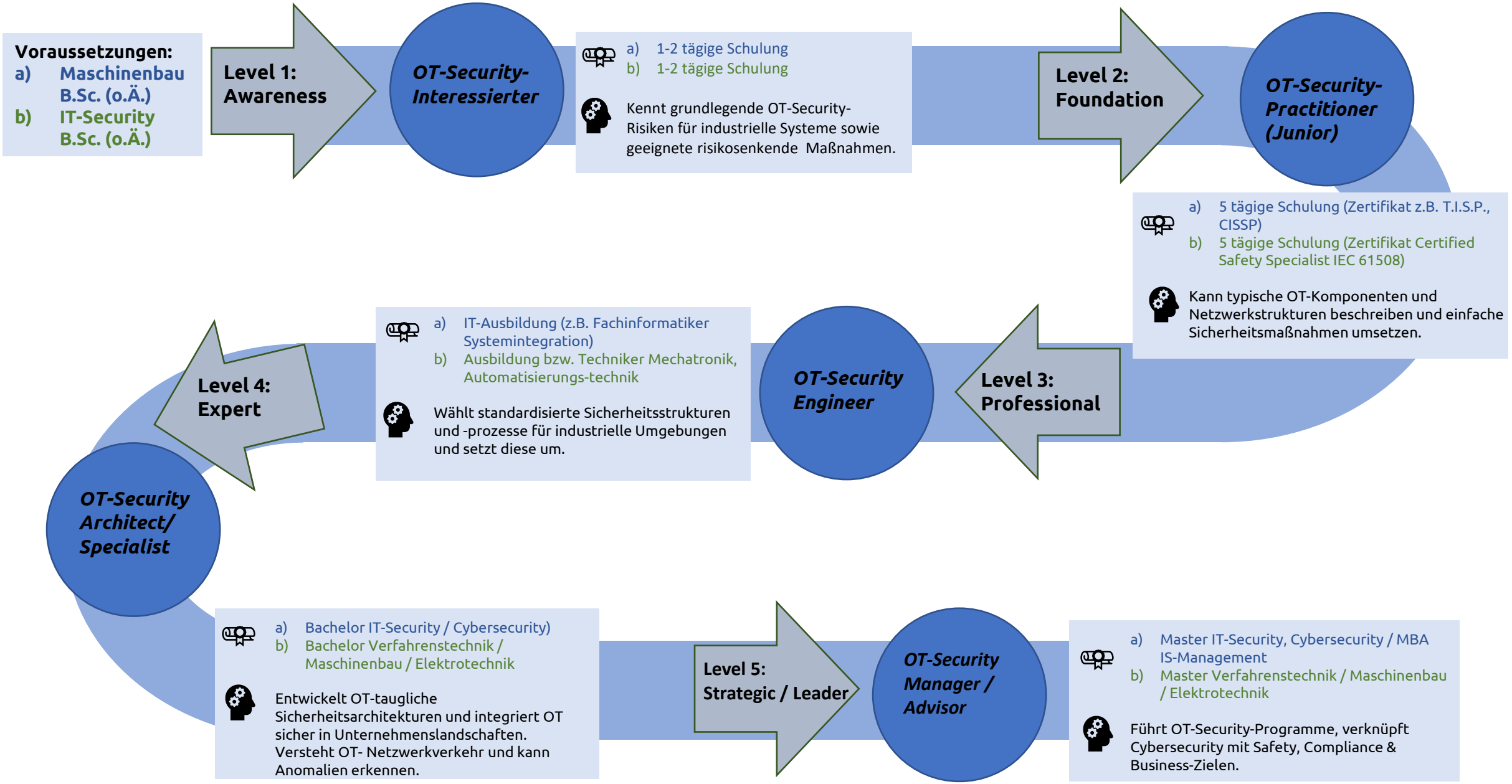
Voraussetzungen:
a) Maschinenbau B.Sc. (o.Ä.)
b) IT-Security B.Sc. (o.Ä.)
Level 1: Awareness
OT-Security-Interessierter
a) 1-2 tägige Schulung
b) 1-2 tägige Schulung
Kennt grundlegende OT-Security-Risiken für industrielle Systeme sowie geeignete risikosenkende Maßnahmen.
Level 2: Foundation
OT-Security-Practitioner (Junior)
a) 5 tägige Schulung (Zertifikat z.B. T.I.S.P., CISSP)
b) 5 tägige Schulung (Zertifikat Certified Safety Specialist IEC 61508)
Kann typische OT-Komponenten und Netzwerkstrukturen beschreiben und einfache Sicherheitsmaßnahmen umsetzen.
Level 3: Professional
OT-Security Engineer
a) IT-Ausbildung (z.B. Fachinformatiker Systemintegration)
b) Ausbildung bzw. Techniker Mechatronik, Automatisierungs-technik
Wählt standardisierte Sicherheitsstrukturen und -prozesse für industrielle Umgebungen und setzt diese um.
Level 4: Expert
OT-Security Architect/ Specialist
a) Bachelor IT-Security / Cybersecurity)
b) Bachelor Verfahrenstechnik / Maschinenbau / Elektrotechnik
Entwickelt OT-taugliche Sicherheitsarchitekturen und integriert OT sicher in Unternehmenslandschaften. Versteht OT- Netzwerkverkehr und kann Anomalien erkennen.
Level 5: Strategic / Leader
OT-Security Manager / Advisor
a) Master IT-Security, Cybersecurity / MBA IS-Management
b) Master Verfahrenstechnik / Maschinenbau / Elektrotechnik
Führt OT-Security-Programme, verknüpft Cybersecurity mit Safety, Compliance & Business-Zielen.

	Anforderungsprofil			Voraussetzung: Bachelor Maschinenbau o.ä.		Voraussetzung: Bachelor IT-Security o.ä.	
Kompetenz-stufe	**Bezeichnung**	**Kompetenzen**	**Erforderliches Wissen**	**Geforderte IT-Kompetenzen**	**Qualifizierungs-maßnahme im IT-Security-Bereich**	**Geforderte OT-Kompetenzen**	**Qualifizerungs-maßnahme im Bereich OT / Maschinenbau / Verfahrenstechnik**
Level 1 – Awareness	*OT-Security-Interessierter*	Kennt grundlegende OT-Security-Risiken für industrielle Systeme sowie geeignete risikosenkende Maßnahmen.	• Grundlagen Automatisierung • Basiswissen Cybersecurity • Verständnis für Safety vs. Security • Lifecycle automatisierter Anlagen	• Grundlagen der IT-Security (CIA-Trias, Authentifizierung, Netzwerksicherheit) • Grundverständnis digitaler Kommunikation (TCP/IP, Protokolle) • Basiswissen zu Cyberrisiken und Angriffsmethoden	1-2 tägige Schulung	• Grundverständnis industrieller Prozesse (Produktion, Qualität, Materiallogistik, Wartung für Prozess, Fertigung, Energie) • Aufbau von Steuerungs- und Automatisierungssystemen • Safety-Konzepte (Funktionale Sicherheit)	1-2 tägige Schulung
Level 2 – Foundation	*OT-Security-Praktiker (Junior)*	Kann typische OT-Komponenten und Netzwerkstrukturen beschreiben und einfache Sicherheitsmaßnahmen umsetzen.	• Netzwerkgrundlagen • OT-Protokolle (Profibus, Profinet) • Firewalls, Segmentierung • Einführung IEC 62443	• IT-Netzwerkgrundlagen (Routing, VLANs, Firewallkonzepte) • Basiskenntnisse Kryptografie und Identitätsmanagement • Grundlagen der Netzwerksicherheit (IDS/IPS, VPN)	Zertifikat (5 Tage), z.B. T.I.S.P, CISSP	• OT-Komponenten (Sensoren, Aktoren, PLC, SCADA, DCS) verstehen • Industrielle Kommunikation (Feldbus, OPC UA) • Prozess- und Anlagensicherheit (Safety-Standards wie IEC 61508)	Zertifikat (5 Tage), z.B. Certified Safety Specialist IEC 61508
Level 3 – Professional	*OT-Security Engineer*	Wählt standardisierte Sicherheitsstrukturen und -prozesse für industrielle Umgebungen und setzt diese um.	• Purdue-Modell, Zonen/Konduiten • Risikoanalyse nach IEC 62443-3-2 • Monitoring & Incident Response • Patch- & Asset-Management	• Anwendung von Security-Frameworks (ISO 27001, NIST) • Netzwerkarchitekturen beschreiben • Security-Monitoring, Logging und SIEM-Grundlagen • Skriptsprachen für Automatisierung (z. B. Python, PowerShell)	IT-Ausbildung (z.B. Fachinformatiker Systemintegration)	• Anwendung von Automatisierungsarchitekturen (Purdue-Modell) • Sicherheitssysteme • Grundlagen der Prozessleittechnik • OT-Risikobewertung • Programmieren in Funktionsplantechnik	Ausbildung bzw. Techniker Mechatronik, Automatisierungs-technik
Level 4 – Expert	*OT-Security Architect / Specialist*	Entwickelt OT-taugliche Sicherheitsarchitekturen und integriert OT sicher in Unternehmenslandschaften. Versteht OT-Netzwerkverkehr und kann Anomalien erkennen.	• Defense-in-Depth-Konzepte • OT-SOC-Design & Forensik • Secure Remote Access • Normen: IEC 62443, ISO 27019, NIST 800-82	• IT-Architekturdesign & Enterprise Security Architektur • Threat Modeling, Forensik und Incident Response • Cloud-/Edge-Security und hybride Infrastrukturen • Identitäts- und Zugriffsmanagement (IAM, PKI)	Bachelor IT-Security / Cybersecurity	• Komplexe Automatisierungsnetzwerke entwerfen • Integration von OT in IT- und Cloud-Systeme • OT-spezifische Forensik und Protokollanalyse • Kenntnis industrieller Kommunikationsstandards und Sicherheitszonen	Bachelor Verfahrenstechnik / Maschinenbau / Elektrotechnik
Level 5 – Strategic / Leader	*OT-Security Manager / Advisor*	Führt OT-Security-Programme, verknüpft Cybersecurity mit Safety, Compliance & Business-Zielen.	• Governance, Risk, Compliance (GRC) • KRITIS/NIS2-Konformität • OT-Sicherheitsstrategie & Schulung • Lieferkettensicherheit & Policy-Design • IEC62443-2-1	• Strategisches IT-Risikomanagement (GRC, ISMS) • Regulatorische Anforderungen (NIS2, BSI-Gesetz) • Unternehmensweite Security-Governance und Audits • Kommunikation mit Management & Behörden	Master IT-Security, Cybersecurity / MBA IS-Management	• Verständnis von Produktionsmanagement & -logistik • Verständnis Anlagen-Lifecycle • Kosten-Nutzen-Bewertung von Sicherheitsmaßnahmen • Change-Management in industriellen Prozessen • Compliance und Safety-Integration im Betrieb	Master Verfahrenstechnik / Maschinenbau / Elektrotechnik