IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems

Daniel Minoli, Kazem Sohraby, and Benedict Occhiogrosso

***Abstract*—The Internet of Things (IoT) is entering the daily operation of many industries; applications include but are not limited to smart cities, smart grids, smart homes, physical security, e-health, asset management, and logistics. For example, the concept of smart cities is emerging in multiple continents, where enhanced street lighting controls, infrastructure monitoring, public safety and surveillance, physical security, gunshot detection, meter reading, and transportation analysis and optimization systems are being deployed on a city-wide scale. A related and cost-effective user-level IoT application is the support of IoT-enabled smart buildings. Commercial space has substantial requirements in terms of comfort, usability, security, and energy management. IoT-based systems can support these requirements in an organic manner. In particular, power over Ethernet, as part of an IoT-based solution, offers disruptive opportunities in revolutionizing the in-building connectivity of a large swath of devices. However, a number of deployment-limiting issues currently impact the scope of IoT utilization, including lack of comprehensive end-to-end standards, fragmented cybersecurity solutions, and a relative dearth of fully-developed vertical applications. This paper reviews some of the technical opportunities offered and the technical challenges faced by the IoT in the smart building arena.**

***Index Terms*—Building management systems (BMSs), Internet of Things (IoT), light emitting diode (LED) lighting, power over Ethernet (PoE), smart building.**

I. Introduction

THE INTERNET of Things (IoT) is entering the daily operation of many industry sectors. For example, the concept of "smart city" is emerging. Smart city systems not only offer improvements in the quality of life of the inhabitants, but also greatly improve efficiency regarding asset management, including intelligent transportation systems (e.g., smart mobility, vehicular automation, and traffic control); smart grids; street lighting management; traffic light management; waste management; environmental monitoring (e.g., sensors on city vehicles to monitor environmental parameters); water management; surveillance/intelligence; smart services, and crowdsensing (where the citizenry at large uses smartphones, wearable, and car-based sensors to collect and forward for aggregation a variety of visual, signal, and environmental data). (Some of these services are known as "smart street" services.) In the short-term smart cities' industries spans five key areas: 1) energy; 2) water; 3) mobility; 4) buildings; and 5) government. The next granular evolution of the smart city is the application of these concepts in a more confined physical space, namely, to commercial building environments. In fact, nearly all the applications for smart cities have comparable applicability to building management [e.g., traffic/access control, surveillance, energy management, indoor environmental and air quality (IEAQ)/comfort control, and so on] [1]–[5].

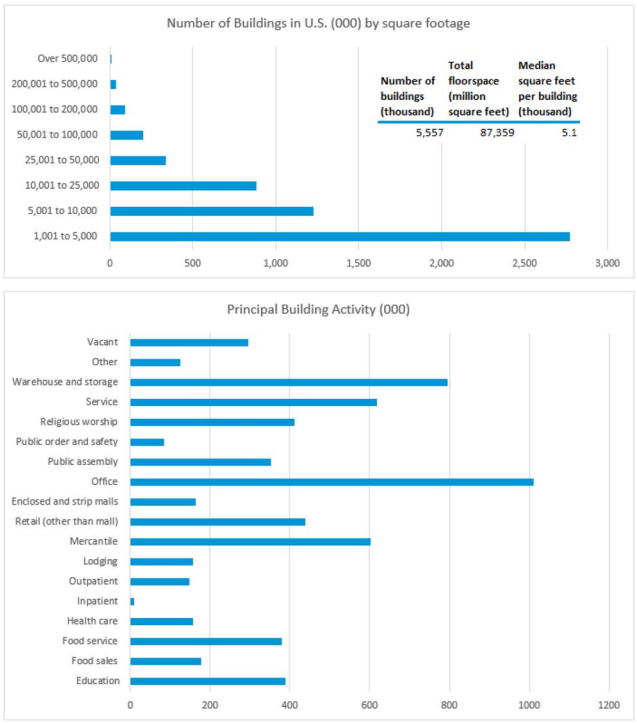


Fig. 1. Number of commercial buildings in the U.S. (data from [6]).

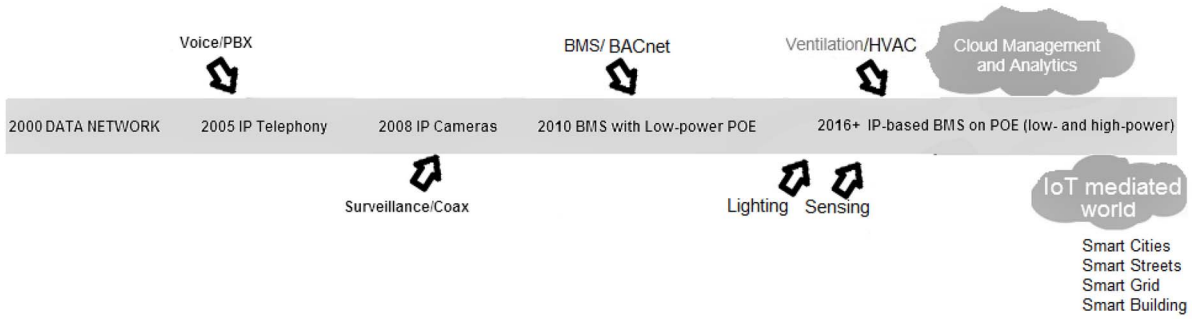
Data from the Commercial Buildings Energy Consumption Survey indicates that there were 5.6 million commercial buildings in the U.S. in 2012 (the most recent year for which data is available), spanning 87.4 billion square feet of floorspace (see Fig. 1) [6]. On a worldwide basis, buildings (residential

Manuscript received August 25, 2016; revised December 22, 2016; accepted December 30, 2016. Date of publication January 4, 2017; date of current version February 8, 2017. The work of K. Sohraby was supported by the National Science Foundation.

D. Minoli and B. Occhiogrosso are with DVI Communications, New York, NY 10007 USA (e-mail: Daniel.minoli@dvicomm.com; ben@dvicomm.com).

K. Sohraby is with the South Dakota School of Mines and Technology, Rapid City, SD 57701 USA (e-mail: kazem.sohraby@sdsmt.edu).

Digital Object Identifier 10.1109/JIOT.2017.2647881



Note: BACnet is an ASHRAE, ANSI, and ISO 16484-5 standard communications protocol for building automation and control (BACnet was subsumed in ASHRAE/ANSI Standard 135 in 1995, and in ISO 16484-5 in 2003.) The BACnet protocol defines several services that are used to communicate between control devices typically utilized in building (including HVAC, lighting control, access control, and fire detection systems). It specifies a number of network, data link, and physical layer protocols, including but not limited to standards such as IP/Ethernet.

Fig. 2. Graphical representation of technology convergence of building-support systems in recent years.

and commercial) are responsible for over 40% of total energy consumption. As per [6], office buildings use an average of 15.9 KWh of electricity per square foot annually; this equates to an annual expenditure of $1.7 per square foot using a general $0.1058/KWh rate. For the average office building in the U.S. (15 000 ft^2), this electricity consumption equates to an expenditure of $25 500 annually. Notice that the rent cost (say at $40/year/square foot) would equate to $600 000 annually; thus, energy costs, which are often, but not always, incremental to the rent are about 4%–5% compared to the rent expenditure.

Data from [6] also shows the following regarding electricity consumption (in recent years).

1) In aggregate (across all commercial buildings) the electrical energy consumption is as follows.
   a) Space heating: 2.0%; cooling: 14.9%; ventilation: 15.8%; water heating: 0.5%; lighting: 17.1%; cooking: 2.2%; refrigeration: 15.8%; office equipment: 4.1%; computers: 9.5%; and other: 18.1%.
   b) Thus, in terms of electricity 32.7% is consumed by space heating, cooling, and ventilation; the next big item is lighting at 17.1%; computers and office equipment accounts for 13.6% (total: 63.4%).
2) For office buildings building only the energy consumption is as follows (they consume 20.1% of the total U.S. electric energy use).
   a) Space heating: 2.2%; cooling: 13.4%; ventilation: 24.7%; water heating: 0.2%; lighting 17.1%; cooking: 0.2%; refrigeration: 3.2%; office equipment: 4.3%; computers: 19.31%; and other: 15.3%.
   b) Thus, in terms of electricity 40.3% is consumed by space heating, cooling, and ventilation; lighting at 17%; computers and office equipment account for 23.6% (total 80.9%).

(Comparable, but not necessarily identical, allocations are expected for other industrialized nations.) This large footprint defines a sizable market opportunity for technical solutions incorporated in building management systems (BMSs),[1] which are now increasingly based on IoT principles. Inexpensive sensors are emerging, and user-friendly applications are becoming available, often as a software-as-a-service cloud-provided service [7]; these developments are now driving the deployment of the IoT in building applications. A BMS is a comprehensive platform that is employed to monitor and control a building's mechanical and electrical equipment; they are used to manage loads and enhance efficiency, thus having the ability to reduce the energy needed to illuminate, heat, cool and ventilate a building. A BMS interacts with controls hardware in the various mechanical/electrical systems to monitor and modulate in real time the energy used; they are typically used to implement demand response (DR) arrangements [8]–[10].

In recent years, one has observed a fruitful convergence for various building technologies and systems to an IP-based infrastructure supported by the firm's intranet (in multitenant buildings a building-oriented intranet may be required). Technological convergence as it relates to building management and smart buildings is accelerating with the increasing deployment of IP-based endpoint devices under the thrust of IoT. A few years ago various building systems utilized different protocols, networks, and cabling systems; clearly, this is inefficient from both a deployment perspective as well from a system management perspective. The realization occurred that it would be easier to install a common cabling infrastructure (for example, twisted pair category 6 cable) for all the various functions, and also migrate to a state of using of a common set of protocols (e.g., the TCP/IP suite); in addition, a common management system can be utilized. Fig. 2 depicts graphically the convergence that has already occurred in recent years, and IoT concepts will further enhance, standardize, and extend the service function and the service scope. Site-based telephony has (generally) converged to an IP-based intranet infrastructure; surveillance has converged to utilize IP-based cameras (which not only facilitate signal distribution but also computer-based storage and analytics). BMSs have migrated to IP-networking (which has the added benefit of allowing several buildings to be remotely monitored by a centralized operations center, such as cloud-based analytics); smart lighting not only allows intelligent centralized (and/or remote) control but also lowers energy consumption while improving the inhabitants' experiences. IoT will take these capabilities to the next level.

[1]BMSs are also known as building automation and control systems (BACSs), or as building control systems, or as building automation systems, or as building energy management systems, although this last term refers more specifically to systems that focus on energy management. ISO 16484-2:2004 uses the term BACSs.

TABLE I
VARIOUS FORECASTS IOT DEVICES IN USE WORLDWIDE

Source	Date Forecast Made	Forecast	Forecast date	Source
Ericsson	2010	50 B	2020	[11]
Cisco	2011	50 B	2020	[12]
IBM	2012	1000 B	2015	[13]
BSRIA	2015	50-200B	2020	[143]
Gartner	2015	6.4 B	2016	[15]
Gartner	2015	20.8 B	2020	[15] (13.5 B consumer, 4.4 B business/horizontal industries, 2.9 B business/vertical-specific) (65%, 21%, 14% respectively)
IDC	2015	9.1 B	2013	[16], [17]
IDC	2015	28.1 B	2020	[16], [17]
IHS	2014	17.6 B	2016	[18]
IHS	2014	40.6 B	2019	[18]
Ericsson	2015	28 B	2021	[19]
Stringify	2016	30 B	2020	[20]
IHS Markit	2016	30.7 B	2020	[21]
Median	**2016**	**30 B**	**2020**	(Estimate: 19.5 B consumer, 6.3 B business across various industries, 4.2 B business/vertical-specific) (65%, 21%, 14% respectively)

Intelligent lighting controls and heating, ventilation, and air conditioning (HVAC) optimization are just two of the key areas that are facilitated by the IoT. *Note:* Industrial energy management systems are not covered in this paper.

The IoT is expected to make major inroads during the second half of this decade and the first half of the next decade. Various forecasts for IoT deployments have been offered by key industry sources, as seen in Table I. The median figure is 30 B devices by 2020, with an estimate of 10.5 B devices in business applications. While this number is smaller than the original estimate, it is still a substantial number. In general, North America represents approximately 50% of the market. IoT is being driven by the precipitous drop in the cost of advanced sensors, computational power, and data storage, all while the device density has increased (and size has decreased).

In this paper, we review requirements for smart buildings (Section II). We then discuss how the IoT can assist buildings reduce energy costs (Section III), followed by a review of recent advances in power over Ethernet (PoE) technology (Section IV) and its application to next-generation building lighting (Section V). We then discuss how IoT can assist improving in-building surveillance (Section VI). Finally, we discuss some critical architecture, standardization, and cybersecurity concerns related to the wide scale deployment of IoT for building management applications (Section VII). Many references are available containing tutorial and survey material on IoT (e.g., but not limited to [22]). This paper intends to provide requirements and architectural concepts for the smart buildings using the IoTs.

II. SMART BUILDING REQUIREMENTS

Commercial buildings have a wide range of monitoring, management, and resource optimization requirements. These requirements span energy management (including lighting), video surveillance, access management, and environmental monitoring including fire detection [23]–[25].

Energy management is where one typically finds the greatest operational expenditures. Commercial buildings have multiple energy requirements. The list that follows (not exhaustive) identifies typical elements and systems where energy is consumed, all of which benefit greatly from improved (IoT-based) sensing, automation, and management.

1) *Server Room:* Telecom closets; racks and servers, including virtualized/blade servers; computer room air conditioners (CRACs); and uninterruptible power supplies (UPSs).
2) *Office Space:* Light emitting diodes (LEDs) lighting and daylight sensors; DR mechanisms (e.g., lighting); and thermostats (used in controlling HVAC systems and energy consumption).
3) *HVAC Room:* Chillers; air compressors; and modular boilers.
4) *Cooling System Elements:* Heat pumps; cooling towers; and rooftop units.
5) *BMS:* Proactive management of various mechanical, electrical, and plumbing (MEP) systems; also, elevator motors/DR.
6) *Electrical System:* Electrical distribution; centralized battery storage/UPSs; and emergency generators.
7) *Plumbing/Water System:* Water heaters; pumps/motors; and variable frequency drives (VFDs).
8) *Common Areas:* Advanced lighting technology; LED exit signs; bi-level lighting in emergency stairwells; and air diffusers.
9) *Retail Areas in Commercial Building:* For example, open and/or closed refrigerated cases; ovens; and LED lighting.

A VFD mentioned above controls the speed or frequency of a motor by monitoring the load: it adjusts the speed of the motor proportionally to the load of the space (or of the underlying function) to optimize the energy and runtime of the motor. VFDs are often used for pumps or fans that do not operate in a predetermined load condition, since reducing the revolution per minute of the motor results in saving energy consumption.

Although BMSs currently tend to focus primarily on electrical consumption, in the future BMSs (and the smart building IoT) are expected to focus on all energy sources supporting a building, also including natural gas, renewable energy, and so on. Additionally, it should manage other utilities such as water use and perhaps steam. IEAQ capabilities are also important. Sensors and sensor technologies of interest include demand-controlled ventilation, energy recovery ventilators, dedicated outdoor air systems, CO2 sensors, ultraviolet germicidal irradiation, displacement ventilation, and underfloor air distribution. As mentioned earlier, BMSs have evolved in recent years to support some of these devices and the underlying functions; however, comprehensive multisystem management using one

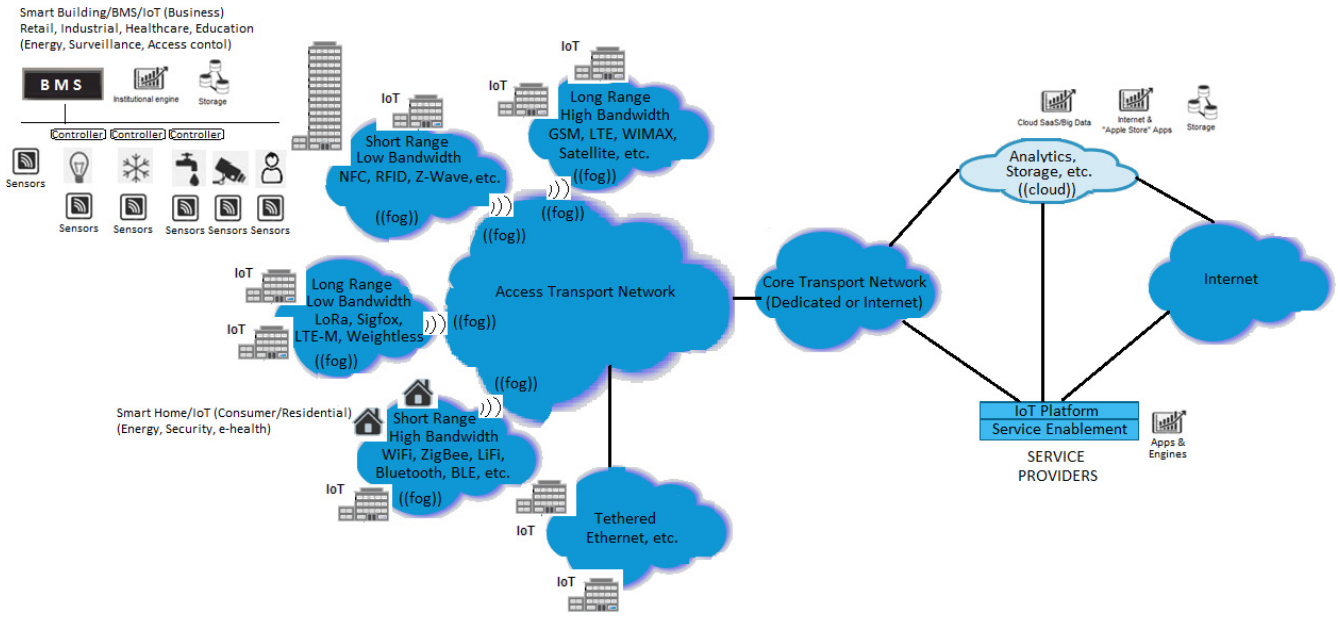


Fig. 3. IoT environment showing sensors, BMSs, aggregation networks, and cloud services.

all-inclusive BMS (in a manager-of-managers role) and standardization of data flows, data analysis, and actuation remain an unattained goal.

Energy efficiency optimization is driven by good business practices as well as by government regulations. In fact, there are a variety of city- and local-government directives to improve efficiencies (also under the auspices of the smart city initiatives). One example is Build Smart NY; it is a New York Governor's program for proactively pursuing energy efficiency in New York State (NYS) government-owned buildings, while advancing economic growth, environmental protection, and energy security in NYS. The Executive Order mandates a 20% improvement in the energy efficiency performance of State government buildings by April 2020 [26].

III. Energy Management

A relevant observation is that energy is a relatively big-ticket item for many industries, including office buildings and office campuses. According to the U.S. Energy Information Administration, Annual Energy Review [6], as an aggregate, the U.S. energy consumption is traditionally around 9% of the gross domestic product, in the range of $1.3T annually. In terms of actual usage, commercial offices consumed 20.4% of the total electrical energy, mercantile operations (retail stores and malls) 16.6%, educational institutions 10.8%, healthcare institutions 8.6%, and lodging 7.2% (the balance is used by other industries). While the energy expenditures vary by industry and by region of the country, as a comparative reference number a typical firm may expect to spend 5%–10% of its operating costs on energy. For example, a $1M company may spend upward of $100 000 a year and a $100M company may spend up to $10M per year in energy (some of these costs may be "sunk" into an office lease fee). As seen, about 81% of the expenditure in an office building, is generally associated with known elements; these elements can be targeted for efficiency improvements. For example, if a 20% improvement can be achieved, a typical $1 000 000 company could save $200 000 per year, or about a million dollars over five years (this assumes that savings accrues to the tenant—in some cases energy costs are prebuilt into the office space lease).

Energy efficiency is driven by a number of factors including: 1) social responsibility for green operations; 2) regulatory requirements; and 3) financial bottom line. BMSs in general and IoT-based environments, in particular, go a long way in addressing these needs. Larger facilities can realize higher relative efficiency gains, based on the idea that the more energy one is already wasting, the more the opportunity there is to save. BMSs are centralized systems that monitor, control and record the functions of building services systems, such as mechanical systems, elevators, electrical systems, HVAC, lighting, plumbing, security/surveillance, and contingency alarms [27]–[29]. BMSs enable the building operator to optimally control energy management; in addition, an IoT-ready BMS or a BMS adjunct can be used to manage other functions such as access, surveillance, fire detection, and so on. Typically, BMSs can be accessed and operated remotely.

Achieving the major benefits in the intelligent building paradigm depend on integrated energy management as enabled by software automation at the aggregation point and at the parameter sensing point; this software supports advanced (IoT-based) automation and control processes, real-time analytics, and building services flexibility. BMSs are evolving to integrate data from a variety of IoT-based sensors, covering multiple building systems (energy, lighting, and surveillance) and undertake, either directly or via cloud-based analytical tools, extensive data, trend, and usage analysis. The building blocks of a BMS are (see Fig. 3 for a pictorial view) as follows.

1) Sensors; these serve the purpose of measuring parameters such as temperature, humidity, lighting levels, and

Fig. 4. Top ten trends for the intelligent buildings market in 2016 and beyond, according to Navigant Research.

room occupancy. The IoT plays a role in facilitating the injection of smart "things" in the environment.

2) Controllers; these develop the system's response—the response is synthetized from the data that is collected by the sensors, by applying appropriate optimization algorithms.
3) Output devices; these actually implement the commands received from the controller.
4) Communications media and supportive protocols.
5) Data analytics.
6) Dashboard; this being the user's GUI for displaying data and accepting user queries or commands.

Typical functions (as implied in the list just provided) include the following.

1) *Operation Scheduling:* Establishing operating times for various lighting groups in the building.
2) Data collection from a large population of various (IoT) sensors for the devices listed in the previous sections.
3) *Trend Analysis:* A capability that provides graphic displays based on various time windows for the various streams/sensors.
4) *DR Simulation:* A capability that depicts the theoretical load impact of localized deployment of DR assets.
5) *DR Activation:* Implementing a DR plan.

Under the auspices of IoT, BMSs will evolve to be more complex, inclusive, and standardized systems, as depicted in Table II. Some industry observers perceive a near-term transition to a cloud-based management approach called "the energy cloud"; the expectation is that this transition will redefine the relationship between a building and the energy it consumes. One market research firm states "In 2016 and beyond [we] anticipate [that] building owners and key decision makers will invest in an array of buildings solutions that embody the technology foundation of the IoT and cloud computing" [30], [31]. As an illustrative example, Fig. 4 depicts some trends in the Intelligent Building market, according to Navigant Research[2] [32].

TABLE II
IOT-ENABLED BMSS

Aspect/ Feature	Current BMSs	Next-Gen/IoT-enabled BMSs
Scope	System (service) specific to given building functions	Supporting multi-system/multi-service fully integrated functions (e.g., energy, surveillance, alarming, etc.)
Function	Basic, tactical	Transformational, strategic
Sensors	Function-specific	Occupancy, motion, face recognition, CO_2, humidity, temperature, and Multifunctional Sensors
Protocols	Plethora of protocols	IP/IoT-based protocols
Access	Closed/local	Open/remote (e.g., app based)
Security	Basic	Advanced
Architecture	Closed, standalone	Open, networked
Analytics	Self-contained, limited functional data analyses	Cloud-based, multiple data sources (networked lighting, access controls, and demand response [DR] signals)
Effectiveness of control, including cost-controls	Basic	More extensive

It is recognized that small and medium commercial buildings (10 000 ft^2 [small] up to 100 000 ft^2 [medium]) have not yet experienced the same deployment of energy efficiency technologies as is the case for larger facilities; this is due in part to the lower disbursements on energy management

[2]According to Navigant Research, the global revenue for energy efficiency commercial building retrofits is expected to exceed $100 billion in 2025 for the commissioning and installation of upgraded HVAC, lighting, building controls, water efficiency, water heating, building envelope, and energy production equipment [32].

and to the ambiguous incentives as perceived by the building owner versus the tenant. An opportunity for expansion, therefore, exists.

The next paragraphs focus on data center-related power considerations. It was mentioned earlier that office buildings use an average of 17 KWh of electricity per square foot annually; however, some offices may also have a mini-data center function (full-fledged data centers are not discussed in this paper). For these offices, the power usage is higher. Racks with blade servers usually are rated at 10 KW per rack (on the average, depending on the number of chassis and blades); there are other power elements in the mini-datacenter (lighting, power distribution, etc.), usually increasing the load by about 40%. For example, a five-rack datacenter would consume 70 KWh. In this example, the room generates 70 KWh of heat. One can convert heat to BTUs or tonnage as follows: 1 KWh = 0.283 tons = 3412 BTUs. The room will have one or more dedicated CRACs. CRACs operate at a certain level of efficiency, typically around 70% also considering associated equipment (obviously, some of the newer technologies will be more efficient). In the example above one would need around 20 tons net of cooling, or about 30 tons rating for the CRAC; this will require 100KWh to operate (naturally, the configuration of the room, enclosures, humidity, etc. will also impact the overall net room efficiency). (A ton of air conditioning can cool about 3.5 kW of heat.) Therefore, the energy needed to run the five racks (in this example) is 170 KWh. Now, the yearly cost at \$0.10/KWh is $24 \times 365 \times 170 \times 0.1 = \$148\,920$ (note: the 2016 U.S. national average was \$0.1058/KWh for commercial customers; some regions have higher rates, e.g., NYS had a \$0.1512 [33]). If the upgrade of the technology and/or better controls could achieve a 10% savings, this would result in about \$15 000/year to the bottom line. The question is "is this sufficient motivation to do anything, especially considering the project management/complexity of replacing online, mission-critical technology?" Another issue is that some tenants pay a fixed power monthly fee embodied in the rent, so there is little motivation to do anything to upgrade the technology. A typical fee is \$2/square foot per year; thus, for a 5000-square foot office (say for a company with 20 employees) the utility fee is \$10 000 per year.

Note that the above calculation assumed that the racks were drawing minimum power on a constant basis (24×365). In reality, and also with the use of virtualized servers, the load may vary, with example in correlation for CPU usage. A figure of 30% KWh cumulative energy consumption, as integrated over a 24-h period, compared with the maximum (peak) load is a heuristic that can be employed in many (but not all) situations. This lower aggregate figure would decrease both raw expenditure for electricity use (if the mini-data center was metered), as well as the potential savings that may be accrued to the bottom line. Additionally, the current trend toward virtualization helps reduce physical server quantities and also reduces energy load. Newer servers typically come with power management systems that can automatically reduce power usage while in low-demand operation. The storage industry has institutionalized a trend to use more solid state rather than mechanical hard drives; just using solid state drives as cache for standard hard drive storage system can get better R/W response, reduce disk I/Os, and thus also decrease the energy usage and cooling cost. Having made these observations, it should not come as a surprise, however, that the computer industry is perhaps ahead of the rest of the industry-at-large in applying automation to manage power consumption, being that the industry has the "tools" and "visibility" to power processes and can thus leverage innovative solutions (also including IoT principles—see Table III). The goal is to extend these capabilities to the other MEP systems in a building.

At the practical level, the actual practice of building energy management is supported by specialized skills and certified professionals, including but not limited to the following (professional capabilities).

1) Leadership in Energy and Environmental Design (LEED) certification.
2) Certified Energy Manager as certified by the Association of Energy Engineers (AEEs).
3) Certified Energy Auditor, as certified by the AEE.
4) High-Performance Building Design Professional as certified by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE).
5) Building Energy Assessment Professional as certified by ASHRAE.
6) (For audits of multifamily residential buildings), Multifamily Building Analyst, as certified by the Building Performance Institute (BPI).
7) Certified Commissioning Professional certified by the Building Commissioning Association.
8) Certified Building Commissioning Professional as certified by the AEE.
9) Existing Building Commissioning Professional as certified by the AEE.
10) Commissioning Process Management Professional as certified by ASHRAE.
11) Accredited Commissioning Process Authority Professional approved by the University of Wisconsin.

IV. PoE Technology

PoE is increasingly being used to support many of the requirements identified in the previous section [34]–[36]. With PoE, dc power is transmitted on data conductors by applying a voltage to each pair. Ethernet utilizes differential signaling, hence the addition of a power signal does not interfere with data transmission. The components of a PoE system include the following.

1) *Power Sourcing Equipment (PSE):* Any device (end-span or mid-span) that allows power to be injected into a PoE network. End-span equipment could be a PoE-enabled Ethernet switch; a mid-span equipment is a mid-span PoE injector (a device that can be added to an existing network to provide energy on the Ethernet cable).
2) *Powered Device (PD):* Any end device powered by a PSE in order to operate [e.g., IP phone, wireless access point (WAP), and a surveillance camera].

TABLE III
EXAMPLES OF METHODS AND TECHNIQUES TO REALIZE ENERGY MANAGEMENT BASED ON IOT

Area of Interest	Energy management capabilities facilitated by IoT mechanisms
BMS (Building Management Systems)	IoT-based building-wide sensors for environmental control; IoT-oriented analytics for resource management. Provides the ability to measure, predict and define energy optimization actions based on defined parameters and time horizons (for example, scheduling). Operational cost management/reduction. Also, providing alerting, diagnosing, trending, and management reports summarization (e.g., monthly data, interval data, subdomain data, and so on.) Forecast usage and set desired goals (for example, to meet LEED requirements.)
HVAC controls	IoT-based environment management based on a plethora of criteria such as but not limited to tenant, floor, heat/AC preferences, time-of-day, day-of-week, seasons, number of people present, while optimizing occupant comfort. Load/peak-load management. For example, control doors/windows during cooling/heating season, vents management, thermostats management. Offers "constant commissioning". Facilitates building's performance tracking and benchmarking (comparisons), and also the synthesis of strategies for improvements.
Energy consumption controls	IoT-enhanced building appliances that are modulated by AMI (Automatic Metering Infrastructure)-oriented techniques. Demand response (DR) integration. Support accurate data collection to enable effective monitoring in real time and all the time.
Smart (indoor) lighting	IoT-based building-wide sensors to control lighting based on people's presence, time of day, natural light status, etc. (IoT-oriented occupancy sensors with timeout controls, motion sensitivity, and other factors). (For example, ascertain that there no areas where there is too much or too little lighting.)
Lighting as a Service (LaaS)	IoT-based building-wide sensors to support smart lighting with IoT-oriented cloud-based systems for lighting administration.
Smart elevator service	Optimal elevator management which allows fast service while minimizing energy consumption.
(In building) Data Center/Data Closet optimal management	IoT-based Computer Room AC (CRAC) management to optimize energy consumption.
Remote/centralized building management control	Manage a suite of building remotely/centrally utilizing IoT sensors/mechanisms, thereby ascertaining that optimal energy usage is achieved by having a complete dashboard of all assets that may belong to an organization.
Management of energy peripherals	IoT-based management/monitoring of emergency generators, automatic transfer switches, digital metering, uninterruptible power supplies, and so on.
Integration with Smart Grid and with Smart City	IoT-based effective integration into mechanisms offered under the auspices of Smart Grid and/or Smart City for enhanced efficiency.
Building-related surveillance/security	Building-related surveillance/security: IoT-based cameras and other presence sensors; IoT-specific analytics Building-based access control: IoT-based access badges that control access to building areas based on security level/clearance, time-of-day, etc.

Building and operations services facilitated by PoE include lighting, energy metering, HVAC, physical security/surveillance, access control, and sensor-rich environments; tenant services include smart meeting spaces, personalized space, IP telephony, WAPs, video distribution, and digital signage. PoE could have a disruptive impact in smart building technologies. The basic feature of PoE is its ability to deliver both content (LAN-based transmission) and device-supporting power over the same cable. PoE's key advantage resides in the economics of an integrated infrastructure, saving material and installation costs (and also including conduit space); in addition, it simplifies the deployment of endpoint devices (such as sensors, WiFi WAPs, and digital cameras), without requiring the installation of a high-voltage ac electric circuit. The expectation of industry proponents is that by 2020 over 90% of the desks in a commercial building [supporting knowledge workers, also with voice over IP (VoIP) at the desk] will have PoE; 80% of the WAPs, 50% of the security cameras, 20% of the access systems, 20% of the lighting systems, and 20% of the BMSs will also utilize PoE [14].

PoE implementation is a step along the continuum of the IoT deployment in smart/green buildings. Specifically, PoE lighting will transform the lighting industry and the enterprise environment, both in the office space as well in the Data Center. While PoE has intrinsic data connectivity applications, it is also being considered in lighting and other applications. LEDs provide improved lumens output compared with older lighting technologies, and a PoE standard for 60 W is reaching maturity (there also are proposals for the standardization for 95 W). PoE-based lighting is a step beyond so-called "smart lighting" because it affords a system that is connected to a centralized, software-based element that coordinates in a granular fashion all the luminaries, sensors, actuators, providing improved control and localized usage information that can be utilized for efficiency implementation (e.g., how many people are in the building at given times and where; how the working spaces are being utilized; natural lighting conditions; and multifloor/multibuilding optimization). The retrofit of older lighting fixtures is relatively straightforward.

In 2003, a standard was developed as the IEEE 802.3af that supported power delivery in the 15 W range (at 48 V dc). In 2009, the powering capabilities were extended with the introduction of IEEE 802.3at; power delivery in the 30 W range (at 53 V) was supported [37]. Extensions of these capabilities are now underway to support wattage in the 50–70 W range (IEEE 802.3bt, type 3) and even 100 W (IEEE 802.3bt, type 4). Delivering higher power to endpoint devices greatly increases PoE's application scope. PoE has been used extensively for VoIP and WAP applications and an increasing share of surveillance cameras are migrating to PoE/IP. Fig. 5 depicts existing and emerging applications of PoE while Table IV depicts the evolving PoE technologies. Some PoE devices (such as WAPs) require a category 6A cable considering its ability to support 10 GbE; other devices (e.g., door locks) do not need a high data rate or power and can, therefore, make use of standard category 5e cable; yet other devices have relatively high current draw, but low data rate flows (e.g., LED lighting), hence, these devices may best make use of a lower gauge category 5e cable. Note that "low" voltage installations are subject to different installation requirements than standard ac circuitry—for

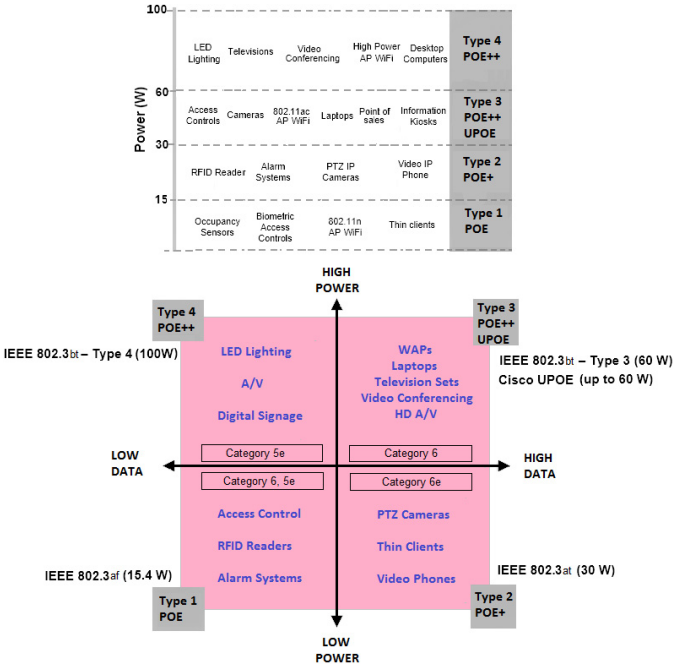


Fig. 5. PoE application examples. Top: POE types and supported power. Bottom: power and bandwidth requirements by application.

TABLE IV
EVOLVING POE TECHNOLOGIES

Standard / Feature	IEEE 802.3af (2003) Type1 PoE	IEEE 802.3at (2009) Type2 PoE+	IEEE 802.3bt (draft) Type 3 (4PPoE)	IEEE 802.3bt (draft) Type 4 (4PPoE)
Cable Pairs	2	2	4	4
Cable Type (minimum category)	Category 3/ Class C	Category 5e/ Class D	Category 5e/ Class D	Category 5e/ Class D
Power available to Powered device (W, max)	12.95	25.5	TBD	TBD
Power at Power Sourcing Equipment output (W, min)	15.4	29.5	49 to 70	100
Power Sourcing Equipment output voltage (V, nominal)	48	53	54	54+
Cable current (DC, mA, max)	350 per port	600 per port	600 per port	960 per port

example in some situations a "licensed" electrician may not be required by regulatory statute.

Category 5e cables typically are 24 gauge wires and achieve 79% power efficiency for PoE applications, while category 6 cables typically have 82% power efficiency. A 22-gauge (AWG) category 5e cable can provide 88% power efficiency for POE+ and future 4PPoE applications over 100 m distances. Calculations show that an 88% efficiency would save $78 in energy consumption compared to a system with 79% efficiency, over a ten-year period, per PD (calculation for a device that draws an average of 71 W over 100-m distances) [37].

One concern that has arisen relates to the temperature buildup in large bundles of cables carrying dc currents, that may be needed to aggregate all the devices in a building (or floor) to the data closet/server room. Temperatures increase when the cable is bundled. Studies show that on a category 5e cable (24 AWG) the 802.3bt can raise the temperature over ambient by about 21 °C; on a category 6 cable (23 AWG) the increase is about 19 °C (at 1000 mA); for category 6a (22 AWG) the temperature increase is 11 °C. As the temperature increases, so does the resistance and the insertion loss increase; this, in turn, results in performance degradation. Installers need to make sure that the temperature increase is not higher than the cable rating (which could also give rise to a fire hazard): for example, for 75 °C rated cable and 45 °C ambient temperature, the aggregation into larger bundles should be such that it does not contribute to more than 30 °C. There is work underway in various industry bodies (e.g., Underwriters Laboratories, IEEE, TIA, etc.) to define maximum temperature increase (for example specifications found in the IEEE 802.3bt and in TIA TSB-184). Table V depicts a current view of the recommended bundle sizes. The following factors impact the power-carrying capabilities of a cable.

TABLE V
POE/POE+/POE++ CABLE BUNDLE SIZE GUIDELINES

Cable Type	Gauge	PoE/PoE+ bundle size (max)	PoE++Type 4 bundle size (max) per Preliminary TIA Guidelines
Category 6A	23 AWG	100	74
Category 6	23 AWG	100	64
Category 5e	24 AWG	100	52
Category 6A	26 AWG	100	24
Category 6A	28 AWG	48	24
Category 6	28 AWG	48	24

1) Gauge size (larger gauge cables generates less heat).
2) Temperature rating (cables with a higher rating can better mitigate heat buildup).
3) Cable construction (shielded cables dissipate heat down the length of the cable and thus have improved performance).

It should be noted, however, that there are smart building applications that make use of wireless sensors. These sensors support control over building systems without requiring traditional cabling to address communications and power. Some sensors have batteries designed to last several years. The market and deployment are relatively small, but growing (estimated to quadruple in ten years). Another technology, although only marginally related deals with wireless powering of cellular-based devices, when they are in the general proximity of a transmitting tower. This is also a small market, but it is developing.

V. LIGHT APPLICATIONS OF POE/IOT

Lighting control using IoTs play an important role in smart building management and control. A number of vendor-specific approaches and technologies have been employed to date to achieve lighting control in buildings. The use of some standards-based methodology would be advantageous. It turns out that PoE in addition to supporting standard data/VoIP connectivity in the intranet and also supporting the IoT power and access to aggregate points, provide additional capabilities that are useful for lighting applications.

LEDs are semiconductors that are powered by dc signals. Commercial LED lighting is now steadily migrating to PoE technologies; this migration process is referred to as "lighting digitalization," "digital lighting transformation," or "networked lighting." UL-2108 allows PoE as a class 2 input power

source for low-voltage LED lighting systems. Systems based on organic LEDs is another area to watch, considering increasing deployment of the technology. The use of PoE affords the following advantages.

1) Lowers the installation costs (labor and material), while often speeding up the installation process.
2) Enables smart lighting controls.
3) Facilitates integration (increased facility flexibility, and access to analytics and metrics).
4) Enables new user experiences by creating specific (or time dependent) lighting situations (e.g., intelligent and granular lighting controls, daylight harvesting, workspace control, human-centric lighting and light temperature control, support of colors for room status, and pathway guidance.
5) Positions firm for future enhancements, e.g., connectivity for fixture-based dense sensor network for motion detection, air quality monitoring (CO2 and other gas sensors), LiFi, Light Fidelity, etc. (PoE lighting provides strategic ceiling asset placement that can later be used for advanced sensor technologies and other devices) [37]–[41].

Traditional lighting uses high-voltage cable carrying 100 or 277 V electrical signals. Control modules associated with a fixture provides some basic control (the connectivity is via a system such as BACnet, RS-485, and other legacy protocols). In a digital lighting infrastructure, the layer 2 switch provides power to the Ethernet cable to supports LED-based lighting and/or support other edge devices (e.g., WAPs, motion sensors, IP cameras, and HVAC variable air valves). Both power and control signals are distributed over the Ethernet cable. The control information (which uses IP at the network layer) is transmitted to an intelligent IP platform that contains analytics software; the platform can be local, but increasingly it is provided at a remote/centralized cloud location.

Digital lighting transformation and IoT will drive the convergence of a building's MEP systems and the intranet (or more generally, a building-dedicated IP network); in fact, building codes are gradually changing to incorporate digital building infrastructures. Some state that digital building infrastructure will be the IoT application that most employees will interact with [37] and [40].

Incremental energy savings related to lighting can be achieved by utilizing dense sensor networks and control of an individual fixture. Use cases include: electrical load shedding, personalized workspaces, granular occupancy, granular daylight harvesting, and flexible scheduling. Human-centric lighting increases productivity and comfort (perhaps even health); here the concept relates to changing the lighting temperature to synchronize with the circadian rhythm of workers. Some of these improvements are applicable to conference rooms, emergency lighting for evacuation or first responders. A low-voltage dc infrastructure is safer and efficient; it facilitates user/device adds, moves, and changes without having the need of turning circuit power off, while at the same time allowing the integration of lighting with applications and other building systems, which in turn has the potential to maximize energy savings.

Because not all users necessarily have the knowledge, resources, or tools to manage their lighting and exploit the latest (cost optimization) features, some see the emergence of a new service, specifically lighting as a service (LaaS) in commercial buildings, where a third-party entity uses cloud-resident management systems to optimally manage the lighting system (e.g., daylight harvesting, human-centric lighting, and so on) on behalf of the user. In some cases the third party also handles the financing of the upgrade to deploy the LED luminaries; occasionally this can be done while collecting rebates from the power companies or from state/national agencies advocating energy conservation.

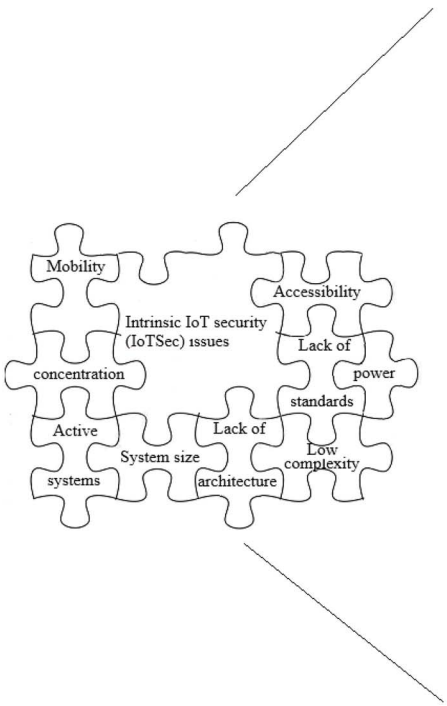
Another development with regards to IoT deployment is visible light communications (VLCs) technologies which may also emerge in the next few years [41], [42]. There have been systems that have used infrared transmission (outdoors as well as indoors—the former known as free space optical communications). VLC is generally thought of as encompassing visible light generated by LEDs. The term light fidelity (LiFi) is also used. In addition to illumination, LEDs can become transmitters of in-room data, based on their ability to modulate content over the optical beam, but with a process that is imperceptible to the human eye (this is achieved by intensity modulation techniques, namely by switching the current to the LEDs off and on at a very high rate, faster that can be noticed by the human eye).

VI. Surveillance/Physical Security

The confluence of IoT, PoE, IP (IPv4 as well as IPv6) is enhancing the functionality of surveillance, while utilizing the common intranet infrastructure [43]. While basic surveillance cameras used a few years ago required less than 12.95 W and thus could make use of the IEEE 802.3af technology, more advanced cameras in use today need more power. The use of PoE+ or 4PPoE is ideal for these applications, as is a migration to IP/IoT-based architectures. Camera construction is typically of the "box," "bullet," "fisheye," "fixed dome," or "pan/tilt/zoom (PTZ) dome" format. PTZ cameras are a common choice for many applications, offering the ability to point and zoom the camera to a specific area of interest. Bullet cameras usually utilize PoE, while domes and box cameras usually use a dedicated 12/24 VAC circuit. In the recent past, however, PTZ cameras have dropped in popularity because of much cheaper fixed-view cameras—basically it is much cheaper to deploy multiple fixed-view cameras than a PTZ, which is subject to more maintenance difficulty; also, 360° cameras have further reduced demand for PTZ technology.

IP-based video surveillance typically employs the following protocols: TCP/IP (IPv4 but in some cases also IPv6, particularly in the context of IoT), user datagram protocol (UDP)/internet protocol (IP) [unicast, multicast internet group management protocol (IGMP)], universal plug and play (UpnP), domain name system (DNS), dynamic host configuration protocol (DHCP), real-time transport protocol (RTP), real time streaming protocol (RTSP), and network time protocol (NTP). Functionally there are two kinds of IP surveillance cameras.

1) Centralized cameras that make use of a central system to support the recording and alarm management.



Intrinsic IoT security (IoTSec) issues	A large attach surface exists in the IoT environment; it encompasses the network-, the software-, and the physical attack surface. Specifically, every communication link (and network element) endpoint -- from the IoT device to the aggregation and/or analytics server – is part of the network attack surface. All software code in the IoT ecosystems has, in principle, exploitable vulnerabilities – again from the IoT device nodes to the aggregation and/or analytics server. At the physical level, if a device is not protected (for example, in its normal mode such as a camera on a pole – or in disturbed mode, if, for example, a device is lost or stolen), an attacker can access the device via physical attacks, and from there the rest of the IoT/IT ecosystem.
Low complexity devices	This predicament limits the amount of on-board computing that can be undertaken, including computing power needed for encryption, firewalling, and deep packet analysis.
Limited on-board power (for mobile devices)	This limits the amount of computing that can be undertaken, including computing needed for security algorithms.
Accessibility	Devices may be in an open environment and physically tampered with, stolen, or lost.
Mobility	The mobility of devices (including roaming on open networks, when outside of one's home) requires a mobility management mechanism (MMM) that not only consumes valuable computing resources but may place the device on some "foreign" network of unknown security status.
Active systems	IoT devices almost invariably "are always connected/always on", therefore they are in principle more susceptible to cybersecurity attacks (periodic re-authentication may be needed).
Points of concentration	Many IoT configurations make use of gateways to connect the devices to the larger network; this IoT gateway represents a concentrated point of attack. Similarly, there are other points of concentration that represent attractive targets point of attack, such as the data repositories.
Lack of agreed-upon end-to-end standards	IoT systems being deployed in the short term tend to be vendor-specific; wide-ranging, comprehensive standard have not been developed, have matured, or have been implemented. This often limits the usage of off-the-shelf security solutions.
Lack of agreed-upon architecture	IoT systems being deployed in the short term tend not to follow an accepted overall layered architecture, which would enable concept/function simplicity/standardization and the ability to integrate systems (including security systems) from various vendors, some of whom may be specialized to a given function (such as security), all of this resulting into a fragmented functional environment.
System size	There will be a large number of devices in the "system", requiring scalable solutions (some existing approaches to security may not scale).

Fig. 6. Challenges impacting deployment of IoT in general and in the smart building arena in particular.

2) Decentralized cameras that do not require a central system since the cameras have an integrated recording function (writing directly to a standard storage media, such as but not limited to a server or secure digital nonvolatile memory card.)

Modern cameras typically support 1080p (progressive) scanning with 1920 × 1080 resolution and a wide field of view (e.g., 180°). Surveillance cameras with lower (e.g., 640 × 480; or 12.5 frames/s at 12 megapixels) or higher (e.g., 2592 × 1944 or even 3200 × 3000, 16:9 aspect ratio, 30 frames/s) resolutions and frame rate are also available. Typically, MPEG-4/H.264 or (scalable) Motion JPEG is utilized for video compression. Connectivity is typically supported with WiFi (IEEE 802.11b/g/n), but Bluetooth or Z-Wave protocols are also supported. Storage is typically in the cloud, but local storage is also possible. Video management software (VMS) typically runs on a Windows-based computer and allows the manager to view multiple cameras, record and retrieve video, and monitor alarms; however, live video can also be viewed on a smartphone or tablet (e.g., with an iOS or Android app), or by using a Web browser. A few years back the Open Network Video Interface Forum and the Physical Security Interoperability Alliance (PSIA) developed some standards for IP video surveillance [44]. Open architecture connectivity allows the extensive use of third-party VMS and recording systems.

VII. IoT Development Issues, Architecture, and Cybersecurity Considerations

A. Development Issues

Industry stakeholders have recognized that there are some challenges to the broader injection of IoT technologies in the smart building arena, including standardization (vendor independent industry-wide architectures, frameworks, protocols), and, critically cybersecurity, challenges. For example, the IoT Security Foundation asserts that less than 10% of all IoT products on the market are designed with adequate IoT security (IoTSec) and the issue is well publicized [45]–[48]. Hence, the intrinsic IoTSec challenges need to be addressed; IoTSec is critically relevant to e/m-health applications. Fig. 6 enumerates some of the IoT-related challenges that have to be addressed by the stakeholder as well by the smart building industry; challenges include the following:

1) Intrinsic IoTSec issues.
2) Use of (vulnerable) gateways/concentration points.
3) Low-complexity devices.
4) Limited on-board power.
5) Open environment, allows tampering.
6) Device mobility.
7) Always connected/always on mode of operation.
8) Lack of agreed-upon end-to-end standards.
9) Lack of agreed-upon end-to-end architecture.
10) Device universe by type and by cardinality.

Although these challenges apply to the entire IoT ecosystem, some are more important to the energy management of smart buildings based on IoT than others; these include possible security issues (including gateways to and use of cloud-resident analytics systems), lack of agreed-upon standards and architectures, and the cottage and fragmented nature of this vertical industry at this time.

B. IoT Architectures

A number of IoT architectures (IoT-As) have emerged in the recent past, but there is not yet an industry-wide

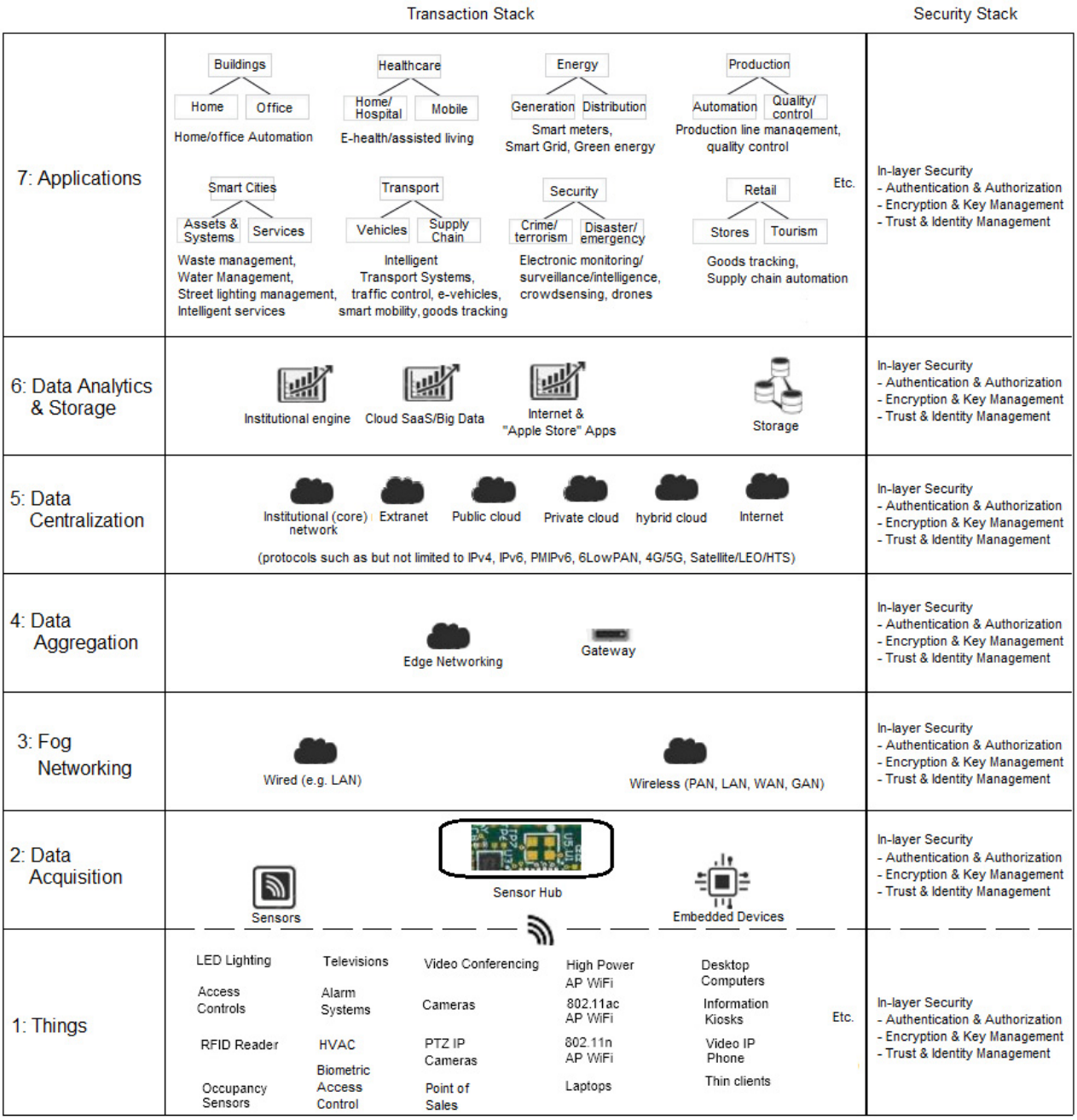


Fig. 7. OSiRM.

acceptance of any one particular framework [49]. The list includes the Arrowhead Framework; the ETSI high-level architecture for M2M; Industrial Internet Reference Architecture (IIRA); IoT-A; the evolving ISO/IEC WD 30141 IoT reference architecture (IoT RA); Reference Architecture Model Industrie 4.0 (RAMI 4.0); and the IEEE Standard for an Architectural Framework for the IoT (see Table VI). The dearth of agreed-upon architectures and standards up to the present have not only impacted the broad IoT deployment *per se*, but also have impeded the full integration of security mechanisms in the IoT applications. IoTSec is a major consideration in IoT, and the security architecture must consistently support a system state comprised of secure components, secure communications, and secure asset access control.

Authors recently introduced a seven-layer IoT-A model which we refer to as the open systems IoT reference model (OSiRM) that highlights the importance of security [57]. In practical terms, layer-specific mechanisms are needed (see Fig. 7 and Table VII). Security in general and security architectures in particular, depend on the availability of an underlying overall information and communication technology architecture, to build required capabilities upon a common, well-defined baseline. Architectures, frameworks, and standards enable seamless, even plug-and-play connectivity and operation. Some of the proposed IoT-As (as highlighted

TABLE VI
PARTIAL LIST OF PROPOSED IOT-AS (ALSO GENERALLY APPLICABLE TO E-HEALTH SYSTEMS)

Entity	Description
Arrowhead Framework [50]	An EU initiative aimed at open-networked collaborative automation of embedded devices with the idea of using TCP/IP everywhere, middleware nowhere. The Arrowhead Framework approach is to view IoTs as abstracted services; thus, intrinsically this IoT framework aims at global interoperability across multiple SOA (Service Oriented Architecture)-defined (IoT) environments. The framework is aimed at applications related to smart production, smart buildings, smart energy, and mobility.
ETSI High level architecture for M2M [51]	A relatively well-accepted framework, but it is principally focused on M2M, not the more general IoT environment. It concentrates on networking and communication. ETSI recognized that the M2M architecture needed to support a number of security capabilities, including sensitive data handling, security association management, access control and authorization, identity protection, and Security Administration.
Industrial Internet Reference Architecture (IIRA) [52]	The IIRA is a standard-based open architecture for Industrial Internet Systems (IISs). It is a general reference architecture developed by the Industrial Internet Consortium (IIC) (which includes firms such as AT&T, Cisco, GE, IBM, Intel, and others) focusing on functionality domains. The goal of IIRA is to enhance interoperability and to foster technology developments and standardization. To support broad industry applicability, the descriptions of the architecture are adequately abstract by distilling common characteristics, features and patterns from typical use cases. Basic characteristics include composability, portability, usability, maintainability scalability, reliability, and security.
Internet of Things Architecture (IoT-A) [53]	An architecture with a functional and data-oriented emphasis (a semantic approach looking at the interpretation of information and data also looking at business processes).
ISO/IEC WD 30141 Internet of Things Reference Architecture (IoT RA) [54]	Effort that aims at defining IoT domains and developing a reference model of IoT systems with the goal of facilitating interoperability among IoT entities. Some security work including defining level of assurance (LoA) was reportedly planned. The document was at Working Draft stage as of mid-2016. (An earlier initiative is documented in the ISO 29182 family of standards published in 2013, specifically the Sensor Network Reference Architecture [SNRA].)
Reference Architecture Model Industrie 4.0 (RAMI 4.0) [55]	A reference architecture for smart factories (domain-specific). The architecture uses a unified model for description of assets (including all assents in a plant from sensor/actuator to the control elements of the plant) and of products. It postulates an all-IP plant. It defines the concept of "Administration Shell (AS)." The AS provides a virtual representation of the real asset; data for status information of the asset in a consistent format; and the set of data that is generated during the process life cycle also in a consistent format. The AS is the central Data-Warehouse for the asset during the entire life cycle of a process.
Standard for an Architectural Framework for the IoT [56]	Architecture proposed by the IEEE P2413 WG; effort aims at developing an IoT framework, with emphasis on security, privacy, protection, and safety.
Other Standardization and/or architecture definition effort (partial list)	The International Telecommunication Union (ITU) (e.g., ITU-T SG 13, ITU-T JCA-IoT); The IEEE (e.g., P2413); The IETF; The 3GPP; The ETSI (e.g., ETSI TC Smart M2M and ETSI IoT Group); The Industrial Internet Consortium (IIC); The oneM2M; The European Research Cluster on the Internet of Things (IREC); The Smart Appliances (SMART) group; The GS1 EPCglobal Architecture Framework; and, The National Institute of Standards and the Technology (NIST) (for Smart Grids, NIST CPS PWG).

above) do include security considerations, but most include security as a homogenous vertical stack. To be truly effective, security mechanisms supporting confidentiality, integrity,

TABLE VII
DESCRIPTION OF SEVEN LAYERS OF OSIRM IN FIG. 7

Layer	Description
Layer 7	This is the "applications" layer. It encompasses a vast array of horizontal and/or vertical applications or "application domains" (also as described in terms Use Cases.) As is the case for Layer 1, effectively the list of applications is 'unlimited' in scope. Applications include smart cities, smart building, smart grid, intelligent transport, surveillance, sensing (including crowdsensing), intelligent production, and logistics, to name just a few.
Layer 6	This layer encompasses the "data analytics and storage functions".
Layer 5	This layer supports the "data centralization" function. This corresponds to the traditional core networking functions of modern networks. It includes institutionally-owned (core) networks, industry-specific extranets, public/private/hybrid cloud-oriented connectivity, and Internet tunnels. These networks are generally comprised of carrier-provided connectivity services and infrastructure and entail wireline and/or wireless links.
Layer 4	This layer supports the "data aggregation" function. This function may entail come kind of data summarization or protocol conversion (for example mapping from a thin, low complexity protocol used by the IoT clients in consideration of low-power predicaments, to a more standard networking protocol), as well as the edge networking capabilities. The data aggregation function is typically handled in a "gateway" device. Edge networking represents the outer tier of a traditional network infrastructure, the access tier, employing well-known networking protocols.
Layer 3	This layer supports "fog networking", that is, the localized (site- or neighborhood-specific) network that is the first hop of the IoT client ('device cloud') connectivity. Typically, fog networking is optimized to the IoT clients' operating environment and may use specialized protocols. It could be a wired link (e.g., on a factory LAN say in a robotics application), or wireless (on a wireless LAN, also optionally including infrared links, e.g., Li-Fi.)
Layer 2	This layer encompasses the "data acquisition" capabilities. It is constituted of sensors (appropriate to the "thing" and the higher layer "application"), embedded devices, embedded electronic, sensor hubs, and so on. Layer 1 and Layer 2 could be seen as being in symbiosis in the IoT world in the sense that things "married" with sensors become the IoT clients or endpoints. The collected information might be data parameters, voice, video, multimedia, localization data, and so on.
Layer 1	This layer is comprised of the universe of "things" that are subject to the automation offered by the IoT. Clearly this is a large domain, including (for example) people (with wearables, e/m-health medical monitoring devices, etcetera), smartphones, appliances (e.g., refrigerators, washing machines, air conditioners, etcetera), homes and buildings (including HVAC and lighting systems), surveillance cameras, vehicles (cars, trucks, planes, construction machinery), utility grid elements, and so on. Effectively, this list is 'unlimited' in scope.

and availability are needed at each of the architecture layers, and, as a bare minimum, encrypted tunnels, encryption of stored data, and key management are a critical part of IoT/IoTSec desiderata, if not absolute imperatives. In OSiRM, such capabilities are included at each layer.

C. Cybersecurity

Fundamentally, IoTSec requires the: 1) ability to the identify IoT devices and their administrative entities (for example a gateway); 2) protect the information flow between those devices and their administrative entities; and 3) prevent device

hijacking. In particular, scalable solutions are needed considering the large number of devices that is expected to be deployed by the end of the decade: a layered "building block" approach intrinsic in the OSiRM allows designers to utilize methods that can scale from low-cost microcontrollers to high-performance platforms.

OSiRM includes three security-related mechanism realms that are standard and effectively exist independently at each layer, as needed.

1) *Authorization and Authentication:* This mechanism supports part of the integrity requirement (who is the "user" and what kind of data can this user read/write/modify). It also supports part of the availability requirement [avoiding denial of service (DoS) incidents] (e.g., can this user multicast; can this user send data to point x in the network; can this user send more than y packets per second to point z in the network).
2) *Encryption and Key Management:* This mechanism supports the confidentiality requirement discussed earlier (keeping data from being read by unauthorized agents). As part of that process, one needs to protect cryptography keys from being misappropriated.
3) *Trust and Identity Management:* This mechanism supports the Integrity requirement (e.g., can the data or user be trusted). As part of that process one needs to control how software is modified (e.g., during a system upgrade) and also how data is modified by a legitimate entity (e.g., at a concentration/summarization gateway).

Other realms and mechanisms can be added to the OSiRM IoTSec model if deemed appropriate. Thus, the following mechanisms are intrinsically supported in a layer-oriented manner by the model: tamper resistance by specifying physical protection of devices; user identification by confirmation of the entities involved in a transaction; assured services with protection against DoS; system-wide secure communication via strong encryption; system-wide management of secure content via data integrity mechanisms; and system-wide secure network access: avoiding man-in-the-middle attacks. Additionally, in this OSiRM model, there will be optimized differences for a given security function at different layers, as well as specializations that may occur with the type of thing and/or type of application.

D. Lower Layers (Fog Networking Layer)

A number of connectivity solutions exist for the fog area, along with some security mechanisms (particularly for transmission confidentiality). For example, ZigBee, BLE, and Wi-Fi HaLow offer MAC-layer encryption in support of first-hop confidentiality, while others do not, and, thus, the developer or technology provider must provide encryption tools. Even when providing first-hop confidentiality, end-to-end confidentiality must be assured. As implied in the OSiRM model discussed above (and illustrated in Fig. 7 and Table VII), strong security measures for authorization and authentication, encryption and key management, and trust and identity management must be implemented at each layer of the model and end-to-end.

VIII. Conclusion

Smart buildings based on IoT concepts are expected to evolve rapidly in the next five years. The confluence of IoT, PoE, IP (IPv4 as well as IPv6) is expected to enhance the functionality, capabilities, energy efficiency, and cost-effectiveness of buildings, moving them up the automation continuum to a "smart building" status. In recent years, governments and regulatory agencies around the world have increased their focus on commercial buildings, given the fact that buildings are large consumers of energy. Continued regulation is expected (at least in some parts of the world), including mandates for greenhouse gas emissions targets. Therefore, stakeholders should investigate evolving technologies such a next-generation BMS, PoE, IoT, cloud services, and converged networks to get a better handle on the issue, save expenses on the bottom line, and future-proof their environments and their investments.

In the face of some of the challenges faced by energy management of smart buildings based on IoT-centered systems (a number of which were highlighted in Section VII), there are significant industry and technical opportunities. The desire to reduce energy costs both by the building owners and the tenants, as well by the energy suppliers looking to cut peak-rate consumption and construction of peaking power plants, along with the optimization of comfort levels for office users and residents for both temperature and lighting conditions, affords this industry a strong business opportunity. From a technology perspective, the development of appropriate architectures and supporting standards, such that both equipment cost-effectiveness and interoperability will be beneficial. It is also critical to develop and deploy strong IoTSec capabilities system-wide. Another important transition is currently underway: core carrier networks are in the process of adopting the principles of function virtualization, driven by the goals of reducing hardware costs and increasing functionality; virtualization has already been successfully and profitably adopted by the enterprise community during the past 15 years for server consolidation and improved computing throughput and goodput. The anticipated migration by carriers to network function virtualization/software defined network-based network elements by the turn of the decade, will enable networks to be better suited to carry IoT traffic (for example from the building to the cloud), increasing communication flexibility, optimizing resource management and service provisioning, and simplifying the administration of the network [58]–[62]. Finally, the development of cloud-based high-quality analytics will facilitate global optimization and appropriate data mining, trending, and forecasting.

Acknowledgment

The authors would like to thank J. Chang, DVI Communications, for very helpful insights.

References

[1] K. Xu, Y. Qu, and K. Yang, "A tutorial on the Internet of Things: From a heterogeneous network integration perspective," *IEEE Netw.*, vol. 30, no. 2, pp. 102–108, Mar./Apr. 2016, doi: 10.1109/MNET.2016.7437031.

[2] S. Ray, Y. Jin, and A. Raychowdhury, "The changing computing paradigm with Internet of Things: A tutorial introduction," *IEEE Des. Test.*, vol. 33, no. 2, pp. 76–96, Apr. 2016, doi: 10.1109/MDAT.2016.2526612.

[3] M.-S. Kim *et al.*, "Managing a very connected world: A report on APNOMS2015," *J Netw. Syst. Manag.*, vol. 24, no. 3, pp. 754–763, 2016, doi: 10.1007/s10922-016-9366-z.

[4] Y. Zorian, "Keynote 3: 'Ensuring robustness in today's IoT era,"' in *Proc. 10th Int. Design Test Symp. (IDT)*, Amman, Jordan, Dec. 2015, p. 1, doi: 10.1109/IDT.2015.7396723.

[5] F. Saffre, "Tutorial II: The green Internet of Things," in *Proc. 11th Int. Conf. Innov. Inf. Technol. (IIT)*, Dubai, UAE, Nov. 2015, p. XXXVII, doi: 10.1109/INNOVATIONS.2015.7381499.

[6] *Commercial Buildings Energy Consumption Survey (CBECS), Energy Usage Summary*, U.S. Energy Inf. Admin., Washington, DC, USA, 2012. [Online]. Available: http://www.eia.gov/consumption/commercial/reports/2012/preliminary/

[7] Q. Wang, W. Wang, and K. Sohraby, "Energy efficient multimedia sensing as a service (MSaaS) at cloud-edge IoTs and fogs," *IEEE Multimedia Commun. Tech. Committee Commun. Front.*, vol. 11, no. 4, pp. 6–8, Nov. 2016.

[8] A. H. Oti, E. Kurul, F. Cheung, and J. H. M. Tah, "A framework for the utilization of building management system data in building information models for building design and operation," *Autom. Construct.*, vol. 72, pp. 195–210, Dec. 2016, doi: 10.1016/j.autcon.2016.08.043.

[9] E. Z. Tragos *et al.*, "An IoT based intelligent building management system for ambient assisted living," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, London, U.K., Jun. 2015, pp. 246–252, doi: 10.1109/ICCW.2015.7247186.

[10] A. Corna, L. Fontana, A. A. Nacci, and D. Sciuto, "Occupancy detection via ibeacon on android devices for smart building management," in *Proc. Design Autom. Test Europe Conf. Exhibit. (DATE)*, Grenoble, France, Mar. 2015, pp. 629–632.

[11] H. Vestberg. *CEO to Shareholders: 50 Billion Connections 2020*. Accessed on Apr. 13, 2010. [Online]. Available: https://www.ericsson.com/thecompany/press/releases/2010/04/1403231

[12] D. Evans. (Apr. 2011). *The Internet of Things: How the Next Evolution of the Internet is Changing Everything Whitepaper*. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[13] J. Iwata. (2012). *Making Markets: Smarter Planet—IBM Investor Briefing*. [Online]. Available: http://www.ibm.com/investor/events/investor0512/presentation/05_Smarter_Planet.pdf

[14] Staff, *BSRIA Study Shows Big Data and Convergence Is Growing*, BSRIA Ltd., Bracknell, U.K., Dec. 2015. [Online]. Available: http://www.bsria.co.uk

[15] *Gartner Says 6.4 Billion Connected Things Will Be in Use in 2016, Up 30 Percent From 2015*, Gartner News, Stamford, CT, USA, Nov. 2015. [Online]. Available: http://www.gartner.com/newsroom/id/3165317

[16] *IDC's Worldwide Internet of Things Taxonomy, 2015, Worldwide Internet of Things Forecast, 2015–2020, and the Worldwide IoT Spending Guide by Vertical*, IDC, Framingham, MA, USA, May 2014. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS25658015

[17] *IDC Market in a Minute: Internet of Things*, IDC, Framingham, MA, USA, May 2014. [Online]. Available: http://www.idc.com/downloads/idc_market_in_a_minute_iot_infographic.pdf

[18] B. Morelli. *IHS Technology Abstract, Internet of Things Report—2014: Internet of Things Installed Base Grows to 40.6B by 2019*. Accessed on Jan. 13, 2017. [Online]. Available: https://technology.ihs.com/518173/internet-of-things-overview-december-2014

[19] *Ericsson Mobility Report*, Ericsson, Coimbatore, India, Nov. 2015. [Online]. Available: http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov 2015.pdf

[20] A. Nordrum. *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated IEEE Spectrum*. Accessed on Aug. 18, 2016. [Online]. Available: http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-isoutdated

[21] A. Green, *Internet of Things Overview Report—May 2016*, Whitepaper, IHS Markit, London, U.K., May 2016. [Online]. Available: http://blog.ihs.com/technology-internet-of-things-iot

[22] D. Minoli, *Building the Internet of Things With IPv6 and MIPv6*. New York, NY, USA: Wiley, 2013.

[23] H. Ghayvat, S. Mukhopadhyay, X. Gui, and N. Suryadevara, "WSN-and IOT-based smart homes and their extension to smart buildings," *Sensors*, vol. 15, no. 5, pp. 10350–10379, 2015, doi: 10.3390/s150510350.

[24] I. Mauser, J. Feder, J. Müller, and H. Schmeck, "Evolutionary optimization of smart buildings with interdependent devices," in *Applications of Evolutionary Computation* (LNCS 9028). Cham, Switzerland: Springer, 2015, pp. 239–251.

[25] C. Keles *et al.*, "A smart building power management concept: Smart socket applications with DC distribution," *Int. J. Elect. Power Energy Syst.*, vol. 64, pp. 679–688, Jan. 2015, doi: 10.1016/j.ijepes.2014.07.075.

[26] G. C. Quiniones *et al.*, *Build Smart NY, Executive Order 88 Guidelines—New York State Government Buildings, Office of the Governor*, New York Power Authority, White Plains, NY, USA, Dec. 2012.

[27] P. Bellagente, P. Ferrari, A. Flammini, and S. Rinaldi, "Adopting IoT framework for energy management of smart building: A real test-case," in *Proc. IEEE 1st Int. Forum Res. Technol. Soc. Ind. Leveraging Better Tomorrow (RTSI)*, Turin, Italy, Sep. 2015, pp. 138–143.

[28] F. Tao, Y. Wang, Y. Zuo, H. Yang, and M. Zhanga, "Internet of Things in product life-cycle energy management," *J. Ind. Inf. Integr.*, vol. 1, pp. 26–39, Mar. 2016, doi: 10.1016/j.jii.2016.03.001.

[29] Y. Sun, T.-Y. Wu, G. Zhao, and M. Guizani, "Efficient rule engine for smart building systems," *IEEE Trans. Comput.*, vol. 64, no. 6, pp. 1658–1669, Jun. 2015, doi: 10.1109/TC.2014.2345385.

[30] C. Talon, *North American Energy Management for Integrated Data Centers Revenue Is Expected to Reach $119.7 Million in 2024*, Navigant Res., Boulder, CO, USA, Jul. 2016.

[31] C. Talon, *Building Energy Management System Revenue Is Expected to Total Nearly $55 Billion From 2015 to 2024—The Transition to the Energy Cloud Will Redefine the Relationship Between Buildings and Energy*, Navigant Res., Boulder, CO, USA, Aug. 2016.

[32] Staff, *Global Revenue for Energy Efficiency Commercial Building Retrofits Is Expected to Exceed $100 Billion in 2025*, Navigant Res., Boulder, CO, USA, Jul. 2016.

[33] *Electric Power Monthly, Table V.6.A. Average Price of Electricity to Ultimate Customers by End-Use Sector*, U.S. Energy Inf. Admin., Washington, DC, USA, Jun. 2016. [Online]. Available: http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_6_a

[34] Electrical and Electronics Engineers (IEEE) 802.3af and IEEE 802.3at (PoE plus), ieee.org.

[35] D. Wesemann, J. Dünnermann, M. Schaller, N. Banick, and S. Witte, "Less wires—A novel approach on combined power and Ethernet transmission on a single, unshielded twisted pair cable," in *Proc. IEEE World Conf. Factory Commun. Syst. (WFCS)*, Palma, Spain, May 2015, pp. 1–4, doi: 10.1109/WFCS.2015.7160588.

[36] R. Hua *et al.*, "Power over Ethernet method, apparatus, device, and system," U.S. Patent 9 268 383, Feb. 23, 2016.

[37] M. Eisen, *Introduction to PoE and the IEEE802.3af and 802.3at Standards*, Marcum Technol., Melville, NY, USA, Oct. 2009. [Online]. Available: https://www.ieee.li/pdf/viewgraphs/introduction_to_poe_802.3af_802.3at.pdf

[38] T. Feiden, *Power Over Ethernet (PoE) Design Considerations, Superior Essex Technical Materials*, Superior Essex Inc., Atlanta, GA, USA, Mar. 10, 2016.

[39] M. Magno, T. Polonelli, L. Benini, and E. Popovici, "A low cost, highly scalable wireless sensor network solution to achieve smart LED light control for green buildings," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2963–2973, May 2015, doi: 10.1109/JSEN.2014.2383996.

[40] *Digital Ceiling Framework: New Lighting Solutions from Digital Ceiling Partners*, Cisco Press Release, Berlin, Germany, Jan. 13, 2017. [Online]. Available: http://investor.cisco.com/investor-relations/news-and-events/news/news-details/2016/Can-Your-Business-Compete-Accelerate-Business-Transformation-With-New-Cisco-Digital-Solutions-and-Offers/default.aspx

[41] H. Haas, L. Yin, Y. Wang, and C. Chen, "What is LiFi?" *J. Lightw. Technol.*, vol. 34, no. 6, pp. 1533–1544, Mar. 15, 2016.

[42] V. S. Saptasagare, "Next of Wi-Fi an future technology in wireless networking Li-Fi using led over Internet of Things," *Int. J. Emerg. Res. Manag. Technol.*, vol. 3, no. 3, Mar. 2014, pp. 142–147.

[43] Z. Li, Z. Tang, and Y. Yang, "Research on architecture of security video surveillance network cascade system with big data," *World J. Eng.*, vol. 13, no. 1, pp. 77–81, 2016. [Online]. Available: http://dx.doi.org/10.1108/WJE-02-2016-010

[44] *ONVIF Expands Profile Concept With Physical Access Control, IP Video Integration Release Candidate*, ONVIF, San Ramon, CA, USA, Aug. 2013. [Online]. Available: http://www.onvif.org

[45] *IoT Security Foundation*. Accessed on Jan. 13, 2017. [Online]. Available: http://www.iotsecurityfoundation.org

[46] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.
[47] J. Granjal, E. Monteiro, and J. Sá Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.
[48] C. Lai, R. Lu, D. Zheng, H. Li, and X. Shen, "Toward secure large-scale machine-to-machine communications in 3GPP networks: Challenges and solutions," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 12–19, Dec. 2015.
[49] R. T. Tiburski, L. A. Amaral, E. de Matos, and F. Hessel, "The importance of a standard security architecture for SOA-based IoT middleware," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 20–26, Dec. 2015.
[50] Arrowhead. *Automation Systems From IoT Arrowhead Framework: Concepts and Basic Architecture*. Accessed on Jan. 13, 2017. [Online]. Available: http://www.arrowhead.eu/material/automation-systems-from-iot-arrowhead-framework-concepts-and-basic-architecture/
[51] *ETSI TS 102 690: Machine-to-Machine Communications (M2M); Functional Architecture*, ETSI, Sophia Antipolis, France, Oct. 2011.
[52] "The industrial Internet reference architecture, version 1.7," Ind. Internet Consortium, Needham, MA, USA, Tech. Rep. IIC:PUB:G1:V1.07:PB:20150601, Jun. 4, 2015. [Online]. Available: http://www.iiconsortium.org/IIRA.htm
[53] *Internet-of-Things Architecture (IoT-A), Project Deliverable D1.2—Initial Architectural Reference Model for IoT*. Accessed on Jun. 16, 2011. [Online]. Available: http://www.iot-a.eu/public/public-documents/d1.2
[54] International Organization for Standardization, ISO Central Secretariat, Geneva, Switzerland, Jun. 2015.
[55] P. Adolphs, *RAMI 4.0: An Architectural Model for Industrie 4.0*, Plattform Ind. 4.0, Berlin, Germany, Jun. 2015. [Online]. Available: www.plattform-i40.de (http://www.omg.org/news/meetings/tc/berlin-15/special-events/mfg-presentations/adolphs.pdf)
[56] IEEE P2413. *Standard for an Architectural Framework for the Internet of Things (IoT), IEEE Standards Association—Working Group Site & Liaison Index*. Accessed Jan. 13, 2017. [Online]. Available: http://grouper.ieee.org/groups/2413/
[57] K. Sohraby, D. Minoli, and J. Kouns, "IoT security (IoTSec) considerations, requirements, and architectures," in *Proc. 14th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2017, Art. no. 888ff.
[58] K. Xu, X. Wang, W. Wei, H. Song, and B. Mao, "Toward software defined smart home," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 116–122, May 2016, doi: 10.1109/MCOM.2016.7470945.
[59] S. K. Tayyaba *et al.*, "Software-defined networks (SDNs) and Internet of Things (IoTs): A qualitative prediction for 2020," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 11, pp. 385–403, 2016.
[60] K. Joshi and T. Benson, "Network function virtualization," *IEEE Internet Comput.*, vol. 20, no. 6, pp. 7–9, Nov./Dec. 2016.
[61] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Commun. Mag.*, vol. 53, no. 2, pp. 90–97, Feb. 2015.
[62] B. Özbek, Y. Aydoğmuş, A. Ulaş, B. Gorkemli, and K. Ulusoy, "Energy aware routing and traffic management for software defined networks," in *Proc. IEEE NetSoft Conf. Workshops (NetSoft)*, Seoul, South Korea, Jun. 2016, pp. 73–77, doi: 10.1109/NETSOFT.2016.7502446.

Daniel Minoli is a Principal Consultant with DVI Communications, New York, NY, USA. He possesses many years of technical hands-on and managerial experience in planning, designing, deploying, and operating secure IP/IPv6-, VoIP, telecom-, wireless-, satellite-, and video-networks for global best-in-class carriers and financial companies. He has taught IT and telecommunications courses with New York University, New York, Stevens Institute of Technology, Hoboken, NJ, USA, and Rutgers University, Brunswick, NJ, USA. He authored or co-authored 60 technical books and 300 papers and has made 85 conference presentations. His current research interests include M2M/Internet of Things, network security, satellite systems, wireless networks, IP/IPv6/Metro Ethernet, video/IPTV/multimedia, VoIP, IT/enterprise architecture, and network/Internet architecture and services.

Kazem Sohraby received the B.S., M.S., and Ph.D. degrees from New York University (Polytechnic Engineering Division), New York, NY, USA, and the M.B.A. degree from the Wharton School, University of Pennsylvania, Philadelphia, PA, USA.

He is a Professor of electrical engineering and computer engineering with the Department of Electrical and Computer Engineering, South Dakota School of Mines and Technology, Rapid City, SD, USA. He was with Bell Labs, Murray Hill, NJ, USA, Lucent Technologies, Murray Hill, the Stevens Institute of Technology, Hoboken, NJ, USA, the University of Arkansas, Fayetteville, AR, USA, and the Computer Sciences Corporation, Falls Church, VA, USA. He has 22 granted and pending patent applications. He has authored or co-authored over 260 peer-reviewed papers and 2 textbooks in the field of computer science, wireless, and electrical engineering. He has been cited 2840 times in IEEE-level papers.

Benedict Occhiogrosso received the degree from the Polytechnic School of Engineering, New York University, New York, NY, USA.

He is a Co-Founder of DVI Communications, New York. His experience encompasses a diverse suite of technical and managerial disciplines including sales, marketing, business development, team formation, systems development program management, procurement and contract administration budgeting, scheduling, QA, technology operational, and strategic planning. As both an Executive and Technologist, he enjoys working and managing multiple client engagements, as well as setting corporate objectives. He is responsible for new business development, company strategy, as well program management. He has also served as a testifying expert witness in various cases encompassing patent infringement and other legal matters.