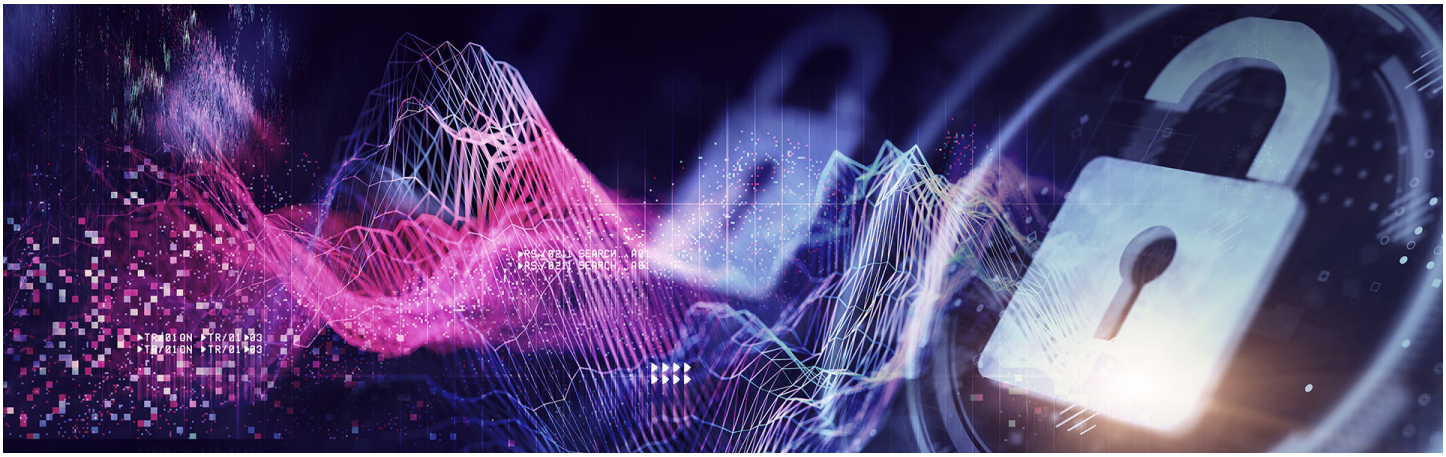
1898 & CO.
PART OF BURNS McDONNELL

WHITE PAPER

Increased Visibility Within OT Environments Can Be Achieved With 5 Core Tools and Technologies

By Jason Vigh

Operational technology (OT) environments are experiencing rapid and comprehensive transformation due to the constantly evolving cyberthreat landscape. Organizations are realizing they must reevaluate how critical systems and operations are secured and managed.



The convergence of operational technology and information technology (IT) systems is making it increasingly difficult for organizations to gain the visibility needed to understand new and more complex layers of risk, and to implement the most effective protection protocols.

Within the OT environment, visibility is defined as the ability to see, understand and monitor the performance of all assets, communications and activities. This includes maintaining a complete and accurate inventory of devices and understanding how they communicate across the network. By tracking system behavior and identifying anomalies or potential threats, organizations are enabled to distinguish between expected behaviors and indicators of risk.

As teams gain these insights, threats may be detected more quickly as system reliability is improved and safety and compliance are strengthened. As OT environments become more connected and complex, visibility becomes a foundational capability for managing cybersecurity risks and maintaining resilient and secure industrial operations. However, gaining these insights in real time requires more than just enhanced awareness. It demands the deployment of purpose-built tools and technologies.

The Role of Visibility

OT visibility in real time plays a critical role in helping organizations monitor the status, performance and security of industrial systems. By gaining actionable insights into asset

inventory, network communications and abnormal system behavior, visibility is enhanced. This empowers teams to:

- Proactively identify and mitigate risks before they escalate.
- Detect and respond to emerging threats in real time.
- Optimize operations to reduce downtime and enhance performance.
- Improve maintenance planning through increased system health monitoring.
- Support compliance efforts by validating security controls and documenting asset data.
- Enable faster, more informed decision-making in dynamic environments.

Visibility is a cornerstone of operational resilience. Without a clear and continuous view of assets and activity, organizations cannot effectively anticipate disruptions, withstand adverse conditions or recover quickly. Visibility allows teams to maintain situational awareness, isolate issues before they spread and adapt to changing threat conditions — all of which are critical for sustaining safe and reliable operations in high-stakes environments.

However, visibility is not a one-size-fits-all solution. OT environments vary widely, often involving legacy systems, proprietary protocols, segmented networks and geographically distributed assets. Selecting the right tools, technologies and integration methods is a critical step toward building the resilient foundation needed to secure and sustain critical infrastructure.

Core Tools and Technologies That Deliver Real-Time OT Visibility

Today's more complex threat environment often requires customized visibility strategies. A combination of tools addressing the unique challenges of OT environments often is required. These are the five core building blocks:

- Passive network monitoring
- Asset management platforms
- Security information and event management (SIEM) systems for OT
- Advanced network visualization tools
- Specialized OT intrusion detection systems (IDS)

1. Passive Network Monitoring

Understanding network traffic and detecting anomalies in a manner that does not disrupt operations requires passive network monitoring tools. Unlike active scanning methods, which can interfere with or destabilize critical systems, passive monitoring solutions safely observe traffic by simply listening to communications across the network. This allows organizations to identify connected assets, detect the protocols in use, and map communication patterns between devices without impacting system performance or availability.

These tools provide real-time visibility into network behavior, enabling the detection of anomalies, suspicious activity or indicators of compromise. They also help establish a baseline of normal operations, making it easier to recognize deviations that may signal cyberthreats or operational issues. Additionally, passive monitoring supports compliance and audit readiness by logging network activity and providing actionable insights without introducing risk. In environments where uptime, safety and reliability are paramount, passive monitoring offers a nonintrusive, effective way to enhance security, reduce blind spots and improve overall situational awareness.

Key capabilities of passive network monitoring tools include:

- **Asset discovery**: Identifies all devices communicating on the network, including undocumented or rogue devices, without actively probing the environment.
- **Protocol identification**: Detects and interprets a wide range of industrial protocols (e.g., Modbus, DNP3, OPC, Ethernet/IP), helping map how devices interact.
- **Network mapping and traffic flow analysis**: Visualizes communication paths, identifies dependencies, and builds a logical map of how systems connect and communicate across zones.
- **Baseline behavior modeling**: Establishes a profile of normal network behavior and system interactions, enabling the detection of deviations or anomalies.
- **Anomaly and threat detection**: Identifies unusual activity, policy violations or indicators of compromise (IOCs), such as unexpected communications, unauthorized devices or protocol misuse.
- **Real-time alerts and notifications**: Provides immediate alerts when anomalies or threats are detected, helping security and operations teams respond quickly.
- **Passive vulnerability identification**: Detects outdated firmware, exposed ports or insecure configurations based on observed traffic — without the risks associated with active scanning.

Water Utility Use Case

A regional water utility operating multiple treatment plants, reservoirs and remote pumping stations was facing a range of cybersecurity risks. With its water distribution network managed via an aging SCADA system, this utility's OT network had grown organically over the years, leaving visibility gaps, undocumented assets and unknown communications pathways. Though the utility was performing its basic mission of maintaining water quality and availability, leadership recognized that without deeper visibility, the utility could not confidently manage cybersecurity risks or maintain compliance with emerging regulatory standards.

Solution

The utility deployed a passive network monitoring solution, purpose-built for OT environments. The tool was installed at strategic locations within the network to observe traffic without disrupting operations, a key requirement for its always-on infrastructure.

Capabilities Deployed and Outcomes Achieved

- **Asset discovery:** The solution identified over 150 OT devices — including undocumented PLCs and HMIs — helping the utility build its first complete asset inventory.
- **Protocol identification and traffic mapping**: By analyzing live traffic, the system revealed use of legacy protocols (e.g., Modbus) and unexpected data flows between zones, enabling the team to strengthen network segmentation.
- **Anomaly detection**: The platform established a behavioral baseline and alerted operators to a misconfigured engineering workstation communicating outside of approved hours.
- **Real-time monitoring and alerts**: Continuous monitoring provided actionable insights without disrupting water operations, improving situational awareness.
- **Compliance support**: The visibility data supported audit preparation, aligned with NIST and AWWA cybersecurity guidelines.

Final Result

Following implementation of its passive network monitoring solution, this utility improved its operational resilience, reduced cyber risk exposure and laid the foundation for a long-term OT cybersecurity strategy — without impacting water delivery or public safety.

- **Integration with security tools**: Feeds data into SIEMs, SOC platforms or other threat detection systems to enhance centralized monitoring and incident response.
- **Compliance and reporting support**: Generates logs, dashboards, and reports to support regulatory compliance (e.g., NERC CIP, NIST, ISA/IEC 62443) and audit readiness.

2. Asset Management Platforms

Serving as a centralized system for identifying, tracking, and managing the life cycle of both physical and digital assets within an organization, asset management platforms are utilized to provide complete visibility into connected devices, a feature that is particularly important in OT environments.

Visibility into PLCs, HMIs, sensors, and control systems and associated software and firmware versions supports risk identification, highlights outdated or vulnerable systems, and boosts proper configuration management. By maintaining an up-to-date asset inventory, the platform also enables organizations to monitor changes, track maintenance history and plan for upgrades or replacements — all features that improve reliability and reduce unplanned downtime.

Many platforms integrate with threat intelligence and vulnerability databases, allowing teams to proactively address risks tied to specific assets. Additionally, asset management platforms support compliance by providing documentation, audit trails and reporting aligned with standards like NERC CIP, NIST or ISA/IEC 62443. In essence, they empower organizations to secure, maintain and optimize critical infrastructure by delivering the visibility and control needed to manage complex, distributed OT environments effectively.

Key capabilities of asset management platforms include:

- **Automated asset discovery**: Identifies and catalogs OT and IT assets across the network — such as PLCs, RTUs, HMIs, sensors, switches, and servers — without manual entry, often using passive monitoring or integrations.
- **Real-time asset inventory management**: Maintains a centralized, continuously updated inventory that includes details like device type, IP address, location, firmware/software versions, vendor and model.
- **Life cycle tracking**: Tracks each asset's life cycle from installation through updates, maintenance and decommissioning, enabling better planning and budgeting.
- **Vulnerability and risk identification**: Maps known vulnerabilities (e.g., CVEs) to specific assets based on firmware versions or configurations and prioritizes them based on risk severity and criticality.

- **Configuration and change monitoring**: Monitors and logs changes to asset configurations, helping detect unauthorized modifications, configuration drift or signs of compromise.
- **Network and communication mapping**: Visualizes how assets interact with each other, showing communication paths, dependencies and potential exposure points.
- **Maintenance scheduling and history**: Supports preventive and corrective maintenance planning by logging maintenance actions and enabling alerts for upcoming service needs.
- **Role-based access and audit logs**: Provides access controls and detailed logging of user interactions with the platform, supporting accountability and compliance.
- **Reporting and compliance support**: Generates reports and audit trails aligned with industry standards (e.g., NERC CIP, ISA/IEC 62443, NIST), supporting both internal reviews and regulatory audits.
- **Integration with other systems**: Connects with SIEMs, CMMS (Computerized Maintenance Management Systems), EDR tools and other platforms for a unified security and asset management ecosystem.

3. Security Information and Event Management (SIEM) Systems

Collecting, correlating and analyzing security-related data across the IT and OT environments is the role of a SIEM system. Centralized visibility into security events, detecting threats in real time and supporting incident response are the primary purposes of a SIEM system. This also helps gain compliance with regulatory standards.

In OT environments like manufacturing, SIEM systems play a crucial role in bridging the gap between cybersecurity and operations by aggregating logs and events from both IT and OT assets. This helps the organization to identify patterns of malicious behavior and generate alerts when something deviates from normal behavior, allowing security teams to act quickly so that damage is limited and system integrity and uptime are maintained.

Key capabilities of SIEM systems include:

- **Centralized log collection and normalization**: Ingests logs from firewalls, endpoints, servers, OT devices and security tools, converting them into a standard format for analysis.
- **Real-time event correlation**: Detects patterns and relationships across events (e.g., multiple failed logins followed by abnormal file access), identifying potential threats or breaches.

Power Utility Use Case

A regional power utility serving over 500,000 customers operates generation, transmission and distribution assets serving several counties. This utility's OT environment provides controls for substations, control centers, relay devices, PLCs and SCADA systems from multiple vendors. Many of the systems have been installed over decades, and with growing concerns around aging infrastructure, cyberthreats and compliance with NERC CIP standards, a centralized, accurate view of all operational assets was needed.

The utility lacked a single source of truth for its OT asset inventory. Many records were manually maintained, out of date or incomplete. Teams had little visibility into firmware versions, device configurations or communication paths. This made it difficult to assess risks, prioritize upgrades, respond to vulnerabilities or prepare for regulatory audits.

Solution

The utility deployed an OT-specific asset management platform for its substations and control networks. Using automated discovery and passive data collection, the platform identified over 2,000 OT assets, including undocumented field devices and outdated firmware. The platform provides detailed asset profiles, real-time updates and visual maps of network communications.

Capabilities Deployed and Outcomes Achieved

- **Automated discovery and inventory**: Hidden assets were revealed and fragmented spreadsheets were replaced with a unified, live inventory.
- **Life cycle and maintenance tracking**: Better scheduling of upgrades and hardware replacements based on asset age and health was achieved.
- **Vulnerability identification**: Known vulnerabilities (e.g., CVEs) to affected devices were mapped, supporting proactive risk mitigation.
- **Change monitoring**: Unauthorized configuration changes were flagged, improving security oversight.
- **Compliance support**: NERC CIP documentation was streamlined, reducing audit preparation time by 40%.

Final Result

Within three months, this power utility had gained full visibility into its OT asset landscape, significantly improving operational efficiency, cyber risk management and regulatory readiness. The platform became a foundational element in the utility's broader cybersecurity and modernization strategy.

Manufacturing Company Use Case

A global manufacturer of automotive components operates a complex network of production lines, robotic systems and PLCs managed via a central SCADA system. With rising cyberthreats targeting manufacturing OT and increasing pressure to meet ISO 27001 and customer security requirements, the company needed greater visibility across both its IT and OT systems.

Security events affecting different departments were siloed, with plant systems logged locally, IT tools reported separately and anomalies unnoticed until operations were disrupted. The manufacturing organization lacked a unified platform to monitor threats, respond to incidents or demonstrate compliance.

Solution

A SIEM platform was implemented to bridge the IT and OT environments. Logs from plant-floor equipment, SCADA systems, firewalls and active directory were ingested into the SIEM, normalized and correlated in real time.

Capabilities Deployed and Outcomes Achieved

- **Log aggregation and normalization**: Unified IT and OT logs were maintained in a centralized view, breaking down visibility silos.
- **Real-time threat detection**: Correlated access anomalies with network activity, in order to detect compromised contractor credentials before reaching critical systems.
- **Dashboards and alerts**: Enabled plant managers and cybersecurity staff to monitor activity through role-based dashboards with live alerts.
- **Forensics and response**: Provided quick analysis of an unexpected shutdown, helping isolate a misconfigured PLC and rule out cyberattacks.
- **Compliance reporting**: Automated evidence generation for ISO 27001 audits, reducing manual reporting by 60%.

Final Result

The SIEM implementation gave the manufacturer real-time insight across its operations, improved incident response time, and strengthened its cyber resilience and audit readiness, positioning it as a more secure and trusted partner in the global supply chain.

- **Alerting and notification**: Automatically triggers alerts based on predefined rules, behavioral baselines or indicators of compromise.
- **Threat detection and analysis**: Identifies anomalies, insider threats, malware behavior and policy violations across IT and OT systems.
- **Dashboards and visualization**: Offers customizable views and visualizations for SOC teams, showing trends, risk levels and critical events.
- **Incident response support:** Helps security teams investigate and respond to incidents through context-rich event timelines and automated workflows.
- **Forensics and audit trails**: Retains historical data to support root-cause analysis, forensic investigations and post-incident reviews.
- **Regulatory compliance reporting**: Automates reporting aligned with frameworks like NIST, ISO 27001, NERC CIP and industry-specific standards.
- **Integration with other tools**: Works with firewalls, intrusion detection/prevention systems (IDS/IPS), endpoint detection and response (EDR), asset management platforms and threat intelligence feeds.

4. Advanced Network Visualization Tools

Real-time graphical views of network infrastructure, device relationships and data flows are among the main functions of advanced network visualization tools. Deep situational awareness spanning both IT and OT environments helps make it easier to understand how systems are interconnected, how they communicate and where potential risks or inefficiencies exist. These tools help identify and map assets, track communication patterns, and visualize changes over time. This helps teams to detect anomalies, enforce segmentation and respond to threats more effectively.

In complex or distributed environments such as logistics, manufacturing or critical infrastructure, network visualization is essential for managing cyber risk, supporting operational continuity and making informed, data-driven decisions about network design, security and performance.

Key capabilities of advanced network visualization tools include:

- **Dynamic network mapping**: Automatically generates real-time visual maps of connected devices, communication flows, and dependencies across IT and OT environments.
- **Topology discovery and monitoring**: Identifies and continuously monitors network structure (i.e., layers, segments, VLANs and zones) detecting changes over time.

Logistics Company Use Case

A national supply chain and transportation company manages a network of distribution centers, smart warehouses and vehicle telematics systems with an IT/OT infrastructure spread across the country. With rapid growth and increasing digitalization, the company faced challenges maintaining visibility in its sprawling, interconnected network.

Among those challenges was the IT team's lack of real-time insight into how devices were connected, where data was flowing and whether new systems were being added securely. OT systems in warehouses that run automated conveyors, barcode scanners, industrial Wi-Fi and other systems were operating in isolated pockets with little oversight. A minor incident in which an unauthorized IoT device gained access to the system was a wakeup call that prompted leadership to prioritize network visibility.

Solution

The logistics company deployed an advanced network visualization tool across its enterprise and operational environments. The platform passively discovered assets, built live visual maps of communication flows, and highlighted network segmentation issues and hidden risks.

Capabilities Deployed and Outcomes Achieved

- **Real-time network mapping**: Revealed more than 500 previously undocumented devices across logistics centers.
- **Traffic flow visualization**: Identified cross-traffic between IT and OT networks, allowing teams to strengthen segmentation.
- **Anomaly alerts**: Flagged a warehouse IoT sensor communicating with an external IP, leading to rapid containment and policy updates.
- **Drill-down views**: Enabled SOC analysts to investigate incidents faster by tracing exact communication paths and device behaviors.
- **Change tracking**: Helped IT track network changes during new facility rollouts, ensuring standardized configurations.

Final Result

The logistics company gained a complete, continuously updated view of its complex infrastructure. Blind spots were reduced, incident response capabilities were improved and more secure integration of new technologies was achieved as it scaled, enhancing the security and resilience of supply chain operations.

- **Protocol awareness and traffic flow analysis**: Displays how systems communicate, highlighting protocols in use and bandwidth usage for both normal and abnormal traffic.
- **Anomaly detection**: Highlights unusual connections, unauthorized communication paths or unexpected asset behavior in real time.
- **Risk and vulnerability mapping**: Visually identifies high-risk nodes, outdated devices or insecure communication paths, aiding in proactive remediation.
- **Drill-down views**: Allows users to click into devices or connections for detailed metadata, event logs and historical behavior.
- **Segmentation validation**: Confirms whether network zones (e.g., OT vs. IT) are properly segmented or if unintended cross-traffic exists.
- **Integration with security tools**: Feeds enriched network context into SIEMs, firewalls and monitoring tools to enhance incident response and threat hunting.
- **Change tracking and history playback**: Records network state over time, allowing teams to review topology changes, trace incidents or investigate past events.

5. Specialized OT Intrusion Detection Systems (IDS)

Unlike traditional IT-focused security tools, specialized IDS are designed to understand the unique protocols, devices and real-time requirements of industrial environments like those commonly in place within water treatment plants, waste management facilities and chemical processing systems. These systems are designed to monitor, detect and in some cases actively block malicious activity with OT networks without disrupting critical industrial processes.

Providing deep visibility into network behavior and device communication patterns is the core IDS purpose, enabling it to detect unauthorized actions or threats like malware, lateral movement or policy violations. This capability allows operators to be alerted before damage occurs.

Some advanced solutions include prevention capabilities such as blocking specific traffic or isolating compromised devices so that essential operations may continue uninterrupted. These systems play a critical role in protecting safety, availability and compliance in environments where uptime is essential, and even minor disruptions can have significant environmental, regulatory or public health consequences.

Environmental Services Company Use Case

A company specializing in wastewater treatment, landfill management and industrial recycling operates a wide array of OT systems, ranging from PLCs controlling pumps and chemical dosing to sensors monitoring environmental compliance metrics. As cyberthreats targeting environmental infrastructure increased and regulatory oversight intensified, this company identified the need for more proactive and intelligent detection capabilities across its operational networks.

Because existing security controls focused primarily on IT systems, the OT environment lacked visibility and was vulnerable to unauthorized access, misconfigurations and insider threats. In one instance, a contractor mistakenly uploaded incorrect logic to a field device, causing a system alarm and near-violation of environmental discharge limits.

Solution

A specialized intrusion detection and prevention system (IDPS) for OT environments was deployed across critical facilities. It was deployed in passive mode for detection, with prevention features enabled in high-risk zones (e.g., chemical dosing systems). The platform immediately began monitoring traffic, analyzing protocol-level data and establishing behavioral baselines.

Capabilities Deployed and Outcomes Achieved

- **Protocol-aware detection**: Identified unsafe command sequences in Modbus traffic that previously had been undetected.
- **Anomaly alerts**: Flagged an unusual communication between a contractor laptop and a field device outside of approved hours.
- **Asset mapping**: Revealed previously undocumented devices and communication paths in legacy SCADA systems.
- **Event correlation and SIEM integration**: Enabled faster incident response by pushing enriched alerts to EcoSecure's central SIEM.
- **Policy enforcement**: Configured prevention rules to block unauthorized write commands to key PLCs in critical zones.

Final Result

This environmental services organization improved its detection capabilities, reduced the risk of operational disruption and environmental noncompliance, and met emerging cybersecurity mandates. The OT IDPS became a cornerstone of the company's industrial cybersecurity program, protecting both the environment and the integrity of essential services.

Key capabilities of IDS include:

- **Protocol-aware threat detection**: Understands and analyzes OT-specific protocols (e.g., Modbus, DNP3, BACnet, OPC) to detect suspicious or malformed commands.
- **Passive monitoring**: Observes traffic without introducing latency or interfering with sensitive industrial control systems.
- **Anomaly detection and behavioral analysis**: Builds baselines of normal operations and alerts when deviations occur (e.g., a PLC receiving commands outside normal hours).
- **Signature-based detection**: Identifies known threats using threat intelligence feeds and predefined rule sets customized for OT.
- **Active prevention (optional)**: Blocks unauthorized or harmful traffic, isolates compromised devices or enforces segmentation policies, when configured for inline use.
- **Real-time alerting and event correlation**: Sends alerts to SOC teams or integrates with SIEM platforms to enhance visibility and enable faster response.
- Asset and communication mapping: Identifies devices and visualizes their communications to aid in network understanding and threat hunting.
- Integration with OT security ecosystem: Connects with firewalls, SIEMs, asset management platforms and visualization tools to support layered defense strategies.
- Regulatory compliance support: Helps meet requirements in frameworks like NIST 800-82, ISA/IEC 62443 and other regulatory mandates.

Integrating Tools for Comprehensive OT Visibility

Deploying visibility tools individually is only part of the solution. Integrating these technologies and tools into a unified and cohesive ecosystem achieves true, real-time OT visibility that supports both security and operational objectives. Integrating data from passive monitoring tools, asset management platforms, SIEMs, intrusion detection systems and network visualization tools provide the complete picture that operators need. Key outcomes include:

- **Unified dashboards**: Aggregating data from multiple sources into a single, intuitive interface for streamlined monitoring, faster analysis and more effective decision-making.
- **Cross-team collaboration**: Bridging the gap between IT, OT and cybersecurity teams to align priorities, share context and support visibility efforts.

- **Scalability and flexibility**: Choosing solutions that can adapt to evolving operational demands, such as the integration of IIoT devices, cloud-based platforms and remote operations.

Industrial environments are evolving rapidly, due to IT/OT convergence, increased digitalization and the growing adoption of connected technologies. Comprehensive, real-time OT visibility has become essential. Visibility is foundational to maintaining cybersecurity, operational resilience and long-term efficiency.

Tools such as passive network monitoring, asset management platforms, SIEMs, OT intrusion detection systems, and advanced network visualization each offer critical insights, and integrating them into a unified ecosystem is the final step to enabling effective decision-making and proactive threat management. By partnering with cybersecurity specialists like 1898 & Co., organizations gain the resources needed to design and implement visibility strategies tailored to their unique operational landscapes.

About 1898 & Co.

1898 & Co. is a business, technology and cybersecurity consulting firm serving the industries that keep our world in motion. As part of Burns & McDonnell, our consultants leverage global experience in critical infrastructure assets to innovate practical solutions grounded in your operational realities. For more information, visit **1898andCo.com**.

8836898663-0525