Reference Design Guide

Technology Considerations in a Connected Building Environment

PANDUIT®

Introduction

Every modern building system (HVAC, lighting, security, and communications) uses some form of IT networking for management and control. The technologies for connecting, managing, and automating building systems include servers for hosting management software and controllers for floor level settings. Components can include a wide variety of endpoint devices (such as desktop computers, lighting, variable air volume [VAV] boxes, surveillance cameras, and interactive lobby kiosks) as well as required network infrastructure (cabling, switches, connectors, and related protocols).

Panduit's Connected Building strategy is an innovative approach to the design and deployment of building systems that leverage an intelligent, open-systems architecture to fulfill current day building system requirements while providing a flexible migration path for adopting future technologies. This Connected Building Design Guide presents key physical infrastructure decisions important to project stakeholders when designing and deploying a Connected Building for light commercial use (i.e., 20 – 500 endpoint sensors/nodes).

This guide starts by breaking out key connected building physical infrastructure design elements – middleware, owner and tenant telecommunications rooms (TRs), connected building data center (CBDC), zone consolidation points, and endpoint sensors/nodes – and discusses best practices for design and deployment. The guide then finishes with a survey of top of mind technology issues when designing a Connected Building, such as open/closed systems infrastructure, key building communication protocols, and sustainable building technologies.

Overall, this Panduit Design Guide is intended to generate increased collaboration and new conversations among functional connected building stakeholder groups, especially between internal IT and facilities teams. The result is an enterprise that generates and shares data to reduce occupancy costs, enhance workplace experiences for their tenants or employees, and increase building efficiency, effectiveness, and overall real estate value.

Elements of Connected Building Technology Design

The responsibility for operating and maintaining building automation systems (BAS) has traditionally fallen to facilities teams who manage each system in its own unique silo. Each system is bid separately and operated independently, often over its own proprietary protocol. However, the increased proliferation of open system protocols now is enabling building stakeholders to converge previously siloed building systems in order to drive operational efficiencies and meet tenant needs.

Building stakeholders are increasingly utilizing connected building technologies to drive interoperability and convergence of building devices and systems that formerly would be separately deployed and managed through proprietary closed technologies. These intelligent infrastructure design strategies reduce operational expenses with no additional capital costs to help make building system data visible, valuable, and tangible. Integrated building systems also contribute to core sustainability objectives by managing energy resources more effectively, reducing waste and shrinking the organization's carbon footprint.

This Technology Design section of the Design Guide helps the reader navigate through core technology decisions that enable the deployment of an intelligent infrastructure throughout all connected building elements (see Figure 1). By using this guide, building owners and stakeholders can take the opportunity to move toward an intelligent, converged building infrastructure that extends throughout the enterprise to both connect technology components and serve stakeholder needs.

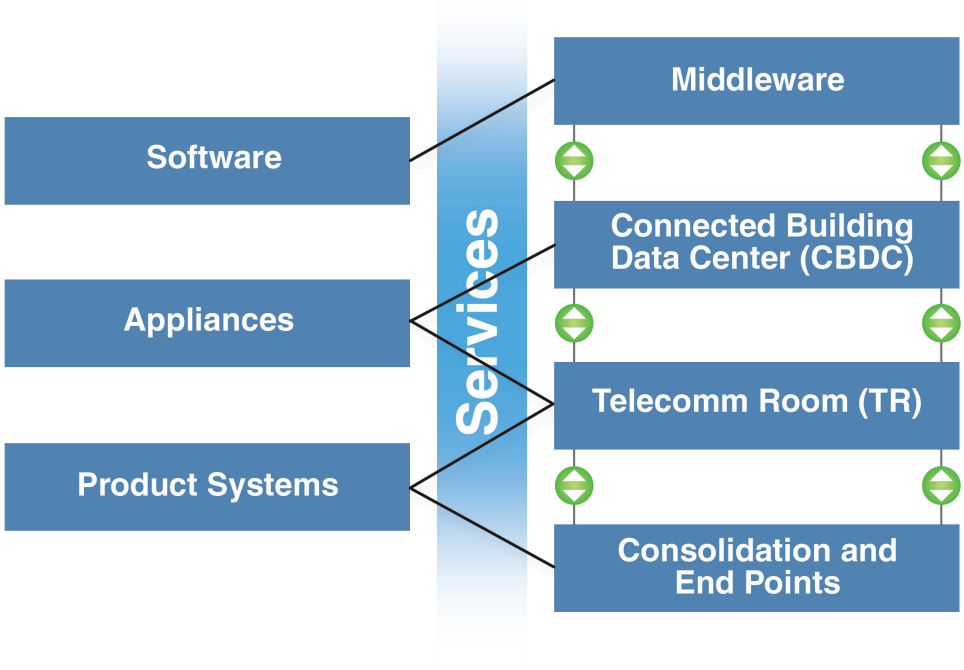

Figure 1: A complete connected building solution is comprised of several key elements.

Middleware

- **Enables effective convergence of systems**
- **Facilitates information flow from edge devices to business systems**
- **Allows (remote) monitoring and control via holistic building policies**

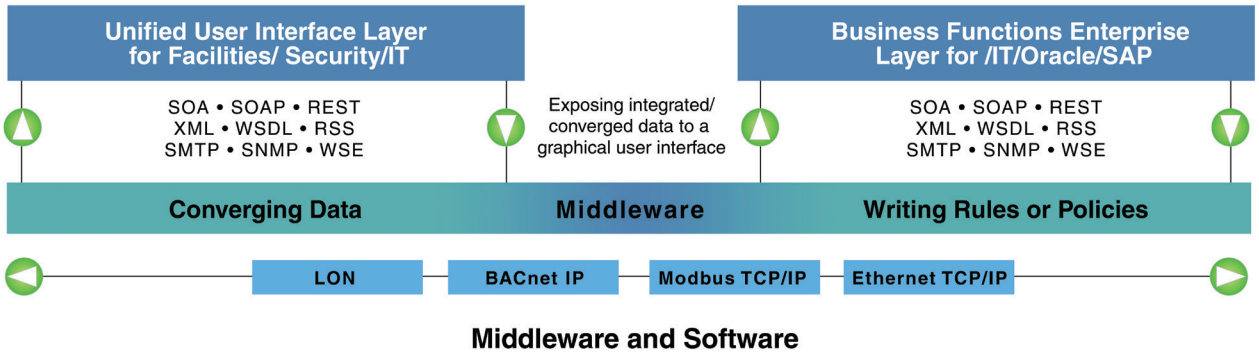

Figure 2: General Middleware BAS system architecture.

Middleware is the internal glue of building automation systems, and is used to translate protocols and normalize the BAS data (see Figure 2). Middleware can take one of several forms – a hardware appliance, a software application, or a combination of both. Custom policies and rules can be written into middleware to leverage and share information between disparate BAS systems such as HVAC, lighting, and security as they relate to occupancy in a building. In this way, middleware plays a foundational role in a connected building solution, as the fundamental tool to enable integration, interoperability, and convergence of building systems.

Many middleware providers use a software application like JAVA to blend and normalize BAS enterprise data on a common interface for increased interoperability. Software drivers are used to integrate or interface to various protocols such as LON, BACnet, and Modbus; these and other BAS protocols then can be converged in the middleware (see Figure 2). In many cases BAS data points can be made transparent to one graphical user interface to provide increased visibility and control over building systems. Some features middleware provides include: reduced cost of ownership, vendor flexibility, more control of a system, interoperability, and integration. Middleware allows the end user freedom of choice and is vendor agnostic.

The ROI for the middleware can be found in the orchestration of rules, policies, and operations that can be implemented to generate resource efficiencies across building systems (i.e., reducing energy/operational costs, improving uptime, and enhancing occupant safety and comfort). For example, an energy demand response can be routed from the service provider directly to the middleware, which then simultaneously instructs HVAC, lighting, and power systems. Each of the BAS systems involved in the energy demand response request will have an independent sequence of operations based on the middleware request. In addition, middleware can provide enhanced environmental conditions, BAS system predictability, remote services, and increased safety.

In summary, normalizing the BAS systems data with middleware allows building stakeholders to improve communication and control across formerly disparate BAS enterprise elements.

Open Systems Approach

When designing a connected building, the first decision point encountered by the design team is to what degree the building will deploy open or closed building automation systems (BAS). A key advantage of middleware over proprietary control technologies is that it enables building owners and stakeholders to take an open systems approach to BAS deployment.

Proprietary or closed systems tend to operate in silos, and complicate construction bidding processes (as well as future moves and migrations) because they are sole-sourced systems. Other drawbacks of using closed systems include but are not limited to: excessive cost of ownership, system scalability issues, integration issues, and end-user flexibility problems.

In contrast, open systems enable BAS scalability and flexibility, and allows the construction scope to be opened up, resulting in reduced capital and operational expenditures. Open protocols are available for all traditional building control systems (lighting, HVAC, and electrical, etc.) that can easily co-exist and interact with IP-based technologies. Although not all building systems are natively IP, all non-native IP systems should have a migration path for connecting to an IP network.

By connecting and harmonizing critical systems and devices, owners can optimize building assets and manage risk into the future.

Connected Building Data Center (CBDC)

- **Enables effective organization of IT assets**
- **Facilitates multi-use tenant space**

Figure 3: Illustration of Connected Building Data Center (CBDC).

There is a need within all buildings to house, manage and organize the growing number of IT assets that are required to operate today's connected buildings. Previous generations of buildings relied on siloed departments to manage, organize and house the specialized equipment required for their specific applications. These were typically spread throughout the building or campus; for example, security was often tasked with managing the video equipment and recorders required to operate their surveillance applications.

The Connected Building Data Center (CBDC) leverages current data center best practices to organize previously disparate building system server, storage, power, and cooling requirements in an efficient footprint (see Figure 3). For example, purpose-built video switches have been replaced by the network IP switch and security recorders replaced with servers and mass storage solutions. The IP network will be flexible and scalable as the physical infrastructure and accommodate nearly all logical connectivity between controllers, management servers and across building systems. It also assures this consolidated and organized environment for the building level server and storage requirements is supported by adequate power and cooling.

This improved organization of assets enables tangible improvements in infrastructure efficiency and assures the integrity and functionality of the connected building. Specific CBDC advantages include improved scalability of new and existing systems, improved management and maintenance of building system application hardware and software, and the consolidation of applications across virtual servers. Existing servers can be used through virtualization of applications.

It is important to note that the CBDC is sized to maintain continuity among critical building systems, and is not designed to supplant other data center requirements. Standalone CBDCs usually are markedly smaller than a traditional data center. The CBDC must be located in a secure environment which minimizes the chances of security breaches or system downtime. Connected building infrastructure can be located in existing data centers.

Telecommunications Room

- **Organized, converged point for all building systems**

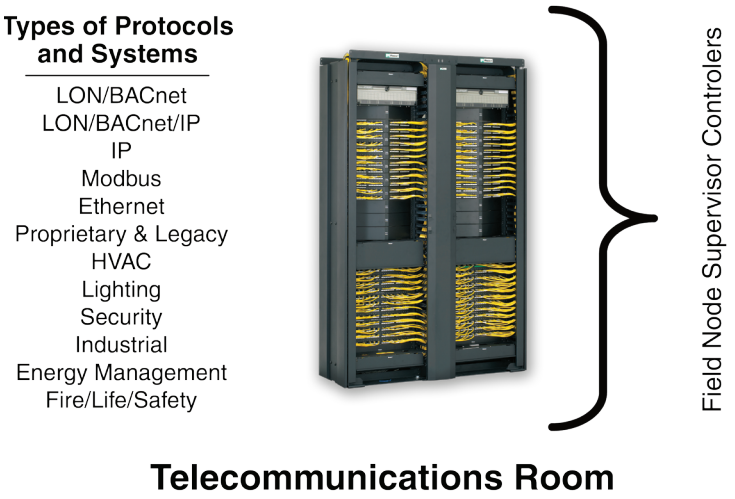

Figure 4: Illustration of telecommunications room/field nodes communicate.

The telecommunications room (TR) is a horizontal zone consolidation point, and is a vital point of aggregation for a series of building control systems (HVAC, lighting, security, badge access, etc.). The TR also functions as the point of physical convergence for field level supervisory BAS components (see Figure 4).

The TR enables the integration of control systems with the IT network and provides a secure environment and consolidation of all network physical connectivity and logical layer equipment. The end result is a consolidated and organized environment for floor level active equipment that optimizes space and provides for floor level control of assets. Connected building infrastructure can be located in existing TR closet areas.

The TR is designed to build flexibility and scalability into the building physical infrastructure, and should be designed to accommodate BAS growth (controllers, management servers, and across building systems). Key TR design and layout considerations include the following:

Security: Both physical (racks, cabinets, enclosures, and IP/Ethernet ports) and logical (network firewalls, demilitarized zones [DMZs]) security should be observed in each TR.

Scalability: The TR often shares real estate with various clients so physical and logical system scalability is important for long-term owner satisfaction and occupant comfort.

Standards: TIA-568 and TIA-569 are ideal resources for new and existing TR design and system layout. Other standards to reference include ANSI/TIA-862, and the ISO/IEC family of documents, including ISO/IEC 11801 and ISO/IEC 18010.

Grounding: Proper bonding and grounding is essential for efficient network performance, dispersing EMI/RFI noise to prevent control system degradation. Grounding systems also provide protection for personnel and equipment. Each TR should link directly into the building-wide bonding and grounding network.

Zone Consolidation Points/Pathways

- **Protect your investment**
- **Minimize cost/impact of reorganization**

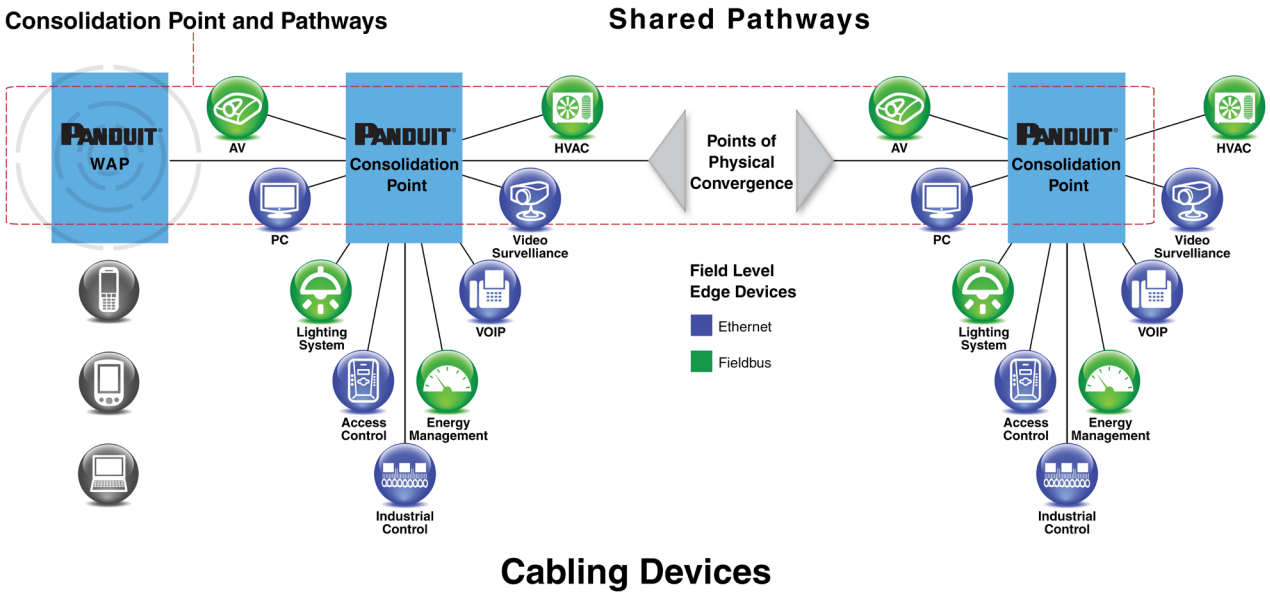

Figure 5: Illustration of how consolidation points/endpoints/sensors communicate.

One of the key enabling technologies of converged physical infrastructures is the use of a zone cabling architecture. Under this approach, all system networks (copper, optical fiber, coaxial and fieldbus cabling) are converged within common pathways from the telecommunications rooms to consolidation points. The final termination is within zone enclosures distributed throughout the building, allowing all cables to be managed and patched in a single enclosure.

This architecture differs from dedicated cabling runs typically used in building systems. Dedicated runs often lead to multiple lengthy and redundant cabling routes along disparate pathways. This leads to inefficiencies in specification, installation, and maintenance. Under a zone architecture, network cabling becomes easier to locate, manage and maintain as each additional building system is routed within the same pathways and enclosures. Managed cabling also helps eliminate abandoned cable in ceilings, making the workplace run more efficiently and safely.

Zone architecture enables upfront cost savings by virtue of its physical design requiring a “single pull” at installation. Future operational cost savings are realized by reducing the time and effort required for moves, adds, and changes. This localizes changes at the zone enclosure and at user/device endpoints, eliminating the more time-consuming changes (such as at the telecommunications room) that a conventional infrastructure would require. A zone architecture also enables you to adopt and deploy new technologies and endpoint devices as well as required network infrastructure to deliver tangible infrastructure and business process improvements.

Endpoints Devices and Sensors

- **Mixture of media**
- **Multi-technology**

Connected building architectures provide a platform for secure, scalable and interoperable systems throughout an enterprise and represent the “last mile” of connectivity to endpoint devices and sensors within the building system infrastructure.

A wide range of endpoint devices that are connected include:

- Surveillance cameras
- Climate controls
- Energy management
- Access controls
- Control valves and actuators
- Wireless communications
- Digital signage

Sensors can include temperature, humidity, CO_2, and more. Endpoint devices and sensors usually are connected/wired to a node which then communicates with the BAS system through a communication protocol (e.g. LON, BACnet, and MODbus) allowing the BAS system extended visibility to log, trend, and alarm data (see Figure 6). Also by exposing these points, control is made possible to increase overall system efficiency.

Wireless Networking/Wireless Application Protocol

Wireless coverage throughout a connected building is a key enabling technology in creating an open and collaborative work environment. All deployed wireless technologies should be 802.11 compliant to avoid proprietary protocol issues in the connected space. In addition, wireless deployment is eased through the use of zone consolidation enclosures to locate Wireless Access Points (WAPs). Wireless coverage can also be an effective future means of reaching out to endpoints and sensors within the space, particularly if these endpoints and sensors are “monitor only” in function. *Note: It is highly recommended that critical control points be served by wired networks.*

Power over Ethernet (PoE)

PoE extends the capabilities of Ethernet by delivering both data and reliable DC power over the same cables to endpoint devices such as VoIP phones, access control and surveillance cameras, and wireless access points. Because PoE converges data and power together over the same cable to each device attached to the local area network, devices can be installed without the need for a dedicated AC outlet. This saves money by eliminating the cost and time associated with AC outlet installations, while providing the flexibility to locate PoE devices where performance is optimum.

Benefits of Connected Buildings

The benefits of deploying a Connected Building architecture over that of a traditional network architecture include the following:

- Lower installed cost resulting from convergence of physical and logical BAS components
- Improved ROI based on centralized management of logical BAS components
- Reduced operational cost resulting from sustainable building design and architecture

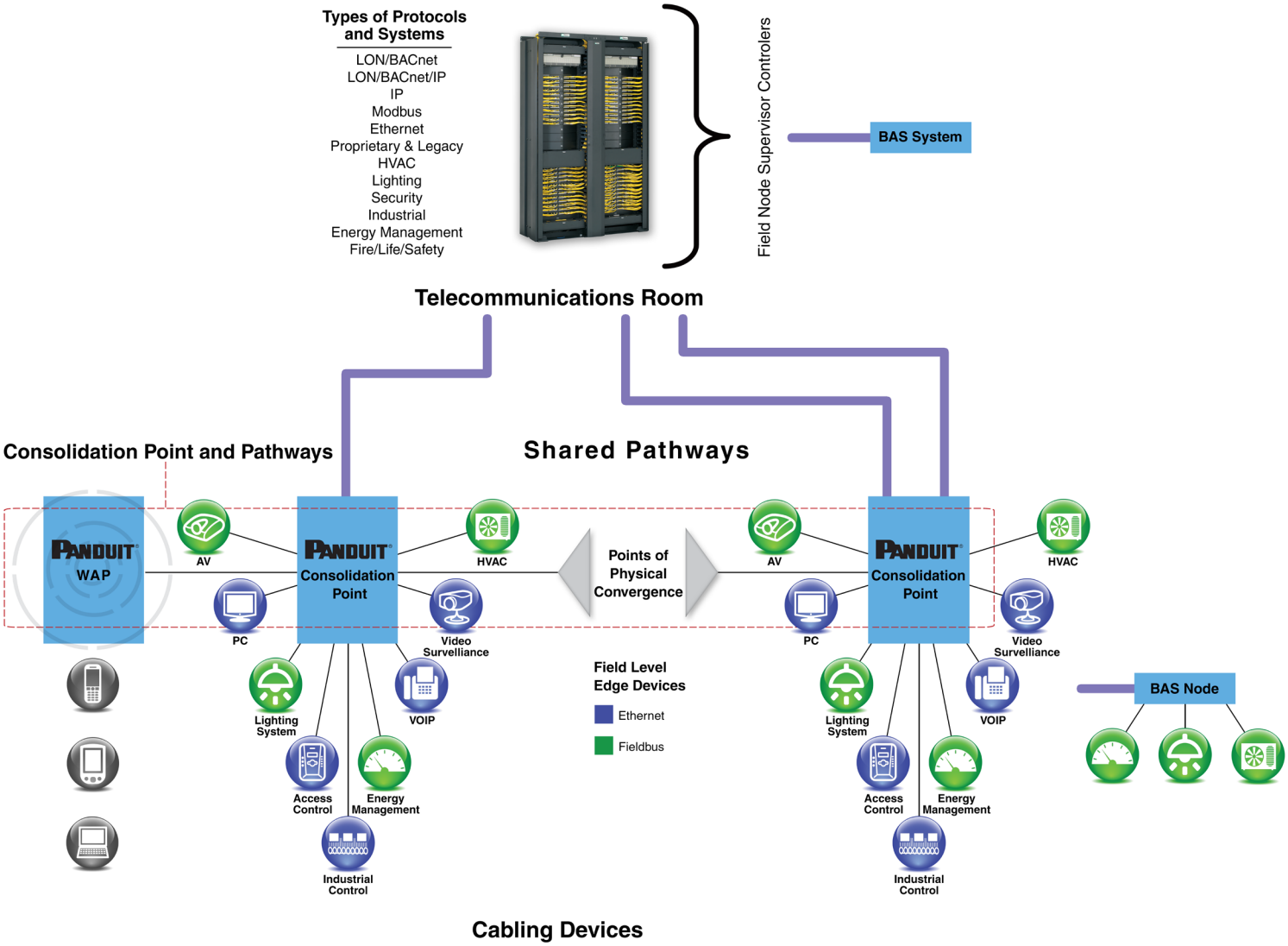

Figure 6: Illustration of how nodes/endpoints/sensors communicate.

Lower Installed Cost: Converged Architecture

Legacy building systems often are installed and operate in silos. These systems are functionally robust but are operationally inefficient and often cost more to install and operate. The increased cost is a result of multiple fieldbus device networks cabled or wired directly to the BAS supervisor control, and the lost efficiency is due to a lack of logical convergence between the disparate BAS systems.

By contrast, a connected building architecture converges both physical and logical networks (Card Access Control, Video Surveillance, HVAC, Power, Fire/Life/Safety systems) and uses middleware to implement rules and policies. This architecture results in a deployment that enables stakeholders to leverage expert policies that can engage any and all of the systems on concert with each other to realize significant operational benefits and savings. An example of a rule or policy might be for all digital signs to show exit routes in the event of a fire or severe weather, leveraging both fire panel and a weather service systems.

Stakeholders also can take advantage of a converged physical infrastructure that extends to all system endpoints and sensors. With all building networks designed to reside in the same pathways, multiple redundant cable runs between controllers and telecommunication rooms are eliminated. This architecture reduces the risk and cost associated with installing disparate networks and enables stakeholders to optimize project and contract resources.

Improved ROI: Centralized System Management

The centralized management and deeper visibility into building systems afforded by a connected building architecture lowers operating costs and improves occupant comfort and safety by enacting rules and policies across any and all building systems in concert.

Traditional siloed building system deployments usually allow the HVAC/Controls contractor to build a common graphical user interface that is used mostly by facilities. Their sequences of operation are typically boiler plate specifications and do not require much if any logical cross communication between other BAS systems or components.

By contrast, the graphical user interface for a connected building is not just for facilities but serves all building occupants. The user interface is designed by a system integrator on a middleware platform. The ROI can be found in the logical convergence with the understanding that just because any two BAS systems can be integrated does not necessarily mean they should.

Reduced Operational Expense: Sustainable Architecture

Physically converged infrastructures also contribute toward larger corporate sustainability initiatives by enabling reduced resource consumption (e.g., energy, real estate) while optimizing the occupant experience. Basic green objectives include reducing consumption of non-renewable resources and creating healthy environments.

Many systems and technologies can contribute to helping owners and other building stakeholders achieve their sustainability goals. Some of the key systems might include dimmable, addressable lighting controls, smart electrical sub-metering, digital building automation controls and automated fault detection and diagnostics. These systems are used to improve occupant comfort, achieve energy efficiencies, and shrink the organization's carbon footprint.

Connected building architectures also add value by differentiating properties from the competition in a business climate where environmental stewardship is increasingly valued. Additionally, a connected building is more ready for interaction with the smart electrical grid and better able to comply with the changing regulatory environment. The result is a property that is both good for the planet and good for the bottom line.

Conclusion

Every building system (HVAC, lighting, security, and communications) uses some form of IT networking for management and control. The technologies for connecting, managing, and automating building systems include servers for hosting management software and controllers for floor level settings. This approach enables the use of an open standards-based, service-oriented architecture framework and is designed to deliver tangible infrastructure and business process improvements.

Panduit has developed the industry's most comprehensive and holistic approach to a connected building infrastructure and can help enterprises align, converge, and optimize critical systems, such as communication, computing, control, power and security. An intelligent network infrastructure extends throughout an enterprise to connect technology components and bridge stakeholder needs. Panduit's advanced services offerings harness our physical infrastructure expertise to help you design and develop a connected building solution that optimizes building efficiency and effectiveness. These solutions enable linked facility and network systems to be built directly into the building fabric, generating and sharing data over a unified intelligent infrastructure to reduce occupancy costs, enhance workplace experiences for their tenants or employees, and increase overall real estate value.

About Panduit

Panduit is a world-class developer and provider of leading-edge solutions that help customers optimize the physical infrastructure through simplification, increased agility and operational efficiency. Panduit solutions give enterprises the capabilities to connect, manage and automate communications, computing, power, control and security systems for a smarter, unified business foundation. Panduit provides flexible, end-to-end solutions tailored by application and industry to drive performance, operational and financial advantages. Panduit's global manufacturing, logistics, and e-commerce capabilities along with a global network of distribution partners help customers reduce supply chain risk. Strong technology relationships with industry leading systems vendors and an engaged partner ecosystem of consultants, integrators and contractors together with its global staff and unmatched service and support make Panduit a valuable and trusted partner.

WORLDWIDE SUBSIDIARIES AND SALES OFFICES

PANDUIT CANADA
Markham, Ontario
cs-cdn@panduit.com
Phone: 800.777.3300

PANDUIT EUROPE LTD.
London, UK
cs-emea@panduit.com
Phone: 44.20.8601.7200

PANDUIT SINGAPORE PTE. LTD.
Republic of Singapore
cs-ap@panduit.com
Phone: 65.6305.7575

PANDUIT JAPAN
Tokyo, Japan
cs-japan@panduit.com
Phone: 81.3.6863.6000

PANDUIT LATIN AMERICA
Guadalajara, Mexico
cs-la@panduit.com
Phone: 52.33.3777.6000

PANDUIT AUSTRALIA PTY. LTD.
Victoria, Australia
cs-aus@panduit.com
Phone: 61.3.9794.9020

For a copy of Panduit product warranties, log on to www.panduit.com/warranty

For more information

Visit us at www.panduit.com

Contact Customer Service by email: cs@panduit.com
or by phone: 800.777.3300

CPDG05--WW-ENG
replaces WW-CPDG02
5/2015