IS YOUR OT ENVIRONMENT CYBER-SECURE?

OT environments are the backbone of critical infrastructure — yet most are assessed only after a breach. OTx Systems delivers a structured, standards-based Cybersecurity Assessment that identifies real risk before it becomes an incident.

IEC 62443 · NIST SP 800-82 · ISA-95 / Purdue

Know Your Exposure. Reduce Your Risk. Protect What Matters.

Why OT Cybersecurity Matters

Operational Technology (OT) systems — PLCs, RTUs, SCADA, DCS — once isolated, are now connected. This connectivity brings efficiency but exposes critical operations to cyber threats that can cause:

- Production shutdowns and unplanned downtime
- Safety incidents and physical equipment damage
- Regulatory non-compliance and insurance exposure
- Intellectual property and process data theft

Unlike IT environments, OT systems often run 24/7, cannot be patched easily, and use legacy protocols with no built-in security. A breach in OT is not just a data problem — it is an operational and safety emergency.

OT THREAT REALITY

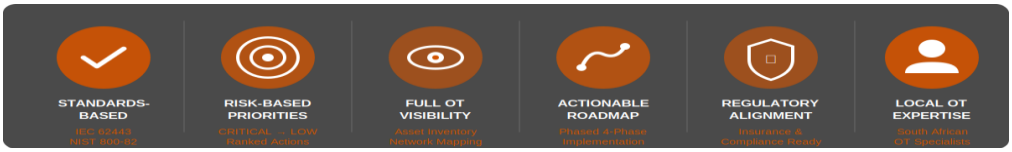
68%	of industrial organisations experienced an OT security incident in the past 12 months
SL-0	typical Security Level found in unassessed OT environments — zero protection
72hrs	average time for OT ransomware to cause physical process disruption
R 4.2M+	average cost of an OT cybersecurity incident in Sub-Saharan Africa

The OTx 5-Phase Assessment Methodology

Our assessment follows a structured 5-phase methodology — fully aligned to IEC 62443, NIST SP 800-82 r3, and the ISA-95 Purdue Model. Each phase delivers a specific set of outputs that together build a complete picture of your OT security posture.

Fig 1 — OTx 5-Phase Assessment Process and 5-Document Deliverable Suite

Why Choose OTx Systems?



Zone-Based Security Assessment

We map every asset to its Purdue/ISA-95 zone and evaluate each zone independently against IEC 62443-3-3 Security Level targets (SL-T). This gives you granular insight into where your weakest links are — not just a site-level score.

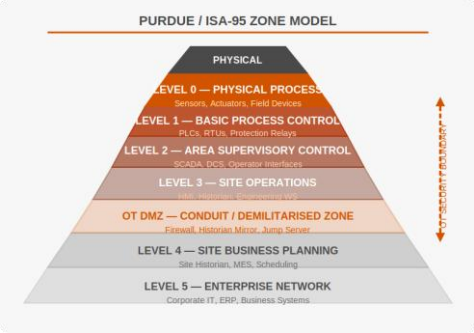


Fig 2 — ISA-95 / Purdue Zone Model

Security Level Gap Analysis

Each Foundational Requirement (FR1–FR7) from IEC 62443 is scored against 29 system requirements. The gap between your Actual Security Level (SL-A) and Target (SL-T) drives the remediation priority. The weakest FR defines your overall SL — the 'weakest link' principle.

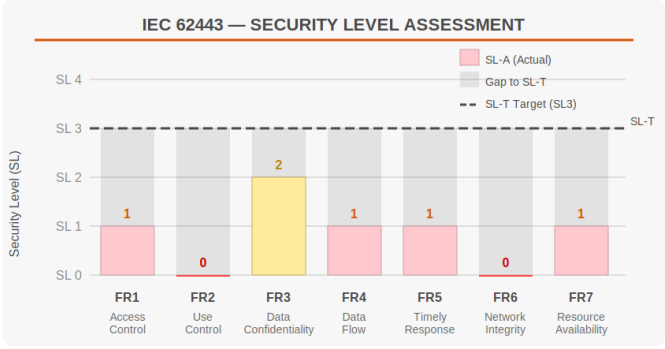


Fig 3 — Illustrative SL-A vs SL-T Gap (FR1–FR7)

From Findings to Action — The Remediation Roadmap

Every assessment concludes with a phased Remediation Roadmap — prioritised actions tied directly to findings, with indicative cost bands, dependencies, and measurable success criteria. No generic recommendations: everything is traceable to a specific gap.

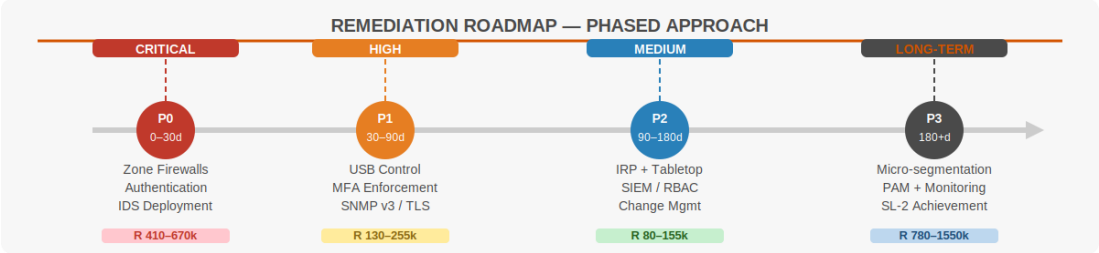


Fig 4 — 4-Phase Remediation Roadmap with Investment Summary

WHAT YOU RECEIVE

- ✓ OT Security Assessment Framework
- ✓ Asset & Network Inventory Workbook
- ✓ IEC 62443 Gap Analysis Matrix
- ✓ OT Assessment Report & Findings
- ✓ Phased Remediation Roadmap

INDUSTRIES SERVED

- Energy & Utilities
- Mining & Resources
- Manufacturing & Process
- Petrochemical & Oil & Gas
- Transport & Logistics
- Building Automation

READY TO ASSESS YOUR OT SECURITY?

Paulo de Sousa Gomes
Managing Director
OTx Systems
16 Cambridge Rd, Bryanston
Gauteng, South Africa 2191
otxsystems.co.za