Deloitte.

*Together makes progress*

KNOWLEDGE EXCHANGE | PERFORMANCE ASSURANCE

# OT Assurance Twin: Context-Aware Asset Management for Operational Technology

**Authors:** Deloitte Performance Assurance Team

**Date:** November 2025
**Industry Focus:** Oil & Gas, Utilities, Manufacturing, Pharmaceuticals

## Executive Summary

Operational Technology (OT) environments face a critical visibility gap: organizations typically have only 50-80% visibility into their OT assets, creating blind spots that compromise security, compliance, and operational efficiency. Traditional approaches—OT security platforms, CMDB systems, and engineering documentation—operate in silos, providing fragmented views that lack context and verification.

The **OT Assurance Twin** addresses this gap by fusing multiple data sources (Engineering baseline, OT discovery, CMMS, Security, Network, Incidents) into a single, verified, context-aware asset canon. Unlike traditional asset lists, the Assurance Twin provides process-aware intelligence—mapping assets to production units, assessing plant completeness, and cross-verifying classifications between engineering intent and operational reality.

> This whitepaper explores the market need for context-aware OT asset management, the unique capabilities of the Assurance Twin, Deloitte's strategic position to deliver this solution, and how it enhances existing tools while laying the foundation for digital twin initiatives.

## 1. The Problem: The OT Asset Visibility Crisis

### 1.1 The Visibility Gap

Industrial organizations manage thousands of OT assets across multiple systems: engineering documentation (P&IDs, CAD), control systems (DCS, SCADA), OT security platforms (Claroty, Dragos, Nozomi), asset management systems (CMMS), and network infrastructure. Each system provides a partial view, but none provides a complete, verified picture.

> **Industry Reality:** Most organizations have **50-80%** visibility into their OT assets, with significant gaps in network discovery, engineering documentation accuracy, and cross-system reconciliation.

### 1.2 The Consequences of Fragmented Data

This fragmentation creates critical business risks:

- **Security Blind Spots:** Engineering says a PLC is networkable, but OT discovery didn't find it. Is it offline, misconfigured, or on an unscanned network segment?
- **Compliance Gaps:** Regulators ask "How do you know your security coverage is accurate?" Without cross-verification, you can't prove it.

- **Operational Inefficiency:** Maintenance teams can't find assets, engineers don't know what's actually deployed, and CISOs can't prioritize security investments.
- **Digital Twin Barriers:** You can't build a reliable digital twin without a verified, complete asset inventory.

### 1.3 Why Traditional Tools Fall Short

> #### The List Problem
>
> Traditional OT asset management tools produce **lists**—inventories of devices with attributes (IP, manufacturer, model). But lists lack context: *What does this device do? Where is it in the production process? Is it critical? What's missing?*
>
> The Assurance Twin provides **context-aware asset management**—not just what you have, but what it does, where it is, how you know, and what's missing.

**OT Security Platforms** (Dragos, Claroty, Nozomi, Tenable.ot) excel at network discovery and threat detection but:

- Only show what's on the network (50-80% coverage due to collector gaps, shadow networks, air gaps)
- Lack engineering context (don't know what devices are supposed to do)
- No process unit mapping (can't answer "what's missing in the Crude Distillation Unit?")
- No cross-verification (can't prove engineering baseline matches reality)

**CMDB Systems** (ServiceNow, Axonius) track configuration items but:

- Mirror what other tools report (garbage in = garbage out)

- No validation layer (can't verify data quality)
- No process awareness (asset-centric, not process-centric)
- No blind spot detection (only know what's reported, not what's missing)

**Engineering Systems** (P&ID/CAD, DCS, Historian) define design intent but:

- Siloed per system (no plant-wide unified view)
- Often stale (not updated when field changes occur)
- No network reality check (design vs. actual deployment mismatch)
- No security context (don't know what needs to be secured)

## 2. Market Analysis: The Growing Need for OT Asset Assurance

### 2.1 Market Size and Growth

The digital twin market is experiencing explosive growth, with OT asset management as a foundational component:

- **Digital Twin Market:** Projected to reach $16.5 billion in 2025, with a CAGR of 25% through 2030
- **OT Security Market:** Growing at 15-20% CAGR, driven by increasing cyber threats to critical infrastructure
- **Manufacturing Adoption:** 29% of global manufacturing companies have implemented digital twin strategies (up from 20% in 2020)
- **Energy Sector:** Utilities and renewables projected to see CAGR exceeding 27%

### 2.2 Market Drivers

### Key Market Drivers

- **Regulatory Pressure:** NERC CIP, IEC 62443, FDA requirements demand provable asset inventories
- **Cybersecurity Threats:** Rising attacks on critical infrastructure (Colonial Pipeline, water treatment facilities) require complete visibility
- **Digital Transformation:** Organizations need verified asset data to build digital twins, predictive maintenance, and AI/ML models
- **IT/OT Convergence:** CISOs need to bridge the gap between IT asset management and OT reality
- **Operational Efficiency:** Plant managers need to know what they have, where it is, and what's missing

## 2.3 Market Gaps

Despite market growth, significant gaps remain:

| Capability | OT Security Tools | CMDB Systems | Engineering Tools | Market Gap |
|---|---|---|---|---|
| Complete Visibility | 50-80% (network only) | Mirrors discovery | 100% design intent | **No verified 100% baseline** |
| Process Context | None | None | Per-system only | **No plant-wide process mapping** |
| Cross-Verification | None | None | None | **No "how do we know?" layer** |

| Capability | OT Security Tools | CMDB Systems | Engineering Tools | Market Gap |
|---|---|---|---|---|
| Blind Spot Detection | Shows what's found | Shows what's reported | Shows what's designed | **No explicit gap identification** |
| Audit Readiness | Dashboards only | Workflow evidence | Not audit-grade | **No regulator-ready evidence** |

### 2.4 Market Appetite

Industry surveys and client engagements reveal strong appetite for OT asset assurance solutions:

- **CISO Priorities:** 78% of CISOs in critical infrastructure cite "OT asset visibility" as a top 3 priority
- **Regulatory Compliance:** 85% of organizations struggle to provide regulator-ready asset inventories
- **Digital Twin Readiness:** 62% of organizations cite "incomplete asset data" as the #1 barrier to digital twin initiatives
- **Budget Allocation:** OT security budgets growing 20-30% annually, with asset management as a key investment area

## 3. The Solution: OT Assurance Twin

### 3.1 Core Capabilities

The OT Assurance Twin is a **Master Data Management (MDM) platform for OT assets with built-in assurance and cross-verification**. It fuses multiple data sources into one verified, context-aware asset canon.

> #### Key Capabilities

> ✓ **Multi-Source Fusion:** Ingests Engineering baseline, OT discovery, CMMS, Security findings, Network segmentation, and Incident data
>
> ✓ **Flexible Matching:** 6 matching strategies (Tag ID, IP, Hostname, MAC, Fuzzy, Intelligent Pairing) with confidence scoring
>
> ✓ **Cross-Verification:** Validates Engineering baseline against OT discovery reality—flags mismatches, unverified devices, suspicious classifications
>
> ✓ **Process-Aware Intelligence:** Maps assets to process units (Crude Distillation, FCC, Tank Farm) and performs multi-layered completeness analysis (reference ranges, relative comparison, functional completeness, baseline tracking)
>
> ✓ **Explicit Gap Detection:** Identifies blind spots (Engineering assets not on network) and orphans (OT assets not in baseline)
>
> ✓ **Multi-Source Enrichment:** Links maintenance history, vulnerabilities, network zones, and incidents to canonical assets
>
> ✓ **Audit-Ready Outputs:** Generates regulator-ready evidence with validation scores and cross-verification summaries

## 3.2 The 4-Phase Process

### Phase 1: Ingest & Standardize

Accepts disparate CSV files from multiple sources. Auto-detects data source type from headers, normalizes field names across varied formats (handles variations: tag_id = tag = asset_tag), merges multiple files of the same type, and deduplicates by tag_id/IP/hostname.

### Phase 2: Match & Canonize

Matches engineering baseline to OT discovery using 6 strategies in order of confidence (Tag ID 100%, IP 95%, Hostname 90%, MAC 85%, Fuzzy 60%, Intelligent Pairing 50%). Builds canonical asset records (one row per matched asset) and identifies gaps: blind spots (Engineering assets not found on network) and orphans (OT assets not in engineering baseline).

#### Phase 3: Verify & Enrich

Cross-validates matches by checking field agreement (tag, IP, hostname, MAC, device_type, manufacturer) and assigns confidence levels (High ≥3 agreements, Medium ≥1, Low 0). Classifies devices by security tier (Tier 1: Critical Network, Tier 2: Smart/Networkable, Tier 3: Passive/Analog). Enriches with multi-source data (CMMS work orders, CVEs, firewall zones, incidents). Maps to process units and performs multi-layered completeness analysis (industry reference ranges, relative comparison, functional completeness, baseline tracking).

#### Phase 4: Analyze & Export

Calculates KPIs (coverage %, security coverage %, plant completeness scores). Generates AI recommendations (data quality issues, security gaps, unknown devices, OT collector deployment locations). Exports canonical inventory, blind spots, and orphans as CSV/JSON.

## 4. Why It's Unique: Context-Aware vs. List-Based Asset Management

### 4.1 The Context-Aware Difference

Traditional asset management tools produce **lists**—inventories of devices with attributes. The Assurance Twin provides **context-aware intelligence**—understanding not just what you have, but what it does, where it is in the production process, and how you know it's correct.

> #### Example: The List vs. Context Problem

> **Traditional Tool Output:** "PLC-101, IP: 192.168.1.10, Manufacturer: Rockwell, Model: ControlLogix"
>
> **Assurance Twin Output:** "PLC-101 controls the Crude Distillation Unit feed pump (critical path). Located in Zone 1, verified by Engineering baseline + OT discovery (HIGH confidence). 2 unpatched CVEs, last maintenance: 45 days ago. Expected 10 PLCs in CDU, found 8—2 missing (blind spots)."

## 4.2 Unique Differentiators

### 1. Cross-Verification: "How Do We Know?"

The Assurance Twin doesn't just merge data—it **verifies** it. Engineering says a device is networkable, but OT discovery didn't find it. The system flags this as "UNVERIFIED" and provides possible causes (offline, wrong IP, unscanned segment, stale data). This "how do we know?" layer is critical for audit readiness and trust.

### 2. Process-Aware Intelligence

Unlike network-centric tools, the Assurance Twin maps assets to **process units** (Crude Distillation, FCC, Tank Farm). It uses a multi-layered completeness analysis: (1) Industry reference ranges for anomaly detection and sanity checks, (2) Relative comparison of similar units within the same plant to identify outliers, (3) Functional completeness assessment to ensure critical process functions have required instrumentation, and (4) Baseline tracking to detect degradation over time. This process context enables operational decision-making, not just security monitoring.

### 3. Explicit Blind Spot Detection

Traditional tools show what they found. The Assurance Twin explicitly identifies what's **missing**:

- **Blind Spots:** Engineering assets not found on network (visibility gaps)

- **Orphans:** OT assets not in engineering baseline (undocumented devices)
- **Suspicious Classifications:** Engineering says passive, but OT found it on network (likely misclassified)

### 4. Multi-Source Reconciliation

Not just network discovery—the Assurance Twin fuses Engineering + OT Discovery + CMMS + Security + Network + Incidents into one verified canon. This multi-source approach provides a complete picture that no single tool can deliver.

### 5. Plant Completeness Analysis

Uses a multi-layered completeness analysis approach that acknowledges plant variability while providing actionable insights:

- **Industry Reference Ranges:** Provides initial sanity checks using industry-typical equipment ranges (min/typical/max) to flag potential anomalies. For example, "CDU Unit 1 has 0 PLCs—this is outside industry norms, investigate." These ranges are reference points, not rigid requirements, and can be customized to match your plant's design standards.
- **Relative Comparison:** Compares similar units within the same plant to identify outliers. For example, "CDU-1 has 150 transmitters, CDU-2 has 80—investigate CDU-2." This plant-specific comparison is more defensible than absolute counts.
- **Functional Completeness:** Assesses whether critical process functions have the required instrumentation, rather than focusing on exact device counts. For example, "Distillation column has no level transmitters—critical gap." This process-aware approach understands what's needed for safe and efficient operation.
- **Baseline Tracking:** When historical data is available, compares current state to previous baselines to detect degradation over time. For

example, "Transmitter count dropped from 120 to 95 in CDU—investigate."

This layered approach provides defensible, engineering-minded analysis that respects plant-specific design while identifying genuine operational risks and gaps.

## 5. Why Deloitte: Unique Position to Fill the Gap

### 5.1 Deloitte's Strategic Advantages

#### 1. Cross-Domain Expertise

Deloitte brings together **OT security, engineering operations, and IT asset management** expertise—the three domains required to build a true assurance layer. Most vendors specialize in one area; Deloitte can bridge all three.

#### 2. Industry-Specific Knowledge

Deloitte's deep industry experience (Oil & Gas, Utilities, Manufacturing, Pharmaceuticals) provides the **process knowledge** needed for context-aware asset management. We understand how process units function, what critical instrumentation is required for safe operation, and how to assess completeness through relative comparison and functional analysis—respecting plant-specific design while identifying genuine operational risks.

#### 3. Regulatory and Compliance Expertise

Deloitte's audit and compliance practice understands what regulators need: **provable, verifiable, audit-ready evidence**. The Assurance Twin is designed from the ground up to meet regulatory requirements (NERC CIP, IEC 62443, FDA).

#### 4. Trusted Advisor Position

As a trusted advisor, Deloitte can deliver this as a **service**—not just software, but the expertise to interpret results, guide remediation, and build the organizational capability. This service layer is critical for enterprise adoption.

#### 5. Integration Capabilities

Deloitte's technology practice can integrate the Assurance Twin with existing client systems (ServiceNow, Axonius, SIEM/SOAR, data lakes) and build the APIs, webhooks, and automation needed for enterprise deployment.

### 5.2 Market Positioning

Deloitte is uniquely positioned because:

- **We're not a vendor:** We're a trusted advisor who can deliver this as a service, not just sell software
- **We understand the problem:** We've seen the visibility gap firsthand in hundreds of client engagements
- **We have the expertise:** OT security, engineering operations, IT asset management, compliance, and technology integration
- **We can scale:** Deloitte's global delivery model can deploy this across multiple clients and industries

## 6. How the Assurance Twin Enhances Existing Tools

### 6.1 Enhancing OT Security Platforms

The Assurance Twin doesn't replace OT security tools—it **validates and contextualizes** their output:

- **Completeness Validation:** "Your OT tool found 8,000 devices, but engineering baseline has 12,000. Here are the 4,000 blind spots."

- **Process Context:** "Those 8,000 devices map to these process units. Here's security coverage by unit."
- **Classification Verification:** "Engineering says these 200 devices are networkable, but OT tool only found 150. Here are the 50 unverified devices."
- **Prioritization:** "Focus security efforts on the Crude Distillation Unit—it has 18 unmanaged PLCs on the critical path."

### 6.2 Enhancing CMDB Systems

The Assurance Twin provides the **verified, cross-checked data** that CMDBs need:

- **Data Quality:** Validates CMDB entries against engineering baseline and OT discovery—flags inconsistencies
- **Completeness:** Identifies assets missing from CMDB (orphans found by OT discovery)
- **Freshness:** Flags stale CMDB entries (engineering baseline updated, but CMDB not synced)
- **Enrichment:** Adds process context, security tier, and completeness scores to CMDB records

**Integration Path:** Assurance Twin can push verified canonical assets to ServiceNow CMDB via API, ensuring CMDB has accurate, validated data rather than unverified imports.

### 6.3 Foundation for Digital Twin

Digital twins require a **complete, verified, context-aware asset inventory**—exactly what the Assurance Twin provides:

#### Digital Twin Requirements vs. Assurance Twin Capabilities

| Digital Twin Requirement | Assurance Twin Capability |
|---|---|
| Complete asset inventory | 100% engineering baseline + verified OT discovery |
| Process unit mapping | Maps assets to process units (CDU, FCC, Tank Farm) |
| Asset relationships | Links assets to loops, units, and process paths |
| Operational context | Multi-layered completeness analysis (reference ranges, relative comparison, functional completeness, baseline tracking) |
| Data quality assurance | Cross-verification and validation scoring |
| Multi-source data fusion | Fuses Engineering + OT + CMMS + Security + Network |

### Layering Digital Twin Capabilities

The Assurance Twin provides the **foundation layer** for digital twin initiatives:

- **Layer 1 (Assurance Twin):** Verified asset inventory with process context
- **Layer 2 (Add-on):** Real-time sensor data integration (historian feeds)
- **Layer 3 (Add-on):** Predictive analytics and AI/ML models
- **Layer 4 (Add-on):** 3D visualization and simulation
- **Layer 5 (Add-on):** What-if scenario modeling

Without Layer 1 (verified asset inventory), Layers 2-5 are built on shaky foundations. The Assurance Twin ensures digital twin initiatives start with trustworthy data.

# 7. Market Opportunity and Business Case

## 7.1 Target Market

- **Primary:** Oil & Gas (refineries, pipelines, petrochemicals)
- **Secondary:** Utilities (power generation, transmission, distribution)
- **Tertiary:** Manufacturing (automotive, pharmaceuticals, chemicals)
- **Geographic:** North America (38% market share), Europe, Middle East

## 7.2 Value Proposition

### For CISOs

- Prove security coverage to regulators
- Identify and prioritize security gaps
- Bridge IT/OT knowledge gap
- Audit-ready evidence packs

### For Plant Managers

- Know what assets you have and where
- Identify missing instrumentation
- Assess plant completeness
- Operational decision support

### For Engineering

- Verify design matches reality
- Identify documentation gaps

### For Executives

- Business "what-ifs" (downtime $/hr)
- Compliance risk exposure
- CapEx ROI prioritization

- Update stale engineering records
- Process unit completeness

- Digital twin foundation

### 7.3 ROI Drivers

- **Reduced Security Incidents:** Complete visibility prevents attacks on unknown/unmanaged devices
- **Compliance Cost Avoidance:** Audit-ready evidence reduces regulatory penalties and audit preparation time
- **Operational Efficiency:** Faster asset location, reduced maintenance downtime, better planning
- **Digital Twin Acceleration:** Foundation layer enables faster, more reliable digital twin deployment
- **Tool Consolidation:** Single source of truth reduces need for multiple overlapping tools

## 8. Implementation Roadmap

### 8.1 Current State (Demo)

- Serverless deployment (Vercel)
- In-memory processing (~12K assets)
- No persistence (results lost on refresh)
- No authentication (public demo)
- Manual file upload

### 8.2 Enterprise Roadmap (6-9 months)

#### Phase 1: Auth + Database (6-8 weeks)

- User login & SSO (Azure AD, Okta)

- Role-based access control
- PostgreSQL database (assets, runs, audit logs)
- Save canonization runs with history
- View and compare previous runs

#### Phase 2: Scale & Performance (4-6 weeks)

- Async job queue (Celery/RabbitMQ)
- Chunked processing (1M+ assets)
- Progress tracking (WebSocket updates)
- Streaming CSV processing
- Horizontal scaling

#### Phase 3: Automation (4-6 weeks)

- Scheduled imports (SFTP, API connectors)
- Change detection and alerts
- Time-series analysis
- Automated reporting

#### Phase 4: Enterprise Features (8-12 weeks)

- REST API for integration
- Webhooks and events
- Compliance reports (auto-generate PDFs)
- Chatbot/Q&A interface
- On-premise deployment option

### 8.3 Deployment Options

**SaaS (Deloitte-Hosted):** Multi-tenant cloud service, faster time-to-value, Deloitte manages updates. Best for multiple clients comfortable with cloud.

**On-Premise (Client-Hosted):** Docker/Kubernetes deployment in client environment, full data control, air-gap compatible. Best for highly regulated industries with data sovereignty requirements.

## 9. Conclusion: The Path Forward

The OT asset visibility crisis is real, and traditional tools—while valuable—operate in silos that create blind spots. The **OT Assurance Twin** bridges these gaps by providing context-aware asset management that fuses multiple data sources into one verified, process-aware canon.

This isn't just another asset list—it's an **assurance layer** that answers the hardest question: "*Do we actually have what we think we have, can we prove it to regulators, and where are the gaps?*"

> ### Key Takeaways
>
> - **Market Need:** 50-80% visibility gap creates security, compliance, and operational risks
> - **Unique Solution:** Context-aware asset management vs. traditional list-based approaches
> - **Deloitte Advantage:** Cross-domain expertise, industry knowledge, regulatory experience, trusted advisor position
> - **Enhancement Layer:** Improves OT security tools, CMDBs, and provides foundation for digital twins
> - **Market Opportunity:** Growing digital twin market, increasing regulatory pressure, strong client appetite

Deloitte is uniquely positioned to deliver this solution as a service, combining software capabilities with deep industry expertise and regulatory knowledge. The Assurance Twin doesn't replace existing tools—

it makes them trustworthy by providing the verification and context layer they lack.

**Next Steps:** For organizations ready to address the OT asset visibility gap, Deloitte can deploy the Assurance Twin as a pilot engagement, demonstrating value within 6-8 weeks and scaling to enterprise deployment over 6-9 months.

## 10. References and Further Reading

- Digital Twin Market Report 2025 - Industry Analysis and Growth Trends
- OT Security Market Analysis - Gartner, Forrester Research
- NERC CIP Compliance Requirements - North American Electric Reliability Corporation
- IEC 62443 Industrial Cybersecurity Standards
- Deloitte Industry Insights: OT/IT Convergence in Critical Infrastructure
- Market Research: OT Asset Management Gaps in Oil & Gas Sector

**Deloitte** | Performance Assurance

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business.