IT Critical Infrastructure Management Solution Brief

Six steps to using the IoT to manage IT critical infrastructure

The Internet of Things (IoT), sometimes called the Industrial Internet, generates huge amounts of data, known as “Big Data,” allowing us to measure, manage and understand the physical environment like never before.

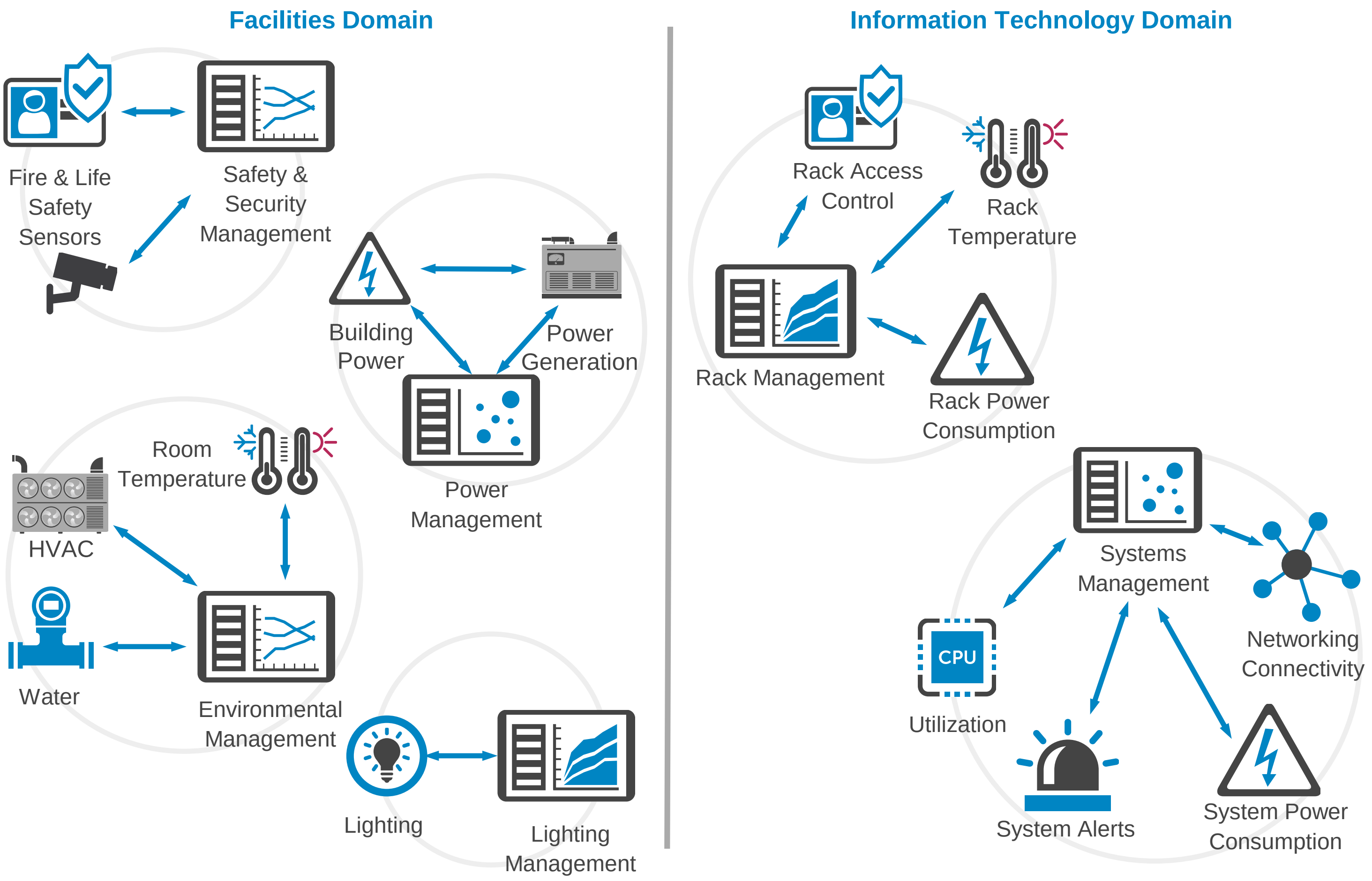
Successfully acquiring, aggregating and analyzing all this data and reducing it to actionable intelligence to make better decisions and make these decisions more quickly can help businesses create more efficient operational processes, optimize energy consumption and reduce costs.

Whether located in the central data center, a remote office or branch office, a cellular base station, a data center container, or isolated remote IT equipment in rugged environments, the increasing numbers of sensors, instruments, and other intelligent devices continue to expand the scope of data sources and analytics required to run a modern IT facility.

IT critical infrastructure equipment also spans both facilities and information technology domains, with different systems, organizations, success metrics, and cultures further complicating deployments.

Critical infrastructure consists of assets found in both facilities and information technology domains

In today’s environment you often find systems in these two domains running independently, limiting integration and insights.



Key trends in IT Critical Infrastructure Management:

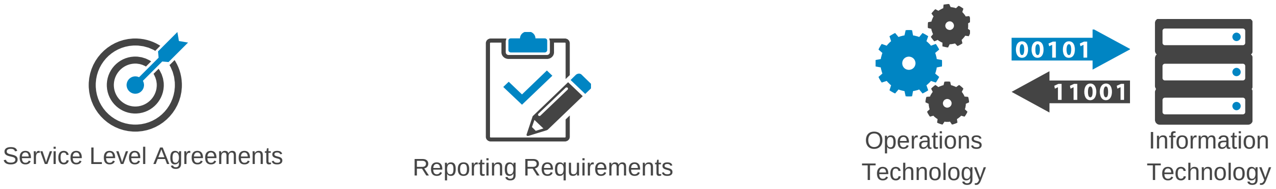
- **Powerful analytics tools provide true, actionable insights** – Make important decisions quickly with real-time analytics
- **Data is integrated from diverse sources** – Organizations are beginning to integrate operational technology data from the physical environment with information technology data from within the data center, correlating events
- **Regulatory requirements will increase** – Maintaining compliance with energy efficiency, security and other regulations will drive new reporting and analytics requirements

Follow these 6 best practice steps to plan your IT Critical Infrastructure implementation

1 | Establish the goals

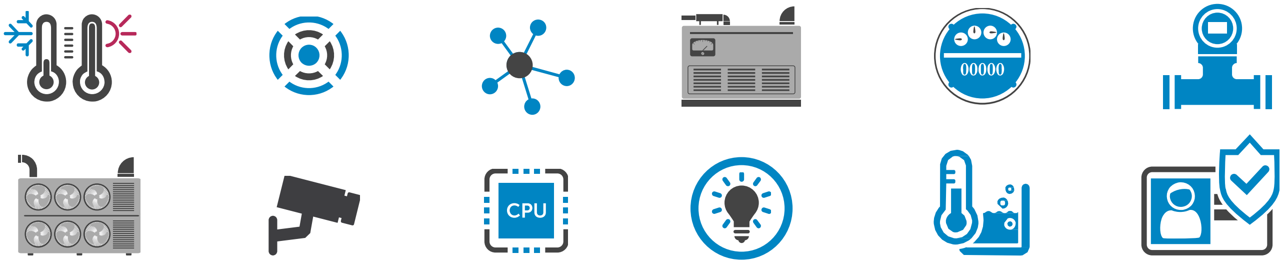
Implementing or expanding an IT critical infrastructure management system will help improve the reliability and availability of the variety of devices and sensors used to maintain the operation of the physical environment, whether they be in remote locations or the central facility. It’s important to understand the key metrics required by the organization to maintain essential business operations and any external reporting requirements. Consider the following questions to identify key goals of your IT critical infrastructure project:

- Determine the uptime and reliability service level agreements that must be met.
- Identify all external reporting and compliance requirements.
- Include plans for temporary loss of connectivity to your sensors or analytics devices depending on their type and location.
- Establish the integration points for data originating from the IT and OT (facilities) departments.
- Identify the owner of actions needed to mitigate issues identified.



2 | Identify the data sources critical to infrastructure management

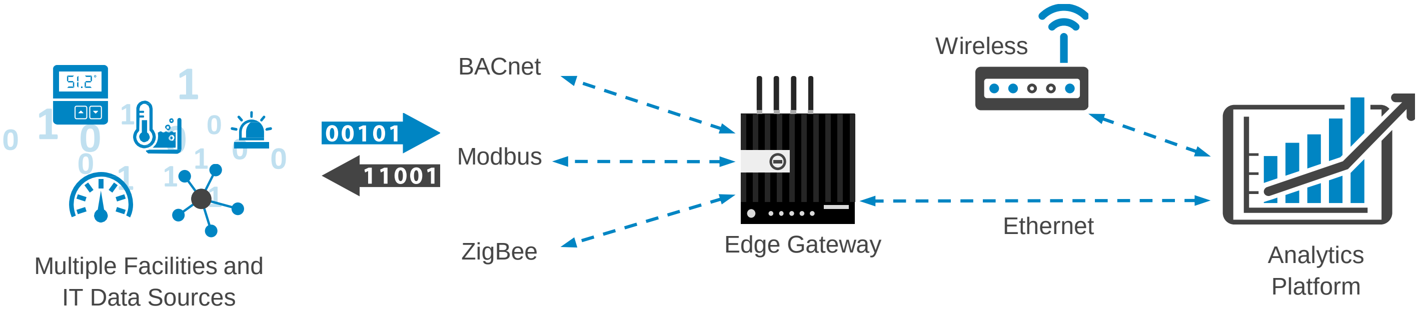
As the price of sensors continues to drop, the number of sensors will proliferate across an ever-expanding number and types of facilities and IT equipment creating substantial amounts of real-time data. Some assets where you should consider gathering data include IT equipment such as power distribution units (PDUs), network switches, and server racks, and facilities equipment such as generators, HVAC equipment (chillers, air handlers, VAV, fan coil units, etc.), access control units, CCTV, fire and life safety, lighting, and more. After determining the critical equipment in your environment you might need to consider additional instrumentation to get the data you require. It is also critical to identify other existing data sources from business systems such as any data center resource monitoring, scheduling, maintenance or other IT management systems and integrate them into the overall solution.



3 | Determine connectivity needs

Different types of IT facilities equipment use different methods to send sensor data to a collection point. Varying connectivity technologies are used, including serial port, wired Ethernet, Wi-Fi and cellular technology. In addition, these devices use a variety of protocols to communicate including BACnet, DNP3, JSON, Modbus, OPC, ZigBee and others. Steps to consider include:

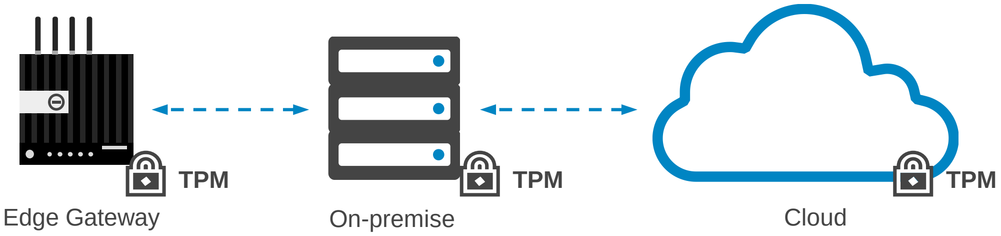
- Identify any equipment installed in a bunker site that may have limited or spotty connectivity.
- Recognize distance limitations affecting the data collection point for the particular communications protocol used.
- Compare the advantages and disadvantages of laying cabling to connect your devices vs using wireless technologies.
- Categorize equipment by protocol translation requirements to determine the right distribution of gateways in your architecture.



4 | Architect for the right level of data integrity

Data integrity is a key element of a good IT critical infrastructure solution. Factors include requirements for real-time data collection such as how frequently the devices communicate to the data collection point(s) and the security and integrity of the connection from the devices to the local gateway, to the on premise data collector, on to the backend system in the cloud. Hardware Trusted Platform Module (TPM) security at every level of the architecture is recommended to ensure secure data transfer. You should also plan for computing headroom so that the long-term analytics goals and growth plans can be fulfilled without a rip and replace upgrade. You know how much data your current equipment generates – imagine what this will be in a year or two.

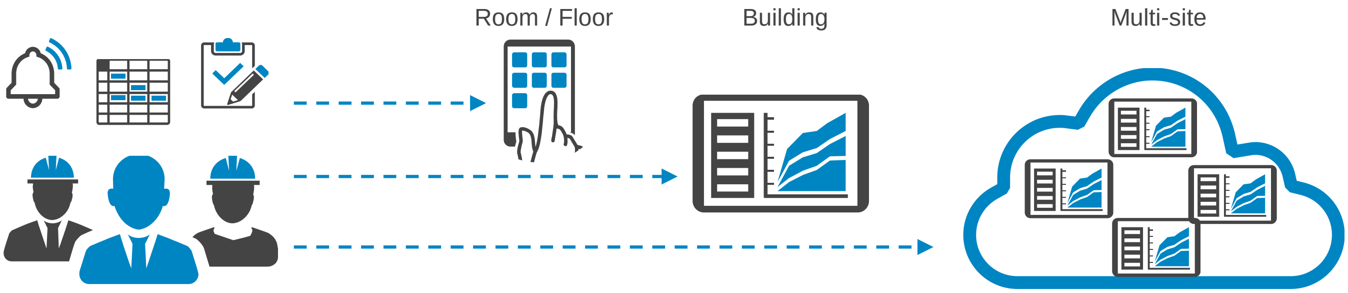
Finally the infrastructure management system should be architected to ensure data redundancy for resiliency, and also include allowances for application updates and security updates without taking down a large part of the system.



5 | Identify where users interact with the data

The user experience is an important factor to consider for these systems. A big part of that experience is where users interact with the data and their scope of management. For example, users want to see some system dashboards in each room of the building separately, monitor certain data on an entire building through a single pane, and sometimes even receive cloud based reporting to monitor multiple sites to review efficiency at a portfolio level.

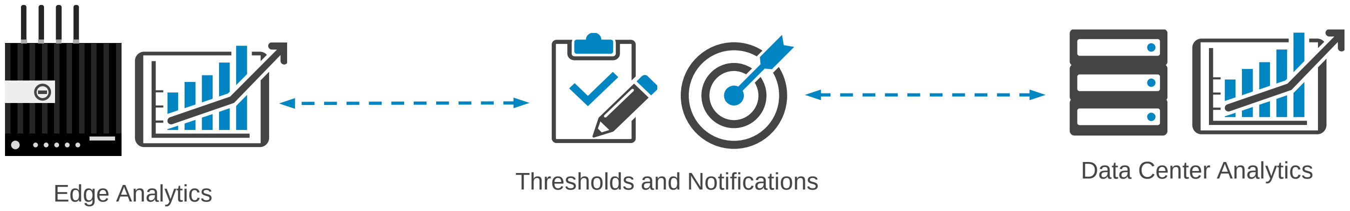
What data needs to be accessible where, and which users need access is a key determining factor for where the optimal location is for the analytical models you will use to produce the reports.



6 | Define key analytics and alarms

Determine what types of information are important to the users and the appropriate alarms, thresholds and notifications which need to be produced by your analytics. The user experience will drive where data resides and where the analytics are performed. For example, some data will need to be sent from the gateway device to the central data center.

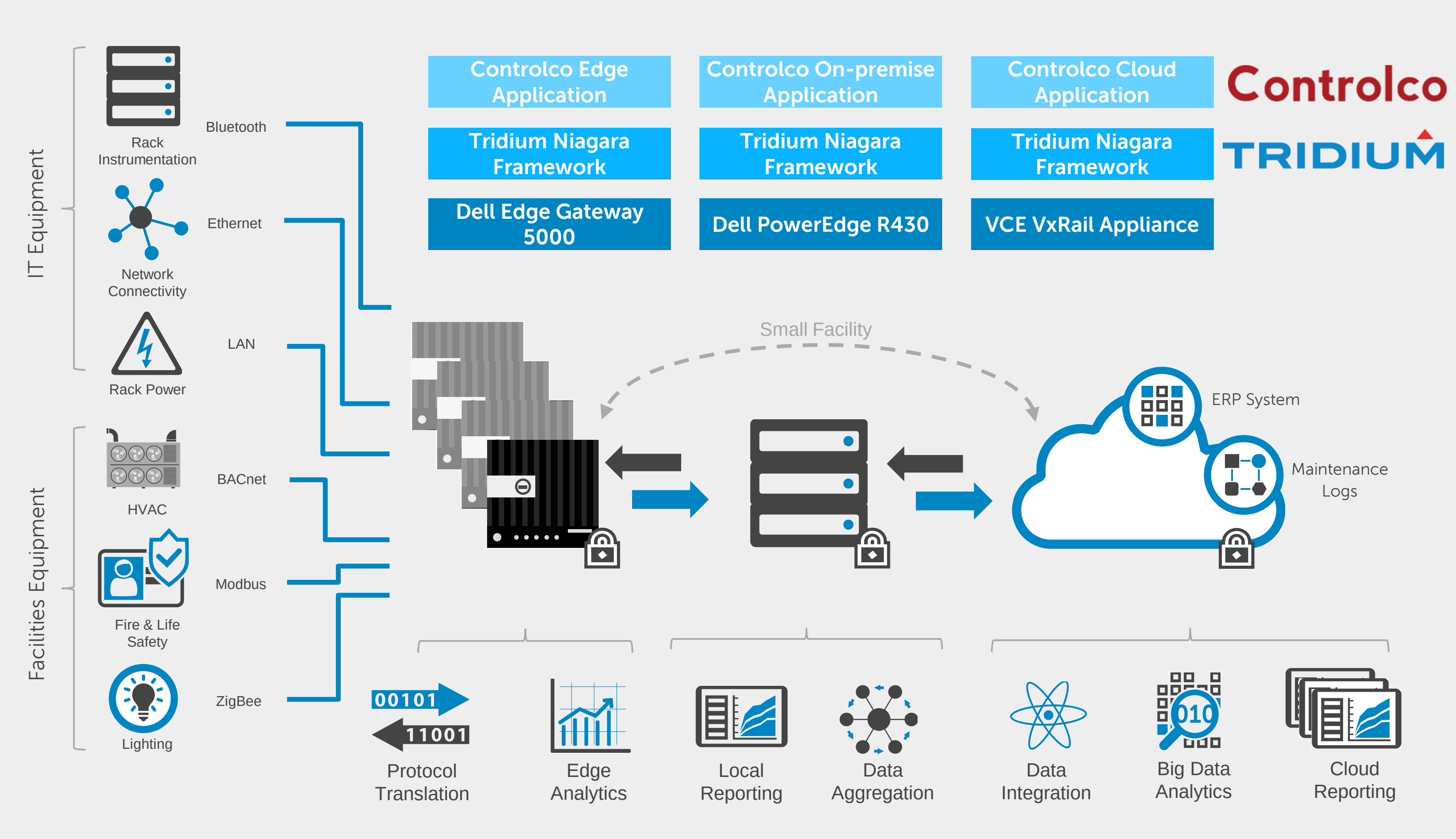
Alarms and thresholds should be reported in a consistent manner. These items can include those where action must be taken immediately and those that proactively anticipate future needs or apply predictive models for future planning. Be sure to consider compliance and external reporting requirements which need to be satisfied by the analytics, and integrated automated reporting where applicable.



IT Critical Infrastructure Management Solution Example

To provide a blueprint for you to build your IT critical infrastructure deployment around, Dell has developed a flexible architecture centered around the Dell Edge Gateway 5000 with qualified partners for a complete solution. The Edge Gateway enables you to collect, analyze, relay, and act on real-time data from machine sensors. With the Tridium Niagara Framework running on the Edge Gateway and the Controlco Edge Application running on Niagara, you can analyze data from diverse IT and facilities equipment. This enables you to measure the physical environment in real time to make smarter operational decisions. For small IT facility deployments the single Edge Gateway can communicate directly back to the cloud. Larger facilities can utilize a Dell PowerEdge R430 on premise to aggregate data from the many Edge Gateways and generate local reporting. Either way perishable data is acted on immediately at the gateway or on premise server level, ensuring that the most meaningful data is reported at the right location to minimize consumption of expensive network bandwidth. The critical data can then be securely transferred to the VCE VxRail appliance in the Controlco cloud running the Niagara Framework and the Controlco Cloud Application where additional structured and unstructured data sources, such as your ERP system and maintenance logs, can be integrated for deeper big data analysis. Finally the Cloud can also integrate data across multiple IT facilities for broader reporting.

This IT critical infrastructure reference example represents a single solution provided by industry leading partners. Your specific application may involve a combination of these and other technology providers within our IoT Partner Program.



Along with our IoT Solutions Partners, we provide technology you can trust to help you get started quickly and efficiently.

Dell takes a pragmatic approach to the Internet of Things (IoT) by building on the equipment and data you already have, and leveraging your current technology investments, to quickly and securely enable analytics-driven action.

The Dell IoT Solutions Partner Program is a multi-tiered partner ecosystem of technology providers and domain experts to complement Dell's broad portfolio of IoT-enabling technologies.

To learn more visit us online at: www.delliotpartners.com

Contact Dell Sales to learn more about the Dell Edge Gateway 5000, our ecosystem of qualified partners, and to deploy this flexible predictive maintenance solution today.

IoT Solutions
Partner Program

Dell IoT Solutions
One Dell Way
Round Rock, TX 78664
www.dell.com/iot
1-800-438-9973