Introduction to IP in Commercial Buildings

Authored & Reviewed by IPSO Alliance Smart Building Workgroup (in alphabetical order):

Bernard Aboussouan, Max Agueh, Daniel Barisic, Christophe Baujault, Rich Blomseth, Bill Butler, Cedric Chauvenet, Paul Chilton, Hamid Daneshmand, Joseph DeNicholas, Bob Dolin, Mathilde Durvy, Jim Garozzo, Pierre Geriniere, Laurent George, Laurent Hua, Ted Humpal, Trae Harrison, Stamatis Karnouskos, Abtin Keshavarzian, Jean-Noel Loiseau, Jerald Martocci, Tim Morneau, Marc Petock, Anton Pfefferseder, Anil Ramachandran, Yuan Tian (Workgroup Chair), Joy Weiss, Patrick Wetterwald, Ming Zhu, Matthew Zieg

Key Contributing Authors

Stamatis Karnouskos, JP Vasseur, Patrick Wetterwald, Jerald Martocci, Ted Humpal, & Ming Zhu (Editor)

Summary: IP (Internet Protocol) based convergence is a mega trend

First, voice data became a packet on IP networks (Voice over IP). Now, video is being packetized through the Triple-play (voice, internet and video/TV). Furthermore, companies like Google are adding mobile device connectivity to make it a quadruple-play. This paper intends to show that the commercial building is joining this convergence trend. Very soon, consumers will be connected not only to their friends and family but to their buildings, houses, and cars. We highlighted the three key business and technology enablers as cost savings from OPEX[1], CAPEX[2] and reduced number of gateways, real-time IP technology readiness and the new IP developments for small constrained devices. This paper also provides an introduction to today's building systems and tomorrow's converged IP platform.

[1] OPEX: Operating Expenditure or Operating Expense. OPEX is an ongoing cost for running a product, business, or system

[2] CAPEX: Capital Expenditure. For example, Capex are used by a company to acquire or upgrade physical assets such as equipment, property, or industrial buildings.

I. Today's Commercial Building

When we enter office buildings, hotels, hospitals, retail stores or theatres, we seldom think about how they work. We just expect that they will work and that we will expect to feel comfortable inside. With the trends toward smart infrastructure, new technologies are being considered to make the buildings responive to our needs (e.g. interact with us in real-time and adjust to our comfort and preferences). To understand what makes it all work, let's first review what the systems behind today's commercial buildings are: Business Systems (IT), Building Management System (BMS) and Specialty Systems. We will present a brief synopsis of the BMS systems; a brief introduction to specialty systems; and how they might integrate into IP business systems with a vision of the "converged" network in the future as depicted in Figure 1.

Figure 1 - The Convergence of Commercial Building Systems

I.1 Business Systems

Business systems describe the IP infrastructure of routers and switches that permeate the interior of a building. The application domain includes email, document management and Internet access, paging, and texting. New data intensive applications such as VoIP and IP video cameras are forcing the IP network towards more reliable and real-time requirements. High reliability and real-time performance are necessary ingredients for building management and specialty systems thereby further endorsing the convergence of these systems.

I.2 Building Management Systems

Enterprise-wide BMS predate IP systems and have been installed in commercial buildings since the 1970s. While these systems are widely utilized and understood by building personnel (e.g. a company's facility management department or corporate services), they are often transparent to most building occupants. These systems are designed and installed to increase occupant comfort while minimizing overall energy usage. The BMS will monitor indoor and outdoor environmental conditions and automatically control the indoor environment to match the selected energy and comfort profile(s) requested by the user(s). These systems control heating, ventilation, air-conditioning, lighting and elevator systems. Building access, security, smoke control and fire monitoring features are also deployed to increase the safety level of the building occupants.

BMS were deployed as proprietary hardware and software solutions into the mid-1990s. The control networks were typically twisted pair copper wiring, and the protocols were proprietary. In the mid-1990s, two open building automation and control network protocols (BACnet and LON) were developed within the industry that fostered interoperability of the software objects. In the first decade of the 2000's, systems started to support native web services in the network control layer of the architecture making the systems able to serve HTML and support other web technologies such as Obix and BACnet web-services. These developments have lead to a convergence of hardware platforms and an explosion of software interoperability. It is now possible to choose from a wide range of 3rd party software applications that can consume data from most major BMS. These days most BMS vendors utilize Ethernet IP running BACnet/IP or LON/IP for enterprise data and twisted-pair for control network communications in the lower layers of the architecture. The introduction of IP-based wireless sensor networks using 6LoWPAN and ROLL technologies will likely further integrate building systems and IP business system networks. Today, most BMS are highly interoperable with most building equipment manufacturers. An example of the classic BMS system is depicted in Figure 2 below.

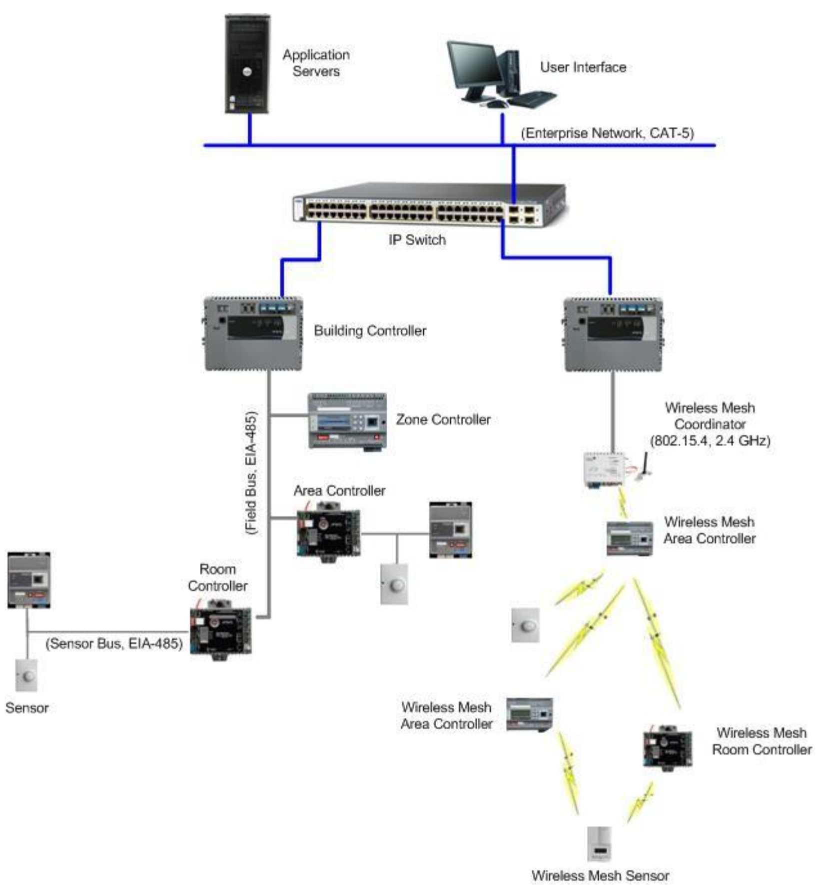

Figure 2 – Classical Building Management Systems

I.3 Specialty Systems

A third enterprise-wide system has emerged in certain markets in the past decade. These are a suite of synergistic applications for a selected market segment. In the healthcare market, for example, hospitals have a myriad of applications that need to be readily available to doctors and patients across the enterprise. Medical records, clinician collaboration, outcome improvement, prescriptions, as well as medication tracking and costing are but a few of the widely used applications needing to be delivered pervasively across the site. Patient tracking, staff tracking and medical telemetry are new applications entering this arena. Mobile access to all this data needs to be readily available to the healthcare staff for patient care through host devices called carts-on-wheels (COWs).

I.4 Building System Convergence

The overlay of the three systems functionality is depicted in Figure 3 - Applications running on an IP network in the Healthcare Market. While these systems could cohabitate the IP

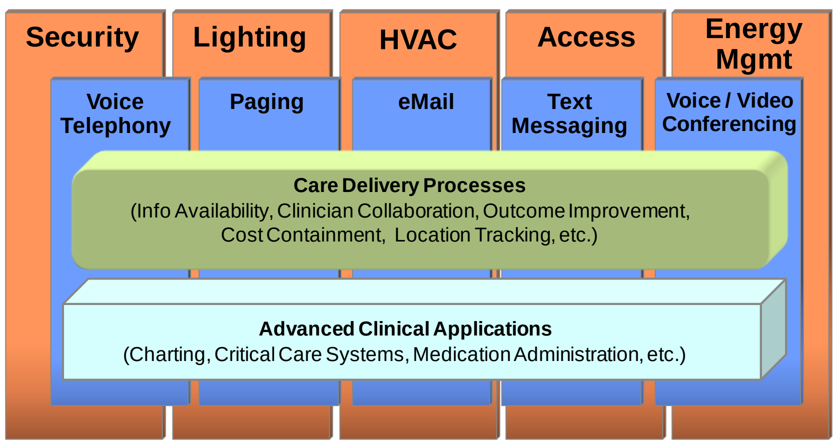

Figure 3 - Applications running on an IP network in the Healthcare Market

network as independent applications as is currently in place, there is further synergy available by melding these separate applications into a cohesive set. For example, facility alarms could be directed to facilities personnel using SMS texting or email applications. The energy management system might interrogate the healthcare location tracking subsystem to determine room occupancy before setting temperature set points. The IP data center may interoperate with the cooling systems to provide reliable IP server farms with minimal energy impact. The installation and maintenance cost savings of a single reliable communication network is clearly advantageous to supporting three independent networks. Hence, the convergence of these networks is in process as shown in Figure 4.

Traditional Approach
- ❑ Multiple control networks and systems
- ❑ Disparate building networks
- ❑ Proprietary & Redundant
- ❑ Sub-optimal information usage

Converged Approach
- ❑ Interoperability
- ❑ Efficient and Scalable
- ❑ Lower TCO
- ❑ Maximize ROI

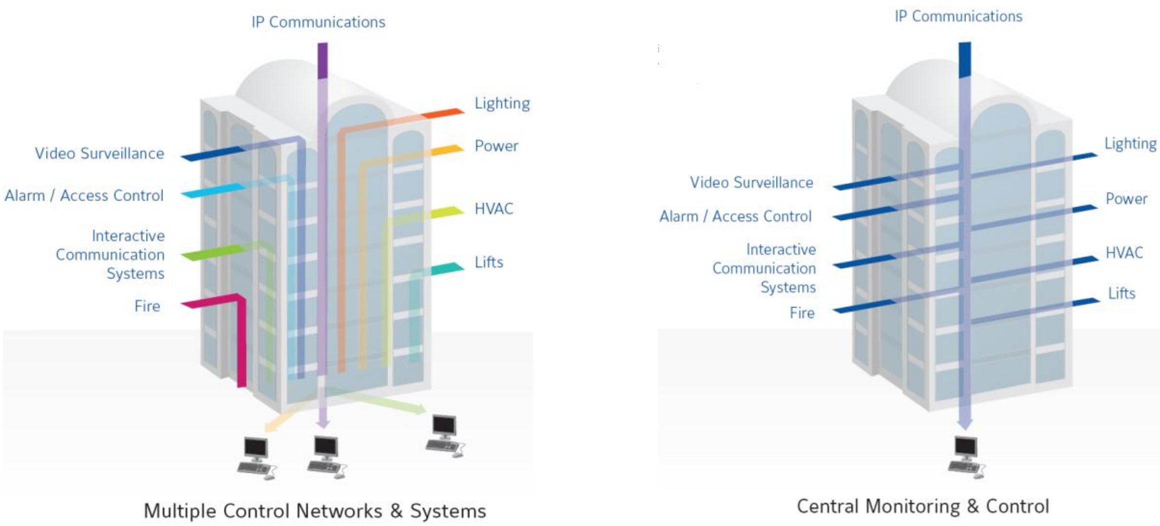

Figure 4 - Convergence of the Applications onto a single IP network

II. Enablers for Convergence

Cost benefits in operational efficiency for the three systems to converge are compelling. Some studies by Cisco® show that converged IP and BMS systems will eliminate standalone gateways by ~50%, reduce installation and integration cost by ~20%, decrease energy cost by ~20%, and reduce operation and maintenance cost by ~30%. We can also look back at voice integration onto data in the past decade for the overall cost considerations. Just as voice data becomes a marginal cost consideration on a converged network, incremental application support on a converged network provides significant cost savings when maintenance, upgrade, changeover, remote monitoring, dynamic real-time response and other operational management aspects are taken into consideration.

IT systems' increased reliability and real-time performance, which are necessary ingredients for building management and specialty systems, further endorse the convergence of these systems. In a user-centric digitally connected world, more real-time response will be required across geographical building locations. An IP based system provides an affordable and feasible solution.

New IP protocols and technologies are being developed specifically for IP smart objects[3] such as sensors and actuators used in buildings, factories, cities, etc. These technologies allow for efficient use of the network and enable devices to expose resources and capabilities that have historically been inaccessible to other network participants. With efficient compression to address the limited bandwidth of lower speed media often used at the edge, sophisticated routing to take into account the unique characteristics of these device level networks (e.g., integrity of links, intermittent connectivity, large number of nodes, lower speed, processor and memory constrained devices, especially when battery operated) IP can reach down to the device level while addressing the unique issues associated with the edge devices. The IETF 6LoWPAN Working Group has specified mechanisms to allow for such header compression and other mechanisms (e.g. fragmentation of large packets). Furthermore, the 6lowpan technology can also help in the convergence of legacy twisted pair into the IPv6 infrastructure. The new routing protocol specified for IP smart objects (called RPL) has been designed by the IETF ROLL Working Group. In addition, there is a lot happening with the application layer in standardization that will make IP more and more useful in building automation. Here are a few examples:

- OASIS oBIX v1.1 is being completed and includes a compact binary payload format useful with web services
- BACnet is working on integrating IPv6 support
- IETF CoRE is working on lightweight security bootstrapping and web service optimizations for building automation
- W3C has worked on standardizing compact XML representations with EXI

The notion of network convergence using IP is fundamental and relies on the use of a common multi-service IP network supporting a wide range of applications and services. This not only means that such networks are ideal to foster innovation but also lead to dramatically reduced overall cost and complexity in contrast with a myriad of incompatible, specialized networks interconnected by hard to manage gateways. History speaks for itself: the IP protocol invented about 30 years ago for slow file transfers and remote terminal control is now used to carry an impressive and fast growing set of applications and services with a variety of constraints and network requirements.

Thanks to its layered architecture, the IP protocol suite has been enriched with a number of new advanced features and capabilities over the past three decades:

- **Multicast:** technology allowing for sending data traffic to a set of hosts while minimizing traffic replication in the network so as to save network resource usage. For example, you can think of this as one-to-many communication method.
- **VPN**: Virtual Private Networks can be built on top of a common IP infrastructure offering a complete isolation between the VPN with technologies such as VLANs, MPLS VPNs. You are likely to have used this technology when you log onto your company's computer network remotely from home or hotels.
- **Quality of Service (QoS[4])**: is the ability to provide different priority to different applications, users, or data flows,

[3] A Smart Object is defined as a small computer, generally with either a sensor or actuator, and also some form of communication device. They are enclosed into cars, switches, machinery or even thermometers. They enable home automation, monitoring, building management systems, smart grid, transportation, energy management and even smart cities.

[4] QoS: In the field of computer networking and other packet-switched telecommunication networks, the traffic engineering term **quality of service** (QoS) refers to resource reservation control mechanisms rather than the achieved service quality. Quality of

or to guarantee a certain level of performance to a data flow. For example, an application itself can indicate the required priority of the message as they are routed over the IP network. A number of IP-based technologies have been developed to truly support a wide variety of qualities of service: IP packets are "colored" when entering the network or by the application itself to indicate the required level of * QoS and then they are routed in the network and handled so as to meet the SLA (Service Level Agreement) thanks to scheduling and congestion avoidance techniques. Current QoS technologies allows for the support of real-time application with tight SLA (Service Level Agreement) constraints. For example, in a converged BMS and IT network in a building, a fire alarm message would take precedence over email traffic.

- **Reliability:** a number of techniques have been developed to provide an extremely high level of reliability thanks to built-in redundancy, the ability to quickly (in a few dozens of millisecond) re-compute a route should a network element fail in the network and so on. In other words, the network can intelligently and autonomously reconfigure an alternative route if the first one should fails.
- **Security**: IP networks can be highly secure. A number of technologies have been developed over the years to ensure authentication, support encryption, avoid Denial of Service (DoS[5]) attacks… to name a few.

Thanks to the development of these IP-based technologies; it became possible to share a common IP network in support of a myriad of applications having a variety of constraints in terms of quality of service, security, VPNs, reliability and so on.

III. Converged World

IP technology is expected to lead the way into the future of a converged world where user-centric architecture and solution is very important as shown in Figure . As we are migrating towards a future infrastructure, you will see many new applications using existing IT technology such as cloud computing services for on-demand building management, mobile and wireless data devices for real-time information relay to users and mash-up services. You will also see new technology to enable the next level of data accuracy and intimacy to the levels we currently cannot achieve cost effectively. At the heart of this data “explosion” are the billions of devices interconnected using IP technologies known as smart objects. Smart objects range from sensors, actuators, IT systems etc, which are and will be deployed more and more in future buildings or retrofitted in currently existing infrastructure. Traditionally, a company’s own facility management team installs and manages such activities. With the adoption of IP and standard application protocols down into the control device and sensor layer of the architecture, value-added applications are now decoupled from dependence on the device manufacturer. New third parties can now join the market, thus providing applications to support new functionality and new business needs. The future buildings will be populated with IP-enabled devices at all levels, and enable an ecosystem of services that will allow interaction among its different components, the environment, and the users. Furthermore, the buildings will no longer be limited to standalone entities but will participate as elements of bigger

---

service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

[5] A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer resource unavailable to its intended users. You may find some examples in popular computer magazines or mainstream news media that have reported some such incidents in the past few years.

infrastructures (e.g. multi-building groups) enabling streamlined management and participation in services such as load management and demand response to achieve goals set at enterprise level. This connected infrastructure is more than just connected buildings, as some would argue, because we already have that today. Conversely, this is a new connected building that connects to individual human needs and not just to facility management's needs. Of course, this does not mean every person will have access to all sensitive building information, but rather, each individual has its customized service and tailored data access rights for a personalized service. Similarly the building will benefit by on-the-fly utilization of additional information coming from users and their devices.

The buildings and their management will be extended to integrate and interact with the majority of those devices in buildings in a ubiquitous manner. For example, the users working or even temporarily being in a building can carry devices such as mobile phones that enable them to bi-directionally and collaboratively interact with the services the building offers.

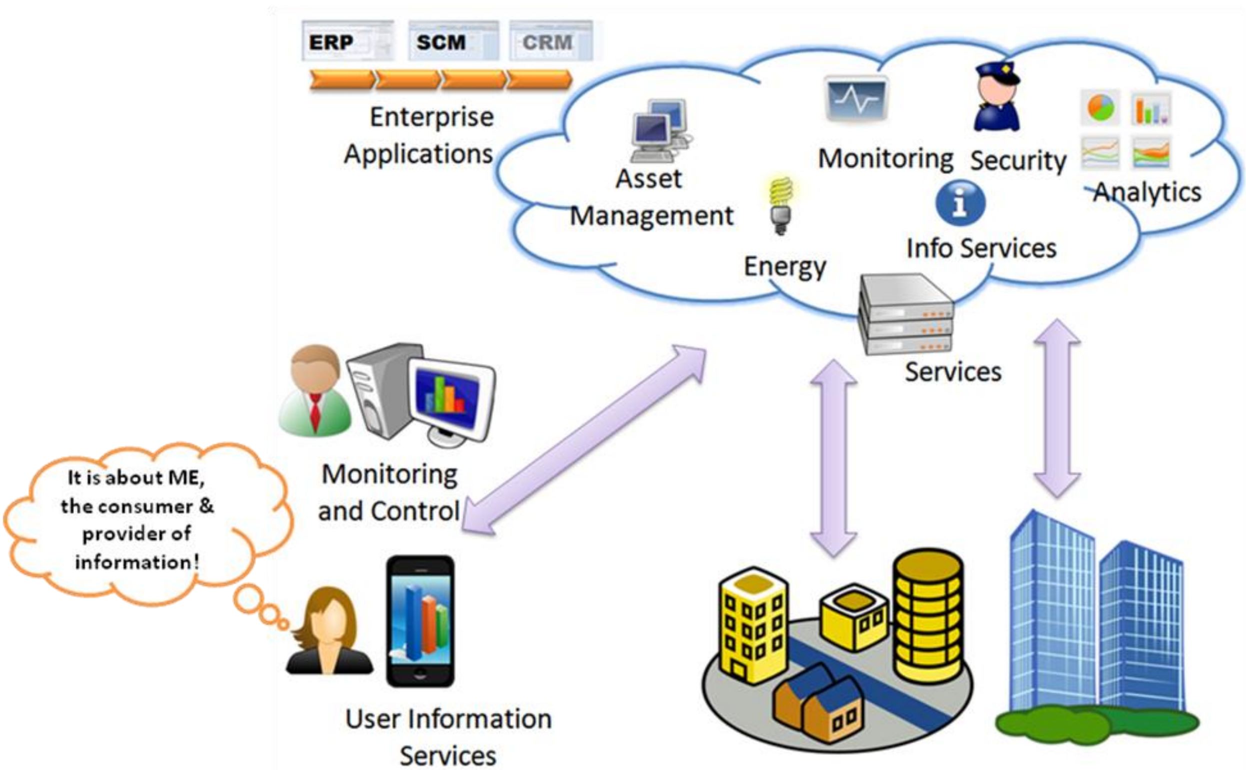

Figure 5 - Enterprise Integration and Facility Management

As we can see, all generated information will be captured and exchanged in a service-based manner, which will enable third party providers to attach and develop innovative new applications and services. When designing and executing new business processes, one should be aware that enterprise applications will be able to get near real-time data from the infrastructure itself. Dynamic decision support based on key performance indicators will be realized and coupled with timely monitoring and control capabilities. Such decisions will be enforced across systems in the building(s). Facility management applications, as well as user-centric applications, will be possible and will depend on mash-ups of services, which will give rise to rapid development of customized innovation with low integration cost. The common denominator to achieve this vision is the ubiquitous communication and boundless information exchange achieved by an ecosystem of IP enabled devices populating the future buildings.

We hope that this paper illustrated the relentless trend for convergence, the enablers for this movement and the ultimate environment where we will all meet. It is our hope that this will stimulate discussions both business and technical in nature to identify the gaps that still exist on our way to the digitally connected space.