QuantLayer

by BDATA Solutions Inc.

WHITE PAPER / 2026

QUANTLAYER · TECHNICAL BRIEFING

Industrial Security Without Downtime

A practical guide to IEC 62443-aligned enforcement in safety-critical environments where uptime is non-negotiable.

PUBLICATION	VERSION	FORMAT	CLASSIFICATION
WP-QL-IND-01	v1.0	Technical	Public

BDATA Solutions Inc.

bdata.ca · info@bdata.ca

© 2026 BDATA Solutions Inc. All rights reserved.

EXECUTIVE SUMMARY

At a glance

Industrial control systems were never designed to share networks with hostile actors. They prioritise deterministic timing, safety integrity, and uptime over confidentiality — yet ransomware groups and state-aligned actors now actively target plant floors, substations, and water-treatment facilities.

QuantLayer was engineered from the start for the OT operating model: passive discovery, non-disruptive enforcement, and protocol-aware policy that respects safety boundaries. This briefing details the IEC 62443 mapping, a six-phase rollout pattern with zero unplanned downtime in protected zones, and the operating model that lets security and engineering teams collaborate without friction.

0	6	8+	100%
UNPLANNED OUTAGES	ROLLOUT PHASES	OT PROTOCOLS	IEC 62443 FRS

© 2026 BDATA Solutions Inc.

CONTENTS

In this briefing

01	Why OT cannot adopt IT playbooks wholesale	4
02	Mapping enforcement to IEC 62443	5
03	A six-phase non-disruptive deployment	6
04	Coexisting with SIS and process safety	7
05	Protocol coverage matrix	8
06	Rollout roadmap & outcomes	9
07	Next steps	10

© 2026 BDATA Solutions Inc.

01 · CONTEXT

Why OT cannot adopt IT playbooks wholesale

Industrial control systems were never designed to share a network with hostile actors. They prioritise deterministic timing, safety integrity, and uptime over confidentiality. Yet ransomware groups, hacktivists, and nation-state actors now actively target plant floors, substations, and water-treatment facilities. Security controls designed for IT — agent installation, frequent patching, active scanning — are often impossible, unsafe, or simply unsupported by legacy controllers.

QuantLayer was engineered from the start for the OT operating model: passive discovery, non-disruptive enforcement, and protocol-aware policy that respects safety boundaries.

- Passive asset discovery with zero impact on safety-instrumented systems.
- Identity-bound microsegmentation at Purdue Levels 2 and 3.
- Protocol-aware enforcement: Modbus, DNP3, OPC-UA, IEC 61850, BACnet, EtherNet/IP.
- Read-only insertion with progressive enforcement gating.

> **DESIGN PRINCIPLE**
>
> Every enforcement action in OT is reversible and observable. Operators always have explicit override authority, and every decision carries an evidence chain.

© 2026 BDATA Solutions Inc.

02 · IEC 62443

Mapping enforcement to the standard

IEC 62443 defines the leading framework for industrial automation security. QuantLayer aligns its policy primitives directly to the standard's zone-and-conduit model, making compliance evidence a by-product of normal operation rather than a separate workstream.

- Zones & Conduits — policy-as-code expressed in IEC 62443 vocabulary.
- Security Levels — SL1 to SL4 enforcement profiles.
- Foundational Requirements — coverage across FR1–FR7.
- Continuous evidence export to GRC platforms (ServiceNow, Archer, OneTrust).

© 2026 BDATA Solutions Inc.

03 · ROLLOUT

A six-phase non-disruptive deployment

The following six-phase pattern has been deployed across utilities, manufacturing, and pipeline operators with no unplanned downtime in protected zones.

- Phase 1 — Passive observation and asset inventory.
- Phase 2 — Baseline behavioural modeling.
- Phase 3 — Policy drafting against zone boundaries.
- Phase 4 — Alert-only enforcement.
- Phase 5 — Progressive blocking with operator approval.
- Phase 6 — Continuous attestation and audit reporting.

OPERATOR EXPERIENCE

Operators interact with QuantLayer through a console designed for control-room ergonomics, with role-based dashboards for site operations, security, and engineering teams.

© 2026 BDATA Solutions Inc.

04 · SAFETY ALIGNMENT

Coexisting with SIS and process safety

QuantLayer never inserts itself in-line with safety-instrumented systems (SIS). Enforcement points are placed where they cannot affect safety logic, and every change request flows through a documented engineering management-of-change process.

- No agents on PLCs, RTUs, or SIS controllers.
- Out-of-band enforcement points only.
- Change-window scheduling aligned to plant operations.
- Engineering MOC integration with Maximo, SAP PM, and IBM TRIRIGA.

© 2026 BDATA Solutions Inc.

05 · PROTOCOL COVERAGE

Industrial protocols & enforcement depth

QuantLayer parses industrial protocols at the application layer, allowing policy decisions based on function code, register range, or command type — not just IP and port.

Protocol	Use Case	Enforcement Depth
Modbus TCP/RTU	Discrete & process control	Function code + register
DNP3	Electric utilities & substations	Object group + variation
OPC-UA	Modern industrial integration	Node ID + method
IEC 61850 MMS/GOOSE	Substation automation	Logical node + dataset
EtherNet/IP (CIP)	Discrete manufacturing	Service + class/instance
BACnet	Building automation	Object type + property

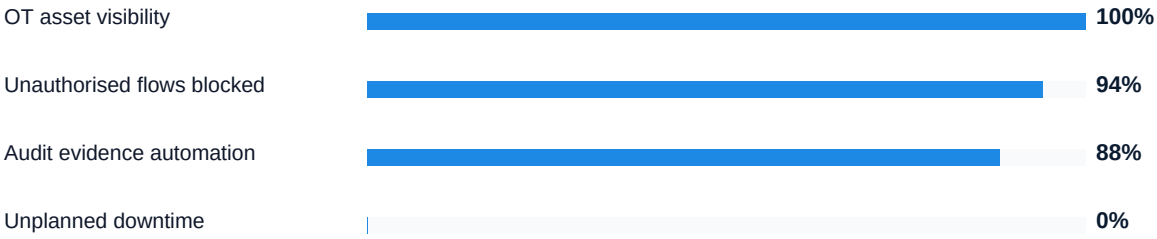
© 2026 BDATA Solutions Inc.

06 · ROADMAP

Six-phase rollout & measured outcomes

Each phase produces a defined deliverable and a checkpoint that engineering leadership signs off before progressing — keeping plant operations in control at every step.

Outcomes after Phase 6



SAFETY GUARANTEE

Every protected zone is deployed with a documented rollback procedure and a 30-day enforcement holdback window before any blocking policy becomes permanent.

© 2026 BDATA Solutions Inc.

NEXT STEPS

Start with one zone, prove the model

BDATA recommends scoping the first deployment to a single zone — typically a Purdue Level 3 supervisory network — and proving the operating model before expanding plant-wide.

- Site survey and IEC 62443 zone/conduit assessment (2 weeks).
- Passive deployment in target zone within 30 days.
- Engineering sign-off package for the first enforcement window.

ENGAGE WITH BDATA

Contact our QuantLayer advisory team to scope an architecture review or request a guided platform demonstration: **info@bdata.ca** · **bdata.ca**

© 2026 BDATA Solutions Inc.

REFERENCES

Standards & frameworks

- NIST SP 800-207 — Zero Trust Architecture
- NIST CSF 2.0
- ISO/IEC 27001:2022
- IEC 62443 — OT Security
- MITRE ATT&CK; & D3FEND
- CISA Cross-Sector CPGs
- FIPS 203 / 204 / 205 — Post-Quantum Cryptography
- Cloud Security Alliance — Zero Trust Guidance v2

BDATA Solutions Inc.
bdata.ca · info@bdata.ca
© 2026 BDATA Solutions Inc. All rights reserved.