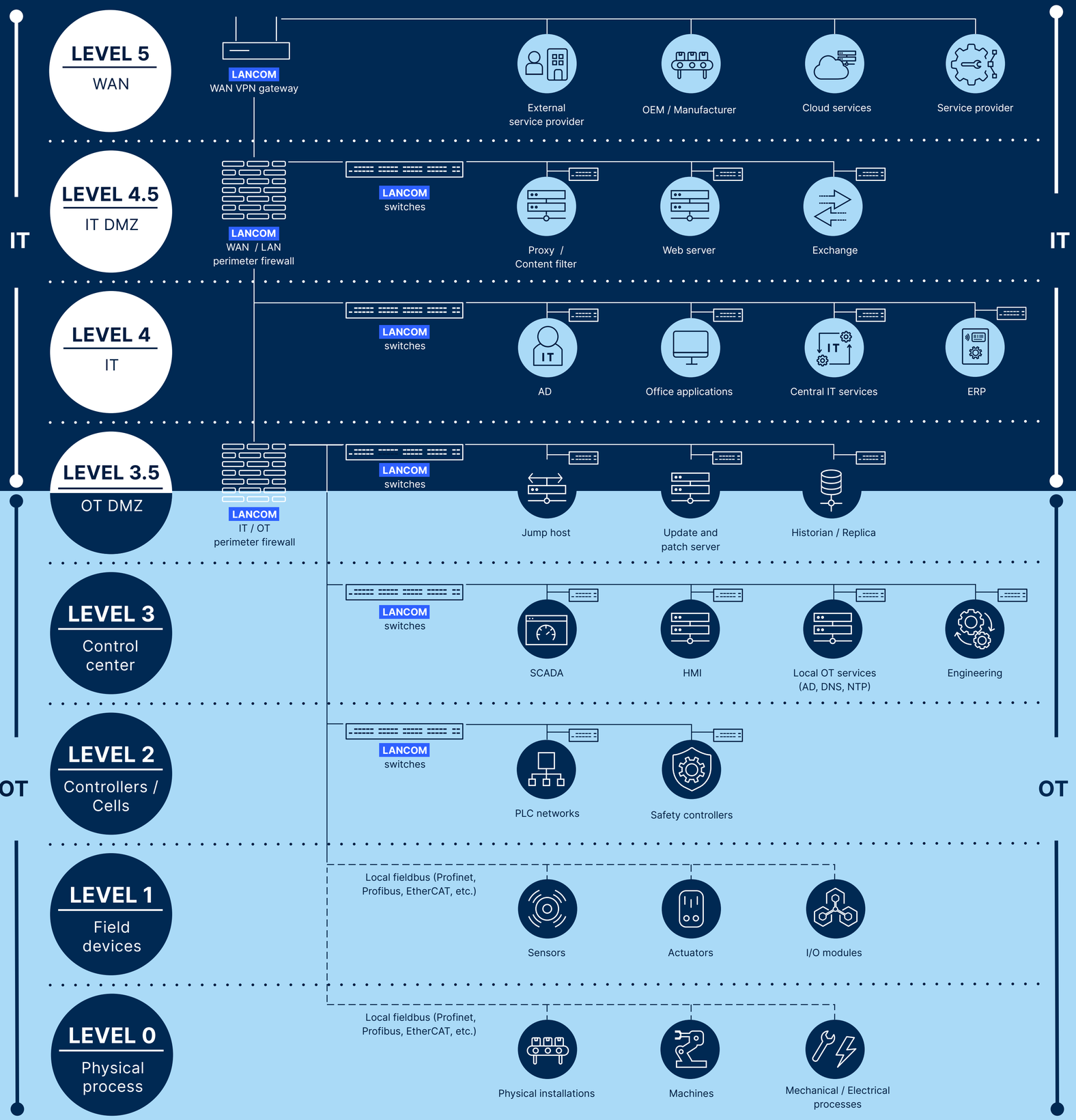
IT REFERENCE ARCHITECTURE FOR CRITICAL INFRASTRUCTURE AND OT NETWORKS

General architectural principles:

- The architecture follows a clear zone and level structure with a distinct separation of Internet, IT, and OT domains in accordance with the defense-in-depth principle.
- Communication relationships between zones are generally prohibited and are only explicitly permitted via defined transfer points (perimeter firewalls, DMZ zones).
- External access and IT / OT communication are carried out exclusively through dedicated DMZ zones with controlled services; direct connections are technically excluded.
- All access follows the principle of least privilege and is regulated according to roles, requirements, and time restrictions.
- The architecture enforces strict segmentation to prevent lateral movement and to limit the impact of security incidents to individual zones.
- Session separation and decoupling ensure that there is no continuous access path from external or IT systems into the OT environment.
- Security-relevant events and accesses are fully logged and centrally monitored to enable traceability, detection, and incident response.
- The OT domain is designed to operate autonomously and independently of IT in order to ensure availability and process reliability even in the event of IT disruptions.

Zone overview of the target IT architecture in critical / OT networks



Level 5: WAN – General requirements

- Central, controlled entry point for external access
- Strong authentication and encrypted connections
- External access enabled only when required
- Complete logging of all accesses
- No direct access to OT networks

Level 4.5: IT DMZ – General requirements

- Central transit point for IT, Internet, and OT
- Internet access only in a controlled manner (proxy, whitelist)
- No direct IT → Internet or IT → OT connections
- Restrictive rules (default deny / allow list)
- Complete logging of all accesses

Level 4: IT – General requirements

- Segmentation of IT networks (client, server, admin, monitoring)
- Separation of user, server, and management traffic
- Secure authentication and role-based administration
- Administration only via dedicated management networks
- Centralized logging and security monitoring (SIEM)
- No direct access to the internet or OT
- Communication exclusively based on the allowlist principle

Level 3.5: OT DMZ – General requirements

- Central transfer zone between IT and OT
- Remote maintenance exclusively via jump host
- No direct IT → OT or external → OT connections
- Clear session separation between IT / external and OT
- Segmentation of the OT DMZ (jump host, update, historian)
- Decoupled update and data provisioning for OT
- Complete logging and monitoring of all OT accesses

Level 3: Control center – General requirements

- Strict segmentation of SCADA, engineering, and HMI networks
- No direct IT → SCADA or external → SCADA connections
- Communication to PLCs exclusively whitelist-based
- Remote maintenance access only via OT DMZ jump host
- No parallel or undocumented access paths
- Complete logging of SCADA, HMI, and engineering events
- Ensuring autonomous OT operation without IT dependencies

Level 2: Controllers / Cells – General requirements

- Contains PLCs, safety controllers, remote IO
- No direct IT / external access to PLC networks
- Protection of field devices against manipulation
- OT autonomy: autonomous operation without IT services
- Pure Layer 2 communication in Levels 1 and 0 (fieldbus / electrical signals only)

Level 1: Field devices – General requirements

- Sensor / actuator networks (temperature, pressure, fill level, speed, etc.)
- IO modules / remote IO (Profinet, Profibus, EtherCAT, Modbus RTU)
- Direct connection exclusively to PLC systems (Level 2)
- Safety IO separated from standard IO (emergency stop circuits, safety doors, light barriers)
- Process-related real-time data, operation possible without IT infrastructure

Level 0: Physical process – General requirements

- Physical systems, machines, pumps, motors, valve
- Mechanical / electrical processes (manufacturing, water treatment, energy processes)
- No network communication (purely electrical / physical signals)
- High protection requirements regarding safety and operational reliability
- Must remain fully functional independently of IT