Winter 2019 Volume 16, Number 4

iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

The Fall 2019 CABA Board Meeting was collocated with the IFMA World Workplace event in Phoenix, AZ. See inside for the full board member list.

CABA CELEBRATING 30 YEARS

iHOMES and BUILDINGS
THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

Winter 2019, Volume 16, Number 4

Contents

iHOMES and BUILDINGS

THE MAGAZINE OF THE CONTINENTAL AUTOMATED BUILDINGS ASSOCIATION

Winter 2019
Volume 16, Number 4

CABA 30 YEARS

Association Office

Continental Automated Buildings Association
1173 Cyrville Road, Suite 210
Ottawa, Ontario, Canada
K1J 7S6

Tel: 613.686.1814; 888.798.CABA (2222) Fax: 613.744.7833

IoT Risks for Building Automation Systems

By Ken Wacks

Introduction

Since the spring of 2016, I have being writing on the Internet of Things (IoT) for homes in *iHomes and Buildings*. Consumers benefit from applications designed with connected devices that use IoT technology. The term IoT fosters the idea that clever things linked to a network result in desirable applications such as entertainment, lighting, environmental control, energy management, health, and safety.

Well-designed applications for homes and buildings depend on more than clever things; they require careful systems engineering and attention to the user-experience. Furthermore, an integrated smart home with cooperation among applications is facilitated by designs that conform to standards for interoperability. This enables seamless operation so, for example, a home theater experience automatically manages lighting, shade control, and entertainment equipment. IoT devices may be components of these systems, but are not *per se* substitutes for integrated systems that deliver desirable applications.

Building Automation Systems for commercial buildings have been evolving about two orders of magnitude slower than home systems. Nevertheless, there are growing discussions in trade associations about how IoT will revolutionize the services in buildings and lower operating costs. This paper examines the elements of building automation systems with a focus on the benefits and risks of adopting IoT for these buildings. Some similarities and differences between IoT for homes and buildings are noted.

Building automation evolution

Building Automation Systems (BAS) usually include:

- Energy management
- Lighting control
- HVAC (heating, ventilating, and air conditioning)
- Life safety
- Power management
- Access controls
- Elevators and escalators (called "vertical transport")
- Public communications (public address, signage, video displays)
- Telecommunications (telephone networks and Internet access).

The BAS industry began in 1883 with the invention of the thermostat by Warren Johnson, the founder of Johnson Controls. He then developed pneumatic (compressed air) signaling for thermostats in 1895. The industry has been slowly adapting to technology changes. For example, a major shift was from pneumatic controls to electronic signaling in the 1980s. These electronic links have been mostly connections from sensors and actuators to a control panel where the sensor states (such as open/closed) or measurements (such as temperature) were displayed, typically with no or limited data processing. The panels also allowed remote control of actuators, which are relays and switches to operate mechanical devices such as valves and motors.

Intelligent controllers that are programmed via user interfaces for analyzing multiple sources of sensor data to operate actuators are relatively recent in the long history of BAS. The trend in BAS is increased observability, which means more remote sensing, and increased controllability. For example, more temperature sensors in a building could enable zone control of the individual office climate. More control is made possible by enhanced device intelligence, microcontrollers, communication networks, and smart phones.

BAS has progressed through major technology changes. However, these transitions have occurred over decades, not in a few years as with home automation.

The "thermostat era": Remote sensing for local control

The thermostat was designed originally to control heating based on one sensing point. Signals from a remote thermostat were sent to a heating controller pneumatically or via an analog electric voltage level.

The "DDC era": Sensors and actuators linked to local intelligence

More sophisticated control is possible with more sensors and actuators. DDC, or Direct Digital Control, manages these sensors and actuators for one system. While DDC offers more accurate control, it does not address integration among BAS subsystems. Until recently many building systems were operated separately from different panels. Larger builders have integrated BAS systems usually supplied by one vendor. During the September 2019 meeting of the CABA Intelligent Buildings Council, the cost of integrated BAS was estimated at $2 to $3 per square foot. Small buildings cannot afford these costs and are likely to install separate non-integrated BAS systems from multiple vendors.

The "hierarchical era": Limited subsystem integration

Where not precluded by safety codes, building management would be simpler if exercised from a central panel, which would involve a single user interface.

The present: Flattening the hierarchy with fewer levels

Fewer levels and control exercised from a central panel can improve building operation. Multiple panels often present the user with too much detailed data from a multitude of sensors and control points (actuators). I have seen operators overwhelmed by such irrelevant data and routinely canceling alarms.

The future: Smart sensors and actuators with distributed control

Building operation can be streamlined with integrated control. Energy management can be improved by coordinating air-handling units distributed in a large office building, especially if air conditioning is reduced in unoccupied areas. In a distributed intelligent system the operator is presented with relevant data for making important decisions. Local controllers process routine data and pass exceptions or major changes upstream to the operator.

Building automation fieldbus

Figure 1 illustrates the organization of BAS. Most of the subsystems operate autonomously with each subsystem under the management of a dedicated controller, often called a unitary controller if it serves one room or zone. The hierarchical organization of a BAS as illustrated is bringing a systems concept to building services. The actuators turn on, off, or modify end-devices such as heating, air-conditioning, and ventilation equipment, lights, audio announcements, and video signage. As shown in the lowest layer of Figure 1, these elements may share a communications medium called a *fieldbus*.

The fieldbus is a commonly used method in BAS for linking sensors, actuators, user interfaces, and control panels. The fieldbus consists of wires and connectors that provide data and power to sensors and actuators, called field devices. Some of the popular fieldbuses include Modbus, ProfiBus, and LonWorks. The traditional fieldbus topology has consisted of wiring from one field device to another (often called a daisy-chain connection). Some fieldbuses support wiring in a star or bus (using a shared medium).

The installation practices of BAS are different from most IT (Information Technology) networks, which link PCs to Ethernet switches with a star topology. BAS equipment is often operated from "zone boxes" in the ceiling or under the floor. Such equipment might include card access devices, paging systems, and VAV boxes (Variable Air Volume fan and ducts for room control of heating and cooling).

IoT for BAS

Proponents of adapting IoT for BAS tout the advantages of increased flexibility, more service integration, and lower operating costs. IoT purists propose inserting an Internet interface into each BAS element, which then communicates via a single bus such as wired Ethernet or wireless Wi-Fi operating at one BAS level, as illustrated in Figure 2. This fundamental redesign may offer additional benefits, but will profoundly change BAS operations, responsibilities, resiliency, and exposure to cybersecurity threats. The primary advantage is a uniform IT infrastructure for information processing, telecommunications, and BAS. This system architecture also supports sharing of sensors and actuators, and remote management across multiple BAS systems.

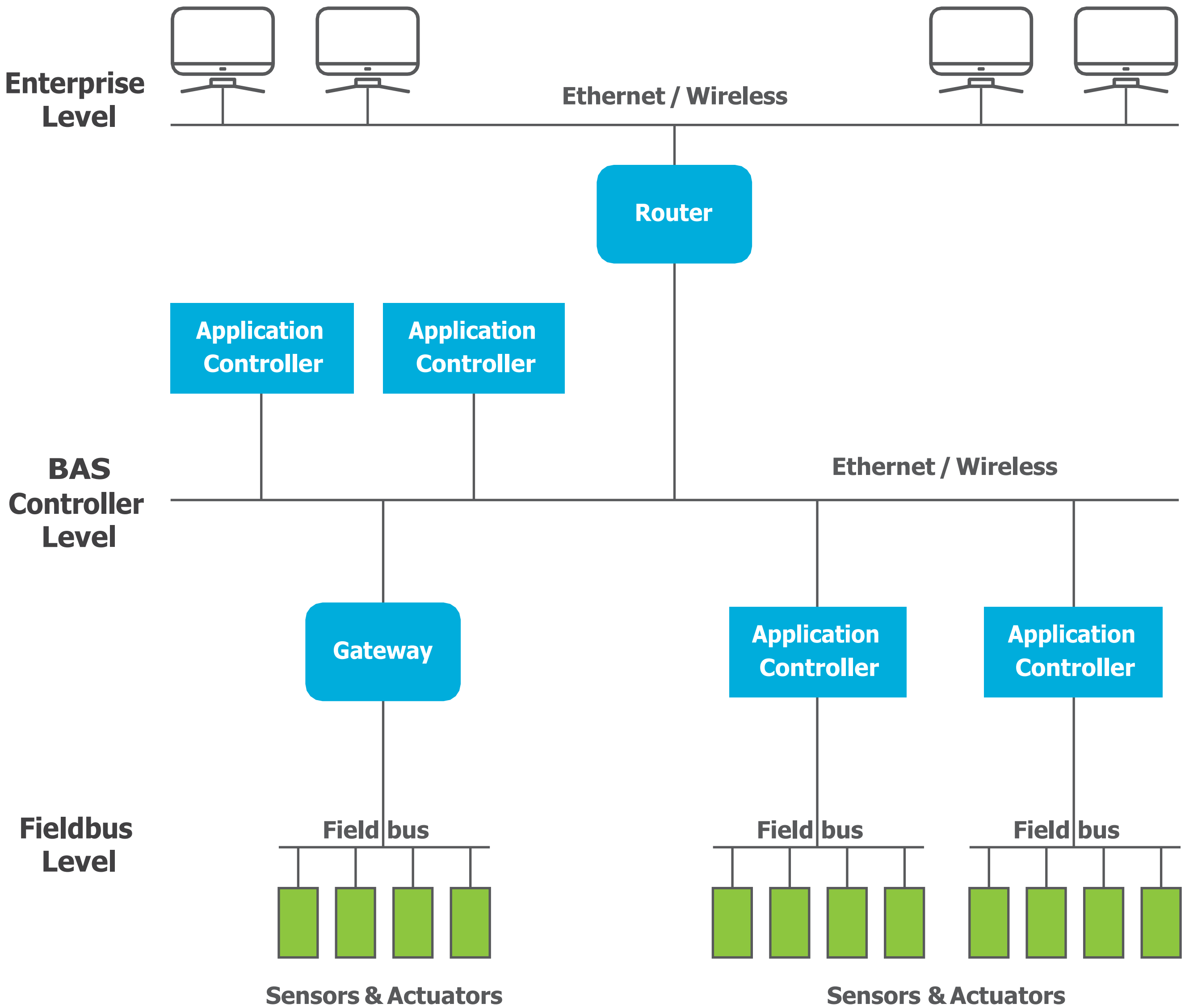

Figure 1 – Hierarchical Organization of a Building Automation System

An objective of remote management is to centralize user access and avoid multiple panels. Some costs might be reduced by sharing sensors across services. For example, occupancy sensor data could impact lighting and HVAC control, not just security. A fire detection system could query thermostats to determine the source of a fire.

The fundamental benefits of remote management are lower operating costs. A BAS with remote management can lower costs for training operating personnel, facilitate building management from an integrated control panel across multiple building services, and lower energy usage through zone management of unoccupied offices.

Integrated BAS might create opportunities for additional rental income. Tenants would be offered a choice of lighting, telecommunications, and access control services for monthly fees beyond the base rental charges. Companies recognize that the office environment can affect employee productivity. A comfortable work place with occupant control of office lighting and HVAC might encourage employees to stay even in a tight labor market. A flexible BAS can facilitate frequent office rearrangements and make the tenant space more desirable.

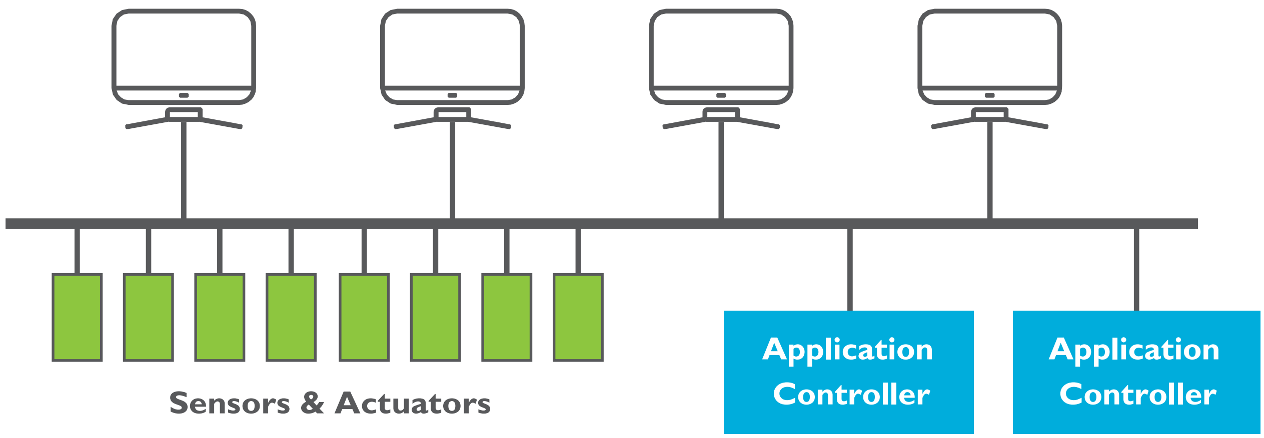

Figure 2 – Single-bus Building Automation System

OT versus IT

BAS systems have traditionally been operated and maintained by facilities management (FM) personnel. There is an emerging struggle between IT managers and FM with the growing push for blending IT and BAS. The IT companies seeking to enter the FM market are calling IT designed for FM OT (Operational Technology).

The outcome of the OT-versus-IT struggle will have a major impact on BAS designs that in the long run will favor IP-enabled devices, including IoT devices. Leading the charge are IT companies who are seeking to displace traditional building automation providers.

The evolution of BAS from FM and fieldbuses to IT and Ethernet or Wi-Fi will provide both physical and functional improvements. BAS using IT networks will facilitate moves, adds, and changes (called MACs in BAS). New BAS network devices will provide distributed control, trending and historical data storage, and network management. A single building data network could integrate the following activities:

- Business: accounting, sales, Internet access.
- BAS
- Media (live, broadcast, recorded audio and video)

IT challenges for BAS

A writer for System Contractor News asked in July 2007, "Should everything be on one network?" and answered, "…because of life safety requirements, legacy systems, and human politics, in most cases, the answer will continue to be 'no'." Now more BAS is migrating to a local area network, but practical realities of BAS still dictate separate networks because:

- Local codes may mandate that life safety be on an independent network.
- Hospitals may demand a separate network for medical monitoring.
- Performance centers (theater and concert halls) may want audio and video on a network that will not experience interference, noise, or delays from other applications.

FM supports fieldbuses. IT managers support Ethernet and wireless networks. Building automation systems must operate ALL the time, with MINIMAL problems. Computer networks must operate MOST of the time without ANY problems when up, but sometimes need to be taken down for maintenance and rebooting. FM seeks low-cost always-on solutions that default to local control if off-line. FM's goal is to keep the building functioning with the lights on even if automation is temporarily out of service.

Cybersecurity is another looming concern for OT. The IT world has been dealing with compromises of data communication networks and databases in servers. Fieldbuses have been more difficult to penetrate especially when they are not connected to the Internet. Moving from fieldbuses to Ethernet or Wi-Fi and inserting gateways to the Internet are opening pathways to problems. Furthermore, end-devices are being designed with embedded microprocessors run by software algorithms.

Cybersecurity protection for end-devices now becomes as challenging as protecting a PC or server. This entails monitoring for malware and establishing secure communication networks.

The continuing BAS evolution

The pace of change for BAS is remarkably slower than the development of home systems. "Products are more capable, but the architecture is not much different from 30 years ago," according to Steven Bushby, Leader of Mechanical Systems and Controls Group at the US National Institute of Standards and Technology (NIST) and head of the ISO committee (International Organization for Standardization) developing BAS standards for large buildings. Steve and I agree that IT has a lot to learn and will grow slowly into the building automation space. FM still has the political power and experience in running the building continuously without "rebooting the building." FM is likely to survive by adopting some IT features rather than delegating BAS to IT. ●

 Dr. Kenneth Wacks has been a pioneer in establishing the home systems industry. He delivers clear and practical advice to manufacturers and utilities worldwide on business opportunities, network alternatives, and product developments in home and building systems. The United States Department of Energy appointed him to the GridWise® Architecture Council to guide the electric industry toward smart grids. For further information, please contact Ken at +1 781 662-6211; kenn@alum.mit.edu; www.kenwacks.com.