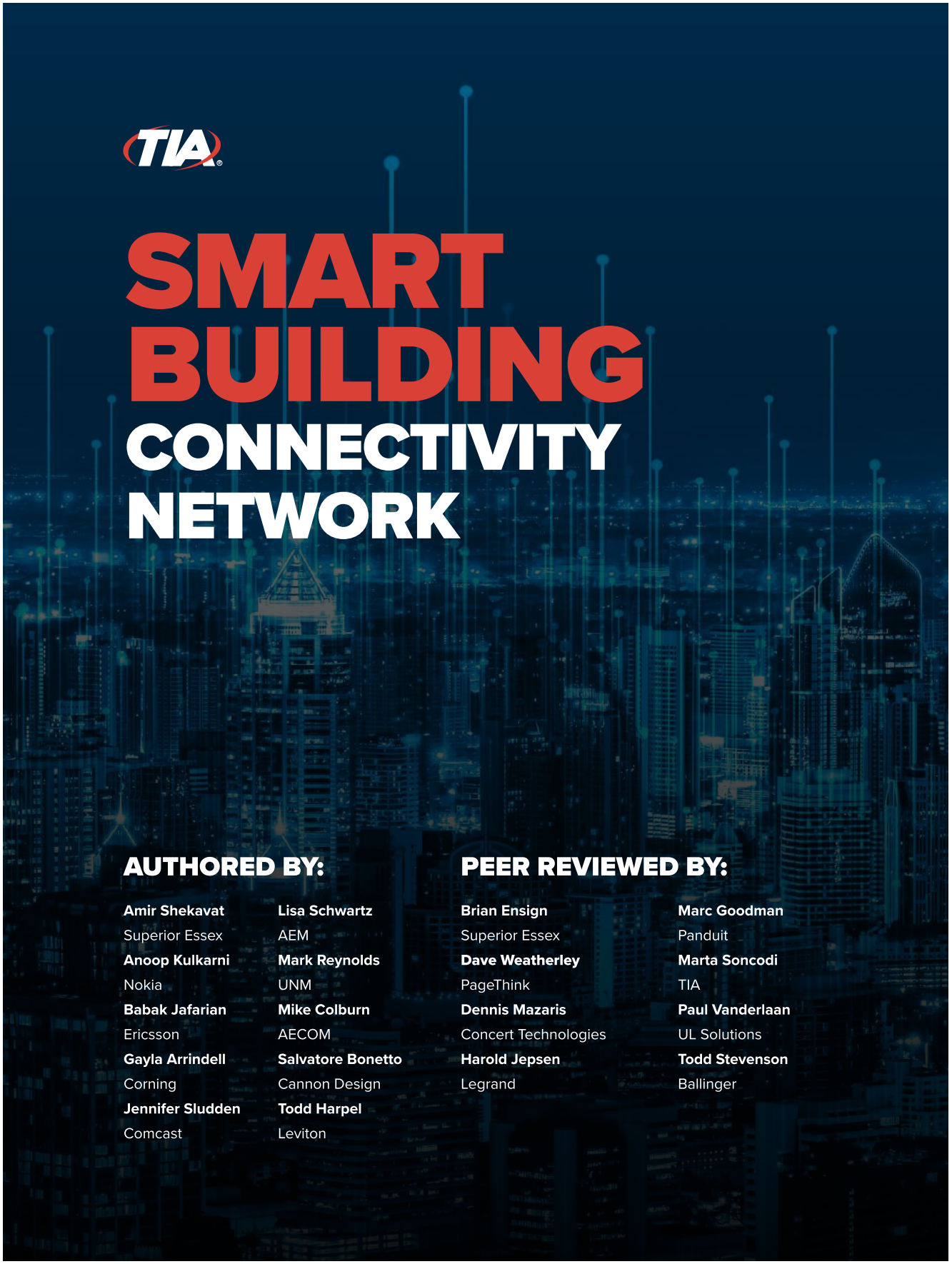

SMART BUILDING CONNECTIVITY NETWORK

AUTHORED BY:

Amir Shekavat
Superior Essex
Anoop Kulkarni
Nokia
Babak Jafarian
Ericsson
Gayla Arrindell
Corning
Jennifer Sludden
Comcast
Lisa Schwartz
AEM
Mark Reynolds
UNM
Mike Colburn
AECOM
Salvatore Bonetto
Cannon Design
Todd Harpel
Leviton

PEER REVIEWED BY:

Brian Ensign
Superior Essex
Dave Weatherley
PageThink
Dennis Mazaris
Concert Technologies
Harold Jepsen
Legrand
Marc Goodman
Panduit
Marta Soncodi
TIA
Paul Vanderlaan
UL Solutions
Todd Stevenson
Ballinger

TABLE OF CONTENTS

I. Introduction 01

II. Physical Media and Assurance Testing 02

III. Wireless Coverage 08

IV. Expansion & Future Proofing/Readiness 14

V. Network Infrastructure Security 15

VI. Building Connectivity Resilience 16

VII. Conclusions and Takeaways: Benefits to the various stakeholders of the connectivity assessment 18

INTRODUCTION

Historically, Information Technology (IT) and multiple facilities management groups involved with Operational Technology (OT) existed in disparate silos, each with its own discrete networks, objectives, requirements, and security protocols. The Internet of Things (IoT) and the pervasive use of Ethernet technology are tearing down these old silos. Building system devices are now integrating on an IP (Internet Protocol) network, blurring the traditional line between IT and OT networks. This integration enables smart buildings to optimize operations, maintenance, overall investment, security, and occupant experience.

While the design of structured cabling infrastructure for IT business networks traditionally focused on voice and data connectivity and evolved to include many IP-based systems, smart buildings challenge the conventional methods of physically connecting the networks in the building. Well-established standards-based best practices for IT connectivity apply to smart buildings and enable the planning and installation of a structured cabling infrastructure without prior knowledge of all the systems or components that will be supported. However, this document recognizes that additional systems and devices are now connecting to the building network and IT and OT networks are collapsing onto one shared physical infrastructure. Designing a physical infrastructure that supports both IT and OT networks and accommodates many types of devices, services, placements, and users therefore also requires additional considerations and input from various stakeholders.

In a coordinated effort with numerous industry experts, the Telecommunications Industry Association (TIA) and Underwriters Laboratory (UL) created the SPIRE™ assessment and verification program. The SPIRE program sets forth metrics by which to gauge the ability of a building's systems, processes, and infrastructure to support, control, and optimize six key aspects of the facility's function: connectivity, health and wellbeing of occupants, life and property safety, power and energy consumption, cybersecurity, and sustainability. Of the facility's six areas of function, connectivity is of pivotal importance as it provides the connection between all the devices, sensors, systems, and occupants and allows them to communicate and integrate. Without a reliable and secure network, both wired and wireless, the data flow between the building's crucial functions that provide the advantage and benefits of being "smart" would not be possible.

The SPIRE Connectivity assessment criteria rewards the use of best practices and processes by weighting scores for each criteria set based on their ability to enhance a building's current functionality and operations, as well as facilitating the implementation of future improvements. The connectivity assessment criteria were developed in collaboration with industry leaders representing all aspects of smart buildings, including manufacturers, system designers, and property owners.

Due to the many varied environments and operational needs of facilities, there is no "perfect" score that will suit all facilities with their applications and deployments. The criteria questions were derived with the intent to help participants evaluate their current structural deployments and the processes by which a facility can be improved and maintained. Through the choice ranking system, participants' facilities are evaluated, while also providing examples of potential improvements for those not already deploying the latest technologies. Participants who are using the criteria as a tool to evaluate a facility for improvements are encouraged to give further consideration of the appropriateness of each technology for their projected needs.

PHYSICAL MEDIA AND ASSURANCE TESTING

PHYSICAL WIRED MEDIA FOR TRANSMITTING DATA WITHIN SMART BUILDINGS

For the purposes of this white paper, physical wired media is defined as the network components that comprise the structured cabling infrastructure that transmits data to and from active devices throughout the building and campus and optionally powers those devices via remote power technologies such as Power over Ethernet (PoE). This includes Wi-Fi access points (WAPs), antennae, and other wireless aggregation devices that use open air as a transfer medium but are physically connected to the network via wired media. The primary physical cabling media types for digital information transmission and power deliver within a smart building are classified into the following three categories.

COPPER CABLING

In commercial buildings, balanced twisted-pair copper cabling and connectivity is commonly used in horizontal building infrastructure to enable IP-based communications and the optional delivery of PoE to end devices. Category 6A is currently the highest performing four-pair copper cable recommended by industry standards for all new deployments and the preferred choice for addressing network bandwidth, PoE delivery, and functionality needs in the smart building.

The continued expansion of Ethernet into traditional OT applications has also given rise to Single Pair Ethernet (SPE) cabling systems that support low-speed data transmission to greater distances over a



single pair of copper wires with the option of delivering power. As a complement to four-pair copper cabling, SPE is becoming an economical alternative for connecting and powering low-bandwidth devices like IoT sensors, controllers, actuators, and meters over longer distances in smart buildings.

FIBER OPTIC CABLING

Fiber optic cabling comprised of glass uses wavelengths of light to transmit data, supporting much higher data rates over significantly longer distances compared to copper cabling. Fiber optic cabling also provides the benefit of reduced weight and volume due to their smaller cable dimensions. The dielectric nature of fiber optic cable also makes it more secure and not susceptible to electromagnetic interference (EMI) in harsh environments.

Fiber comes in multi-mode used primarily in shorter-reach data center applications and single mode that provides the highest potential bandwidth capacity at much longer distances. Traditionally used in campus and building backbones for Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN) connectivity, fiber optic cabling is being increasingly deployed in the horizontal building infrastructure as data generation and consumption continue to increase.

HYBRID OR COMPOSITE FIBER CABLES

Hybrid copper-fiber cables (sometimes referred to as composite cables) are comprised of both fiber strands for high-bandwidth data transmission and twisted or linear-laid copper conductors for centralized power or control signals to edge devices, as shown in Figure 1.

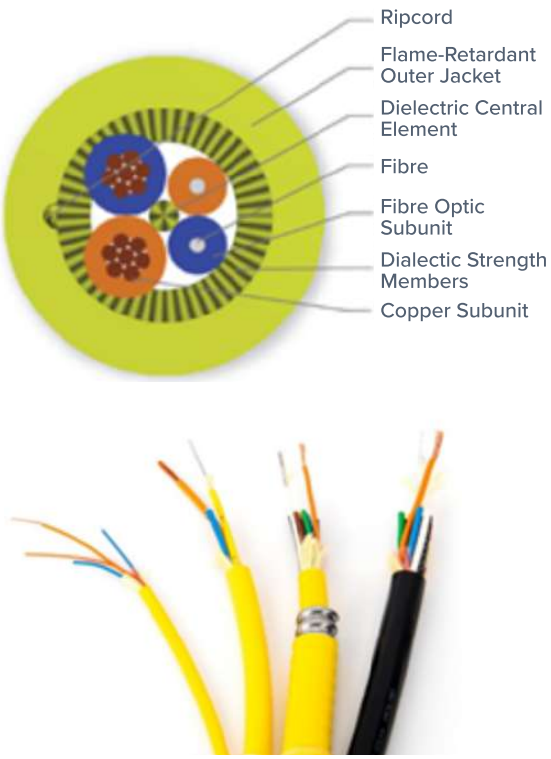

Figure 1. Hybrid Copper-Fiber Cable, Courtesy of Corning

CONNECTIVITY TO THE BUILDING

Incoming cabling from external service providers terminates in a building's Entrance Facility (EF) at the demarcation point on equipment owned by the provider. Beyond the demarcation point, the building owner/manager provides, maintains, and operates the building's network equipment and cabling, either via copper or fiber optic cable depending on the speeds and service levels supported by the service providers.

Generally, the more service providers that provide circuits to a building, the more reliable the services are to that building due to redundancy. The amount of bandwidth required to operate the building and support the applications needed to achieve smart building initiatives should be considered when determining the minimum contracted data transmission speeds and service levels from service providers.

BACKBONE INFRASTRUCTURE

Backbone infrastructure distributes service provider and carrier service to the building's Equipment Room (ER), or to multiple ERs in a campus environment, that house more sophisticated equipment to support the smart building network. From the building's ER, primary and optionally redundant backbone cabling connects to telecommunications rooms (TRs) throughout the building via a star topology. Single mode fiber optic cabling is the preferred main transport media for backbone infrastructure due to its greater transmission distance and bandwidth capabilities that enable transmitting high volumes of aggregated data from TRs. Forward thinking building owners typically install extra fiber strands (i.e., dark fiber) in their backbone cabling along with sufficient pathway capacity to accommodate future services and expansions.

HORIZONTAL INFRASTRUCTURE

Horizontal infrastructure connects devices and work area outlets at the edge to the smart building network. Horizontal cabling can be either copper cable or fiber optic cable. As the highest-performing and recommended twisted-pair copper cabling, Category 6A cable supports up to 10 Gbps data transmission speeds simultaneously with up to 90 Watts (W) of PoE to a distance of 100 meters (m), making it ideal for connecting and powering devices such as Voice Over IP (VOIP) telephones, WAPs, IP cameras, and many other devices.

SPE cables can also be used in the horizontal infrastructure for connecting lower-bandwidth devices, such as IoT sensors, controllers, actuators, and meters used in HVAC, air quality, waste management, lighting, security, and other smart building control systems. It supports transmission speeds up to 10 Mbps to a distance of 1000 m. SPE technology improvements under development within IEEE are expected to support higher transmission speeds and support multi-drop topologies (i.e., multiple devices on the same link) that are more in line with traditional building automation system topologies.

Due to its bandwidth capabilities, fiber optic cabling enables horizontal infrastructure to be future ready, substantially reducing the need to rip-and-replace with every technology refresh. While fiber cannot deliver power, hybrid copper-fiber cabling combines the benefit of fiber's bandwidth and distance capabilities with the power-carrying capability of copper conductors. The bandwidth and distance capability of fiber is especially important when considering implementation and migration to very high bandwidth applications. Fiber cabling in the horizontal infrastructure can also accommodate point-to-multipoint passive optical technologies.

PASSIVE OPTICAL INFRASTRUCTURE

A passive optical LAN (POL), also referred to as a Gigabit Passive Optical Network (GPON), is a point-to-multipoint fiber architecture that originated in the residential Fiber to the Home (FTTH) world. Rather than a traditional star topology with fiber backbone infrastructure connecting telecom spaces and copper horizontal infrastructure connecting devices, a POL extends single-mode optical fiber cabling directly from an Optical Line Terminal (OLT) in the ER to Optical Network Terminals (ONTs) at the edge of the network that connect to individual devices. This is achieved via passive optical splitters that distribute signals from one optical fiber to two or more fibers.

In a POL, the distinction between backbone cabling and horizontal cabling is blurred. Because POL architectures utilize high-bandwidth single mode fiber optic cables that offer virtually unlimited bandwidth, only the OLTs and ONTs need be upgraded to support future higher-speed transmission. Additionally, the POL architecture can support multiple networks and speeds running over the same fiber optic cables, allowing multiple building system networks to utilize the same physical cabling infrastructure and supporting network segregation.



NETWORK-BASED POWERING OPTIONS

Networked devices that require power are not always located near a convenient AC power outlet or other power source. Consequently, there are a variety of remote power delivery options for delivering DC power to network-connected devices via Class 2 limited-power circuits. Class 2 power can be delivered via twisted-pair copper cables in the form of PoE or Single-pair PoE (SPoE) or via copper conductors in a hybrid copper-fiber cable. Power can also be delivered to devices via newer fault managed power (FMP).

PoE provides the benefits of a regulated power source via category cable, while eliminating the need to install an AC power outlet near the device. As powering demands increased, PoE evolved from being delivered over two pairs of a category cable to four pairs, enabling higher wattage to support a broader range of devices such as WAPs, LED lights, and video displays. Higher PoE levels also allow for more features.

For example, a simple surveillance camera can operate via Type 1 PoE, while a pan-tilt-zoom camera may require Type 2 PoE, and an outdoor thermal (heated) camera may require Type 3 PoE. With higher power levels comes concern over efficiency and increased heat generation and signal loss, which can be mitigated by limiting cable bundle sizes, using UL Limited-Power (LP) rated cables, or using larger gauge conductors.

Power can also be delivered in SPE applications to power low-speed control devices. Due to the tremendous popularity of PoE, single-pair powering technology has been commonly identified as SPoE. However, SPoE employs different powering methods than PoE. Table 1 lists the IEEE twisted-pair powering standards, their power levels, and delivery method.

IEEE STANDARD	NAME	MAXIMUM POWER FROM SUPPLY	MAXIMUM POWER TO DEVICE	POWER DELIVERY PAIRS
IEEE 802.3af	PoE/Type 1	15.4 W	12.95 W	2/4-pair
IEEE 802.3at	PoE+/Type 2	30 W	25.5 W	2/4-pair
IEEE 802.3bt (Type 3)	PoE++/Type3	60 W	51 W	4-pair
IEEE 802.3bt (Type 4)	PoE++/Type 4	90 W	71.3 W	4-pair
IEEE 802.3cg	SPoE	79 W	52 W	1-pair

Table 1. IEEE twisted-pair powering standards

A hybrid copper-fiber cable can also be used as a Class 2 limited-power circuit along with the added benefit of providing significant bandwidth to edge devices to distances far beyond the maximum 100 m reach of traditional twisted-pair copper cables. The distances that a hybrid copper-fiber cable can deliver power is a function of the required power of the device and the gauge of the copper conductors, with larger gauge conductors able to carry power farther distances. Power is delivered over the copper conductors via centralized power supply units, which simplifies power management and back-up for edge devices. If a hybrid-copper fiber cable cannot connect directly to a device, media conversion equipment that connects and powers the device via twisted-pair category cabling up to 100 m may be required.

Another way to power devices is a new generation of power distribution called fault-managed power. Fault-managed power can supply up to 2000 Watts or reach distances of 2000 m, depending on the power level. Defined as Class 4 power within the National Fire Protection Association's (NFPA) 2023 National Electric Code (NEC), fault-managed power provides more power but intelligently limits the amount of energy that can go into a fault, making it as safe as Class 2 power. Cables used for delivering fault-managed power include two- and four-conductor copper cables and hybrid copper-fiber cables. Like Class 2 limited-power systems, power demands and delivery distances will dictate the size of the copper conductors.

TESTING AND INSPECTION

It is important to know the performance of the cabling media so that future technology implementations may be simpler and more manageable. This can be achieved by testing the infrastructure for compliance to applicable cabling standards and current and future application standards, as well as maintaining documentation of the test results for future review. Power distribution over twisted-pair copper cables and hybrid copper-fiber cables that are gaining acceptance and traction rely on certain performance characteristics that that may not be visually apparent, requiring more in-depth verification.

Assuring performance of any network requires industry standards compliance testing of Pass/Fail performance parameters for twisted-pair category cabling, with a strong recommendation for testing additional parameters for smart buildings as outlined in Table 2. Measurements such as pre-qualifying the link's ability to support the PoE load can help assure operation, particularly for devices requiring higher wattages such as digital lighting. Additionally, testing on live links under both traffic and PoE load may help reveal any undesirable electromagnetic interference and thermal impacts on network performance. By performing comprehensive testing, concerned parties will have increased confidence that the infrastructure can support the intended applications.



Once the IP components are installed and performance verified for all IP-enabled applications, the responsibility to manage and keep the network up and running is turned over to the network manager, integrator, or building owners.

With multiple building systems converging on the network, traditional IT and OT roles need to work together to ensure the physical network infrastructure is capable of optimal system performance, while providing headroom for connecting more devices in the future.

	ANSI/TIA 1152-A PASS/FAIL PARAMETERS	ANSI/TIA 1152-A OPTIONAL PARAMETERS	TIA 1152-A ADDITIONAL PARAMETERS	ADDITIONAL TESTING FOR SMART BUILDINGS
PARAMETERS	Length, Delay, DC Loop Resistance, Insertion loss, Return Loss, NEXT, PSNEXT, ACRF, PSACRF	TCL, ELTCTL, DC Resistance Unbalance	TDR to Fault Location for RL, NEXT, Shield, ACRN, PSACRN, Impedance	2.5/5/10BASE-T PoE 802.3 af/at/bt SPoE 802.3cg Other Class 2 circuits (e.g., hybrid fiber)
USE CASE	Cabling Standards Compliance	Recommended for noisy environments, 10GBASE-T, and PoE	Fault Identification	Application Assurance (i.e., live links under traffic and power load)

Table 2. Copper Twisted-Pair Testing, Courtesy AEM Test

THE WIRED IN WIRELESS

Existing traditional wireless bandwidth consumption, combined with the integration of numerous wireless IoT devices, can create bottlenecks between network switches and WAPs. Current enterprise-grade Wi-Fi 6/6E WAPs can reach theoretical speeds up to 9.6 Gbps and Wi-Fi 7, currently under development, is expected to reach speeds of up to 40 Gbps. The cabling infrastructure to connect WAPs should therefore meet or exceed those speeds. This can be accomplished by deploying multiple category cables to WAPs. Industry standards currently recommend connecting Wi-Fi 6/6E WAPs with a minimum of two Category 6A cables that each support speeds up to 10 Gbps and PoE up to 90 W.

Multi-mode or single mode fiber with its substantial potential bandwidth can be used as WAP capacity requirements continue to increase. As previously mentioned, power can be delivered to the WAPs via hybrid copper-fiber cable or via local AC power. For networks requiring high bandwidth, low latency, or a combination of the two, single mode fiber may be the better option to support systems such as in-building cellular, 5G, and Citizens Broadband Radio Service (CBRS), or Private LTE. If your IoT project requires the rollout of Wi-Fi 6/6E, pre-existing Category 6 or lower performing twisted-pair cabling will need to be verified.

WIRELESS COVERAGE

The demand for in-building wireless has been growing steadily for decades to the point where 80% of wireless data traffic originates indoors, according to a widely-cited statistic. As buildings get smarter, occupants often utilize building apps or applications installed on mobile devices to access building services, adjust environmental comfort settings, or take advantage of more flexible space usage. Smarter building management systems also support additional functionality for building engineers in the field including using QR codes, augmented reality (AR) overlays, and digital twins to understand in real time what is happening with building equipment. All these scenarios involve accessing building information from wirelessly-connected laptops, tablets, or smartphones. At the same time, low-power, low-speed wireless IoT sensor devices throughout a smart building are becoming increasingly vital for monitoring and maintaining building performance.

Demand for seamless wireless connectivity throughout smart buildings will continue to increase, calling for adoption of a universal wireless approach via a blend of technologies that include cellular (public and private), Wi-Fi, and short- and long-range low-power wireless, or a combination thereof.



IN-BUILDING CELLULAR

Cellular wireless connectivity was originally serviced mostly through carriers, referred to a Mobile Network Operators (MNOs). The biggest limitation of this model is that carriers are funding less and less enterprise cellular systems. Other limitations, like installation logistics, MNO funding, and bring-your-own-device (BYOD) policies, provided incentives for building owners to install and fund their own in-building wireless infrastructure. MNOs still have an important part to play as they typically need to provide the cellular signal source for enterprise-funded systems.

Neutral Host Providers (NHPs) have emerged as an alternative in providing enhanced wireless service in targeted buildings and venues across several enterprise verticals, like transportation (e.g., airports and rail hubs), entertainment (e.g., stadiums and arenas), civic and convention centers, healthcare, hospitality, and higher education. As NHP Distributed Antenna Systems (DAS) solutions gained adoption for in-building cellular, NHPs began offloading data traffic to contracted Wi-Fi network operators, as well as MNOs servicing Wi-Fi along with cellular service. The NHP typically owns and operates the in-building wireless infrastructure and signs long term leases with multiple MNOs. In addition to managing Capex procurement and funding, the NHP also assumes the operations role that includes management of building/venue owner relationships, renting equipment room space, upgrading power/HVAC/physical security, and monitoring, and maintaining the wireless infrastructure.

REPEATERS, DAS, AND SMALL CELLS

Repeaters, also known as signal boosters or bi-directional amplifiers, are passive systems that use donor antennas to boost and transmit nearby cellular signals via copper cabling to internal antennas that broadcast the signal throughout the building. Repeaters depend on the quality of the original signal and are typically serviced by single operators. They are not typically adequate for providing coverage in larger buildings.

DAS solutions can be operated as neutral hosts, allowing multiple MNOs to provide cellular service via a common wireless infrastructure. Signal source for a DAS can be an on-site Base Transceiver Station (BTS), or a small cell that offloads carrier traffic. Historically passive and relying primarily on copper cabling, DAS solutions are now active systems that improve coverage and capacity via single mode fiber, with hybrid copper-fiber cable often used to connect and power antennas throughout the building.

With exponential data traffic, there is increased demand for coverage and capacity. Indoor deployments based on small cells have gained momentum, both for 4G-LTE and more recently for high-speed 5G cellular. Unlike DAS systems, indoor small cell solutions are more convenient to install and maintain, and they also enable advanced features like location-based services. Small cells typically do not support the neutral-host, multi-operator model utilizing a shared infrastructure.

While NHPs or building owners can fund the wireless infrastructure and charge mobile operators for utilizing the network, MNOs can utilize their dedicated 5G spectrum bands for indoor deployments (e.g., location-based services), not supported by DAS. These systems can also be leveraged by enterprises that are planning to own and operate private cellular networks (i.e., CBRS/ private LTE).

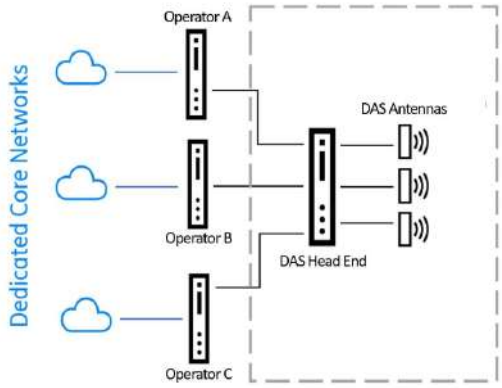

Figure 2. Classical Architecture of a Neutral Host Active Distributed Antenna System

PRIVATE CELLULAR NETWORKS

Private cellular networks like CBRS operates in an unlicensed band of frequency, allowing enterprises to gain the advantage of today's carrier-grade 4G LTE and 5G cellular connectivity. In a private cellular network, the enterprise controls its own radio assets, data, and operations, which is ideal for those with large numbers of fixed IoT devices, such as a university. Private cellular networks have also presented a new opportunity for neutral host owners who are now positioned to provide indoor coverage and infrastructure for mobile operators. In this scenario, mobile operators connect their core network to the shared network, allowing them to share the spectrum with other operators. At the same time, building owners can benefit from deploying CBRS as a dedicated private network.

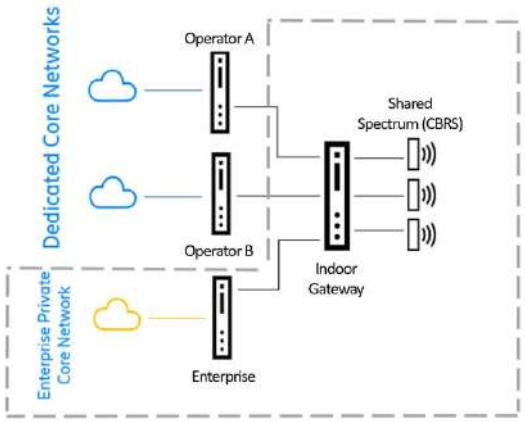

Figure 3. Shared private network

WI-FI NETWORKS

Wi-Fi is a LAN-based wireless application operating within an unlicensed frequency spectrum that is an essential element of a smart building's connectivity infrastructure.

With sustained efforts by IEEE on 802.11 WLAN (Wireless Local Area Network) standardization, as well as Wi-Fi Alliance efforts on interoperability, security, and promotion, Wi-Fi solutions continue to improve in terms of transmission speed, latency, range, capacity, and security. The explosion of IoT devices in everyday life adds continuous demand for simultaneous wireless connections over wider ranges, while high-resolution video streaming and Augmented Reality/Virtual Reality (AR/VR) applications drive the need for higher speeds and lower latency.

As shown in Table 3, the most commonly used IEEE 802.11 WLAN standards have evolved over the past 20 years to support a wider range of applications, improve speed, and optimize the number of simultaneous connections, capacity, and latency while generally maintaining backwards compatibility to accommodate longer technology refresh cycles. Wi-Fi 7 is still new, with devices just starting to be developed. Wi-Fi 6/6E is the latest Wi-Fi technology, with Wi-Fi 6E adding operation in the 6 GHz spectrum for increased bandwidth to support high-speed applications such as high-definition video streaming. Because the 6 GHz spectrum is less crowded, Wi-Fi 6E can also support backhaul for high-density IoT sensor networks and enhance coverage for larger, heavily-populated spaces (e.g., arenas).

IEEE STANDARD IDENTIFIER	WI-FI ALLIANCE VERSION	FREQUENCY BAND	# OF CHANNELS	CHANNEL WIDTH (MAX)	MAX DATA RATE	DATA CABLING REQUIREMENT (MINIMUM)
802.11n	Wi-Fi 4	2.4 & 5 GHz	4	40 MHz	600 Mbps	Cat 5e
802.11ac	Wi-Fi 5	5GHz	8	80 MHz	1.3 Gbps	Cat 5e
802.11ax	Wi-Fi 6	2.4 & 5 GHz	14	160 MHz	9.6 Gbps	Cat 6A
802.11ax-2021	Wi-Fi 6E	2.4, 5 & 6GHz	21	160 MHz	9.6 Gbps	Cat 6A
802.11be	Wi-Fi 7	2.4 & 6GHz	16	320 MHz	30 Gbps	Three Cat 6A or SM Fiber

Table 3. IEEE 802.11 Wi-Fi Protocol Versions Summary

LOW-SPEED, LOW-POWER WIRELESS NETWORKS

Traditional remote sensing devices used in industrial Machine-to-Machine communications have long communicated via cellular networks. The implementation of a new generation of wireless IoT sensing devices to acquire actionable data needed to achieve smart building initiatives helps build the “data” bridge that closes the IT-OT divide.

These devices are characterized by infrequent and small amounts of data transfers and prolonged battery operation. They can communicate via short-range or long-range wireless. Deployments can be small-scale with just a few devices, or they can be high density and cover vast areas.

SHORT-RANGE WIRELESS

There are a variety of available short-range wireless technologies, including Bluetooth Low-Energy (BLE), Zigbee, and RFID. These technologies are primarily deployed for specific applications such as device-to-device communications and monitoring and tracking systems for warehouse inventory, mobile payment, wayfinding/proximity marketing, access control card readers, indoor location services, patient health monitoring, and asset tracking. They can also be used for energy metering, climate control, smoke detection, and other sensor communications.

BLE is a low-cost, power-saving variant of Bluetooth with long battery life that transmits in the 2.4 GHz frequency band for exchanging data in device-to-device communications, as well as mesh communications to support larger-scale device deployments. The latest version, BLE5, can transfer data up to speeds of 48 Mbps to about 50 m indoors with longer distances outdoors. Readily available across a wide range of devices, Zigbee transmits in the 2.4 GHz frequency band, up to about 20 m and speeds of 250 Kbps using a central hub, with the ability to support unlimited hops between thousands of devices. Its shorter range makes it better suited for smaller facilities.

RFID is another short-range wireless technology that captures data encoded in RFID tags that contain an integrated circuit and antenna.

RFID tags are typically attached to an asset for applications like inventory management, equipment and patient tracking in healthcare, electronic parking gates, and anti-theft in retail.

LONG-RANGE LOW-POWER WIRELESS

Long-range low-power wireless (LPWAN) connectivity is ideal for transmitting small amounts of data over much longer distances from large numbers of IoT sensing devices serving a wide area, such as an apartment complex, large retail store, healthcare facility, higher education campus, business campus, manufacturing/shipping facility, or warehouse. Depending on the application, LPWAN sensing devices can use unlicensed spectrum, with deep penetration indoors and underground. Devices can have a 10-year battery life and be installed in remote or hard-to-reach areas. In addition, these devices are conveniently monitored and operated remotely via gateways placed in a star topology that can leverage wireless or wired backhaul infrastructure to send data to the cloud for complex analytics and operations. The flexibility of LPWAN hardware and connectivity enables IoT use cases such as utilities monitoring and management, occupant wellbeing, safety and compliance initiatives, and facilities management as shown in Figure 4.



Figure 4. LPWAN Use Cases for Smart Buildings. Courtesy of Comcast's MachineQ

LPWAN technology includes cellular-based NB-IoT and LTE-M that can be supported by all variants of LTE cellular service, with different variants of LTE optimized for certain use cases. For example, consumer LTE (designated as CAT-4 and above) can be used for high-bandwidth IoT applications such as 4K high-resolution surveillance cameras. These high-bandwidth applications require more power via a fixed power source compared to other IoT devices that operate on battery power. New narrowband mobile IoT technologies such as LTE CAT-M1 and CAT NB-IoT support applications with less complexity and power needs as shown in Figure 5. A comparison of the range, coverage, battery life, speed, latency, and mobility between LTE CaT-M1 and CAT NB-IoT are shown in Table 4.



Figure 5. LTE evolution scales to meet the diverse needs of IoT.[1]

[1] https://www.telit.com/resources/whitepapers/designing-cellular-iot-devices-for-battery-life/

ATTRIBUTE	LT-ME/CAT-M1	NB-IOT
RANGE	1 km Urban / 10 km Rural	1 km Urban / 10 km Rural
INDOOR COVERAGE	Yes	Yes (slightly better than LTE-M)
BATTERY LIFE	Several Years	Several Years
MAXIMUM SPEED	1 Mbps in both directions	26 Kbps downlink / 62 Kbps uplink
LATENCY	10 – 20 ms	1.6 – 10 ms
MOBILITY SUPPORT	Good, with handovers supported	Poor, with handovers not supported

Table 4. LTE CaT-M1 and CAT NB-IoT range, coverage, battery life, speed, latency, and mobility

One non-cellular LPWAN technology gaining traction globally is LoRaWAN® (Long Range Wide Area Network), an ITU-T open standard network protocol based on unlicensed spectrum and supported by the LoRa Alliance®. LoRaWAN devices can have ultra-low power consumption, mitigating the need for a wired power supply, which is often a barrier in IoT deployments. Battery-powered LoRaWAN devices can last years in the field and can be deployed almost anywhere in a building with minimal disruption. While low power consumption comes at the expense of bandwidth, most IoT sensors only need to transmit small data packets, such as a flow measurement or temperature reading. LoRaWAN also operates in lower frequency bands, providing excellent immunity to interference and the ability to penetrate walls and dense building materials, such as metal and concrete.

BLENDED WIRELESS FOR THE SMART BUILDING

No single wireless technology can address all requirements in a smart building. Public and private cellular, Wi-Fi, and short-reach and long-reach low-power wireless work alongside each other in a complementary way to meet a wide range of smart building applications. Often, these technologies work in tandem as part of a multi-protocol strategy. For example, LoRaWAN can be used extend to the range of a BLE-based IoT solution. Devices like LED lights and WAPs are also increasingly integrating BLE and Zigbee radios to help building operators simplify the deployment of location-based services.

Figure 6 below is a simple classification of most available wireless IoT technologies and provides a comparison based on key attributes such as range, bandwidth, and battery power.

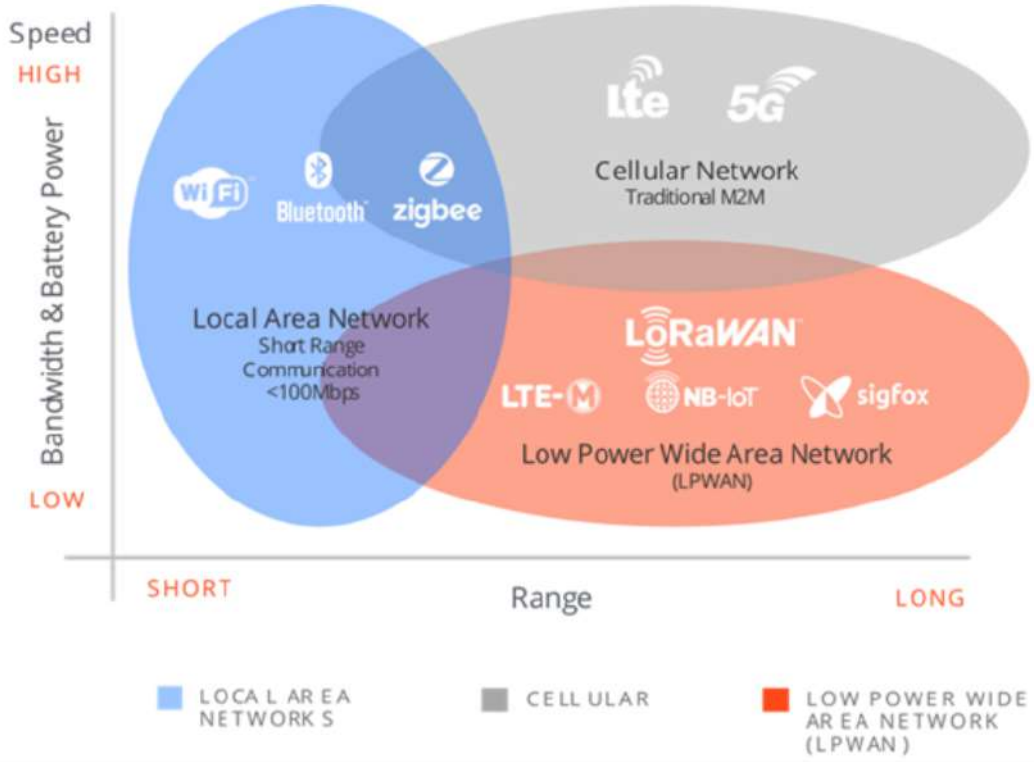

Figure 6. Wireless technologies comparison, Courtesy of Comcast's MachineQ

EXPANSION & FUTURE PROOFING/READINESS

A robust network infrastructure is the most critical aspect of a smart building, as it encompasses the physical and logical connectivity between all the devices, sensors, and systems. With the rapid pace of technology improvements, the definition of a smart building also evolves quickly and is determined by new applications, improved devices, and systems availability. The ability to upgrade, expand, and connect previously siloed systems will be critical for the owners of smart buildings.

Developing a smart building strategy early in the decision process is key for planning and implementation of connectivity that allows for growth and expandability. Considerations for future proofing should be part of the evaluation process, even if the funding or design does not warrant the approach on day one. At a minimum, the impact of future expansion upon pathways and spaces should be evaluated as future rework can incur considerable investment and disruption to a facility.

It is advantageous for building stakeholders to develop a strategy before defining the objectives of a project, the expected benefits of the applications to be implemented, and how the applications will impact the project's evolution. It is usually preferable to have a future-proof network than to re-cable the building after occupancy. The impacts to the various stakeholders, including time, materials, and investments could be significant. Additionally, upfront investment in the cabling infrastructure can make it easier to manage future technology implementations of PoE, Wi-Fi, and other technologies by allowing simplified endpoint equipment upgrades. As an example, deploying dark fiber in predetermined areas could improve building future-readiness if bandwidth-intensive applications are expected to be deployed.



New technologies used in future applications will enable improved building efficiency, smarter functionality, a more collaborative environment, and less power usage, resulting in a better occupant experience, reduced carbon footprint, and an eco-friendlier building. To specify the current and future requirements for applications, building stakeholders (e.g., owner integrator, system designer) must continually define and evaluate short- and long-term future needs. A structured and periodic technology assessment program can assist in the evaluation of the needs, the development and review of roadmaps, and review of recent technological and standards developments to maintain or improve the property's performance. It is not merely about specifying the technologies required, but also the need to define the magnitude of upgrades needed for future expansion.

NETWORK INFRASTRUCTURE SECURITY

Smart buildings must assist in ensuring the physical safety of their occupants, while maintaining a level of security around the network and its physical infrastructure, including pathways and spaces (e.g., telecom spaces, wall-mount cabinets). Connectivity to the network infrastructure in a smart building enables the systems, sensors, controls, and intelligent control platforms to communicate with one another. Without a secure, proactively monitored, always-on, resilient communication network, the various components and systems in the building are susceptible to network compromises. These compromises can lead to acts such as ransomware, data breaches, user identification loss, or end devices used to hijack sensors, devices, and buildings systems.

The security of the network is paramount to ensuring that critical building functions can provide for uninterrupted operation. If the smart building network is compromised in any way, the resulting interruption in control or potential operational failure could pose a wide range of risks, including inconvenience, cost to the enterprise, serious life safety threats, cybersecurity vulnerabilities, and damage to the operators' reputation. This holds true for any business, whether that be a corporation, healthcare provider, university, building owner or any other entity that safeguards data and building operations. In addition, an interruption in network operations due to unauthorized usage or control can cause network outages ranging from hours to several weeks, depending on the type and level of the compromise and the severity of damage inflicted on the network and stored data.

From a physical network standpoint, SPIRE assessment evaluates the degree to which wiring closets, equipment rooms, pathways, and other key connection points are properly secured, monitored, and tracked, with appropriate measures for granting access.

This includes a riser management system that controls, monitors, and documents access and changes made in the building's riser system that connects telecom spaces, including those that may be occupied by different tenants.

The program also evaluates whether real-time client or asset tracking systems are deployed. These systems may be used to perform multiple functions such as identifying the location of critical assets or individuals in time of need, provide marketing information on consumer behavior, or vehicle tracking in parking facilities. This identification process can provide first responders with accurate information for life safety requirements. Tracking systems can leverage various wired and wireless technologies to support real-time locating systems (RTLS).

Building OT, such as HVAC control, energy management systems, water use monitoring and control, and even waste monitoring are assessed on whether they are segmented from the building owner's primary business data network. This can be achieved physically using a parallel cabling infrastructure or wireless network, or using network security practices, such as firewalls and virtual private networks (VPNs). Segmentation helps to ensure that critical business functions on the IT network are protected from potential interruption caused by facilities staff access to IT equipment or cybersecurity vulnerabilities of OT devices, such as a Denial-of-Service Attack (DoS), and vice versa. It also ensures the critical building functions controlled by the building management system are not subjected to potential data flow interruption caused by Quality-of-Service (QoS) parameters that may prioritize throughput for business-critical or life safety applications. Device detection is another important aspect of physical network security, providing instant notification through alerts and alarms when an unauthorized/rogue device is connected to the network.

Similarly, to protect network security and bandwidth provisioning, SPIRE evaluates the degree to which IT and OT networks, as well as tenant and guest wireless networks are separated. It is recommended that guest Wi-Fi networks be isolated from the primary business network and password protected with the latest encryption technology. For example, guest-specific log-on credentials with specified validity timeframes and limitations on ports allowed (i.e., access to applications, services) are more secure than open enterprise LAN or Wi-Fi networks.

It should be noted that SPIRE's Connectivity assessment criteria does not address Cybersecurity. This is addressed as its own separate SPIRE criteria. However, the physical security of the network infrastructure, endpoints, and end-devices used in smart buildings is equally important and plays a key role in helping to prevent cybersecurity attacks.

BUILDING CONNECTIVITY RESILIENCE

Building connectivity resilience that includes reliability, availability, and redundancy is required to support Service Level Agreements (SLAs), sustainability, and business continuity. It is a requirement for commercial facilities across all verticals, including enterprise, healthcare, hospitality, education, entertainment, and others.

RESILIENCE REQUIREMENTS EVALUATION

Resilience considerations start with a general assessment of business continuity dependent on internal and external connectivity infrastructure. This covers building systems inventory of critical and non-critical systems for business continuity and includes cabling, available power capacity, and security, as well as identification of on-call support and contact information for service providers. Specifying resilience requirements and justifying the investment of implementing appropriate levels of resiliency should be based on the business needs and building objectives.[2] It can also help evaluate the ability for the building to stand alone (i.e., self-healing or able to continue critical operations) if there is a loss of some or all services with disaster recovery requirements.

CRITERIA AND DESIGN CONSIDERATIONS

Building infrastructure resilience allows the building to adapt, recover, stand alone, and maintain critical and non-critical operations. Smart building connectivity infrastructure should have the necessary flexibility and adaptability to provide uninterrupted system operations during and after an unforeseen event or scheduled maintenance. Resilient infrastructure design factors to consider include:

- Infrastructure complexity versus serviceability and security
- Cost considerations for design and implementation, ongoing support and service, value engineering (original versus actual), and Capex versus Opex cost structure
- Degree of redundancy, both logical and physical, with avoidance of critical single points of failure that can cause widespread outages
- Power considerations, such as type (i.e., AC vs. DC), power backup (e.g., UPS, battery, generators), source (e.g., provider, self-generated), redundancy, and remote power delivery application (e.g., Class 2 power via PoE, SPoE, or hybrid copper-fiber cable or Class 4 fault-managed power)
- Monitoring considerations, such as proactive (real-time) or reactive (incident-based)
- Occupant use and interaction with building technologies using mobile or fixed applications
- OT-IT network separation and cyber protection

IMPLEMENTATION RECOMMENDATIONS

Resilience is a core capability in business continuity, especially in vertical-specific situations where a lack of back-end connections and disaster recovery paths could impact delivery of essential services and business continuity. As a general approach, building connectivity resilience should be incorporated in the project lifecycle, starting with the design phase. Risk management using diverse pathways for infrastructure is generally considered good practice. In general, allowing diverse pathways for all building utilities (e.g., connectivity, power, water/wastewater) protects the overall building system in case of a segment failure.

Resilience is managed with critical infrastructure operations that include proactive surveillance, stress test of facilities, condition monitoring, and incident response and recovery. Operational support functionality could also include reset state, safe mode, high-level of fault tolerance and self-healing, diagnostic support, and degrading performance indicators. These need to be considered against business needs and goals because they can represent a significant investment and add system complexity.

PROCESS CONSIDERATION

Building resilience relies on people and processes, starting with well-defined and understood roles and responsibilities for all business functions. Activities that ensure building resilience include backup and recovery of critical systems, equipment (spares), operating systems, and data operations. Preparedness is ensured with event response practice, plan review, and both scheduled and unscheduled drills. This includes Virtual Tabletop Exercises (VTTX), dry runs, fire drills, and preparing for response to various potential events, from power outages to natural disasters and pandemic outbursts. Good practice also calls for reviewing lessons learned after an event, such as the Hotwash after-action debriefing used by the Federal Emergency and Management Association (FEMA). The importance of testing a system for the failover processes is key to the resilience lifecycle, with constant improvement and refresh as needed to sustain business continuity.



[2] https://resilienceshift.org/wp-content/uploads/2017/10/046_Resilience-Return-on-Investment.pdf

CONCLUSIONS AND TAKEAWAYS: BENEFITS TO THE VARIOUS STAKEHOLDERS OF THE CONNECTIVITY ASSESSMENT

Connectivity is the most essential utility of a smart building and is the foundation to optimize all other aspects of a smart building. The entire ICT industry gains significant business opportunities from an effective smart building assessment program that considers the importance of connectivity as it relates to the entirety of the building. These benefits cross the entire spectrum of the ICT industry—from designers, installers, and consultants, to manufacturers, service providers, and integrators

- **Smart Building system architects, designers, integrators, and consultants** can leverage assessment criteria to ensure smart building performance for their customers, to collaborate with other stakeholders (e.g., mechanical (HVAC), electrical, plumbing, lighting, security, audiovisual, etc.), and to position themselves as subject matter experts and trusted advisors in the smart building design, specification, and construction process.
- **Manufacturers of cabling, connectivity, equipment, and devices** can leverage assessment criteria to demonstrate their expertise and enhance their industry stature by driving best practices for the deployment of standards-based high-performance infrastructure. They can help their customers make informed decisions surrounding equipment, devices, and solutions that enable low-latency data transmission, wireless coverage, physical security, cybersecurity, and power and environmental monitoring and control.
- **Managed service providers and cloud solution providers** can leverage smart building data and SPIRE assessment results to develop and deliver innovative platforms, software, and services that optimize building intelligence to manage, monitor, control, and safeguard devices, systems, and information.
- **Service providers and integrators** can leverage the assessment criteria to provide recommendations for the deployment of critical communications infrastructure and technologies that support smart buildings and enable digital transformation, ultimately establishing the foundation for smart, safe eco-friendly buildings, smart cities, and a myriad of emerging applications.

INDUSTRY RESOURCES

- ANSI/TIA-568 Balanced Single Twisted-pair Telecommunications Cabling and Components Standard
- ANSI/TIA-862- Structured Cabling Infrastructure Standard for Intelligent Building Systems
- TIA-5017 – Telecommunications Physical Network Security Standard
- BICSI 007 - Information Communication Technology Design and Implementation Practices for Intelligent Buildings and Premises.
- IEEE 802.3at/bt/bu/cg remote powering standards (PoE, PoDL, and SPoE)
- IEEE 802.11 series of Wi-Fi standards
- Wi-Fi Alliance
- GSMA
- LoRa Alliance

BRIEFING PAPER



THANK YOU

TIA SMART BUILDING PROGRAM SPONSORS

AECOM

CORNING

Comcast Smart Solutions