uptime INTELLIGENCE

INTELLIGENCE UPDATE

Real-time telemetry requires modern, flexible cybersecurity

John O'Brien 11 Jun 2026

Telemetry: Part 2

Many operators use air gaps or air gap principles, to separate operational technology (OT) networks from IT and ensure critical facility controls remain on protected out-of-band networks.

However, the air gap is often crossed, so that OT and IT systems can share data for reporting or management and maintenance purposes. This may be performed via connecting systems and exchanging data via removable media/USB devices, software APIs, and virtual private network web portals. Uptime Intelligence continues to discuss the security implications of these practices (see **Related reports** at end of report).

The exchange of live IT-OT telemetry data is less common (either internally or externally) because it requires greater trust in the security and integrity of the connected systems and data. For decades, the default approach has been to either restrict IT-OT data exchange or, where possible, lock down connectivity to reduce risk.

This de facto position is, however, no longer justifiable for many operators, who are under pressure to use their live operational data to identify availability and capacity constraints, particularly in relation to power, space and cooling, to accommodate rising IT densities and more complex AI infrastructure and facility systems.

To achieve continuous data exchange across networks, security needs to be a top priority, but it should not impede operational uptime or risk exposure of mechanical and electrical control systems, such as supervisory control and data acquisition (SCADA), programmable logic controllers (PLCs) and building management system (BMS).

In Part 1 of this series, Uptime Intelligence showed how telemetry data exchange (the collection and exchange of data used and produced by the IT and facility OT equipment) is already complicated by the proliferation of different OT and IT messaging protocols (see *IT-OT telemetry failings are hindering real-time applications*). In this report, we consider the security concerns and challenges posed by IT-OT telemetry, alongside emerging applications and potential solutions.

Airgap limitations

Operators face a fundamental security challenge: how to permit live telemetry data to exchange between IT and OT systems, while maintaining airgap integrity.

Genuine, physical airgaps are rare outside a high-security setting, such as military or defense environments. Nonetheless, the principle of physically or logically separating IT and OT networks remains accepted best practice to protect critical control systems.

Airgaps have become less enforced because of the growing need to share "static data" from system registers, databases and files, such as data relating to power consumption, asset records, and their performance and maintenance (see **Table 1**). Established multi-factor authentication, verification, user access privileges and network firewalls may provide adequate security when maintained and updated appropriately.

Real-time telemetry adds further complexity, however, since exchanging IT-OT data every minute or second, versus once a week or once a quarter, requires network ports and communication channels to remain open and connected. This presents orders of magnitude more data for exchange and processing by real-time applications such as those for live system monitoring.

Real-time applications depend on the continuous availability of quality, high volume telemetry data. Unnecessary security restrictions, system compatibility and interoperability issues will therefore also restrict their efficacy and ability to scale across multiple systems and environments (see *IT-OT telemetry failings are hindering real-time applications*).

Table 1 Static data versus real-time data examples and applications

Data types	Data examples	Data sources and applications
Static and historical data Collected, stored, updated, and retrieved occasionally. Manageable risk due to restricted data exposure.	**Operations management** Asset records, registers, configuration files, setpoint settings, MOPs, SOPs.	Operation and control software: DCIM, CMMS, BMS, SCADA, etc.
	Ad-hoc requests Read-write files, downloads, management, and regulatory reports.	Productivity and analytics tools: Microsoft CSV files, Excel, PDF, etc.
	System administration Updates, user account IDs, passwords, security keys.	System firmware, security patches, authentication and verification systems.
Real-time telemetry data Live continuous data streams and event feeds. Elevated risk due to open data and networks. May use cloud for elastic scaling and response.	**Operational performance** Temperatures, air and water pressure, fluid flows, velocity, humidity.	IT and OT equipment sensors and telemetry (e.g., servers, UPS, CDUs, PDUs/iPDUs).
	Physical security Motion detection, video imaging, audio temperature and biometric data.	IoT device sensors and telemetry (e.g., from mobile PDAs, CCTV, biometric scanners, drones, robots).
	ITOM observability System logs, events, API responses, latency, transactions, failed requests, IT and network availability.	IT service management, security information and event management, IT-OT cybersecurity monitoring, FinOps, digital sustainability (GreenOps).

BMS, building management system; CCTV, closed-curcuit television; CDU, cooling distribution unit; CMMS, computerized maintenance management system; CSV, comma separated values; DCIM, data center infrastructure management; MOP, method of procedure; PDA, personal digital assistant; PDU, power distribution unit; SCADA, supervisory control and data acquisition; SOP, standard operating procedure; UPS, uninterruptible power supply.

UPTIME INSTITUTE 2026

uptime INTELLIGENCE

Additional security risks

IT and OT systems already face common security vulnerabilities that target weak system and user access controls, and insecure web portals and remote access (see *DCIM vulnerabilities increase threat of cyberattacks).*

There are additional risks specifically related to real-time telemetry, which further increase the security risks and potential for compromise:

- **Open system access.** Live OT monitoring and control systems typically require communication protocols and ports to remain open. Connected OT systems that exchange data with IT can become vulnerable to inbound compromises if messaging is not encrypted and ports, VPNs and firewalls are not managed effectively. Even then, novel or zero-day cyberattacks may render these monitoring and control systems ineffective.
- **Protocol interoperability issues.** Different IT and OT protocols may be incompatible or unsupported by different vendor systems and some legacy protocols may not be adequately secure. Exchange attempts can lead to data corruption and security vulnerabilities (see *IT-OT telemetry failings are hindering real-time applications*).
- **Configuration issues**. These can pose additional risks, particularly within TCP/IP networks and systems that are widely used to support on-site and remote management

and physical security/access control (see *IT-OT security: rising critical vulnerabilities, widespread risks*).

- **IoT device connectivity.** IoT devices, such as CCTV, scanners and sensors typically use wireless and mobile networks. Surveillance cameras are often situated externally and connected to internal networks. Many ship with default login credentials; some may have inadequate encryption or use insecure messaging protocols.
- **API connectivity.** IT and OT software rely increasingly on APIs to exchange information across IP networks. APIs offer a fast and reliable method for real-time data exchange, and most are read-only to prevent tampering. However, read-only permissions do not prevent compromises that can occur before, during or after data exchange. Similarly to other software products, APIs require effective authentication, verification and encryption.

Potential solutions

Uptime Intelligence has commented on the need for rigorous enforcement of user identification and verification, access privileges, and ensuring routine implementation of system updates and security patches.

Additional security layers may be required for real-time IT-OT telemetry exchange, to ensure that monitoring functions are monitored effectively and controls remain securely isolated on the protected network.

These solutions should be capable of operating without impacting critical operations and control systems. "Zero-impact security" is an emerging field focused on the ability to instantly isolate compromised areas without disrupting operations. The two examples below attempt to minimize the impact on operations, while addressing specific issues identified in this report:

Protecting air gap integrity

Unidirectional gateways. These include data diodes and hardware-enforced appliances, which can enforce one-way data traffic across the air gap, for example, from OT to IT only. Data diodes operate by enabling data exchange through separate send and receive channels, hardware and circuitry, providing physical separation of inbound and outbound traffic. These gateways maintain secure segmentation between IT and OT networks and can protect air-gap integrity as part of a defense-in-depth security strategy.

Hardware solutions, such as those from Owl Cyber Defense and Waterfall Security, provide a physical barrier between IT and OT, while software platforms, such as Modius OpenData, preserve air-gap principles via a one-way, normalized telemetry path into the IT layer.

A global colocation operator, for example, is exploring the use of data diodes and data center infrastructure management (DCIM) to connect its global network of facilities and securely identify available power and cooling capacity in real time. The operator hopes to gain visibility across the network, then dynamically move and orchestrate GPU workloads accordingly.

Proactive network monitoring

External attack surface management (EASM). EASM is an emerging area of cybersecurity that combines threat intelligence and response capabilities to address external threats targeting internet-facing applications, including IP domains, APIs, cloud services and network endpoints. EASM continuously scans, acting as an attacker, to trigger alerts within a centralized platform, and may help identify issues, such as weak segmentation between IT and OT/facilities systems. Examples include Microsoft Defender EASM, Palo Alto Networks Cortex Xpanse, and Falcon Surface (CrowdStrike).

Security incident and event management (SIEM). SIEM is an adjacent capability, which is often used by security operations teams to monitor hybrid and distributed network environments. SIEM is used to log events and anomalies and to support deep analysis of incidents and threats for remediation. Examples include Splunk (Cisco), SentinelOne, WIZ (Google), Datadog and Dynatrace.

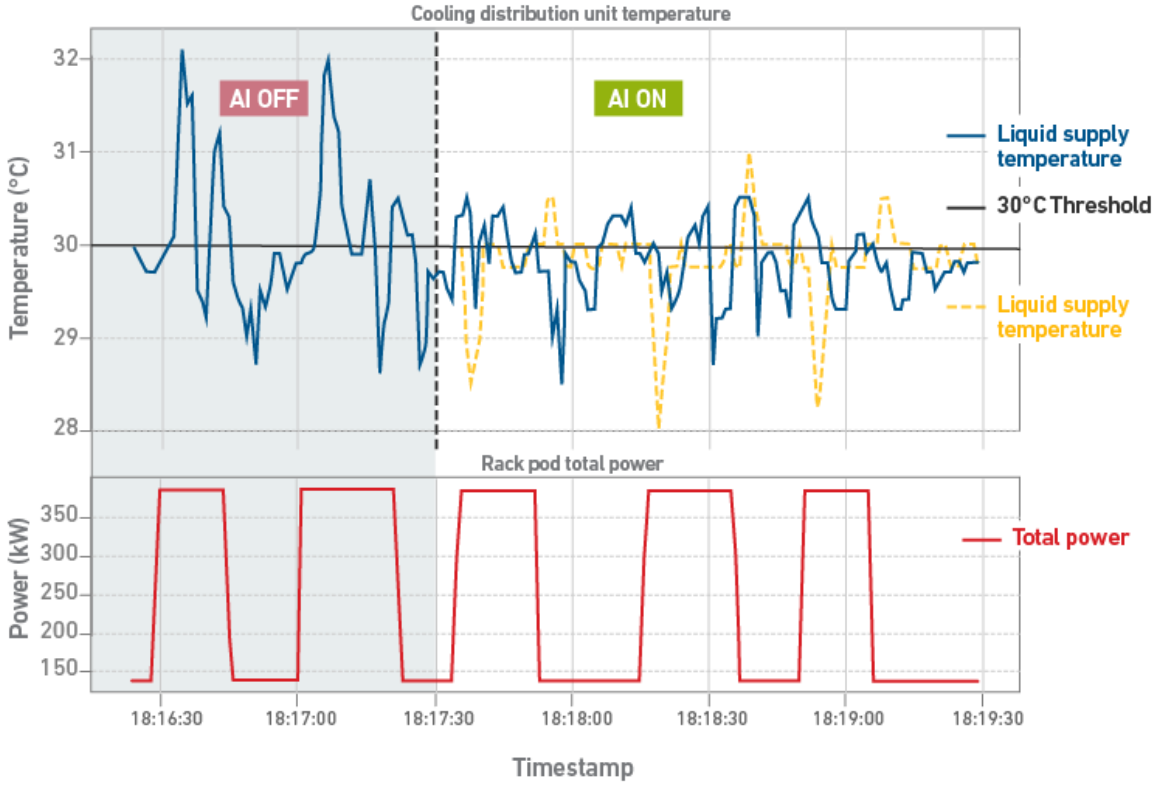
Risks in emerging applications

Emerging applications are increasingly demonstrating strong potential for adapting and optimizing AI infrastructure. As pilots move into production, they likely point in the direction of travel for many operators. However, the security complications of real-time IT-OT convergence, with AI agents and AI-assisted controls, are not yet receiving adequate attention.

In March 2026, a successful AI infrastructure optimization pilot between Phaidra, CoreWeave, Nvidia, and Applied Digital reported an impressive 75-80% reduction in GPU thermal spikes, across Nvidia GB200 clusters (see **Figure 1**).

Since GPU workloads experience unpredictable power swings, thermal spikes can occur if temperatures exceed the thermal limit (T-Limit). Phaidra's system works by proactively directing cooling to the GPUs ahead of time, avoiding GPU throttling, damage and wasted power.

Figure 1 Cooling distribution unit temperatures using AI and non-AI control



SOURCE: PHAIDRA

uptime INTELLIGENCE

In **Figure 1**, the liquid supply temperature (blue line) shows the thermal spikes reducing when AI control is on. The liquid supply temperature (yellow line) shows the new AI control setpoints. The total power (red line) represents the continuous power swings of the GPU workloads.

Outages or downtime of the AI system is managed by a fail-over to the default cooling distribution unit (CDU) control. However, there are specific security issues to consider:

- **Continuous bi-directional connectivity** is likely required between the power ports on the GPU racks and the CDU proportional-integral-derivative (PID) controller to ensure near real-time response: under 10 seconds, compared to 3-5 minutes under direct CDU control.
- **AI agents perform control functions** by applying optimized setpoint changes to the CDU. This makes it likely that agents connect to the CDU via OT protocols on the IP network. Operators will need to be reassured that OT protocols are securely managed and isolated from protected networks.
- **The use of the cloud.** Although data is sent one-way and is read-only, many operators will be cautious about the risks posed by APIs if they are not properly managed or secured. Meanwhile, there are plans to introduce electric power management system (EPMS) and BMS connections in the future.

The Uptime Intelligence View

For most operators, maintaining the status quo, where IT and OT data is locked up in separate network environments, is becoming increasingly difficult to justify. Given the advances in real-time telemetry and AI applications, operators are fast approaching an inflection point. However, while emerging applications show promise, they still require

more security focus.

It is likely that most operators will remain opposed to the convergence of telemetry data and skeptical of AI-based controls, certainly until security and interoperability concerns are resolved. But those prepared to explore options for security telemetry and protecting air gap integrity, at this early stage are likely to be better positioned to adapt.

Other related reports published by Uptime Institute include:
IT-OT telemetry failings are hindering real-time applications
Supply chain exploits: the blind spots operators need to address
OT security: rising critical vulnerabilities, widespread risks
DCIM vulnerabilities increase threat of cyberattacks
Seven fallacies of data center cybersecurity
OT protection: is air-gapping the answer?

ABOUT THE AUTHOR

John O'Brien

11 Jun 2026

John is Uptime Institute's Senior Research Analyst for Cloud and Software Automation. As a technology industry analyst for over two decades, John has been analyzing the impact of cloud migration, modernization and optimization for the past decade. John covers hybrid and multi-cloud infrastructure, sustainability, and emerging AIOps, DataOps and FinOps practices.

jobrien@uptimeinstitute.com

About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. With over 4,000 awards issued in over 122 countries around the globe, and over 1,100 currently active projects in 80+ countries, Uptime has helped tens of thousands of companies optimize critical IT assets while managing costs, resources, and efficiency. For over 30 years, the company has established industry-leading benchmarks for data center performance, resilience, sustainability, and efficiency, which provide customers assurance that their digital infrastructure can perform across a wide array of operating conditions at a level consistent with their individual business needs. Uptime's Tier Standard is the IT industry's most trusted and adopted global standard for the design, construction, and operation of data centers.

Offerings include the organization's Tier Standard and Certifications, Management & Operations reviews and assessments including SCIRA-FSI financial sector risk assessment, the Sustainability Assessment, and a broad range of additional risk management, performance, availability, and related offerings. Uptime Education training programs have been successfully completed by over 100,000 data center professionals, such as the much-valued ATD (Accredited Tier Designer) and AOS (Accredited Operations Specialist). The Uptime Education curriculum has been expanded by the acquisition of CNet Training Ltd. In 2023.

Uptime Institute is headquartered in New York, NY, with offices in London, Sao Paulo, Dubai, Riyadh, and Singapore, and full-time Uptime professionals based in over thirty-four countries around the world.

For more information, visit www.uptimeinstitute.com