

THIRD PARTY INTEGRATION, TELEMETRY & APIs

Version 1.0

October 2025

Author (s) : Scott Sharp: Google, Masa Kaneko: Microsoft, Mark (Heyang) Chen: Oracle, Pardeep Shahi: NVIDIA, Saket Karajgikar: NVIDIA, Dennis James: Microsoft

Revision History

Version	Date	Comments
0.1	Jan 10, 2…	Draft
0.9	Sept. 26,2025	Final Draft
1.0	Sept. 29, 2025	Submitted Final Document

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Definitions

Telemetry: A process that automatically collects, transmits, and analyzes data from remote sources

List of Abbreviations

API - Application Programming Interface

CE - Critical Environment

BMS - Building Management System

EWT - Entering Water Temperature

ICS - Industrial Control System

LWT - Leaving Water Temperature

MUW - Make Up Water

OT - Operational Technology

PCWR - Process Cooling Water Return

PCWS - Process Cooling Water Supply

PMS - Power Monitoring System

PDU - Power Distribution Unit

PUE - Power Usage Effectiveness

RAT - Return Air Temperature

SAT - Supply Air Temperature

TCS - Technical Cooling Loop

WUE - Water Utilization Efficiency

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Table of Contents

Revision History **2**
Definitions **3**
List of Abbreviations **3**
Table of Contents **4**
Table of Figures **5**
1. Introduction **6**
2. Data Center Telemetry **7**
Data Center Incident Reporting / Response 7
Power Usage Efficiency (PUE) 8
Data Center Workloads & Transient Response 8
Emissions Reporting 8
3. Connected Systems End-to-End (Security Boundaries) **8**
Common Components of Telemetry Systems 8
Common Components 8
Secure Boundaries 9
4. Common Interfaces **11**
Common Protocols 11
Requirements 11
Push/Pull methods 12
5. Hierarchy of Critical and Operational Technology Devices **12**
Base Building Telemetry 12
Data Hall Telemetry 13
Mechanical 13
Electrical (Power Monitoring) Devices 16
6. Secure Data Transmission: Bridging Trust Boundaries **20**
Architectural Solutions for Zero Trust Data Exchange 20
7. Conclusion and Call to Action **21**
Call to Action: Defining the Telemetry Standard 21
8. Bibliography **23**
9. Appendix A: Standard API functions **24**
10. Common Point List / Naming Convention **25**
11. License **26**

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Table of Figures

Figure 1: Five Levels of Industrial Control Systems (ICS) (Alei et al., 2021) 10
Figure 2: Example of Power Monitoring hierarchy 18

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

1. Introduction

The data center industry faces a pivotal challenge: reconciling explosive growth with aggressive mandates for efficiency and sustainability. The ability to maximize the performance of every watt consumed has become an economic and environmental necessity. This shift requires moving beyond traditional infrastructure management to a reliance on granular, real-time data—a capability known as telemetry.

Telemetry, the automated collection and analysis of metrics spanning power, thermal, and mechanical systems, is the key to unlocking the next generation of data center operation. For operators, it provides the essential visibility required for proactive fault detection, optimizing cooling infrastructure to achieve optimal Power Usage Effectiveness (PUE) and Water Usage Effectiveness (WUE), and ensuring regulatory compliance. For customers, telemetry empowers them to profile specific IT workloads, rebalance loads, and make data-driven decisions that dramatically improve performance per watt.

However, the pursuit of these benefits introduces a critical conflict: the demand for real-time data exchange must cross the most sensitive boundaries in the facility. Data from the operator's Operational Technology (OT) systems—the Building Management System (BMS) and Power Monitoring Systems (PMS)—must be securely shared with the tenant's Enterprise Technology networks. This paper asserts that the current, fragmented methods for data transmission are insufficient to support the security and speed required for features like coordinated load shedding, real-time incident response, and end-to-end PUE optimization.

This paper will first detail the critical functions and components of modern data center OT systems, utilizing the Purdue Model to establish a baseline understanding of control system hierarchy. It will then analyze the vital telemetry points required for both base building and data hall operations (power, cooling, and security). Finally, we will propose that achieving high efficiency and resilience at scale requires the industry to adopt a Zero Trust framework and a standardized protocol for secure data exchange, transforming the current security vulnerability at the IT/OT boundary into a fundamental, reliable, and secure operational capability.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

2. Data Center Telemetry

Telemetry, in the context of data centers, refers to the automated collection and analysis of real-time data from various systems and devices within the facility. This data encompasses a broad spectrum, including power consumption, temperature, humidity, and the operational status of critical equipment. Telemetry solutions provide data center operators with a comprehensive and dynamic view of their infrastructure. This visibility is essential for optimizing performance, pinpointing inefficiencies, preemptively identifying potential faults, and driving data-backed decision-making processes within the data center.

In addition to operational benefits, customers can also analyze this data to identify energy-wasting hotspots, rebalance loads across the data center, and ultimately reduce their power bills while lowering their environmental impact. For example with telemetry, customers have the ability to profile the power and resource consumption patterns of specific workloads. This visibility allows them to optimize their applications and hardware deployments for maximum efficiency. Detailed power usage information can also help in deciding whether to consolidate lightly-used servers, retire older inefficient equipment, or shift workloads to take advantage of off-peak power rates. By pinpointing power-hungry processes, customers can make data-driven decisions that improve performance per watt. These are just a few examples of what sharing data center telemetry can achieve.

Data center power usage is expected to double by 2026, as reported by the International Energy Agency (IEA) (Gooding, 2024). Increased energy efficiency and maintaining optimal Power Usage Effectiveness PUE is imperative for the data center industry. Telemetry data on temperature, humidity, and airflow can help operators fine-tune the data center's cooling infrastructure. This leads to reduced energy waste from over-cooling, while still ensuring equipment operates within safe tolerances. Reporting power usage efficiencies, in addition to other important metrics, is becoming a requirement in many locations across the world. To enable the industry to improve we must have better data to support operational changes, and improvements to the way we operate.

Data Center Incident Reporting / Response

- Real time alerting for customers
- Ability to coordinate power usage, or cooling usage, during an event to prevent a complete building outage (combined tenant load shedding and coordination)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Power Usage Efficiency (PUE)

- EU Code of Conduct Reporting Requirements - Link
- Increase power utilization in a data hall
- WUE Reporting
- iMasons Climate Accord - Link
- PUE optimization across tenants

Data Center Workloads & Transient Response

- Workload profile to assess load stability across tenants, the building, and the campus
- Maintain cold aisle temperature and humidity for optimal server performance

Emissions Reporting

Generator emission tracking is very important to environmental agencies across the world. In Europe certain regulators are requiring PUE and WUE reporting from customers within multi-tenant facilities. Tracking generator runtime, fuel use, and emissions is likely to become a required reporting metric as well.

3. Connected Systems End-to-End (Security Boundaries)

Common Components of Telemetry Systems

As discussed in the prior sections, data center telemetry can no longer be treated as a local resource. With the ever increasing demand for telemetry data to be provided to end customers, there needs to be a baseline architecture that defines a secure pathway for data center telemetry data to be sent or collected between operators and customers. This section will go through what a “typical” data center controls architecture would consist of for the purposes of providing a baseline understanding of a data center’s controls system. Once the baseline has been established, this section will move onto how communications is primarily handled between customers and the data center’s telemetry system.

Common Components

When talking about control components within a datacenter, it’s often a good idea to refer to the Purdue Model. The Purdue model conveniently breaks down components of an industrial control system into several levels and acts as a great way to categorize control system components and describe the methods in which they interact.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

The figure below showcases the 5 levels of an ICS defined by the Purdue model along with common networks that are involved between each layer.

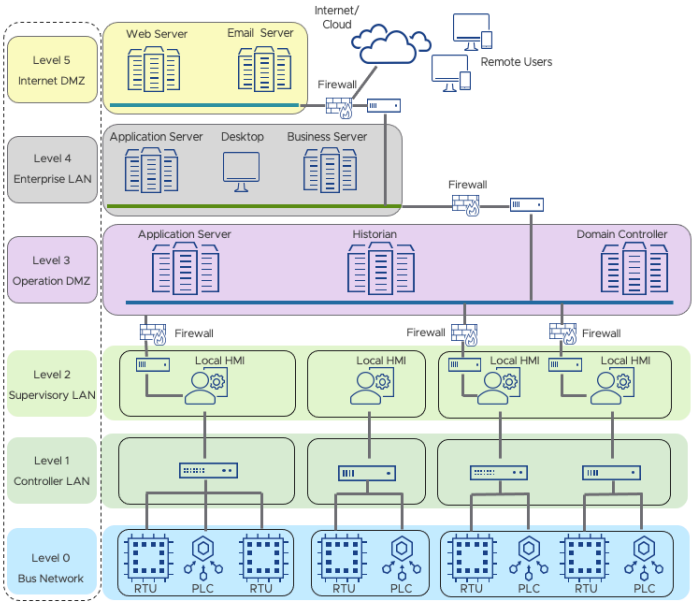


Figure 1: Five Levels of Industrial Control Systems (ICS) (Alei et al., 2021)

Secure Boundaries

The Purdue model makes discussing secure boundaries much easier, each layer of the model is usually connected to a network layer that exists within between the layers. The traditional Purdue model has been updated with a Level 3.5 that calls out for a DMZ to serve as a separation between the Enterprise (IT) layer and the OT layers below. The table below details the networks called out by the figure above along with some notes on securing these networks.

Network Type	Description	Comments
Local Isolated Networks	Networks that typically exist in level 0 are primarily IO networks. A common example would be a DLR network	These networks are configured to be isolated from the building facilities networks. Backplane access ports should be disabled to ensure no network bridging is allowed. Network

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

	that's used to connect several remote IO stations to a supervisory rack.	monitoring and control is often done by the PLC architecture itself.
Building Facilities Networks	The building facilities network connects all the layer 1 devices and allows the layer 2 supervisory control systems to function.	Network segmentation should be used to control device access to needed access only. 802.1X should be utilized to authenticate and verify devices on the network. Segmentation of devices that utilize open protocols such as Modbus or BACNet. Extra caution to be used for open protocol support. (network monitoring, blocking write packets from unknown sources, etc)
Site Level Networks	The network connects multiple buildings together allowing for layer 3 functionality.	At this layer no network access into the building layer 1/2 devices should be necessary. Centralization of network traffic into dedicated front ends or remote data services. Network connections should be limited to layer 2 devices that utilize device authentication and encryption.
DMZ	This layer acts as the boundary between IT and OT systems. Security systems such as firewalls and network monitors are necessary in this layer.	
Enterprise Networks	This network is the broader IT system.	Services that need to cross into this boundary should be well defined and controlled.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

		Common services that are passed from this network include SMTP, Identity services, Remote Data services (MQTT).

4. Common Interfaces

Common protocols generally accepted for securely collecting data are discussed in this section. Note that no matter which protocol is utilized, encryption and authentication will be required.

It is best to avoid the use of proprietary APIs. Proprietary APIs create increased complexity and result in extended integration requirements for the end customer. Upkeep of collection systems are necessary in the event the API is updated.

Common Protocols

MQTT - Message Queuing Telemetry Transport: A lightweight, publish-subscribe network protocol that transports messages between devices. It is ideal for connecting remote devices with a small code footprint and minimal network bandwidth.

RESTful API - Representational State Transfer: A software architectural style that defines a set of rules for building web services. It uses standard HTTP methods (like GET, POST, PUT, DELETE) to interact with resources identified by URIs (Uniform Resource Identifiers). Communication is typically stateless and often uses JSON as the data format.

Redfish: An open industry standard for secure and scalable data center hardware management. Maintained by the Distributed Management Task Force (DMTF), Redfish® is a RESTful API that uses JSON payloads and OData to provide a modern, human-readable interface for managing servers, storage, networking, and other converged infrastructure. It is designed to be the successor to older, less secure protocols like IPMI. By standardizing the API for hardware telemetry and control, Redfish simplifies automation and integration, aligning with the goal of using common, non-proprietary interfaces.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Requirements

- **TLS** - Transport Layer Security, is a cryptographic protocol that provides a secure communication channel between two applications, typically a client and a server, over a network. It ensures data confidentiality and integrity by encrypting the data transmitted and verifying the identity of the communicating parties.

- **mTLS -** Mutual Transport Layer Security (mTLS) is a security method that extends standard TLS by adding mutual authentication. This means both the client and server verify each other's identities using digital certificates, ensuring that only trusted parties can communicate securely. It's essentially "regular TLS" with the extra stipulation that the client is also authenticated.

Push/Pull methods

Datacenter telemetry data is collected through two main communication architectures.

- **Pull** - This is commonly known as Polling. The client will initiate the information requests to the COLO server for telemetry data. The COLO will then process the request and send the appropriate response back to the client.
- **Push -** The Push architecture involves the COLO servers sending updates to the client without the need to be requested.
- **Pub/Sub -** This subset of push architecture is commonly used and the backbone of the MQTT protocol. In this scheme the COLO will set up data collection up to a data broker. The data is then configured into topics for subscription. Clients will subscribe to topics configured on the COLO server and any updates to that topic will be published to the client.

5. Hierarchy of Critical and Operational Technology Devices

Understanding the details of data center components is crucial for effective management. Modern data centers are complex systems where electrical and mechanical components must work together. Capturing the technical specifics of each device helps us understand their contributions. This includes how electricity flows from utility power to servers and racks, and how HVAC and chillers maintain optimal conditions. Traditionally, these devices were managed separately, but now they require a coordinated approach. For example, the Coolant Distribution

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Unit for GPU cooling needs careful orchestration. It's essential to accurately capture the hierarchy of critical environment and operating technology devices to ensure all systems function seamlessly.

Base Building Telemetry

Points included in base building telemetry are those that could provide services to multiple tenants, or span across multiple data halls. In a third party environment, the central plant can be shared across multiple tenants as an example. Base building telemetry is generally all shared infrastructure above the tenants secure boundary. Third party data centers could segregate across data halls, or buildings. Below are a few types of services that would be lumped into the base building category.

- Utility / Substation Information
    - Incoming Voltage, amperage, power consumption, load power factor, etc.
- Backup Power Generation
    - Generator Status, Alternator Winding Voltages, Amperage, Frequency, Total Power, Fuel Fuel Level, Run-hours, etc.
        - Note: When isolated lineups are providing critical power for dedicated tenants, the generator information would only be provided to the tenants being served.
- Central Utility Plant Operation
    - PCWS/PCWR Temperatures, Pump Speeds, MUW Storage Level, WUE, Chillers Status, Chillers Available

Data Hall Telemetry

Within third party data centers, generally the data halls are the secure boundary dedicated to any particular customer. Telemetry from equipment or services serving the data hall is specific to that tenant or data hall. For example, the busway in the data hall would be dedicated to that tenant.

- Power Measurement Information for the following (Voltage, Amperage, Frequency, Power)
    - Dedicated UPS system(s), PDUs, Busway, Static Switches, RPPs, etc.
- Cooling Measurement Information
    - CRAH/CRAH Unit RAT, SAT, Fan Speed, EWT, LWT
    - Data Hall Temp / Humidity / Cold Aisle / Hot Aisle Differential Pressure
- Liquid Cooling/Technology Cooling System

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

    - CDU status, Technical Cooling Loop Supply Temp (TCS) , Technical Cooling Loop Return Temp (TCR), CDU ΔP, Rack ΔP, CDU flow rates, PCWS Valve Position, CDU Commanded Pump Speed, CDU Pump Speed Feedback
    - Rack information (supply/return temperatures, flow rates, etc.)
    - Secondary Loop differential pressure, temperatures, flow rates
    - Secondary Loop liquid quality
    - Leak Detection
- Data Hall Security Devices
    - Badge Readers, camera systems, motion sensors, etc.

Mechanical

Mechanical infrastructure devices are critical systems responsible for maintaining the correct **environmental conditions**—primarily **temperature, humidity, and airflow** —required for the reliable and efficient operation of IT equipment. They form a distributed network, each component contributing to the overall thermal management and often reporting vital health and performance data to a central Data Center Infrastructure Management (DCIM) platform.

- **Central Chilled Water Plant:**
    - **Description:** For future data centers, having liquid cooled interfaces is critical. For each data center, generally there will be a central chiller plant, or similar. The main central utility building is where the main mechanical plant exists. Whether using cooling towers and water cooled chillers or air cooled chillers, there will be a central plant supporting the facility.
    - **Function:** Provides the main source of cooling for the data center, or data center campus. Mechanical equipment used to remove heat from the building is housed here.
    - **Monitoring Role:**
        - **Overall Facility Load:** Monitoring total chillers online, total capacity being cooled by the central plant.
        - **Operational State:** Monitoring number of active chillers, current pump speed, chilled water supply / return temperatures. This is monitoring the main ‘heartbeat’ of the cooling systems.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

- **Fluid Temperature:** Monitors chilled water supply/return temperatures to ensure efficient heat transfer and proper cooling capacity.
- **Pump Status & Pressure:** Tracks pump speed and differential pressure to detect leaks, or component wear, ensuring adequate flow.
- **Condenser Efficiency:** Monitors the temperature difference across the cooling tower/dry cooler to ensure optimal heat rejection, often tied to outdoor wet-bulb temperature.
- **Water Quality & Usage:** Tracks Water Usage Effectiveness (WUE) and monitors water quality to prevent scale buildup in pipes and cooling towers.

    - **Peak Demand Management:** Monitoring and data logging information from the mechanical plant helps forecast when additional capacity needs to be added to the central plant. As more IT load is deployed it is important to trend this data.
    - **Mechanical Plant Efficiency:** By monitoring and trending data from the central plant, it can be overlaid with power consumption information to determine the best operating practices to reduce PUE for the building.

- **Computer Room Air Conditioners/Handlers:**
    - **Description:** Large indoor units that receive chilled water (CRAH) or use a direct refrigeration cycle (CRAC) to cool the air inside the data hall.
    - **Function:** Conditions the air (cooling, dehumidifying, or humidifying) and manages air circulation into the cold aisles.
    - **Environmental Monitoring Role:**
        - **Airflow Capacity:** Monitors fan speed and static pressure to ensure the correct volume of air is delivered to the IT equipment.
        - **Supply/Return Air Temperature:** Tracks the thermal efficiency of the unit and confirms that the cold aisle setpoint is being met.
        - **Component Health:** Monitors compressor run hours (CRAC), coil temperatures, and filter status for maintenance scheduling.
- **Thermal Containment (Hot/Cold Aisle)**
    - **Description:** Physical structures (walls, doors, blanking panels, strip curtains) used to separate hot exhaust air from cold intake air.
    - **Function:** Maximizes the efficiency of cooling units by ensuring only hot return air enters the CRAC/CRAH and only cold supply air enters the rack inlets.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

    - **Environmental Monitoring Role:**
        - **Differential Pressure:** Monitors the pressure difference between the hot and cold aisles to confirm containment integrity and prevent air mixing (recirculation/bypass).
        - **Air Leak Detection:** Checks for sudden drops in ΔP\Delta P or spikes in rack inlet temperatures that would indicate a containment breach (e.g., an open door or missing panel).
- **Rack and Area Sensors**
    - **Description:** Distributed sensors placed strategically throughout the white space and inside the racks.
    - **Function:** Provide granular, localized readings of the environment exactly where the IT equipment is operating.
    - **Environmental Monitoring Role:**
        - **Inlet Temperature/Humidity:** Monitors the air entering the servers to ensure compliance with ASHRAE and/or customer requirements.
        - **Hotspot Detection:** Identifies localized thermal anomalies or failing equipment (e.g., a server with a failing internal fan).
        - **Water/Leak Detection:** Sensors placed under piping, raised floors, and cooling units to provide early warnings of liquid intrusion.

How monitoring mechanical and environmental parameters plays a role :

Monitoring mechanical and environmental parameters is fundamental to data center reliability, efficiency, and safety. Here's how it integrates intelligence into the mechanical infrastructure:

- **Proactive Fault Prediction:** Continuous monitoring of component health (e.g., pump vibration, compressor pressure) allows for predictive maintenance, shifting from reactive repairs to scheduled, non-critical interventions, thereby minimizing the risk of a catastrophic cooling failure.
- **Energy Efficiency Optimization:** Granular temperature and airflow data enables precise tuning of cooling setpoints and fan speeds. By minimizing overcooling or reducing fan RPM based on actual thermal load, organizations can dramatically improve their PUE (Power Usage Effectiveness).
- **Airflow Management Intelligence:** Monitoring pressure differentials and return air temperatures confirms the success of hot/cold aisle containment. This intelligence ensures that all cooled air is delivered to the IT equipment inlets, eliminating wasted energy from bypass air.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

- **Regulatory Compliance & Reporting:** Environmental monitoring provides auditable proof that the data center has consistently maintained conditions within safety and manufacturer-specified ranges, which is essential for compliance and Service Level Agreements (SLA).
- **Root Cause Analysis:** In the event of an outage or thermal alarm, detailed logs from all sensor points allow operators to quickly pinpoint the failure's root cause—whether it was a component failure, a containment breach, or an environmental event.

Electrical (Power Monitoring) Devices

Electrical devices are essential components that distribute, control, and convert electrical power throughout a system, from the utility power entrance down to individual pieces of equipment like servers (*How Power Distribution Systems Work?*, 2024). They form a hierarchy, each level managing power for the subsequent ones and often providing critical monitoring capabilities.

Here's an example of a power device hierarchy and how power monitoring plays a crucial role within it:

Power Device Hierarchy Example:

2. **Utility Power / Main Switchgear:**
    - **Description:** This is where the power enters the facility from the utility grid. Incoming utility power typically steps down at a utility-provided transformer, then enters the building's main switchgear.
    - **Function:** Provides primary protection for the entire facility and distributes power to downstream distribution switchgear.
    - **Power Monitoring Role:**
        - **Overall Facility Load:** Monitors total power consumption of the entire building.
        - **Power Quality:** Detects issues like voltage sags, swells, harmonics, and frequency deviations that could impact downstream equipment.
        - **Peak Demand Management:** Helps identify periods of high power usage, allowing for strategies to reduce demand charges.
        - **Utility Billing Verification:** Confirms the accuracy of utility bills by comparing them to actual consumption data.
3. **Uninterruptible Power Supplies (UPS):**

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

- **Description:** Typically a double conversation power system that conditions utility power and provides backup power for a specified duration during an outage.
- **Function:** Ensures continuous operation of critical equipment by bridging power gaps and smoothing out power anomalies.
- **Power Monitoring Role:**
  - **Battery Status & Health:** Monitors battery charge levels, remaining runtime, and overall battery health to predict potential failures.
  - **Input/Output Voltage & Current:** Tracks power flowing into and out of the UPS, indicating load levels and potential overload conditions.
  - **Bypass Status:** Indicates if the UPS is operating on battery, utility power, or bypass, helping to diagnose issues.
  - **Efficiency:** Measures the efficiency of the UPS itself, identifying potential energy waste.

4. **Power Distribution Units (PDUs) / Remote Power Panels (RPPs):**
   - **Description:** These devices distribute power from the UPS (or directly from the main switchgear in some cases) to various racks and equipment within a specific area of the facility. They often have multiple circuits and outlets.
   - **Function:** Further distributes and protects power to groups of equipment, often providing individual circuit breakers for each branch.
   - **Power Monitoring Role:**
     - **Rack-Level Load:** Monitors the power consumption of individual racks or rows of equipment.
     - **Circuit Load Balancing:** Helps identify imbalances across different circuits, preventing overloads.
     - **Capacity Planning:** Provides data on available power capacity within specific areas, aiding in future equipment deployment.
     - **Environmental Monitoring (often integrated):** Some PDUs can monitor temperature and humidity within the rack.

How Power Monitoring Plays a Role:

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Power monitoring is not just about seeing numbers; it's about gaining **visibility, control, and intelligence** over the entire power infrastructure. Here's how it plays a critical role at every level of the hierarchy:

- **Proactive Issue Detection:** By continuously monitoring voltage, current, power factor, and other parameters, abnormalities can be detected before they lead to outages or equipment damage (e.g., an overloaded circuit, a failing UPS battery).
- **Capacity Management & Optimization:** Accurate power monitoring data allows facility managers to understand exactly how much power is being consumed and how much capacity is available at each level. This prevents over-provisioning (wasting resources) and under-provisioning (risking outages).
- **Energy Efficiency & Cost Reduction:** Identifying inefficient equipment, optimizing load balancing, and understanding peak demand patterns allows organizations to implement strategies to reduce energy consumption and lower operational costs.
- **Troubleshooting & Root Cause Analysis:** When an issue occurs, detailed power monitoring data provides invaluable insights into the sequence of events, helping to quickly identify the root cause and minimize downtime.
- **Compliance & Reporting:** Many industries have regulations regarding power usage and reliability. Power monitoring provides the data necessary for compliance reporting.
- **Chargeback/Showback:** In multi-tenant environments or large organizations, granular power monitoring data at the rPDU level enables accurate allocation of power costs to specific departments or clients.
- **Predictive Maintenance:** Analyzing trends in power consumption, voltage fluctuations, or battery degradation can help predict potential equipment failures, allowing for scheduled maintenance before a critical issue arises.

In essence, power monitoring acts as the "nervous system" of the electrical infrastructure, providing the critical data needed to ensure reliability, efficiency, and optimal performance of all connected devices.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

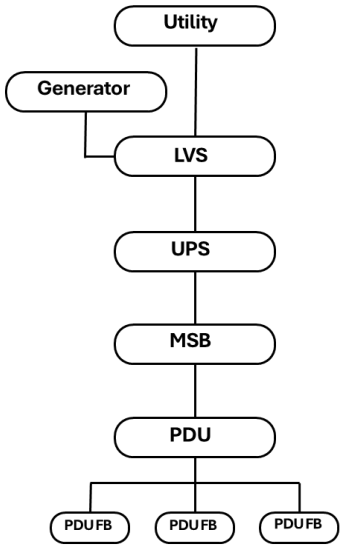


Figure 2: Example of Power Monitoring hierarchy

6. Secure Data Transmission: Bridging Trust Boundaries

Both the landlord and the tenant have networks that require a high level of security. Many times, each party has many networks, each serving specific purposes (e.g., corporate, IT workload, OT controls). Data transmission between any two networks, especially across the trust boundary separating the data center operator's infrastructure controls (BMS) and the tenant's IT workload network, inherently creates vulnerabilities for both.

The industry would benefit from the development of a standard for securely transmitting operational data between these two secure networks in a Zero Trust environment. Under the Zero Trust principle of "never trust, always verify," the goal is to eliminate any implicit trust granted simply by a connection being established.

There are likely a few architectural solutions to secure this transmission, but they must also match the required reporting frequencies to allow for real-time adjustments of IT workloads (by the tenant) and mechanical plant parameters (by the operator).

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

1. **Data Diode Technology (Unidirectional Gateways):** This solution offers the highest level of security by physically enforcing one-way data flow. The BMS data is allowed to flow out to the tenant's network, but no communication is permitted to flow back in. This ensures that even if the tenant's network is compromised, the attacker cannot manipulate the underlying critical infrastructure control systems. While ideal for security, data diodes complicate bi-directional communication necessary for adaptive, real-time control logic, often limiting the exchange to basic, read-only monitoring metrics.

2. **Message Broker and API Gateways:** A more flexible approach involves using a secure, intermediating service (often a message broker like Kafka or an API gateway) placed within a highly scrutinized Demilitarized Zone (DMZ) or a secured enclave. This method requires both the BMS and the tenant's network to only communicate with the broker, never directly with each other. This adheres to Zero Trust by:

    - **Micro-segmentation:** Isolating the BMS and IT networks from direct contact.
    - **Explicit Verification:** Requiring explicit authentication and authorization (via tokens and certificates) for every single data request or data push between the endpoints and the broker.
3. **Application-Layer Protocol Encapsulation:** Utilizing modern application-layer protocols such as MQTT or secured RESTful APIs ensures data is encrypted and validated at the application layer, not just the transport layer. This allows for granular control over what data is exchanged (e.g., only temperature and PUE values) and who can access it, aligning with the principle of least-privilege access.

Dedicated physical pathways (network cabling) between the two security zones do not, on their own, provide a solution, as they merely establish a connection point that opens up both networks to security threats if not governed by strict, application-layer security controls. The final, universally adopted solution is yet to be determined, but it will undoubtedly revolve around a high-speed, authenticated, and highly segmented data exchange that eliminates implicit trust between the operator's control systems and the tenant's compute environment.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

7. Conclusion and Call to Action

The evidence is clear: data center telemetry is no longer a luxury for operational reporting—it is the critical nexus of reliability, efficiency, and environmental compliance for the entire industry. As IT load demands continue to grow, it's imperative to move beyond siloed operations. The deep-dive into mechanical and electrical infrastructure monitoring, combined with the necessity for real-time coordination (e.g., combined tenant load shedding) and regulatory compliance (e.g., PUE and WUE reporting), demonstrates that granular data exchange between data center operators and their customers is essential for achieving the next step-change in efficiency.

However, a fundamental challenge remains: securely bridging the trust boundary between the operator's control networks (BMS/PMS) and the tenant's IT networks. Our analysis shows that while architectural solutions like Data Diodes, Message Brokers, and mTLS-secured APIs offer pathways for secure data exchange under a Zero Trust model, a universally accepted and easily implemented framework does not yet exist. The current lack of a standardized approach creates friction, increases integration costs, and introduces bespoke security risks every time a tenant or operator attempts to share mission-critical data.

Call to Action: Defining the Telemetry Standard

To unlock the full potential of data center telemetry—from global PUE optimization to coordinated incident response—the industry must collectively address this challenge. We call upon all stakeholders—data center operators, cloud providers, technology vendors, and industry consortiums (such as iMasons and ASHRAE) — to engage immediately in developing a formal specification for Zero Trust Telemetry Data Exchange.

This industry-wide effort must focus on three objectives:

1. **Standardizing a Secure Architecture:** Define a common architecture (e.g., using a secured DMZ message broker) and a mandated security protocol (mTLS over MQTT or REST) that guarantees data integrity and non-repudiation while strictly enforcing the Zero Trust principle of least-privilege access.
2. **Defining Data Schemas and Frequencies:** Establish standardized data schemas for core telemetry points (like PUE, WUE, circuit current, and cold aisle temperature) and define minimum reporting frequencies required for real-time operational coordination.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

3. **Ensuring Auditability and Compliance:** Integrate requirements for continuous monitoring and logging of data exchange to facilitate quick root cause analysis and streamline global compliance reporting mandates.

The time for siloed network boundaries is over. By collaborating to create a unified telemetry specification, the data center industry can transform a significant security challenge into an unprecedented opportunity for operational efficiency, power conservation, and collective resilience.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

8. Bibliography

Alei, S., Altamirano, C., & Mazzini, D. (2021, August 24). *4 Ways to Boost OT Security - VMware Professional Services*. VMware Blogs. Retrieved June 20, 2025, from https://blogs.vmware.com/professional-services/2021/08/4-ways-to-boost-ot-security.html

Gooding, M. (2024, January 26). *Global Data Center electricity use to double by 2026 - IEA Report*. All Content RSS. Retrieved December 04, 2024, from https://www.datacenterdynamics.com/en/news/global-data-center-electricity-use-to-double-by-2026-report/

How Power Distribution Systems Work? (2024, September 10). Shanghai Yingtong Electric Co., Ltd. Retrieved June 20, 2025, from https://www.ytelect.com/blog/how-power-distribution-systems-work_b250

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

9. Appendix A: Standard API functions

Create Request

Initialize a service request.

Add Case Note to Existing Request

2-way communication between the tenant and landlord to aid in any special handling of the request.

Retrieve Case Note from Existing Request

2-way communication between the tenant and landlord to aid in visibility of the request.

Attach Files to a Request

Attach a file such as an access request form.

Retrieve Files Attached by Landlord

Retrieve forms or other documentation from the landlord.

Query Request Status

The status of a service request, including the access approval status for the requested locations. This query can be combined with the case note retrieval.

Close Request

Close (or request to close) a case to signal that the request has been fulfilled or the tenant access team doesn't need further actions related to this case from the landlord.

Revoke Access

Revoke previously granted access.

Get Access Reports

Revoke previously granted access.

Get Request Updates

Retrieve status updates of an existing request.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

10. Common Point List / Naming Convention (Example)

This points list is an example of future work to be completed when a common specification is published. The intent is to have a common points list, naming convention, sampling rate, and other requirements clearly documented for use by all.

Category	Name	Area	Units	Telemetry Reporting Frequency
Power	UPS (TYP)	Electrical Plant	Frequency (hz)	
Power	UPS (TYP)	Electrical Plant	Low Voltage (V)	
Power	UPS (TYP)	Electrical Plant	Amperage (A)	
Power	UPS (TYP)	Electrical Plant	Power (KVA)	
Power	UPS (TYP)	Electrical Plant	Power Factor (PF)	
Power	PDU (TYP)	Data Hall	Frequency (hz)	
Power	PDU (TYP)	Data Hall	Low Voltage (V)	
Power	PDU (TYP)	Data Hall	Amperage (A)	
Power	PDU (TYP)	Data Hall	Power (KVA)	
Power	PDU (TYP)	Data Hall	Power Factor (PF)	
Power	Busway (TYP)	Data Hall	Frequency (hz)	
Power	Busway (TYP)	Data Hall	Low Voltage (V)	
Power	Busway (TYP)	Data Hall	Amperage (A)	
Power	Busway (TYP)	Data Hall	Power (KVA)	
Power	Busway (TYP)	Data Hall	Power Factor (PF)	

11. License

Creative Commons

OCP encourages participants to share their proposals, specifications and designs with the community. This is to promote openness and encourage continuous and open feedback. It is important to remember that by providing feedback for any such documents, whether in written or verbal form, that the contributor or the contributor's



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

organization grants OCP and its members irrevocable right to use this feedback for any purpose without any further obligation.

It is acknowledged that any such documentation and any ancillary materials that are provided to OCP in connection with this document, including without limitation any white papers, articles, photographs, studies, diagrams, contact information (together, “Materials”) are made available under the Creative Commons Attribution-ShareAlike 4.0 International License found here: https://creativecommons.org/licenses/by-sa/4.0/, or any later version, and without limiting the foregoing, OCP may make the Materials available under such terms. As a contributor to this document, all members represent that they have the authority to grant the rights and licenses herein. They further represent and warrant that the Materials do not and will not violate the copyrights or misappropriate the trade secret rights of any third party, including without limitation rights in intellectual property. The contributor(s) also represent that, to the extent the Materials include materials protected by copyright or trade secret rights that are owned or created by any third-party, they have obtained permission for its use consistent with the foregoing. They will provide OCP evidence of such permission upon OCP’s request. This document and any "Materials" are published on the respective project's wiki page and are open to the public in accordance with OCP's Bylaws and IP Policy. This can be found at http://www.opencompute.org/participate/legal-documents/. If you have any questions please contact OCP.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.