Cybersicherheit mit IIoT in kritischen Infrastrukturen

Eine umfassende Untersuchung der IT/OT-Konvergenz & Schutzmaßnahmen

Autoren:

- Olaf Krause

Stand:

Version 1.2 vom 23.05.2025

Aktualisierungen finden Sie hier.

Herausgeber:

OKIT GmbH, https://www.okit.de

Executive Summary

Die fortschreitende digitale Transformation kritischer Infrastrukturen (KRITIS) durch die Anbindung betriebstechnischer (OT) Anlagen an das Internet bietet erhebliche Effizienzsteigerungen und innovative Möglichkeiten. Diese Konvergenz von Informationstechnologie (IT) und OT führt jedoch zu komplexen Cybersicherheitsherausforderungen, da ehemals isolierte Systeme nun neuen Bedrohungen ausgesetzt sind. Diese Untersuchung analysiert aktuelle und zukünftige Anwendungsfälle, die damit verbundenen Risiken sowie die maßgeblichen nationalen und internationalen Regulierungsrahmen, darunter das IT-Sicherheitsgesetz 2.0, die BSI-KritisV, IEC 62443 und das NIST Cybersecurity Framework. Darüber hinaus werden technische Architekturmuster und Schutzmaßnahmen, insbesondere die Rolle von Layer-7-Proxy-Servern mit Deep Packet Inspection (DPI) und Intrusion Detection/Prevention Systems (IDS/IPS), beleuchtet. Abschließend wird die Eignung des OKIT SCADA-Proxy als zentrale Sicherheitskomponente in dieser Architektur bewertet.

Die Analyse zeigt, dass die IT/OT-Konvergenz die Angriffsfläche erheblich erweitert und die inhärenten Schwachstellen von älteren OT-Systemen und deren spezialisierten Protokollen ausnutzt. Deutsche und internationale Vorschriften schreiben robuste Sicherheitsmaßnahmen, regelmäßige Audits und die Meldung von Vorfällen vor, wobei bei Nichteinhaltung erhebliche Sanktionen drohen. Layer-7-Proxys, DPI und IDS/IPS sind für eine granulare Kontrolle und Bedrohungserkennung auf der Anwendungsebene unerlässlich, erfordern jedoch eine sorgfältige Abwägung der OT-spezifischen Leistungs- und Protokollkompatibilität. Der OKIT SCADA-Proxy adressiert viele dieser Herausforderungen durch seine Fähigkeiten als Anwendungsschicht-Gateway, seine umfassende Protokollunterstützung und integrierte Sicherheitsfunktionen. KRITIS-Betreiber müssen eine mehrschichtige Verteidigungsstrategie (Defense-in-Depth) verfolgen, die Netzwerksegmentierung (z.B. iDMZ), spezialisierte OT-Sicherheitslösungen, kontinuierliche Überwachung und eine strikte Einhaltung der sich entwickelnden regulatorischen Anforderungen umfasst.

1. Einleitung: Die digitale Transformation kritischer Infrastrukturen

1.1 Definition und Bedeutung von KRITIS

Kritische Infrastrukturen (KRITIS) umfassen Organisationen und Einrichtungen, deren Funktionsfähigkeit für das Gemeinwesen von entscheidender Bedeutung ist. Eine Störung oder Zerstörung dieser Infrastrukturen könnte zu erheblichen Versorgungsengpässen, Problemen der öffentlichen Sicherheit oder anderen schwerwiegenden Konsequenzen führen.[1] Zu den KRITIS-Sektoren gehören die Energieversorgung (Elektrizität, Gas, Mineralöl), die Wasserwirtschaft (Trinkwasserversorgung, Abwasserentsorgung), die Informationstechnik und Telekommunikation, das Gesundheitswesen, das Finanz- und Versicherungswesen, der Transport und Verkehr, die Ernährung sowie der Staat und die Verwaltung.[1]

Die Einstufung eines Unternehmens als KRITIS-Betreiber hängt von verschiedenen Faktoren ab, darunter die Anlagengröße bzw. der Durchsatz (z.B. Megawatt-Leistung im Energiesektor), der Versorgungsgrad (z.B. Versorgung von mehr als 500.000 Menschen) und die zentrale Steuerungsfunktion (z.B. Leitstellen oder Netzwerke, von denen andere Systeme abhängen).[1] Ein Ausfall dieser Systeme kann weitreichende Folgen für die öffentliche Sicherheit, Gesundheit oder Versorgung der Bevölkerung haben.[1]

1.2 Die Notwendigkeit und Herausforderungen der IT/OT-Konvergenz

Die zunehmende Vernetzung von Informationstechnologie (IT) und Betriebstechnologie (OT) ist eine direkte Folge von Industrie 4.0 und dem Industrial Internet of Things (IIoT). Ziel dieser Konvergenz ist es, die Produktivität, Effizienz und Innovationskraft in industriellen Prozessen erheblich zu steigern.[3] Während OT-Systeme historisch oft physikalisch isoliert (Air-Gapped) betrieben wurden, um sie vor externen Bedrohungen zu

schützen, erfordern moderne Anwendungen wie intelligente Sensoren, Echtzeitdatenanalyse und Fernwartung eine zunehmende Internetanbindung.[5]

Dieser Übergang vom traditionellen "Air-Gapping" zu internetverbundenen OT-Systemen stellt einen grundlegenden Paradigmenwechsel in der KRITIS-Sicherheit dar. Die frühere Annahme, dass ein System durch physische Isolation vor externen Angriffen geschützt sei, ist mit der Notwendigkeit der Konnektivität für Datenaustausch, Fernüberwachung und Automatisierung hinfällig geworden.[6] Dies ist nicht nur eine inkrementelle Erhöhung des Risikos, sondern eine tiefgreifende Veränderung, die eine vollständige Neubewertung der Sicherheitsstrategien erfordert. Der Fokus verschiebt sich von einer perimeterzentrierten Isolation hin zu einer dynamischeren, mehrschichtigen Verteidigung. Diese Konvergenz setzt die kritische Infrastruktur neuen und gefährlichen Cyberbedrohungen aus.[3]

1.3 Definition von IioT

Das Industrial Internet of Things (IIoT) ist eine Untergruppe des Internets der Dinge (IoT), die sich auf die Anwendung von IoT-Technologien in industriellen Umgebungen konzentriert. Die Kernmerkmale und Komponenten des IIoT umfassen:

- **Vernetzte Sensoren und Geräte:**
  Industrielle Maschinen, Anlagen und Geräte sind mit Sensoren ausgestattet und über Netzwerke (häufig das Internet oder industrielle Kommunikationsprotokolle, die über IP laufen) miteinander verbunden.

- **Datenerfassung:**
  Sensoren sammeln Daten aus der physischen Umgebung (z.B. Temperatur, Druck, Vibration, etc.).

- **Datenübertragung:**
  Die gesammelten Daten werden über Kommunikationsinfrastrukturen (z.B. WLAN, 5G, Ethernet) an zentrale Systeme (lokal, Edge oder Cloud) übertragen.

- **Datenverarbeitung und -analyse:**
  Gesammelte Daten werden verarbeitet und analysiert, oft unter Einsatz von Algorithmen, KI und Machine Learning, um Muster zu erkennen, Vorhersagen zu treffen oder Anomalien zu identifizieren.

- **Industrieller Anwendungsbereich:**
  Die Technologie wird eingesetzt, um industrielle Prozesse zu optimieren, die Effizienz zu steigern, Kosten zu senken, die Sicherheit zu verbessern, vorausschauende Wartung zu ermöglichen und neue Geschäftsmodelle zu entwickeln. Der Fokus liegt auf Maschinen- und Anlageneffizienz, Arbeitsschutz und Instandhaltung.

- **Automatisierung und Steuerung:**
  Die gewonnenen Erkenntnisse können zur automatischen Steuerung von Prozessen oder zur Unterstützung menschlicher Entscheidungen genutzt werden.

2. Anwendungsfälle der Internetanbindung von OT-Anlagen

Die Internetanbindung betriebstechnischer Anlagen in kritischen Infrastrukturen ermöglicht eine Vielzahl von Anwendungsfällen, die von der Effizienzsteigerung bis zur Verbesserung der Versorgungssicherheit reichen.

2.1 Aktuelle Use Cases

Aktuell werden internetbasierte Technologien in KRITIS-Sektoren vielfältig eingesetzt:

- **Fernüberwachung und -steuerung:**
  - Ein prominentes Beispiel ist die Anbindung von Kurzschlussanzeigern über Mobilfunk-Technologie. Dies ermöglicht eine schnelle Fehlerlokalisierung und Wiederherstellung der Versorgung in Stromnetzen.[7]
  - Lade- und Energiemanagement profitiert von intelligenter Lastverteilung für eine stabile Stromversorgung und punktgenauen Strom-Verbrauchsprognosen.[4]
  - Im Bereich der Wasserwirtschaft wird eine vernetzte Wasserinfrastruktur mit Echtzeitdaten zur Leckageerkennung und Diebstahlprävention genutzt.[4]
  - Die Retrofit von Wasserkraftwerken zeigt den Übergang von proprietären Steuerungen zu offenen IoT-Plattformen.[4]
  - Intelligente Messsysteme (iMSys) nutzen die 450-MHz-Frequenz für eine stabile Erreichbarkeit, was die Fernauslesung von Zählern ermöglicht.[7]
- **Anlagensicherheit und Wartung:**

- Die intelligente Überwachung gasisolierter Schaltanlagen erhöht die Anlagensicherheit.[4]
- Digitale Wartungsbücher für Protokollierung und Rechtssicherheit werden eingeführt.[4]
- Die Fernüberwachung medizinischer Geräte führt zu Kosteneinsparungen und Compliance-Vorteilen.[4]

- **Verkehr und Logistik:**
  - Die sichere Anbindung von Straßenausstattung und Verkehrsleittechnik gewährleistet verschlüsselte Datenübertragung.[4]
  - IoT-basierte Lösungen für die netzunabhängige Notfallhilfe verbessern die Reaktionsfähigkeit.[4]
  - Intelligente Container-Services optimieren manuelle Arbeitsschritte in Reinigungsanlagen.[4]

2.2 Zukünftige Use Cases im Industrial IoT (IIoT)

Im Industriellen Umfeld ist Industrial IoT (IioT) bereits bestehende Realität. Die weitere Entwicklung im IIoT verspricht eine noch tiefere Integration und Automatisierung in kritischen Infrastrukturen. Es ist zu erwarten, dass die begonnenen Entwicklungspfade fortgesetzt werden:

- **Prädiktive Wartung und automatisierte Prozesse:**
  - IIoT-Analysen werden in der Lage sein, geringfügige Abweichungen in der Maschinenleistung zu erkennen und prädiktive Wartungsmaßnahmen zu planen, bevor ein Ausfall auftritt.[8]
  - Automatisierte Aktionen basierend auf Echtzeitdaten, wie die Anpassung von

Maschineneinstellungen oder das Senden von Warnmeldungen an Techniker, werden zur Norm.[8]

- Die Optimierung von Fahrzeugwartungsstrategien wird von reaktiv zu proaktiv verschoben.[9]

- **Smart Grids und erweiterte Sensorik:**
  - Der Energiesektor wird IIoT nutzen, um das Netzmanagement zu verbessern, Ausfallzeiten zu reduzieren und die Energieverteilung zu optimieren.[8]
  - Intelligente Zähler und Sensoren überwachen den Energieverbrauch in Echtzeit, was es Verbrauchern ermöglicht, ihren Verbrauch zu verfolgen und Kosten zu senken.[9]
  - Smart Grids werden Sensoren, Datenanalysen und Konnektivität nutzen, um Stromausfälle schneller zu erkennen und darauf zu reagieren.[9]

- **Integration von KI und Big Data in OT-Prozesse:**
  - Echtzeitüberwachung von Pipelines, Bohrinseln und Raffinerien im Öl- und Gassektor wird Unfälle verhindern und die Leistung optimieren.[8]
  - Wearables mit IIoT-Technologie ermöglichen die Überwachung der Tiergesundheit und -bewegung in der Landwirtschaft.[8]
  - Die Sonar-Objekterkennung in Echtzeit für autonome Untersuchungsroboter wird neue Möglichkeiten in verschiedenen Sektoren eröffnen.[4]

Auch wenn von den genannten Themen schon vieles in der Realität angekommen scheint, so ist in der Breite der bestehenden Anwender noch ein erhebliches Potential für Verbesserung zu erkennen. Ein nicht unerheblicher Anteil von potentiellen Anwendern hat die Einführung überhaupt erst noch vor sich.

Die Entwicklung von aktuellen Überwachungs- und Steuerungsanwendungen hin zu zukünftigen prädiktiven und autonomen IIoT-Anwendungen bedeutet eine Verschiebung von der reinen Datenerfassung hin zu datengesteuerten Entscheidungen und Automatisierung. Dies erhöht die Kritikalität der Datenintegrität und der Echtzeitverarbeitung erheblich.

Aktuelle Anwendungsfälle konzentrieren sich hauptsächlich auf die Fernüberwachung und grundlegende Steuerung, bei der Daten für die menschliche Analyse und Aktion gesammelt und übertragen werden (z.B. Kurzschlussanzeiger, die einen Fehler signalisieren). Zukünftige IIoT-Anwendungen gehen jedoch in Richtung prädiktiver Wartung, automatischer Anpassungen und sogar autonomer Operationen.[8] Dieser Übergang bedeutet, dass Daten nicht mehr nur informativ sind; sie beeinflussen direkt operative Entscheidungen und physikalische Prozesse. Daher werden die Integrität, Aktualität und Verfügbarkeit dieser Daten noch wichtiger. Ein kompromittierter Datenstrom oder eine verzögerte Reaktion könnte unmittelbare und schwerwiegende physische Folgen haben, was eine exponentielle Zunahme der Risiken für die Cybersicherheit verdeutlicht.

Tabelle: Ausgewählte aktuelle und zukünftige KRITIS-Use-Cases mit Internetanbindung also im Kontext IIoT

Sektor (KRITIS-Branche)	**Use Case (Aktuell/Zukünftig)**	**Technologie/ Anbindung**	**Primärer Nutzen**
Energie	Kurzschlussanzeiger (Aktuell)	Mobilfunk (z.B. 450 MHz), LPWAN	Schnelle Fehlerlokalisierung, Wiederherstellung der Versorgung [7]
Energie	Lade- und Energiemanagement (Aktuell)	IoT-Plattformen	Intelligente Lastverteilung, präzise Verbrauchsprognosen [4]
Wasser	Vernetzte Wasserinfrastruktur (Aktuell)	IoT-Plattformen	Echtzeitdaten gegen Leckagen und Diebstahl [4]
Energie	Intelligente Messsysteme (iMSys) (Aktuell)	Mobilfunk (z.B. 450 MHz), LPWAN	Stabile Erreichbarkeit für Smart Meter [7]
Allgemein	Prädiktive Wartung (Zukünftig)	IIoT, KI, Sensoren	Erkennung von Maschinenfehlern vor dem Ausfall, Optimierung der Wartung [8]
Energie	Smart Grids (Zukünftig)	IIoT, Sensoren, Datenanalyse	Verbessertes Netzmanagement, schnellere Reaktion auf Ausfälle [8]
Öl & Gas	Pipeline-Monitoring (Zukünftig)	IIoT, Sensoren	Echtzeit-Erkennung von Druckschwankungen und Lecks [8]
Landwirtschaft	Tierüberwachung (Zukünftig)	IIoT-Wearables	Überwachung von Tiergesundheit und -verhalten [8]

Sektor (KRITIS-Branche)	Use Case (Aktuell/Zukünftig)	Technologie/ Anbindung	Primärer Nutzen
Verkehr	Autonome Untersuchungsroboter (Zukünftig)	KI, Sonar	Echtzeit-Objekterkennung [4]

3. Cyber-Risiken und Schwachstellen in konvergenten IT/OT-Umgebungen

Die Konvergenz von IT und OT in kritischen Infrastrukturen bringt eine Reihe spezifischer Cyber-Risiken und Schwachstellen mit sich, die eine besondere Betrachtung erfordern.

3.1 Spezifische Risiken der IT/OT-Konvergenz

- **Erweiterte Angriffsfläche und laterale Bewegung:**
  Die Integration von IT- und OT-Systemen vergrößert die potenzielle Angriffsfläche exponentiell.3 Angreifer können Kompromittierungen in IT-Systemen (z.B. durch Phishing-Mails) nutzen, um sich über ungesicherte Schnittstellen lateral in das OT-Netzwerk zu bewegen und so Zugang zu SCADA-Systemen und kritischen Steuerungen zu erhalten.[5] Ein bemerkenswertes Beispiel hierfür ist der Sandworm-Angriff auf die ukrainische Energieversorgung im Jahr 2023, bei dem diese Taktik angewendet wurde, um systematisch Umspannwerke abzuschalten.[5]

- **Anfälligkeit von Legacy-OT-Systemen:**
  Viele OT-Systeme wurden vor Jahrzehnten entwickelt und verfügen nicht über integrierte Sicherheitsmechanismen. Ihre Architektur ist auf Langlebigkeit und Stabilität ausgelegt, nicht auf Cybersicherheit.[5] Diese Systeme weisen oft einen Mangel an modernen Sicherheitsfunktionen wie Verschlüsselung, starker Authentifizierung und regelmäßigen Updates auf, was sie anfällig für Ransomware, Malware und Lieferkettenangriffe macht.[10] Der grundlegende Unterschied in der Designphilosophie zwischen IT (Agilität, schnelle Updates, Datenvertraulichkeit) und OT (Langlebigkeit, Stabilität, Sicherheit, Verfügbarkeit) schafft eine inhärente Sicherheitslücke in konvergenten Umgebungen. IT-Systeme sind für schnelle Entwicklung, häufige Patches und Datenvertraulichkeit konzipiert und akzeptieren oft Ausfallzeiten für Updates. OT-Systeme hingegen sind für extreme Langlebigkeit, Stabilität und Sicherheit ausgelegt, mit minimaler Toleranz für Ausfallzeiten.[5] Dies bedeutet, dass Sicherheitspatches, die in der IT üblich sind, in OT-Umgebungen aufgrund von Stabilitätsbedenken, langen

Zertifizierungszyklen oder sogar der Einstellung der Unterstützung durch den Hersteller oft schwierig, wenn nicht unmöglich oder schädlich sind.[5] Dies führt zu einer "Sicherheitslast", bei der Schwachstellen über längere Zeiträume bestehen bleiben, was diese Systeme zu Hauptzielen macht. Dies verdeutlicht, dass IT-Sicherheitsstrategien nicht einfach auf OT übertragen werden können; es sind spezialisierte Ansätze erforderlich, die diese grundlegenden Unterschiede berücksichtigen.

- **Risiken durch spezialisierte OT-Protokolle und Fernwartungsschnittstellen:** OT nutzt spezifische, oft proprietäre Protokolle (z.B. Modbus, OPC UA, DNP3, IEC 61850), die häufig keine oder nur sehr einfache Sicherheitsmechanismen wie Verschlüsselung oder Authentifizierung besitzen.[5] Fernwartungsschnittstellen, obwohl für die Effizienz unerlässlich, sind oft unzureichend gesichert und bieten Angreifern direkte Einfallstore.[5] Die Kombination aus spezialisierten, unsicheren OT-Protokollen und anfälligen Fernzugriffspunkten schafft einen kritischen "blinden Fleck" für traditionelle IT-Sicherheitstools, was Anwendungsschicht-Sicherheitslösungen erfordert, die den OT-Kontext verstehen. Herkömmliche IT-Sicherheitstools wie Firewalls und SIEMs sind oft "blind" für die Nuancen von OT-Protokollen.[5] Sie könnten legitimen Datenverkehr erkennen, aber keine bösartigen Befehle, die in diesen Protokollen eingebettet sind, da sie den Anwendungsschicht-Kontext nicht verstehen. In Kombination mit schlecht gesicherten Fernwartungsschnittstellen entsteht so ein direkter, unüberwachter Pfad für Angreifer, um physische Prozesse zu manipulieren. Dies bedeutet, dass Sicherheitslösungen auf Layer 7 (Anwendungsschicht) operieren und über ein tiefes Protokollwissen verfügen müssen, um den tatsächlichen Inhalt und die Logik von OT-Befehlen zu überprüfen, anstatt nur grundlegende Paket-Header. Hier werden Lösungen mit DPI und protokollspezifischer Analyse unerlässlich.

3.2 Herausforderungen bei der Implementierung von Layer 7 Proxies, DPI und IDS/IPS in OT

- **Latenz- und Performance-Anforderungen:** Die Inspektion auf Layer 7 ist komplexer und ressourcenintensiver als auf Layer 4, was potenziell Latenzen verursachen kann.[15] OT-Systeme haben jedoch oft strenge

Echtzeitanforderungen, bei denen geringe Latenz für Steuerungsschleifen und die Betriebsführung kritisch ist.[5] Der inhärente Kompromiss zwischen tiefer Sicherheitsinspektion (L7, DPI) und Echtzeit-Performance in OT-Umgebungen erfordert eine sorgfältige Balance und spezialisierte Lösungen, die für industrielle Kontexte optimiert sind. Layer-7-Proxys und DPI bieten eine granulare Sicherheit, indem sie den Inhalt der Anwendungsschicht überprüfen, was für die Erkennung ausgeklügelter Bedrohungen in OT-Protokollen entscheidend ist.[18] Diese tiefe Inspektion führt jedoch zu zusätzlichem Verarbeitungsaufwand und kann Latenz verursachen.[15] In der OT können selbst kleine Verzögerungen kritische Steuerungsprozesse stören, was zu Sicherheitsrisiken oder Betriebsausfällen führen kann.[5] Dies schafft einen direkten Konflikt zwischen Sicherheitstiefe und betrieblicher Notwendigkeit. Daher sind generische IT-Layer-7-Lösungen möglicherweise nicht geeignet. Spezielle OT-fokussierte Layer-7-Proxys, die für geringe Latenz und hohen Durchsatz in industriellen Umgebungen optimiert sind, sind unerlässlich, um diesen Kompromiss zu mildern.

- **Kompatibilität mit proprietären und industriellen Protokollen:** Layer-7-Awareness erfordert ein sehr tiefes Verständnis der anwendungsspezifischen Protokolle.[20] OT-Umgebungen nutzen eine breite Palette spezialisierter und oft proprietärer industrieller Kommunikationsprotokolle[5], was es für generische L7-Proxys schwierig macht, diese zu interpretieren und abzusichern.[22] Die Fragmentierung der OT-Protokolle stellt eine erhebliche Interoperabilitäts- und Sicherheitsherausforderung für Layer-7-Lösungen dar, die entweder umfangreiche kundenspezifische Entwicklungen oder zweckgebundene industrielle Proxys erfordert. Während Layer-7-Proxys für HTTP/HTTPS-Verkehr leistungsstark sind, wird die OT-Landschaft von verschiedenen, oft proprietären und nicht standardisierten Industrieprotokollen (Modbus, DNP3, IEC 61850 usw.) dominiert.[5] Ein generischer Layer-7-Proxy würde diese Protokolle nicht von Natur aus "verstehen", was seine Fähigkeit zur Durchführung von Deep Packet Inspection oder zur Durchsetzung von Regeln auf Anwendungsebene einschränkt. Dies bedeutet, dass für eine effektive Sicherheit ein Layer-7-Proxy in einer OT-Umgebung entweder kundenspezifisch entwickelt werden muss, um diese spezifischen Protokolle zu unterstützen, oder eine speziell entwickelte Lösung sein muss, die diese Kompatibilität bereits besitzt.[22] Dies unterstreicht eine kritische Eintrittsbarriere für viele IT-zentrierte Sicherheitstools in der OT und betont den Wert spezialisierter Lösungen.

- **Komplexität der Konfiguration und Wartung:**
  Die Implementierung von DPI kann Firewalls und andere Sicherheitssoftware komplexer und schwieriger zu verwalten machen, da sie ständige Aktualisierungen und Überarbeitungen der Richtlinien erfordert.[17] Die OT-Sicherheit führt oft zu einer Verschiebung der Verantwortlichkeiten und erfordert klare Pläne sowie eine enge Zusammenarbeit zwischen IT- und OT-Teams.[6] Die Komplexität der Integration und Verwaltung fortschrittlicher Layer-7-Sicherheitsfunktionen in OT-Umgebungen kann zu Fehlkonfigurationen und einer erhöhten betrieblichen Belastung führen, was potenziell die Sicherheit, die sie gewährleisten sollen, untergräbt. Layer-7-Proxys, DPI und IDS/IPS bieten eine ausgeklügelte Kontrolle, aber diese Komplexität geht mit einem erhöhten Konfigurationsaufwand einher.[17] In der OT, wo Systeme empfindlich sind und Änderungen physische Auswirkungen haben können, sind Fehlkonfigurationen nicht nur Sicherheitsrisiken, sondern auch betriebliche Gefahren. Die Notwendigkeit ständiger Richtlinienaktualisierungen und das spezialisierte Wissen, das zur Verwaltung dieser Systeme erforderlich ist[5], können bereits überlastete IT/OT-Teams überfordern. Dies bedeutet, dass benutzerfreundliche Schnittstellen, Automatisierung und speziell für OT-Umgebungen entwickelte Lösungen, die die Verwaltung vereinfachen, entscheidend sind, um eine effektive und nachhaltige Sicherheit zu gewährleisten.

Tabelle: Vergleich von IT- und OT-Sicherheitsmerkmalen

Merkmal	**Informationstechnologie (IT)**	**Betriebstechnologie (OT)**
Primäres Ziel	Datenvertraulichkeit, Integrität, Verfügbarkeit	Verfügbarkeit, Sicherheit, Integrität
Priorität (CIA-Triade)	Vertraulichkeit > Integrität > Verfügbarkeit	Verfügbarkeit > Sicherheit > Integrität
Lebenszyklus	Kurz (wenige Jahre)	Lang (Jahrzehnte)[5]
Toleranz für Ausfallzeiten	Hoch (geplante Wartung möglich)	Sehr niedrig (direkte Auswirkungen auf Produktion/Sicherheit)[12]
Typische Protokolle	HTTP, TCP/IP, SMTP, DNS	Modbus, DNP3, IEC 61850, OPC UA[5]
Patching-Frequenz	Regelmäßig, oft automatisiert	Selten, komplex, oft manuell[5]
Hauptrisiken	Datenverlust, Diebstahl, Reputationsschaden	Physischer Schaden, Betriebsunterbrechung, Lebensgefahr[5]
Sicherheitsmechanismen	Firewalls, EDR, Verschlüsselung, IAM	Netzwerksegmentierung, IDS, Asset Visibility Tools[10]

4. Normen, Vorgaben und verpflichtende Maßnahmen für KRITIS-Betreiber

Die Cybersicherheit kritischer Infrastrukturen ist in Deutschland und international durch eine Reihe von Gesetzen, Verordnungen und Standards geregelt, die Betreiber zu umfassenden Schutzmaßnahmen verpflichten.

4.1 Nationaler Rahmen: Das IT-Sicherheitsgesetz 2.0 und die BSI-KritisV

- **Pflichten zur Absicherung und Meldung von Sicherheitsvorfällen:**
  Das am 28. Mai 2021 in Kraft getretene IT-Sicherheitsgesetz 2.0 verpflichtet KRITIS-Betreiber zur Umsetzung von IT-Sicherheitsmaßnahmen, die dem "Stand der Technik" entsprechen.[11] Unternehmen müssen eine Kontaktstelle (in der Regel eine funktionale Mailbox) benennen, um eine konsistente Kommunikation mit dem BSI zu gewährleisten.[25] Darüber hinaus besteht die Pflicht, ungeplante Störungen und unmittelbare Cyberangriffe auf die IT-Infrastruktur unverzüglich über diese funktionale Mailbox an das BSI zu melden.[25]

- **Anforderungen an Angriffserkennungssysteme (SzA) und Audit-Pflichten:**
  Seit dem 1. Mai 2023 sind KRITIS-Betreiber verpflichtet, Systeme zur Angriffserkennung (SzA) einzusetzen.25 Die Einhaltung der Vorschriften muss alle zwei Jahre durch ein Audit-Zertifikat (gemäß § 8a Abs. 3 BSIG) eines externen Prüfers nachgewiesen werden.[11] Eine detaillierte Dokumentation der IT-Systeme, Prozesse und Sicherheitsmaßnahmen ist für diese Audits zwingend erforderlich.[11]

- **Reifegrade der BSI Orientierungshilfe:**
  Die BSI Orientierungshilfe legt die Anforderungen für SzA fest und unterteilt diese in die Phasen LOGGING, DETECTION und RESPONSE.25 Die darin beschriebenen Maßnahmen sind in SOLL-, MUSS- und KANN-Anforderungen kategorisiert und in Reifegrade

priorisiert (Reifegrad 3 ist zunächst ausreichend, Reifegrad 4 ist ein langfristiges Ziel).[25] Die Betonung des BSI auf "Stand der Technik"-Maßnahmen und vorgeschriebene Angriffserkennungssysteme (SzA) deutet auf eine proaktive, kontinuierliche Sicherheitshaltung hin, anstatt eines reaktiven, nur auf Compliance ausgerichteten Ansatzes. Es genügt nicht mehr, lediglich Sicherheitsmaßnahmen zu haben. Das BSI fordert explizit "Stand der Technik"-Maßnahmen[11] und schreibt Angriffserkennungssysteme (SzA) mit definierten Reifegraden vor.[25] Dies geht über eine statische Checklisten-Compliance hinaus zu einer dynamischen, sich entwickelnden Sicherheitsanforderung. Es bedeutet, dass Organisationen ihre Abwehrmaßnahmen kontinuierlich bewerten, implementieren und verbessern müssen, aktiv nach Bedrohungen suchen und auf diese reagieren, anstatt nur darauf zu warten, dass Vorfälle auftreten. Dies impliziert auch die Notwendigkeit fortschrittlicher Tools, die Anomalien erkennen und Echtzeit-Einblicke liefern können, über die traditionelle signaturbasierte Erkennung hinausgehend.

- **Rechtliche Konsequenzen bei Nichteinhaltung:**
  Die Nichteinhaltung kann zu erheblichen Geldstrafen führen (bis zu 20 Millionen Euro oder 4% des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist, ähnlich den Regelungen der DSGVO).[26] Die persönliche Haftung für die Geschäftsführung rückt zunehmend in den Fokus, wenn keine angemessenen Sicherheitsmaßnahmen getroffen oder deren Umsetzung nicht ausreichend kontrolliert werden.[1] Weitere Konsequenzen können Betriebsunterbrechungen, Reputationsschäden, Kundenverlust und Diebstahl geistigen Eigentums sein.[28] Die persönliche Haftung für das Management und erhebliche finanzielle Sanktionen unterstreichen, dass Cybersicherheit in KRITIS nicht länger nur eine Angelegenheit der IT-Abteilung ist, sondern eine kritische strategische Priorität auf Vorstandsebene. Die Verhängung hoher Bußgelder und, noch wichtiger, die persönliche Haftung für die Geschäftsführung[1] heben Cybersicherheit von einem technischen Betriebsproblem zu einer grundlegenden Verantwortung der Unternehmensführung. Dies bedeutet, dass Cybersicherheitsentscheidungen, Ressourcenzuweisung und Überwachung in die höchsten Ebenen der Organisationsführung integriert werden müssen. Es erzwingt einen Mentalitätswandel, bei dem Sicherheit nicht nur als Kostenfaktor, sondern als wesentlicher Geschäftsfaktor und rechtliche Verpflichtung angesehen wird, die die Rentabilität und den Ruf des

KRITIS-Betreibers direkt beeinflusst.

4.2 Internationale Standards und Frameworks

- **ISA/IEC 62443:**
  Fokus auf industrielle Automatisierungs- und Steuerungssysteme (IACS): IEC 62443 ist eine Reihe von Standards, die Verfahren zur Implementierung elektronisch sicherer industrieller Automatisierungs- und Steuerungssysteme (IACS) definieren. Sie umfassen Systemanforderungen, Richtlinien und technische Kontrollen.30 Der Standard definiert vier Sicherheitslevel (SL1 bis SL4), basierend auf dem potenziellen Ausmaß eines Cybersicherheitsvorfalls, mit zunehmend strengeren Sicherheitsanforderungen.[31] Zu den Schlüsselkomponenten gehören das Sicherheitsmanagementprogramm (IEC 62443-2-1), System-Sicherheitsanforderungen (IEC 62443-3-3) und Komponenten-Sicherheitsanforderungen (IEC 62443-4-2).30 Diese Standards adressieren Datenintegrität, Verfügbarkeit und Vertraulichkeit durch Maßnahmen wie Zugriffssteuerung, Sicherheitsüberwachung, Datensicherheit und Wiederherstellungsplanung.[30]

- **NIST Cybersecurity Framework (CSF):**
  Allgemeiner Rahmen für Cybersicherheitsrisikomanagement: Das NIST CSF ist ein freiwilliges Framework, das aus Standards, Richtlinien und Best Practices zur Verwaltung von Cybersicherheitsrisiken besteht. Es ist um fünf Kernfunktionen herum strukturiert: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.[30] Es bietet Organisationen Flexibilität bei der Bestimmung ihrer eigenen Risikostufen und der Priorisierung ihrer Bemühungen.[31] Die Komplementarität von IEC 62443 (OT-spezifisch, präskriptive Sicherheitsstufen) und NIST CSF (breiter, flexibles Risikomanagement) legt nahe, dass KRITIS-Betreiber eine hybride Compliance-Strategie anwenden sollten. IEC 62443 ist hochspezifisch für industrielle Steuerungssysteme und definiert konkrete Sicherheitsstufen.[31] NIST CSF hingegen ist ein allgemeineres, risikobasiertes Framework.[30] Eine Zuordnung zwischen ihnen ist möglich und wird empfohlen.[30] Dies bedeutet, dass ein robustes KRITIS-Cybersicherheitsprogramm nicht das eine dem anderen vorziehen sollte, sondern beide integrieren muss. IEC 62443 liefert das tiefgehende technische "Wie" für die OT, während NIST CSF die

übergeordnete organisatorische Risikomanagement- und Governance-Struktur bietet. Dieser hybride Ansatz gewährleistet sowohl eine granulare technische Sicherheit als auch eine umfassende, anpassungsfähige Risikomanagement-Haltung, was angesichts der sich entwickelnden Bedrohungslandschaft und der Komplexität von KRITIS entscheidend ist.

Tabelle: Überblick relevanter Normen und Gesetze mit Fokus auf KRITIS-Anforderungen

Norm/Gesetz	**Geltungsbereich**	**Schwerpunkt**	**Verpflichtend für KRITIS**	**Wichtige Maßnahmen/Anforderungen**
IT-Sicherheitsgesetz 2.0	National (Deutschland)	Erhöhung der IT-Sicherheit, Stärkung des BSI	Ja [26]	"Stand der Technik" IT-Sicherheit, Meldepflichten, Kontaktstelle zum BSI [11]
BSI-KritisV	National (Deutschland)	Konkretisierung der IT-Sicherheitsanforderungen für KRITIS	Ja [26]	Einsatz von Angriffserkennungssystemen (SzA), 2-jährliche Audits, detaillierte Dokumentation [11]
ISA/IEC 62443	International (IACS)	Cybersicherheit für industrielle Automatisierungs- und Steuerungssysteme	Empfohlen, oft de facto verpflichtend [30]	Netzwerksegmentierung, Zugriffssteuerung, Sicherheitsüberwachung, Risikobewertung, Security Levels (SL1-SL4) [30]
NIST Cybersecurity Framework (CSF)	International (Allgemein)	Allgemeiner Rahmen für Cybersicherheits-risikomanagement	Freiwillig, aber weit verbreitet [30]	Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen; risikobasierter Ansatz [30]

5. Technische Realisierung sicherer IT/OT-Architekturen

Die sichere Anbindung von OT-Anlagen an das Internet erfordert durchdachte technische Architekturen, die die spezifischen Anforderungen und Risiken von Industriesteuerungssystemen berücksichtigen.

5.1 Architekturmuster für IT/OT-Netzwerksegmentierung

- **Industrielle DMZ (iDMZ) mit Dual-Firewalls:**
  Eine industrielle DMZ (iDMZ) ist entscheidend für die Trennung von IT- und OT-Netzwerken, um Cyberangriffe daran zu hindern, zwischen diesen Bereichen zu wechseln.[13] Sie fungiert als Pufferzone zwischen zwei Firewalls (einer "Front-Firewall" zur IT und einer "Back-Firewall" zur OT), die Geräte beherbergt, die mit beiden Netzwerken interagieren (z.B. Datenhistoriker, Datenprotokollierungsserver, Gateways).[13] Dieses Konzept entspricht den Empfehlungen der IEC 62443 für Netzwerksegmentierung (dem "Zones & Conduits"-Modell).[13]

- **Mikro-Segmentierung und Jump Hosts:**
  Mikro-Segmentierung beinhaltet die Unterteilung des OT-Netzwerks in kleinere, isolierte Funktionszonen, um Sicherheitsverletzungen einzudämmen und die Angriffsfläche zu reduzieren.[10] Die Regeln für die Mikro-Segmentierung werden von OT-Firewalls durchgesetzt.[13] Jump Hosts bieten einen einzigen, kontrollierten Zugangspunkt zum OT-Netzwerk, der Authentifizierung und Autorisierung erfordert und so direkte Zugriffe minimiert.[13] Benutzer verbinden sich zuerst mit dem IT-Netzwerk, dann mit dem Jump Host und schließlich über die iDMZ mit dem OT-Netzwerk.[13] Die Entwicklung von perimeterbasierten Firewalls hin zu iDMZs, Mikro-Segmentierung und Jump Hosts spiegelt eine Evolution hin zu einem Zero-Trust-Sicherheitsmodell in KRITIS wider, bei dem keiner Entität von Natur aus vertraut wird. Traditionelle Sicherheit konzentrierte sich auf einen starken Perimeter (eine einzige Firewall). Mit der IT/OT-Konvergenz wird der Perimeter jedoch durchlässig.[5] Die Einführung von iDMZs mit Dual-Firewalls[13]

bedeutet einen Übergang zu einer mehrschichtigen Verteidigung. Mikro-Segmentierung[10] verfeinert dies weiter, indem interne Netzwerksegmente isoliert werden, was die laterale Bewegung von Bedrohungen einschränkt. Jump Hosts[13] erzwingen eine strenge Zugriffssteuerung auf kritische Zonen. Dieser mehrschichtige Ansatz, bei dem jede Verbindung und jeder Benutzer unabhängig von ihrem Standort innerhalb des Netzwerks authentifiziert und autorisiert wird, stimmt perfekt mit den Prinzipien von Zero Trust überein. Es ist eine proaktive Anerkennung, dass Sicherheitsverletzungen auftreten werden, und der Fokus verlagert sich darauf, sie einzudämmen und ihre Auswirkungen zu minimieren.

- **Rolle von Daten-Dioden für unidirektionalen Datenfluss:**
  Daten-Dioden sind hardwarebasierte Cybersicherheitsbarrieren, die einen unidirektionalen Datenfluss erzwingen.[36] Daten können physikalisch nur in eine Richtung von einem Netzwerk zum anderen übertragen werden, ohne die Möglichkeit eines Rückkanals.[36] Dies ist entscheidend, um sensible Systeme vollständig von externen Bedrohungen zu isolieren und Angriffsvektoren wie Malware-Injektion oder Datenexfiltration zu eliminieren.[36] Sie sind ideal für ICS/SCADA-Netzwerke, wo strenge Isolation von größter Bedeutung ist, da sie den sicheren Export von Überwachungsdaten ermöglichen, ohne Steuerungssysteme offenzulegen.[36] Daten-Dioden tragen zur Erfüllung von Anforderungen in Standards wie ISO 27001, NIST, NERC CIP und IEC 62443 bei, indem sie eine physikalische Netzwerksegmentierung erzwingen.[36] Daten-Dioden stellen die ultimative physische Durchsetzung der Datenflusskontrolle dar und bieten eine unvergleichliche Sicherheit für den Export hochsensibler OT-Daten. Ihre unidirektionale Natur verdeutlicht jedoch die anhaltende Herausforderung, Sicherheit mit bidirektionalen Kommunikationsanforderungen in Einklang zu bringen. Während Firewalls und Proxys den Datenverkehr filtern, verhindern Daten-Dioden physisch jeden Rückkanal.[36] Diese hardwareerzwungene Unidirektionalität bietet das höchste Maß an Sicherheit gegen eingehende Angriffe und Datenexfiltration, was sie ideal für die Spiegelung kritischer Daten von OT nach IT macht.[36] Diese Strenge bedeutet jedoch, dass sie keine Anwendungen unterstützen können, die eine Zwei-Wege-Kommunikation erfordern.[36] Diese Einschränkung zwingt Organisationen dazu, sorgfältig abzuwägen, wo eine solche extreme Isolation notwendig ist, und wo flexiblere, wenn auch weniger absolute Sicherheitsmaßnahmen

(wie Layer-7-Proxys) akzeptabel sind. Es unterstreicht, dass es keine einzige "perfekte" Sicherheitslösung gibt; vielmehr ist eine Kombination von Tools erforderlich, die auf spezifische Kommunikationsbedürfnisse und Risikoprofile zugeschnitten sind.
Hier sind allerdings Lösungen wie der SCADA-Proxy der OKIT eine Ausnahme, da sie beispielsweise auch in bidirektionalen Kommunikationen wie IEC 60870-5-104 sicher stellen können, dass Informationen oder Kommandos nur in eine gewollte Richtung fließen, während protokollbedingte bidirektionale Kommunikation (Acknowledgements, Test-Telegramme etc.) weiterhin möglich ist. Dies ist die bestmögliche Annäherung an eine physikalische Datendiode.

5.2 Integration von Layer 7 Proxy-Servern, DPI und IDS/IPS

- Funktionsweise und Vorteile im Kontext der IT/OT-Sicherheit:

  - **Layer 7 Proxy:**
    Operiert auf der Anwendungsschicht des OSI-Modells und inspiziert den tatsächlichen Inhalt der Daten.[15] Er kann Daten manipulieren, spezifische Aktionen ausführen und den Datenverkehr basierend auf Inhalten (z.B. URLs, HTTP-Headern) routen.[15] Zudem bietet er erweiterte Sicherheitsfunktionen wie die Integration von Web Application Firewalls (WAF) und SSL-Entschlüsselung.[15]

  - **Deep Packet Inspection (DPI):**
    Inspiziert Daten über Layer 3 des OSI-Modells hinaus, einschließlich Header und Nutzlast.[18] DPI wird zur Basislinienbestimmung des Anwendungsverhaltens, zur Analyse der Netzwerknutzung, zur Überprüfung auf bösartigen Code und zur Identifizierung von Protokollverletzungen eingesetzt.[18] Sie kann den Datenverkehr basierend auf Signaturdatenbanken oder Protokollanomalien identifizieren und klassifizieren.[18]

  - **IDS/IPS:**
    Intrusion Detection Systems (IDS) erkennen verdächtige Aktivitäten, während Intrusion Prevention Systems (IPS) erkannte Angriffe in Echtzeit blockieren können.[18] Sie werden oft mit DPI kombiniert, um Angriffe zu erkennen, die keines

der Systeme allein erfassen könnte.[18] IDS/IPS erkennen primär "unerwünschtes Verhalten" oder "Angriffe" mittels Signaturen, während L7-Firewalls definieren, welches Verhalten erlaubt ist.[20] Layer-7-Proxys mit integriertem DPI und IDS/IPS sind unerlässlich, um die "Protokolllücke" zwischen IT und OT zu schließen und granulare Sicherheitsrichtlinien sowie Anomalieerkennung für Industrieprotokolle zu ermöglichen. Traditionelle Firewalls arbeiten auf unteren OSI-Schichten (L3/L4) und konzentrieren sich auf IP-Adressen und Ports. OT-Bedrohungen nutzen jedoch oft Schwachstellen innerhalb der Anwendungsschicht industrieller Protokolle aus.[5] Layer-7-Proxys können durch die Überprüfung des Inhalts von Paketen (DPI) und das Verständnis von Anwendungsprotokollen bösartige Befehle oder anomales Verhalten identifizieren, die eine Firewall auf niedrigerer Ebene übersehen würde.18 Diese Fähigkeit, Modbus-, DNP3- oder IEC 61850-Befehle zu "verstehen", ermöglicht eine feingranulare Kontrolle (Whitelisting spezifischer Befehle) und Echtzeit-Anomalieerkennung, was für den Schutz der Integrität und Verfügbarkeit von OT-Systemen entscheidend ist. Dies adressiert direkt die Schwäche spezialisierter OT-Protokolle, die keine inhärenten Sicherheitsfunktionen besitzen.[5]

- **Platzierung in der Architektur:**
  Layer-7-Proxys werden typischerweise an der Grenze zwischen Netzwerken (z.B. IT und OT innerhalb einer iDMZ) platziert, um den Datenverkehr zwischen verschiedenen Vertrauenszonen zu inspizieren.[13] Sie fungieren als Vermittler und verhindern den direkten Kontakt zwischen externen und internen Netzwerken.[39] Die Implementierung kann als Hardware-Appliance oder als Software (z.B. Nginx, HAProxy) erfolgen.[38]

5.3 Sichere Anbindungstechnologien

- **Mobilfunk (z.B. 450 MHz Netz) und VPN-Verbindungen:**
  Das 450-MHz-Funknetz ist speziell für KRITIS konzipiert und bietet eine zuverlässige, flächendeckende und ausfallsichere Kommunikationslösung für Energie- und Wasserversorger.[7] Es ermöglicht eine gute Gebäudedurchdringung für intelligente Messsysteme und eine stabile Kommunikation in Krisensituationen.[7] Geräte für das 450-MHz-Netz sind mit Sicherheitsfunktionen wie IPsec- oder OpenVPN-Tunneln und integrierten Firewalls ausgestattet.[7] Die Mobilfunk-Redundanz gewährleistet

unterbrechungsfreie Verbindungen.[7] Das dedizierte 450-MHz-Netz für KRITIS in Deutschland signalisiert eine strategische nationale Investition in eine sichere, resiliente Kommunikationsinfrastruktur, die allgemeine Internetrisiken für kritische Remote-Assets mindert. Während allgemeine Mobilfunknetze (z.B. 5G) Konnektivität bieten, unterliegen sie breiteren Internetbedrohungen und potenziellen Überlastungen. Die Einrichtung eines dedizierten 450-MHz-Netzes für KRITIS[7] erkennt die einzigartigen Sicherheits- und Verfügbarkeitsanforderungen kritischer Infrastrukturen an. Dieses spezialisierte Netz, mit seinem Fokus auf robuster Gebäudedurchdringung, Krisenkommunikationsfähigkeiten und integrierten Sicherheitsfunktionen wie VPNs auf Geräteebene, bietet ein kontrollierteres und widerstandsfähigeres Kommunikationsrückgrat im Vergleich zur ausschließlichen Nutzung des öffentlichen Internets. Es reduziert die Angriffsfläche, indem es einen semi-privaten, zweckgebundenen Kanal bereitstellt, was ein erheblicher Vorteil für die Sicherung verteilter OT-Anlagen ist.

- **Sicherheitsmerkmale von MQTT und SparkplugB (TLS, Birth/Death Certificates):**
  MQTT ist ein leichtgewichtiges Publish/Subscribe-Protokoll, das im IIoT für effiziente Datenübertragung weit verbreitet ist.[40] SparkplugB ist ein Interoperabilitätsprotokoll, das auf MQTT aufbaut und Daten Kontext hinzufügt sowie einen standardisierten Topic-Namespace und eine Payload-Definition für das IIoT festlegt.[40] Sicherheitsmerkmale: Sparkplug ist vollständig gesichert, erfordert keine offenen Ports für neue Geräte und schreibt TLS für den gesamten Datentransport vor.[40] Kontinuierliche Sitzungsüberwachung: Sparkplug und MQTT bieten eine Echtzeit-Online-/Offline-Statusanzeige von Geräten durch "Birth"- und "Death"-Zertifikate (unter Verwendung des MQTT Last Will and Testament-Mechanismus), was für die betriebliche Situationswahrnehmung und Datenintegrität in IIoT-Implementierungen entscheidend ist.[41] Report by Exception: Daten werden nur gesendet, wenn sie sich ändern, was Bandbreite und Rechenleistung spart.[41] Auto-Discovery: Anwendungen und Geräte können Daten und Topics automatisch erkennen, was die Integration vereinfacht.[41] Die Kombination aus MQTTs Effizienz und SparkplugBs Kontextualisierung und Zustandsmanagement (Birth/Death Certificates) bietet eine robuste und von Natur aus sicherere Datentransportschicht für IIoT in KRITIS im Vergleich zu traditionellen

Poll/Response-Mechanismen. Traditionelle Industrieprotokolle basieren oft auf Poll/Response, was ineffizient ist und keine inhärenten Sicherheitsfunktionen bietet. Das Publish/Subscribe-Modell von MQTT ist effizienter, aber rohen MQTT-Daten fehlt der Kontext. SparkplugB begegnet dem, indem es ein standardisiertes Datenmodell, einen Topic-Namespace und vor allem "Birth"- und "Death"-Zertifikate hinzufügt.[40] Diese Zertifikate bieten eine Echtzeit-Gerätezustandserkennung, die für die Aufrechterhaltung der Betriebsführung und die schnelle Identifizierung getrennter oder kompromittierter Geräte in kritischen Infrastrukturen unerlässlich ist. Die Vorschrift von TLS[40] sorgt für Verschlüsselung und adressiert eine wesentliche Schwachstelle vieler älterer OT-Protokolle.[5] Diese Kombination schafft eine widerstandsfähigere, effizientere und von Natur aus sicherere Datenarchitektur für das IIoT, wodurch das Risiko von Datenintegritätsproblemen reduziert und die Situationswahrnehmung verbessert wird.

6. Bewertung des OKIT SCADA-Proxy in der KRITIS-Architektur

Der OKIT SCADA-Proxy ist ein Anwendungsschicht-Gateway (Layer 7) mit Deep Packet Inspection (DPI) und einem Protokollkonverter, der speziell für die Cybersicherheit in industriellen Anwendungen und für die rechnergestützte Messdatenverarbeitung und Sensorik entwickelt wurde.[23]

6.1 Funktionen und Spezifikationen

- **IEC-60870 Gateway, SCADA-Firewall mit Deep Packet Inspection (Layer 7):**
  Der SCADA-Proxy fungiert als Anwendungsschicht-Gateway (Layer 7) mit DPI für die Plausibilitätsprüfung übertragener Daten.[23] Er agiert als SCADA-Firewall, die eine präzise Definition und Filterung von Datenpunkten/Datenobjekten und deren Inhalten ermöglicht.[23]

- **Anomalie-Detektion in Echtzeit und Protokollkonvertierung:**
  Das System bietet Echtzeit-Anomalieerkennung.[23] Es ist ein flexibler Protokollkonverter, der zwischen verschiedenen Feldbus-, SCADA- und IT-Protokollen vermittelt.[23] Dies umfasst die Konvertierung, das Routing und die Verteilung von Datenströmen.[23]

- **Unterstützte SCADA- und IT-Schnittstellen:**
  Der SCADA-Proxy bietet eine umfassende Unterstützung für Industrieprotokolle wie IEC 60870-5.104/101, IEC 61850, DNP3, MQTT, Modbus sowie Anbindungen an WAGO-, Beckhoff- und Phoenix-Contact-Knoten.[23] Zudem unterstützt er eine breite Palette von IT-Schnittstellen, darunter Datenbanken (JDBC/ODBC, Cassandra, InfluxDB, SAP HANA), REST (XML/JSON), WITSML, SFTP/SCP/FTP, CSV/XLS/JSON/TXT und Icinga/Nagios.[23] Die breite native Unterstützung des OKIT SCADA-Proxy für sowohl ältere OT- als auch moderne IT/IIoT-Protokolle ist ein entscheidender Faktor für eine sichere IT/OT-Konvergenz, da sie die Notwendigkeit mehrerer, komplexer Punktlösungen reduziert. Eine große Herausforderung bei der IT/OT-Konvergenz ist die unterschiedliche Natur der

Protokolle.[5] Ältere OT-Systeme verwenden oft unsichere Protokolle, während moderne IT/IIoT-Systeme andere Standards wie MQTT/SparkplugB verwenden.[40] Die Fähigkeit des SCADA-Proxy, eine Vielzahl dieser Protokolle nativ zu unterstützen[23], bedeutet, dass er als einziger, zentraler Übersetzungs- und Sicherheitspunkt fungieren kann. Dies vereinfacht die Architektur, reduziert die Komplexität der Integration und minimiert die Angriffsfläche, die sonst durch mehrere Protokollkonverter oder Gateways mit jeweils eigenen Schwachstellen und Verwaltungsaufwand entstehen würde. Es adressiert direkt die Herausforderung der "Protokollkompatibilität" für Layer-7-Proxys.

6.2 Eignung für die Anforderungen

- **Beitrag zur IT/OT-Isolation und Einhaltung von BDEW-Empfehlungen:**
  Der SCADA-Proxy ist explizit für die IT/OT-Integration konzipiert und gewährleistet die Datensicherheit in kritischen Infrastrukturen durch die Isolation und Kopplung von Netzwerkinfrastrukturen gemäß den BDEW-Empfehlungen.[42] Er fungiert als inhaltsbasierte Firewall zwischen Netzwerken, die die Echtzeit-Datenübertragung an unterschiedliche oder weniger sichere Netzwerke ohne Kompromittierung ermöglicht.[23] Das System ist als gehärtetes Application-Layer-Gateway verfügbar.[23]

- **Kompatibilität mit den genannten Technologien und Use Cases:**
  Der SCADA-Proxy unterstützt direkt MQTT[23], was die Grundlage für SparkplugB bildet.[40] Seine Anwendungsbereiche umfassen Kurzschlussanzeiger, Redispatch 2.0 und allgemeines Netzmonitoring.[42] Seine Fähigkeiten zur Messdatenerfassung, -vorverarbeitung, -filterung und Echtzeit-Anomalieerkennung[42] unterstützen direkt die identifizierten aktuellen und zukünftigen IIoT-Anwendungsfälle.4

- **Potenzial zur Risikominimierung und Effizienzsteigerung:**

  - **Risikominimierung:**
    Die Deep Packet Inspection ermöglicht Plausibilitätsprüfungen übertragener Daten und die Echtzeit-Erkennung von Anomalien, was entscheidend ist, um Risiken durch spezialisierte OT-Protokolle zu mindern.[23] Seine Funktion als SCADA-Firewall mit granularer Filterung verbessert die Sicherheitsposition.

- **Effizienzsteigerung:**
  Der SCADA-Proxy konsolidiert viele Gegenstellen, Protokolle und Formate in eine einheitliche Datenpunkt-basierte SCADA-Gegenstelle.[42] Er vereinfacht den Betrieb in verteilten Systemen und ermöglicht sichere Verbindungen über Netz- und Organisationsgrenzen hinweg, die sonst nur mit aufwendigen und teuren Integrationslösungen umgesetzt werden könnten.[23] Die Fähigkeit des OKIT SCADA-Proxy, verschiedene Protokolle zu konsolidieren und Layer-7-Sicherheit mit Anomalieerkennung zu bieten, positioniert ihn als zentrale Instanz zur Durchsetzung der Datenintegrität und der operativen Resilienz an der IT/OT-Schnittstelle. Durch die Konsolidierung verschiedener OT- und IT-Protokolle[23] fungiert der SCADA-Proxy als einziger Kontroll- und Inspektionspunkt. Diese Zentralisierung, kombiniert mit seiner Layer-7-DPI und Echtzeit-Anomalieerkennung[23], bedeutet, dass er den Datenverkehr nicht nur auf der Grundlage des Inhalts filtern, sondern auch Abweichungen von normalen Betriebsmustern identifizieren kann. Dies ist entscheidend, um Datenintegritätsangriffe (z.B. Manipulation von Sensorwerten) zu verhindern und die Verfügbarkeit von Steuerungssystemen durch das Blockieren bösartiger Befehle zu gewährleisten. Seine Einhaltung der BDEW-Empfehlungen zur Netzwerkisolation stärkt die allgemeine Resilienz zusätzlich und macht ihn zu einer Schlüsselkomponente in einer Defense-in-Depth-Strategie für KRITIS.

Tabelle: OKIT SCADA-Proxy: Funktionen und Eignung für KRITIS

Funktion/Merkmal	**Spezifikation (OKIT SCADA-Proxy)**	**Relevanz für KRITIS/IT/OT-Konvergenz**
Layer 7 DPI (Deep Packet Inspection)	Plausibilitätsprüfung übertragener Daten auf Anwendungsebene [23]	Ermöglicht granulare Sicherheitskontrolle und Erkennung komplexer Angriffe innerhalb industrieller Protokolle; Schutz vor Manipulation von Steuerbefehlen.
Protokollkonvertierung	Vermittlung zwischen IEC 60870-5.104/101, IEC 61850, DNP3, MQTT, Modbus, etc. sowie IT-Protokollen (REST, Datenbanken) [23]	Überbrückt die Protokolllücke zwischen IT und OT; ermöglicht Integration von Legacy-Systemen in moderne IIoT-Architekturen; reduziert Komplexität und Kosten.
Anomalie-Detektion in Echtzeit	Erkennung ungewöhnlicher Kommunikationsmuster und Verhaltensweisen [23]	Frühzeitige Erkennung von Cyberangriffen, die legitime Systemfunktionen missbrauchen; Schutz vor unbekannten Bedrohungen und Zero-Day-Exploits.
Unterstützte Protokolle (Beispiele)	IEC 60870-5.104, MQTT, Modbus, DNP3, REST, Datenbanken [23]	Hohe Kompatibilität mit bestehenden und zukünftigen KRITIS-Anlagen; breite Anwendbarkeit für diverse Use Cases (z.B. Kurzschlussanzeiger, Redispatch 2.0).
IT/OT-Isolation (BDEW-konform)	Isolation und Kopplung von Netzwerkinfrastrukturen gemäß BDEW-Empfehlungen [42]	Stellt eine sichere Trennung zwischen IT- und OT-Netzen her; verhindert laterale Bewegung von Bedrohungen; erfüllt regulatorische Anforderungen.
Datenpunkt-basierte Filterung	Exakte Definition der durchgeleiteten Datenpunkte und Inhalte [23]	Ermöglicht präzise Zugriffssteuerung auf kritische Prozessdaten; minimiert die

Funktion/Merkmal	Spezifikation (OKIT SCADA-Proxy)	Relevanz für KRITIS/IT/OT-Konvergenz
		Angriffsfläche durch Whitelisting.
Skalierbarkeit und Redundanz	Skalierbar von Single-Board-Computern bis zu virtualisierten Servern; unterstützt redundante Installationen [23]	Gewährleistet hohe Verfügbarkeit und Ausfallsicherheit, entscheidend für KRITIS-Betrieb.

7. Fazit und Handlungsempfehlungen

Zusammenfassung der zentralen Erkenntnisse zur Absicherung internetangebundener OT-Anlagen

Die digitale Transformation kritischer Infrastrukturen (KRITIS) durch die Anbindung von Betriebstechnologie (OT) an das Internet bietet zwar enorme Vorteile, verändert aber grundlegend die Cybersicherheitslandschaft. Ehemals isolierte OT-Systeme sind nun ausgeklügelten Bedrohungen ausgesetzt. Die inhärenten Unterschiede zwischen IT und OT, insbesondere hinsichtlich Systemlebenszyklen, Echtzeitanforderungen und spezialisierten Protokollen, erfordern spezialisierte Sicherheitsansätze. Die Einhaltung nationaler (IT-Sicherheitsgesetz 2.0, BSI-KritisV) und internationaler (IEC 62443, NIST CSF) Standards ist zwingend erforderlich und zieht bei Nichteinhaltung erhebliche rechtliche und finanzielle Konsequenzen nach sich. Layer-7-Proxys mit DPI und IDS/IPS sind für die Deep Packet Inspection und die Sicherheit auf Anwendungsebene an der IT/OT-Schnittstelle unerlässlich, trotz der Herausforderungen in Bezug auf Leistung und Kompatibilität. Technologien wie das 450-MHz-Netz und MQTT/SparkplugB bieten sichere und effiziente Datenkommunikationswege. Der OKIT SCADA-Proxy ist eine hochrelevante Lösung, die viele dieser Herausforderungen direkt adressiert, indem er ein robustes Anwendungsschicht-Gateway, umfassende Protokollunterstützung und integrierte Sicherheitsfunktionen bietet, die auf industrielle Umgebungen zugeschnitten sind.

Konkrete Empfehlungen für KRITIS-Betreiber zur Implementierung und Aufrechterhaltung robuster Cybersicherheitsmaßnahmen

Um die Resilienz kritischer Infrastrukturen in der Ära der IT/OT-Konvergenz zu gewährleisten, werden folgende konkrete Handlungsempfehlungen für KRITIS-Betreiber abgeleitet:

- **Verfolgung einer mehrschichtigen Verteidigungsstrategie (Defense-in-Depth):**

KRITIS-Betreiber sollten mehrere Sicherheitsebenen implementieren, da keine einzelne Maßnahme ausreicht. Dies umfasst physische Sicherheit, Netzwerksicherheit und Systemintegrität.[13]

- **Priorisierung der Netzwerksegmentierung:**
  Eine industrielle DMZ (iDMZ) mit Dual-Firewalls zwischen IT- und OT-Netzwerken sollte implementiert und die OT-Umgebung zusätzlich in funktionale Zonen mikrosegmentiert werden. Dies begrenzt die laterale Bewegung von Bedrohungen erheblich.[10]

- **Implementierung von Anwendungsschicht-Sicherheit:**
  Layer-7-Proxys mit DPI- und IDS/IPS-Funktionen sind an der IT/OT-Schnittstelle einzusetzen, um den Datenverkehr auf Anwendungsebene zu inspizieren und zu kontrollieren, insbesondere für Industrieprotokolle. Lösungen wie der OKIT SCADA-Proxy sind für diese Rolle aufgrund ihrer nativen Protokollunterstützung und ihrer Deep-Inspection-Funktionen besonders gut geeignet.[20]

- **Sichere Fernzugriffe gestalten:**
  Jump Hosts und starke Authentifizierungsmechanismen (z.B. Multi-Faktor-Authentifizierung) sind für alle Fernzugriffe auf OT-Systeme zu implementieren, unter Einhaltung des Prinzips der geringsten Privilegien.[3]

- **Umfassendes Asset Management und Transparenz gewährleisten:**
  Ein präzises und aktuelles Inventar aller IT- und OT-Assets, einschließlich ihrer Schwachstellen und Konfigurationen, ist zu führen. Dies ist die Grundlage für ein effektives Risikomanagement und eine zuverlässige Bedrohungserkennung.[6]

- **Kontinuierliche Überwachung und Anomalieerkennung implementieren:**
  Spezialisierte, OT-fähige Überwachungstools und Security Information and Event Management (SIEM)-Systeme sind einzusetzen, um ungewöhnliche Kommunikationsmuster und Verhaltensweisen in Echtzeit zu erkennen, da traditionelle signaturbasierte Erkennung möglicherweise nicht ausreicht.[5]

- **Einhaltung regulatorischer Vorschriften:**

Eine rigorose Einhaltung des IT-Sicherheitsgesetzes 2.0, der BSI-KritisV und internationaler Standards wie IEC 62443 ist unerlässlich. Dies beinhaltet die Durchführung regelmäßiger Audits, die Pflege detaillierter Dokumentationen und die Erfüllung von Meldepflichten bei Sicherheitsvorfällen.[11]

- **Investition in spezialisierte OT-Sicherheitslösungen:**
  Es ist zu erkennen, dass generische IT-Sicherheitstools für OT-Umgebungen möglicherweise nicht ausreichend sind. Lösungen, die speziell für industrielle Steuerungssysteme entwickelt wurden und deren einzigartige Eigenschaften und Protokolle berücksichtigen, sind zu priorisieren.[5]

- **Entwicklung von Incident Response und Wiederherstellungsplänen:**
  Robuste Pläne für die Geschäftskontinuität und Notfallwiederherstellung sind zu erstellen, einschließlich der Fähigkeit, OT-Systeme im Falle eines Cyberangriffs manuell zu betreiben.[13]

- **Förderung der IT/OT-Zusammenarbeit:**
  Silos zwischen IT- und OT-Teams sind aufzubrechen, um ein gemeinsames Verständnis, gemeinsame Verantwortlichkeiten und kollaborative Sicherheitsbemühungen zu fördern.[6]

Referenzen

1. Kritische Infrastruktur (KRITIS): Definition & Richtlinien | IoT Telekom, Zugriff am Mai 22, 2025, https://iot.telekom.com/de/blog/kritische-infrastrukturen-schutz-pflichten-und-betroffene-unternehmen

2. IT-Sicherheitsgesetz für Kritis umsetzen - Telekom Public, Zugriff am Mai 22, 2025, https://public.telekom.de/digitalisierungsloesungen/oeffentliche-verwaltung/kritis-sicherung

3. Securing Industry 4.0: Protecting Critical Infrastructure in the Age of IT/OT Convergence, Zugriff am Mai 22, 2025, https://www.wallix.com/securing-critical-infrastructure-for-it-ot-convergence/

4. Kritische Infrastruktur (KRITIS) | IoT Use Case, Zugriff am Mai 22, 2025, https://iotusecase.com/de/funktionsbereiche/kritis/

5. IT-OT-Konvergenz: Die unsichtbare Gefahr für ..., Zugriff am Mai 22, 2025, https://www.strom.ch/de/perspective/it-ot-konvergenz-die-unsichtbare-gefahr-fuer-energieversorgungsunternehmen

6. Was ist unter OT-Sicherheit und IT/OT-Konvergenz zu verstehen ..., Zugriff am Mai 22, 2025, https://de.tenable.com/source/operational-technology

7. 450 MHz - Frequenz für kritische Infrastrukturen - MC Technologies, Zugriff am Mai 22, 2025, https://mc-technologies.com/450mhz/

8. What Is Industrial IoT (IIoT)? Use Cases & Benefits, Zugriff am Mai 22, 2025, https://www.appventurez.com/blog/what-is-industrial-iot

9. 10 Use Cases, Examples, and Applications of IIoT Technology - Appinventiv, Zugriff am Mai 22, 2025, https://appinventiv.com/blog/application-of-iiot/

10. The Top 8 IT/OT/IoT Security Challenges and How to Solve Them | Balbix, Zugriff am Mai 22, 2025, https://www.balbix.com/insights/addressing-iot-security-challenges/

11. BSI KRITIS Regulation: Requirements and IT Security - Docusnap, Zugriff am Mai 22, 2025, https://www.docusnap.com/en/it-documentation/bsi-kritis-regulation-the-german-it-security-act

12. What is Operational Technology (OT)? Challenges & Best Practices - SentinelOne, Zugriff am Mai 22, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/operational-technology/

13. Core architecture strategies for IT/OT network integration - Control ..., Zugriff am Mai 22, 2025, https://www.controleng.com/core-architecture-strategies-for-it-ot-network-integration/

14. Primary Mitigations to Reduce Cyber Threats to Operational Technology | CISA, Zugriff am Mai 22, 2025, https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

15. Layer 4 vs Layer 7 Load Balancing: Which Should I Choose? - Cloudways, Zugriff am Mai 22, 2025, https://www.cloudways.com/blog/layer-4-vs-layer-7-load-balancing/

16. Understanding and Troubleshooting High Latency in Proxy Servers and Web Scraping, Zugriff am Mai 22, 2025, https://www.bomberbot.com/proxy/understanding-and-troubleshooting-high-latency-in-proxy-servers-and-web-scraping/

17. What is a Proxy Firewall? | NordLayer Learn, Zugriff am Mai 22, 2025, https://nordlayer.com/learn/firewall/proxy/

18. Deep packet inspection - Wikipedia, Zugriff am Mai 22, 2025, https://en.wikipedia.org/wiki/Deep_packet_inspection

19. What is Deep Packet Inspection? (And How it Really Works) | Fortra's Digital Guardian, Zugriff am Mai 22, 2025, https://www.digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

20. Difference between Layer 7 FW (DPI) vs IPS : r/networking - Reddit, Zugriff am Mai 22, 2025, https://www.reddit.com/r/networking/comments/1ajmog8/difference_between_layer_7_fw_dpi_vs_ips/

21. What is L4 / L7 Proxy and How it Works? - Tencent EdgeOne, Zugriff am Mai 22, 2025, https://edgeone.ai/learning/l4-l7-proxy

22. l7mp/l7mp: L7mp: A L7 multiprotocol proxy and service mesh - GitHub, Zugriff am Mai

22, 2025, https://github.com/l7mp/l7mp

23. SCADA-Proxy – Netzwerksicherheit in beliebigen SCADA ..., Zugriff am Mai 22, 2025, https://www.scada-proxy.de/

24. Exposure Management for Operational Technology - XM Cyber, Zugriff am Mai 22, 2025, https://xmcyber.com/use-case/operational-technology/

25. KRITIS - IT security in critical infrastructures - Enginsight, Zugriff am Mai 22, 2025, https://enginsight.com/en/kritis-cybersecurity-for-critical-infrastructure/

26. Cybersecurity Laws and Regulations in Germany | UpGuard, Zugriff am Mai 22, 2025, https://www.upguard.com/blog/cybersecurity-laws-and-regulations-germany

27. The German IT Security Act 2.0 - BSI, Zugriff am Mai 22, 2025, https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig-2-0_node.html

28. The Cost of Non-Compliance: Real-World Consequences of Ignoring Cybersecurity Regulations | SecOps® Solution, Zugriff am Mai 22, 2025, https://www.secopsolution.com/blog/the-cost-of-non-compliance-real-world-consequences-of-ignoring-cybersecurity-regulations

29. EU NIS 2 and RCE Directives for EU Critical Infrastructures - OpenKRITIS, Zugriff am Mai 22, 2025, https://www.openkritis.de/eu/eu-nis-2-rce-directive.html

30. Mapping ISA/IEC 62443 to NIST Cybersecurity Framework (CSF ..., Zugriff am Mai 22,

2025, https://iotsecurityinstitute.com/iotsec/index.php/iot-security-institute-blog/97-mapping-isa-iec-62443-to-nist-cybersecurity-framework-csf

31. What is the difference between NIST and IEC 62443? | Answers - 6clicks, Zugriff am Mai 22, 2025, https://www.6clicks.com/resources/answers/what-is-the-difference-between-nist-and-iec-62443

32. IEC 62443 explained | isecjobs.com, Zugriff am Mai 22, 2025, https://infosec-jobs.com/insights/iec-62443-explained/

33. Cybersecurity regulations IEC 62443 & ISO 27001: FAQ with OT security experts, Zugriff am Mai 22, 2025, https://www.ssh.com/blog/cybersecurity-regulations-iec-62443-and-iso-27001-faq-with-ot-security-experts

34. What is a DMZ Network? - Check Point Software, Zugriff am Mai 22, 2025, https://www.checkpoint.com/cyber-hub/network-security/what-is-a-dmz-network/

35. Industrial DMZ Infrastructure - Siemens Global, Zugriff am Mai 22, 2025, https://www.siemens.com/global/en/products/services/digital-enterprise-services/industrial-security-services/idmz.html

36. What is a Data Diode? - OPSWAT, Zugriff am Mai 22, 2025, https://www.opswat.com/blog/data-diodes

37. Defense in Depth: The Critical Role of Data Diodes in Government Industrial Control Systems - MeriTalk, Zugriff am Mai 22, 2025,

https://www.meritalk.com/articles/defense-in-depth-the-critical-role-of-data-diodes-in-government-industrial-control-systems/

38. Layer 4 and Layer 7 proxy setup - Teamwork Cloud and Services 2024x - Documentation, Zugriff am Mai 22, 2025, https://docs.nomagic.com/display/TWCloud2024x/Layer+4+and+Layer+7+proxy+setup

39. What Is a Perimeter Firewall? - Palo Alto Networks, Zugriff am Mai 22, 2025, https://www.paloaltonetworks.com/cyberpedia/what-is-a-perimeter-firewall

40. MQTT Sparkplug: Building Powerful Industrial IoT Systems - HiveMQ, Zugriff am Mai 22, 2025, https://www.hivemq.com/solutions/technology/mqtt-sparkplug/

41. MQTT Sparkplug Architecture - HiveMQ, Zugriff am Mai 22, 2025, https://www.hivemq.com/blog/sparkplug-essentials-part-2-architecture/

42. Anwendungsfälle – SCADA-Proxy, Zugriff am Mai 22, 2025, https://www.scada-proxy.de/anwendungsfaelle/

43. Protecting OT and Critical Infrastructure in an Evolving Threat Landscape | CDW, Zugriff am Mai 22, 2025, https://www.cdw.com/content/cdw/en/articles/security/protecting-ot-and-critical-infrastructure-in-an-evolving-threat-landscape.html

44. CISA, FBI, EPA, DOE issue joint alert on rising cyber threats to critical infrastructure OT systems, Zugriff am Mai 22, 2025, https://industrialcyber.co/cisa/cisa-fbi-epa-

doe-issue-joint-alert-on-rising-cyber-threats-to-critical-infrastructure-ot-systems/