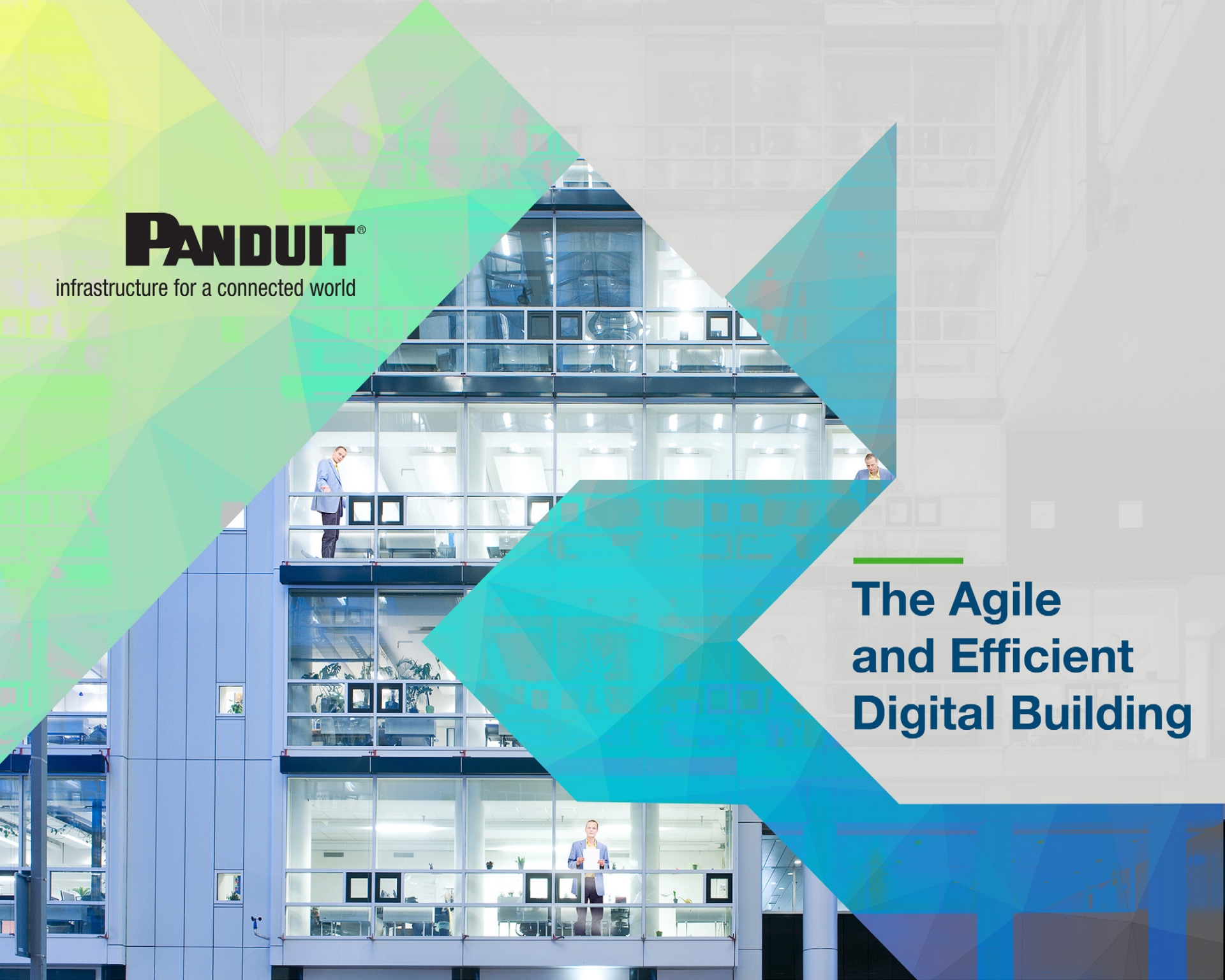
PANDUIT®

infrastructure for a connected world



The Agile and Efficient Digital Building

Table Of Contents

Defining The Digital Building

Current trends show a transformation in the work environment. Wide open, one-size-fits-all, wall-to-wall cubicle spaces are being replaced by an environment that is smaller, flexible, intimate, and fun. Employers are wooing a younger, more collaborative workforce that cares about things like the health and wellness of the work space and flexible working conditions. Connected devices such as sensors provide the intelligence that allows these flexible, healthy, efficient spaces to be created.

These devices are part of the Internet of Things (IoT), which is changing the way we do business and manage our environment. Combine all this interconnected technology on the IP network with the ability to gather data and develop analytics and you have a digital building.

The digital building isn't a new phenomenon, but it is made more agile by IoT. More than 20 years ago, communication and data were converged onto the same network and access control and security followed several years later. Since the early 2000s, more and more systems have converged onto the network, making buildings smarter, more efficient, and easier to manage.

Advantages of a digital building go well beyond energy savings and optimized building operations. For many organizations, the true benefit of a highly connected building is a more satisfying customer experience, higher employee productivity and satisfaction, better student performance, or improved patient health.

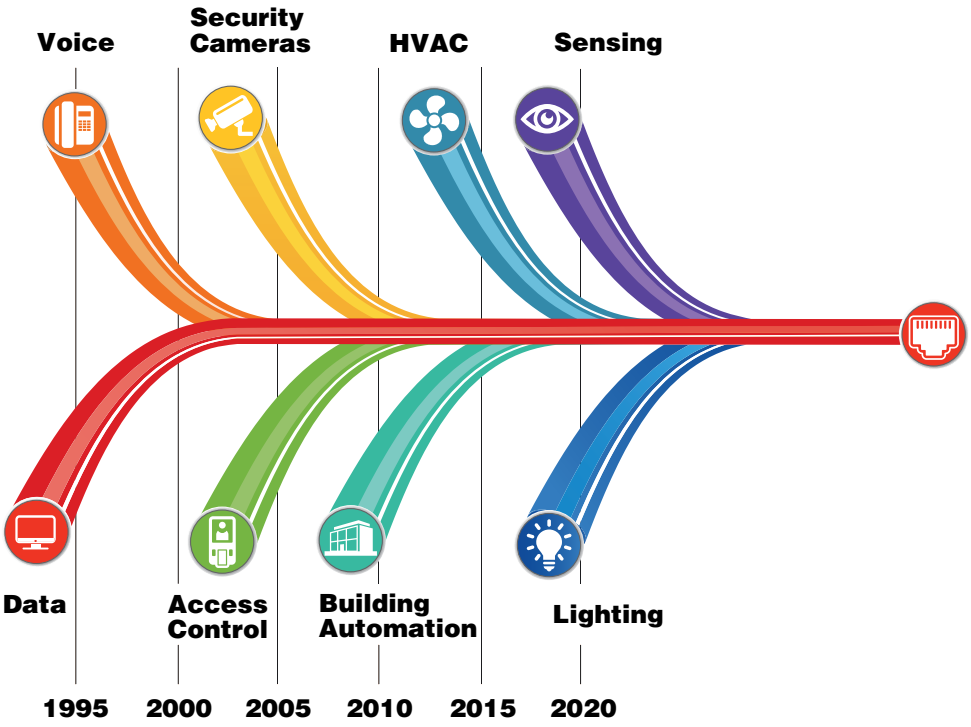
Digital Building

To define the digital building, we first look at the smart devices used in the work environment. The modern building needs a variety of smart devices and systems to meet the needs of the business. Video cameras, lighting and environmental sensors, wireless access points, security devices, and LED lighting are all connected to an IP network infrastructure using a backbone of Category structured cabling. To power and control these devices, that same Category cabling delivers Power over Ethernet (PoE) from a PoE-enabled IP switch. When you add in control systems, applications, and analytics, the final result is a digital building.

Connected devices collect data which provides insight into building parameters like energy usage, occupancy, and building wellness. The analytics can then be used to add intelligence to the network. This actionable information is the foundation for a highly-optimized building, where devices can automate lights and temperature, send notifications for changes in building wellness, and enact alarms and send notifications around security issues.

IP Advantage

The backbone of the digital building is a converged IP infrastructure that enables integrated systems and devices to share data across the network. Centralized management oversees the network which can be managed and controlled on premise or remotely via mobile devices. The IP network provides a platform for easy moves, adds, and changes (MACs) which can lower your cost of operations.



- Voice and data
- Lighting
- HVAC/Building Automation System
- Sensors
- Wireless
- Security
- A/V
- Supporting Infrastructure

A Deeper Dive: Digital Building Systems

The defining characteristic of a digital building is having diverse systems that rely on technology to – ideally – make management and operation of building functions easier, more efficient or more cost-effective. Let's dig a little deeper into each of these systems.

Building Management Systems

Building Management Systems (BMS) are a more mature system within the building, and have evolved as the industry has matured. In the early days, they provided a single viewpoint or dashboard to monitor and manage the various systems. Today, BMS goes well beyond that, with the IP network linking those building systems to each other, to sensors, and to other systems. The systems can track when someone badges into a building, and respond by turning on the lights in his or her office and adjusting the blinds and room temperature to their preferred setting. At the same time, the system is troubleshooting an HVAC unit on the other side of campus that isn't operating within defined parameters, and is adjusting the temperature in a training center because sensors indicate a large number of people in the room.

As the systems have changed, so have the names. Is there a difference between a BMS and a Building Automation System (BAS), Building Information Management System (BIMS), Building Automation and Control System (BACS), or a Building Energy Management System (BEMS)? It depends. Vendors, analysts, and publications may have different names for the same system, or they may consider nuances between the systems and identify them differently based on that. Because of overlap between the different types of systems, it is becoming harder to differentiate and the terms frequently are used interchangeably.

The Market

"Commercial Building Automation Systems," published by Navigant Research points to Building Automation Systems as a mature industry with moderate, consistent growth. The BAS market was $67.1 billion in 2016. Navigant predicts growth of 4.8% annually, for a value of $102 billion in 2026. North America is the largest market for commercial BAS, followed closely by Asia Pacific and Europe. (For their reporting, Navigant defines BAS as an umbrella system that includes five subsystems: HVAC, lighting, fire and life safety, security and access controls, and building management systems.)

The BAS market is projected to grow to $102 billion by 2026

The Solution

BMS systems are varied. At a basic level, sensors, devices, valves, and controllers combine with hardware and software to form the BMS. The components vary depending upon the system that is connected and controlled. HVAC, for instance, collects data through sensors, actuators and meters that measure temperatures, pressures, flows, set points, etc. Granular information is delivered in real-time to show how the HVAC system is operating, and problem areas.

Along with measuring and monitoring individual systems, a BMS also connects systems. For example, when lighting sensors detect building or room occupancy, the BMS alerts air handlers and chillers to adjust air flow and temperature.

Building management systems today commonly integrate:

- HVAC
- Security and access control
- Lighting

Additionally, other systems that are being connected to BMS include:

- Fire and life safety
- Intruder alarms
- Elevators

Beyond that, the BMS can incorporate a variety of other components and services including audio/video, digital signage, irrigation, scheduling, and specialty systems such as nurse call, classroom communication and campus alerts.

One feature of modern systems is mobile compatibility, allowing facility operators to manage and control the systems from any device, anywhere, 24/7. And, sophisticated systems also give environmental control capabilities to employees, who can control things like lights and temperature at their workspace via their mobile device.

The IP Advantage

Technology has the potential to transform the operation of buildings. Connecting disparate systems and devices to an IP network allows those systems to share data on occupancy, space usage, temperature, and more, which makes buildings more responsive and more efficient. This also leads to higher employee satisfaction and productivity.

Security

The demand for secure infrastructure is at an all-time high. From school campuses to office high-rises to warehouses and factories, security systems protect people, property and assets.

70% of distributed building services connections are security devices

The market

A May 2017 report from BSRIA, “Convergence and Digitalization of Commercial Buildings in the US,” identifies physical security products, including cameras, access control and intruder alarms, as the most common products installed on the network. The installed base of security cameras in North America totaled 62 million by the end of 2016, with more than 9 million added in 2016 alone. Security devices accounted for 70 percent of the distributed building services connections. While BSRIA predicts the number of security devices will continue to grow over the next five years, security’s share of the network will decrease, due to rapid growth of other non-security systems, such as lighting.

Security systems are common in all vertical markets, and in both new construction and existing facilities. IP network integration is highest for cameras – of the 9.4 million cameras installed in North America in 2016, nearly 8 million (75 percent) were integrated into the organization’s IP network. An estimated 55-60 percent of access control readers are networked; and about 40 percent of intrusion systems are on the IP network.

75% of installed cameras are networked

The solution

Building or property security is a multi-faceted solution that typically includes some combination of video surveillance, intrusion detection, and access control. Some organizations include life safety systems under that security umbrella, as well. The systems are typically integrated, so that when one component engages (such as an intrusion alert), it can cause other components to react (a camera turns on, recording begins, doors lock, alarms sound, etc.), dependent upon the specific system and its configuration.

Typical components include:

- Cameras with a recording device and monitoring equipment
- Access control readers or keypads
- Intrusion sensors

Systems can also include radar-based detectors, analytic systems, and video or audio-based communication to allow security staff to communicate with visitors at a secure entry.

Cameras
A variety of cameras are available ranging from simple to complex. Beyond resolution and picture quality, camera features may include the ability to remotely control the angle and zoom of the camera, such as pan-tilt-zoom (PTZ) functionality, and heating elements in cameras designed for outdoor use in cold climates.

Access Control
Access control can be as simple or as complex as the organization requires. Many organizations issue access codes, key cards or badges to employees in lieu of keys, with each employee receiving credentials to access specific areas. Security levels are set as needed, for the right balance between safety and convenience. Credentials are easily activated and deactivated with personnel changes.

Intrusion Sensors
Intrusion detection sensors can detect a variety of activities that may indicate unauthorized access to a building or property. These can include door sensors, glassbreak detectors, or motion detectors. The sensors are tied into the control system, which reports the incident to a central control panel for resolution.

Biometric scanners take **security** a step further, requiring a **fingerprint** or **iris scan** for access to secure areas.

The IP Advantage

Most security systems installed today are IP-based, replacing the analog systems of yesterday. IP-based systems deliver significant advantages over their analog counterparts:

- Improved image quality
- Easy installation and integration
- Scalability
- Access real-time video from any authorized device anywhere
- Cost-effective

Leading systems boast open IP standards, making them easy to connect with existing IT equipment, and other systems. Beyond interconnecting the cameras, recording devices, monitors, access control, and intrusion sensors, the security system can be tied in with other IP systems, such as building management, lighting, or point-of-sale.

And, cameras, sensors, and access control are commonly powered via Power over Ethernet, so the same network cable that delivers data to the device also delivers power.

Lighting

Intelligent lighting is expected to be the next big thing for buildings. Smart lighting delivers high-quality and energy-efficient lighting. Intelligent lighting, however, goes well beyond just lighting. Today's lighting systems also include sensors and controls that tie into building management systems, providing new levels of control, while delivering a wealth of information on room usage, occupancy levels, atmospheric conditions, and more. This visibility, management and control leads to buildings that are highly efficient and conducive to conducting business with today's workforce.

Gartner, in its market report "Market Trends: The Five Phases That Smart Lighting Providers Must Address to Be Successful in the Internet of Things," says that smart lighting has the potential to reduce energy costs by 90 percent. And, LED lighting alone won't drive these results. "To successfully achieve the lowest electricity cost, in addition to achieving safety and security and enhancing the office environment, lighting product managers at technology and service providers will need to implement five key strategic phases of smart lighting: (1) LED lighting, (2) sensors and controls, (3) connectivity, (4) analytics and (5) intelligence," said Dean Freeman, research vice president at Gartner.

Smart Lighting has the potential to reduce energy costs by 90%

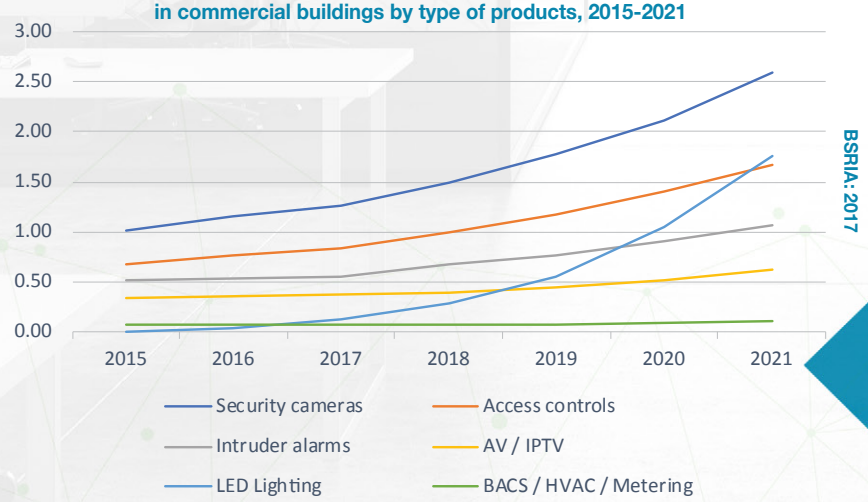
The market

In its 2017 report, Convergence and Digitalisation of Commercial Buildings in the US, BSRIA predicts “explosive growth” for PoE-powered LED lighting. BSRIA predicts that installed nodes or outlets for lighting will grow from a base of almost none in 2015 to nearly 2 million by 2021. It projects as the fastest growing application among distributed building services.

BSRIA reports that while uptake is slow, they expect PoE lighting to follow the same trend as phones within the office space and their move to VoIP.

Some suppliers estimate cost savings of 20-40% with PoE lighting, with the PoE switch being a significant portion of the installation cost. As low-voltage lighting becomes more common, BSRIA predicts that cost will likely come down as new equipment becomes available and competition increases.

Distributed Building Services, million nodes/outlets in commercial buildings by type of products, 2015-2021



BSRIA: 2017

The Solution

Intelligent lighting equipment vendors have variations in their architectures, but lighting systems generally include an end-to-end system that includes:

- Luminaires
- Control
- Sensors

Luminaires

The foundation of any lighting system is the luminaire, or light fixture, including the lamp or bulb, any lens, diffuser, or cover, and the fitting. Bulbs are LED, which have a longer life and consume significantly less energy, thus having the biggest impact on the energy budget for most organizations.

Control

The control feature is where the vendors really differentiate. Via software and hardware, facility managers and occupants can control brightness and color, along with daylight harvesting, occupancy detection, and more.

Sensors

Measuring everything from room occupancy levels to energy usage to daylight levels, sensors provide actionable data that facility managers can use to add another level of efficiency to their operation.

The IP Advantage

In the same way that voice over IP (VoIP) drove exciting changes to enterprise telecommunications networks, PoE lighting is shaping up as the platform that defines new building capabilities.

In a digital lighting system, each light links to the building's IP network. The system can drive new ways to interact with people and places, sense the environment, gather and share data, and provide a more productive and enjoyable working environment. Lighting fixtures can deliver intelligence, gathering and sharing a wealth of data, including occupancy, activity patterns, temperature, and daylight levels.

IP connectivity also provides an exceptional level of control. Occupants and building managers can control workspace lighting via their own smart device, creating an environment most conducive to each individual.

Ease and efficiency of installation is also a benefit, as data and power are delivered via the same low-voltage Ethernet cable, eliminating the need for an electrician and additional wiring.

Emergent Systems

As technology advances, it seems new systems are being adapted to the network on a daily basis. Some of these systems are specific to an industry, such as nurse call systems in hospitals or smart whiteboards and learning tools in schools. Still others, like A/V, point of sale, and digital signage, are seeing widespread adoption across a variety of markets.

93% of Educators say video improves the learning experience.

The Market

It is difficult to pinpoint the potential for these new systems, as they represent a small portion of the overall market. A/V represents the largest segment of these “other” systems, with BSRIA reporting that 5-6% of the other systems are A/V; digital signage is around 4%; room scheduling systems are around 3%; and smartboards (education) come in at about the same rate.

The Solutions

Solutions are widespread and varied. Among the types are:

- A/V
- Smart whiteboards
- Online learning
- Classroom engagement
- Digital signage
- Point of sale readers
- Room scheduling systems
- Nurse call
- Clocks
- Public address
- Elevators
- Landscape irrigation
- Parking
- Window coverings
- Bathroom fixture monitoring

The list grows continually, as start-ups enter the field and existing companies expand their portfolios.

The IP Advantage

Like many of the systems outlined, these types of solutions benefit from being able to link to and communicate with sensors and other systems. Networked solutions are also more likely to be generating data that can be used to further enhance efficiencies within the facility.

Additionally, PoE powering makes it easy to install, expand, and optimize these systems without the need to run electrical lines.

Why Infrastructure Matters

The one defining characteristic that makes a digital building different from any other building is the interconnectedness of its systems. So, it stands to reason that if you want to insure and optimize the performance of those systems, you need an infrastructure that supports that interconnectedness – an infrastructure built on structured cabling.

Add in the fact that many of the connected devices will be powered by Power over Ethernet, and the importance of that infrastructure multiplies.

Here we answer some common questions regarding the infrastructure needed for the digital building of today – and tomorrow!

Q: My lighting system, security system, and wireless system all recommend different types of Category cabling. How do I know what I really need?

A: A Category 6A cabling system best supports all known current and future applications. Some digital building systems, such as intelligent lighting, don't require Category 6A performance. But, other systems – like the latest generation of wireless access points (WAPs) – do, so it makes sense to install Category 6A to connect all devices on the network.

There may be instances where it makes sense within your building to run two types of cable (e.g. Category 6 for lighting and Category 6A for everything else), but that is harder to manage and maintain post-installation, and could limit future growth. Most organizations will find Category 6A to be the best end-to-end solution for their work areas.

Q: What about fiber?

A: Fiber is the best choice for the building's backbone, connecting the data center/main distribution facility to the telecommunications rooms. That fiber backbone insures that your pipe is big enough to support whatever systems are there today and those that are added in the future. OM4 fiber optic cable is the best choice, as it meets today's needs and provides a safety net for the future.

Q: Do I need anything special to run PoE?

A: A PoE switch and category cabling are all that is needed to power PoE-enabled devices. There are things to be aware of, however. PoE causes heat rise within the cable and connectors, which can affect network performance. This is another place where Category 6A cabling carries inherent benefits. Category 6A cabling plant has the best thermal properties to handle temperature rise issues from PoE, and has no bundling restrictions. A relatively new UL designation – Limited Power (LP) – also can impact installation. The National Electric Code was revised in 2017 and places new requirements on projects that are using the highest levels of PoE. While the NEC doesn't mandate LP cables, using cabling with that designation makes it easy to ensure the NEC requirements are met.

Q: Do I have to use special connectors or will any connector work?

A: As much as we hate the answer 'it depends', that is really the best answer here. Things like geography and the standards that are in place in your locale come into play, as well as the type of device you are installing and the architecture you're using. In North America, for instance, any materials installed in the ceiling must be plenum rated; in Europe the new CPR standard comes into play. You (or your installer) need to be sure you're meeting whatever the local requirements are.

If you're looking to direct attach devices, then field term plugs make installation a snap. Or, you may be installing a patch panel, box, or even the PoE switch in the ceiling, and will run patch cords directly from that point to the device. These components are all standard, but again must meet the local standards.

Putting It into Practice

The best way to envision what a digital building can look like is to see one in action. When Cisco Systems, Inc., built a new Canadian headquarters in 2016, they relied on a Panduit infrastructure to increase network availability and employee productivity, while enhancing the workplace experience for employees.

Enabling IoT Capabilities through a Converged IP Network

The Oxford Properties high rise (RBC Waterpark Place III) was a prime location for Cisco's new Canadian headquarters. The building was equipped with a converged backbone network which the Cisco Canada Smart & Connected Real Estate team had worked on with Oxford Properties. The new headquarters occupies more than 100,000 sq. ft. of space in the building, comprised of employee office space, meeting rooms, system engineer and testing labs, solution demo rooms, and an executive briefing facility for customers.

Cisco IT and the Smart & Connected Real Estate team collaborated to develop a plan to incorporate a variety of technologies to enhance the workplace experience for employees. These included IP-based and PoE-powered lighting, environmental monitoring, HVAC control, building automation, and energy management, as well as traditional technologies like Voice over IP (VoIP) phones, IP security, access control, and wireless access points (WAPs).

Strategic Objectives

Cisco had several key objectives for the building:

- A secure, converged IP infrastructure that used real-time information across building systems to centrally manage resources, enable greater risk management and increase overall performance; this would replace siloed networks, achieving savings in capital expenses and operational expenses
- Improved visibility into operations to streamline processes while controlling most IP-related utilities on each floor
- Expansive PoE system to power the various devices in the space, including lighting, variable air volume (VaV) controllers, security cameras, environmental sensors, VoIP phones, and door access controls
- High-speed wired and wireless access
- Enhance employees' experience in the workplace, and showcase its ability to help implement such technologies with customers

The Solution and Results

Cisco built its converged IP network on an infrastructure of Panduit copper and fiber cabling systems. “Panduit was influential in helping us decide which technology components should be a part of our converged backbone,” said William R. MacGowan, P.Eng, CEM, Cisco Canada. “With the appropriate network infrastructure to support our continuous growth, Cisco Canada can achieve more sustainable operations through increased network availability and productivity.”

The building has more than 2,500 PoE connections, supporting the wide variety of PoE-powered devices. A Category 6A cabling system connects switches, while a Category 6 system delivers data and PoE to the networked devices. The fiber backbone included several thousand OM4 and OS1/OS2 fiber optic connections, providing support for 40 Gb applications.

The secure converged IP network is providing several benefits for Cisco:

- Real-time monitoring of external daylight levels, temperature, and occupancy
- All equipment operates on one network, allows tenants to connect devices such as lighting to access control to heating.
- The network provides a flexible migration path for future growth and allows Cisco to respond to customer demands easier and faster

According to MacGowan, “Through its converged network infrastructure system, Panduit is helping Cisco transform the way buildings are designed, built, managed, and experienced. Placing all devices and equipment onto a single IT infrastructure increases Cisco’s business operations while reducing capital expenses to achieve a secure, scalable facility.”

PANDUIT®

Since 1955, Panduit's culture of curiosity and passion for problem solving have enabled more meaningful connections between companies' business goals and their marketplace success. Panduit creates leading-edge physical, electrical, and network infrastructure solutions for enterprise-wide environments, from the data center to the telecom room, from the desktop to the plant floor. Headquartered in Tinley Park, IL, USA and operating in 112 global locations, Panduit's proven reputation for quality and technology leadership, coupled with a robust partner ecosystem, help support, sustain, and empower business growth in a connected world.

For more information

Visit us at www.panduit.com

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

PANDUIT US/CANADA
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