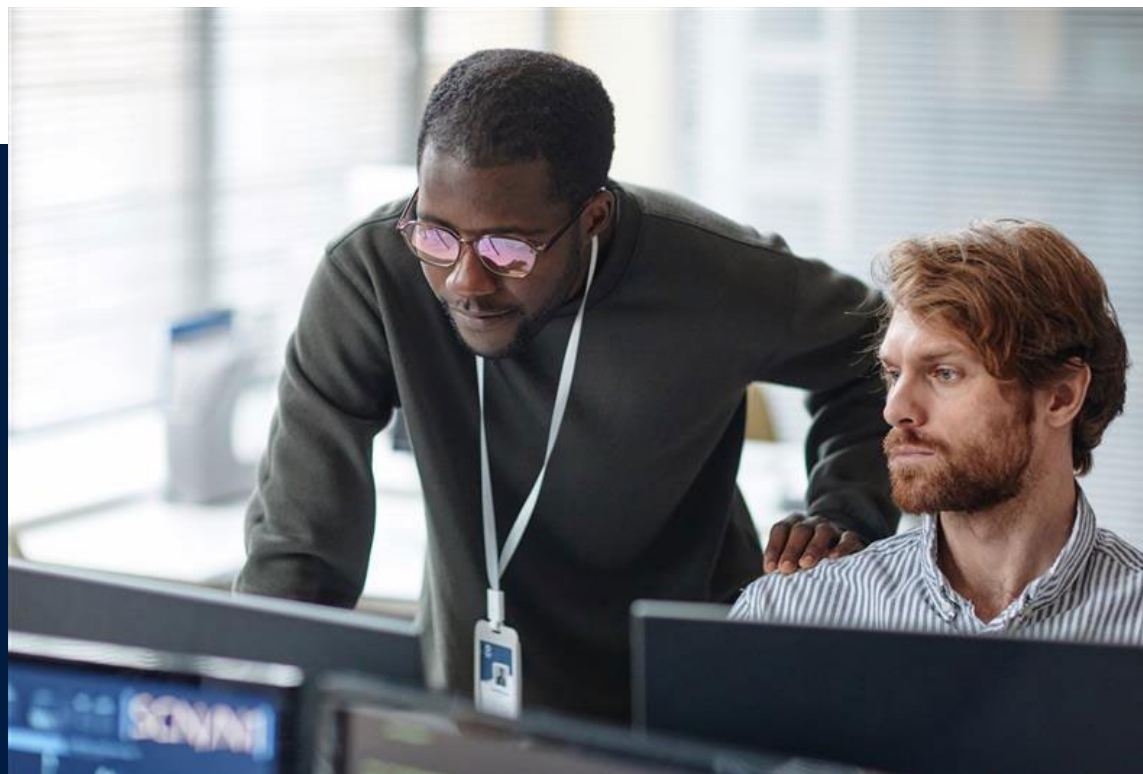




LANCOM
SYSTEMS

Whitepaper

Sichere IT-Netzwerke für kritische Infrastrukturen (KRITIS) und Operational Technologies (OT)





Zusammenfassung

Betreiber von kritischen Infrastrukturen (KRITIS) stehen in OT/ICS-Umgebungen (Operational Technology / Industrial Control Systems) vor einem netzwerktechnischen Zielkonflikt: IT-Sicherheitsmaßnahmen müssen wirksam sein, dürfen die Prozesse aber nicht gefährden. OT ist langlebig, oft echtzeit- und verfügbarkritisch, und viele Komponenten lassen sich nur eingeschränkt patchen. Gleichzeitig steigt die Konnektivität durch IT/OT-Konvergenz, Fernwartung, Partnerzugänge und Edge-Integrationen. Dieses Whitepaper zeigt deshalb keine reine Tool-Landschaft, sondern ein konsistentes Zielbild für sichere OT-Infrastrukturen: Kommunikation wird minimiert, Übergänge werden kontrolliert, und der Betrieb bleibt auch im Störfall bestehen.

Im Mittelpunkt stehen drei wiederkehrende Pfade, an denen sich OT-Security im Alltag entscheidet: (1) Zugriffe (z. B. Fernwartung), (2) Datenflüsse (z. B. Reporting/Analytics) und (3) Änderungen (z. B. Updates). Für jeden Pfad wird ein robustes Architektur- und Betriebsprinzip beschrieben, inklusive konkreter Anwendungsfälle und einer Checkliste für die Umsetzung und Nachweisbarkeit.

Wie sich dieses Zielbild technisch umsetzen lässt

Für Betreiber kritischer Infrastrukturen stellt sich nicht nur die Frage nach dem Zielbild, sondern auch nach dessen belastbarer technischen Umsetzung. Entscheidend sind dabei Komponenten und Architekturen, die Segmentierung, kontrollierte Übergänge, sichere Fernzugriffe und nachvollziehbare Betriebsprozesse unterstützen. Genau an diesen Punkten leisten LANCOM Netzwerk- und Security-Komponenten einen Beitrag zur praktischen Umsetzbarkeit des beschriebenen OT-Sicherheitsmodells.

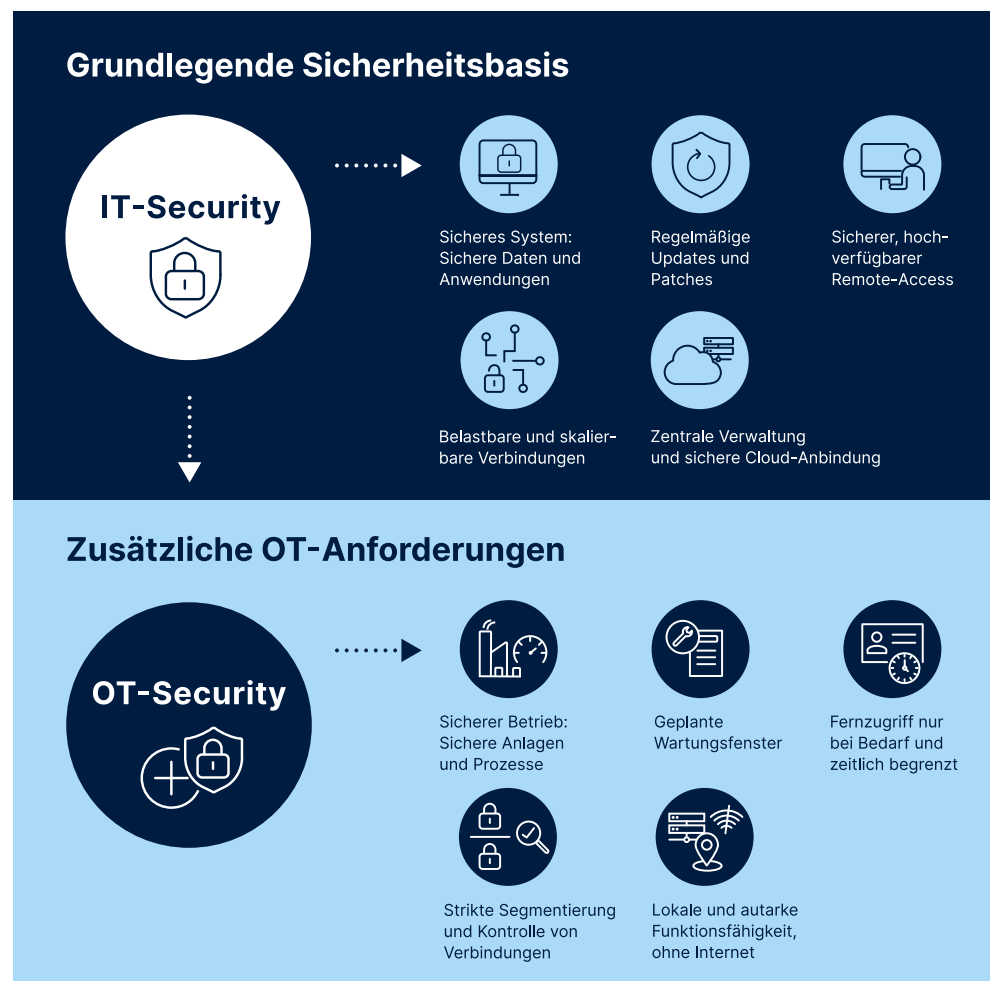
1. Was macht KRITIS-OT-Security besonders?

Operational Technology und Industrial Control Systems koordinieren reale Prozesse: von Gebäudeautomation und Sicherheitstechnik bis zu Energie- und Produktionssteuerungen. OT-Security folgt zwar denselben Grundprinzipien wie IT-Security, muss in kritischen Infrastrukturen aber zusätzliche Anforderungen berücksichtigen: physische Prozessnähe, hohe Verfügbarkeitsanforderungen, deterministisches Verhalten, lange Lebenszyklen, eingeschränkte Patchbarkeit und in vielen Bereichen auch funktionale Sicherheit. Sicherheitsmaßnahmen müssen deshalb nicht nur wirksam, sondern zugleich betrieblich beherrschbar und validierbar sein.

OT- und ICS-Strukturen haben dabei einige spezielle Eigenschaften, die berücksichtigt werden müssen. Typische Rahmenbedingungen, die Architekturentscheidungen prägen, sind lange Lebenszyklen (oft 10–15+ Jahre), planungs- und genehmigungspflichtige Änderungen, begrenzte Patchbarkeit sowie hohe Anforderungen an Nachvollziehbarkeit und Resilienz. Wirksame Sicherheit entsteht hier über Kompensationskontrollen:

Netzwerksegmentierung, kontrollierte Übergänge, Session-Trennung, Monitoring und belastbare Betriebsprozesse.

In vielen OT-Umgebungen betrifft Cybersicherheit nicht nur Verfügbarkeit und Integrität von Systemen, sondern mittelbar auch die funktionale Sicherheit von Anlagen. Sicherheitsmaßnahmen müssen deshalb so gestaltet werden, dass sie Schutzwirkungen erhöhen, ohne sicherheitsgerichtete Funktionen, Freigaben oder betriebliche Schutzmechanismen unbeabsichtigt zu beeinträchtigen.





2. Leitprinzipien einer sicheren KRITIS-OT-Architektur

Eine sichere KRITIS-OT-Architektur konzentriert Kommunikation auf wenige, kontrollierbare Übergänge und macht jeden privilegierten Zugriff nachvollziehbar. Die Formel dafür lautet:

Segmentierung (Zonen) + definierte Kommunikationspfade und kontrollierte Übergänge (Conduits) + starke Identitäten und Authentisierung + Sichtbarkeit (Logging) + Betriebsfähigkeit (Resilienz / Autarkie)

Anschaulich gedacht heißt das: Zonen sind „Bereiche mit ähnlichem Schutzbedarf“ (z.B. Leitstand/SCADA, Engineering, Zellen/PLCs). Conduits sind die wenigen, bewusst freigeschalteten Verbindungen dazwischen (z.B. SCADA darf auf definierte PLCs sprechen, Engineering nur über einen Jump-Host). Mit „starker Identität“ ist gemeint, dass privilegierte Zugriffe personenbezogen und zeitlich begrenzt sind (z.B. MFA / Multi-Faktor-Authentifizierung, Wartungsfenster). Logging macht diese Ketten überprüfbar und nachvollziehbar – nicht nur für Netzwerkereignisse, sondern auch für Audits, Vorfallanalysen und betriebliche Nachweise. Resilienz / Autarkie bedeutet schließlich: Die OT bleibt auch dann steuerbar, wenn es Störungen in der IT oder im WAN gibt. Ermöglicht wird dies durch lokale Dienste, klare Segmentgrenzen und definierte Isolation.

3. Zielarchitektur: Klar voneinander getrennte Sicherheitszonen

Das robuste Grundmuster einer resilienten KRITIS-Netzwerkarchitektur trennt Büro- / Business-IT und OT über klar definierte Übergänge und ergänzt diese um eine OT-DMZ (Demilitarized Zone; kontrollierbare Übergabebzone). Das Ziel ist ausdrücklich: keine direkten Pfade von Extern/IT in produktive OT-Zonen. Stattdessen laufen Zugriffe, Daten und Updates über festgelegte Kontrollpunkte.

3.1 Einordnung der Zielarchitektur

Die nachfolgend dargestellte Zielarchitektur orientiert sich an einem vereinfachten, an Purdue/IEC 62443 angelehnten Referenzmodell. Dieses dient im Whitepaper als Ordnungsrahmen für vertikale Trennung, horizontale Segmentierung und kontrollierte Kommunikationsflüsse. Unternehmens-IT, Übergabebzonen und produktive OT werden dabei bewusst voneinander getrennt; Übergänge erfolgen über definierte Zonen und Conduits. Das Modell wird hier nicht als starre 1:1-Abbildung jeder realen Anlage verstanden, sondern als praxistaugliches Sicherheitsprinzip für Segmentierung, Zugriffskontrolle und Nachvollziehbarkeit.



3.2 Vertikale Trennung: IT – IT-DMZ – OT-DMZ – OT

Die IT-DMZ ist die Übergabezone zur Außenwelt (Internet/Partner) und der Ort für kontrollierten Zugriff über Proxies / Reverse-Proxies. Die OT-DMZ dient als technische und organisatorische Pufferzone zwischen IT und OT: Hier liegen typischerweise Jump-Hosts, Update-/Patch-Repositories sowie Historian/Replica-Instanzen für die Datenentkopplung. Diese zusätzliche Schicht sorgt für eine auditierbare und betriebs-sichere Trennung.

Praktisch macht die OT-DMZ zwei Dinge „greifbar“: (1) Zugriffe werden an einem einzigen Punkt gebündelt (z. B. Fernwartung endet immer am Jump-Host – nie direkt im OT-Netz), und (2) riskante oder lastintensive Funktionen werden aus der produktiven OT herausgezogen (z. B. Patch-Ablage, Virensignaturen, Daten-Replica). So bleibt die OT ruhig und deterministisch, während IT-nahe Anforderungen trotzdem erfüllt werden.

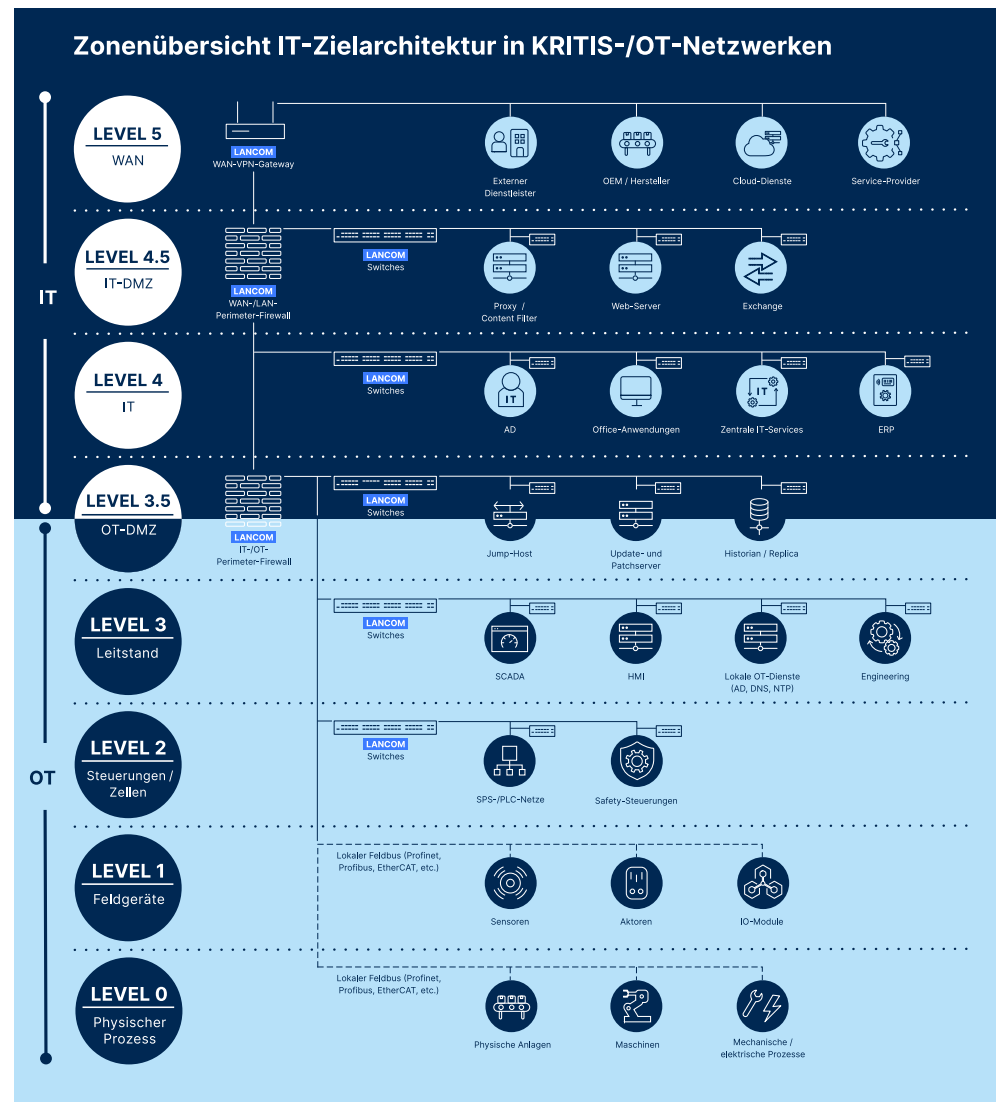
In dieser Logik entspricht die OT-DMZ der Übergangszone zwischen Unternehmens-IT und produktiver OT, also funktional der häufig als Ebene 3.5 beschriebenen DMZ-Schicht: Sie bündelt kontrollierte Zugriffe, entkoppelt Datenflüsse und verhindert Direktkommunikation zwischen IT und OT.

3.3 Horizontale Segmentierung: OT in funktionale Bereiche

Innerhalb der OT wird zusätzlich segmentiert, um laterale Bewegung zu begrenzen und um Kommunikation explizit erlauben und dokumentieren zu können. Übliche Bereiche sind Leitstand / SCADA (Supervisory Control and Data Acquisition), Engineering, HMI (Human Machine Interface), OT-Services sowie Zell- / PLC-Netze (Programmable Logic Controller).

Beispiel: Der Leitstand / SCADA braucht typischerweise nur Verbindungen zu ausgewählten PLC-Zellen und OT-Services (z. B. Historian). Engineering-Systeme benötigen oft breitere Rechte, aber nur temporär und kontrolliert (z. B. im Wartungsfenster über einen Jump-Host). Eine Zelle (PLC-Netz) wiederum sollte möglichst nur das Nötigste „nach außen“ sprechen. Diese Logik (wer braucht wirklich welche Verbindung?) ist der Kern der Segmentierung und nicht die Anzahl der VLANs.

Wichtig ist: Die Segmentierung folgt dem Kommunikationsbedarf. Das Ziel ist nicht maximale Kleinteiligkeit, sondern minimale, begründete Kommunikation.





4. Die drei kritischen Pfade im Betrieb von OT- und ICS-Netzwerken

Die folgenden drei Pfade lassen sich als typische, sicherheitsrelevante Kommunikationsmuster über mehrere Ebenen einer an Purdue/IEC 62443 angelehnten OT-Architektur lesen. Je nach Anwendungsfall sind dabei nicht alle Ebenen gleichermaßen betroffen; entscheidend sind die kontrollierten Übergänge zwischen den jeweils berührten Zonen.

4.1 Zugriffspfad: Fernwartung ohne Kontrollverlust

Fernwartung ist häufig ein wichtiger Bestandteil von flexiblen Instandhaltungsprozessen, aber auch einer der häufigsten Angriffswege. Ein VPN allein ist in KRITIS kein ausreichendes Schutzprinzip. Stattdessen wird Fernwartung als kontrollierter Prozess gestaltet: Externer Zugang wird nur bei Bedarf aktiviert, Ziele sind strikt begrenzt, Sessions werden getrennt und protokolliert.

Strukturierungsempfehlung (logische Kette):

1. Externer Dienstleister/Operator authentisiert sich stark am VPN-Gateway (z.B. Zertifikat + MFA).
2. Perimeter-Firewall erlaubt ausschließlich den Zugriff in ein dediziertes Remote- / DMZ-Segment, aber nicht in die OT.
3. Jump-Host trennt die Session (Session Break): Administration findet vom Jump-Host zum Ziel statt, nicht direkt aus dem VPN.
4. Zugriff ist zeitlich begrenzt (Wartungsfenster) und wird vollständig geloggt (VPN, Firewall, Jump-Host, Zielsystem).

4.2 Datenpfad: Reporting/Analytics ohne Öffnung der OT

KRITIS-OT braucht Daten für ein transparentes Reporting, ebenso wie für Trendanalysen und Nachweise. Direktzugriffe aus der IT auf produktive OT-Systeme erhöhen jedoch das Risiko für Ausfälle und für unbeabsichtigte Last- / Query-Effekte. Das empfohlene Muster ist daher Datenentkopplung: OT schreibt in eine Historian- / Replica-Instanz in/nahe der OT-DMZ, die IT liest daraus read-only. Produktive OT-Datenbanken und SCADA bleiben von IT-Queries isoliert.

4.3 Änderungspfad: Updates, Integrität und Change-Kontrolle

Updates werden in OT nach strikten Vorgaben und geplanten Zeitfenstern gehandhabt und nicht spontan: Feste Wartungsfenster, eine vorherige Validierung und eindeutige Freigabeprozesse sind üblich. Zudem sind Updates ein Supply-Chain-Risiko, da im Fehlerfall Prozesse gefährdet sind. Ein kontrollierter Update-Pfad führt Updates daher über eine DMZ-Strecke (Repository / Patch-Server), prüft Integrität / Authentizität (Signaturen / Prüfsummen) und macht Freigaben audittierbar. Die OT bezieht Updates nicht direkt aus dem Internet.



5. OT-Security in der Praxis: Konkrete Use Cases

Die folgenden Use Cases beschreiben typische Situationen aus KRITIS-OT-Projekten. Jeder Use Case folgt derselben Struktur: Ausgangslage, Risiko, Zielbild und praxistaugliche Umsetzungsschritte. So lassen sich Architekturprinzipien direkt in Betriebsabläufe übersetzen.

Die Abbildungen in diesem Kapitel nutzen ein vereinfachtes, an Purdue/IEC 62443 angelehntes Ebenenmodell. Nicht betroffene Ebenen bleiben sichtbar, werden aber neutral dargestellt; hervorgehoben werden nur die für den jeweiligen Pfad oder Use Case relevanten Ebenen und Übergänge.

Use Case 1: Dienstleister muss kurzfristig eine Störung beheben (sichere Fernwartung)

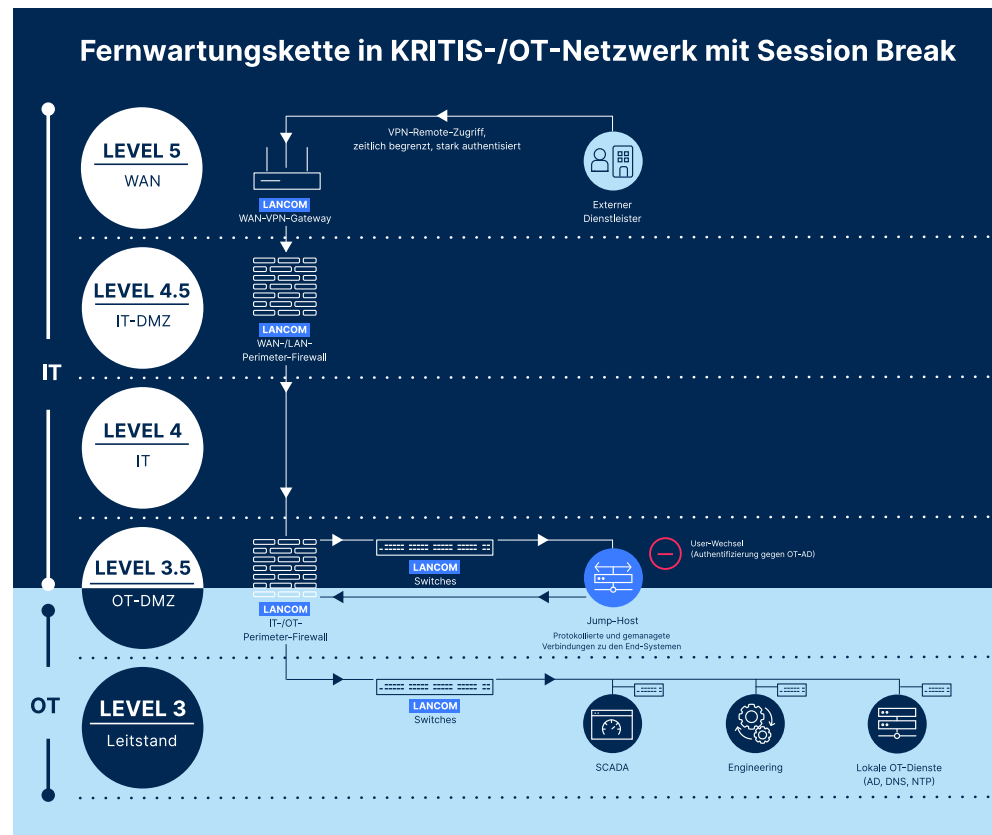
Ausgangslage:	Ein externer Dienstleister soll außerhalb der Bürozeiten auf ein Engineering- oder SCADA-System zugreifen, um eine Störung zu analysieren.
Typische Risiken:	Dauerhaft offene Zugänge, Direktzugriff aus dem VPN ins Zielnetz, fehlende Protokollierung, unklare Verantwortlichkeiten.
Betroffene Ebenen im Purdue-Modell:	Extern / Internet, Unternehmens-IT bzw. Remote-Zugang, OT-DMZ (Ebene 3.5) sowie die adressierten OT-Systeme auf Betriebsführungs- oder Prozessleitebene.
Zielbild:	Zeitlich begrenzter, stark authentisierter Zugriff über VPN, Zielbegrenzung auf Jump-Host, Session Break und vollständiges Logging.

Umsetzung (praxisnah):

1. Remote-Access in ein dediziertes OT-Remote-Segment terminieren (nicht ins OT-Produktivnetz)
2. Firewall-Policy: Default-Deny, explizit nur Jump-Host als Ziel erlauben
3. Jump-Host mit Rollen / Richtlinien (wer darf auf welche Zielsysteme, wie lange, zu welchem Ticket)
4. Wartungsfenster-Prozess: Aktivierung nur nach Freigabe; automatische Deaktivierung nach Zeitablauf
5. Session-Logging aktivieren (Aufzeichnung oder zumindest Befehls- / Audit-Logs) und zentral ablegen

Nachweisbarkeit / Betrieb:

- VPN- und Firewall-Logs: wer, wann, von wo, zu welchem Ziel
- Jump-Host-Logs inkl. Session-Informationen und Ticket- / Change-Referenz
- Regelmäßiger Review der Rollen und der erlaubten Ziele (Least Privilege)



Use Case 2: Controlling und Analytics benötigen OT-Prozessdaten (Datenentkopplung)

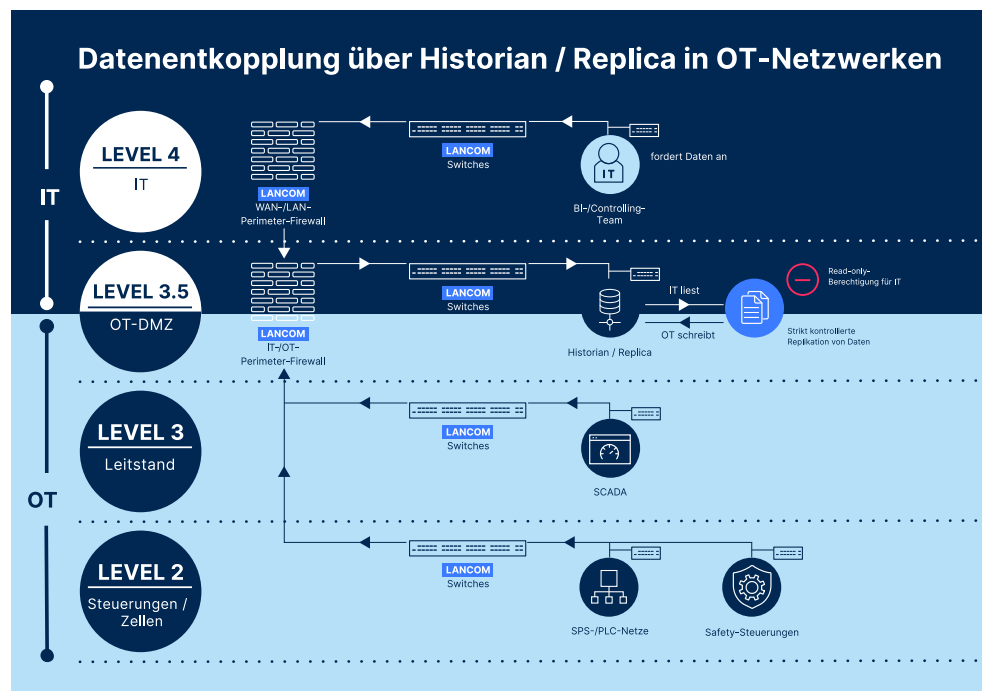
Ausgangslage:	Ein BI- oder Controlling-Team möchte Prozess- und Statusdaten aus der OT für Berichte, Kennzahlen, Trendanalysen und Nachweise nutzen.
Typische Risiken:	Direktzugriffe aus der IT erzeugen zusätzliche Last auf produktiven OT-Systemen; im Worst Case beeinflussen Queries den Betrieb. Außerdem entstehen neue Angriffswege.
Betroffene Ebenen im Purdue-Modell:	Unternehmens-IT, OT-DMZ (Ebene 3.5) sowie OT-Systeme der Betriebsführungs- und Prozessebene, aus denen Daten kontrolliert repliziert werden.
Zielbild:	Das OT-System stellt Daten über eine Replica/Historian in der OT-DMZ bereit. Das IT-System erhält ausschließlich read-only Zugriff auf diese Replica.

Umsetzung (praxisnah):

1. In der OT-DMZ eine Historian/Replica-Instanz platzieren, die Daten aus der OT übernimmt (Write/Sync)
2. Replikationspfad strikt definieren (nur benötigte Datenpunkte, definierte Protokolle / Ports)
3. IT-Zugriff ausschließlich auf die Replica erlauben; produktive OT-Systeme bleiben für IT nicht adressierbar
4. Read-only-Accounts und getrennte Identitäten (keine geteilten OT-Admin-Accounts)
5. Logging entlang der Datenkette in Monitoring / SIEM (Security Information and Event Management) einspeisen

Nachweisbarkeit / Betrieb:

- Dokumentiertes Datenmodell: welche Daten werden repliziert und warum
- Firewall-Regeln und Read-only-Berechtigungen als Audit-Artefakte
- Alarme bei abweichendem Datenvolumen oder unerwarteten Zugriffsmustern



Use Case 3: Sicherheitsupdate für einen OT-Server muss eingespielt werden (kontrollierte Update-Strecke)

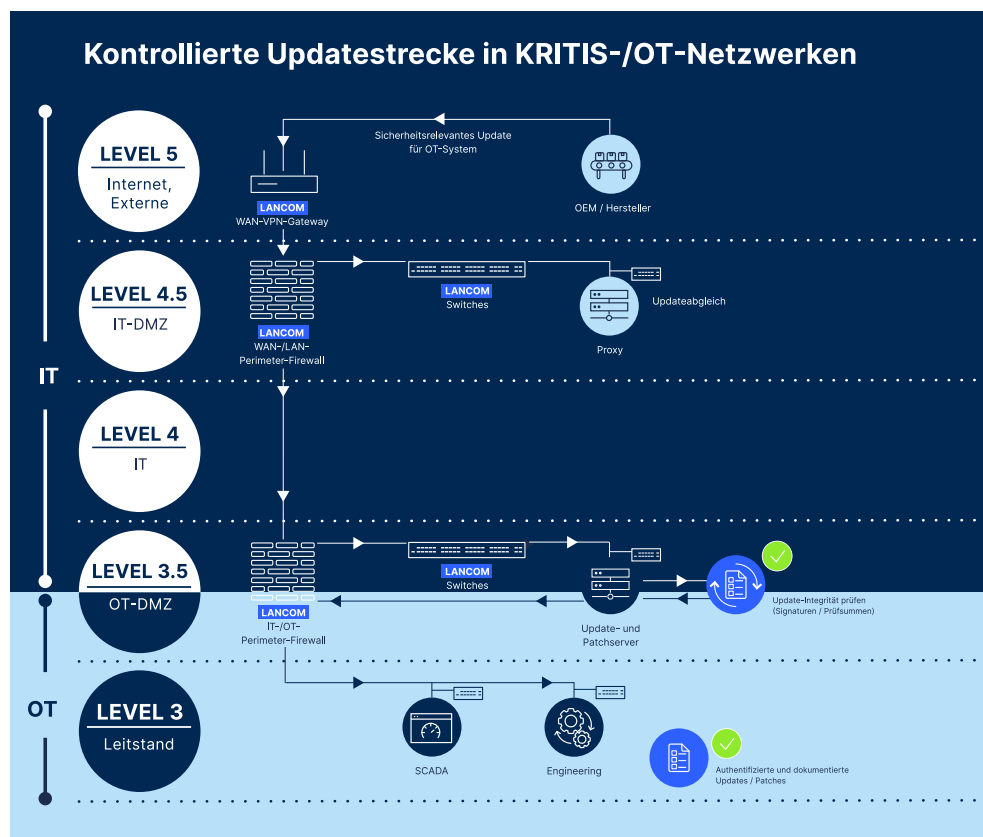
Ausgangslage:	Ein Hersteller veröffentlicht ein sicherheitsrelevantes Update. Die OT darf keinen Direktzugang ins Internet haben und Änderungen müssen validiert werden.
Typische Risiken:	Unkontrollierte Update-Quellen, fehlende Integritätsprüfung, unklare Rollback-Strategie, Updates außerhalb von Wartungsfenstern
Betroffene Ebenen im Purdue-Modell:	Externe Quelle bzw. Hersteller, Übergabe- und Prüfinstanzen in der DMZ sowie die jeweils betroffenen OT-Systeme in den oberen OT-Ebenen.
Zielbild:	Updates laufen über DMZ-Repository mit Integritätsprüfung, Freigabeprozess und geplanter Verteilung im Wartungsfenster

Umsetzung (praxisnah):

1. Update- / Patch-Repository in der (OT-)DMZ betreiben; OT-Systeme beziehen Updates ausschließlich von dort
2. Integrität / Authentizität prüfen (Signaturen, Checksummen) und Ergebnisse dokumentieren
3. Test / Validierung in einer Staging-Umgebung oder in abgestimmten Pilot-Systemen durchführen (wo möglich)
4. Freigabe und Rollout an Wartungsfenster koppeln; Backup / Rollback festlegen
5. Nach dem Rollout: Funktionsprüfung und Abgleich der installierten Versionen

Nachweisbarkeit / Betrieb:

- Audit-Trail: Quelle, Prüfsummen/Signaturprüfung, Freigabe, Zeitpunkt, betroffene Systeme
- Change- und Incident-Referenzen (Ticketing), inklusive Verantwortlichkeiten
- Regelmäßige Reportings: Patch-Stand nach Zonen / Systemklassen



Use Case 4: Sicherheitsvorfall in einer OT-Zone – Segment-Isolation ohne Stillstand

Ausgangslage:	Ein Monitoring schlägt Alarm wegen: ungewöhnlicher Kommunikation in einer PLC-Zelle. Der Betrieb soll weiterlaufen, während der Vorfall eingegrenzt wird.
Typische Risiken:	Unklare Segmentgrenzen, Abhängigkeit von zentralen IT-Diensten (DNS / NTP / Auth), fehlende vorbereitete Isolationsmaßnahmen
Betroffene Ebenen im Purdue-Modell:	Vor allem horizontale Segmente innerhalb der OT, insbesondere auf Prozessleit-, Steuerungs- und Zellebene; vertikale Übergänge bleiben davon konzeptionell getrennt.
Zielbild:	Alle Zellen und OT-Services sind so segmentiert, dass eine betroffene Zone isoliert werden kann, ohne den Gesamtsystembetrieb zu verlieren (Autarkie)

Umsetzung (praxisnah):

1. Zellen/Segmente so definieren, dass kritische Prozesspfade lokal bleiben.
2. Lokale OT-Dienste vorsehen (z. B. DNS / NTP / Auth nach Konzept), um IT- / WAN-Abhängigkeiten zu minimieren.
3. Isolation Playbook: Vordefinierte Maßnahmen (z. B. Regeln / ACLs), um eine Zone abzukoppeln.



4. Logging- und Monitoring-Pfade so gestalten, dass Ereignisse auch im isolierten Zustand sichtbar bleiben (wo möglich).
5. Nach Isolation: Forensische Sicherung, Wiederanlaufplan und kontrollierte Rückintegration.

Nachweisbarkeit / Betrieb:

- Dokumentierte Segmentgrenzen und Isolationsschalter (technisch / organisatorisch)
- Regeltests in Wartungsfenstern (z. B. halbjährliche Übung)
- Nachweis: OT bleibt in definierten Störfällen funktionsfähig

6. Welche Rolle spielen Netzwerk- und Security-Komponenten für die OT- und KRITIS-Security?

Dieses Kapitel beschreibt die Rollen typischer Infrastrukturkomponenten (Switches, Gateways, Firewalls, Remote Access- und Monitoring-Systeme). Hierbei liegt der Fokus darauf, welche Rolle das Bauteil im Zonen- und Conduits-Modell spielt und wie es die Nachweisbarkeit und Betrieb jeweils unterstützt.

6.1 Firewalls

Firewalls setzen die festgelegten Conduits praktisch um: Default-Deny ist die Baseline, Kommunikation wird explizit als Allow-List freigeschaltet. In OT-Kontext geht es häufig um Zonenbeziehungen (IT-DMZ ↔ OT-DMZ ↔ OT ↔ Zellen) und um nachvollziehbare Policies, nicht primär um die klassische Absicherung des Internetzugangs. Logging und – je nach Schutzbedarf – Redundanz / Failover sind zentrale Anforderungen.

6.2 Gateways / Proxies

Gateways und Proxies helfen, Übergänge zu entkoppeln und Inhalte kontrollierbar zu machen (Layer-7, Protokoll- und Zielkontrolle). Typisch sind kontrollierter Internetzugang in der DMZ, Reverse-Proxies für veröffentlichte Dienste sowie NAT (Network Address Translation) / Adressentkopplung bei kollidierenden Netzen.

6.3 Remote-Access / VPN

Remote-Access erfordert in KRITIS deutlich mehr Sicherheit als die Verwendung einer VPN-Verbindung. Wichtig sind starke Authentisierung (z. B. Zertifikat + MFA), Segment-Terminierung (dediziertes Remote-Segment), zeitliche Begrenzung (Wartungsfenster) und auditierbares Session-Logging. Der Zugriff auf OT-Ziele erfolgt anschließend über Jump-Hosts und nicht direkt aus dem VPN.



6.4 Switches / Portkontrolle

Switches bilden die Basis für saubere Segmentierung, Portdisziplin und die technische Durchsetzung lokaler Zugriffsvorgaben. Je nach Betriebskonzept können dazu auch Mechanismen wie NAC oder 802.1X gehören – immer mit Fallback-Strategien, um die Betriebsfähigkeit nicht zu gefährden. Wichtig sind klar dokumentierte Segmentgrenzen, getrennte Managementpfade und Logfähigkeit für relevante Ereignisse. Unbenutzte Ports sollten deaktiviert oder isoliert sein, damit „zufällige“ Verbindungen nicht zum Normalzustand werden.

6.5 Monitoring / SIEM

Monitoring und SIEM sind keine klassischen Netzwerkkomponenten, aber zentrale Sicherheitsfunktionen für Nachvollziehbarkeit, Detektion und Nachweisbarkeit. Sie verbinden Ereignisse aus Zugriffen, Datenflüssen und Änderungen zu einer Ende-zu-Ende-Sicht. Klare Nachvollziehbarkeit und schnelle Detektion basieren auf Logs. Ein sinnvolles Design sammelt Ereignisse entlang der kritischen Ketten (VPN, Firewalls, Proxies, Jump-Hosts, relevante Server- und Switch-Events) und führt sie in ein zentrales Monitoring / SIEM. Das Ziel ist dabei nicht die maximale Logmenge, sondern eine eindeutige Ende-zu-Ende-Sichtbarkeit für Zugriffe, Datenflüsse und Änderungen.

7. Von der Planung in die praktische Umsetzung: So können Sie Ihre OT-Security auf den Weg bringen

Viele OT-Security-Projekte scheitern nicht am Zielbild, sondern an der Überführung in den Betrieb. Die folgende Vorgehenslogik ist bewusst einfach gehalten und eignet sich als Blaupause für die Projekt- und Betriebsplanung.

1. Kommunikationsmatrix erstellen
Welche Systeme sprechen mit welchen Zielen, über welche Protokolle, mit welchem Zweck und welcher Kritikalität?
2. Zonen- und Übergabemodell definieren
Vertikale Trennung (IT / IT-DMZ / OT-DMZ / OT) und horizontale Segmentierung (Bereiche / Zellen).
3. Regel- und Freigabematrix ableiten
Welche Conduits sind erlaubt, wer genehmigt sie, wie werden Änderungen dokumentiert?
4. Betriebsprozesse festlegen
Fernwartung, Updates, Freigaben, Rollback, Wartungsfenster, Ausnahmeprozesse.
5. Nachweis- und Monitoringkonzept definieren
Welche Ereignisse werden protokolliert, zentral korreliert und regelmäßig überprüft?
6. Incident- und Isolations-Playbooks vorbereiten
Wer darf was im Störfall tun, welche Zone kann wie isoliert werden, wie erfolgt die kontrollierte Rückintegration?



8. Checkliste: Was Auditoren und Betrieb wirklich brauchen

- Dokumentiertes Zonen- und Conduits-Modell (inkl. Verantwortlichkeiten)
- Default-Deny-Policy mit begründeten Allow-Lists und regelmäßiger Überprüfung
- Sichere Fernwartung als Prozess (Freigabe, Wartungsfenster, Jump-Host, Logging)
- Datenentkopplung für Reporting (Replica / Historian, read-only, keine IT-Queries auf produktive OT)
- Kontrollierte Update-Strecke (Repository in DMZ, Integritätsprüfung, Freigabe, Rollback)
- Ende-zu-Ende-Logging in Monitoring / SIEM (Zugriff, Daten, Änderungen)
- Resilienz / Autarkie: definierte Isolation im Incident, minimierte IT- / WAN-Abhängigkeiten

Die beschriebenen Maßnahmen entfalten ihren vollen Nutzen erst dann, wenn sie in ein gelebtes Informationssicherheitsmanagement beziehungsweise ein OT-Sicherheitsprogramm eingebettet sind – etwa auf Basis von ISO/IEC 27001 und IEC 62443-2-1.

9. Fazit

Eine resiliente KRITIS-OT-Architektur erkennt man nicht an einer langen Feature-Liste, sondern an wenigen, konsequent umgesetzten Prinzipien: Übergänge sind bewusst gestaltet (IT-DMZ / OT-DMZ), jegliche Kommunikation ist minimal und explizit freigeschaltet (Default-Deny / Allow-List) und privilegierte Zugriffe laufen kontrolliert über Session-Break (Jump-Host) und sind vollständig nachvollziehbar (Logging / SIEM).

Wenn zusätzlich Datenflüsse entkoppelt (Replica / Historian) und Änderungen kontrolliert (Update-Strecke mit Prüfung und Freigabe) umgesetzt werden, entsteht ein Betrieb, der sowohl sicher als auch verlässlich bleibt – auch unter KRITIS-Randbedingungen wie engen Wartungsfenstern, langen Lebenszyklen und hohen Verfügbarkeitsanforderungen.



10. Glossar (kurz)

Begriff	Definition
OT (Operational Technology)	Systeme und Netzwerke zur Steuerung physischer Prozesse (z. B. Automatisierung, Gebäude- oder Sicherheitstechnik)
ICS	Industrial Control Systems; Sammelbegriff für industrielle/technische Steuerungssysteme, inkl. OT-Komponenten
SCADA	Überwachungs- und Leitsysteme (Supervisory Control and Data Acquisition) für Prozesse und Anlagen
Ebene 3.5 / OT-DMZ	Übergangszone zwischen Unternehmens-IT und produktiver OT im an Purdue/IEC 62443 angelehnten Referenzmodell; dient der Entkopplung von Zugriffen, Datenflüssen und Änderungen.
Purdue-Modell / PERA	Referenzmodell zur hierarchischen Gliederung von OT-/ICS-Architekturen in Ebenen. Im Whitepaper dient es in vereinfachter Form als Ordnungsrahmen für vertikale Trennung, OT-DMZ, Segmentierung und kontrollierte Kommunikationsflüsse; reale Umgebungen weichen davon je nach Anwendungsfall ab.
SPS/PLC	Speicherprogrammierbare Steuerung (Programmable Logic Controller) – steuert Maschinen/Prozessschritte
Zone	Sicherheitsbereich mit ähnlichem Schutzbedarf und klaren Kommunikationsregeln
Conduit	Definierter Kommunikationspfad zwischen Zonen, typischerweise durch Firewalls/Gateways kontrolliert
DMZ	Demilitarized Zone; Übergabebzone, die Netze trennt und Übergänge kontrollierbar macht (z. B. IT-DMZ, OT-DMZ)
OT-DMZ	Zwischenschicht zwischen IT und OT, häufig für Jump-Hosts, Patch-Repositories und Datenreplikation
Allow-List/Whitelist	Prinzip: nur explizit erlaubte Kommunikation ist zulässig
Default-Deny	Grundsatz: alles ist verboten, bis es begründet freigeschaltet wird
Jump-Host / Bastion Host	System in der DMZ, über das administrative Zugriffe auf Zielsysteme geführt und protokolliert werden (Session Break)
Session Break	Trennung einer Remote-Session: kein direkter Kanal vom externen Zugang bis zum Zielsystem; der Jump-Host bildet den kontrollierten Übergang
Historian / Replica	Zwischensystem zur Datensammlung oder Replikation; OT schreibt/synchronisiert, IT liest typischerweise read-only
NAC / 802.1X	Network Access Control; Mechanismen zur Geräte-/Benutzer-Authentisierung am Netzwerkport und zur Zonen-/Rollen-Zuweisung
SIEM	Security Information and Event Management; zentrale Sammlung, Korrelation und Auswertung von Sicherheitsereignissen
MFA	Multi-Faktor-Authentisierung, z. B. zusätzlich zum Passwort ein Token/Authenticator
RADIUS	Protokoll zur zentralen Authentisierung/Autorisierung, häufig für Netzwerkzugänge und MFA-Integration