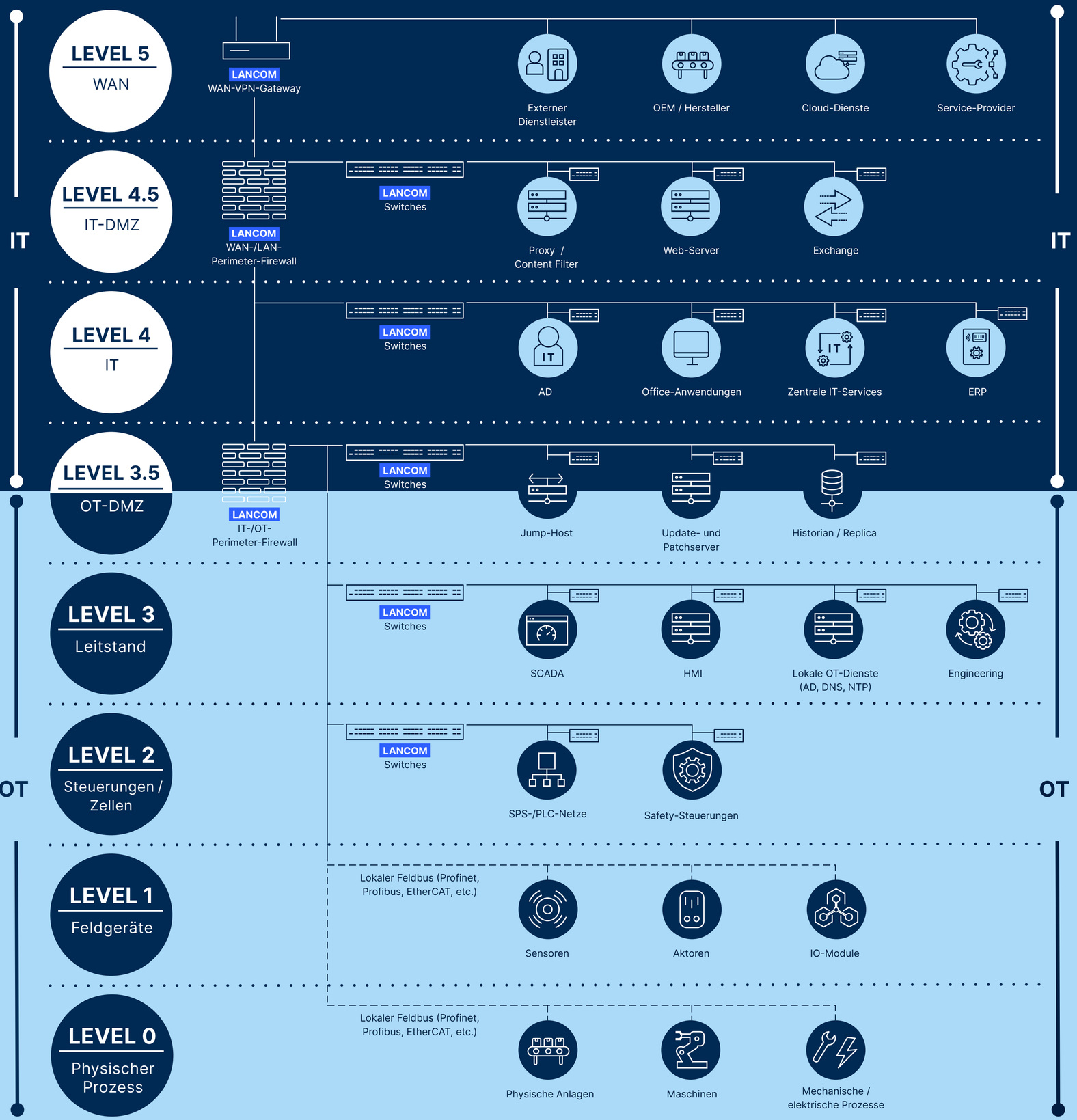
IT-REFERENZARCHITEKTUR KRITIS- UND OT-NETZWERKE

Generelle Aufbauprinzipien:

- Die Architektur folgt einer klaren Zonen- und Ebenenstruktur mit eindeutiger Trennung von Internet, IT- und OT-Domänen gemäß dem Defense-in-Depth-Prinzip.
- Kommunikationsbeziehungen zwischen Zonen sind grundsätzlich verboten und werden ausschließlich über definierte Übergabepunkte (Perimeter-Firewalls, DMZ-Zonen) explizit freigegeben.
- Externe Zugriffe sowie IT-/OT-Kommunikation erfolgen ausschließlich über dedizierte DMZ-Zonen mit kontrollierten Diensten; direkte Verbindungen sind technisch ausgeschlossen.
- Alle Zugriffe unterliegen dem Prinzip der minimalen Berechtigung und sind rollen-, bedarfs- und zeitbezogen geregelt.
- Die Architektur erzwingt eine strikte Segmentierung, um laterale Bewegungen zu verhindern und Auswirkungen von Sicherheitsvorfällen auf einzelne Zonen zu begrenzen.
- Session-Trennung und Entkopplung stellen sicher, dass kein durchgängiger Zugriff von Externen oder IT-Systemen bis in die OT möglich ist.
- Sicherheitsrelevante Ereignisse und Zugriffe werden vollständig protokolliert und zentral überwacht, um Nachvollziehbarkeit, Detektion und Incident-Response zu ermöglichen.
- Die OT-Domäne ist so ausgelegt, dass sie autark und unabhängig von der IT betrieben werden kann, um Verfügbarkeit und Prozesssicherheit auch bei IT-Störungen sicherzustellen.

Zonenübersicht IT-Zielarchitektur in KRITIS-/OT-Netzwerken



Level 5: WAN – Generelle Anforderungen

- Zentraler, kontrollierter Einstiegspunkt für externe Zugriffe
- Starke Authentisierung und verschlüsselte Verbindungen
- Externe Zugänge nur bei Bedarf aktiv
- Vollständige Protokollierung aller Zugriffe
- Kein direkter Zugriff auf OT-Netze

Level 4.5: IT-DMZ – Generelle Anforderungen

- Zentrale Durchgangsstelle für IT, Internet und OT
- Internetzugang nur kontrolliert (Proxy, Whitelist)
- Keine direkten IT→Internet- oder IT→OT-Verbindungen
- Restriktive Regeln (Default-Deny / Allow-List)
- Vollständige Protokollierung aller Zugriffe

Level 4: IT – Generelle Anforderungen

- Segmentierung der IT-Netze (Client, Server, Admin, Monitoring)
- Trennung von Benutzer-, Server- und Management-Verkehr
- Sichere Authentisierung und rollenbasierte Administration
- Administration nur über definierte Management-Netze
- Zentrale Protokollierung und Security-Monitoring (SIEM)
- Kein direkter Zugriff auf Internet oder OT
- Kommunikation ausschließlich nach Allow-List-Prinzip

Level 3.5: OT-DMZ – Generelle Anforderungen

- Zentrale Übergabezone zwischen IT und OT
- Fernwartung ausschließlich über Jump-Host
- Keine direkten IT→OT oder Extern→OT-Verbindungen
- Klare Session-Trennung zwischen IT / Extern und OT
- Segmentierung der OT-DMZ (Jump-Host, Update, Historian)
- Entkoppelte Update- und Datenbereitstellung für OT
- Vollständige Protokollierung und Überwachung aller OT-Zugriffe

Level 3: OT-Netz – Generelle Anforderungen

- Strikte Segmentierung von SCADA-, Engineering- und HMI-Netzen
- Keine direkten IT→SCADA oder Extern→SCADA-Verbindungen
- Kommunikation zu PLCs ausschließlich Whitelist-basiert
- Fernwartungs-Zugriffe nur über OT-DMZ-Jump-Host
- Keine parallelen oder undokumentierten Zugriffspfade
- Vollständige Protokollierung von SCADA-, HMI- und Engineering-Ereignissen
- Sicherstellung eines autarken OT-Betriebs ohne IT-Abhängigkeiten

Level 2: Steuerungen / Zellen – Generelle Anforderungen

- Enthält SPS / PLC, Safety-Controller, Remote-I/O
- Keine direkten IT-/Extern-Zugriffe auf PLC-Netze
- Schutz der Feldgeräte vor Manipulation
- OT-Autonomie: Autarker Betrieb ohne IT-Dienste
- Reine Layer-2-Kommunikation in Level 1 und 0 (nur Feldbus / elektrische Signale)

Level 1: Feldgeräte – Generelle Anforderungen

- Sensor-/Aktor-Netzwerke (Temperatur, Druck, Füllstand, Drehzahl, etc.)
- IO-Module / Remote-IO (Profinet, Profibus, EtherCAT, Modbus-RTU)
- Direkte Anbindung ausschließlich an PLC-Systeme (Level 2)
- Safety-IO getrennt von Standard-IO (Not-Aus-Kreise, Schutztüren, Lichtschranken)
- Prozessnahe Echtzeitdaten, Betrieb auch ohne IT-Infrastruktur

Level 0: Physischer Prozess – Generelle Anforderungen

- Physische Anlagen, Maschinen, Pumpen, Motoren, Ventile
- Mechanische / elektrische Prozesse (Fertigung, Wasseraufbereitung, Energieprozesse)
- Keine Netzkommunikation (rein elektrische / physikalsiche Signale)
- Hoher Schutzbedarf bzgl. Safety & Betriebssicherheit
- Muss unabhängig von IT vollständig funktionsfähig bleiben