The role of data networks in smart buildings

What are smart buildings and why are they important?

Alcatel·Lucent Enterprise

White Paper

Table of contents

Overview

Governments and municipalities have been driving the evolution of smart city technologies for sometime in a quest for operational cost savings, energy consumption optimisation, as well as other intangible goals such as increasing public employee productivity and improving citizen wellbeing.

Today, with the threat of **climate change** and the large-scale problems derived from it, **sustainability** has become one of the main drivers for smart cities and smart buildings.

Ongoing migration from rural areas has resulted in 57% of the world's population living in urban areas and cities[1] accounting for 75%[2] of the global energy demand worldwide. Clearly, cities are important participants in the bid to attain sustainability levels as set by the international protocols and agreements signed in Kyoto and Paris. Buildings make up a significant part of a cities' footprint, and as such, smart cities are tightly linked to how their buildings perform in the context of energy consumption and optimisation. According to recent studies, buildings and the building construction sector account for 39% of global energy-related carbon emissions.[3] Therefore, greener buildings capable of optimising energy consumption and reducing CO2 emissions can greatly contribute to the fight against climate change.

Artificial Intelligence (AI) has become critical driver in the advancement of smart buildings. AI technology optimizes energy consumption, enhances security, and improves occupant comfort and productivity. By analyzing data from sensors, AI algorithms can make real-time adjustments to HVAC systems, lighting, and other building operations, leading to significant energy savings and a reduced environmental footprint.[4]

A smart building makes occupants more comfortable, safer and productive, at the lowest operational cost and with minimum environmental impact. An example would be a building able to automatically regulate the inside temperature and lighting in different areas, in a dynamic way, based on actual occupancy and on external weather and light conditions. This simple use case, exemplifies how the objectives of energy efficiency[5] and occupants' increased comfort and productivity can be achieved with minimum operational effort.

Another example is a building that can monitor occupancy levels and record how people are moving and gathering inside. Imagine facility managers being able to establish occupancy levels per area in a building, receive alerts automatically when the number of people exceeds a threshold, and have the ability to trace close contacts of a specific person, if necessary. These services can be further enhanced with Artificial Intelligence by providing predictive insights and automated responses to optimize building performance and safety.[6]

Smart buildings can use information and communications technology to connect a variety of subsystems to enable them to share information to improve building performance and operations. With automation, smart buildings can make decisions and execute actions with the objective of optimising energy consumption and increasing the comfort and safety of its occupants. Connectivity and automation are key components.

1 https://www.statista.com/statistics/270860/urbanization-by-continent/#:~:text=In%202023%2C%20the%20degree%20of,population%20residing%20in%20urban%20areas
2 https://unhabitat.org/topic/urban-energy#:~:text=Urban%20areas%20require%20an%20uninterrupted%20supply%20of%20energy%2C%20consuming%2075%25%20of%20global%20primary%20energy.
3 https://worldgbc.org/advancing-net-zero/embodied-carbon/
4 https://green.org/2024/01/30/artificial-intelligence-and-machine-learning-in-smart-buildings/
https://green.org/2024/01/30/the-future-of-building-automation-insights-from-industry-leaders/
5 Note: It is estimated that the energy consumption of an office building can be reduced by up to 30% through smart building automation.
What is the difference between smart homes and smart buildings? https://smarthomescope.com/smart-home-vs-smart-building/
6 https://green.org/category/artificial-intelligence/

Smart building technology

Buildings are very complex structures, consisting of many different subsystems, including:

- Heating, ventilation, and air conditioning (HVAC)
- Lighting control system
- Fire alarm system
- CCTV and video surveillance system
- Access and occupancy control system

Main elements

A smart building must be able to manage and control the different subsystems centrally, and to orchestrate their operation based on global objectives. In addition to the subsystems, smart building can also be identified by their three key elements: a Building Management System, Internet of Things (IoT) devices, and a data network.

The first key element of a smart building is the **Building Management System (BMS)**. A BMS is a centralised computer-based system to manage, monitor, and control building equipment and services, and to automate building functions. A Building Automation System (BAS) is defined as a BMS that adds smarter analytics and advanced automated controls. In practice both terms are often used interchangeably. We will use BMS to refer to the smart building management, control, and automation system.

The second key elements are the **IoT[7] devices** installed and connected across the property to collect data and ultimately execute actions as instructed by the BMS. There are a large variety of IoT devices, from very simple sensors and actuators, to highly sophisticated PTZ cameras.

The third key element is the **data network**. The equipment and subsystems in a smart building need to interact and communicate either from machine-to-machine, or from machine-to-human. The data network is the infrastructure that interconnects and enables the communications between the different subsystems, IoTs, and the BMS.

Smart buildings are enabled by the building management system, the IoTs, and the data network. In a simple analogy with the human body, the IoT devices are the building senses; the data network is the nervous system; and the building management system is the brain. The IoT captures the metrics and data that are needed to understand what is happening. The building management system processes the data and triggers actions based on the building automation rules. The data network transports data and instructions across the building.

In the past, building management and control existed in silos, because the different building subsystems were based on technologies that did not interact. Subsystems like HVAC, alarms, or lighting were isolated and separate infrastructures, in many cases managed by proprietary vendor solutions. Additionally, the BMS generally had limited integration capabilities, provided elementary analytic tools, and user interfaces were not particularly friendly.

With the surge of smart building, the industry is developing innovative products and solutions to enable building management digital transformation. Silos are being eliminated due to the ability to integrate different functions at different levels based on standards. Today, with high-speed networks, IoT, cloud-based applications, big data analytics, programmability, and cutting-edge technologies, such as Artificial Intelligence (AI) and digital twins, almost anything is possible.

7 comprehensive approach to the IoT challenge, Alcatel-Lucent Enterprise Whitepaper (November 2020)

Essential features

When approaching a smart building project, designers must ask themselves: Do I need a building that is just a little smart or one that is truly intelligent? Requirements must be carefully defined, but the final intelligence quotient will usually depend on the budget. The challenge is reaching the right balance between goals and cost. However, two things are a must for a building to be smart: Connectivity and automation.

Connectivity is an essential. With so many disparate elements involved, the definition of open network protocols and standards is paramount for building subsystems and equipment to communicate and interoperate with each other and with the BMS. New smart building solutions and products are required to be standard certified, with proprietary protocols being used less and less. Today there are many standard communication protocols to choose from, following is a list of just some of the options.

Interoperability is one of the most important aspects; that is, the ability to communicate with the building subsystems and to integrate with other business and operation platforms. Openness is key. Open programming languages, standardised databases, APIs and cloud connectors allow for seamless integration and data exchange with external systems and applications via software. Additionally, using programmability, software developers can extend automation by using customised developments.

The BMS user interface (UI) is also important. Even in the smartest building there are still a lot of things to monitor and alerts to attend to, 24x7. With this premise in mind, friendly graphical UIs, with fully customisable dashboards, that can be accessed using a standard browser or mobile app, at anytime from anywhere makes building managers' lives easier.

Lastly, building management systems must perform big data processing and **advanced analytics**. There are many parameters that can be measured in a building, from environmental variables such as temperature and humidity, brightness, and air quality, to security and safety conditions, like entrance and exit records, room occupancy rates and contact tracing data, as well as water, gas and electricity metering. Large amounts of heterogeneous data are generated, and decision maps may become unmanageable. If this is the case, you may need a sophisticated building management system that leverages AI and machine learning (ML) applications to make the right decisions and push automation capabilities to the limits.

Smart building wired communication protocols:

BACnet is a data communication protocol for Building Automation and Control Networks that has made an impact on the HVAC industry. BACnet is standard in America and Europe, and is an ISO global standard. It is used in many different markets, including industrial, transportation, energy management, building automation, regulatory, and health and safety.

- **Modbus** is a data communication protocol for transmitting information over serial lines and has become a de facto standard protocol for connecting industrial electronic devices in HVAC, lighting, life safety, access controls, energy management, and maintenance, and is used mostly in industrial environments.
- **LonWorks** is a data communication network protocol used in building automation applications for networking devices through power lines, fibre optics, and other media. A large number of devices are installed with LonWorks technology, including lighting, HVAC and machinery in industry, transportation, utilities, and home automation.
- **KNX** is an open standard for commercial and domestic building automation. KNX devices can manage lighting, blinds and shutters, HVAC, security systems, energy management, audio, video, and displays, among others.

Smart building wireless communication protocols:

- **Wi-Fi** is one cost-effective and easily accessible way to connect wireless IoT devices, as deployment is done simply over an existing Wi-Fi network, available in most commercial, institutional and office buildings today. For building automation, Wi-Fi is most commonly used for devices that are plugged in, such as most smart thermostats and lighting, and for user smart devices that can be charged. Wi-Fi is also a great choice in smart building networks powered by cloud-based software applications.
- **Bluetooth®** is known for its use in smartphones and wireless user wearables, but it is also used widely in home and building automation. Designed for small data transmission and low power consumption, Bluetooth Low Energy (BLE) is the technology of choice for indoor location services that require accuracy in the range of three to five metres.
- **Zigbee**, a protocol created specifically for commercial use is perhaps the most widely used protocol for building automation. Known for operating with minimal power usage (Zigbee devices batteries can last up to several years), it is also one of the most secure IoT protocols. Typical Zigbee applications are in industrial control, monitoring, sensor networks, and building automation.
- **LoraWAN** is a low-power wide-area network (LPWAN) protocol specifically designed for connecting battery operated IoTs over long ranges. LoraWAN covers uses cases for smart cities, smart buildings, and smart metering, among others, and is the most widely adopted LPWAN technology to date.

Each protocol has its application and it is up to the smart building project designers to choose the right application for the right job, according to the requirements.

How data networks contribute to smart buildings

Smart building industry specialists agree that information technologies are increasingly infiltrating building equipment as well as building control and management systems[8].

Proof of this exists in the fact that main data communication protocols for buildings, such as BACnet, Modbus and LonWorks, now have IP versions that run on top of the data network. Similarly, many IoT devices are IP-based and connect directly to the building network. For non-IP IoT devices there is an extensive offer of open protocol controllers and gateways that can be used.

Why is this move towards IP happening in the smart building industry? One important reason is that IP-based smart building solutions can leverage existing data networks, which contributes to lower installation costs. In addition to the economic reasons, IP is a versatile, interoperable, proven and secure networking technology. The IT infrastructure allows for improved network security, remote access to systems, remote notification of events and alarms, and use of Power over Ethernet (PoE). Most importantly, however, it allows for the integration and interoperability of building systems.

The data network is fundamental to making smart buildings truly smart. However, smart building requirements put a lot of pressure and challenges on the network, and there are several important aspects to be considered for the design or renewal of a building network.

Multi-standard networking support: The data network is the foundation for secure onboarding of IoT devices, and for communication between them and with the building management system. To do this, the network must support a variety of connectivity standards.

IP networks are versatile enough to support wired and wireless connectivity, as well as several other protocols, like BACNet or Modbus, and Zigbee or BLE, on the same physical network. The response to the IoT phenomena has led to further evolutions in IP networking, such as Wi-Fi access points that natively support Zigbee and BLE. Building network designers must check that all IoT devices can connect to the network, either natively or through integrated gateways.

Security: IoTs are headless devices, with little processing capacity and, in general, with little or no embedded security. With more and more IoTs connected to a smart building, the surface exposed to hackers is becoming larger and so too is the risk of cyber attacks.

Security has been always a critical aspect of IP networking. For this reason, the IP protocol supports many security standards, which are continuously being revised and improved. This means the data network must provide the security that IoTs cannot implement themselves, to protect access to the network and integrity of the data and applications running on it.

Performance: While some IoTs send and receive small amounts of data over long periods of time, as is typically the case for sensors and actuators, others, such as high-quality video CCTV cameras, stream a lot of information that must be processed in real-time. In both scenarios, data from IoTs must reach the appropriate systems, be processed and produce an answer or result, in a timely manner.

The building network must be designed to provide for today, as well as future needs in terms of scalability, bandwidth, and speed. IP protocols designed for highly reliable and low latency networks, such as Short Path Bridging (SPB) and IP multicast support, must be considered to guarantee the required performance levels.

8 AutomatedBuildings.com http://www.automatedbuildings.com/index.htm

Automation: Monitoring and managing the significant and increasing number of users, IoTs, and applications running on the network, has become a real challenge for IT staff.

Network automation is essential for mission-critical networks and plays a decisive role in the design of smart buildings. With network automation, the complete IoT onboarding process can be automated, from the device discovery to the fingerprinting, classification, authorisation, segmentation, and connection to the network edge, saving IT managers the time and risks of doing it manually.

Power over Ethernet (PoE) and Multigig Functionality: Power over Ethernet (PoE) and Multigigabit (Multigig) functionality in smart buildings delivers significant benefits in terms of cost savings and enhanced performance. PoE allows devices like LEDs and IoT sensors to receive both power and data through a single cable, reducing the need for additional wiring and infrastructure. Multigig functionality boosts data transmission rates over existing cabling, supporting the growing demand for high-bandwidth applications such as video surveillance and data analytics. Together, PoE and Multigig enable efficient power distribution and high-speed connectivity, optimizing network performance and scalability. This integrated approach ensures that smart buildings can support a wide range of devices and applications, enhancing overall operational efficiency and flexibility.

Battery life efficiency: With an increasing number of IoT devices that depend on batteries, optimising the consumption for a longer battery life is essential. It translates directly into equipment cost and operational expense savings, with less staff required on-site to replace batteries or IoT devices themselves. Choosing IP equipment that implements standards designed to optimise the battery use of connected devices, such as Target Wake Time (TWT) in Wi-Fi 6/6E and Restricted Target Wake Time (R-TWT) in Wi-Fi 7 is an excellent choice.

Openness: Integration with BMS, dedicated IoT platforms and other business and operation applications is another vital point for smart building projects. This is a heavily fragmented market. Project managers and building owners must decide which solutions best meet their needs. The data network should integrate and interoperate with as many different solutions as possible.

Operational efficiency in smart buildings is enhanced through advanced networking and automation technologies. By proactively monitoring infrastructure and creating efficient processes, buildings reduce operating costs and improve system capacity. Autonomous networks automate service provisioning and manage operations, while secure IoT onboarding simplifies device integration. These technologies enable predictive maintenance, rapid issue response, and optimal resource use, ensuring buildings operate efficiently, safely, and comfortably.

As mentioned previously, IP networks are based on standards, which guarantee integrability with other standards-based equipment and applications. It is recommended that the network management system provides standard APIs, like Restful APIs, to allow for integration with external business and operation applications. As well, network equipment programmability using open programming languages, such as Python, augments the network interoperability and automation capabilities, opening the door to a world of smart building use cases.

Conclusion

Smart buildings enhance urban sustainability, energy efficiency, and occupant comfort while reducing maintenance costs and environmental impact.

Alcatel-Lucent Enterprise (ALE) supports this transformation with comprehensive digital infrastructure solutions, focusing on three pillars of its Digital Age Networking:

- **Autonomous Network**: Ensures reliable, secure connectivity for all subsystems and IoT devices, simplifying the management and integration of digital services.
- **IoT Enablement**: Provides secure onboarding, management, and monitoring of IoT devices, enhancing efficiency and supporting energy savings and sustainability goals.
- **Business Innovation**: Integrates advanced services, including indoor location tracking or asset tracking, video surveillance, and AI-driven analytics for improved safety, resource optimization, and maintenance cost reduction.

For additional information or to speak to an expert, please feel free to contact us

DID21102901EN (August 2024)

Alcatel·Lucent Enterprise