



Asset Management: Why IT/OT
Monitoring is Critical to Achieving
ROI in Automation Investments

Matthew Butler

Managing Partner, SCT Advisory

Effective manufacturing and distribution processes require the seamless interoperability of a complex set of assets. Optimal performance depends on a network of underlying functions, including server infrastructure, application logic, integration tools, network bandwidth, edge devices, and an intuitive user experience.

In warehousing, distribution, and industrial operations, process exceptions and IT/OT connectivity challenges can create significant operational costs, which vary depending on facility scale, automation level, and the criticality of affected systems. Common impacts include labor inefficiency, lost throughput and productivity, shipping and fulfillment errors, increased equipment stress and maintenance, and operational risk or compliance fines. Without proper monitoring processes and tools, **these challenges can increase operating costs by 5–15% of facility budgets**, with spikes during peak volumes or in highly automated networks.

However, responsibility for IT/OT monitoring and maintenance is often distributed across manufacturing, distribution, transportation, maintenance, and IT teams, and frequently lacks consistent processes and KPI tracking for incident management, remediation, asset performance, and supplier management.

A best-in-class solution requires:

- a) IT/OT monitoring infrastructure with supporting processes and personnel to detect and resolve disruptions
- b) Centralized incident management with intelligent trend analysis

This white paper outlines the tools and processes that comprise a best-in-class approach to IT/OT monitoring excellence.

A Five-Step Approach to IT/OT Monitoring Excellence

To achieve this vision, a cross-functional team should map the existing architecture, processes, and points of failure. They should begin by developing a current-state inventory of monitoring tools and alerts and a roadmap to improve both localized and systemic monitoring capabilities. Next, they should design the architecture or solutions needed to aggregate outputs into a centralized data ecosystem for correlation and trend analysis. Processes should be established to enable real-time problem capture by end users when system performance or experience is sub-optimal, and this can be supplemented by simulation tools that test the outer boundaries and thresholds of acceptable performance at the point of failure, testing impacts to the overall process to identify causality. Finally, this data should feed a systems intelligence platform capable of incident tracking and correlation-based insights to monitor the frequency and root cause of exceptions, degraded user experience, or impacted system processes – ultimately enabling alert based interventions or agentic AI to address problems before they occur. A breakdown of these steps is as follows:

1. **Leverage Localized Monitoring Capabilities** – Many established tools exist to monitor specific points of failure within the IT/OT ecosystem. Ensuring awareness of alerts is the first critical step, followed by tracking processes to identify trends. Examples include:
 - Server and VMware Monitoring – Observes physical and virtual infrastructure, including CPU, memory, storage, I/O, network throughput, and host cluster health. It detects bottlenecks, stalled processes, or hardware issues to maintain application continuity.
 - Application Performance Monitoring – Tracks response times, throughput, latency, errors, and transaction success while correlating with CPU, memory, and network usage to detect bottlenecks, diagnose issues, and ensure reliability.
 - Integration Monitoring – Monitors data flows and connections between applications, middleware, and OT/IT systems, tracking message delivery, processing errors, latency, and transaction integrity to identify bottlenecks, failures, or misconfigurations.
 - Network Monitoring – Measures bandwidth, latency, packet loss, device availability, and traffic patterns. By comparing metrics to baselines and thresholds, it identifies congestion, misconfigurations, failures, or security risks.
 - IT/OT Device Monitoring – Monitors servers, controllers, sensors, gateways, and automation devices for health, utilization, firmware, configuration, and connectivity, identifying faults or security risks for timely remediation.

- Security and Integrity Monitoring – Ensures systems, devices, applications, and networks are secure and properly configured. By analyzing logs, telemetry, and access activity against baselines and policies, it identifies threats, unauthorized changes, or vulnerabilities for rapid remediation.
2. **Explore Systems-Based Monitoring and Management** – Aggregated tools and standard adapters enhance reliability and adoption of individual components and the overall ecosystem. Examples include:
 - **Automation Integration Platforms** – Connect enterprise systems (WMS/WES/ERP) with robots, AMRs, AS/RS, and other automation technologies using prebuilt connectors, real-time visibility, alerts, troubleshooting tools, and unified orchestration. These platforms accelerate automation deployment, reduce downtime, simplify management, and centralize operational and IT issue escalation.
 - **Computerized Maintenance Management Systems (CMMS)** – Ingest real-time telemetry, alerts, and performance metrics from APM and IoT sensors to assess asset condition, predict failures, and trigger preventive or condition-based maintenance tasks. CMMS prioritizes work orders and schedules resources, enabling a shift from reactive to proactive, data-driven maintenance that reduces downtime, extends asset life, and improves efficiency.
 - **Asset Performance Management (APM)** - Tracks equipment condition, usage, and availability via sensors measuring temperature, vibration, power, and fault codes. It detects anomalies early to prevent downtime and extend asset life.
 3. **Establish Centralized Incident Tracking** – Centralized incident tracking and diagnostic capture leverage ITSM tools via APIs, email, or webhooks to collect data from points of failure that may impact mobility-enabled transactions in WMS or MES. By integrating multiple layers, this capability complements existing monitoring with end-user experience visibility.
 4. **Enable Systems Wide Problem Capture and Diagnostics Simulation** – Recording actual communications and interactions as problems occur captures the complete state across system layers in real time. This approach preserves the exact sequence, timing, and content of events, revealing true causality rather than just symptoms. Once an advanced set of diagnostics have been collected, it is further possible to simulate and explore what if scenarios that test the thresholds of performance and can help to fill in the blanks to identify likely sources of one time and/or recurring problems when the data is not immediately available.

5. **Empower Insights and Agentic AI for Systems Intelligence** – Event-based correlation platforms analyze logs and alerts after problems occur, using timestamps and pattern-matching to infer relationships across the infrastructure. While powerful for identifying system-wide patterns, correlation does not always equal causation and should be combined with real-time problem capture. These insights can be applied to identify the source of problematic issues, and advanced methods can employ alerting to address issues before they manifest, and ultimately, leverage agentic AI to address the problem at the source without any required intervention.

Justifying the Investment and Getting Started

Advanced monitoring, incident tracking, and intelligence platforms provide real-time visibility, predictive insights, and centralized control across complex IT/OT and operational environments. They enable organizations to detect anomalies, prevent downtime, and respond to issues before they escalate. By correlating data from applications, networks, assets, servers, and devices, these platforms improve efficiency, equipment reliability, safety, and compliance. They support data-driven decision-making, optimize maintenance and resource allocation, and increase throughput, ultimately delivering cost savings, operational resilience, and competitive advantage in environments where even brief disruptions can be costly.

Getting started and generating some quick wins to build momentum can be straightforward – here's the three recommended early actions that can set you on a path forward.

1. Establish a cross-functional team that includes engineering, procurement, and operations to embed proactive monitoring and controls into design processes.
2. Set a regular cadence to review issues by frequency, criticality, and restoration complexity, with the goal of addressing root causes and improving monitoring and alerting processes.
3. Develop a technology roadmap to enhance capabilities, with budgets and KPIs to demonstrate progress and value.

Organizations do not have to take this journey alone. SCT Advisory, together with partners in mobile systems intelligence, automation integration, and maintenance software ecosystems, brings expertise and market awareness to design and accelerate the journey. Executive workshops with cross-functional teams are an effective way to identify inefficiencies, quantify potential opportunities, and align leadership around a shared purpose.