1898 & CO®

PART OF BURNS & McDONNELL

WHITE PAPER

Overcoming Challenges in Operational Technology Visibility Implementation: Technical and Organizational Strategies for Industrial Resilience

By Jason Vigh

Across a regional community, neighborhoods suddenly lose power. Traffic lights stall at intersections, businesses close unexpectedly and hospital backup generators activate to protect critical care. Within hours, water pressure begins to drop as pumps at the nearby treatment facility fall offline, leaving operators scrambling to maintain service with limited backup capacity. What begins as an unexplained outage quickly escalates into a multisector emergency.

```
INASSIGN.OPEN("C:\\TROJAN\\ASSIGN.TXT");
INASSIGN >> ASSIGN;
INASSIGN.CLOSE();
INASSIGN.CLEAR();

WHILE(1) {

    REMOVE("C:\\TROJAN\\OPTION.TXT");
    REMOVE("C:\\TROJAN\\TARGET.TXT");

    IFSTREAM INFILE;
    INFILE.CLEAR();
    INFILE.OPEN("C:\\TROJAN\\OPTION.TXT");
    INFILE >> OPTION;
    INFILE.CLOSE();
    INFILE.CLEAR();

    IFSTREAM INTARGET
```

The source of the disruption lies upstream at the regional power utility. In the early morning hours, control room operators noticed breakers opening unexpectedly, remote terminal units (RTUs) dropping offline and alarms flooding the supervisory control and data acquisition (SCADA) system. Initially dismissed as equipment malfunctions, the anomalies soon revealed a coordinated cyber intrusion. Unauthorized commands were traversing the control network, tripping feeders and forcing the utility into emergency response mode.

While this scenario is hypothetical, such threats and attacks are increasingly part of our reality. Attacks against industrial control systems (ICS) are growing in frequency and sophistication, with adversaries leveraging the increased connectivity between information technology (IT) and operational technology (OT) networks to exploit blind spots. What often determines whether such an incident is contained quickly or spirals into a wider crisis is one capability: OT visibility.

OT visibility has become a foundational requirement in ICS environments, driven by two converging trends: the expanded attack surface created by merging IT and OT network environments, and the rise in targeted and opportunistic attacks on critical infrastructure. At its core, OT visibility refers to the continuous ability to identify, monitor and understand all assets, communications and processes within an operational environment. In practical terms, it means maintaining a dynamic and accurate inventory of devices, observing network traffic, and detecting anomalies that may signal either a cyber intrusion or a system malfunction.

OT visibility has become increasingly important to detecting cyber events. Without it, organizations lack the situational awareness needed to identify unauthorized activity, respond effectively to incidents, or validate system behavior against expected baselines. At the same time, visibility serves as a critical enabler of broader cyber risk management, because it provides the asset intelligence required to prioritize vulnerabilities, assess risks and align defenses with operational priorities.

Despite its importance, OT visibility remains challenging to achieve. Legacy devices lacking telemetry, geographically dispersed infrastructures, and technical and organizational divides between IT and OT teams often create persistent blind spots. These challenges are compounded by resource constraints, leading to partial or inconsistent implementations. To overcome these barriers, organizations must adopt a multifaceted approach that integrates technical methods with organizational alignment.

Legacy Systems and Protocol Limitations

Industrial environments often depend on older programmable logic controllers (PLCs), RTUs, distributed control systems (DCS) and SCADA systems. These systems remain essential to operations, but the design reflects an era when cybersecurity and visibility may not have been considered or prioritized. Many of these devices are resource-constrained, lack sufficient onboard logging or telemetry and in some cases run unsupported firmware or operating systems with limited functionality, making them particularly difficult to monitor natively.

At the same time, they continue to communicate using protocols such as Modbus, DNP3 or Process Field Bus (PROFIBUS) — protocols that are still reliable and efficient for real-time control but offer little in the way of built-in security. Their simplicity and determinism make them well-suited for industrial processes where predictability, uptime and safety are paramount; yet from a security viewpoint, however, they create persistent blind spots, making it difficult to natively monitor communications or detect compromises of inherent vulnerabilities.

These qualities present risks that warrant closer examination. For instance, these protocols lack modern safeguards such as authentication, encryption and integrity checking, leaving them vulnerable to misuse when integrated into broader, more interoperable networks where connectivity can expand the attack surface resident in higher-level systems. Because many of the older devices that depend on these protocols also lack native telemetry or logging — and are often too fragile to tolerate active scanning — operators are left with limited options for gaining insight into system communications and behavior.

In the power utility scenario, the limited telemetry from older RTUs prevented operators from quickly distinguishing between a hardware fault and malicious control commands. That delay contributed to the cascading impact on the water utility, illustrating how legacy communication methods can amplify visibility gaps across interconnected systems.

These limitations underscore why visibility strategies must account for legacy systems and insecure protocols. In many environments, passive monitoring and protocol-aware tools are the only feasible means of gaining insight into traffic and behavior without disrupting fragile devices. Today, passive monitoring effectively functions as a compensating control, filling the gap left by protocols that were never designed with security in mind. If these industrial communication standards had incorporated security features, such as authentication and encryption, operators could depend more heavily on secure device telemetry and trusted logs. In the absence of those features, passive network monitoring remains indispensable, providing independent insight into system behavior and enabling anomaly detection in environments where other forms of visibility are not feasible.

Geographic and Operational Complexity

Operational technology environments are rarely confined to a single location. In sectors such as energy, manufacturing and transportation, organizations often manage assets that span multiple facilities or regions. For example, a power utility may oversee dozens or even hundreds of substations distributed across a large service area. Through direct observations, many organizations operate sites that have evolved independently over time due to factors such as incremental technology upgrades, vendor diversity and regional autonomy. This independence has resulted in variations in architecture, local practices and equipment mix — a trend backed by industry assessments and surveys of large OT environments. This variability produces inconsistent data formats, protocol differences and uneven monitoring practices, complicating efforts to achieve standardized visibility.

This geographic dispersion introduces several challenges that must be overcome in monitoring and detection. Remote assets may be difficult or costly to observe directly, particularly when organizations must rely on leased telecom links, over-the-air (OTA) connections or field technicians to access sites with limited connectivity.

Bandwidth constraints can also make it impractical to transmit large volumes of raw telemetry back to a centralized monitoring system for analysis. In addition, inconsistent practices and proprietary vendor solutions can fragment data collection, creating silos that prevent organizations from building a comprehensive view of their operational landscape. Taken together, these factors can slow incident detection and make it harder to coordinate effective response efforts across the enterprise.

In the power utility scenario, operators initially struggled to determine whether anomalous breaker operations were isolated faults or part of a broader pattern. Because the utility's substations were geographically dispersed, the control center had only partial visibility into events occurring at the edge of the network. Without a unified monitoring framework, it was difficult to correlate activity across multiple substations in real time. This delay not only prolonged the disruption to the grid but also left the dependent water utility with little warning before its own operations were impacted.

These challenges highlight why visibility must extend consistently across distributed environments. Without a consolidated view of assets and activity, organizations are significantly hindered in their ability to distinguish localized faults from coordinated cyber events, and they may be unable to anticipate cascading impacts on dependent systems. A visibility framework that unifies monitoring across distributed environments is essential to narrowing these gaps and supporting timely, coordinated response.

Cultural and Organizational Silos

One of the most persistent challenges in OT visibility stems from the technical differences between IT and OT systems. IT environments are built around business applications and enterprise services where downtime often can be tolerated or recovered through backups, redundancy or patching. By contrast, OT systems are tightly integrated with physical processes and must operate with deterministic performance, minimal latency and continuous availability. Because understanding these systems requires distinct knowledge and skills, technical differences often lead to organizational silos that, over time, evolve into broader cultural divides shaping how each group approaches the concepts of monitoring and visibility.

These divides manifest when each group applies its own assumptions and interpretations to visibility initiatives. IT teams may introduce monitoring solutions designed for enterprise networks, often without fully considering the operational risks of scanning fragile devices or introducing latency. OT teams, on the other hand, may prioritize continuity and process stability, sometimes at the expense of collecting security-relevant telemetry. Without a shared framework, these differences lead to misaligned or overlooked requirements, leaving gaps in the overall visibility strategy.

In the power utility scenario, this divide directly contributed to delays in incident recognition. IT analysts monitoring network traffic suspected unusual activity but lacked the operational context to determine whether anomalies represented real threats or normal process behavior. OT operators, meanwhile, hesitated to classify the incident as cyber-related without definitive evidence, since their priority was maintaining safe and stable operations. The absence of a shared visibility framework delayed coordinated action, allowing the disruption to cascade to the dependent water utility.

Overcoming these silos requires more than deploying additional technology — it requires integrated governance and a unified visibility strategy. Organizations that establish cross-functional frameworks, define common goals and align requirements across IT and OT can reduce misalignment and close monitoring gaps. By leveraging nonintrusive monitoring tools and embedding shared objectives into visibility initiatives, enterprises can strengthen trust across disciplines and achieve a more resilient visibility posture across their operational environments.

Scalability and Resource Constraints

Implementing OT visibility solutions across large or complex environments is not simply a technical task — it is a resource-intensive undertaking. Many organizations face budgetary constraints, limited staffing or competing operational priorities that slow the pace of visibility initiatives. Even when tools are deployed, they are often implemented unevenly across facilities due to differences in site budgets, local knowledge or lack of standardized processes. This results in inconsistent coverage and blind spots in the enterprise view. In some cases, organizations achieve initial success through pilot projects but struggle to extend those efforts at scale, leading to fragmented implementations that fail to deliver comprehensive visibility.

Resource limitations also affect how effectively telemetry is used once it is collected. Understaffed security operations centers (SOCs) may be unable to manage the high volume of alerts generated by visibility platforms, leading to alert fatigue and triage challenges. Operational teams may also lack the specialized knowledge needed to interpret network data in the context of physical processes. When these constraints are combined, the result is not just incomplete coverage but also inefficient use of the visibility that does exist, diminishing both its operational and security values.

In the power utility scenario, resource constraints compounded the challenge of detecting and responding to the incident. The utility had deployed visibility tools at only a subset of its substations due to budget limitations. As a result, anomalies were not correlated across the broader network, delaying recognition of the coordinated nature of the event. The lack of trained personnel further slowed analysis, and by the time action was taken the outage had cascaded to the dependent water utility.

Addressing scalability and resource challenges requires a strategic approach that balances priorities with available capacity. Organizations can strengthen their visibility strategy by adopting a risk-based deployment model, prioritizing monitoring of the most critical assets and expanding coverage outward as capacity allows. Scalable platforms — including, where appropriate, hybrid or cloud-based solutions — reduce infrastructure costs while providing room for growth. External partnerships with managed service providers can extend staff capacity and help maintain continuous monitoring, allowing internal teams to focus on core operations. By aligning resources with risk and adopting scalable architectures, organizations can close visibility gaps without overextending their teams or budgets.

Strategies for Enhancing OT Visibility

The challenges of legacy systems, geographic dispersion, organizational silos and resource constraints are significant, but they can be addressed with deliberate planning. Organizations that take a phased and strategic approach to OT visibility can mitigate these barriers and build a stronger foundation for both security and operational resilience.

For environments dependent on legacy assets, visibility is properly advanced through incremental improvements rather than wholesale replacement. Passive monitoring tools are often the most practical way to observe fragile devices without disrupting operations, while protocol converters can normalize proprietary communications into formats compatible with modern visibility platforms. Prioritizing high-value or high-risk devices helps direct scarce resources where they will reduce risk most effectively.

In distributed environments, visibility requires consistent monitoring across sites despite connectivity and bandwidth limitations. Centralized platforms that aggregate data enterprisewide provide the unified view necessary for correlation, while edge-based monitoring components can process data locally and forward only critical telemetry for analysis. Standardized procedures across sites further support alignment between local practices and enterprisewide objectives.

Achieving effective visibility also depends upon bridging IT–OT silos. Because these environments differ in context and knowledge, monitoring solutions must reflect both operational and security requirements. Cross-functional governance frameworks, shared success metrics and nonintrusive monitoring tools help promote visibility initiatives that are embraced rather than resisted. Training programs that expose IT and OT staff to each other's environments can further strengthen the trust required for collaboration.

Finally, visibility efforts must be designed to scale. Risk-based deployment models help prioritize monitoring of the most critical assets and expand coverage outward as capacity allows. Scalable platforms — including, where appropriate, hybrid or cloud-based solutions — reduce infrastructure costs while providing room for growth. External partnerships with managed service providers can extend staff capacity and help maintain continuous monitoring, allowing internal teams to focus on core operations.

Taken together, these strategies provide a road map for overcoming the most persistent barriers to OT visibility. They support the development of a resilient framework capable of balancing security and operational priorities.

Conclusion

The cascading impact of the power utility incident illustrates what is at stake when visibility gaps persist. Localized outages quickly spread to critical services, forcing hospitals onto backup generators and reducing water pressure across the community. What began as anomalous activity inside a control room escalated into a multisector emergency that disrupted daily life and placed public safety at risk.

The underlying causes are familiar. Legacy systems lacked telemetry, distributed infrastructures fragmented monitoring, organizational silos slowed analysis and resource constraints limited coverage. These barriers collectively delayed detection and response, allowing the incident to spread beyond the utility's boundaries.

The strategies outlined provide a framework for mitigating such risks. Incremental improvements for legacy assets, centralized monitoring across distributed environments, cross-functional governance to bridge IT/OT divides and risk-based models for scalability all strengthen the ability to detect and contain incidents. Applied together, these measures could have enabled earlier recognition of anomalous commands, more effective correlation across substations and faster coordination between IT and OT teams, supported by adequate resources. While no strategy eliminates all risk, the combined effect would have substantially reduced both the duration and scope of the outage.

Operational technology visibility is therefore not merely a technical aspiration but a strategic imperative. By addressing the persistent barriers of legacy infrastructure, geographic complexity, organizational divides and resource limitations, organizations can position themselves to contain incidents before they escalate, safeguard dependent sectors and strengthen resilience across critical services.

About 1898 & Co.

1898 & Co. is a global business, technology, and security consultancy serving critical infrastructure industries. We partner with clients to plan, secure and optimize their business. As part of Burns & McDonnell and our 120 years of industry experience, we understand the complexity of your asset-intensive business model, the trends impacting your industry, and the need to ground big ideas in operational realities. Learn more at **1898andCo.com**

9920122205-0925