommunikation & Übersetzung (Niedrig → Mittel): Regelmäßige Fallstudien gemeinsam mit OT und Security besprechen, Übung zur Incident-Kommunikation, in der technische Befunde in Produktionsauswirkungen, notwendige Entscheidungen und nächste Schritte übersetzt werden.

4.3.2.5. Qualitätsmanagement

9. Security (Niedrig → Mittel): Grundlegende Security-Anforderungen und Nachweise in Qualitäts- und Auditprozesse integrieren; relevante Bezüge zu ISO 27001 und BSI-Grundlagen erschließen.
10. Kommunikation & Übersetzung (Niedrig → Mittel): Security-Feststellungen adressatengerecht dokumentieren, nachverfolgen und mit OT-Fachbereichen in umsetzbare Korrekturmaßnahmen übersetzen.

4.3.2.6. *Safety, Health & Environment (SHE)*

1. Security (Niedrig → Mittel): Cyberrisiken mit Auswirkungen auf sichere Anlagenzustände in bestehende Risiko- und Schutzprozesse aufnehmen.
2. Kommunikation & Übersetzung (Niedrig → Mittel): Safety- und Security-Perspektiven in gemeinsamen Bewertungen, Übungen und Eskalationswegen verständlich zusammenführen.

4.3.2.7. *CISO*

1. OT & Technik (Niedrig → Mittel): Ein praxisnahes OT-Crash-Programm mit Anlagenbesuchen, Einblicken in Steuerungs-/Leitsysteme und typischen Betriebszwängen absolvieren, um OT-Risiken und Maßnahmenentscheidungen fundiert einordnen zu können.

4.3.2.8. *BISO (Business Information Security Officer)*

1. Security (Niedrig → Mittel): Ein belastbares Grundlagenverständnis aufbauen, beispielsweise über eine grundlegende Cybersecurity-Qualifizierung (CISM oder vergleichbar) und deren Übertragung auf OT-Risiken.
2. Prozesse & Organisation (Niedrig → Mittel): OT-relevante Risiko- und Maßnahmenregister, Verantwortlichkeiten und Eskalationswege in bestehende Business-, Prozess- und Qualitätsmanagementstrukturen integrieren.

4.3.2.9. *OT Security Expert / Architect*

1. Prozesse & Organisation (Niedrig → Mittel): Projekt-, Change- und Governance-Prozesse systematisieren, damit technische Architekturentscheidungen zuverlässig in Planung, Freigabe, Umsetzung und Betrieb überführt werden.
2. Kommunikation & Übersetzung (Mittel → Hoch): Technische Risiken und Architekturentscheidungen zielgruppengerecht bis auf Managementebene vermitteln, Optionen und Zielkonflikte transparent darstellen und Entscheidungen nachvollziehbar begründen.

4.3.2.10. *OT Security Coordinator / Engineer*

1. OT & Technik (Mittel → Hoch): Technische OT-Security-Kompetenz vertiefen, etwa durch praxisorientierte Schulungen zu IEC 62443, OT-Architekturen, Segmentierung, Härtung und sicheren Fernzugriffen. Die Anwendung durch Job Shadowing bei Expert/Architect und durch konkrete Anlagen- oder Projektaufgaben absichern.
2. Security (Mittel → Hoch): Von der Anwendung bekannter Verfahren zur selbstständigen Analyse und Bewertung komplexerer Sicherheitsfragen entwickeln. Dazu gehören technische Risikobewertungen, die Priorisierung von Maßnahmen, die Bewertung von Schwachstellen im OT-Kontext und die nachvollziehbare Dokumentation von Entscheidungen.

4.3.3. Kein Kompetenzdelta

Für die anderen Kompetenzfelder wird in der Workshop-Matrix kein Unterschied zwischen Ist- und Sollniveau ausgewiesen. Entsprechend wird hier keine zusätzliche Entwicklungsmaßnahme abgeleitet.

4.4. Detaillierte Entwicklungsempfehlungen

Im Anschluss an die übergreifende Einordnung werden die Entwicklungsbedarfe für jede Rolle einzeln betrachtet. Die Empfehlungen orientieren sich an den jeweiligen Soll-Ist-Differenzen und

unterscheiden zwischen dem gezielten Aufbau fehlender Kompetenzen und dem Erhalt bereits erreichter Niveaus. Wo kein formales Delta ausgewiesen ist, können dennoch Maßnahmen zur Aktualisierung, Anwendung oder Weitergabe vorhandenen Wissens sinnvoll sein. Die Vorschläge sind als fachliche Empfehlungen und nicht als verbindliche Workshop-Beschlüsse zu verstehen. Die vorgeschlagenen Maßnahmen sind am jeweiligen Kompetenzdelta ausgerichtet. Wo das Soll bereits erreicht ist, liegt der Schwerpunkt auf Erhalt und Wissenstransfer.

4.4.1. Rollenprofil Instandhaltung

Die technische Ausgangsbasis ist bereits hoch und soll gehalten werden. Die Entwicklungsbedarfe liegen vor allem in Security-Grundlagen sowie in der Einbindung von Security in Prozesse und Kommunikation. Mitarbeitende müssen nicht zu Security-Architekten werden, aber Risiken und typische Angriffspfade erkennen, sichere Arbeitsweisen anwenden und relevante Beobachtungen zuverlässig melden können.

4.4.1.1. OT & Technik

Soll-Ist-Delta: Hoch → Hoch

2. Kein ausgewiesenes Kompetenzdelta; das technische Anlagenwissen ist zu erhalten und als Multiplikator einzusetzen.
3. Erfahrene Mitarbeitende pflegen eine kompakte Übersicht kritischer Anlagenkomponenten, Steuerungen, Kommunikationsverbindungen und bekannter Legacy-Systeme. Die Informationen werden in Wartungs- und Übergabedokumentation integriert.
4. Bei Anlagenbegehungen mit OT-Security werden technische Abhängigkeiten und mögliche Auswirkungen von Eingriffen auf Verfügbarkeit und sicheren Betrieb erläutert.

4.4.1.2. Security

Soll-Ist-Delta: Niedrig → Mittel

3. Die größte Entwicklung liegt in der Fähigkeit, Security-Grundlagen in der täglichen Instandhaltung anzuwenden.
4. Basisschulung „OT Security Fundamentals“ mit Fokus auf typische Angriffswege, Schadsoftware, Phishing, Schwachstellen, privilegierte Konten, Fernwartung und Wechseldatenträger.
5. Praxisfälle an der eigenen Anlage nutzen: Welche Auffälligkeiten sind sicherheitsrelevant? Was darf nicht eigenmächtig verändert werden? Wann und an wen wird eskaliert?
6. Eine begleitete Übung zu sicherer Wartung und dem Umgang mit einem verdächtigen Laptop, Datenträger oder Herstellerzugang durchführen.

4.4.1.3. Prozesse & Organisation

Soll-Ist-Delta: Niedrig → Mittel

1. Security muss als normaler Bestandteil des Instandhaltungszyklus verstanden und angewendet werden.
2. Workshop zur Integration von Security-Checklisten in Wartungsaufträge, geplante Stillstände, Störungsbehebung und Change-Prozesse.
3. Freigaben für Herstellerzugänge, Dokumentation von Ausnahmen, Patch-/Update-Abstimmung und Meldewege mit OT-Security und Anlagenbetrieb festlegen.

4. Ein reales Wartungsbeispiel gemeinsam durchgehen und prüfen, ob Verantwortlichkeit, Freigabe, Rückfallplan und Dokumentation vollständig sind.

4.4.1.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Niedrig → Mittel

1. Entwicklungsbedarf besteht bei klarer, verlässlicher Kommunikation über Security-Auffälligkeiten und deren Betriebswirkung.
2. Training zu Kommunikationsstrukturen im Incident-Fall: Beobachtung, vermutete Ursache, betroffene Anlage und unmittelbare Auswirkungen getrennt beschreiben.
3. Übergaben und Eskalationen zwischen Schicht, Instandhaltung, Produktion, IT und OT-Security in einer kurzen Übung simulieren.
4. Eine einseitige Meldehilfe mit Kontaktwegen, Mindestinformationen und Verhalten bis zur Rückmeldung erstellen.

4.4.2. Rollenprofil Engineering

Prozess- und Kommunikationskompetenzen sind bereits hoch und sollen erhalten bleiben; OT-Technik bleibt auf mittlerem Niveau. Der zentrale Gap liegt bei Security: von niedrigen Grundlagenkenntnissen zu einem mittleren Niveau, auf dem Security-Anforderungen in Engineering-Arbeit übersetzt und bei Design- und Änderungsentscheidungen angewendet werden. Die Rolle ist ein wichtiger Hebel, weil Security bereits in Planung und Änderung statt erst im Betrieb berücksichtigt werden kann.

4.4.2.1. OT & Technik

Soll-Ist-Delta: Mittel → Mittel

1. Kein ausgewiesenes Delta. Vorhandenes Engineering- und Anlagenwissen erhalten; bei kritischen Projekten technische Abhängigkeiten und betriebliche Randbedingungen systematisch dokumentieren.
2. Bei Design Reviews die Auswirkungen von Änderungen auf Verfügbarkeit, Safety, Wartbarkeit und vorhandene Legacy-Komponenten berücksichtigen.

4.4.2.2. Security

Soll-Ist-Delta: Niedrig → Mittel

1. Primäres Kompetenzdelta: Security-by-Design muss von einer bekannten Idee zu einer praktisch angewendeten Engineering-Methode werden.
2. Training zu IEC 62443 mit besonderem Fokus auf Zonen und Conduits, Schutzanforderungen, sichere Konfigurationen und kontrollierte Lieferanten-/Fernzugriffe.
3. Workshop zur Risikoabwägung zwischen Funktionalität, Verfügbarkeit und Security im Anlagenbau; an einem realen Entwurf Schutzbedarf und Maßnahmen ableiten.
4. Security-Anforderungen in Lastenhefte, Spezifikationen, Design Reviews, Beschaffung, FAT/SAT und Betriebsübergabe integrieren.
5. Ein Projekt durch ein begleitetes Security-Review führen und die Entscheidungen einschließlich Restrisiken dokumentieren.

4.4.2.3. Prozesse & Organisation

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Die bestehende Prozesskompetenz sollte genutzt werden, um Security systematisch in vorhandene Engineering- und Qualitätsabläufe einzubetten.
2. Prüfpunkte und Verantwortlichkeiten für Security in Projekt-Gates, Änderungsmanagement und Lieferantenabnahmen verankern; Doppelprozesse vermeiden.

4.4.2.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Die hohe Schnittstellenkompetenz ist zu erhalten und für die Vermittlung von Security-Anforderungen an Betrieb, Lieferanten und Projektleitung zu nutzen.
2. Als Praxisnachweis eine technische Security-Anforderung in verständliche Akzeptanzkriterien für Projektteam und Lieferant übersetzen.

4.4.3. Rollenprofil Automatisierung / Digitalisierung

Das Prozess- und Organisationsverständnis ist hoch, Kommunikation mittel; beides soll beibehalten werden. OT- und Technikverständnis soll von mittel auf hoch steigen, Security von niedrig auf mittel. Damit wird erwartet, dass die Rolle nicht nur Automatisierungslösungen realisiert, sondern technische Abhängigkeiten, OT-Protokolle und Schutzmaßnahmen in ihrer Produktionswirkung beurteilen kann.

4.4.3.1. OT & Technik

Soll-Ist-Delta: Mittel → Hoch

1. Die technische Tiefe muss so erweitert werden, dass Automatisierungs- und Digitalisierungslösungen mitsamt ihren industriellen Kommunikationsbeziehungen und Betriebsabhängigkeiten beurteilt werden können.
2. Vertiefende Trainings zu OT-Protokollen, SPS-/PLS-/SCADA-Architekturen, industriellen Netzwerken, Latenzen, Legacy und Abhängigkeiten zwischen Steuerungs- und Leitebene.
3. Eine konkrete Anlagen- oder Testbed-Architektur mit Kommunikationspfaden, kritischen Assets und betrieblichen Abhängigkeiten dokumentieren und durch eine erfahrene OT-Fachrolle reviewen lassen.

4.4.3.2. Security

Soll-Ist-Delta: Niedrig → Mittel

1. Security muss in der technischen Umsetzung praktisch angewendet werden, nicht nur als allgemeine Anforderung bekannt sein.
2. Training zu Hardening von PLS-/SCADA-Systemen, sicherer Konfiguration, Segmentierung, Zugriffsschutz, Fernwartung und Schwachstellenbehandlung.
3. Ein kleines Praxislabor aufbauen oder nutzen, in dem sichere Konfigurationen und die Auswirkungen ausgewählter Maßnahmen getestet werden.
4. Für eine Automatisierungszelle ein Threat-Modelling durchführen und Schutzmaßnahmen mit OT-Security nach Risiko und Umsetzbarkeit priorisieren.

4.4.3.3. Prozesse & Organisation

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Bestehende Prozesskompetenz nutzen, um Security-Anforderungen in Digitalisierungsprojekte, Change-Prozesse und Abnahmekriterien aufzunehmen.
2. Security-Verantwortlichkeiten und Nachweise in Projektvorlagen und Betriebsübergaben festlegen.

4.4.3.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Mittel → Mittel

1. Kein ausgewiesenes Delta. Die vorhandene Kommunikationsfähigkeit ist zu stabilisieren.
2. Technische Security-Risiken und geplante Änderungen so aufbereiten, dass Betrieb und Projektleitung Auswirkungen auf Verfügbarkeit, Stillstandsfenster und Wiederanlauf verstehen.

4.4.4. Rollenprofil Anlagenbetreiber

Prozesse und Kommunikation sind hoch und sollen hoch bleiben. OT-Technik ist sehr niedrig und soll auf mittel, Security niedrig und soll ebenfalls auf mittel steigen. Die Rolle muss die technische Funktionsweise und Abhängigkeiten der eigenen Anlage so weit verstehen, dass sie Security-Risiken, Auswirkungen auf die Produktion und notwendige Eskalationen beurteilen kann. Der Fokus liegt auf fundierten Betriebsentscheidungen, nicht auf technischer Umsetzung im Detail.

4.4.4.1. OT & Technik

Soll-Ist-Delta: Sehr niedrig → Mittel

1. Das technische Grundverständnis muss deutlich steigen, damit Betriebsentscheidungen auf realistischen Vorstellungen der Anlage und ihrer Abhängigkeiten beruhen.
2. Grundkurs „Technische Grundlagen der OT“ mit Anlagenarchitektur, Steuerungen, Netzwerken, Legacy, Produktionsabhängigkeiten und sicheren Betriebszuständen.
3. Site Visits mit Engineering und Instandhaltung; eine einfache Anlagenlandkarte kritischer Komponenten und Abhängigkeiten erstellen.
4. Anhand eines Beispiels erläutern, welche Produktionsbereiche von einer Komponente oder Kommunikationsverbindung abhängen und welche Folgen ein Ausfall hätte.

4.4.4.2. Security

Soll-Ist-Delta: Niedrig → Mittel

1. Security-Kompetenz soll eine belastbare Einschätzung typischer Cyberrisiken und angemessene betriebliche Entscheidungen ermöglichen.
2. Awareness-Training zu Cyberrisiken in der Produktion mit Fokus auf Erkennung, Meldung, Eskalation und sichere Verhaltensweisen.
3. Tabletop-Übung zu kompromittiertem System, Produktionsunterbrechung, manuellen Verfahren, Isolierung und Wiederanlauf durchführen.
4. Mit OT-Security Kriterien festlegen, wann eine Maßnahme sofort umgesetzt, geplant oder auf Managementebene als Restrisiko entschieden werden muss.

4.4.4.3. Prozesse & Organisation

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Vorhandene Prozesskompetenz für Freigaben, Risikoakzeptanz, Business Continuity und Notfallplanung einsetzen.
2. OT-Security als festen Punkt in Betriebsrunden, Change-Freigaben und Notfallübungen verankern.

4.4.4.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Die bestehende Kommunikationskompetenz für Lagebilder, Eskalationen und die Koordination von Betriebsentscheidungen nutzen.
2. Kommunikations- und Entscheidungsrollen im Cybervorfall vorab festlegen und in einer Übung überprüfen.

4.4.5. Rollenprofil Produktions-IT

Hier ist das deutlichste mehrdimensionale Entwicklungsprofil zu sehen: OT-Technik ist sehr niedrig und soll auf mittel steigen; Security ist mittel und soll hoch werden; Prozesse und Kommunikation sollen von niedrig auf mittel steigen. Besonders wichtig ist, dass klassische IT-Sicherheitsmaßnahmen nicht unbesehen auf Produktionssysteme übertragen werden. Es braucht ein solides Verständnis von Anlagenverfügbarkeit, Legacy und Safety sowie vertiefte OT-Security-Fähigkeiten.

4.4.5.1. OT & Technik

Soll-Ist-Delta: Sehr niedrig → Mittel

1. Dies ist eines der größten Kompetenzdeltas. Klassisches IT-Wissen muss um ein belastbares Verständnis der Produktions- und Steuerungsebene ergänzt werden.
2. Intensivkurs „OT für IT-Experten“ zu Hardware, SPS/SCADA, industriellen Protokollen, Latenzen, Legacy-Systemen, Safety und Produktionsabhängigkeiten.
3. Begleitete Site Visits und Gespräche mit Instandhaltung, Engineering und Anlagenbetreibern durchführen, um den realen Anlagenbetrieb kennenzulernen.
4. Eine Produktionszelle samt Asset-Landkarte, Datenflüssen und kritischen Abhängigkeiten dokumentieren; Ergebnisse durch den Anlagenverantwortlichen validieren lassen.

4.4.5.2. Security

Soll-Ist-Delta: Mittel → Hoch

1. Die vorhandenen Security-Kenntnisse müssen für die OT-Welt vertieft und um die Konsequenzen für den Produktionsbetrieb ergänzt werden.
2. Vertiefung zu IEC 62443, Zonen/Conduits, OT-Segmentierung, sicherem Remote Access, Monitoring, Schwachstellenmanagement und Incident Response.
3. Workshop zur Risikoabwägung in der OT: Produktionsfähigkeit, Verfügbarkeit und sichere Betriebszustände gegen Schutzmaßnahmen und Restrisiken abwägen.
4. Eine Schutzmaßnahme für eine abgegrenzte Produktionszelle planen, in einer freigegebenen Testumgebung prüfen und mit Betrieb und OT-Security bewerten.

4.4.5.3. Prozesse & Organisation

Soll-Ist-Delta: Niedrig → Mittel

1. IT-Prozesse müssen an die längeren Lebenszyklen und eingeschränkten Änderungsmöglichkeiten von OT-Systemen angepasst werden.
2. Gemeinsame Abläufe für Patchfenster, Notfalländerungen, Ausnahmen, Asset-Verantwortung, Freigaben, Rückfallpläne und Wiederanlauf mit dem Produktionsbetrieb definieren.
3. Training zu OT-spezifischem Prozess- und Change-Management; eine Änderung von der Risikoanalyse bis zur Betriebsfreigabe als Fallstudie bearbeiten.

4.4.5.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Niedrig → Mittel

1. Die Rolle muss zwischen klassischer IT-Security und Produktion übersetzen und Zielkonflikte früh sichtbar machen.
2. Regelmäßige gemeinsame Fallbesprechungen mit Instandhaltung, Engineering und Anlagenbetrieb durchführen.
3. Eine Übung zur Incident-Kommunikation durchführen, in der technische Befunde in Produktionsauswirkungen, notwendige Entscheidungen und nächste Schritte übersetzt werden.

4.4.6. Rollenprofil Qualitätsmanagement

Prozesse und Organisation sind bereits hoch; OT-Technik bleibt niedrig. Security muss von niedrig auf mittel und Kommunikation von niedrig auf mittel steigen. Ziel ist kein tiefes technisches Spezialistentum, sondern die Fähigkeit, OT-Security-Anforderungen in prüfbare, praktikable und wirksame Managementprozesse zu überführen und die Umsetzung verständlich zu begleiten.

4.4.6.1. OT & Technik

Soll-Ist-Delta: Niedrig → Niedrig

1. Kein formales Delta in der Workshop-Matrix. Es ist keine technische Spezialistenqualifikation erforderlich.
2. Ein begrenztes Orientierungsmodul zu OT-Anlagen, Verfügbarkeit, Legacy und Safety ist dennoch sinnvoll, damit Audits und Qualitätsprozesse die betrieblichen Randbedingungen nicht übersehen.

4.4.6.2. Security

Soll-Ist-Delta: Niedrig → Mittel

1. Security-Anforderungen und deren Nachweise müssen in Qualitäts- und Auditprozessen zuverlässig bewertet werden können.
2. Schulung zu regulatorischer Orientierung und Managementsystemen, insbesondere ISO 27001 und einschlägigen BSI-Vorgaben, jeweils mit Bezug zu OT-Prozessen.
3. Training zur Vorbereitung und Durchführung von Security-Audits für OT-Prozesse: Kontrollziel, Nachweis, Verantwortlichkeit, Abweichung und Wirksamkeitsprüfung.

4. Ein Pilot-Audit gemeinsam mit OT-Security durchführen und daraus nachvollziehbare Korrekturmaßnahmen ableiten.

4.4.6.3. Prozesse & Organisation

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Bestehende QM-, Audit-, Abweichungs- und Verbesserungsprozesse sind der zentrale Hebel für die Integration von OT-Security.
2. Security-Kontrollen in bestehende Prozesslandkarten und Maßnahmenverfolgung einbetten, statt ein paralleles Kontrollsystem zu etablieren.

4.4.6.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Niedrig → Mittel

1. Das Delta liegt darin, Security-Feststellungen in klare, umsetzbare und überprüfbare Anforderungen für Fachbereiche zu übersetzen.
2. Moderations- und Berichtstraining für Auditfeststellungen, Risikobewertung und Korrekturmaßnahmen.
3. Ein Beispiel einer OT-Security-Abweichung in eine verständliche Maßnahmenbeschreibung mit Verantwortlichem, Frist und Wirksamkeitskriterium überführen.

4.4.7. Rollenprofil SHE

Das Prozess- und Organisationsverständnis ist hoch und bleibt hoch. OT-Technik bleibt niedrig; Security steigt von niedrig auf mittel und Kommunikation von niedrig auf mittel. Der Schwerpunkt liegt auf dem Verständnis der Wechselwirkungen zwischen Cybersecurity, Safety und Betriebsrisiken. SHE soll Security nicht technisch verantworten, aber sicherheitskritische Abhängigkeiten erkennen und in Risikobewertungen und Notfallplanung einbringen.

4.4.7.1. OT & Technik

Soll-Ist-Delta: Niedrig → Niedrig

1. Kein formales Delta. Ein begrenztes technisches Orientierungswissen ist dennoch nützlich, damit SHE relevante Verbindungen zwischen OT, Safety und sicheren Betriebszuständen erkennt.
2. Eine gemeinsame Anlagenbegehung oder Szenarioanalyse mit Anlagenverantwortlichen nutzen; technische Detailanalysen bleiben bei den zuständigen OT-Fachrollen.

4.4.7.2. Security

Soll-Ist-Delta: Niedrig → Mittel

1. Das Security-Verständnis muss auf die möglichen Auswirkungen auf Menschen, Umwelt und sichere Betriebszustände ausgerichtet werden.
2. Workshop „Konvergenz von Safety und Security“ zu cyber-physischen Risiken, kompromittierten Steuerungen und möglichen Auswirkungen auf Schutzfunktionen.
3. Training zu Risikoanalysemethoden für cyber-physische Systeme; ein Szenario mit OT-Security und Anlagenverantwortlichen gemeinsam analysieren.
4. Maßnahmen und Eskalationspunkte für Fälle definieren, in denen Cybersecurity-Ereignisse Safety- oder Umweltfolgen haben können.

4.4.7.3. Prozesse & Organisation

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Bestehende Risiko-, Audit-, Change- und Notfallprozesse nutzen, um Security- und Safety-Aspekte zusammenzuführen.
2. Verantwortlichkeiten und Übergabepunkte zwischen SHE, OT-Security und Anlagenbetrieb in vorhandenen Verfahren dokumentieren.

4.4.7.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Niedrig → Mittel

1. Das Delta liegt in der bereichsübergreifenden Vermittlung von Cyber-/Safety-Wechselwirkungen.
2. Gemeinsame Übungen und kurze Leitfäden zu Meldung, Eskalation und sicheren Betriebsentscheidungen entwickeln.
3. Üben, technische Befunde in verständliche Risiken für Personen, Umwelt und Betriebsabläufe zu übersetzen.

4.4.8. Rollenprofil CISO

Security, Prozesse und Kommunikation sind bereits hoch und sollen es bleiben. Das OT- und Technikverständnis ist niedrig und soll auf mittel steigen. Die Entwicklungsaufgabe besteht darin, OT-spezifische Randbedingungen zu verstehen, damit Governance und Entscheidungen nicht ausschließlich aus IT-Perspektive getroffen werden. Besonders relevant sind Verfügbarkeit, Safety, Legacy, Produktionsabhängigkeiten und die Grenzen kurzfristiger Änderungen.

4.4.8.1. OT & Technik

Soll-Ist-Delta: Niedrig → Mittel

1. Das einzige signifikante Kompetenzdelta liegt im grundlegenden Verständnis der Produktions- und Steuerungsebene. Ziel ist keine operative Technikexpertise, sondern die Beurteilung der Machbarkeit und Nebenwirkungen von Security-Strategien.
2. OT-Crashkurs bzw. „OT Security Fundamentals“ mit Anlagenarchitektur, industriellen Steuerungen, Legacy, Produktionsabhängigkeiten und dem hohen Stellenwert der Verfügbarkeit.
3. Begleitete Site Visits auf dem Shopfloor, um physische Anlagenrealität, Betriebsabläufe und Abhängigkeiten zu verstehen.
4. Regelmäßige Executive Briefings durch den Head OT Security zu neuen technischen Entwicklungen, Bedrohungen und Lessons Learned.
5. Als Lernnachweis die betrieblichen Folgen einer vorgeschlagenen Security-Maßnahme und mögliche Alternativen für das Management erläutern.

4.4.8.2. Security

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Die bestehende Security-Kompetenz erhalten und auf OT-spezifische Risiken und Betriebsbedingungen anwenden.

2. Mit Head OT Security sicherstellen, dass Risikoberichte OT-Auswirkungen und nicht nur klassische IT-Kennzahlen abbilden.

4.4.8.3. Prozesse & Organisation

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Governance, Risikomanagement und regulatorische Orientierung sind zu erhalten.
2. Entscheidungsrechte, Risikoakzeptanz und Eskalation für OT-Risiken klar definieren und in die Unternehmens-Governance integrieren.

4.4.8.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Die vorhandene Managementkommunikation nutzen, um OT-Risiken in Geschäftsauswirkungen, Handlungsoptionen und Restrisiken zu übersetzen.
2. Regelmäßige Abstimmung mit Head OT Security zu strategischen Prioritäten, Ressourcenbedarf und wesentlichen Abhängigkeiten.

4.4.9. Rollenprofil Head OT-Security

Laut Workshop besteht in allen vier Kompetenzfeldern kein ausgewiesenes Delta: Ist und Soll sind jeweils hoch. Die Entwicklungsaufgabe ist daher primär Erhalt und kontinuierliche Weiterentwicklung. Da die Rolle alle Kompetenzfelder integriert, sollte sie zugleich Wissensaufbau, Nachfolgefähigkeit und systematischen Kompetenztransfer in andere Rollen verantworten.

4.4.9.1. OT & Technik

Soll-Ist-Delta: Hoch → Hoch

1. Kein Delta. Die breite technische Kompetenz erhalten und aktuelle Anlagen- und Architekturentwicklungen verfolgen.
2. Site Visits, technische Peer-Reviews und Lessons Learned aus Projekten nutzen, um Referenzarchitekturen aktuell zu halten.

4.4.9.2. Security

Soll-Ist-Delta: Hoch → Hoch

1. Kein Delta. Laufende Weiterbildung zu neuen Bedrohungsszenarien und Trends, einschließlich KI-gestützter Detection, sowie zu Normen und technischen Schutzansätzen.
2. Erkenntnisse aus Incidents, Übungen und Assessments in Standards, Architekturprinzipien und die OT-Security-Roadmap zurückführen.

4.4.9.3. Prozesse & Organisation

Soll-Ist-Delta: Hoch → Hoch

1. Kein Delta. Governance, operative Umsetzung und organisationsübergreifende Projektsteuerung auf hohem Niveau halten.
2. Kompetenzmatrix und Lernpfade regelmäßig überprüfen; Fortschritt über Umsetzung, Übungsergebnisse und wirksame Risikoreduktion verfolgen.

4.4.9.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Hoch → Hoch

1. Kein Delta. Die Rolle sollte als fachlicher Multiplikator und Coach wirken.
2. Mentoring für OT Security Expert/Architect und OT Security Coordinator/Engineer anbieten; technische Risiken und Business-Entscheidungen in beide Richtungen übersetzen.

4.4.10. Rollenprofil BISO

OT-Technik und Kommunikation liegen bereits auf dem geforderten Niveau; Kommunikation soll hoch bleiben. Security und Prozesse/Organisation sind niedrig und sollen auf mittel steigen. Der BISO benötigt ein solides Verständnis von OT-Security-Risiken und den zugehörigen Governance- und Umsetzungsprozessen, um Business-Prioritäten mit zentralen Security-Anforderungen zu verbinden. Technische Detailkompetenz ist nicht das primäre Ziel.

4.4.10.1. OT & Technik

Soll-Ist-Delta: Mittel → Mittel

1. Kein formales Delta laut Matrix. Das vorhandene Grundverständnis sollte aber anhand der für den Geschäftsbereich relevanten Anlagen und Produktionsabhängigkeiten konkretisiert werden.
2. Bei Site Visits oder Anlagenreviews mitgehen, um Business-Auswirkungen technischer Risiken präziser beschreiben zu können.

4.4.10.2. Security

Soll-Ist-Delta: Niedrig → Mittel

1. Das Security-Wissen muss so weit vertieft werden, dass der BISO Risiken einordnen und geeignete Spezialisten einbinden kann.
2. Eine grundlegende Cybersecurity-Qualifizierung absolvieren, beispielsweise CISM oder ein vergleichbares Grundlagenprogramm, sofern Umfang und Zielgruppe passen.
3. OT-spezifische Risikobewertung und IEC-62443-Grundlagen ergänzen; an Fallbeispielen Anforderungen und Maßnahmen für den Geschäftsbereich priorisieren.

4.4.10.3. Prozesse & Organisation

Soll-Ist-Delta: Niedrig → Mittel

1. Das Delta betrifft die Integration von Security-Anforderungen in bestehende Geschäfts- und Produktionsprozesse.
2. Workshop zu OT-spezifischem Prozessmanagement und Qualitätsmanagement durchführen.
3. Governance, Verantwortlichkeiten, Risikoakzeptanz und Maßnahmenverfolgung an einem bereichsbezogenen OT-Risikoregister üben.
4. Mit Head OT Security einen realen Prozess auswählen und konkrete Security-Kontrollen, Verantwortliche, Fristen und Eskalationswege eintragen.

4.4.10.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Hoch → Hoch

1. Kein Aufbau-Gap. Die hohe Kommunikationskompetenz ist der zentrale Hebel der Rolle.

2. Ein Management-Briefing erstellen, das technische Risiken in Business-Auswirkungen, Optionen, Kosten-/Nutzen-Abwägung und Entscheidungsbedarf übersetzt.

4.4.11. Rollenprofil OT-Security Expert / Architect

OT-Technik und Security sind hoch und bleiben hoch. Prozesse und Organisation sind niedrig und sollen auf mittel, Kommunikation mittel und soll hoch steigen. Der zentrale Entwicklungsbedarf besteht darin, technische Expertise stärker in Governance, Lifecycle-, Projekt- und Änderungsprozesse einzubetten und Architekturentscheidungen überzeugend gegenüber Betrieb, Engineering, Management und Lieferanten zu vermitteln.

4.4.11.1. OT & Technik

Soll-Ist-Delta: Hoch → Hoch

1. Kein Delta. Technische Expertise zu OT-Systemen, Netzwerkarchitektur und industriellen Randbedingungen erhalten und weiterentwickeln.
2. Referenzarchitekturen, technische Standards und Erkenntnisse aus Assessments und Projekten laufend aktualisieren.

4.4.11.2. Security

Soll-Ist-Delta: Hoch → Hoch

1. Kein Delta. Fachliche Tiefe in Architektur, IEC 62443, Threat Modelling, Segmentierung, Hardening, Detection und Monitoring erhalten.
2. Neue Schutzansätze und Lessons Learned in Architekturprinzipien und technische Abnahmekriterien überführen.

4.4.11.3. Prozesse & Organisation

Soll-Ist-Delta: Niedrig → Mittel

1. Ein zentrales Delta liegt darin, technische Architekturentscheidungen besser in Projekt-, Qualitäts- und Veränderungsprozesse einzubetten.
2. Grundlagenkurs in Projektmanagement und Veränderungsmanagement; interne Governance-, Qualitätsmanagement- und Change-Prozesse kennenlernen.
3. Ein Architekturvorhaben vom Assessment über Risiko- und Maßnahmenplanung bis zur Implementierung und Betriebsübergabe begleiten.
4. Gemeinsam mit Projektleitung und Betrieb Verantwortlichkeiten, Freigaben, Abhängigkeiten und Restrisiken dokumentieren.

4.4.11.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Mittel → Hoch

1. Die vorhandene Kommunikationsfähigkeit muss zur adressatengerechten Vermittlung komplexer Konzepte und zur Herbeiführung von Entscheidungen ausgebaut werden.
2. Coaching zu Präsentation und „Technical to Executive Communication“: dieselbe Architekturentscheidung für Technikteams, Betrieb und Management unterschiedlich aufbereiten.
3. Architektur-Reviews moderieren, Zielkonflikte zwischen Verfügbarkeit, Risiko und Aufwand erläutern und Alternativen nachvollziehbar begründen.

4. Feedback zu mindestens einer Präsentation oder einem Review durch Stakeholder aus Technik und Management einholen.

4.4.12. Rollenprofil OT-Security Coordinator / Engineer

OT-Technik und Security sind mittel und sollen beide hoch werden. Prozesse und Organisation sind niedrig und sollen mittel erreichen; Kommunikation bleibt mittel. Damit ist die Rolle ein zentraler operativer Entwicklungspfad: Sie braucht sowohl technische Vertiefung als auch die Fähigkeit, Maßnahmen strukturiert durch den Betrieb zu bringen. Anders als beim Architect liegt der Schwerpunkt stärker auf Umsetzung, Koordination und Nachverfolgung.

4.4.12.1. OT & Technik

Soll-Ist-Delta: Mittel → Hoch

1. Großes Entwicklungsfeld: von einem mittleren Verständnis zu einer fundierten, praktisch anwendbaren technischen Kompetenz.
2. Hands-on-Trainings zu OT-Architekturen, industriellen Protokollen, Anlagenabhängigkeiten, Segmentierung und sicherer Fernwartung durchführen.
3. Zeitweise Job-Shadowing beim OT Security Expert/Architect, um Architekturentscheidungen, technische Reviews und die Übertragung von Anforderungen in die Umsetzung nachzuvollziehen.
4. Ein abgegrenztes Arbeitspaket an einer freigegebenen Testumgebung oder Pilotanlage bearbeiten und durch eine erfahrene Fachrolle reviewen lassen.

4.4.12.2. Security

Soll-Ist-Delta: Mittel → Hoch

1. Die operative Anwendung von Security-Methoden und Tools muss vertieft werden, damit Maßnahmen selbstständig vorbereitet, umgesetzt und überprüft werden können.
2. Intensive Hands-on-Qualifizierung zu OT-Security-Tools und Frameworks, einschließlich IEC 62443; Schwerpunkt auf Asset-Erfassung, Hardening, Schwachstellen, Monitoring und Incident Response.
3. Ein Security-Arbeitspaket von der Risikoanalyse bis zum Maßnahmenplan bearbeiten; Abnahmekriterien und mögliche Auswirkungen auf den Produktionsbetrieb dokumentieren.
4. Incident- und Wiederherstellungsübungen mit OT-Security, Instandhaltung und Produktion durchführen.

4.4.12.3. Prozesse & Organisation

Soll-Ist-Delta: Niedrig → Mittel

1. Deutliches Delta bei der organisatorischen Einbettung: Maßnahmen müssen planbar, nachvollziehbar und über Schnittstellen hinweg steuerbar werden.
2. Prozess-Training zu interner Governance, Qualitätsmanagement, Change-Management, Freigaben, Dokumentation und Eskalationswegen.
3. Ein Maßnahmenpaket vom Befund bis zum Abschluss steuern und Verantwortliche, Fristen, Abhängigkeiten, Risiken und Wirksamkeitsnachweis dokumentieren.

4. Mit dem Head OT Security klären, welche Entscheidungen selbst getroffen werden dürfen und wann Architektur-, Betriebs- oder Managementfreigaben erforderlich sind.

4.4.12.4. Kommunikation & Übersetzung

Soll-Ist-Delta: Mittel → Mittel

1. Kein ausgewiesenes Delta laut Matrix. Kommunikation ist dennoch für die operative Koordination entscheidend.
2. Regelmäßige Statusmeldungen mit Befund, Risiko, Betriebswirkung, nächstem Schritt und benötigter Entscheidung trainieren.
3. Bei Job-Shadowing und Übungen Feedback von Technikern vor Ort, OT Security Expert und Anlagenbetrieb zur Verständlichkeit und Verlässlichkeit der Kommunikation einholen.

5. Diskussion, Handlungsempfehlungen und Grenzen

Die Ergebnisse verdeutlichen, dass OT-Security-Kompetenz als organisationsweite Fähigkeit verstanden werden muss. Die zwölf Rollenprofile zeigen unterschiedliche fachliche Schwerpunkte, zugleich aber auch eine ausgeprägte Abhängigkeit von funktionierenden Schnittstellen zwischen Produktion, Engineering, Instandhaltung, IT, Security und Management. Die nachfolgenden Empfehlungen führen diese Befunde zusammen und formulieren Ansatzpunkte für die organisatorische Verankerung eines nachhaltigen Kompetenzaufbaus.

5.1. Empfehlungen

5.1.1. Zwei komplementäre Entwicklungspfade etablieren

Pfad A führt aus der betrieblichen Praxis in Security-Rollen: vorhandenes Anlagen- und Produktionsverständnis bewahren und Security-Methodik, Risikoanalyse, IEC 62443, Meldewege und Incident-Praxis ergänzen. Pfad B führt aus IT-Security, Informatik oder Engineering stärker in OT: OT-/Anlagenverständnis, Legacy, Verfügbarkeit, Safety und Shopfloor-Praxis systematisch aufbauen.

5.1.2. Rollenbezogene Lernpfade statt Einheitscurriculum

Alle Rollen erhalten ein gemeinsames OT-Security-Grundverständnis; Vertiefungen richten sich nach dem Soll-Profil. Coordinator/Engineer und Produktions-IT benötigen praktische technische Übungen; CISO und BISO stärker Risiko-, Governance- und Entscheidungsfälle; QM und SHE die Integration in bestehende Management- und Risikoprozesse.

Die Lernpfade sollten außerdem eine rollenbezogene regulatorische Grundqualifizierung enthalten. CISO und Head OT Security benötigen insbesondere Kenntnisse zur Anwendbarkeit und Umsetzung des BSIG/NIS-2 einschließlich Risikomanagement und Meldeprozessen. Engineering und Automatisierung sollten die maschinenrechtlichen Anforderungen und deren zeitliche Anwendung einordnen können. Instandhaltung, Anlagenbetrieb und SHE benötigen ein gemeinsames Verständnis der Schnittstellen zu Gefährdungsbeurteilung, Betriebssicherheit und – sofern einschlägig – Störfallprävention und Gefahrenabwehr.

5.1.3. Lernen am realen Betrieb ausrichten

Anlagenbegehungen, Fallstudien, sichere Testumgebungen, begleitete Assessments, Design Reviews und Incident-Übungen verbinden Theorie mit der industriellen Realität. Maßnahmen müssen Verfügbarkeit und Safety berücksichtigen und dürfen produktive Systeme nicht unkontrolliert gefährden.

5.1.4. Kompetenznachweise definieren

Jede Qualifizierungsmaßnahme sollte ein erwartetes Verhalten und einen Nachweis benennen: z. B. eine OT-Risikoanalyse erstellen, eine Abweichung korrekt eskalieren, Security-Anforderungen in einen Change integrieren oder eine Managemententscheidung verständlich vorbereiten.

Als Kompetenznachweise eignen sich beispielsweise eine begründete NIS-2-Betroffenheits- und OT-Scope-Einordnung, die Bewertung eines Cybereignisses im Rahmen einer Gefährdungsbeurteilung, ein Security-/Safety-Review einer Maschinenänderung oder eine Übung zur Bewertung cyberbedingter

Störfallszenarien. Die Nachweise sollten jeweils mit den zuständigen Rechts-, Arbeitsschutz-, Safety- und Betriebsfunktionen abgestimmt werden.

5.1.5. Verantwortung und Zeitbudget sichern

Führungskräfte sollten Lernzeit, Praxisgelegenheiten und Mentoring verbindlich einplanen. Ohne konkrete Aufgaben im Arbeitsalltag bleiben Schulungen häufig deklaratives Wissen und schließen das Kompetenzdelta nicht zuverlässig.

5.1.6. Matrix regelmäßig aktualisieren

Das Mapping sollte mindestens jährlich sowie nach größeren Anlagen-, Organisations- oder Bedrohungsänderungen überprüft werden. Bewertungen sollten durch Beispiele belegt und von Führungskraft, Rolleninhaber und OT-Security-Fachvertretung gemeinsam kalibriert werden.

5.2. Grenzen, Annahmen und Übertragbarkeit

Die Aussagekraft des Modells ist im Lichte seiner Datengrundlage und seines Entwicklungszwecks zu beurteilen. Die folgenden Einschränkungen markieren, welche Schlussfolgerungen aus den Workshops gezogen werden können und an welchen Stellen eine organisationsspezifische Validierung erforderlich bleibt.

Die Stellenbeschreibungen sind typische, aus den Workshop-Kompetenzen abgeleitete Vorschläge und keine Analyse bestehender Stellenprofile. Sie sollten vor Verwendung mit tatsächlichen Aufgaben, Entscheidungsbefugnissen, Standortanforderungen und vorhandenen Organisationsstrukturen abgeglichen werden.

Die Workshop-Matrix enthält für Engineering sowie Automatisierung/Digitalisierung unterschiedliche Ist-/Soll-Ausprägungen; diese wurden unverändert übernommen. Die Formulierungen der Bloom-orientierten Niveaus konkretisieren die vier Stufen für die Rollen, ersetzen aber keine organisationsweit abgestimmten Bewertungsanker.

5.3. Weitere Schritte

Das Kompetenzmodell leistet einen Beitrag, indem es normative und fachliche OT-Security-Anforderungen in eine handlungsorientierte Beschreibung betrieblicher Rollen übersetzt. Sein Mehrwert liegt weniger in einer neuen Definition technischer Sicherheitsanforderungen als in der systematischen Verbindung von Kompetenzfeldern, Rollenverantwortung und Entwicklungswegen. Die Ergebnisse sprechen dafür, gemeinsame Grundlagenqualifizierungen mit rollenspezifischen Lernpfaden zu kombinieren und Lernen eng an reale Anlagen, Prozesse und Entscheidungsfälle zu koppeln.

Für die weitere Entwicklung bieten sich drei Schritte an: Erstens sollten die Rollenprofile in ausgewählten Unternehmen mit den tatsächlichen Aufgaben- und Verantwortungszuschnitten abgeglichen werden. Zweitens sollten die beschriebenen Kompetenzniveaus durch konkrete Beobachtungsanker, Arbeitsproben und geeignete Nachweisformen operationalisiert und pilotiert werden. Drittens sollte das Mapping in regelmäßigen Abständen sowie bei wesentlichen Änderungen der Anlagenlandschaft, Bedrohungslage oder Organisationsstruktur überprüft werden. Auf diese Weise kann aus der workshopbasierten Ausgangsversion schrittweise ein belastbares, organisationsspezifisch anwendbares Instrument der Personal- und Organisationsentwicklung werden.

6. Literaturverzeichnis

[1] Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S.; Hahn, A.; Saravia, S.; Sherule, A.; Thompson, M. (2023): Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

[1a] Stouffer, K. et al. (2026): Guide to Operational Technology (OT) Security – NIST SP 800-82 Rev. 4, Initial Public Draft. National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-82r4.ipd

[2] International Electrotechnical Commission (IEC) (2018 ff.): IEC 62443 – Security for industrial automation and control systems. Normenreihe, insbesondere IEC 62443-2-1, IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1 und IEC 62443-4-2. https://www.iec.ch/

[3] International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) (2022): ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Genf: ISO.

[4] National Institute of Standards and Technology (NIST) (2024): The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024): ICS-Security-Kompendium. Bonn: BSI. https://www.bsi.bund.de/

[6] Anderson, L. W.; Krathwohl, D. R. (Hrsg.) (2001): A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. New York: Longman.

[7] I2M-Workshop „Aufbau von OT Security Kompetenzen" (03. Juli 2026 und 25. September 2026): Workshop-Präsentationen und Rollen-Kompetenz-Mapping. Unveröffentlichte Arbeitsunterlagen; interne Primärquelle der in diesem Bericht ausgewerteten Ergebnisse.

[8] Chowdhury, N.; Gkioulos, V. (2021): Key competencies for critical infrastructure cyber-security: a systematic literature review. Information and Computer Security, 29(5), S. 697–723. DOI: https://doi.org/10.1108/ICS-07-2020-0121

[9] Ani, U. D.; He, H.; Tiwari, A. (2019): Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), S. 2–35. DOI: https://doi.org/10.1108/JSIT-02-2018-0028

[10] Ramezan, C. A.; Coffy, P. M.; Lemons, J. (2024): Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for? Journal of Cybersecurity Education, Research and Practice, 2024(1), Article 6. DOI: https://doi.org/10.32727/8.2023.31

[11] Petersen, R.; Santos, D.; Wetzel, K.; Smith, M.; Witte, G. (2020): Workforce Framework for Cybersecurity (NICE Framework). NIST Special Publication 800-181 Rev. 1. National Institute of Standards and Technology. DOI: https://doi.org/10.6028/NIST.SP.800-181r1

[12] Bundesrepublik Deutschland (2025): Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2. Dezember 2025, BGBl. 2025 I Nr. 301; BSI-Gesetz in der jeweils geltenden Fassung.

[13] Bundesrepublik Deutschland: Arbeitsschutzgesetz (ArbSchG), insbesondere §§ 3 und 5; Betriebssicherheitsverordnung (BetrSichV), insbesondere §§ 3, 4, 10 bis 12, jeweils in der geltenden Fassung.

[14] Europäisches Parlament und Rat (2023): Verordnung (EU) 2023/1230 über Maschinen. Amtsblatt der Europäischen Union L 165 vom 29.6.2023. https://eur-lex.europa.eu/eli/reg/2023/1230/oj

[15] Bundesrepublik Deutschland: Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung – 12. BImSchV), insbesondere §§ 3 bis 5, 8 bis 10 und Anhang III, in der geltenden Fassung.

Die Literatur dient der fachlichen Kontextualisierung des Kompetenzmodells. Die konkreten Ist-/Soll-Einstufungen, Rollenbeschreibungen und Entwicklungsprioritäten stammen aus den I2M-Workshops und den dazugehörigen Arbeitsunterlagen [7]. Normen sind urheberrechtlich geschützt; die Nennung ersetzt nicht die Beschaffung und Prüfung der jeweils aktuellen Originalausgabe.