BEST PRACTICE GUIDE

BEST PRACTICE GUIDE - PART 1

Vendor-neutral best-practice framework for 3rd party access to Operational Technology (OT)

JUNE 2026, PART 1 - VERSION 1.21

Published by BifrostConnect, with Technical Review by **Mikael Vingaard, ICSRange.**

BIFROST connect

TABLE OF CONTENTS

ABOUT THIS PUBLICATION

BEST-PRACTICE FRAMEWORK FOR THIRD-PARTY OT ACCESS

3rd Party Access to Operational Technology in Critical Infrastructure

A Vendor-Neutral Best-Practice Guide for Increased Cybersecurity and Operational Resilience

June 2026

Part 1, Version 1.21

Published by BifrostConnect, Technical Review by Mikael Vingaard, ICSRange.

This document is Part 1 of a two-part publication. Part 2 (the BifrostConnect Implementation Guide, June 2026) is the implementation companion that maps each Part 1 control to a BifrostConnect deployment. All citations are traceable to primary sources listed at the end of this document - all three files must be distributed together; clause-level traceability depends on the source-verification companion.

EXECUTIVE SUMMARY

Third-party vendors with remote access into Operational Technology are now the most common entry path for the most consequential cybersecurity incidents in critical infrastructure. This guide describes the access pattern that closes the path, the standards that mandate it, and how a complete programme integrates it. This page is the two-minute version. The rest of the document is the evidence and the detail.

BIFROST connect

THE THREE THREATS THIS GUIDE ADDRESSES

First: legitimate remote-access channels weaponised by nation-state and criminal actors (Volt Typhoon, Sandworm, CyberAv3ngers). Second: vendor-laptop access into OT segments that bypass enterprise security stacks (Colonial Pipeline pattern, SektorCERT, attacks May 2023, public report November 2023). Third: standing privilege - credentials and tunnels that exist whether anyone is using them or not, providing an always-on attack surface.

THE FIVE CORE PRINCIPLES

1. Zero Standing Privilege. Access exists only inside a bounded window; before and after, privilege is zero. 2. The OT Island Principle. OT initiates outbound; OT does not accept inbound. 3. Defence in depth. No single control is load-bearing; six layers wrap the asset, including session evidence and monitoring so that misuse is detected and answered, not only prevented. 4. Minimum viable controls scale to context. The same five common control gates (identity, authorisation, session evidence, kill-switch, supply-chain assurance) apply across every pattern, but the implementation depth scales with maturity. 5. Verification over assumption. Every claim in this guide is anchored in a verifiable clause; every implementation should be acceptance-tested. Zero Standing Privilege, the OT Island Principle, and Defence in Depth each anchor a dedicated section below; the remaining two principles are cross-cutting and applied throughout the patterns and methodology.

THE FOUR ACCESS PATTERNS AT A GLANCE

Pattern	Where it applies	Primary control
A · Large OT, customer station	Utility, pharma, large-scale industrial - station owned and managed by customer	Enterprise IAM + jump host + PAM wraps the existing station
B · Large OT, vendor laptop	Large-site commissioning - vendor laptop enters the network	NAC + vendor DMZ + OT-IDS contain an untrusted device
C · Small OT, customer station	Small water utility, district heating - station present, no IT staff	Control sits at the station: local identity + offline MFA + recording + log export
D · Small OT, vendor laptop	Hardest case: small utility plus vendor-owned device with no enterprise infra	Hardware broker at the boundary: scoped access + session evidence + log export

Each pattern is treated in full under Four OT Access Patterns later in this guide. The table above is the at-a-glance version; the detailed sections give the per-pattern controls, framework anchors, and failure modes.

RECOMMENDED FIRST ACTIONS (30 DAYS)

Inventory every active third-party remote-access path into OT. 2. Verify default credentials have been changed on all jump hosts, VPN concentrators, shared accounts, and every other network-reachable device. 3. Enable session logging on existing remote-access channels. 4. Identify the assets that fall under each of Patterns A through D. 5. Plan migration of any always-on tunnel toward time-bounded access. The detailed phase plan is in section Implementation priority.

This guide is one element of a complete cybersecurity programme. Per IEC 62443-2-1:2024, asset owners are required to maintain a Cybersecurity Management System (CSMS) covering risk analysis, access control, supplier governance, and incident response. This guide addresses third-party access; readers building a complete OT cybersecurity programme should treat it as one chapter, not the whole book.

THE CENTRAL INSIGHT

Every remote session a third-party vendor opens into Operational Technology is a potential supply-chain risk vector. The risk is rarely the vendor alone; it is the architecture that lets a single set of standing credentials become a standing path into a Programmable Logic Controller (PLC) or Supervisory Control and Data Acquisition (SCADA) station, compounded where the supplier's own security maturity is low. The problem is not Virtual Private Network (VPN) as a technology. NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, recognises VPN as a valid component of strong authentication and encryption for remote access. The 2015 attack on the Ukrainian power grid is the canonical illustration: adversaries operated SCADA through legitimate remote access and stolen VPN credentials, not through a flaw in VPN itself. The problem is flat, persistent, multi-purpose remote access without per-session brokering, time-bounding, or evidence. The fix is brokered, time-bound, recorded, and revocable access.[1]

This guide presents that pattern in vendor-neutral terms, anchored in eight frameworks: the EU NIS2 Directive (2022/2555); the Danish NIS2 implementation (LOV nr. 434 af 6. maj 2025 - Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau); BEK nr. 260 af 6. marts 2025 with the underlying Danish law on resilience and preparedness in the energy sector; the IEC 62443 series, specifically IEC 62443-3-3:2019 (system security requirements), IEC 62443-2-4:2024 (service provider security programme), and IEC 62443-2-1:2024 (asset owner cybersecurity programme); NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security (2023); NIST SP 800-207

[1] NIST SP 800-82r3, Guide to OT Security. Retrieved 2026-04-22.

(Zero Trust Architecture, 2020); the joint UK-led NCSC Secure Connectivity Principles for Operational Technology (published 18 March 2024); and the joint US-led CISA Adapting Zero Trust Principles to Operational Technology (29 April 2026). Where a claim cannot be traced to a specific verified clause, this guide does not make it.[2]

ARCHITECTURAL NEUTRALITY

This guide describes requirements and principles, not a specific architecture. Organisations may implement these requirements through various architectural approaches including but not limited to: VPN combined with Privileged Access Management, hardware-enforced network segmentation with out-of-band access broker, cloud-brokered session management, traditional jump-host designs with strict access governance, or hybrid combinations thereof. Where this guide describes specific implementation patterns (for example brokered, time-bounded sessions in Figure 2 panel B), the patterns are illustrative of how the principles can be satisfied, not the only architecture that satisfies them.

AUDIENCE

Chief Information Security Officers (CISOs), OT security architects, compliance officers, and risk managers at critical infrastructure operators. Also relevant for system integrators, vendors performing remote work into customer OT, and auditors evaluating third-party access controls.

SCOPE

This guide covers third-party remote access to OT systems via controlled conduits, where a human operator (vendor technician, engineer, integrator) initiates a session into operational technology. Out of scope: physical site access, IT-only systems above the demilitarised zone (DMZ), the broader OT-IT convergence in the office layer, and machine-to-machine (M2M) traffic between OT components. M2M access does not involve a human session and therefore cannot be addressed by session brokering or recording; for device-level identity and authentication of M2M traffic, readers should reference IEC 62443-4-2 (technical security requirements for IACS components). The guide is deliberately vendor-neutral; it names control patterns and standard clauses, not products.

[2] NCSC UK, "Secure connectivity principles for operational technology (OT)", Principle 5: Harden your OT boundary. Published 18 March 2024. Retrieved 2026-05-06.

METHODOLOGY AND LIMITATIONS

Every claim in this guide is traceable to a clause-level entry in the source citations below, which records verbatim primary citations from the official PDFs and licensed standards: NIS2 (EU 2022/2555), the Danish NIS2 implementation act (LOV nr. 434 af 6. maj 2025), BEK nr. 260 af 6. marts 2025 for the energy sector, NIST SP 800-207, NIST SP 800-53 Rev. 5, NIST SP 800-82 Rev. 3, and the IEC 62443 series, specifically DS/EN IEC 62443-3-3:2019 (system security requirements), DS/EN IEC 62443-2-4:2024 (service provider security program requirements), and DS/EN IEC 62443-2-1:2024 (asset owner cybersecurity programme requirements).[3]

The guide also draws on the joint UK-led Secure Connectivity Principles for Operational Technology (NCSC et al., published 18 March 2024) and the joint US-led CISA Adapting Zero Trust Principles to Operational Technology (CISA, DoW, DOE, FBI, DOS with NIST contributions, 29 April 2026). Empty cells in the compliance crosswalk (Figure 7) are deliberate and labelled with the reason; they are honest gaps, not fabricated coverage.

Per IEC 62443-2-1:2024, asset owners are required to maintain a cybersecurity management system (CSMS) covering risk analysis, access control, supplier governance, and incident response. This guide addresses one element of that programme: third-party operational technology access. Readers building a complete OT cybersecurity programme should treat this guide as one chapter, not the whole book.

Two distinct claim types appear in this guide. REQUIREMENT statements reproduce the wording of a specific legal or standards clause and carry a direct citation to its source PDF. GUIDE INTERPRETATION statements express this guide's reading of how a requirement should be met in practice; they build on primary text but add engineering judgment. The two are distinguished in-line where the distinction is load-bearing for an audit reader, using the labels REQUIREMENT and GUIDE INTERPRETATION in bold small caps.

[3] DS/EN IEC 62443-3-3:2019. Single user license, BifrostConnect ApS, retrieved 2026-05-04.

AUTHOR'S SUPPLY-CHAIN DISCLOSURE

BifrostConnect is the publisher of this guide and is itself a third-party vendor inside its own customer environments. The same principles advocated here - brokered, time-bound, recorded, and revocable access - govern BifrostConnect's own operational and support access to customer systems.

This guide presents an architectural pattern that would hold even if BifrostConnect were not the publisher; the pattern is intellectually consistent with how any serious third-party vendor, including this one, should be treated by an asset owner. The architectural patterns described in this guide align with the publisher's product approach, which may create blind spots regarding alternative architectures; readers are encouraged to read the Architectural neutrality section above and to evaluate alternative implementations on their own merits. Product-anchored implementation detail is deliberately deferred to the companion document BifrostConnect Implementation Guide (Del 2).

THE PURDUE MODEL:
A SHARED REFERENCE FRAME

Before any control discussion, this guide adopts the Purdue Model as a shared vocabulary for OT zones. The model originated in the Purdue Enterprise Reference Architecture (Theodore Williams, 1990) and was subsequently adopted by ISA-95 / IEC 62264 and by NIST SP 800-82 Rev. 3 as the standard reference frame for industrial control system (ICS) topology.

Level 3.5 is an industrial DMZ layer that sits between Level 3 and Level 2; it is not a Purdue level in the original sense but is consistently treated as a named zone in modern OT architectures and in NIST SP 800-82 Rev. 3. Six Purdue levels, plus an industrial demilitarised zone (DMZ) at Level 3.5, from top to bottom: Level 5 Enterprise (Enterprise Resource Planning, Customer Relationship Management, business email); Level 4 Business Logistics (Manufacturing Execution Systems, scheduling); Level 3 Site Operations (historian, plant-level analytics); Level 3.5 the OT demilitarised zone (jump host, vendor proxy); Level 2 Area Supervisory (Human-Machine Interface, SCADA); Level 1 Basic Control (PLC, Remote Terminal Unit); Level 0 Physical Process (sensors, actuators).

The deeper the zone, the higher the blast radius and the fewer the legitimate remote-access use cases. Third-party access typically targets Levels 2 and 1, where engineering tools meet controllers. That is the zone this guide is about.

FIGURE 1. The Purdue Model

Six Purdue levels plus an industrial DMZ at Level 3.5, from enterprise IT down to the physical process.

Level 3.5 is an industrial DMZ layer between Level 3 and Level 2.
It is not a Purdue level in the original sense, but is consistently treated as a named zone in modern OT architectures and in NIST SP 800-82 Rev. 3.

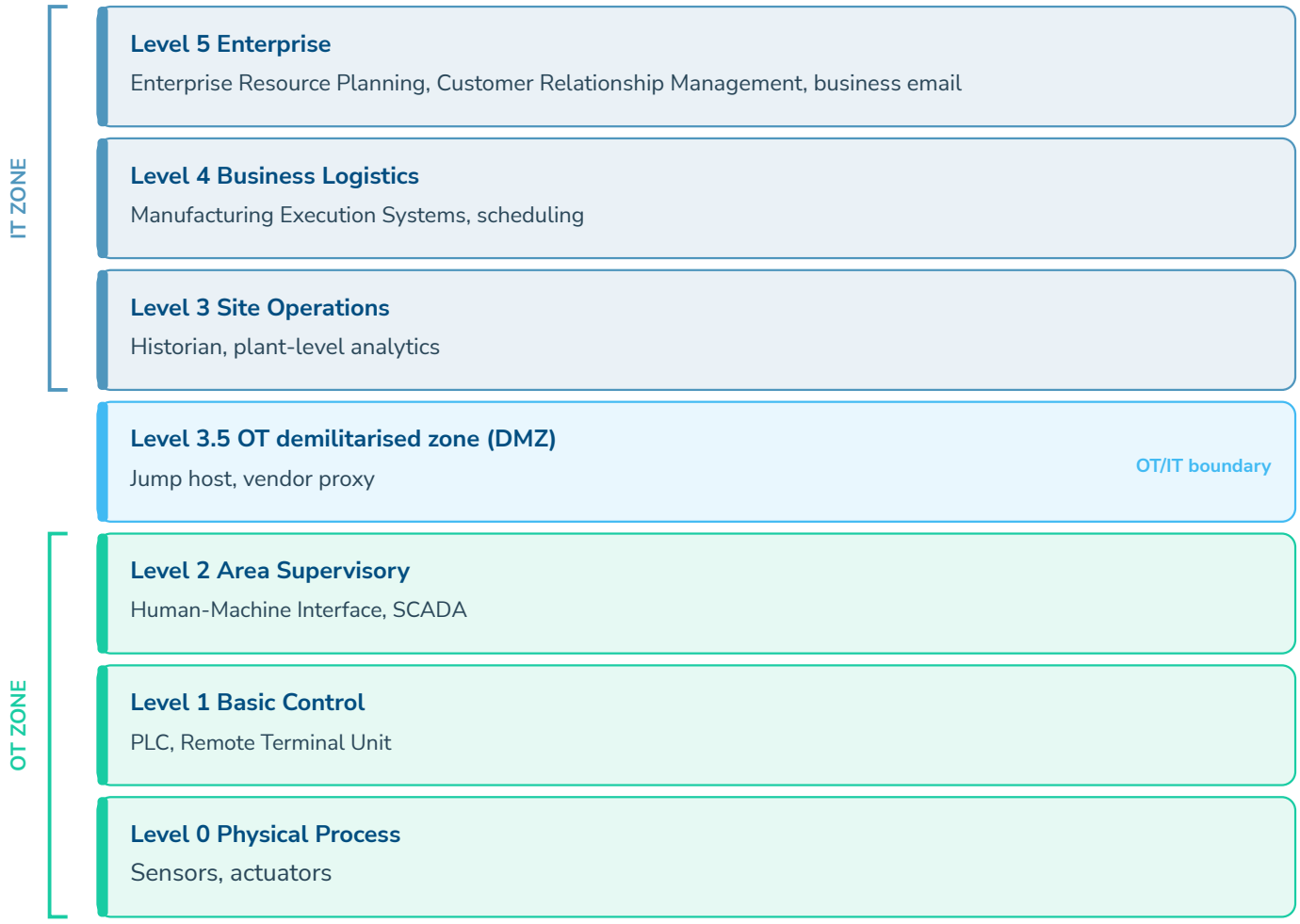


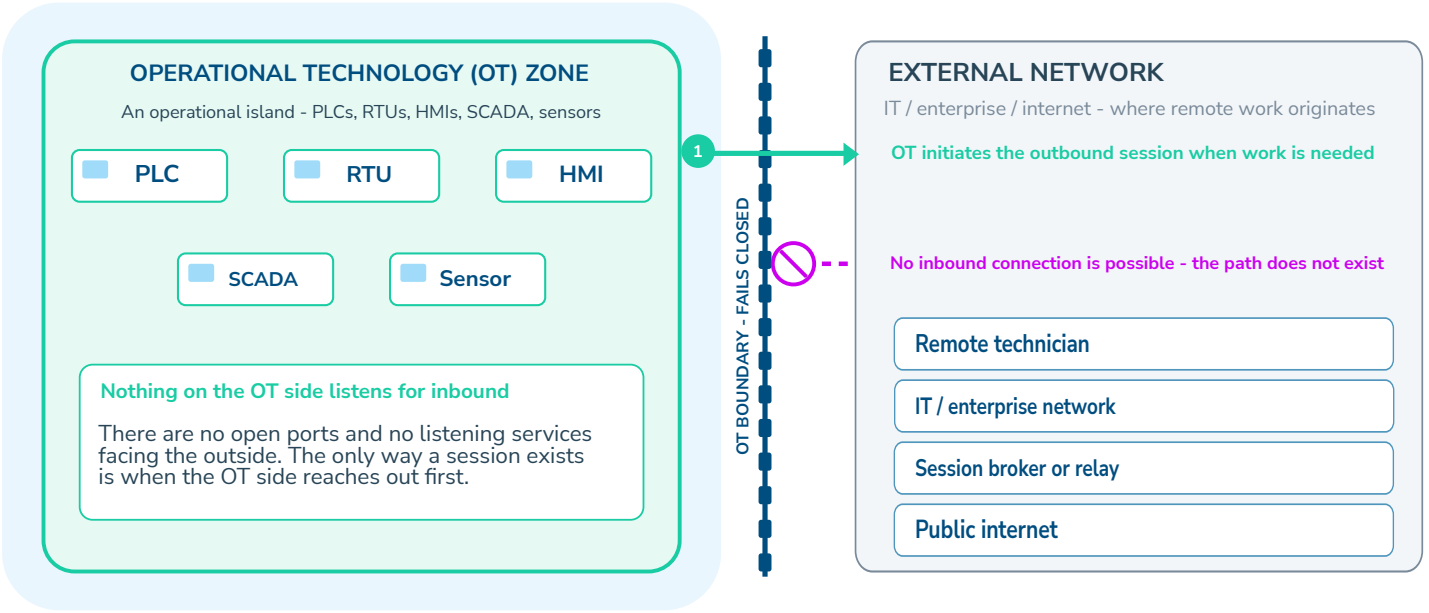
Figure 1. The Purdue Model. Six Purdue levels plus an industrial DMZ at Level 3.5, with blast radius increasing from Level 5 to Level 0. Third-party access typically targets Levels 2 and 1. Source: ISA-95 / IEC 62264 reference architecture; NIST SP 800-82 Rev. 3.

THE OT ISLAND PRINCIPLE

A single directional rule governs the architecture of every defensible pattern in this guide: OT calls out (initiates outbound). OT never receives. The operational zone initiates outbound sessions to an external broker when work is needed; the zone does not accept inbound connections from any external network. Inbound paths are structurally absent, not blocked by configuration. This principle is the shape common to Patterns A through D, and it is the structural answer that lets a single pattern satisfy disparate regulatory regimes at once.

The OT Island Principle

OT initiates outbound; OT never accepts inbound. Inbound paths are structurally absent, not merely blocked by configuration.



Vendor-neutral. The OT Island Principle: OT calls out, OT never receives.

Anchors. NIST SP 800-207 Tenet 3 (per-session access) and Tenet 6 (dynamic, strictly enforced authentication and authorisation) together describe an access model in which the resource does not listen for callers; the caller requests, and a policy engine grants. IEC 62443-3-3 SR 1.13 (access via untrusted networks) requires the control system to monitor and control all methods of access to the

control system via untrusted networks; the cleanest way to monitor and control is to not accept them inbound at all. The OT Island Principle is the architectural phrasing of these two anchors.[4]

***Brownfield reality**. Most OT environments contain legacy systems that require inbound connections, lack outbound-only capability, or run protocols pre-dating modern segmentation. The OT Island Principle remains the target for new builds, refurbishments, and any system whose vendor offers a path to outbound-only operation. Where migration cannot be immediate, compensating controls shall include continuous monitoring of inbound paths, strict session time-boxing, VLAN isolation of legacy segments, and an explicit migration plan with a verified end date. The principle is the destination toward which exceptions migrate.*

WHY NOW

Two regulatory shifts make 2024 to 2026 the inflection point for third-party OT access. First, the EU NIS2 Directive (2022/2555) replaced checklist compliance with outcome-based, board-accountable risk management. Article 21(2) names ten technical and organisational measures that essential and important entities must implement. Three of them bear directly on third-party access: litra (d) supply-chain security, litra (i) human resources security, access control policies and asset management, and litra (j) multi-factor authentication.

Second, in the Danish energy sector, Lov om styrket beredskab i energisektoren §§ 6, 7 and 8 codify the same direction at national law. §6 stk. 2 nr. 3 requires identification and access-control policies that protect against unauthorised access. §6 stk. 2 nr. 7 imposes supply-chain security between the entity and its direct suppliers and service providers. §8 stk. 2 nr. 6 requires logging that supports alarms, investigation, and incident handling. §8 stk. 2 nr. 10 requires MFA or continuous authentication and access protection against unauthorised access. BEK 260, the executive order issued under this law, derives its technical detail directly from §§ 6 to 8.

The pattern is consistent across both instruments: the regulator is no longer asking whether the firewall is configured. The regulator is asking who accessed what, when, for what work, with what approval, and where the evidence is. This guide answers those questions in pattern terms.

[4] NIST SP 800-207, Zero Trust Architecture. Retrieved 2026-04-22.

THIRD-PARTY ACCESS TODAY VERSUS A DEFENSIBLE PATTERN

The most common pattern observed across OT environments is also the most exposed: the third-party vendor connects through an always-listening VPN concentrator into a flat OT LAN, where credentials persist beyond the work, the network path stays open between sessions, and no recording exists of what happened inside the zone. Lateral movement to a PLC is unaudited, because nothing was watching.

A defensible pattern looks structurally different. The vendor authenticates against an identity broker that requires multi-factor authentication and per-session approval. On approval, a session broker mediates the connection into the OT zone, records the session, and terminates it on a timer. Logs flow outward through a unidirectional channel to an audit vault; no inbound path is opened by the act of recording.

FIGURE 2. Common today vs. defensible pattern

Two-pattern reference for third-party access into operational technology. Vendor-neutral.

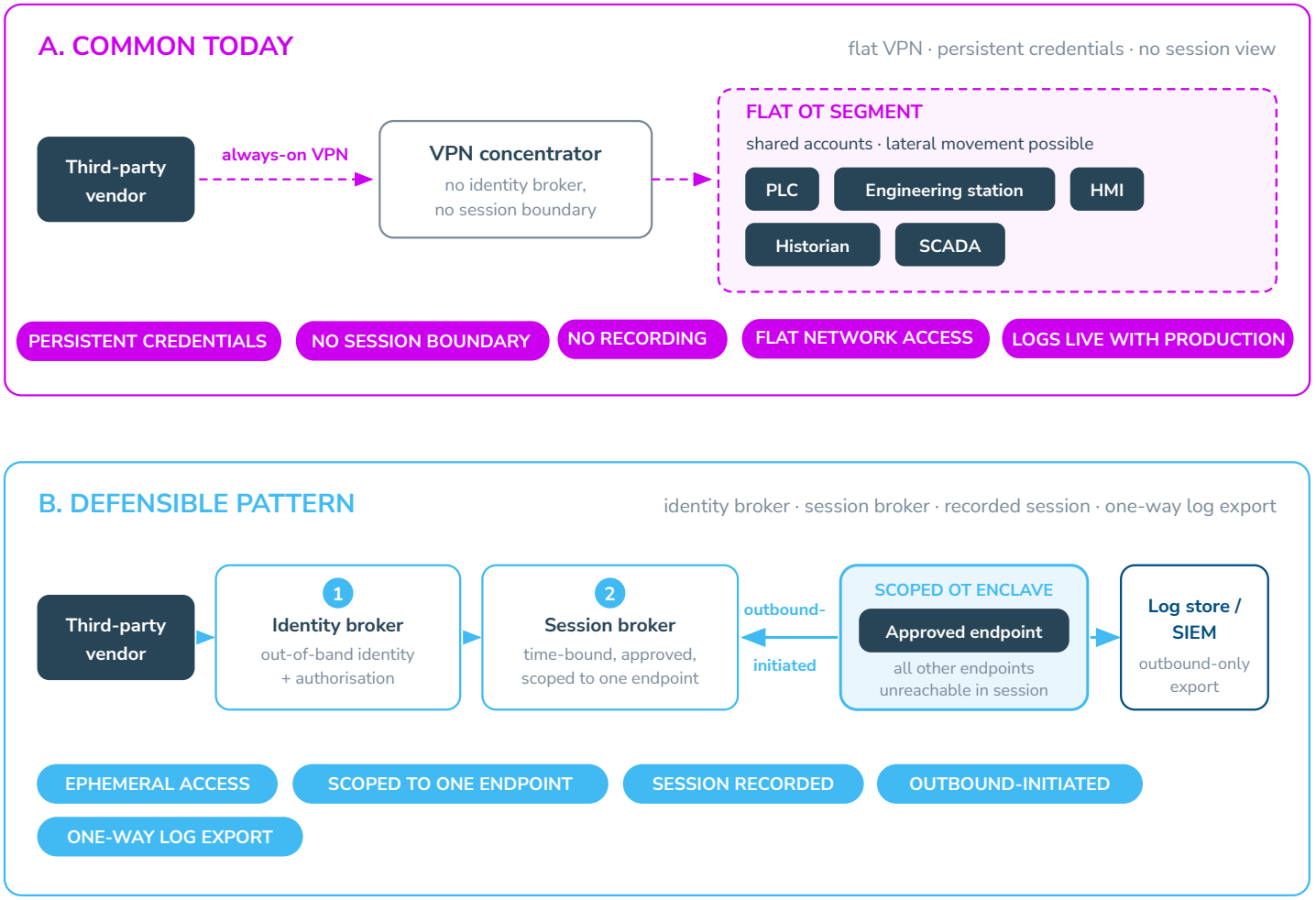


Figure 2. Common today vs. defensible pattern. Two-panel reference for third-party access into operational technology, vendor-neutral. Panel A (top) shows the most exposed pattern still in production use (persistent VPN credentials, flat OT segment, no session boundary). Panel B (bottom) shows the defensible pattern this guide describes (identity broker, session broker, recorded session, one-way log export).

THREAT CONTEXT

The pattern in the previous section is not compliance theatre. It is an operational response to a concrete and escalating threat landscape. Three named actor groups illustrate the risk profile that third-party OT access must now defend against.

Sandworm (also tracked as APT44 and attributed by Mandiant and CISA to GRU Unit 74455) deployed the Industroyer2 and CaddyWiper malware against Ukrainian electricity substations in April 2022. Industroyer2 is specifically designed to manipulate electricity substation equipment (IEC 60870-5-104); CaddyWiper destroys data on Windows hosts. The intrusion chain relied on pre-existing access into the OT environment, which is exactly the exposure a flat vendor tunnel creates. Reference: CERT-UA advisory (April 2022); Mandiant APT44 profile (2024).

Volt Typhoon is a People's Republic of China state-sponsored group tracked jointly by CISA, NSA and Five Eyes partners. The 7 February 2024 CISA advisory AA24-038A documents the group's pre-positioning activity inside United States critical infrastructure, including energy, water and transport sectors, using compromised small-office and home-office (SOHO) devices and living-off-the-land (LOTL) techniques to avoid detection. The advisory describes the pattern as deliberate positioning for future disruptive or destructive effects, not espionage. Reference: CISA Advisory AA24-038A (7 February 2024).

CyberAv3ngers is a group of IRGC-affiliated cyber actors, per CISA Advisory AA23-335A. CISA Advisory AA23-335A (1 December 2023) documents the group’s exploitation of internet-exposed Unitronics Vision series programmable logic controllers at multiple United States water utilities in late 2023. The attack vector was default credentials on devices reachable from the public internet – the low-end of the same exposure profile that unbrokered third-party remote access creates. Reference: CISA Advisory AA23-335A (1 December 2023).

LIVING OFF THE LAND AND THE CASE FOR SESSION BROKERING

Across these and similar intrusions, a recurring technique is the abuse of legitimate remote-access sessions and built-in operating system binaries, known as living off the land (LOTL). CISA Advisory AA24-038A and the joint guidance Identifying and Mitigating Living Off the Land Techniques (February 2024) both describe the pattern: an attacker who has obtained a foothold in a legitimate remote session can avoid detection by using tools that are already present and expected on the host. The direct structural response is session brokering with recording: if the only way a vendor session reaches the zone is through a broker that records what is entered and what is executed, LOTL behaviour generates evidence even when the tooling itself looks legitimate.

REFERENCE INCIDENTS FOR THE ‘WHY SHOULD I CARE’ QUESTION

Three publicly reported incidents answer the question in concrete terms. The 2021 Colonial Pipeline ransomware incident reached the billing systems through a compromised, unbranded VPN account with no MFA, and the operational fuel shutdown followed from the business decision to halt pipeline operations.
The 2023 SektorCERT disclosure of the coordinated attack against 22 Danish energy companies documents the value of sector-level detection and of disciplined remote-access control; the SektorCERT report itself is the primary Danish reference document on OT intrusion patterns and the value of collective defence. TRITON / TRISIS, first reported by FireEye and Dragos in December 2017, targeted a Saudi Arabian petrochemical safety instrumented system and is the reference incident for attacks reaching the safety-integrity layer, not only the control layer. References: CISA and FBI joint advisory on Colonial Pipeline (2021); SektorCERT rapport (November 2023); Dragos TRITON analysis (2017-2018).[5]

ZERO STANDING PRIVILEGE

Privilege without a timer is the real vulnerability, not the person holding it. Zero Standing Privilege (ZSP) means access does not exist between sessions. Every session is requested, evaluated against current policy, opened for a bounded window, and revoked at close. The control surface moves from credential possession to session lifecycle.

ZSP is anchored in two places. NIST SP 800-207 Tenet 3 states that access to individual enterprise resources is granted on a per-session basis. Tenet 6 requires that all resource authentication and authorisation are dynamic and strictly enforced before access is allowed. IEC 62443-3-3 SR 2.6 requires the system to terminate a remote session either by user action or after an inactivity period; SR 2.1 requires authorisation enforcement for all human users to support segregation of duties and least privilege.

[5] SektorCERT, "Angrebet i november 2023". Retrieved 2026-05-04.

FIGURE 3. Standing privilege vs. Zero Standing Privilege

Two access models on a 24-hour timeline. Vendor-neutral.

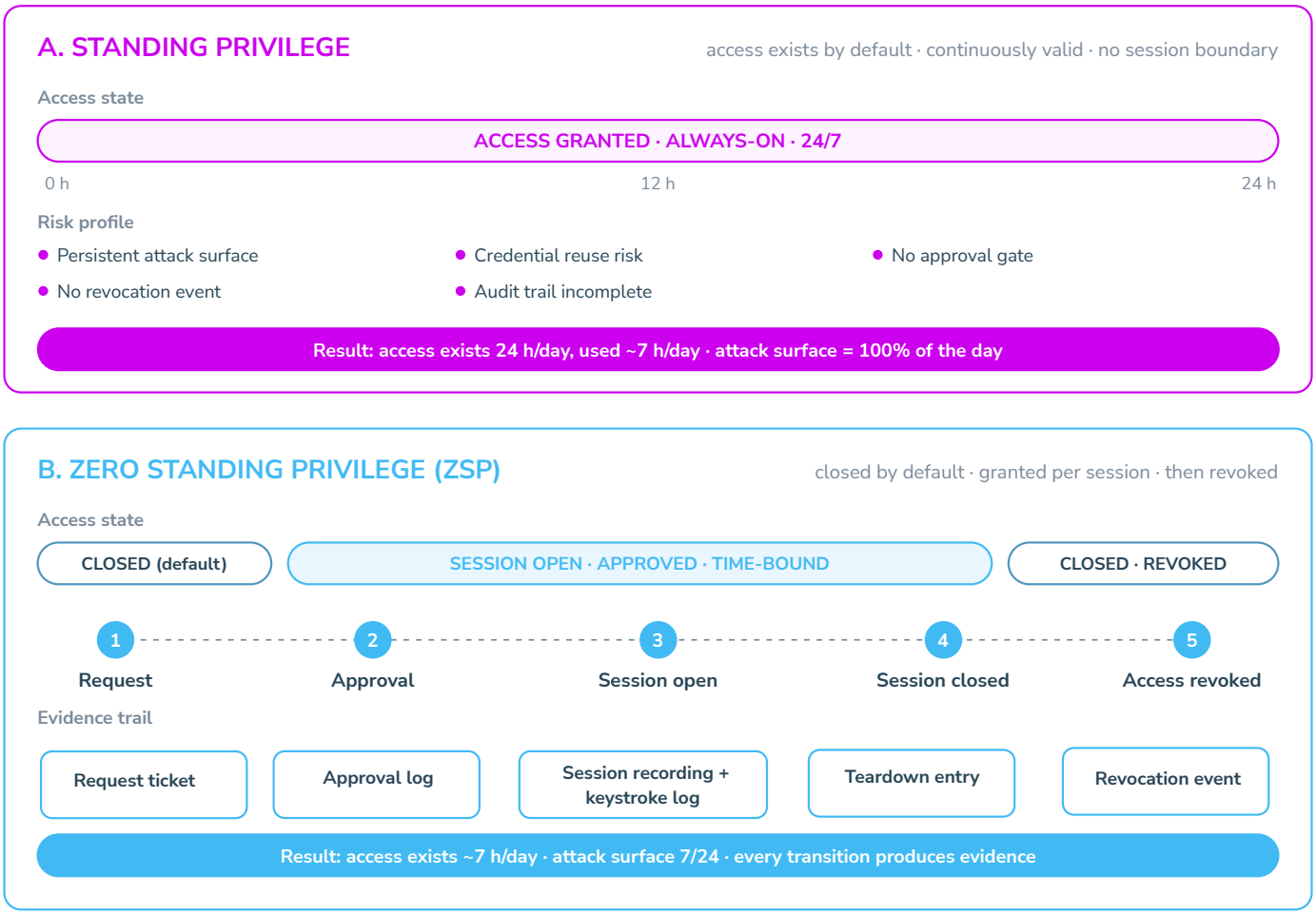


Figure 3. Standing privilege (always on) compared to Zero Standing Privilege (a single bounded window with five labelled transitions: Request, Approval, Session open, Session closed, Access revoked). Anchors: NIST SP 800-207 Tenets 3 and 6; IEC 62443-3-3 SR 2.1, SR 2.6.

FOUR OT ACCESS PATTERNS

Not all third-party OT access is the same problem. Two dimensions shape what control is achievable in practice: site scale (the level of enterprise infrastructure available to wrap the access path) and where the programming software runs (on a customer-owned, customer-managed station, or on a vendor-owned laptop the vendor brings to the work).

The two dimensions yield four patterns. The axis framing is observational, drawn from field experience across OT deployments rather than from a single standard. The controls inside each quadrant, however, map only to verified clauses in the cited frameworks. These four patterns expand the at-a-glance summary in the Executive Summary (The Four Access Patterns at a Glance): the summary gives the one-line version of each pattern, while this section gives the per-pattern controls, framework anchors, and failure modes.

FIGURE 4. Four OT access patterns

Site scale by where the software runs. Each quadrant maps to a scenario and a risk level.

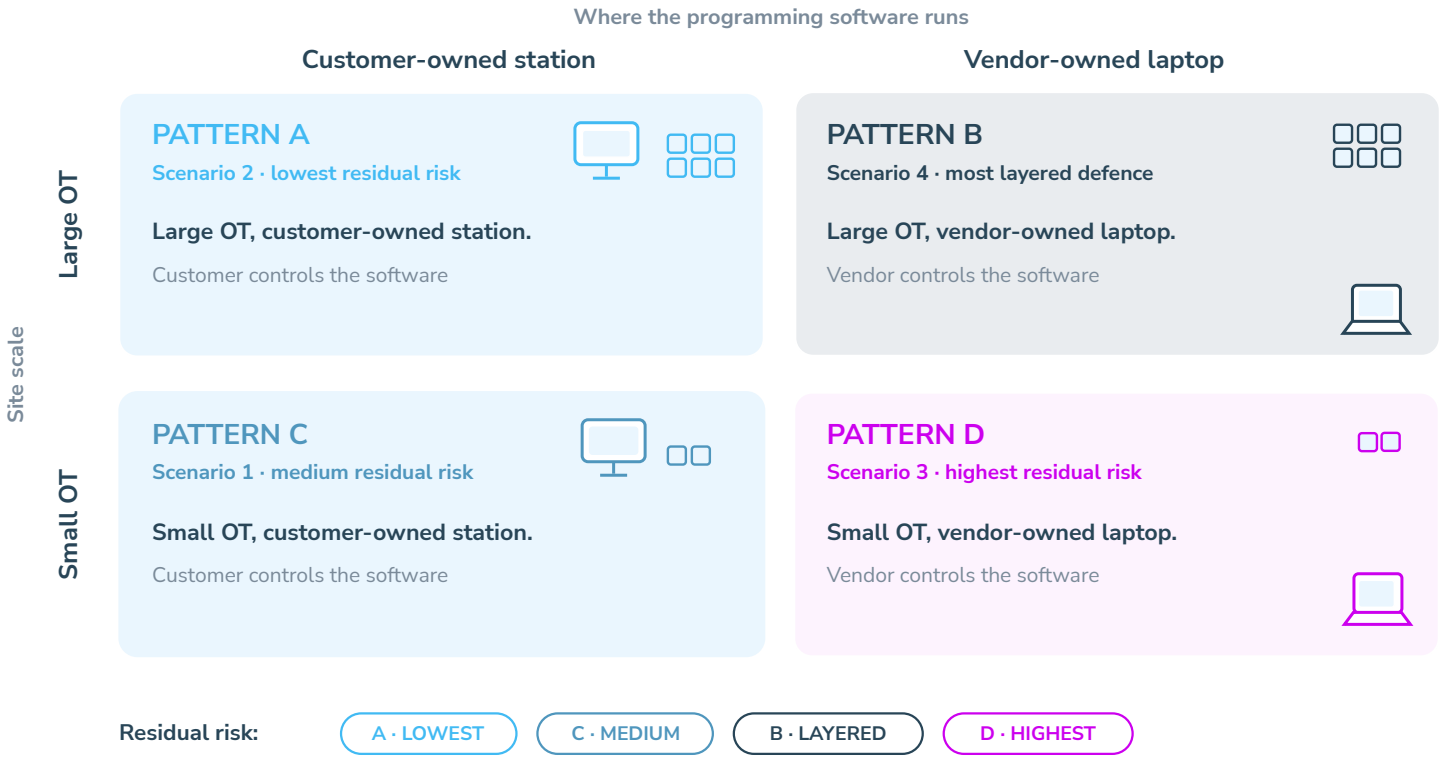


Figure 4. Four OT access patterns. Site scale (Large / Small) by where the programming software runs (Customer-owned station / Vendor-owned laptop). Per-quadrant controls anchored in IEC 62443-3-3:2019 SR 1.1, 1.13, 2.1, 2.6; NIS2 Article 21(2)(d), (i), (j); Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 10; NCSC UK Principles 2 (limit the exposure of your connectivity) and 7 (logging and monitoring).

PATTERN A: LARGE OT, CUSTOMER-OWNED STATION (SCENARIO 2)

The third-party vendor logs into a station the customer owns, manages, and patches. Typical settings: large utility operator, pharmaceutical manufacturer, transport operator. Enterprise infrastructure is available: directory services, jump hosts, Security Information and Event Management (SIEM), Privileged Access Management (PAM), and a Security Operations Centre (SOC). The control problem is integration, not invention.

Defensible controls in this pattern. Identity: the vendor's account exists in the customer's identity broker and inherits its lifecycle (joiner, mover, leaver). MFA is enforced at the broker, supporting NIS2 Article 21(2)(j) and Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 10. Approval: a per-session ticket is required before the session opens, in support of NIST SP 800-207 Tenet 6 and IEC 62443-3-3 SR 2.1. Mediation: the session traverses a jump host or PAM session broker that records the session and terminates it on inactivity, providing evidence for IEC 62443-3-3 SR 2.6 and FR 6. Network: the path into the OT zone exists only for the duration of the approved session, in line with IEC 62443-3-3 SR 1.13. Evidence: session recording is shipped to the SIEM via the SOC's existing log pipeline, providing evidence for Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 6.

Failure mode to watch for: the standing PAM credential. PAM systems are often configured with a long-lived service account that satisfies the audit requirement but defeats Zero Standing Privilege. The control is rotation discipline plus session-bound credential issuance, not the existence of PAM.

PATTERN B: LARGE OT, VENDOR-OWNED LAPTOP (SCENARIO 4)

The third-party vendor brings their own equipment into a managed OT zone. Typical setting: large-scale commissioning of new automation, where the vendor's laptop carries the engineering software licences and the customer's environment must accept the device for the duration of the project. Enterprise infrastructure is available but the device entering the network is not customer-managed. Device posture cannot be assumed.

Defensible controls in this pattern. Network Access Control (NAC) gates which devices may attach; the vendor laptop receives a posture-attested attachment to a vendor demilitarised zone (vendor-DMZ) rather than the operational network directly. An OT intrusion detection system (OT-IDS) monitors the resulting traffic into Level 2 and Level 1 for anomalies. Identity, approval, mediation and evidence controls follow Pattern A. The key delta is the boundary: the vendor's device is treated as untrusted regardless of vendor reputation. NIS2 Article 21(2)(d) supply-chain security is the legal anchor, with BEK 260 §§29-32 providing the operational specifics for supplier procedures and remote-access procedures for direct suppliers; NCSC UK Principles 2 (limit the exposure of your connectivity) and 5 (Harden your OT boundary) are the operational anchors.[6]

Failure mode to watch for: the implicit trust gradient. Once a vendor laptop has been on the network for weeks, the controls around it tend to relax. The discipline is to treat each session as a new posture check, not a renewal of the previous trust decision.

[6] Regulation (EU) 2022/2555 (NIS2 Directive), Article 21(2)(d) and recital 81. Retrieved from EUR-Lex CELEX 32022L2555, 2026-04-22.

PATTERN C: SMALL OT, CUSTOMER-OWNED STATION (SCENARIO 1)

The third-party vendor logs into a customer-owned engineering station at a site with no on-site IT staff. Typical settings: a small water utility, a district heating remote business unit (RBU), a regional automation site. Internet connectivity is unreliable or prohibited by policy. There is no jump host, no SIEM, no SOC. The control surface must sit at the station itself.

This is the pattern most often misread. The common claim is that a small site without enterprise infrastructure cannot meet NIS2 or Lov om styrket beredskab i energisektoren. That claim is false. Five station-local controls satisfy the same regulatory clauses without requiring any live network path.

FIGURE 5. Quadrant C unpacked

Five control points that bridge vendor-to-station without a live network. Vendor-neutral.

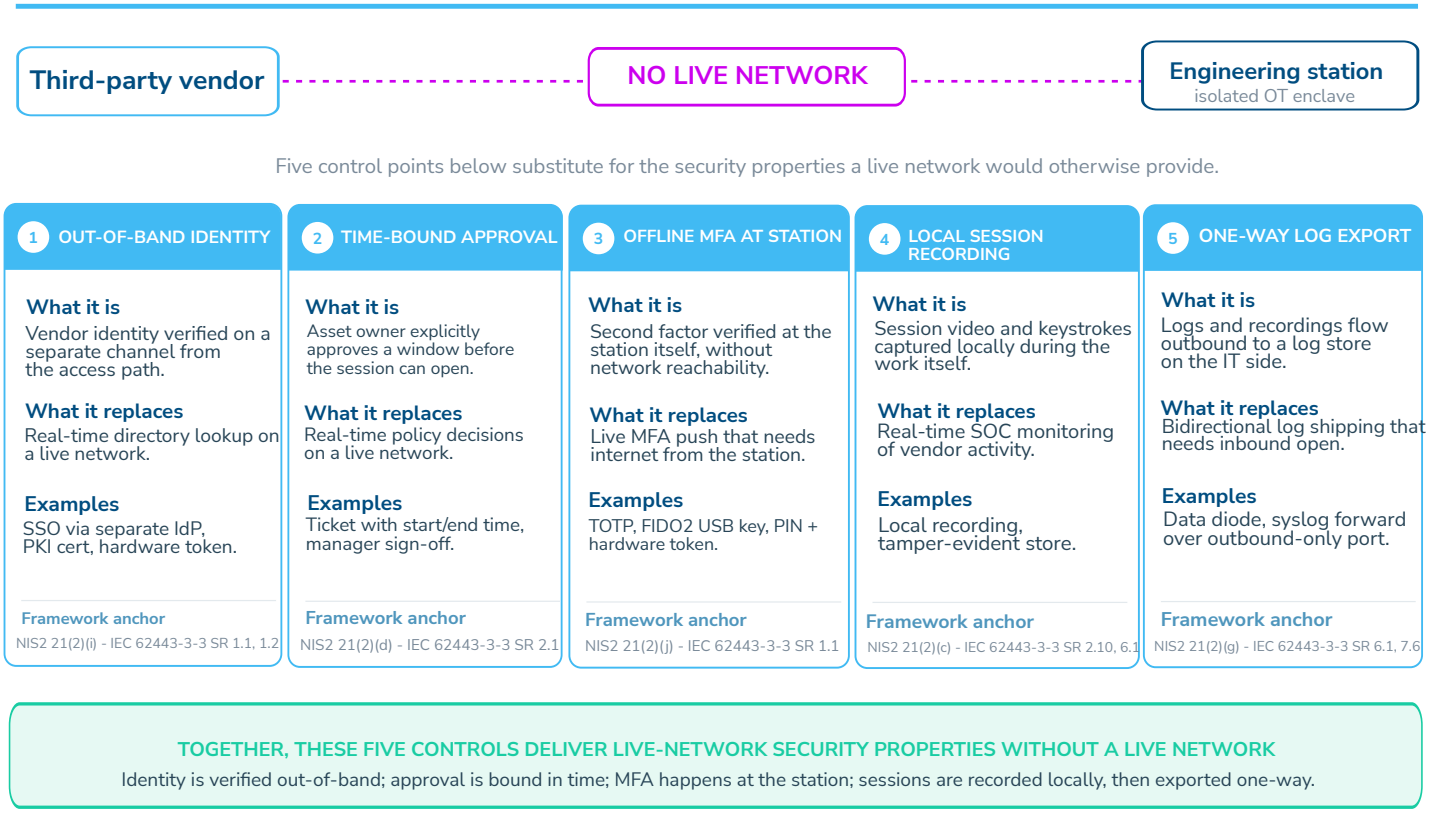


Figure 5. Quadrant C unpacked. Five control points bridge the vendor-to-station gap without a live network path: out-of-band identity verification; time-bound approval from the site owner; offline MFA at the station; local session recording; one-way log export when the site is next visited. Anchors: NIS2 Article 21(2)(d) and (j); Lov om styrket beredskab i energisektoren §§ 6, 7, 8; IEC 62443-3-3 SR 1.1 and FR 6; NIST SP 800-82 Rev. 3 (AC and IA control families).

Each of the five controls maps to verified clauses. Out-of-band identity verification (a separate channel before the vendor reaches the site) supports IEC 62443-3-3 SR 1.1 (human user identification and authentication). Time-bound approval from the site owner supports NIST SP 800-207 Tenet 6. Offline MFA at the station, via TOTP, hardware token, or PIV card, supports NIS2 Article 21(2)(j) without requiring internet. Local session recording provides evidence for IEC 62443-3-3 FR 6 and Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 6. One-way log export, through a unidirectional gateway or signed media at the next site visit, preserves the air gap while delivering the evidence the regulator requires.

Failure mode to watch for: the assumption that 'no internet' equals 'no compliance'. Most small sites operate this way today not because the controls are technically infeasible but because the operating discipline (authorised collection visits, signed media chain of custody, station-local credential lifecycle) has not been established. The fix is process design, not infrastructure investment.

PATTERN D: SMALL OT, VENDOR-OWNED LAPTOP (SCENARIO 3)

The third-party vendor brings their own laptop to a small site with no on-site IT infrastructure. Typical setting: a remote business unit visited rarely by an automation contractor whose engineering tools live on the contractor's machine. This is the residual hardest case. The device is untrusted, the site has no enterprise infrastructure to wrap it, and the controls cannot sit at a station the customer manages because the work is happening on the vendor's hardware.

Defensible controls in this pattern must sit at the boundary between the vendor's device and the operational equipment. The architectural ingredients are scoped session brokers (so the vendor never gets a flat tunnel into Level 1), session evidence captured outside the vendor's machine (so the recording is not under vendor control), and structured log export off-site (so the evidence reaches the asset owner).

The legal anchor is the same as Pattern B: NIS2 Article 21(2)(d) supply-chain security, and §6 stk. 2 nr. 7 of Lov om styrket beredskab i energisektoren on supply-chain security between the entity and its direct suppliers, with the operational specifics in BEK 260 §§29-32 (supplier procedures and remote-access procedures for direct suppliers).

MINIMUM VIABLE CONTROLS FOR PATTERN D

Pattern D is the most common scenario for small sites served by external contractors (small water utilities, regional wind or solar sites, local SCADA integrators). A minimum viable set of controls, formulated in vendor-neutral terms, is achievable even at sites with no on-site enterprise infrastructure. Each control below maps to a primary-verified clause where possible; where the control rests on IEC 62443-2-4:2024 (paywalled) it is flagged as GUIDE INTERPRETATION.

- **Mandatory per-session MFA across the chain.** MFA at the point the vendor authenticates, plus MFA at the point of entry to the site broker. NIS2 Article 21(2)(j); Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 10 (REQUIREMENT).

- **Session brokering via a hardware appliance at the site.** No direct VPN from the vendor's own laptop to the operational network. The vendor authenticates to a broker physically present at the site; the broker mediates into Level 2 / Level 1 equipment. IEC 62443-3-3 SR 1.13; NIST SP 800-82 Rev. 3 Remote Access overlay (REQUIREMENT).

- **Forced session recording regardless of licence location.** The session is recorded outside the vendor's machine, regardless of where the engineering software licence lives. Recording under vendor control is not evidence for the asset owner. IEC 62443-3-3 FR 6; §8 stk. 2 nr. 6 (GUIDE INTERPRETATION of 'forensic capability').

- **Time-bound access measured in hours, not days.** Access is authorised for the length of the expected work, not for the length of the contract. NIST SP 800-207 Tenet 3; IEC 62443-3-3 SR 2.1, SR 2.6 (REQUIREMENT).

- **Session-log export to the asset owner's SIEM or SOC.** Logs leave the site through a unidirectional path and land in the asset owner's monitoring stack. §8 stk. 2 nr. 6 requires logs to support alarms, investigation, and incident handling; a log that never leaves the site does not satisfy that purpose (GUIDE INTERPRETATION).

Program-level controls from IEC 62443-2-4:2024. The standard, current edition DS/EN IEC 62443-2-4:2024 (which supersedes IEC 62443-2-4:2015 with Amendment 1:2017), defines security programme requirements for industrial automation and control system service providers. Primary PDF access to the underlying IEC text is paywalled, so specific clause wording is not reproduced here. Based on three independent secondary summaries of the standard, the following categories of programme controls are referenced: vendor security programme governance; patch level and anti-

malware posture of service-provider laptops; anti-tampering and change control of vendor tooling; contractual evidence obligations including log delivery and retention; personnel security and background checks for vendor technicians. Because the underlying IEC text is paywalled, these controls appear here as GUIDE INTERPRETATION drawn from three independent secondary summaries, not as verbatim clause quotations.

Pattern D (vendor-laptop programmes) is treated here at principle level and, in product-anchored terms, in Part 2; its deepest clause-level anchor is IEC 62443-2-4:2024, which addresses security programme requirements for industrial automation and control system service providers. A companion document, BifrostConnect Implementation Guide (Del 2), addresses Pattern D in product-anchored terms. Readers seeking a fully clause-referenced Pattern D treatment should read IEC 62443-2-4:2024 alongside NCSC UK Principles 1 (balance the risk and opportunities) and 6 (limit the impact of compromise).

DEGRADED MODE OPERATIONS: WHEN THE BROKER IS UNAVAILABLE

Patterns C and D depend on a broker mediating between the vendor and the OT zone. WAN outages, central-broker failures, and configuration changes inevitably mean the broker will be unavailable at moments when work is required, including emergencies. An access architecture that fails closed in every degraded scenario is also an architecture that prevents emergency response. The discipline is to define explicitly what degrades gracefully and what never bypasses, and to write that boundary into the operational runbook before the first outage. For sites that must keep operating during WAN or broker loss (island-mode operation), define a pre-authorised local break-glass path that is itself identity-bound, time-limited, and logged, so continuity never becomes an ungoverned backdoor.

Controls that may degrade gracefully in a documented degraded mode: MFA may temporarily fall back to single-factor where the second factor depends on the unavailable service, provided that the resulting session is logged and tagged as degraded; access decisions may temporarily fall back to a cached policy with a defined maximum cache age (typically 24 to 72 hours); session recording targets may temporarily fall back to local storage if the central evidence vault is unreachable, provided the recordings are exported on broker recovery. Each of these is a documented break-glass step, not a permanent state.

Controls that shall never bypass, regardless of degradation.

- **Audit trail.** The fact that a degraded-mode session occurred, who initiated it, and what they did must be captured even when the central monitoring stack is unreachable; storage is local until exfil is restored.

- **Identity.** A degraded-mode session shall still be tied to a named individual by some local mechanism (badge, station-resident TOTP, supervisor co-presence).

- **Approval.** A break-glass session shall require explicit authorisation by a designated role; absence of the broker is not absence of approval.

- **Time-bounding.** Degraded sessions shall expire automatically; degraded mode must not be a stable operating state.

- **Anchors.** NIST SP 800-82 Rev. 3 §6.2.10 (remote access OT overlay) recommends mechanisms to manage the removal of access on a configurable schedule and to support emergency disconnect; NIST SP 800-53 Rev. 5 AC-17(9), per the NIST SP 800-82 Rev. 3 OT overlay, defines a documented disconnect-or-disable capability that extends OT baselines. Both anchors imply that degraded modes must be designed in, not improvised under pressure.

COMPENSATING CONTROLS FOR LEGACY EQUIPMENT

OT estates contain equipment that pre-dates modern remote-access architecture. Serial links (RS-232, RS-485), Modbus RTU, proprietary fieldbus protocols, engineering workstations on Windows XP or Windows 7 (and servers on Windows Server 2003 or 2008), and vendor support tools that presume a flat network are common in installations with 15- to 25-year operating horizons. The principles in this guide apply, but the specific implementation patterns described in Figures 2 through 6 require supplementary controls when the underlying equipment cannot natively support session brokering, MFA, or modern transport security.

SERIAL CONNECTIONS VIA PROTOCOL CONVERTERS

A serial-only PLC cannot be reached by a session broker that speaks IP. The compensating pattern is a protocol converter at the boundary that terminates an authenticated, time-bounded IP session on one side and presents an isolated serial link to the legacy device on the other.

The session broker's authentication, time-bounding, recording, and log-export properties apply on the IP side; the serial side becomes a controlled extension of the brokered session. Anchors: IEC 62443-3-3 SR 5.1 (network segmentation) supports this approach by requiring zone boundaries with controlled communication; NIST SP 800-82 Rev. 3 §6.2.1 (Network Architecture) describes protocol converters and unidirectional gateways as legitimate boundary devices for legacy zones.

The converter is itself a networked device: an ethernet-to-serial gateway (for example a Moxa NPort) has its own firmware, credentials, and management interface, so it becomes part of the attack surface and must be hardened, segmented, patched, and monitored like any other boundary device.

AIR-GAPPED SYSTEMS AND CONTROLLED MEDIA TRANSFER

Some installations are deliberately air-gapped, with no network path in or out. Engineering changes are delivered on physical media (USB, CD, signed update packs). The principles still apply, but the brokering happens in the human and procedural layer rather than the network layer.

Compensating controls: chain-of-custody for every piece of media that crosses the air gap, including who created it, who carried it, and what was on it; a media-staging workstation in a controlled IT area

where incoming files are scanned for malware (multi-engine where the data permits) and where outgoing files are reviewed before they leave the OT zone; a tamper-evident transfer log that is itself archived in the asset owner's evidence stack. The session is the physical visit; the recording is the chain-of-custody.
Anchors: NIST SP 800-82 Rev. 3 §5.2.3.1 (Network Segmentation) supports physical separation as the strongest form of zone boundary; NCSC UK Principle 5 (Harden your OT boundary) applies whether the boundary is a firewall or a doorway.

PROPRIETARY SYSTEMS THAT CANNOT HOST A SESSION AGENT

Some legacy automation platforms cannot run additional software, cannot accept external authentication, and cannot be patched. These devices remain in service because their replacement is a multi-year capital project. The compensating pattern is to wrap, not modify. The legacy device sits inside a small, dedicated VLAN behind a deny-by-default firewall; the only path in or out is through a session broker that treats the device as a destination, not a participant; the broker imposes the identity, time-bounding, recording, and log-export properties externally.

The legacy device contributes nothing to its own security; the boundary contributes everything.
Anchors: IEC 62443-3-3 SR 5.1 (network segmentation) and SR 7.1 (denial of service protection); NIST SP 800-82 Rev. 3 §6.2.1 (Network Architecture) explicitly endorses isolation of legacy equipment behind hardened boundaries with compensating monitoring.

MINIMUM ACCEPTABLE CONTROLS WHEN BEST PRACTICE CANNOT BE MET

For each legacy scenario, the question is not whether the ideal is achievable but what minimum the asset owner can defend. The minima below apply to legacy paths that cannot yet meet the full pattern: a documented inventory of every legacy asset and every remote path into it; identity of every individual who has ever connected, captured manually if not automatically; time-bounded engagement (a maintenance ticket with a start and an end); a session record of some form (video of the engineer at the local console where remote brokering is impossible); and a written migration plan with a target date for moving the legacy asset under a modern boundary. The migration plan is the difference between a legacy compensating control and a permanent exception.

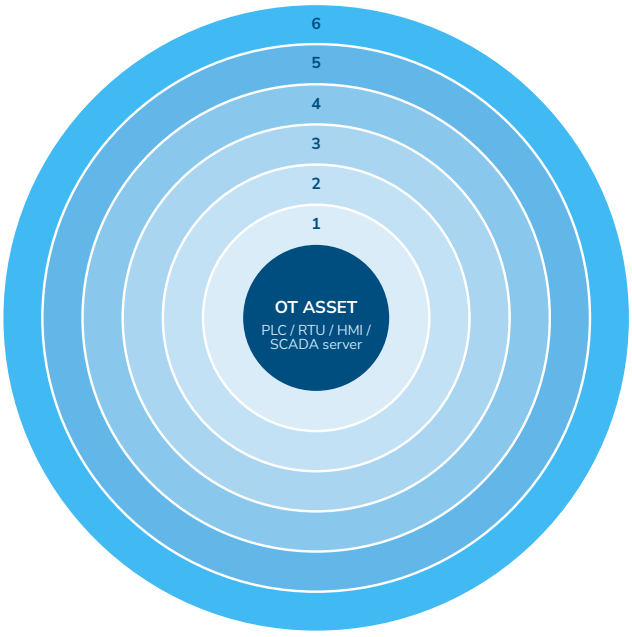
DEFENCE IN DEPTH

Across all four patterns, the same structural answer recurs: no single control is load-bearing. A defensible third-party access pattern is a stack of independent layers, each catching what the previous missed. If one layer fails, the asset is still protected by the next. This is the structural answer to the supply-chain risk that NIS2 Article 21(2)(d) addresses, and it is the reason Patterns A through D differ in implementation but not in shape.

The six layers, from outermost to innermost: Identity and Access (who is requesting); Approval and Ticketing (why and when); Network Path Control (where the session may go); Session Mediation (how the session is rendered into the zone); Session Recording and Monitoring (the witness); Log Integrity and Export (the evidence). Each layer carries its own framework anchor; together they cover the FR 1 through FR 7 spectrum of IEC 62443-3-3.

FIGURE 6. Defence in depth

Six concentric control layers wrap a single OT asset, jointly spanning IEC 62443-3-3's seven Foundational Requirements.



6 Governance & audit
Process documentation, evidence retention, periodic review.
NIS2 21(2)(f)+(g) - IEC 62443-3-3 FR 6, FR 7

5 Network controls
No inbound. Outbound-initiated only. One-way log export.
NIS2 21(2)(i)+(d) - IEC 62443-3-3 FR 5

4 Session controls
Time-bound, scoped sessions. Recording. Keystroke logs.
NIS2 21(2)(j) - IEC 62443-3-3 FR 3, FR 4

3 Authorisation
Asset owner approves per session. Least-privilege scope.
NIS2 21(2)(i)+(d) - IEC 62443-3-3 FR 2

2 Identity & authentication
Out-of-band identity verification. MFA at the station.
NIS2 21(2)(i) - IEC 62443-3-3 FR 1

1 Physical & local
Tamper-evident hardware. Local authorisation. Cabinet keys.
NIS2 21(2)(i) - IEC 62443-3-3 FR 1, FR 3

IEC 62443-3-3 FRs covered: FR 1 to FR 7, all seven, distributed across the six layers. The loss of any one layer does not collapse the others.

Figure 6. Six concentric control layers wrap a single OT asset. Each layer carries its own framework anchor; together they span the seven Foundational Requirements of IEC 62443-3-3.

INCIDENT HANDLING ACROSS THE LAYERS

NIS2 Article 21(2)(b) requires entities to implement incident handling as a named technical and organisational measure. The layers above are structured for prevention; a defensible pattern also needs structured detection and response when prevention fails. Incident handling threads through three of the six layers.

At the Session Recording and Monitoring layer, the recording is not passive; it is piped into an automated rule set that alarms on specific anomalies: attempts to stop or restart a PLC, unauthorised code upload, command sequences that do not match the ticketed work, and authentication events outside the approved window. Anchors: IEC 62443-3-3 SR 6.1 (audit log accessibility) and SR 6.2 (continuous monitoring); audit log generation is anchored in SR 2.8 (auditable events) and SR 2.9 (audit storage capacity); Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 6 (parent law) and BEK 260 §66 stk. 2 nr. 2 (logging on remote-access equipment).

At the Log Integrity and Export layer, the pipeline feeds an OT intrusion detection system or a security operations centre that can see events in near-real-time, not only after the fact. Passive logs without alarming do not satisfy §8 stk. 2 nr. 6, because §8 stk. 2 nr. 6 requires the log to support alarms and incident handling, not only forensic reconstruction. The same obligation is reinforced by NIST SP 800-53 Rev. 5 control AU-6 (Audit Record Review, Analysis, and Reporting), which requires review with frequency matched to the risk of the system.

At the Approval and Ticketing layer, incident handling closes the loop: a detected anomaly revokes the active session, notifies the site owner, and opens an incident record with the same identifiers as the session recording. This makes the incident handling response traceable to a specific session, a specific vendor identity, and a specific set of actions, which is the evidence pattern NIS2 Article 23 (significant incident reporting) requires.

Personal data note. *Session recordings typically contain personal data within the meaning of the EU General Data Protection Regulation (GDPR). Retention periods, access control, data subject rights, and processing grounds must be addressed in the recording policy, independently of the technical control. GDPR obligations apply to the recording whether or not the underlying OT system is subject to NIS2.*

COMPLIANCE CROSSWALK

The same set of controls earns credit under multiple frameworks. The crosswalk in Figure 7 maps six control areas introduced in this guide against five frameworks: NIS2 Article 21, Lov om styrket beredskab i energisektoren and BEK 260, IEC 62443-3-3, NIST SP 800-82 Rev. 3, and NIST SP 800-207. Each non-empty cell carries the specific clause reference, not just a checkmark.

Empty cells are deliberate. They mean the framework does not address the principle at a clause level that this guide is willing to cite verbatim. Where a framework offers a closely matching control without an exact verbatim clause, the cell cites the most specific available clause and the descriptor remains conservative. Supply-chain hygiene for the IEC 62443 family is anchored to IEC 62443-2-4:2024 (service-provider programme requirements) rather than to 62443-3-3, because the service-provider programme is the system-of-systems requirement most directly applicable to third-party access governance.

Control area	NIS2 Art. 21	Lov om styrket beredskab i energisektoren / BEK 260	IEC 62443-3-3:2019	NIST SP 800-82	NIST SP 800-207
1. Zero Standing Privilege (Privilege expires)	**Art. 21(2)(i)** access control policies	**§ 52 stk. 1 nr. 1 + § 55 stk. 2** adgangskontrol; ophører ved opgavens afslutning	**SR 2.1 + RE 2** authorization enforcement; permission mapping to roles	**§ 6.2.10** remote access OT overlay: removing access when no longer required	**Tenet 3** per-session access
2. Ad-hoc access beats standing (No always-on paths)	**Art. 21(2)(e)** network and information system security	**§ 62** segmentering og logisk adskillelse	**SR 5.1** network segmentation	**§ 6.2.1.3** network architecture; deny-all default	**Tenet 2** all comms secured regardless of location
3. Layered controls (Defense in depth)	**Art. 21(2)(b)** incident handling	**§ 55 stk. 3** mulighed for at afbryde og terminere adgang	**SR 5.1** network segmentation (zone boundary)	**AC-17(9)** remote access; disconnect/disable	**Tenet 6** dynamic, strictly enforced authentication
4. Session evidence (Recorded, reviewed)	**Art. 21(2)(b)+(f)** incident handling; effectiveness	**§ 66 stk. 2 nr. 2** logning og opbevaring af adgangshændelser	**SR 6.1** audit log accessibility	**§ 5.2.3.2** centralized logging	**Tenet 7** monitor posture; collect info; improve

Control area	NIS2 Art. 21	Lov om styrket beredskab i energisektoren / BEK 260	IEC 62443-3-3:2019	NIST SP 800-82	NIST SP 800-207
5. Supply-chain hygiene (Vendors are assets too)	**Art. 21(2)(d) + para 3** supply-chain security	**§ 29 + § 30 + § 31** leverandørstyring ; krav til tredjepart	**IEC 62443-2-4 SP.07** service provider security program	**§ 6.2.10** third-party access	**n/a** outside ZTA scope
6. Offline-capable design (Works when internet doesn't)	**Art. 21(2)(j)** MFA / continuous authentication	**§ 53** flerfaktor-autentificering	**SR 1.1 + RE 2** identification and authentication; unique IDs	**§ 6.2.10** identification and authentication	**Tenet 6** authZ enforced before access

Figure 7. Compliance crosswalk. Six control areas by five frameworks, with the specific clause reference in each non-empty cell. Empty cells are deliberate and explicitly marked. Product-specific coverage mapping lives in the companion BifrostConnect Implementation Guide (Del 2).

IMPLEMENTATION PRIORITY

A reader finishing the crosswalk typically asks a practical question: what do I do on Monday morning? This guide's answer is a vendor-neutral maturity staging. The ordering is deliberately technology-agnostic; it reflects the natural sequence in which controls stabilise on top of each other. A competitor to the publisher of this guide could adopt the same sequence without change.

PHASE 1 - STOP THE BLEEDING (0-30 DAYS)

Inventory every third-party access path currently in use: named vendor, purpose, entry point, protocol, and whether MFA is enforced. Remove or disable any standing VPN account for which no current, approved work exists. Disable inbound listening ports that are not accounted for in the inventory. This phase is discovery and containment; it does not require new procurement.

PHASE 2 - ESTABLISH THE PATTERN (30-90 DAYS)

Introduce a session broker, MFA on every session, and per-session approval. Replace shared vendor credentials with named identities bound to the broker. Enforce a time-out policy measured in hours. At this phase, the access path may still be imperfect; the goal is to make every session a discrete, identifiable, revocable event. These windows assume an organisation with existing identity and logging foundations; a site starting from zero should treat the same steps as a longer programme and sequence them over a realistic horizon.

PHASE 3 - EVIDENCE AND MONITORING (90-180 DAYS)

Turn on session recording and route logs to the asset owner's SIEM or SOC. Tune alarming on specific OT anomalies (PLC stop attempts, unauthorised code upload, command sequences outside ticketed work). Institutionalise incident response for detected anomalies: session revocation, site-owner notification, incident record. A 90-to-180-day window is realistic only where log collection already exists; building SIEM or SOC visibility from nothing is itself a multi-quarter effort and should be planned as one.

PHASE 4 - PROGRAM MATURITY (180+ DAYS)

Move from per-session controls to programme-level controls. Vendor onboarding checklists, contract clauses for security posture, background checks where the regulatory regime allows it, vendor-specific threat modelling, and joint incident response playbooks with named vendors. This phase is the substance of IEC 62443-2-4:2024 and NIS2 Article 21(2)(d) read together.

RESIDUAL RISKS: UNSOLVABLE BY TECHNOLOGY ALONE

The pattern in this guide is complete at the architectural level. It is not complete at the programme level. A set of residual risks sits outside what technology can address on its own; they require procedural, contractual, or organisational controls and should be named explicitly so they are not silently assumed away.

- **Insider threat from vendor personnel.** A technician with legitimate, approved access still has that access during the approved window, and the case includes a disgruntled or departing insider acting deliberately. Controls: background checks where allowed by national law, role separation within the vendor organisation, two-person rules for high-risk work, and contract clauses that require the vendor to report personnel changes.

- **Geopolitical supply-chain risk.** The vendor's own national jurisdiction, ownership structure, and exposure to state pressure are not addressable through session controls. Controls: vendor due diligence, national origin of key components, alternative-supplier continuity planning. NIS2 Article 21(3) requires entities to take into account vulnerabilities specific to each direct supplier and service provider, and the overall quality of their products and practices.

- **Social engineering against asset-owner personnel.** A well-designed session architecture can still be defeated by a phone call that causes a site operator to approve a session that should not have been approved. Controls: security awareness training, separation of approval authority from the requester's chain of contact, out-of-band verification for unexpected requests.

- **Contractual enforceability at the moment of breach.** A service-level agreement without enforceable remedy is not a control. Controls: clause drafting that creates specific obligations with measurable breach conditions, liability caps calibrated to the actual potential harm, and jurisdiction clauses that allow enforcement in the asset owner's home forum.

The message is not that technology fails; the message is that a technical pattern plus a programme is the whole answer, and presenting the technical pattern alone would misstate the completeness of the defence.

DEFINITIONS AND KEY TERMS

The terms below are used throughout this guide. All definitions are vendor-neutral and drawn from the cited standards.

- **Zero Standing Privilege (ZSP):** An operating model where no access exists by default. Every session is requested, approved, opened for a bounded window, and revoked on close. Anchored in NIST SP 800-207 Tenets 3 and 6 and IEC 62443-3-3 SR 2.6 (remote session termination).

- **Out-of-Band (OOB) access:** An access path that is logically or physically independent of the operational network, so it remains usable when the operational network is degraded, isolated, or compromised.

- **Air gap:** A network posture in which an OT environment has no physical network connection to external networks and no automated logical connection. Strict definition per NIST Computer Security Resource Center glossary. Used in this guide only for genuinely isolated sites, where no physical or logical connection exists. Isolation is defined by the absence of connectivity, not by site size; air-gapped sites are most often small Pattern D installations, but it is the absence of any connection, not the scale, that makes a site air-gapped. Outbound-only brokered architectures are not air gaps and are named separately below.

- **Egress-only session pattern:** An access architecture in which every session is initiated outbound from the OT zone to an external broker. No listening port exists on the OT side; inbound access is structurally impossible. Distinct from an air gap because a logical path exists when the zone itself opens it. This is the dominant posture for Patterns A through C in this guide and is the practical phrasing of the OT Island Principle.

- **Multi-Factor Authentication (MFA):** Authentication that combines at least two independent factors. Required per session by NIS2 Article 21(2)(j) and Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 10.[7]

- **Time-based One-Time Password (TOTP):** A short-lived numeric code derived from a shared secret and the current time (RFC 6238, the TOTP: Time-Based One-Time Password Algorithm). Suitable as a second factor in environments without persistent internet connectivity.

[7] Regulation (EU) 2022/2555 (NIS2 Directive), Article 21(2)(j). Retrieved from EUR-Lex CELEX 32022L2555, 2026-04-22.

- **Identity broker:** A control plane component that authenticates the human, evaluates approval policy, and issues a session-scoped credential. The identity broker holds no operational privilege itself.

- **Session broker:** A control plane component that mediates the authenticated session into the OT zone, records the session, and terminates it on inactivity or timer expiry.

- **Network Access Control (NAC):** A control that gates which devices may attach to a network based on identity, posture, and policy. Relevant where vendor-owned hardware enters a managed OT zone.

- **Vendor demilitarized zone (vendor-DMZ):** A segregated network segment that hosts vendor-originated sessions before they are mediated into the operational zone. Limits blast radius if vendor equipment is compromised.

- **OT intrusion detection system (OT-IDS):** Passive network monitoring tuned to industrial protocols. Provides session evidence and anomaly detection inside the OT zone. Where a dedicated OT-IDS is not deployed, equivalent visibility can come from SIEM correlation of session and network logs.

- **Unidirectional gateway / data diode:** A hardware or hardware-enforced software component that permits data flow in one direction only. Standard pattern for log export from OT zones without creating an inbound path.

- **NIS2:** Directive (EU) 2022/2555. Imposes risk-management and incident-reporting obligations on essential and important entities, including OT operators in energy, water, transport, and other critical sectors.

- **Lov om styrket beredskab i energisektoren:** Danish parent law for energy-sector preparedness. §§ 6, 7, and 8 cover organisational, physical, and cybersecurity requirements. BEK 260 is the executive order issued under this law.[8]

[8] Bekendtgørelse nr. 260 af 6. marts 2025 om net- og informationssikkerhed for energisektoren. Retrieved from retsinformation.dk, 2026-04-22.

- **IEC 62443-3-3:2019:** International standard (DS/EN harmonization 2019) defining seven Foundational Requirements (FR 1-7) and associated System Requirements (SR) for industrial automation and control systems.

- **IEC 62443-2-1:2024:** International standard (DS/EN IEC 62443-2-1:2024) defining cybersecurity programme requirements for IACS asset owners. The companion to 3-3 on the asset owner side.

- **IEC 62443-2-4:2024:** International standard (DS/EN IEC 62443-2-4:2024) defining security programme requirements for IACS service providers. Annex A specifies twelve SP categories including SP.07 Remote access.

- **NIST SP 800-82 Rev. 3:** Guide to Operational Technology (OT) Security, published September 2023. Functions as an OT overlay on NIST SP 800-53 Rev. 5 and is the authoritative vendor-neutral reference for OT-specific control selection.

- **NIST SP 800-207:** Zero Trust Architecture, published August 2020. Defines the seven Zero Trust Tenets used as the conceptual foundation for per-session, per-resource access decisions.

- **Joint NCSC Secure Connectivity Principles for OT:** Eight principles, published 18 March 2024, by the United Kingdom National Cyber Security Centre in joint partnership with the Australian Signals Directorate's Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the United States Cybersecurity and Infrastructure Security Agency, the United States Federal Bureau of Investigation, Germany's Federal Office for Information Security, the Netherlands' National Cyber Security Centre, and New Zealand's National Cyber Security Centre. Principle 5 ("Harden your OT boundary") is the most directly relevant for the third-party access framework, with its hardening checklist explicitly including the requirement to enforce security requirements on third parties.

- **Joint CISA Zero Trust for OT:** Adapting Zero Trust Principles to Operational Technology, published 29 April 2026 by the United States Cybersecurity and Infrastructure Security Agency (CISA), Department of War, Department of Energy, Federal Bureau of Investigation, and Department of State, with contributions from the National Institute of Standards and Technology. Aligns with NIST CSF 2.0 functions and provides the most recent authoritative application of Zero Trust principles to OT environments.[9]

[9] CISA, DoW, DOE, FBI, DOS with NIST contributions, "Adapting Zero Trust Principles to Operational Technology", 29 April 2026. Retrieved 2026-05-04.

- **Danish energy-sector regime:** For Danish energy entities, Lov om styrket beredskab i energisektoren and BEK 260 govern preparedness, including cybersecurity of remote access, to the extent the entity is covered by that regime. The Danish NIS2 implementation (LOV nr. 434 af 6. maj 2025) does not apply to the extent the entity is already covered by Lov om styrket beredskab i energisektoren. Energy entities should consult both regimes for the applicable obligations.

SOURCES AND REFERENCES

Each citation below names the primary source and retrieval date.

- **EU NIS2 Directive (2022/2555).** Article 21, paragraph 2, points (a) through (j). Primary source: EUR-Lex CELEX 32022L2555. Relevant for third-party access: (d) supply chain, (i) access control policies, (j) multi-factor authentication.

- **LOV nr. 434 af 6. maj 2025.** Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau - Danish implementation of NIS2. § 6, stk. 1, nr. 1 to 10 transpose NIS2 Article 21(2)(a) to (j). Primary source: Retsinformation (Lovtidende, 2025).

- **Lov om styrket beredskab i energisektoren.** §§ 6, 7, 8. Parent law for BEK 260. Relevant clauses: §6 stk. 2 nr. 3 access control policies; §6 stk. 2 nr. 7 supply chain; §8 stk. 2 nr. 2 network architecture; §8 stk. 2 nr. 6 logging; §8 stk. 2 nr. 10 MFA and access protection. Danish energy entities are governed by this regime to the extent of its coverage; LOV nr. 434 af 6. maj 2025 does not apply for those obligations that are already covered by the energy-sector regime.

- **BEK 260 af 6. marts 2025.** Executive order on cybersecurity preparedness in the energy sector, issued under Lov om styrket beredskab i energisektoren. Relevant paragraphs: §§29-32 supply-chain security and remote-access procedures (incl. supplier agreement requirements); §§51-53 access control policy, access control, and multi-factor authentication; §55 stk. 2 zero standing privilege evidence (time-limited remote access only during approved work-related need); §62 network segmentation; §§64-66 logging and monitoring (with §66 stk. 2 nr. 2 explicitly covering remote-access equipment).

- **IEC 62443-3-3:2019.** International standard for industrial automation and control systems security. Foundational Requirements FR 1 to FR 7. System Requirements relevant to third-party access: SR 1.1 human user identification and authentication; SR 1.13 access via untrusted networks; SR 2.1 authorisation enforcement; SR 2.6 remote session termination; SR 2.8 auditable events; SR 6.1 audit log accessibility; SR 6.2 continuous monitoring.

- **IEC 62443-2-4:2024.** Security programme requirements for industrial automation and control system service providers. Current edition (DS/EN IEC 62443-2-4:2024), supersedes IEC 62443-2-4:2015 with Amendment 1:2017. Paywalled; this guide references the standard for Pattern D and for supply-chain hygiene controls based on three independent secondary summaries. Primary PDF acquisition recommended for any legally binding use.

- **NIST SP 800-82 Rev. 3.** Guide to Operational Technology (OT) Security. Published 28 September 2023. Functions as an OT overlay on NIST SP 800-53 Rev. 5. Relevant control families: Access Control (AC) and

Identification and Authentication (IA). Includes a dedicated section on Network Segmentation and Isolation and OT-specific remote access overlay for AC-17.

- **NIST SP 800-53 Rev. 5.** Security and Privacy Controls for Information Systems and Organizations. Relevant audit family controls: AU-2 event logging; AU-3 content of audit records; AU-6 audit record review, analysis, and reporting; AU-12 audit record generation; AU-14 session audit.
- **NIST SP 800-207.** Zero Trust Architecture. Published August 2020. Section 2.1 defines seven Zero Trust Tenets used as the conceptual foundation for per-session, dynamic-policy access decisions in this guide.

- **Joint NCSC Secure Connectivity Principles for Operational Technology.** Published 18 March 2024, by the United Kingdom National Cyber Security Centre in joint partnership with the Australian Signals Directorate's Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the United States Cybersecurity and Infrastructure Security Agency, the United States Federal Bureau of Investigation, Germany's Federal Office for Information Security, the Netherlands' National Cyber Security Centre, and New Zealand's National Cyber Security Centre. Eight principles for OT connectivity; Principle 5 ("Harden your OT boundary") is the most directly relevant for the third-party access framework, with its hardening checklist explicitly including the requirement to enforce security requirements on third parties.

- **CISA Adapting Zero Trust Principles to Operational Technology.** Joint guide published 29 April 2026 by the United States Cybersecurity and Infrastructure Security Agency, Department of War, Department of Energy, Federal Bureau of Investigation, and Department of State, with contributions from the National Institute of Standards and Technology. Aligned with NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover). The most recent authoritative application of Zero Trust to OT, used in this guide alongside NIST SP 800-207 as the dual anchor for the Zero Standing Privilege principle (Figure 3).

- **ISA-95 / IEC 62264.** Reference architecture for enterprise-control system integration. Adopts the Purdue Model layers used in Figure 1.

- **CISA Advisory AA24-038A.** PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (Volt Typhoon). Joint advisory by CISA, NSA, FBI and international partners, 7 February 2024. Reference for the threat context section.

- **CISA Advisory AA23-335A.** IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities (CyberAv3ngers). Published 1 December 2023. Reference for the threat context section.

- **Mandiant APT44 profile and CERT-UA Industroyer2 advisory.** Mandiant report on APT44 / Sandworm (2024); CERT-UA advisory on the April 2022 attack against Ukrainian electricity substations using Industroyer2 and CaddyWiper. Reference for the threat context section.

- **SektorCERT rapport (November 2023).** De koordinerede angreb mod dansk, kritisk infrastruktur. Danish sector CERT documentation of the May 2023 coordinated attack against 22 Danish energy companies. Reference for the threat context section.

- **Dragos TRITON / TRISIS analysis.** Technical analysis of the 2017 attack on a Saudi Arabian petrochemical safety instrumented system, first reported by FireEye and Dragos. Reference incident for attacks reaching the safety-integrity layer.

- **EU GDPR (2016/679).** General Data Protection Regulation. Relevant for session recordings that contain personal data of vendor technicians or site operators. Retention, access control, and data subject rights must be addressed in the recording policy.

OPERATIONAL LIFECYCLE

Third-party access requirements vary across the operational lifecycle of an OT asset. Commissioning concentrates vendor presence and tolerates higher-bandwidth, less-bounded access; the controls in Pattern B and the discipline of documented entry and exit are essential. Day-to-day operations occur with no third-party access most of the time; the controls in Patterns A and C are dormant until the next vendor visit. Ad-hoc maintenance is the most common pattern in practice and the focus of this guide; the minimum-viable controls in Patterns C and D apply.

Incident response demands break-glass access that the degraded-mode rules above already cover. Decommissioning requires the explicit removal of access paths, credentials, and keys; this is the step most often skipped, and the source of forgotten tunnels and standing privilege that this guide describes as the antipattern. The five lifecycle phases share the five core principles; the depth of implementation varies.

PRACTICAL APPLICATION ACROSS THE LIFECYCLE

Third-party access requirements remain constant across the lifecycle, but the operational context changes how they are applied.

- During **commissioning**, access windows are longer, vendor-driven, and often involve vendor-owned equipment (Pattern B/D). Strict network containment and device validation are critical.
- During **day-to-day maintenance**, access is predictable and should be pre-approved, time-bound, and tied to named individuals with repeatable workflows.
- During **ad-hoc support**, access is reactive and must remain fully brokered, explicitly approved per session, and tightly time-scoped.
- During **incident response and recovery**, speed is critical, but controls must not be bypassed. Pre-approved emergency access procedures, including break-glass accounts with full session logging, should be defined in advance.
- During **decommissioning**, all third-party access paths, credentials, and dependencies must be removed, verified, and documented as part of system closure.

APPENDIX: SAMPLE PROCUREMENT REQUIREMENTS FOR OT REMOTE ACCESS

The clauses below are illustrative drafting language for use in tender documents, Master Service Agreements, and statements of work where third-party remote access into operational technology is in scope. The wording is anchored in IEC 62443-2-4:2024 (service provider security programme requirements) and the BEK 260 §§ 30 to 32 family of supplier-agreement obligations. Adopting organisations should adapt the wording to their legal framework and purchasing process; the clauses are not a substitute for qualified legal counsel.

1. The Vendor shall support session brokering in such a manner that no direct network path exists from the Vendor's equipment to Customer's operational technology assets outside of an active, authorised session. (Anchor: IEC 62443-2-4:2024 SP.07 Remote access; BEK 260 §31.)

2. The Vendor shall enforce multi-factor authentication on every session, with at least one factor independent of the Vendor's own infrastructure. (Anchor: IEC 62443-3-3:2019 SR 1.1 RE 1; NIS2 Article 21(2)(j); BEK 260 §53.)

3. The Vendor shall operate under a security programme demonstrably aligned with IEC 62443-2-4:2024 SP.01 to SP.12, with documented evidence of training, background checks, configuration management, and patch management for personnel and tooling engaged on Customer's site. (Anchor: IEC 62443-2-4:2024 Annex A; BEK 260 §29 and §30.)

4. The Solution shall provide cryptographic audit trail of all access events with a minimum retention period of thirteen (13) months, with audit records meeting the content requirements of NIST SP 800-53 Rev. 5 AU-3. *(Anchor: NIST SP 800-53 Rev. 5 AU-2 and AU-3; BEK 260 §66 stk. 2 nr. 2 logging of remote-access events, and §67 stk. 3 retention period (13 months, niveau 4-5).)*

5. The Vendor shall obtain explicit, time-bounded approval from a designated Customer representative prior to each session. Standing or open-ended approvals are not permitted.

(Anchor: IEC 62443-2-4:2024 SP.07.04; NIST SP 800-207 Tenet 3 and Tenet 6; BEK 260 §55 stk. 2.)

6. The Vendor shall support automated session termination at a configurable time limit and shall support unilateral termination by the Customer at any time without operational degradation of OT systems. (Anchor: IEC 62443-3-3:2019 SR 2.6 (remote session termination); NIST SP 800-82 Rev. 3 AC-17(9).)

7. The Vendor shall provide forced session recording of all activity occurring inside the brokered session, with the recording stored under Customer-controlled infrastructure. Vendor-controlled recording is not acceptable as evidence. (Anchor: GUIDE INTERPRETATION of IEC 62443-3-3:2019 FR 6 and NIST SP 800-53 Rev. 5 AU-14 in the OT supplier context; Lov om styrket beredskab i energisektoren §8 stk. 2 nr. 6.)

8. The Vendor shall notify the Customer of any security incident affecting Vendor personnel, tooling, or infrastructure used to deliver the Service within twenty-four (24) hours of detection. (Anchor: NIS2 Article 23; BEK 260 §30 stk. 1 nr. 2.)

9. The Vendor shall, on Customer's written request, support Customer's reporting obligations under NIS2 Article 23 and applicable national law, including timely delivery of session logs, audit records, and forensic artefacts. (Anchor: BEK 260 §30 stk. 1 nr. 3 and §32.)

10. On termination of the engagement, the Vendor shall, within a defined transition period not exceeding thirty (30) days, return or securely destroy all Customer access credentials, keys, configurations, and operational data, and shall provide written attestation of completion. *(Anchor: NIS2 Article 21(2)(i) access control and asset management; NIS2 Article 21(2)(d) supply-chain security; BEK 260 §52 nr. 2 deactivation and removal of accounts, and §30 stk. 1 nr. 8 customer data ownership.)*

These clauses are starting points, not finished contract language. Each should be reviewed against the specific Vendor relationship, the Customer's regulatory environment, and the relevant procurement process. The clauses cite primary sources where available and are labelled GUIDE INTERPRETATION where they extend a primary clause beyond its literal text into the OT supplier context.