T.I.S.P./T.P.S.S.E. Community Meeting 2026

Berlin, 10. - 11.11.2026

OT-Security in der pharmazeutischen Industrie

Stephan Weller, Wacker Biotech GmbH


für die Pharma-Produktion
Qualifizierung von OT-Infrastrukturen unter Berücksichtigung von IEC 62443, GAMP 5 und NIS2
SICHER | COMPLIANT | ZUKUNFTSFÄHIG
01
Steigende Cyber-Bedrohung
Jede digitale Schnittstelle erhöht die Effizienz – und gleichzeitig die Angriffsfläche.
02
Manipulierte Prozessparameter, Chargenverlust
Veränderte GMP-Daten, fehlerhafte Batch Records
Unternehmensrisiko
Bußgelder, Reputationsschäden, Haftungsrisiken
Anlagenverfügbarkeit
Produktionsstillstand, Lieferengpässe
03
wie spezifiziert?
Und:
Ist es gegen Cyberbedrohungen geschützt?
Neue Anforderungen an die Qualifizierung
Security-by-Design
Sicherheit von Anfang an
Security-by-Default
Sichere Standardkonfiguration
Security-by-Lifecycle
Sicherheit über den gesamten Lebenszyklus
04
05 Die wichtigsten OT-Security-Maßnahmen
Mehrschichtiger Schutz für eine resiliente Produktion
Netzwerksegmentierung
Trennung von IT und OT, Firewalls, DMZs
Zugriffskontrolle
Rollen, Least Privilege, MFA
System Hardening
Sichere Konfiguration, unnötige Dienste deaktivieren
Vulnerability- & Patch-Management
Schwachstellen identifizieren, Updates kontrolliert einspielen
Monitoring & Logging
Erkennung ungewöhnlicher Aktivitäten, Audit Trails
Backup & Disaster Recovery
Regelmäßige Backups, Restore-Tests, Notfallpläne
DEFENSE IN DEPTH
Mehr Sicherheit.
Mehr Verfügbarkeit.
Mehr Vertrauen.
05
06 IEC 62443: Der Standard für OT-Security
Ein strukturierter Ansatz für industrielle Cybersicherheit
IEC 62443
Risk Assessment
Risiken verstehen
Zones & Conduits
Netzwerke strukturieren
Security Levels
Schutzniveau definieren
Defense in Depth
Mehrschichtiger Schutz
Lifecycle Management
Sicherheit über den gesamten Lebenszyklus
Risikobasiert. Praxisnah. International anerkannt.
06
07 Zonenmodell nach IEC 62443
Segmentierung als zentrale Schutzmaßnahme
Unternehmens-IT
Office-Netzwerk
Zone IT / Enterprise
DMZ
z. B. Historian, Patch-Server, Jump-Server
Zone DMZ
Produktionsnetzwerk (OT)
SCADA, MES, Engineering
Zone OT / Operations
Produktionszelle 1
SPS, HMI, Sensoren, Aktoren
Produktionszelle 2
SPS, HMI, Sensoren, Aktoren
Laborumgebung
LIMS, Laborgeräte, Workstations
Zone Control
07
08 OT-Security in der Qualifizierung
Sicherheit über den gesamten Lebenszyklus
DQ
Security by Design
Sicherheitsanforderungen, Zonenkonzepte, Risikoanalyse
IQ
Sichere Installation
System-Härtung, Netzwerkkonfiguration, Berechtigungen
OQ
Sicherheitsfunktionen testen
Zugriffe, Alarme, Logging, Backups
PQ
Sicherer Betrieb nachweisen
Leistung, Resilienz, Notfallszenarien
Cybersecurity wird zum prüfbaren und dokumentierten Bestandteil der Qualifizierung.
08
09 Regulatorische Anforderungen im Zusammenspiel
Ein integrierter Ansatz für Compliance und Sicherheit
GMP
EU-GMP
Annex 11
Annex 15
CSV
GAMP 5
Security
IEC 62443
ISO 27001
Regulierung
NIS2
BSI-Gesetz
KRITIS
Gemeinsames Ziel: Sichere, konforme und resiliente Produktionsanlagen.
09
10 Management-Verantwortung
OT-Security ist Chefsache
Strategie
Sicherheitsstrategie verabschieden und Ressourcen bereitstellen
Compliance
Regulatorische Anforderungen erfüllen und überwachen
Risiko
Cyberrisiken bewerten und aktiv steuern
Resilienz
Sicherheitskultur fördern und Business Continuity gewährleisten
Die Geschäftsleitung trägt Verantwortung für das Risikomanagement und die Wirksamkeit der Sicherheitsmaßnahmen. (NIS2)
10
11 Zielbild der cyberresilienten Pharma-Produktion
Sicher. Compliant. Zukunftsfähig.
Qualifizierte Systeme
Sichere OT-Netzwerke
Kontrollierte Zugriffe
Erhöhte Cyberresilienz
Nachweisbare Compliance
Schutz von Patienten und Produkten
Sichere Produktion. Gesunde Menschen.
Heute sicher. Morgen verfügbar. Für eine gesündere Welt.
11
12 Fazit
Die zentrale Botschaft
Die Frage ist nicht mehr, ob ein System qualifikiert ist.
Die entscheidende Frage lautet:
Ist das qualifizierte System auch sicher?
IEC 62443
+ GMP + NIS2 =
Cyber Resiliente Produktion
Sichere OT-Infrastrukturen schützen nicht nur Systeme.
Sie schützen die Produktqualität, die Lieferfähigkeit und letztlich den Patienten.
12

Ich stelle mich kurz vor

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Head of PNS (Processes, Networks and Systems)

- **Berufliche Stationen**
  - Schering Deutschland GmbH (Systemadministrator, Anwendungs- und Anwenderbetreuung)
  - Bayer Vital GmbH (IT-Security und Datenschutz, Change-Management, Projektmanagement)
  - Steigerwald Arzneimittelwerk GmbH – Bayer Consumer Health (Head of IT)
  - Bayer AG Supply Center Leverkusen (Manufacturing Information Security Manager)
  - Schwarz Produktion (OT Information Security Manager)
  - Wacker Biotech GmbH (Infrastructure, OT-Security, GmP)



Ich stelle mich kurz vor

- **Head of PNS (Processes, Networks and Systems)**
- **Qualifikationen und Ausbildung**
  - B.Sc. IT-Management und Informatik (aktuell) und Wirtschaftsinformatik
  - GmP IT-Infrastruktur und Virtualisierung
  - Informationssicherheitsbeauftragter
  - Datenschutzbeauftragter (TüV-Zertifizierung)
  - Cyber Security Practitioner (ISACA/BSI (Information System Audit and Control Association / Bundesamt für Sicherheit in der Informationstechnik)
  - T.I.S.P. Teletrust Information Security Professional
  - COBIT Practitioner
  - IT-Notfallmanagement (Business Continuity Management (TüV-Zertifiziert), Incident Responce Management, Desaster Recorver)
  - ISO 27001 (Standard für IT-Security Management) und BSI-Grundschutz (Leadauditor)



Agenda

- Was ist GxP (GmP)
- Die neue Bedrohungslage in der OT
- Die Pharmaindustrie als kritische Infrastruktur
- IT versus OT
- Cyber-Risiken in vernetzten Produktionsanlagen
- Defence in Depth
- NIS2 im Kontext von IEC 62443, ISO 27001 und GAMP5
- Fazit

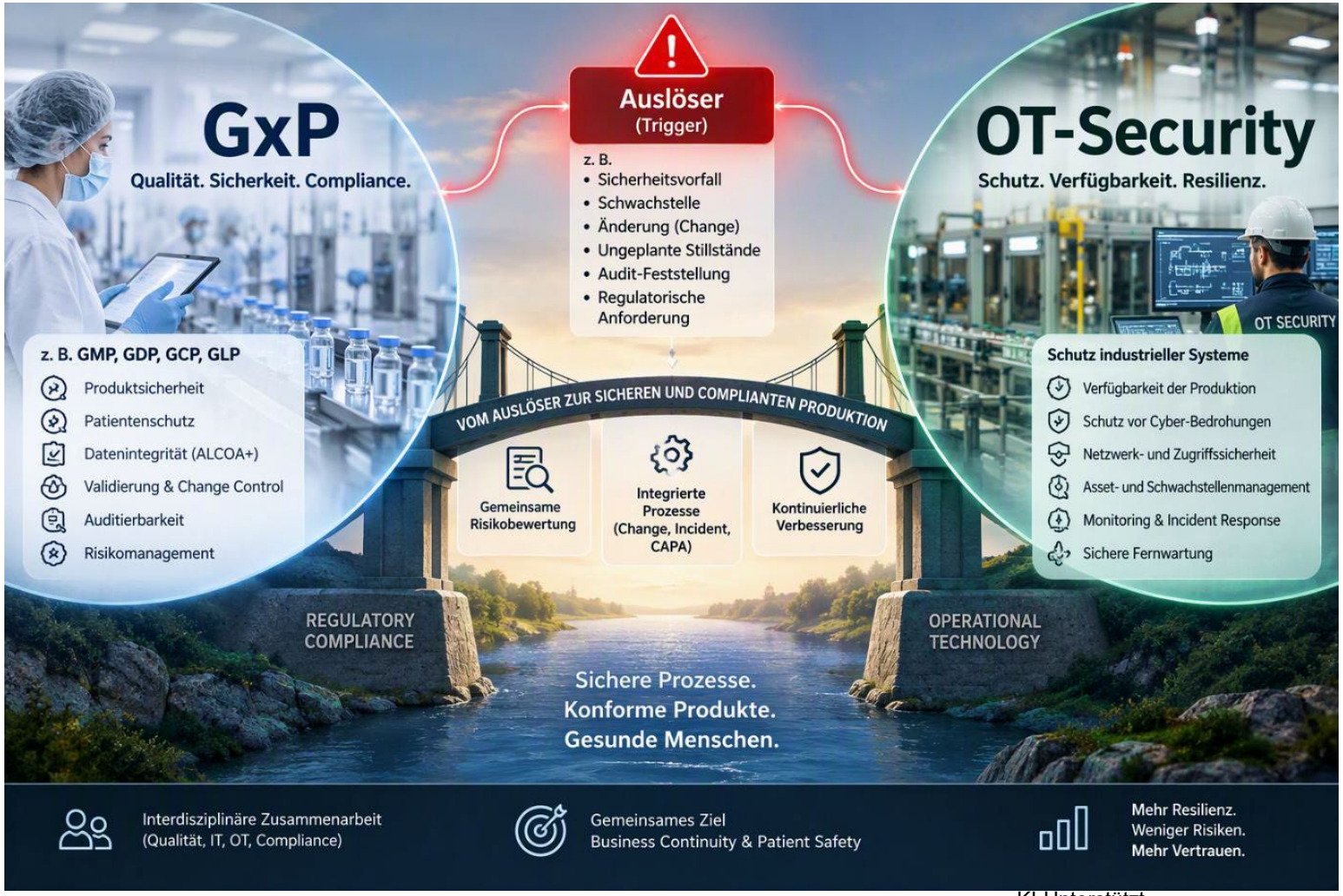


Was ist GmP



KI-Unterstützt

Was ist GmP



KI-Unterstützt

Die neue Bedrohungslage in der OT

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Die neue Bedrohungslage in der OT



KI-Unterstützt

Die Pharmaindustrie als kritische Infrastruktur

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



KI-Unterstützt

IT versus OT

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Kriterium	IT (Information Technology)	OT (Operational Technology)
Zweck	Verarbeitung von Informationen	Steuerung physischer Prozesse
Hauptziel	Vertraulichkeit & Integrität	Verfügbarkeit & Safety
Auswirkungen eines Angriffs	Datenverlust, Datenschutz	Produktionsausfall, Sach- oder Personenschäden
Lebenszyklen	Kurz (3–5 Jahre)	Lang (10–30 Jahre)
Patch-Fähigkeit	Regelmäßig möglich	Stark eingeschränkt
Echtzeit	Meist irrelevant	Kritisch
Beispiele	Server, PCs, Cloud, ERP	SPS, SCADA, DCS, Sensoren
Normen	ISO 27001	IEC 62443

IT versus OT

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Was gehört zur OT (IEC-62443-konform)?

Operational Technology (OT) umfasst gemäß IEC 62443 alle Systeme, Komponenten und Netzwerke, die zur Überwachung, Steuerung oder Automatisierung physischer Prozesse eingesetzt werden.

Level 4: Produktions-IT

MES	Reporting	LIMS	ERP-Schnittstellen

Level 3.5: OT-DMZ

Jump Server	OPC-UA Proxy	Remote Access Gateway	Patch- und AV-Server	Historian-Replikation

Level 3: Betriebs- und Produktionssysteme

Historian	Engineering Workstations	Batch-Systeme	Alarm-Management	Asset-Management

Level 2: Prozessführung

HMI-Systeme	SCADA-Systeme	Operator Workstations

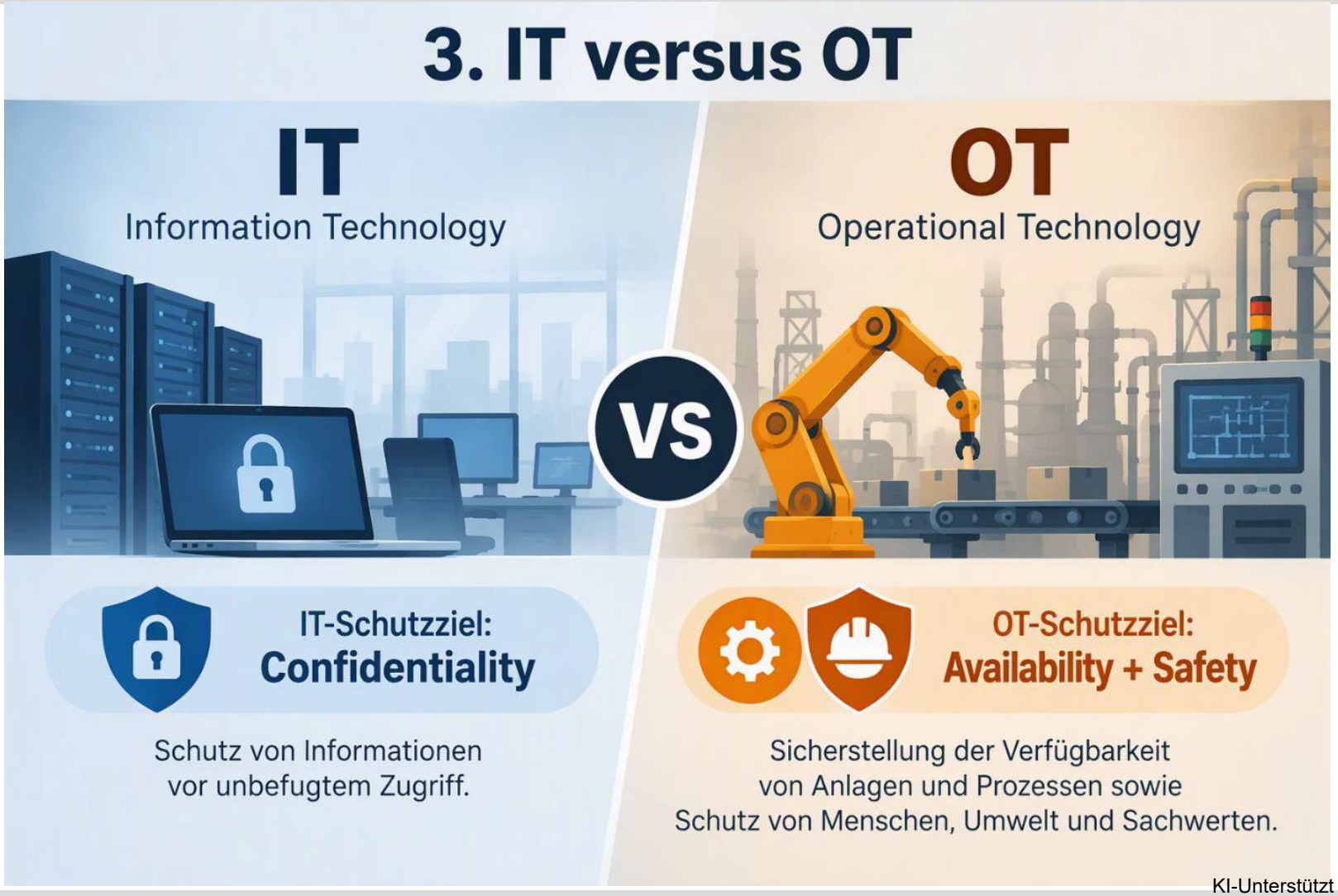
Level 1: Steuerungsebene

SPS/PLC	Embedded Controller	Safety Controller

Level 0: Feldgeräte

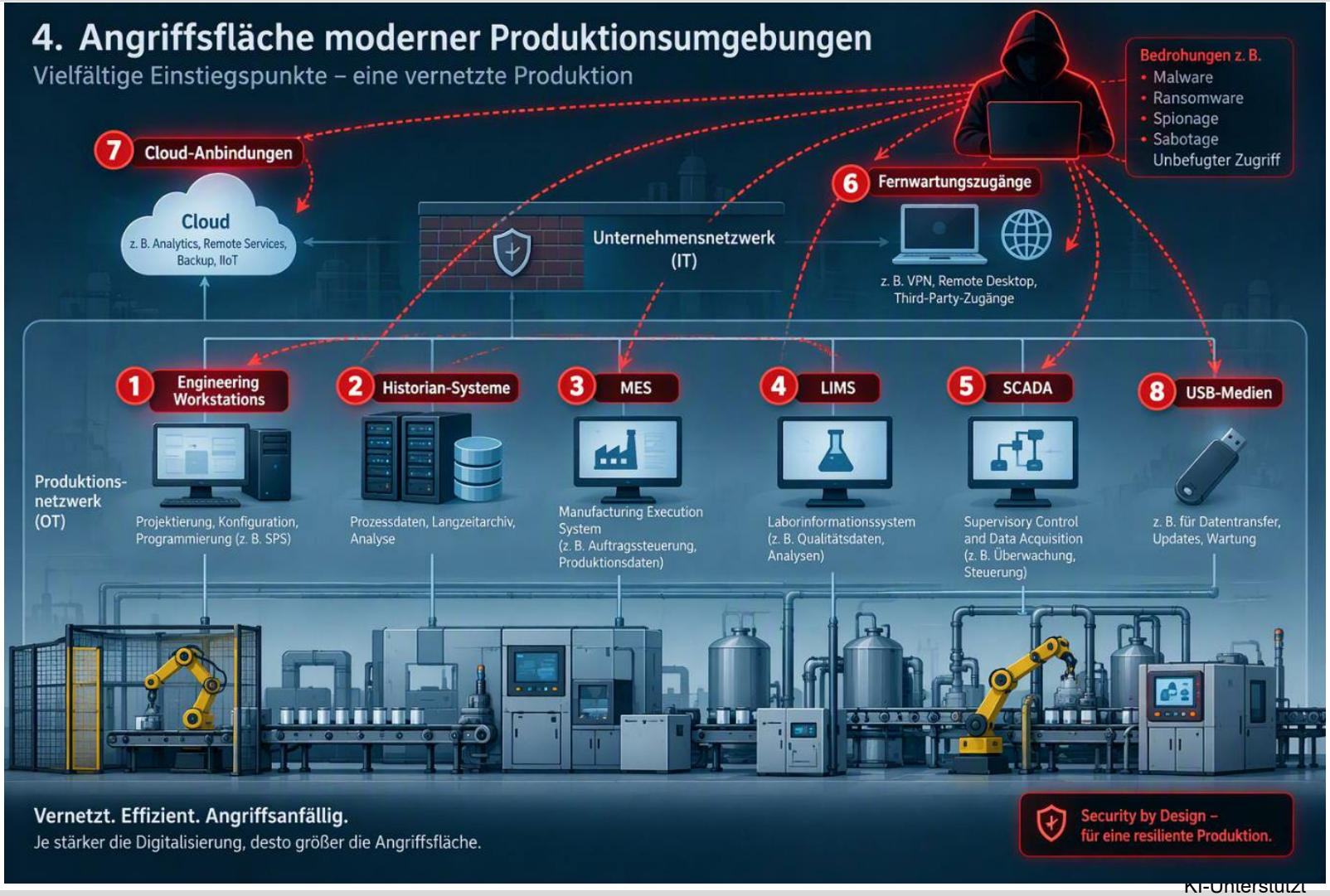
Sensoren (Temperatur, Druck, Durchfluss, Leitfähigkeit)	Aktoren (Ventile, Antriebe)	Remote-I/O-Systeme	Messumformer

IT versus OT



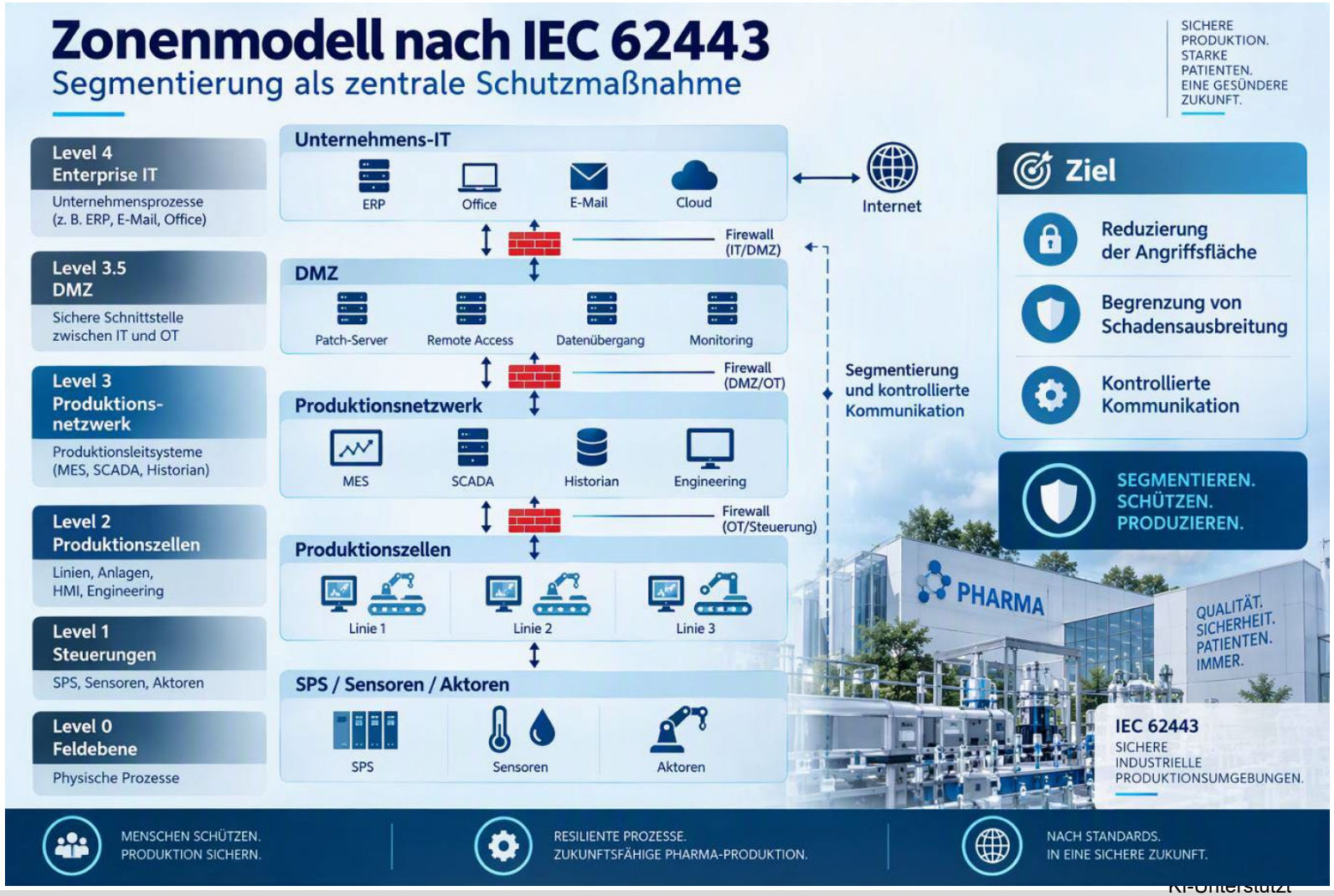
KI-Unterstützt

Cyber-Risiken in vernetzten Produktionsanlagen



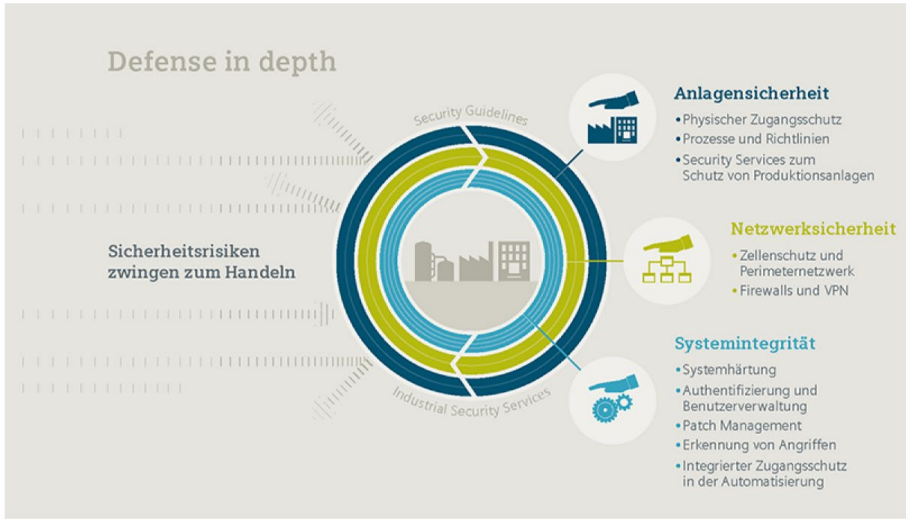
KI-unterstützt

Defence in Depth

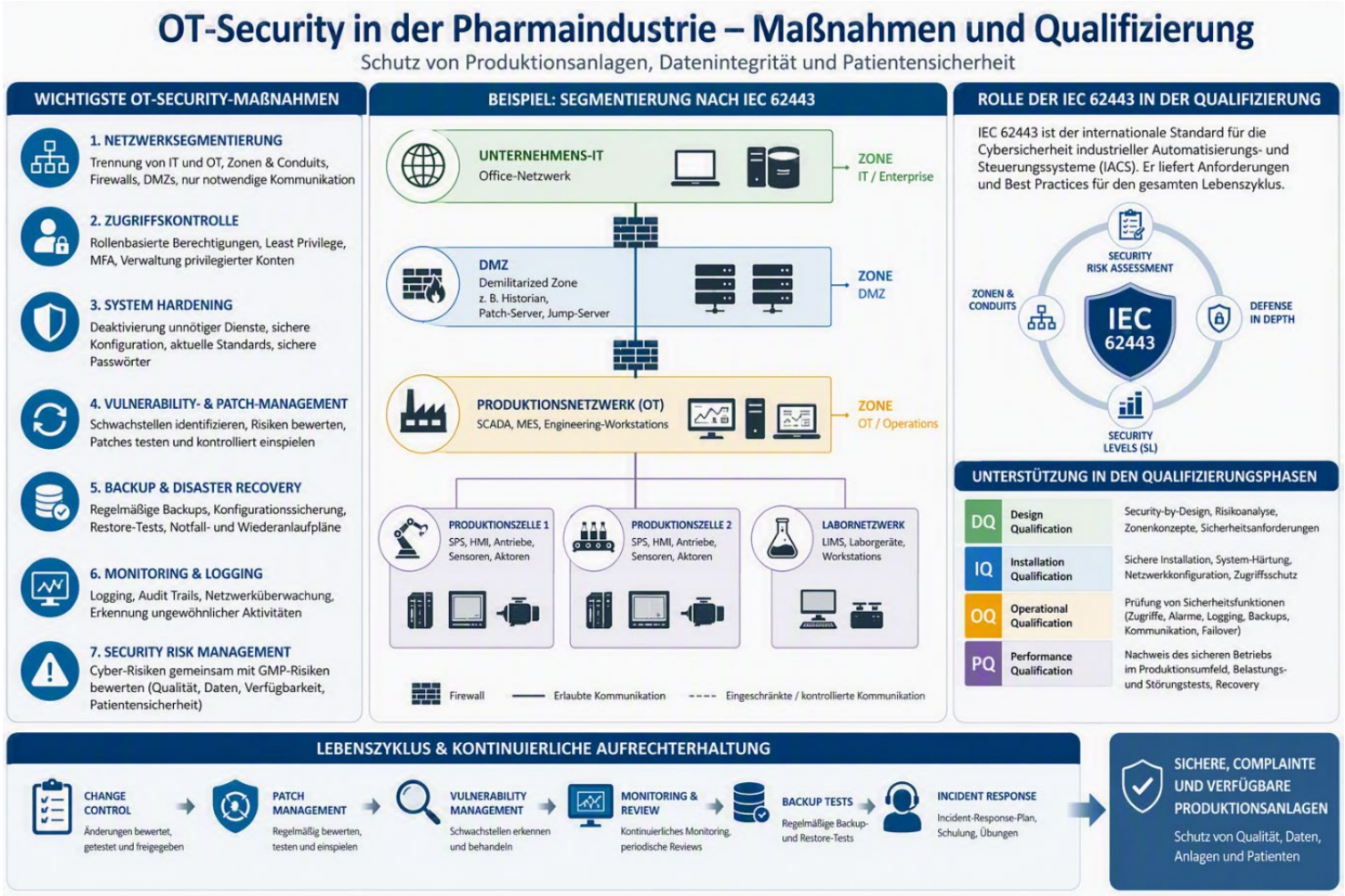


KI-unterstützt

Defence in Depth



Siemens Kompendium F V.10



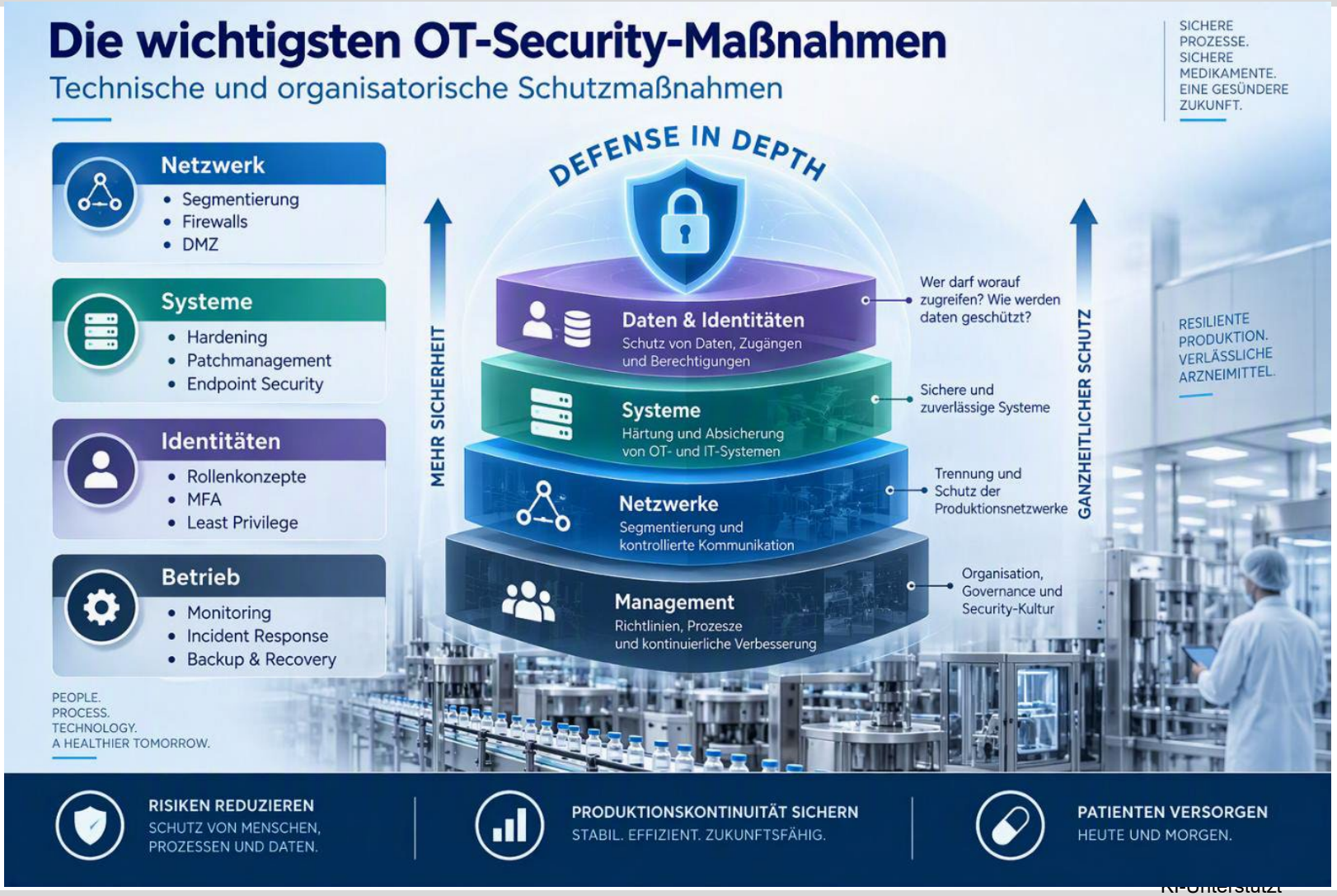
KI-Unterstützt

Defence in Depth



KI-unterstützt

Defence in Depth



KI-Unterstützt

NIS2 im Kontext von IEC 62443, ISO 27001 und GAMP5

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Gesamtübersicht: NIS-2, Annex 11, IEC 62443, ISO 27001, TISAX und GAMP 5

Einordnung · Schwerpunkte · Gemeinsamkeiten · Unterschiede

Themenbereich	NIS-2 Network and Information Security Directive 2	Annex 11 EU-GMP Annex 11 (Good Manufacturing Practice)	IEC 62443 Industrial Automation and Control Systems Security	ISO 27001 Informationssicherheits-Managementsystem	TISAX® Trusted Information Security Assessment Exchange	GAMP 5 Good Automated Manufacturing Practice
Zielsetzung	Cybersicherheit kritischer und wichtiger Einrichtungen	Sicherer Einsatz computergestützter Systeme im GMP-Umfeld	Cybersecurity für industrielle Automatisierungs- und OT-Systeme	Informationssicherheits-Managementsystem (ISMS)	Informationssicherheit in der Automobilindustrie	Risikobasierte Validierung computergestützter Systeme
Anwendungsbereich	KRITIS und wesentliche Einrichtungen	Pharma, Biotech, Medizinprodukte	Produktions- und OT-Umgebungen	Alle Organisationen	Automotive-Lieferkette	GxP-regulierte Systeme
Fokus	Cyber-Resilienz	Datenintegrität und Compliance	Verfügbarkeit, Integrität und Safety	Vertraulichkeit, Integrität, Verfügbarkeit	Schutz von Prototypen, Informationen und Datenschutz	Produktqualität und Patientensicherheit
Risikomanagement	Verpflichtend	Gefordert	Zentrale Anforderung	Kernbestandteil	Verpflichtend	Risikobasiertes Vorgehen
Asset-Management	Gefordert	Indirekt	Umfassend	Verpflichtend	Verpflichtend	Systeminventar erforderlich
Identitäts- und Zugriffsmanagement	MFA, Zugriffskontrollen	Benutzerverwaltung	SR 1 Identifikation & Authentifizierung	Annex A Controls	TISAX Anforderungen	Rollen- und Berechtigungskonzepte
Netzwerksegmentierung	Empfohlen	Nicht explizit	Fundamentaler Bestandteil	Empfohlen	Gefordert	Nicht explizit
Patchmanagement	Verpflichtend	Kontrolliert und dokumentiert	Security-Level abhängig	Verpflichtend	Verpflichtend	Change Control
Schwachstellenmanagement	Verpflichtend	Risikobasiert	Zentrales Security-Thema	Verpflichtend	Verpflichtend	Bewertung im Validierungsprozess
Logging & Monitoring	Verpflichtend	Audit Trail Pflicht	SR 6 Audit Log	Logging Controls	Nachweis erforderlich	Audit Trail Bewertung
Incident Management	Verpflichtend	Abweichungsmanagement	Incident Response Requirements	ISMS-Prozess	Incident Management	CAPA-Prozess
Business Continuity & Recovery	Verpflichtend	Backup & Restore	System Recovery	BCM-Anforderungen	Bestandteil	Disaster Recovery Tests
Lieferantenmanagement	Supply-Chain-Security	Lieferantenqualifizierung	Anforderungen an Komponentenlieferanten	Supplier Controls	Hohe Relevanz	Lieferantenbewertung
Dokumentation	Nachweis erforderlich	Umfangreiche GMP-Dokumentation	Technische Dokumentation	Verfahrensdokumentation	Nachweisführung	Validierungsdokumentation
Auditierbarkeit	Behördliche Prüfung	GMP-Inspektionen	Assessments	Zertifizierungsaudits	TISAX Assessment	CSV-Audits
Data Integrity	Indirekt	Kernanforderung (ALCOA+)	Integrität von OT-Systemen	Integrität als Schutzziel	Relevant	Schwerpunkt
Validierung	Nicht explizit	Verpflichtend	Security Assessments	Nicht explizit	Nicht explizit	Kernanforderung
Security Levels	Nein	Nein	SL1 – SL4	Nein	Nein	Nein
Safety-Bezug	Teilweise	Produktqualität	Enge Verbindung zu Safety	Indirekt	Gering	Produkt- und Patientensicherheit
Management-Verantwortung	Sehr hoch	Qualified Person / Management	Betreiberverantwortung	Top-Management	Management Commitment	System Owner

Die Standards auf einen Blick

NIS-2	Annex 11	IEC 62443	ISO 27001	TISAX	GAMP 5
Regulatorische Cybersecurity-Anforderungen	GMP-Compliance für computergestützte Systeme	OT-Security in der Produktion	Managementsystem für Informationssicherheit	Informationssicherheit in der Automobilindustrie	Validierung computergestützter Systeme

Typische Einsatzbereiche

Cybersecurity Governance	NIS-2, ISO 27001
OT-Security	IEC 62443
Pharma Compliance	Annex 11, GAMP 5
Datenintegrität (ALCOA+)	Annex 11, GAMP 5
Informationssicherheit	ISO 27001, TISAX
Lieferkettensicherheit	NIS-2, ISO 27001, TISAX
Automatisierungsanlagen	IEC 62443
Computervalidierung (CSV)	GAMP 5

Kernaussage

Die Standards ergänzen sich und adressieren unterschiedliche, aber miteinander verknüpfte Aspekte von Sicherheit, Compliance und Qualität. Je nach Branche und Umfeld – z. B. Pharma oder Automotive – ist eine Kombination der Standards sinnvoll, um regulatorische Anforderungen, Informationssicherheit, OT-Security, Datenintegrität und Validierung ganzheitlich abzudecken.

» „Gemeinsam für sichere, konforme und resiliente Prozesse und Produkte."

Stand: 2025 | Keine Rechtsberatung – Überblicksdarstellung

NIS2 im Kontext von IEC 62443, ISO 27001 und GAMP5

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



KI-Unterstützt

NIS2 im Kontext von IEC 62443, ISO 27001 und GAMP5

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



KI-unterstützt

Regulatorische Anforderungen



KI-Unterstützt

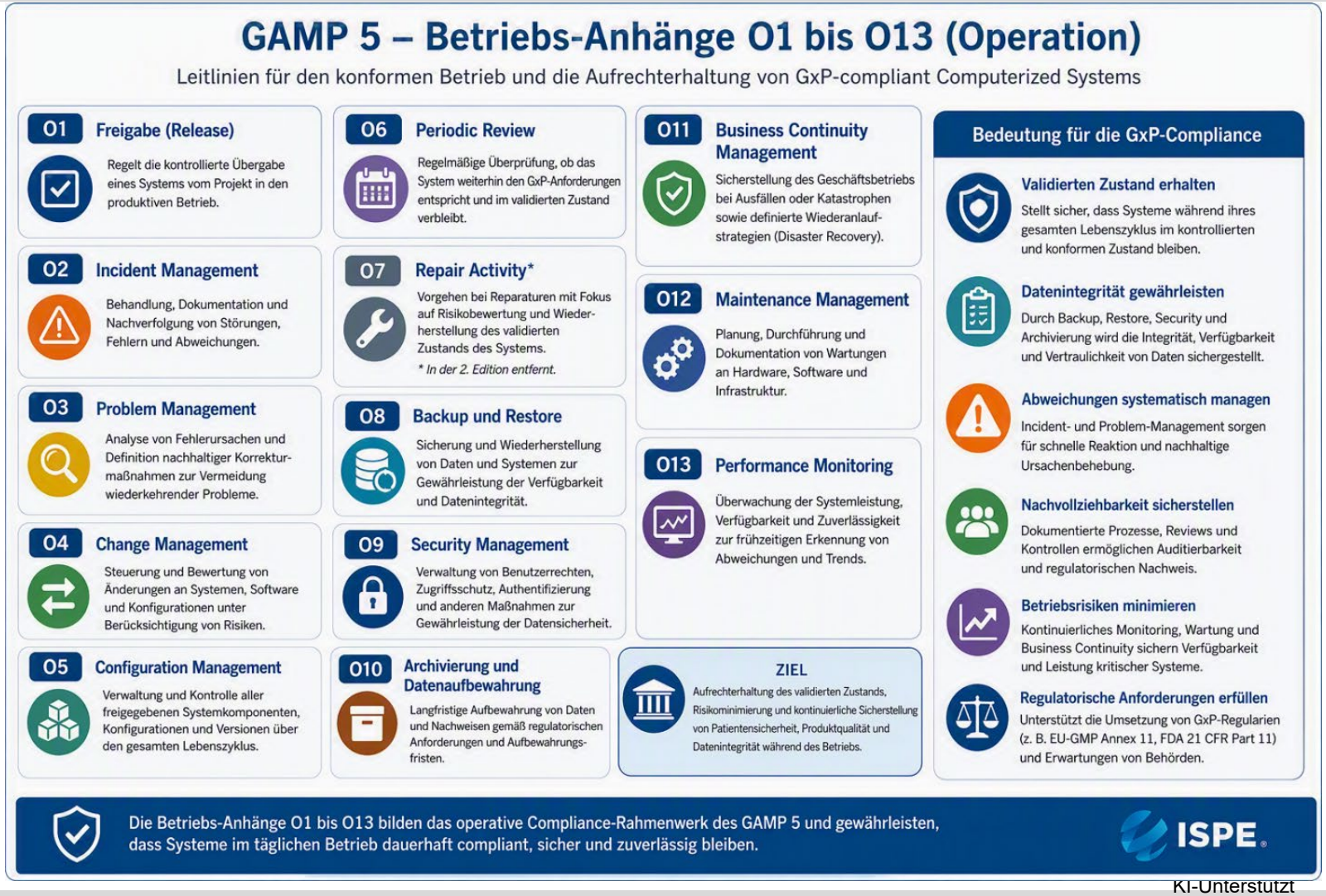
Regulatorische Anforderungen



KI-unterstützt

Regulatorische Anforderungen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



KI-Unterstützt

Vielen Dank für Ihre Aufmerksamkeit