INARA WHITE PAPER SERIES / WP-02

OT & ICS Security

A Procurement Guide for Pakistan's Critical Infrastructure Buyers

Audience: CISOs, Plant IT/OT Heads, and Procurement Leaders in Oil & Gas, Power, Water, and Manufacturing organizations operating in Pakistan.

Format: 12 pages · Reading time: ~25 minutes · ISO 27001 · IEC 62443 aligned

Published by Inara Technologies · Islamabad, Pakistan · www.inara.pk
ISO 9001:2015 · ISO 27001 · Authorized partner: Fortinet, Palo Alto, Cisco, Dell, NetBackup, Veeam

TABLE OF Contents

EXECUTIVE
Summary

Pakistan's critical infrastructure operators – refineries, terminals, transmission grids, water utilities, and large-scale process plants – are under structural pressure on three fronts. Plants commissioned in the 1990s and 2000s carry control-system stacks designed for isolated networks, but those networks are no longer isolated: remote support, predictive maintenance, IIoT sensors, and corporate-IT integration have made every refinery a potential target. The global ICS Security market is projected to expand from USD 13.27 billion in 2025 to USD 32.89 billion by 2030 at a 16.5% CAGR (MarketsandMarkets), a growth rate that reflects how rapidly the threat is being industrialized. And in Pakistan, the OT cybersecurity talent pool is narrow – buyers cannot rely on the IT SOC team they already have to run an OT SOC.

This guide gives procurement leaders, plant CISOs, and OT/IT heads the structured framework, due diligence questions, and 18-item RFP scorecard needed to evaluate OT security providers in a market where most vendors are repositioning IT services as 'OT-capable' without operational substance.

Central Argument

An OT security program cannot be built on top of an IT SOC by re-skinning the tooling and the analyst playbooks. Successful programs invest separately in three things: (1) an asset-discovery layer designed for legacy industrial protocols, (2) a control-network segmentation architecture aligned to IEC 62443 zones and conduits, and (3) an OT-SOC operations team with control-engineering literacy, distinct from the IT SOC.

WHY OT SECURITY
Is Different from IT Security

Five Structural Differences That Break IT-Style Tooling

Buyers who treat OT security as 'IT security with industrial protocol decoders' fail in predictable ways. The five differences below are not preferences – they are engineering constraints that determine what tooling, what operating model, and what SLA framework will actually work in a plant environment.

#	Dimension	IT Environment	OT Environment
1	Primary risk objective	Confidentiality, integrity, availability – in that order	Safety and availability first; integrity next; confidentiality last
2	Patch cadence	Monthly or faster; reboots accepted	Annual TAR (turnaround) windows; reboots can shut down production
3	Endpoint footprint	Modern OS, AV/EDR feasible everywhere	Windows XP/7, vendor-locked HMIs, no EDR support on most PLCs
4	Network protocols	IP, TCP, HTTP, TLS – fully decoded by IT tooling	Modbus, DNP3, OPC UA, IEC 61850, Profinet – require OT-aware tooling
5	Recovery objective	Restore from backup in hours	Recover the plant's physical state – days to weeks if unsafe shutdown occurs

These five differences mean an IT SOC analyst who pages a refinery shift engineer at 2 a.m. with an 'isolate the host' recommendation is, in practice, recommending that the refinery be tripped. The OT-SOC analyst recommends something different: a containment posture that holds the threat without disrupting production until the next safe maintenance window. That judgement is the operating-model difference – not a tooling difference.

THE IEC 62443
Reference Model & Purdue Levels

Zones, Conduits, and the Foundational Requirements

IEC 62443 is the international reference standard for industrial control system security. It defines a layered model of zones (logical groupings of assets with similar security requirements) and conduits (the controlled communication paths between zones). Every architecture decision in OT security – segmentation, monitoring coverage, access control – should map back to a zone-and-conduit diagram. If a provider cannot show you their reference architecture expressed in IEC 62443 terms, they are improvising.

Purdue Level	Zone Description	Typical Assets	Inara Reference Pattern
Level 4 / 5	Enterprise / Business Network	ERP, email, Active Directory, internet-facing services	Standard IT zero-trust segmentation (Fortinet, Palo Alto perimeter)
Level 3.5	Industrial DMZ (IDMZ)	Patch repository, jump server, historian replica, AV update server	Mandatory in every brownfield design; no L3/L4 traffic crosses without IDMZ inspection
Level 3	Site Operations	Engineering workstations, plant historian, asset management	Segmented from Level 4 via IDMZ; Fortinet OT-aware firewalls; visible to OT-SOC
Level 2	Supervisory (SCADA / HMI)	SCADA servers, HMI screens, operator consoles	Read-only telemetry to OT-SOC; no inbound corporate traffic
Level 1	Basic Control (PLC/DCS)	PLCs, DCS controllers, safety controllers	Passive monitoring only; SPAN/TAP-based asset discovery
Level 0	Process / Physical	Sensors, actuators, motors, valves	Out of scope for cyber controls; physical security domain

Practical Test

Ask a prospective OT security provider to draw the IDMZ for one of your existing plants. If they draw a single firewall between Level 3 and Level 4, they are not IEC 62443-aligned – the standard requires a double-firewall (or equivalent) with no direct protocol pass-through.

THE FIVE-DOMAIN
OT Security Capability Framework

Scoring Provider Maturity Across Five Domains

Score every prospective OT security provider 1–4 on each of the five domains below. A provider scoring below 2.5 average should not be shortlisted. A provider scoring above 3.0 on all five is rare in the Pakistan market today.

#	Domain	What to Evaluate
01	Asset Discovery & Visibility	Passive (SPAN/TAP) discovery for legacy protocols (Modbus, DNP3, Profinet, IEC 61850). Inventory completeness for vendor-locked HMIs and PLCs. Time-to-discover for a newly-added asset. Risk scoring per asset.
02	Network Segmentation Architecture	Reference architecture expressed in IEC 62443 zones and conduits. IDMZ design pattern. Brownfield segmentation approach (logical via virtual firewalls vs. physical re-cabling). Treatment of safety-instrumented systems (SIS).
03	OT-SOC Operating Model	Dedicated OT-SOC analysts (not IT analysts with a Modbus decoder). Coverage model. Escalation runbook that respects plant safety. Joint exercises with plant shift engineers. Distinct playbook library for OT incidents.
04	Vendor & Tooling Stack	Tooling choices justified against the plant's protocol mix and asset vendors. Approach to legacy Windows endpoints. OT-aware firewall stack (Fortinet OT, Palo Alto). Backup architecture for engineering workstations (NetBackup, Veeam).
05	Regulatory & Audit Readiness	Mapping of controls to IEC 62443, ISO 27001, and any sector-specific Pakistani regulations. Evidence package for audit. Approach to incident reporting under emerging Pakistan cyber regulations.

THE PAKISTAN
Threat Landscape for Critical Infrastructure

Why Generic Global Threat Intel Is Not Enough

Pakistan's critical infrastructure operators face a threat mix that does not align cleanly with global threat reports. Three risks dominate the OT-incident pattern we see at Inara across oil & gas, power, and utilities engagements.

Threat Pattern	Typical Vector	Plant Impact	Mitigation Priority
IT-to-OT lateral movement after IT compromise	Phishing on corporate IT → credential theft → jump from corporate AD to engineering workstation	Engineering workstation compromise; risk of HMI configuration change	P0: Hardened IDMZ; no shared AD between IT and OT; segmented engineering domain
Insider misuse via legitimate remote access	Vendor / third-party support session with weak controls; shared credentials; lack of session recording	Configuration drift; undocumented changes to control logic	P0: Privileged access management for OT; session recording; just-in-time access; vendor RACI
Ransomware encrypting engineering workstations and historians	Commodity ransomware spreads from IT; engineering workstations and historian DBs encrypted	Loss of process visibility; loss of historical data needed for safe restart	P1: Air-gapped backups via Veeam/NetBackup; immutable copies; tested restore drills
Supply-chain compromise via OEM update channels	Compromised firmware update or vendor management tool installed during commissioning	Latent backdoor in PLC firmware or vendor toolchain	P2: Firmware integrity verification; vendor sub-processor disclosure; SBOM where available

ARCHITECTURE PATTERNS
Brownfield Segmentation

How to Segment a Plant That You Cannot Shut Down

Greenfield OT segmentation is easy: design the zones, deploy the equipment, commission. Brownfield segmentation is the real challenge – the plant is running, the turnaround window is twelve months away, and the existing network is a flat Layer-2 fabric carrying every protocol from every era of the plant's history. The brownfield pattern below is what Inara deploys when the customer cannot accept production downtime.

Phase	Activities	Duration	Production Impact
1. Passive Discovery	Install SPAN/TAP sensors; passive asset inventory; protocol map; communication-pair heatmap	4–6 weeks	Zero
2. IDMZ Standup (logical)	Deploy IDMZ firewalls and jump servers in parallel; do not route production traffic through them yet; build the patch repository, historian replica, AV update server, and Active Directory bridge	6–8 weeks	Zero
3. Service Migration	Move corporate-to-OT services one at a time through the IDMZ: AV updates, patch distribution, OEM remote support, historian replication. Each service is cut over individually with rollback ready	8–12 weeks	Brief per-service windows agreed with operations
4. Zone Enforcement	Apply default-deny between zones at the IDMZ; previously-discovered legitimate flows are whitelisted; anomalous flows generate OT-SOC alerts but are not blocked initially	4–6 weeks	Zero – alert-only mode
5. Enforcement Hardening	Move from alert-only to block at the IDMZ for previously-anomalous flows; SOC reviews exceptions with the plant	Ongoing (post-go-live)	Per-flow review only

OT-SOC
Why an IT SOC Will Not Work

Operating Model Differences That Demand a Separate Practice

An IT SOC analyst is trained to contain threats. An OT-SOC analyst is trained to contain threats without tripping the plant. The difference is not in the SIEM dashboard – it is in the response playbook, the escalation runbook, and the engineering literacy of the analyst on shift.

Capability	IT SOC Standard	OT-SOC Requirement
Analyst literacy	Networking, OS internals, threat analysis	All of IT – plus control-system concepts (PLC scan cycle, HMI logic, safety interlocks, hot standby)
Containment philosophy	Isolate the host; quarantine the endpoint	Contain at the IDMZ; preserve plant visibility; never isolate a live HMI without operator approval
Escalation path	On-call engineer → incident commander	On-call analyst → plant shift engineer (jointly authorized) → operations manager → incident commander
Playbook coverage	Ransomware, phishing, identity compromise, lateral movement	All IT playbooks – plus engineering-workstation compromise, historian tampering, HMI configuration change, vendor session anomaly
Joint exercise cadence	Annual tabletop with IT leadership	Quarterly OT-specific tabletop including plant shift engineers; annual full plant simulation

Buyer Test

Ask the prospective provider for their OT incident-response playbook for a compromised engineering workstation on a live refinery. A credible response describes coordination with the shift engineer, the safety system status check, the containment posture at the IDMZ, and the criteria for escalation – not 'isolate the host and reimage.'

VENDOR & TOOLING
Selection Criteria

Six Buyer Questions That Separate OT-Native from IT-Repositioned

#	Question	What a Good Answer Looks Like
1	Which industrial protocols does your asset-discovery tool decode natively, and which require add-on modules?	Specific protocol list (Modbus, DNP3, OPC UA, IEC 61850, Profinet, EtherNet/IP); honest about gaps; pricing for add-ons disclosed
2	How does your tooling handle Windows XP/7 engineering workstations and HMIs that cannot run EDR?	Network-based detection rather than endpoint agent; integration with whitelisting tools; documented compensating controls
3	What is your firewall stack for the IDMZ, and why? (Fortinet OT, Palo Alto, Cisco ISA, others?)	Vendor-neutral recommendation tied to existing plant stack; willingness to mix vendors per zone; honest about partner economics
4	How are engineering workstations backed up, and how do you guarantee an immutable, air-gapped restore point?	Veeam / NetBackup with immutable repository; documented restore drills; defined RPO/RTO per asset class
5	What is your incident-response runbook when the only safe containment is to wait for the next turnaround?	Documented holding posture; communication plan with operations; daily monitoring intensification; defined go/no-go criteria
6	What ISO 27001 controls in your ISMS apply to OT-SOC operations specifically, beyond the IT SOC?	Specific clauses (access control, asset management, supplier relationships) mapped to OT delivery; auditor evidence available

REGULATORY
& Compliance Alignment

IEC 62443, ISO 27001, and Pakistan Sector-Specific Requirements

OT security in Pakistan sits at the intersection of three regulatory and standards frameworks. A credible program demonstrates control alignment across all three, with auditor-ready evidence for each.

Framework	Scope	Evidence to Request from Providers
IEC 62443 (IEC/ISA)	International OT/ICS security standard – zones, conduits, foundational requirements, security levels	Reference architecture in IEC 62443 terms; mapping of provider controls to the foundational requirements; SL-Target capability statement per zone
ISO 27001:2022 ISMS	Provider's own information-security management system covering OT-SOC operations	Current certificate with scope statement explicitly including OT services; Statement of Applicability; sample internal audit report
Pakistan PDPA – emerging	Personal data handling within OT environments (rare in pure plant ops, common in mixed IT-OT)	Data Processing Agreement; data residency commitment for any telemetry stored; breach-notification procedure
Sector regulatory (OGRA, NEPRA, sector-specific)	Sector-specific cyber and safety regulations applicable to oil & gas, power, water	Evidence of prior engagements with the sector regulator; familiarity with reporting timelines; willingness to support customer audit

THE 18-QUESTION
OT Security RFP Scorecard

Use the following questions in RFP responses, provider presentations, and reference checks. Score each response 0 (not addressed), 1 (partially addressed), or 2 (fully addressed). A provider scoring below 28/36 should not advance to commercial evaluation.

#	Category	Question	Score /2
Q1	Asset Discovery	Which industrial protocols does your discovery tool decode natively? Provide the full list.	__ /2
Q2	Asset Discovery	What is the typical time-to-inventory for a 5,000-asset plant? What are the most common gaps?	__ /2
Q3	Architecture	Show a sample IDMZ design from a comparable Pakistan brownfield engagement.	__ /2
Q4	Architecture	Describe your brownfield segmentation phasing. How do you avoid production downtime?	__ /2
Q5	OT-SOC	How many dedicated OT-SOC analysts do you have, distinct from your IT SOC team?	__ /2
Q6	OT-SOC	Describe your escalation path when a P1 detection at 2 a.m. requires the plant shift engineer to authorize action.	__ /2
Q7	OT-SOC	How many OT-specific playbooks do you maintain? List coverage of engineering-workstation compromise and HMI config change.	__ /2
Q8	Tooling	Walk us through your firewall stack choices per Purdue level and why.	__ /2
Q9	Tooling	How do you protect engineering workstations and historians against ransomware? Show your backup architecture.	__ /2
Q10	Vendor Access	Describe your privileged-access model for third-party vendors accessing OT. Session recording? JIT?	__ /2
Q11	Incident Response	Provide a redacted incident report from a comparable OT engagement in the last 24 months.	__ /2
Q12	Incident Response	What is your runbook when the only safe containment is to wait for the next turnaround?	__ /2
Q13	Compliance	Show your ISO 27001 certificate with a scope statement that explicitly includes OT services.	__ /2
Q14	Compliance	Map your controls to IEC 62443 foundational requirements. SL-Target per zone?	__ /2

#	Category	Question	Score /2
Q15	Operations	What are your committed MTTD and MTTR targets for OT detections, by priority? Measurement methodology?	__ /2
Q16	Operations	Provide a sample monthly report from a comparable client. Differentiate operational data from management insight.	__ /2
Q17	References	Provide two references from Pakistan critical-infrastructure clients you have served for 12+ months.	__ /2
Q18	References	Provide one reference from a regulator engagement where you supported the customer's audit.	__ /2

Scoring Guide: Below 22/36: Do not advance / 22–28/36: Conditional – address gaps before contracting / 29–36/36: Qualified for commercial evaluation.