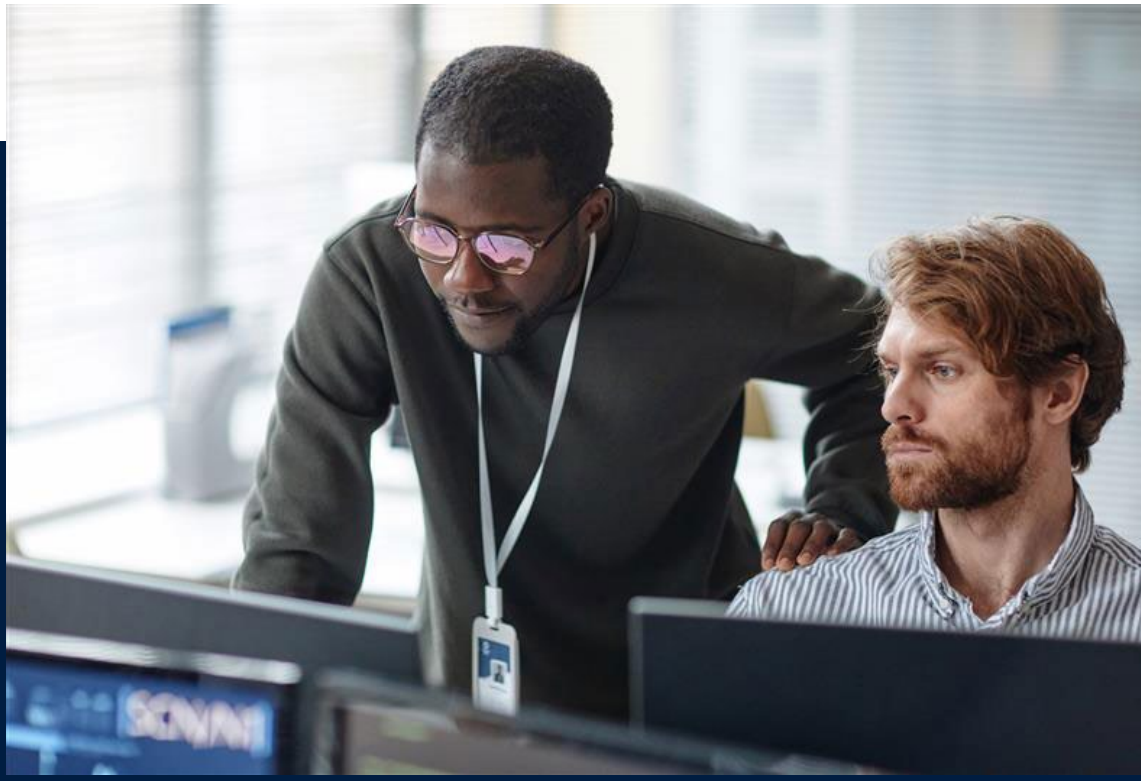
LANCOM SYSTEMS

Whitepaper

Secure IT networks for critical infrastructure (KRITIS) and operational technology (OT)



Summary

Operators of critical infrastructures (KRITIS) face a networking-related conflict of objectives in OT/ICS environments (Operational Technology / Industrial Control Systems): IT security measures must be effective, but they must not jeopardize operational processes. OT environments are long-lived, often real-time- and availability-critical, and many components can only be patched to a limited extent. At the same time, connectivity is increasing due to IT/OT convergence, remote maintenance, partner access, and edge integrations. This whitepaper therefore does not present merely a landscape of tools, but rather a consistent target vision for secure OT infrastructures: communication is minimized, transitions are controlled, and operations remain sustainable even in the event of disruptions.

The focus is on three recurring pathways that determine OT security in everyday operations: (1) access (e.g., remote maintenance), (2) data flows (e.g., reporting/ analytics), and (3) changes (e.g., updates). For each pathway, a robust architectural and operational principle is described, including concrete use cases and a checklist for implementation and verifiability.

How this target architecture can be implemented technically

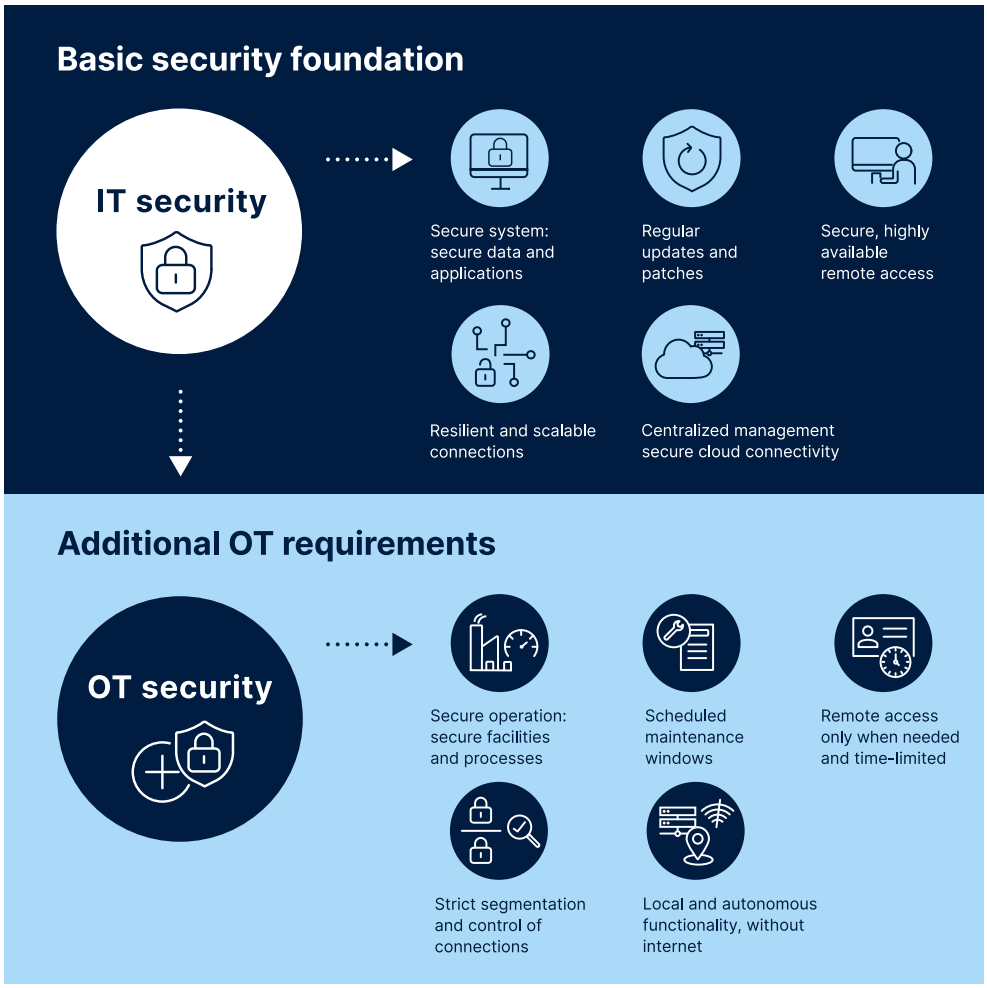
For operators of critical infrastructures, the challenge is not limited to defining the target architecture itself, but also to implementing it in a technically robust manner. Decisive factors are components and architectures that support segmentation, controlled transitions, secure remote access, and traceable operational processes. This is exactly where LANCOM network and security components contribute to the practical implementation of the OT security model described above.

1. What makes KRITIS OT security unique?

Operational technology and industrial control systems coordinate real-world processes: from building automation and security technology to energy and production control systems. While OT security follows the same fundamental principles as IT security, critical infrastructures must address additional requirements: close integration with physical processes, high availability requirements, deterministic behavior, long life cycles, limited patchability, and, in many areas, functional safety. Security measures must therefore not only be effective, but also operationally manageable and verifiable.

OT and ICS structures have several specific characteristics that must be taken into account. Typical boundary conditions that shape architectural decisions include long life cycles (often 10–15+ years), changes requiring planning and approval, limited patchability, and high demands for traceability and resilience. In these environments, effective security is achieved through compensating controls: network segmentation, controlled transitions, session separation, monitoring, and robust operational processes.

In many OT environments, cybersecurity affects not only the availability and integrity of systems, but also indirectly the functional safety of facilities and processes. Security measures must therefore be designed in a way that increases protection without unintentionally impairing safety-related functions, approvals, or operational protection mechanisms.



2. Guiding principles of a secure KRITIS OT architecture

A secure KRITIS OT architecture concentrates communication on a limited number of controllable transitions and makes every privileged access traceable. The formula is:

Segmentation (zones) + defined communication paths and controlled transitions (conduits) + strong identities and authentication + visibility (logging) + operational continuity (resilience / autonomy)

In practical terms, this means: zones are “areas with similar protection requirements” (e.g., control room/SCADA, engineering, cells/PLCs). Conduits are the few deliberately enabled connections between them (e.g., SCADA may communicate with defined PLCs, engineering access only via a jump host). “Strong identity” means that privileged access is tied to individuals and limited in time (e.g., MFA / multi-factor authentication, maintenance windows). Logging makes these chains verifiable and traceable — not only for network events, but also for audits, incident analyses, and operational evidence. Resilience / autonomy ultimately means that the OT environment remains controllable even in the event of disruptions in the IT infrastructure or WAN. This is enabled through local services, clear segment boundaries, and defined isolation mechanisms.

3. Target architecture: Clearly separated security zones

The robust foundation of a resilient KRITIS network architecture separates office/ business IT and OT through clearly defined transitions and complements them with an OT DMZ (demilitarized zone; controllable transfer zone). The explicit objective is: no direct paths from external networks or IT systems into productive OT zones. Instead, access, data, and updates are routed through predefined control points.

3.1 Classification of the target architecture

The target architecture shown below is based on a simplified reference model derived from Purdue / IEC 62443. Within this whitepaper, it serves as a structural framework for vertical separation, horizontal segmentation, and controlled communication flows. Enterprise IT, transfer zones, and productive OT are deliberately separated from one another, with transitions taking place through defined zones and conduits. In this context, the model is not intended as a rigid 1:1 representation of every real-world installation, but rather as a practical security principle for segmentation, access control, and traceability.

3.2 Vertical separation: IT – IT DMZ – OT DMZ – OT

The IT DMZ is the transfer zone to the outside world (Internet/partners) and the location for controlled access via proxies / reverse proxies. The OT DMZ serves as the technical and organizational buffer zone between IT and OT: this is where jump hosts, update/

patch repositories, and historian/replica instances for data decoupling are typically located. This additional layer provides an auditable and operationally secure separation.

In practice, the OT DMZ makes two things “tangible”: (1) access is consolidated at a single point (e.g., remote maintenance always terminates at the jump host — never directly in the OT network), and (2) risky or resource-intensive functions are removed from productive OT environments (e.g., patch repositories, virus signatures, data replicas). This keeps the OT environment stable and deterministic while still meeting IT-related requirements.

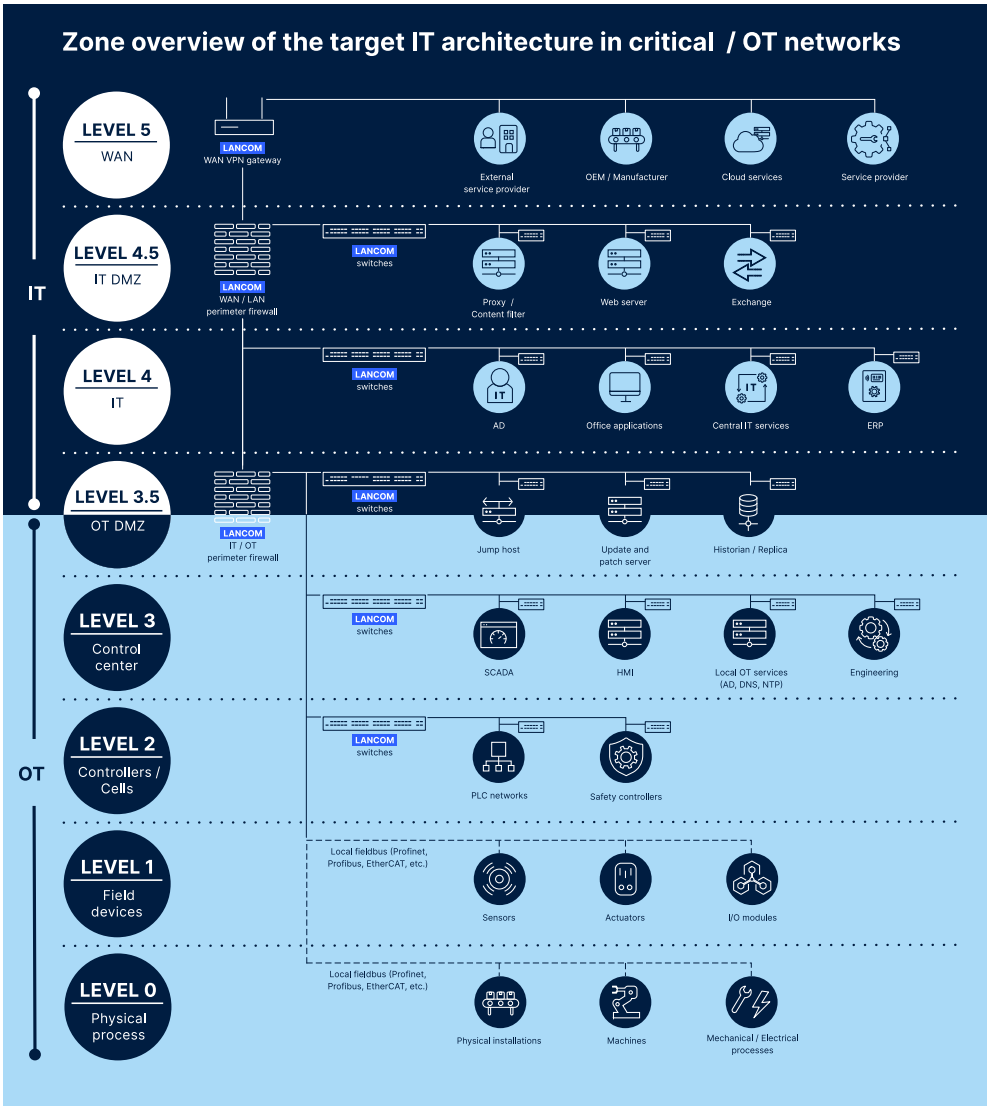
Within this logic, the OT DMZ corresponds to the transition zone between enterprise IT and productive OT, functionally equivalent to the DMZ layer often described as Level 3.5: it consolidates controlled access, decouples data flows, and prevents direct communication between IT and OT.

3.3 Horizontal segmentation: OT into functional areas

Within the OT environment, additional segmentation is implemented in order to limit lateral movement and to ensure that communication can be explicitly permitted and documented. Typical areas include control room / SCADA (Supervisory Control and Data Acquisition), engineering, HMI (Human Machine Interface), OT services, and cell / PLC networks (Programmable Logic Controller).

Example: The control room / SCADA environment typically only requires connections to selected PLC cells and OT services (e.g., historians). Engineering systems often require broader permissions, but only temporarily and in a controlled manner (e.g., during maintenance windows via a jump host). A cell (PLC network), in turn, should communicate externally only to the minimum extent necessary. This logic — who actually requires which connection? — is the core of segmentation, not the number of VLANs.

The key point is: segmentation follows communication requirements. The goal is not maximum granularity, but minimal, justified communication.



4. The three critical pathways in the operation of OT and ICS networks

The following three pathways can be understood as typical security-relevant communication patterns spanning multiple layers of an OT architecture based on Purdue / IEC 62443 principles. Depending on the use case, not all layers are equally affected; the decisive factor is the controlled transition between the respective zones involved.

4.1 Access pathway: Remote maintenance without loss of control

Remote maintenance is often an essential component of flexible maintenance processes, but it is also one of the most common attack vectors. In KRITIS environments, a VPN alone is not a sufficient security principle. Instead, remote maintenance is designed as a controlled process: external access is enabled only when required, target systems are strictly limited, sessions are separated and logged.

Structuring recommendation (logical chain):

1. The external service provider/operator authenticates strongly at the VPN gateway (e.g., certificate + MFA).
2. The perimeter firewall permits access exclusively to a dedicated remote access / DMZ segment, but not to the OT environment.
3. The jump host separates the session (session break): administration is performed from the jump host to the target system, not directly from the VPN connection.
4. Access is limited in time (maintenance window) and is fully logged (VPN, firewall, jump host, target system).

4.2 Data pathway: Reporting/analytics without opening the OT environment

KRITIS OT environments require data for transparent reporting as well as for trend analyses and compliance evidence. However, direct access from IT systems to productive OT systems increases the risk of outages and unintended load/query effects. The recommended pattern is therefore data decoupling: OT systems write to a historian/replica instance in or near the OT DMZ, while IT systems access this data in read-only mode. Productive OT databases and SCADA systems remain isolated from IT queries.

4.3 Change pathway: Updates, integrity, and change control

In OT environments, updates are handled according to strict procedures and scheduled maintenance windows — not spontaneously: predefined maintenance windows, prior validation, and clearly defined approval processes are standard practice. In addition, updates represent a supply chain risk, since operational processes may be jeopardized in the event of failure. A controlled update pathway therefore routes updates through a DMZ-based path (repository / patch server), verifies integrity and authenticity (signatures / checksums), and makes approvals auditable. OT systems do not obtain updates directly from the Internet.

5. OT security in practice: Concrete use cases

The following use cases describe typical scenarios from KRITIS OT projects. Each use case follows the same structure: initial situation, risk, target architecture, and practical implementation steps. This makes it possible to translate architectural principles directly into operational processes.

The figures in this chapter use a simplified layer model derived from Purdue / IEC 62443 principles. Layers that are not affected remain visible but are shown neutrally; only the layers and transitions relevant to the respective pathway or use case are highlighted.

Use case 1: A service provider must resolve a fault at short notice (secure remote maintenance)**

Initial situation:	An external service provider needs to access an engineering or SCADA system outside regular office hours in order to analyze a fault.
Typical risks:	Permanently open access paths, direct access from the VPN into the target network, lack of logging, and unclear responsibilities.
Affected layers in the Purdue model:	External / Internet, enterprise IT or remote access, the OT DMZ (Level 3.5), as well as the addressed OT systems at the operations management or process control level.
Target architecture:	Time-limited, strongly authenticated access via VPN, restricted target access to the jump host, session break, and complete logging.

Implementation (practical approach):

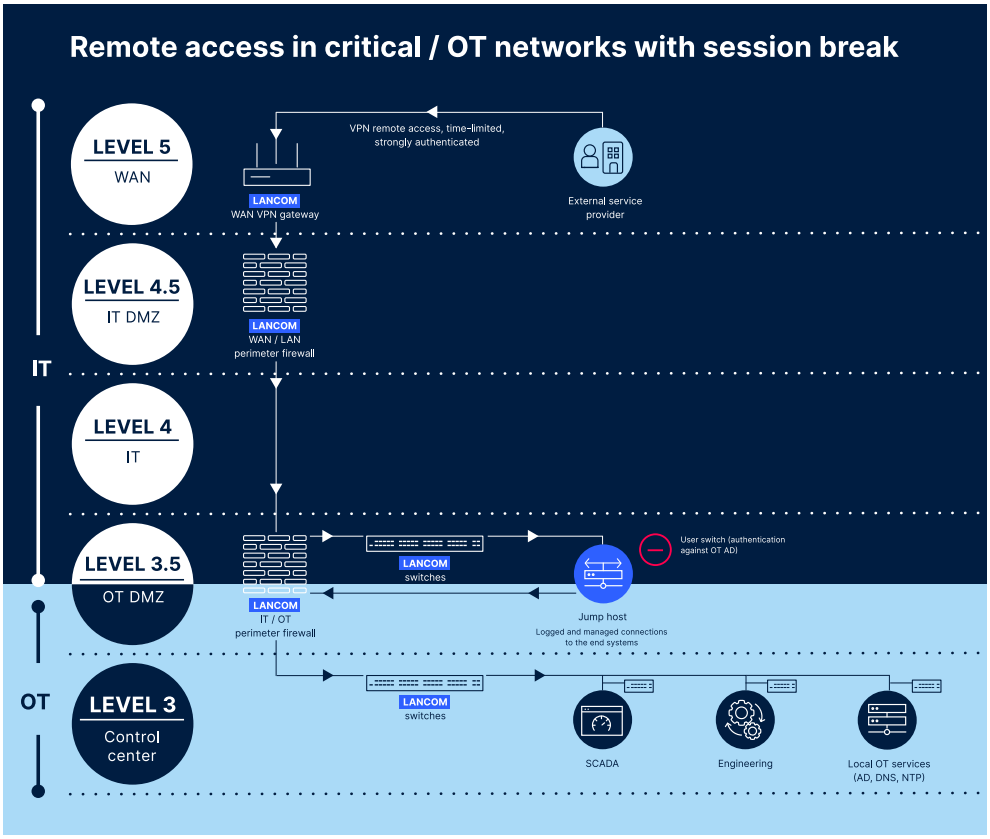
1. Terminate remote access in a dedicated OT remote segment (not in the productive OT network)
2. Firewall policy: default deny, explicitly allow only the jump host as the target
3. Jump host with roles/policies (who is allowed to access which target systems, for how long, and under which ticket)
4. Maintenance window process: activation only after approval; automatic deactivation after the defined time period
5. Enable session logging (session recording or at least command/audit logs) and store logs centrally

Verifiability / operations:

→ VPN and firewall logs: who, when, from where, and to which target

→ Jump host logs including session information and ticket/change references

→ Regular review of roles and permitted targets (least privilege principle)



Use case 2: Controlling and analytics require OT process data (data decoupling)

Initial situation:	A BI or controlling team wants to use process and status data from the OT environment for reports, KPIs, trend analyses, and compliance evidence.
Typical risks:	Direct access from IT systems generates additional load on productive OT systems; in the worst case, queries may affect operations. In addition, new attack paths are created.
Affected layers in the Purdue model:	Enterprise IT, the OT DMZ (Level 3.5), as well as OT systems at the operations management and process control level from which data is replicated in a controlled manner.
Target architecture:	The OT system provides data through a replica/historian in the OT DMZ. The IT system receives exclusively read-only access to this replica.

Implementation (practical approach):

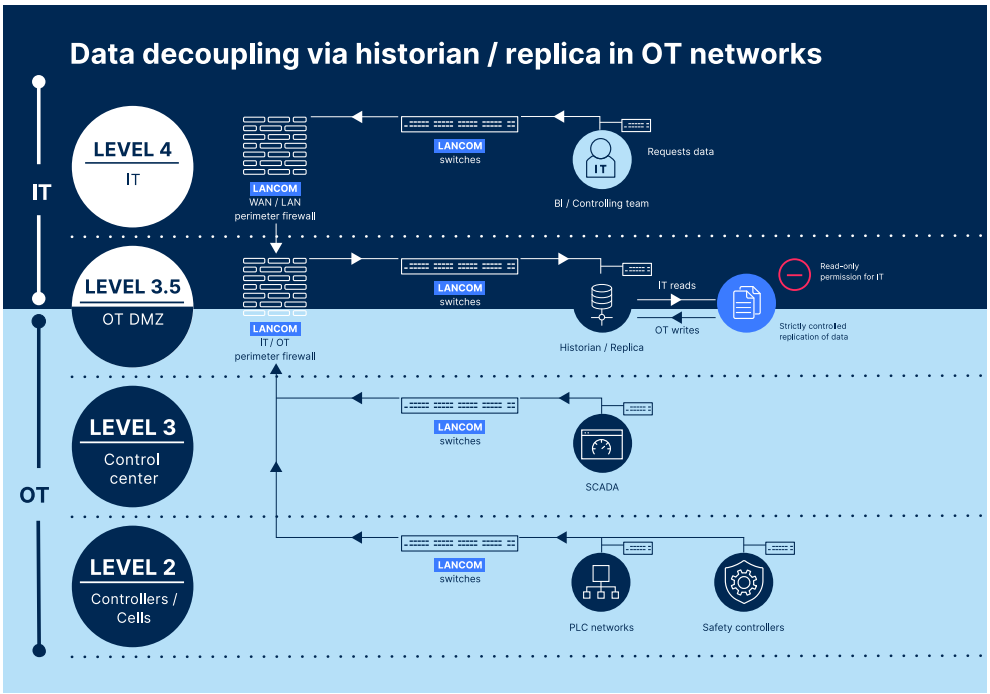
1. Place a historian/replica instance in the OT DMZ that receives data from the OT environment (write/sync)
2. Strictly define the replication path (only required data points, defined protocols/ports)
3. Permit IT access exclusively to the replica; productive OT systems remain non-addressable from IT
4. Use read-only accounts and separate identities (no shared OT administrator accounts)
5. Feed logging along the entire data chain into monitoring / SIEM (Security Information and Event Management) systems

Verifiability / operations:

→ Documented data model: which data is replicated and for what purpose

→ Firewall rules and read-only permissions as audit artifacts

→ Alerts for abnormal data volumes or unexpected access patterns



Use case 3: A security update for an OT server must be deployed (controlled update path)

Initial situation:	A manufacturer releases a security-relevant update. The OT environment must not have direct Internet access, and all changes must be validated.
Typical risks:	Uncontrolled update sources, lack of integrity verification, unclear rollback strategy, and updates performed outside maintenance windows.
Affected layers in the Purdue model:	External source or manufacturer, transfer and verification instances in the DMZ, as well as the respective affected OT systems in the upper OT layers.
Target architecture:	Updates are routed through a DMZ repository with integrity verification, an approval process, and scheduled deployment during a maintenance window.

Implementation (practical approach):

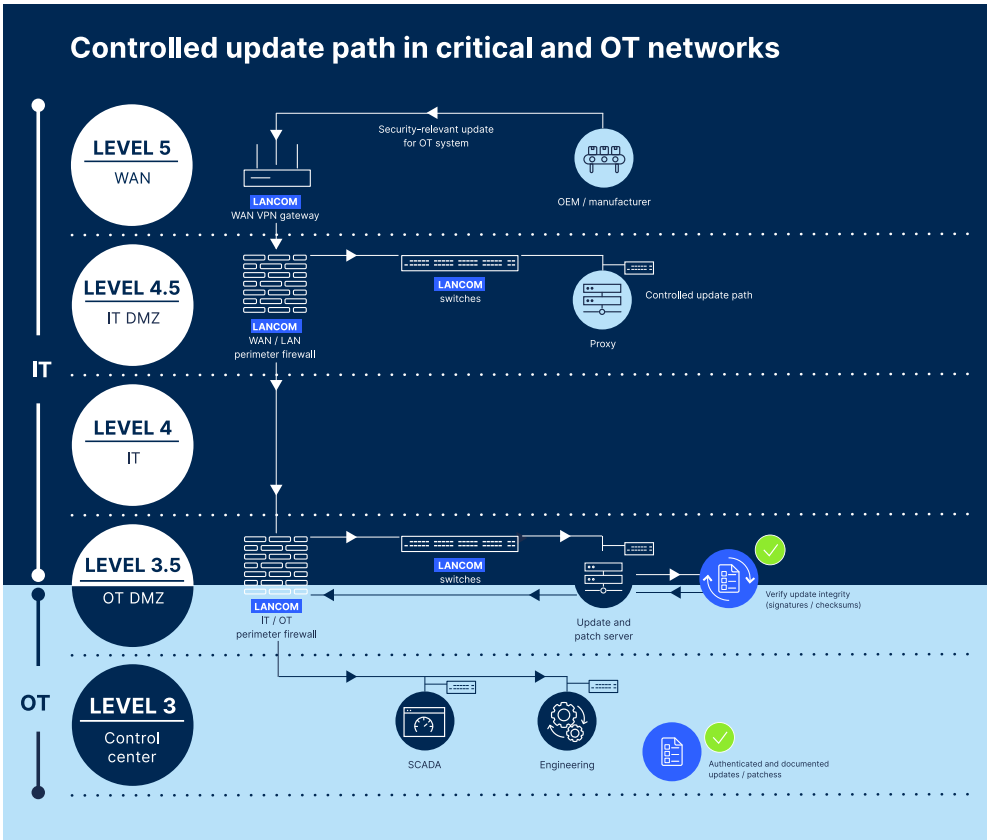
1. Operate an update/patch repository in the (OT) DMZ; OT systems obtain updates exclusively from this repository
2. Verify integrity/authenticity (signatures, checksums) and document the results
3. Perform testing/validation in a staging environment or on coordinated pilot systems (where possible)
4. Link approval and rollout to maintenance windows; define backup/rollback procedures
5. After rollout: perform functional testing and verify installed versions

Verifiability / operations:

→ Audit trail: source, checksum/signature verification, approval, timestamp, and affected systems

→ Change and incident references (ticketing), including responsibilities

→ Regular reporting: patch status by zones/system classes



Use case 4: Security incident in an OT zone – segment isolation without shutdown	
Initial situation:	Monitoring triggers an alarm due to unusual communication in a PLC cell. Operations should continue while the incident is being contained.
Typical risks:	Unclear segment boundaries, dependency on centralized IT services (DNS/NTP/authentication), lack of prepared isolation measures
Affected layers in the Purdue model:	Primarily horizontal segments within the OT environment, especially at the process control, control system, and cell levels; vertical transitions remain conceptually separated from this.
Target architecture:	All cells and OT services are segmented in such a way that an affected zone can be isolated without losing overall system operation (autonomy)

Implementation (practical approach):

1. Define cells/segments in such a way that critical process paths remain local.
2. Provide local OT services (e.g., DNS/NTP/authentication according to the concept) to minimize dependencies on IT/WAN services.
3. Isolation playbook: predefined measures (e.g., rules/ACLs) to disconnect a zone.
4. Design logging and monitoring paths so that events remain visible even in an isolated state (where possible).
5. After isolation: forensic preservation, restart plan, and controlled reintegration.

Traceability / operations:

→ Documented segment boundaries and isolation switches (technical/organizational)

→ Regular tests during maintenance windows (e.g., semiannual exercises)

→ Evidence: OT remains operational during defined fault scenarios

6. What role do network and security components play in OT and KRITIS security?

This chapter describes the roles of typical infrastructure components (switches, gateways, firewalls, remote access, and monitoring systems). The focus is on the role each component plays within the zones and conduits model and how it supports traceability and operations.

6.1 Firewalls

Firewalls implement the defined conduits in practice: default deny is the baseline, and communication is explicitly enabled via allow lists. In OT contexts, the focus is often on zone relationships (IT DMZ ↔ OT DMZ ↔ OT ↔ cells) and traceable policies, rather than primarily on traditional Internet access protection. Logging and — depending on protection requirements — redundancy/failover are key requirements.

6.2 Gateways / proxies

Gateways and proxies help decouple transitions and make content controllable (Layer 7, protocol, and destination control). Typical examples include controlled Internet access in the DMZ, reverse proxies for published services, and NAT (Network Address Translation)/address decoupling in networks with overlapping address ranges.

6.3 Remote access / VPN

In KRITIS environments, remote access requires significantly more security than simply using a VPN connection. Important factors include strong authentication (e.g., certificate + MFA), segment termination (dedicated remote segment), time limitations (maintenance windows), and auditable session logging. Access to OT targets is then performed via jump hosts rather than directly from the VPN.

6.4 Switches / port control

Switches form the basis for clean segmentation, port discipline, and the technical enforcement of local access policies. Depending on the operational concept, this may also include mechanisms such as NAC or 802.1X—always with fallback strategies to avoid jeopardizing operational capability. Important aspects include clearly documented segment boundaries, separated management paths, and logging capabilities for relevant events. Unused ports should be disabled or isolated so that “accidental” connections do not become the norm.

6.5 Monitoring / SIEM

Monitoring and SIEM are not traditional network components, but they are essential security functions for traceability, detection, and verifiability. They combine events from access activities, data flows, and changes into an end-to-end view. Clear traceability and rapid detection are based on logs. A meaningful design collects events along the critical chains (VPN, firewalls, proxies, jump hosts, relevant server and switch events) and consolidates them into a central monitoring / SIEM system. The objective is not to maximize log volume, but to achieve clear end-to-end visibility for access activities, data flows, and changes.

7. From planning to practical implementation: How to get your OT security initiative underway

Many OT security projects fail not because of the target architecture, but because of the transition into operational practice. The following procedural logic is intentionally kept simple and is suitable as a blueprint for project and operational planning.

1. Create a communication matrix
   Which systems communicate with which targets, via which protocols, for what purpose, and with what level of criticality?
2. Define a zones and transfer model
   Vertical separation (IT / IT DMZ / OT DMZ / OT) and horizontal segmentation (areas / cells).
3. Derive a rules and approval matrix
   Which conduits are permitted, who approves them, and how are changes documented?
4. Define operational processes
   Remote maintenance, updates, approvals, rollback, maintenance windows, exception processes.
5. Define a verification and monitoring concept
   Which events are logged, centrally correlated, and reviewed regularly?
6. Prepare incident and isolation playbooks
   Who is authorized to do what during an incident, which zone can be isolated and how, and how is controlled reintegration performed?

8. Checklist: What auditors and operations teams really need

- → Documented zones and conduits model (including responsibilities)
- → Default deny policy with justified allow lists and regular review
- → Secure remote maintenance as a process (approval, maintenance windows, jump host, logging)
- → Data decoupling for reporting (replica/historian, read-only, no IT queries against productive OT)
- → Controlled update path (repository in the DMZ, integrity verification, approval, rollback)
- → End-to-end logging in monitoring / SIEM (access, data, changes)
- → Resilience/autonomy: defined isolation during incidents, minimized IT / WAN dependencies

The measures described only achieve their full benefit when they are embedded into an actively practiced information security management system or OT security program—for example, based on ISO/IEC 27001 and IEC 62443-2-1.

9. Conclusion

A resilient KRITIS OT architecture is not defined by a long list of features, but by a few consistently implemented principles: transitions are deliberately designed (IT DMZ / OT DMZ), all communication is minimized and explicitly enabled (default deny / allow list), and privileged access is controlled through session breaks (jump hosts) and remains fully traceable (logging / SIEM).

If data flows are additionally decoupled (replica/historian) and changes are implemented in a controlled manner (update path with verification and approval), the result is an operational environment that remains both secure and reliable — even under KRITIS conditions such as narrow maintenance windows, long life cycles, and high availability requirements.

10. Glossary (brief)

Term	Definition
OT (Operational Technology)	Systems and networks used to control physical processes (e.g., automation, building technology, or security systems)
ICS	Industrial Control Systems; collective term for industrial/technical control systems, including OT components
SCADA	Supervisory control and monitoring systems (Supervisory Control and Data Acquisition) for processes and facilities
Level 3.5 / OT-DMZ	Transition zone between corporate IT and productive OT in the Purdue/IEC 62443-aligned reference model; used to decouple access activities, data flows, and changes.
Purdue-model / PERA	Reference model for the hierarchical structuring of OT/ICS architectures into levels. In this whitepaper, it serves in simplified form as an organizational framework for vertical separation, the OT DMZ, segmentation, and controlled communication flows; real-world environments deviate from this depending on the use case.
PLC	Programmable Logic Controller – controls machines/process steps
Zone	Security area with similar protection requirements and clearly defined communication rules
Conduit	Defined communication path between zones, typically controlled by firewalls/gateways
DMZ	Demilitarized Zone; transition zone that separates networks and makes transitions controllable (e.g., IT DMZ, OT DMZ)
OT DMZ	Intermediate layer between IT and OT, commonly used for jump hosts, patch repositories, and data replication
Allow list/whitelist	Principle: only explicitly permitted communication is allowed
Default deny	Principle: everything is prohibited until it is explicitly justified and enabled
Jump host / bastion host	System in the DMZ through which administrative access to target systems is routed and logged (session break)
Session break	Separation of a remote session: no direct channel from external access to the target system; the jump host provides the controlled transition
Historian / replica	Intermediate system for data collection or replication; OT writes/synchronizes, while IT typically has read-only access
NAC / 802.1X	Network Access Control; mechanisms for device/user authentication at the network port and for zone/role assignment
SIEM	Security Information and Event Management; centralized collection, correlation, and analysis of security events
MFA	Multi-factor authentication, e.g., an additional token/authenticator besides the password
RADIUS	Protocol for centralized authentication/authorization, commonly used for network access and MFA integration

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com