IQT QUARTERLY

VOL. 4 NO. 3 WINTER 2013

BUILDING INTELLIGENCE: Envisioning Smart Infrastructure

IQT IN·Q·TEL

IQT Quarterly is a publication of In-Q-Tel, Inc., the strategic investment firm that serves as a bridge between the U.S. Intelligence Community and venture-backed startup firms on the leading edge of technological innovation. *IQT Quarterly* advances the situational awareness component of the IQT mission, serving as a platform to debut, discuss, and debate issues of innovation in the areas of overlap between commercial potential and U.S. Intelligence Community needs. For comments or questions regarding IQT or this document, please visit www.iqt.org, write to iqtquarterly@iqt.org, or call 703-248-3000. The views expressed are those of the authors in their personal capacities and do not necessarily reflect the opinion of IQT, their employers, or the Government.

EDITORIAL

IQT Quarterly, published by In-Q-Tel, Inc.
Editor-in-Chief: Emma Resnick
Theme Editor: James H. Smith
Contributing Editor: Brittany Smith
Managing Editors: Lisa L. Bader and Lisbeth Poulos

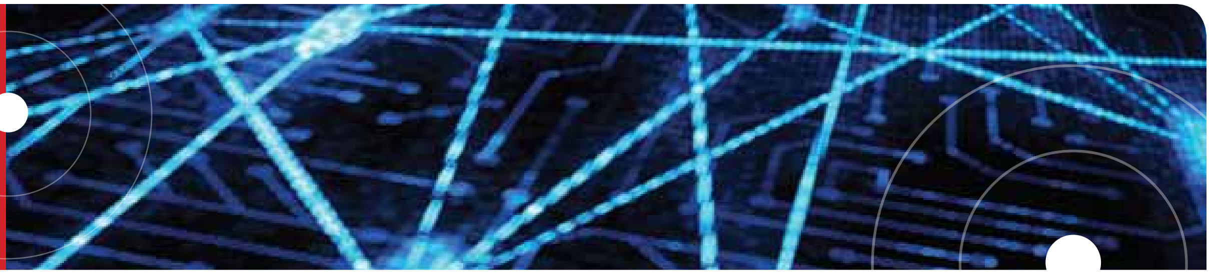
Design by Lomangino Studio LLC
Printed in the United States of America

IQT QUARTERLY

Identify. Adapt. Deliver.™

TABLE OF CONTENTS

ON OUR RADAR



BUILDING INTELLIGENCE — THE FIRST THINGS THAT MATTER IN THE INTERNET OF THINGS

By James H. Smith

The Internet of Things and, in particular, the availability of home automation, is beginning to affect each of us. In addition to managing high energy consumption for heating and cooling, access control, security, and life safety in both commercial and residential applications, connected widgets are having a dramatic impact on our lives, starting with our local indoor environments (homes, schools, offices, factories, etc.). Smart devices include baby monitors for infants, latchkey monitors for children, and systems that help the disabled and elderly continue to live in their own homes, with higher quality of life and less need for assistance from caregivers.

Home automation has been developing since 1885, when Albert Butz patented the furnace regulator and alarm — which became the company Honeywell. These systems evolved slowly over the next century but predominately remained as single purpose, stand-alone, dedicated control and reporting systems that were hardwired between fixed monitoring and control locations. As the Internet (and the concept of generalized connectivity) entered the picture in the 1980s and 90s, followed by the widespread adoption of mobility (i.e., smartphones, PDAs, tablets, laptops) in the 2000s, home automation systems began to slowly adopt IP-based communications, while also introducing the mobile handset as a tool for monitoring and controlling these systems. Today we are witnessing the interconnection and coordination of these systems.

The use of IP-based communications within each of these (previously) dedicated systems means that the coordination of systems is only a few lines of code and a quick modification to a firewall away from integrating information and control across these individual domains into a cohesive system.

My experience with smart buildings includes a beach house originally built in 1873 that now is bursting at the seams with IP-based networks such as GigE, Wi-Fi, Bluetooth, Z-Wave, and General Packet Radio Service (GPRS), the data service on GMS phones. For the first 137 years of its existence, the most sophisticated control system this house contained was a modern derivative of the furnace regulator developed by Butz — a two to four wire control system that closed an electrical circuit when the temperature dropped below a set level at a central monitoring point (called the thermostat) and closed a switch that activated the furnace. Access to the home was managed with the old style skeleton key in a mortised lock until it was replaced by a deadbolt in the 1970s. Remote access control and monitoring were accomplished by neighbors or in-person visits from rental agencies and home watch companies well into the 2000s.

In the current decade, rapid changes have occurred. A residential home monitoring and control system from 2GIG provides HVAC control, access control, fire and burglar monitoring, and lighting control. It also monitors for unexpected events such as out-of-range temperatures (indicating the furnace is malfunctioning) and flooding (indicating a pipe has burst). The classic wired central station monitoring has been replaced by a cellular GPRS data connection that is accessible by the user not only at a dedicated control panel within the house but also from any web browser or smartphone. Calls from the central station have been replaced by SMS messages. In order to monitor these previously disparate systems, the control panel has interfaces not only for the conventional "wired" sensors but also for Z-Wave locks, lights, and thermostats; for ISM-band wireless security (doors and windows, motion, glass break, flood, etc.) sensors; and for cellular data (GPRS).

Visits by home watch companies have been replaced by a 2GIG system, monitoring various sensors within the house and an outdoor IP-based camera (which does double duty monitoring for storm damage and providing a view of the ocean to my desktop in Virginia). The rental agent distributing a physical key to the occupants has been replaced by a Z-Wave door lock and an access code. Instructions to turn the heat down and the A/C off when the occupants leave have been replaced by a set of Z-Wave thermostats interconnected with the alarm system so that temperatures adjust automatically depending upon the occupancy of the house. Simple coordination functions such as disabling the circulation fans within the HVAC system if a fire is detected within the house are also implemented. All of these control systems can operate independently (including battery backup) on the premises but they also report to a cloud-managed service over a GPRS cellular modem. The cloud service manages the rules that interconnect these systems and provides remote monitoring and access from web browsers and mobile devices.

Although most people only interface with a remotely managed system like this for a week's vacation, these systems are becoming ubiquitous and will have dramatic effects on all of us as we and our loved ones age.

Members of the Intelligence Community (IC), need to ask themselves how to prepare both defensively and offensively for the coming adoption of Building Intelligence. Classic "INT"s such as MASINT or SIGINT overlap the area of Building Intelligence. However, a new term such as BuildINT or IoTINT (for Internet of Things) would be more appropriate. Significant intelligence on patterns of life can be derived from access to the information flowing among these systems. Even if the information is protected by encryption, the timing, volume, and header information of these packets can be used to provide meaningful insights on patterns of life. Moreover, these systems are migrating towards cloud management, where the data is no longer confined to the premise, and the potential economical and societal benefits of centralized management need to be tempered by the security implications of the Cloud.

Perhaps some of these systems are already helping to manage your household or care for loved ones, giving you the opportunity to contemplate the future implications of this technology. My next venture into automated systems will start with a trip to the Apple Store for their new line of IP-connected light bulbs that change color based on the colors in photographs on your iPhone. I have no idea (today) of what real value a light bulb with an IP address has (except the cool factor), but perhaps you can start to imagine the intelligence applications of mauve vs. amber lighting changes. That's up to the reader. For now, I'm going to stare at the ocean feed at my desk and ignore the IP packets around me. Q

James H. Smith *serves as Technology Vice President on IQT's Technical Staff in the Physical and Biological Technologies practice. He has previously held VP Engineering and Director of Technology roles with Fortune 500 companies such as L-3 Communications, Honeywell, and AlliedSignal. He co-founded Transparent Networks, Inc., a Silicon Valley-based developer of switches for all optical networks. Early in his career, Smith developed a number of MEMS-based technologies and components at Sandia National Laboratories. He earned a Ph.D. in Engineering from Penn State, has an MBA, and is a registered Professional Engineer. He is a senior member of the IEEE and a member of the American Society of Mechanical Engineers.*

A LOOK INSIDE: ENVISIONING SMART INFRASTRUCTURE

This edition of the *IQT Quarterly* considers how the Internet of Things is manifesting in smart buildings — both commercial and residential. The smart devices that make up these networks are designed to enhance the comfort and productivity of building occupants while optimizing systems to save energy and money. The contributors in this issue provide perspective on the future of automated systems and on the relevance of analytics, discuss the application of cloud computing to smart infrastructure, and offer case studies for the use of smart, connected devices.

Kamin Whitehouse's article frames the issue by discussing both the opportunities for improved efficiency as well as the security and privacy challenges presented by intelligent buildings, particularly residential structures. He outlines some of the threats presented by having sensors in a building, detailing what information an intruder may be able to glean by observing or tapping into relevant communications.

Mark M. Duszynski follows with an explanation of how building automation systems bring together sensor data from throughout a building onto a single user interface, resulting in an "Internet of Things" within the building. This allows a building owner or tenant to control loads from a centralized location and improves occupant comfort and energy consumption. He also considers the role of analytics in building automation.

James Caton explores the implementation of smart building technology in federally owned and administered buildings. He focuses on programs currently being implemented by GSA, and looks to the future of monitoring technology to imagine where it could take us.

Next, Gordon Feller discusses the potential for smart cities and communities. He recognizes that converged IP networks and cloud-managed IT infrastructures are key to the scaling and integration of automation in large buildings, smart communities and cities, and in large-scale residential rollouts. He also reviews the benefits of cloud computing for IT management and cost.

In his article, Jeremy Warren outlines how the building automation trend specifically affects the residential and small business markets. Recent developments in this space have focused on simpler, standardized, cost-effective solutions that contrast with the previous generation of high-cost, custom products. Warren explains how the next generation of devices for smart buildings integrate seamlessly with existing devices to enhance user comfort and energy and cost savings.

Finally, Joseph F. Coughlin, Bruce Mehler, and Bryan Reimer from the MIT AgeLab discuss the emerging trend of high-performance environments that support elderly care and aging independently. In particular, they describe the MIT AgeLab's AwareCar, which detects driver state and performance to indicate driver stress and can provide real-time interventions to achieve optimal driver performance, thus allowing aging drivers to experience the freedom and independence of mobility.

As automated systems continue to proliferate in our homes, offices, schools, and vehicles, we encourage you to contemplate the power of those smart and connected devices. Consider both their potential to improve quality of life, as well as their role as a unique source of information on habits and lifestyle.

THE RISE OF THE INTELLIGENT BUILDING

By Kamin Whitehouse

Americans spend a great deal of time indoors. Homes, office buildings, and commercial buildings serve as the literal foundation of society, enabling — and in many ways also influencing — the nation's business, personal, and family operations. In recent years, buildings have rapidly transformed from static brick-and-mortar structures to dynamic and highly responsive pieces of machinery that are infused with information technology, including an extensive array of sensors and controllers. Indeed, many buildings today require a "brain" to operate properly, typically in the form of a computer server. The dawn of these intelligent buildings brings a host of new opportunities for improved performance and efficiency, as well as new threats to privacy and security.

Opportunities

Sensing, intelligence, and control can improve building performance along several dimensions, including comfort, safety, and even structural integrity. However, energy efficiency and physical security have been two of the biggest factors driving trends toward building instrumentation and digitalization over the past several decades.

Buildings account for about 40 percent of the total U.S. energy budget, which is more than all trains, planes, cars, buses, and boats combined. Additionally, buildings account for 70 percent of the nation's electricity usage, and are a significant factor in growing pressure on generation plants and the power grid. The biggest energy consumers in buildings include lighting, water heating, and space heating, ventilation, and cooling (HVAC). Therefore, the conventional way to save energy is through physical retrofits such as improved insulation, equipment upgrades, or LED lighting replacements. However, these retrofits often face resistance in the marketplace due to the high capital expenses required. In contrast, computer intelligence can reduce energy usage substantially, often at a fraction of the cost of a physical building retrofit. As a result, building energy management systems (BEMs) are already in widespread use in commercial buildings to monitor, analyze, and manage lighting systems and the HVAC system, and recent studies have demonstrated energy savings of up to 15 percent by aggressive monitoring and optimization of commercial buildings.[1] Today, BEMs have higher market penetration in commercial buildings than residential buildings, due in part to the difficulty of reaching residential markets, as well as lower financial incentives for home owners in comparison to building managers. Instead, residential homes are much more likely to contain an ad hoc set of commercial electronic products, such as programmable thermostats, lighting automation, and wireless sensors. Despite their do-it-yourself nature, these systems offer big opportunities for improved comfort and energy efficiency. For example, recent studies have found that investing $25 in additional sensing systems — when combined with the right computer algorithms — can reduce home heating and cooling energy by 28 percent by heating or cooling the home only when people are actually present.[2] In comparison, thousands of dollars of building insulation would be required to achieve a similar level of energy savings.

Home automation and energy efficiency have been recent trends in the digital home, but historically it was physical security that drove the installation of sensors in homes. Today, an estimated 32 million homes in the U.S. have security sensors installed on doors and windows, as well as motion sensors installed inside and/or outside the home. In commercial buildings, security systems not only secure the perimeter of the building, they provide fine-grained access control within the building using RFID "key cards" or electronic passcodes. Many commercial buildings are also equipped with dozens of security cameras both inside and outside, motion sensors to actuate doors automatically, and automated lighting systems. As these systems become more economical, more intelligent, and more connected to the Internet, they will provide detailed information about who is in the building, which rooms they have used at any given time, and which other people were in the rooms at the same time. This information creates new opportunities far beyond physical security, with applications ranging from real-time meeting scheduling to social network and productivity analysis.

Threats

In order to provide useful services, sensors in buildings must collect rich information about the occupants' daily lives. However, these same systems can often collect far more information than needed, and can do so with or without the occupants' knowledge or permission. Researchers have shown that electrical power consumption data collected by power utilities can be used to infer when a household has gone on vacation, when it cooks dinner, and even which television shows it watches.[3] Smart power meters are already widely deployed in homes across the U.S. by utility companies for billing purposes, and are increasingly equipped with wireless communication for real-time data collection and fine-grained power metering. Similar approaches could be used on commercial buildings to infer, for example, when machinery is in heavy use or when employees are working late — perhaps to guess the upcoming release date of a competitor's new product. Many building information systems are connected to the Internet for remote monitoring and management, leaving companies and government agencies vulnerable to attack.

Many sensors in buildings, and particularly in homes, now use wireless communication to reduce the cost of installing communication lines. Wireless, battery-powered devices can be easily installed with a few screws or even double-sided tape, with no wiring required. Many professional home security systems today use wireless communication, and millions of homes also contain do-it-yourself systems, such as wireless doorbells, appliance controls, or wireless light switches. Today, over 30 percent of homes are estimated to contain some form of wireless sensors, and the home automation industry is expected to grow rapidly in coming years, marketing products for home security, automation, energy conservation, and elderly monitoring. However, researchers have shown that wireless transmissions can reveal even more information about a household than power meters. For example, an intruder can drop a small, battery-powered receiver outside a home and infer detailed activities such as showering, toileting, and sleeping, and can even differentiate between the preparation of hot and cold food.[4] Information is revealed even if all wireless messages are securely encrypted. This attack uses only the *fingerprint* of each radio message: a set of features of a radio frequency waveform that are unique to a particular transmitter. Based on the fingerprints, the attacker can infer how many wireless devices are in the home, and when each of them transmits. Then, by analyzing patterns and similarities in their wireless transmissions, the attacker can classify each device as a motion sensor, light switch, or refrigerator, identify which devices are in the same rooms, and infer the activities of the building occupants.

In addition to an increasing number of sensors and electronic devices, buildings are also becoming increasingly connected to the Internet, which further increases the electronic attack surface of a building. Modern commercial buildings are extensively instrumented with occupancy sensors, lighting automation, door or window status, AV systems, and power and water meters. This data is typically collected in an online Building Information System (BIS), and could be used to infer activity

Many building information systems are connected to the Internet for remote monitoring and management, leaving companies and government agencies vulnerable to attack.

patterns inside the building if the BIS security is compromised. Other home activities that collect data are connected to the Internet through game and movie consoles, home monitoring systems, and Internet-enabled thermostats.

On the Horizon

New developments in sensor technology will continue to produce richer information at a lower cost, multiplying both the opportunities and the threats related to building monitoring. For example, a recent sequence of developments has made it possible to monitor individual electrical, water, and gas fixtures with a single sensor on each system. These sensors use noise in the electrical signal, pressure waves in the water pipes, or movement of gas in the gas lines to identify when individual fixtures are being turned on or off. The single-point sensing solutions reduce hardware and installation costs while simultaneously providing rich information and creating new opportunities for home monitoring and analysis. At the same time, these developments open new threats because similar sensors could also be installed outside of the home without the occupants' knowledge, for example, on the power transformer or on the city gas or water lines.

One key challenge for building monitoring is to identify what people are doing without instrumenting the people themselves, particularly in homes where people do not use key cards for security access and are less likely to carry cell phones or wireless transmitters. This problem is now being addressed by so-called weak biometric sensors that identify people based on height, weight, color, and other features that distinguish people but don't uniquely identify them. For example, the Doorjamb sensing system uses ultrasonic range finders mounted above each doorway and pointed downward to measure the distance to the person as he or she walks between rooms.[5] It estimates the height of a person by measuring the distance to the top of the head when the person is directly under the door frame and estimates walking direction based on its ability to detect the person on either side of the door frame before and after walking through it. The system then differentiates people based on their heights and identifies room locations based on their walking direction and the sequence of doorways through which they pass. The Doorjamb sensors snap in behind the door jamb to hide architecturally and contain motion sensors, door latch sensors, temperature, light, and humidity sensors, and a magnetometer. These sensors are used to automatically infer the floor plan of the house and the location of the sensors within that floor plan so that the meaning of sensor data can be interpreted. Once the system knows the floor plan and the room occupancy, it correlates occupancy patterns with aggregate electrical and water data to learn the existence and location of fixtures in each home. For example, if kitchen occupancy is commonly associated with 100W electrical on/off events, the system infers that the kitchen has a 100W light bulb. All of this information is learned within 1-2 weeks, at which point the system goes into real-time monitoring mode to detect who is in the house, which rooms they are located in, and the activities they are performing in terms of water and electrical fixture usage. This system is called the "Marauder's Map" because it performs this monitoring without instrumenting the occupants or the fixtures; it does not require occupants to wear RFID tags or wearable devices, nor does it include privacy-invasive sensors such as cameras or microphones. The Marauder's Map can provide a detailed, real-time picture of both occupancy and energy usage in the home, which can be used for wide-scale analytics and prediction of energy usage information for improved management of a smart power grid. In production quantities, systems like these will be inexpensive and can be installed in minutes, creating a range of new opportunities for home and occupant monitoring.

Conclusion

Recent developments in technology are transforming buildings from primarily structural designs to complex electro-mechanical systems, where software and data are as important to proper function as roof and walls. This transformation is expanding the capabilities of buildings and creating a range of new opportunities for improved comfort, convenience, energy efficiency, and physical security. There is a fundamental tension, however, between privacy and the creation of new information, and buildings are no exception. Engineers, policy makers, occupants, and all building stakeholders must be aware of both the opportunities and the threats, because the infusion of technology into intelligent buildings will continue to accelerate. Q

__Kamin Whitehouse__ works in the area of wireless embedded systems, with a focus on applications in intelligent buildings. He is an Associate Professor in the Computer Science Department at the University of Virginia, and was awarded a CAREER award by the National Science Foundation. He earned his BA and BS from Rutgers University and his MS and PhD from UC Berkeley.

REFERENCES

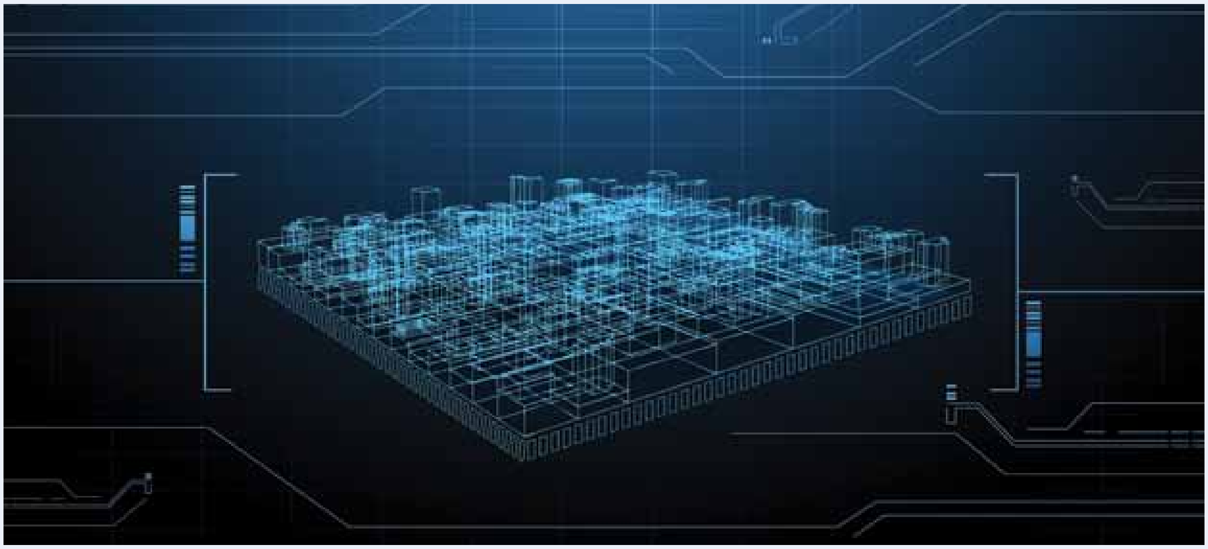
[1] Yuvraj Agarwal, Bharathan Balaji, Seemanta Dutta, Rajesh K. Gupta, and Thomas Weng. Duty-Cycling Buildings Aggressively: The Next Frontier in HVAC Control. In Proceedings of the 10th Conference on Information Processing in Sensor Networks: Sensor Platforms, Tools and Design Methods (IPSN / SPOTS '11), April 2011.

[2] Jiakang Lu, Tamim Sookoor, Vijay Srinivasan, Gao Ge, Brian Holben, John Stankovic, Eric Field, Kamin Whitehouse. The Smart Thermostat: Using Occupancy Sensors to Save Energy in Homes. The 8th ACM Conference on Embedded Networked Sensing Systems (SenSys). November 3-5, 2010, Zurich, Switzerland.

[3] P. McDaniel and S. McLaughlin. Security and privacy challenges in the smart grid.IEEE Security & Privacy, volume 7, pages 75-77, 2009..

[4] Vijay Srinivasan, John A. Stankovic and Kamin Whitehouse. Protecting Your Daily In-home Activity Information from a Wireless Snooping Attack. In Proceedings of the Tenth International Conference on Ubiquitous Computing (UbiComp). Seoul, Korea, September 2008.

[5] Timothy Hnat, Erin Griffiths, Raymond Dawson, and Kamin Whitehouse. Doorjamb: Unobtrusive Room-level Tracking of People in Homes using Doorway Sensors. The 10th ACM Conference on Embedded Networked Sensing Systems (SenSys'12). November 7-9, 2012, Toronto, Canada.



THE POWER OF INTEGRATED BUILDING AUTOMATION SYSTEMS

By Mark M. Duszynski

In the office building of the future, dozens of disparate systems and sensors will work together to provide for the comfort, convenience, and safety of its occupants. Tenants' needs for lighting and temperature control will be anticipated. Air quality will be monitored and maintained. Life safety and security systems will combine to offer enhanced protection. New information networks will control these activities and many more to provide an optimal and productive work environment for building occupants.

This will all be accomplished with significant improvements in energy efficiency. Vast quantities of systems data will be automatically analyzed to present facility managers with the means to fine tune building operations. The future office building will even communicate with the power grid to shift energy needs to meet the most advantageous pricing schedules.

For years, futurists have written about smart buildings that can do all of these things. But that future is here today. Here is a look at how a smart building of today might operate:

A federal agency executive prepares to drive to her office building early Saturday morning to catch up on work. Before she leaves, she opens a smartphone app to notify the building automation system of her expected arrival time. As she parks in the underground garage, the elevator is ready to transport her to her 26th floor office. The lights in hallways and her office turn on just before she arrives. As she enters her office on this hot summer morning, the room is already cooled to a comfortable temperature. When she leaves several hours later, sensors detect her absence and automatically turn off the lights and A/C. This was a pleasant and convenient experience for the employee, while the building owner saved money by using the building systems only when and where needed.

Building Automation Networks Conserve Energy and Optimize Systems Operation

Significant recent advances in integrated building automation technology and the ability to utilize wide-ranging networks are what make smart buildings possible.

Many existing buildings contain a collection of autonomous systems that do not consistently cooperate to reduce energy usage. Each system has its own design intent: comfort, lighting, security, communications, information management, or power distribution. Smart buildings are designed to integrate different systems, including heating, ventilation and air conditioning (HVAC), lighting, physical security, fire and life safety, energy metering, networking, computing resources, telephones, projectors, elevators, escalators, plug loads, and parking. The results are improved occupant comfort, reduced energy consumption, and cooperation with the emerging smart energy grid.

The Basic Technology Creates an "Internet of Things" Within a Facility

In its most basic form, a building automation system brings together all sensor data across the building onto a single user interface, allowing a building owner to control loads from a centralized location. More advanced smart buildings automate building management and decentralize control by allowing the device that creates the data to interoperate with other building devices over one or more communications networks. Features like comfort control, time scheduling, weather response, optimal start, intelligent demand response, energy and emissions reporting, and distributed energy resource management are delegated to policies running on networked devices. These devices collectively create the "Internet of Things" within a building.

To achieve the desired convenience and savings, commercial building owners are bringing virtually all facility subsystems together under a single point of control. These open-platform, network-based systems constantly monitor building operations, collecting data, controlling systems, and providing building staff with the information it needs to more efficiently manage and maintain systems and equipment.

The freedom of the future-ready IT infrastructure is powerful. Building owners and tenants have the flexibility to add best-in-class enhancements and technologies as they become available. The building automation system allows operators to better program equipment based upon the occupants' needs or process requirements, while providing tenants with more control of their own space during off hours.

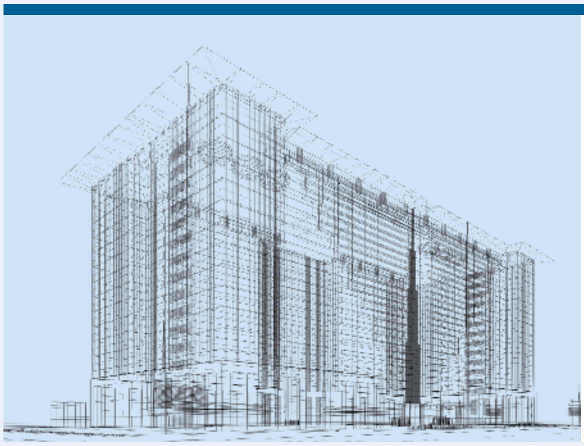
This technology fits with new construction as well as with retrofits of existing buildings. A good example is New York City's iconic Empire State Building. An extensive energy efficiency makeover is already saving building owners and tenants $2.4 million annually. When the project is fully completed, yearly savings will increase to $4.4 million.

Building automation systems monitor and control the security function through a shared control, allowing operators to conveniently manage all functions from one console. The savings can be significant. One Florida university that completed the convergence process was able to reduce the number of system operators, saving $350,000 annually in staffing costs.

Optimization Routines in More Detail

Minimizing energy consumption is an important application within buildings, which account for 40 percent of U.S. energy use. Here are several steps that are helping to achieve energy conservation.

Demand limiting is for managing both electric consumption and demand to meet contractual electricity requirements. Some buildings have contracts that impose a penalty for over-consuming instantaneous energy. A typical contract uses the peak demand set during a previous block of time (typically a month) to establish the demand charge for the next year. A smart building implements one or more corrective actions when electrical demand exceeds the predefined level. Within the building, automated demand response applications use pricing information to minimize electrical costs by starting/stopping equipment, adjusting set points, and starting distributed generation assets.



Critical to the smart electric grid is open, frequent, and seamless communication between a wide range of systems, devices, platforms, and operators using Internet protocols.

Load shifting reduces electrical costs but does not typically lower the total energy consumed by a facility. It shifts electrical demand to times of low grid demand — often accompanied by lower prices and, in some situations, "negative prices," where the building owner is paid to consume energy to help maintain a steady load on spinning resources on the grid. One of the more common load-shifting strategies is thermal energy storage, which creates ice at low-cost electricity times, using it to replace electrically powered mechanical cooling when electricity prices are high.

Smart buildings also need to **measure distributed energy resources** such as solar, wind, or micro turbines to help manage and forecast energy usage. This is especially true when generating excess kilowatt-hours that are being sold back to the grid or credited to the bill.

Building Systems also Interact with the Electrical Distribution Grid

Communication between the electric grid and a customer-owned building is a top priority and an important enabler of the smart grid. Critical to the smart electric grid is open, frequent, and seamless communication between a wide range of systems, devices, platforms, and operators using Internet protocols. In this "Internet of Things," a smart building is not only self-aware, but also receives and acts on signals from outside the facility. In order to get the necessary scale, grid services like tariff awareness, ancillary services, demand forecasting, emissions reporting, and intelligent demand response will need to be sent directly to the devices within the building. These devices will act upon all major infrastructure systems including HVAC, process control, lighting, elevators, access control, and electrical distribution.

With more customers affected by time-varying energy tariffs, a smart building will be able to interpret tariffs and provide recommendations to customers on how to operate buildings to optimize energy costs. The smart building will provide a decision support service by analyzing different usage scenarios and determining the lowest cost option that meets the occupants' overall objectives. After the customer selects an option, the smart building will schedule the equipment to operate at the appropriate times and at the capacity to meet the objectives.

Analytics Play a Key Role in Building Automation

Building automation systems excel at providing information about a building's energy use and equipment operations. This vast quantity of information is an example of what is known as "big data." These data sets can become so large and complex that it becomes difficult to process the information in a meaningful way.

New software-based building analytical processes are putting building operators in total control, from anywhere, at any time. They are expanding the functionality of existing building management systems driven by the technologies that are a part of

our everyday world — the Cloud, apps, smart devices, and online communities. These technologies allow building professionals to see exactly how every system is functioning and to take actions to improve their performance.

The open technology platforms work with any building management system. By creating cloud-based Software as a Service (SaaS) subscription offerings for data access and storage, the need for large capital investments has been eliminated. Building owners can then choose to focus on the most critical priorities to themselves and their tenants.

Using cloud computing, building data is forwarded to offsite controllers via the Internet or cellular networks. These controllers analyze the data and send commands to building actuators over the same communications paths. Mission critical control continues to be hosted on-site but many of the less time-critical control algorithms are hosted at the remote controller.

This approach to building efficiency will help building managers to detect abnormal energy consumption and equipment faults; track energy usage and carbon emissions across an enterprise; create energy baseline models and track savings from energy-efficiency projects; and provide flexible trend analysis to compare facilities, diagnose problems, and report performance. With the information all cloud-based, it can be viewed from virtually any PC or mobile device with web access.

By adding additional data sources such as lighting schedules, conference room booking, water use patterns, entry/exit statistics, wireless network load, unused parking spaces, after-hours overrides of ventilation and lighting systems, individual tenant occupancy behaviors, and deliveries and shipments, big data analytics could provide tremendous insight into the operations of a company or institution and employee activities.

Network Security and Vulnerabilities

State-of-the-art smart buildings rely on the same open protocols and communication standards used in the IT community to facilitate communication between disparate nodes in the building and external devices. Open standards enable a common Internet language where information can be shared between data producers and data consumers, unlocking the proprietary roadblocks of older building systems.

Many legacy building system networks are open and unsecured. At the time they were built, information security was provided through closed, unpublished communications protocols. As more systems adopt standard or open communications protocols, security vulnerabilities have increased. Again, smart buildings are looking to Internet technology to solve this problem by adopting security protocols like Hyper Text Transfer Protocol Secure, Secure Sockets Layer, and Private Key Infrastructure. User credentials also protect smart building user interfaces.

The building automation system is designed to easily connect systems from different suppliers. Open standard communication protocols, such as BACnet, facilitate this connectivity. Using the existing IT network infrastructure lowers the cost of installing and maintaining a building automation system. An insecure system on a secure IT network has the potential to introduce vulnerabilities, but this can be overcome with careful design. It is also important to consider the security implications when access to the building automation system is provided through mobile and handheld devices.

Beyond IT security, a building automation system controls the fans, ducts, and dampers that comprise an effective system for distributing air, and anything the air is carrying, throughout a facility. Aerosol hazards introduced in easily accessed ground-level outdoor intake vents could propagate quickly. Using these same HVAC fans and air dampers, building systems can be designed to create pressure differentials throughout a facility. This is a common strategy in healthcare, where certain areas benefit from negative pressure (isolating an infectious airborne pathogen), or from positive pressure (protecting an immune-deficient patient from non-sterile air inrush when a door is opened). These same strategies can be used to route smoke away from egress routes during a fire, or to protect critical facilities from malicious introduction of biohazards. The ability to pressurize and route smoke was credited with protecting survivors of the September 11, 2001 attack on the Pentagon.

Attracting the Federal Tenant

Today, any commercial building owners seeking to attract federal tenants will have to place their facilities on the cutting edge of energy efficiency. That will mean incorporating building automation systems and data management platforms.

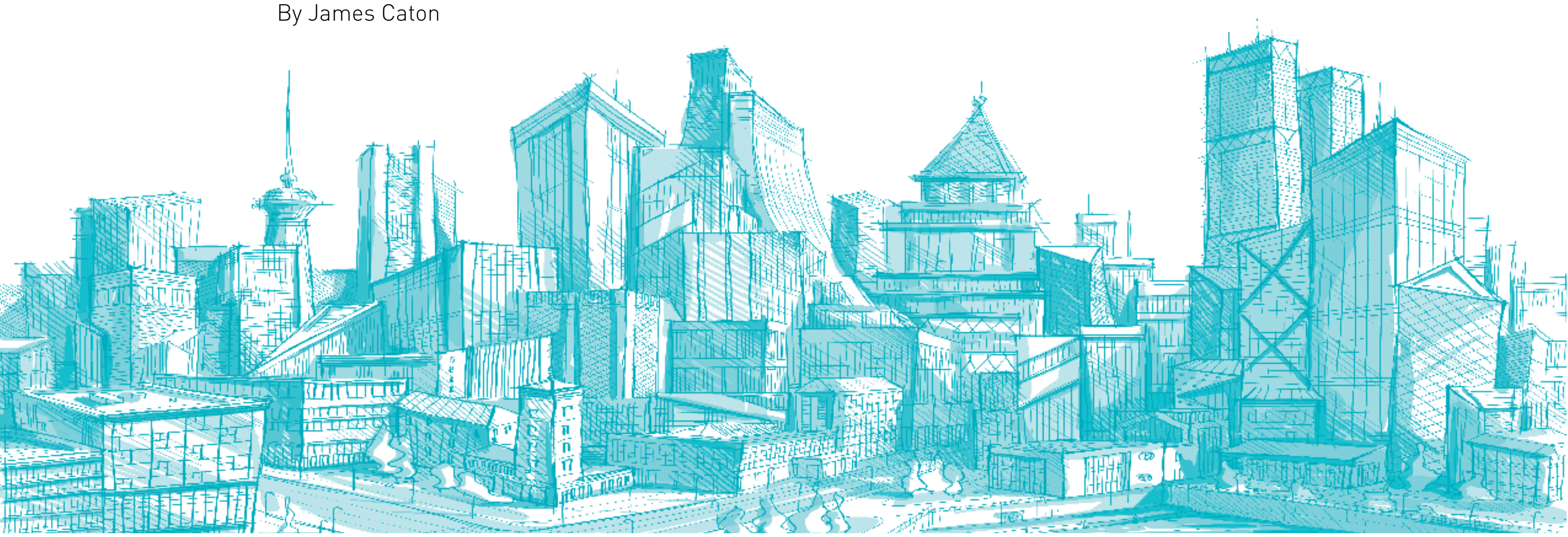
The ever-evolving building automation technologies have created new standards for energy efficiency, physical security, life safety, and tenant comfort and convenience. Today's smart buildings automatically operate more efficiently, provide detailed operational data, and know when to take advantage of smart grid opportunities for added savings.

All this helps to meet the growing list of federal requirements regarding the performance of leased and owned space for federal intelligence and other agencies.

Mark M. Duszynski *is Vice President of Strategic Marketing, Federal Systems for Milwaukee-based Johnson Controls, the global leader in delivering facility management systems and solutions that increase the overall efficiency of commercial, institutional, and industrial buildings. He received a Bachelor's degree in chemical engineering and an MBA from the University of Wisconsin, and has over 30 years of experience in the building systems and energy management industries.*

GSA IMPLEMENTS SMART BUILDINGS 2.0

By James Caton



One of the Obama administration's key initiatives has been a series of Executive Orders that require federal agencies to address energy efficiency, greenhouse gas management, overall sustainability, and meet specific energy reduction targets. This has perhaps had the biggest influence on the General Services Administration, Public Buildings Service (GSA PBS), which acts as the landlord for civilian federal government. The agency owns or operates almost 10,000 buildings and manages 370 million square feet of space every day for 1.1 million federal employees.

The PBS has been actively working to reduce their environmental footprint for years. In 2008, agency representatives visited one of IBM's "green" data centers in Boulder, Colorado to understand how industry was addressing data center energy efficiency and what might also apply in the federal space.

GSA BuildingLink

Fast forward to April 2012, when the GSA PBS awarded IBM a contract to implement Smart Building technologies to monitor the agency's top energy consuming buildings. The system, now dubbed BuildingLink, will monitor thousands of data points in each building at up to five-minute intervals.

Over a 12-month period, the BuildingLink system will continuously monitor hundreds of billions of data points, using very specific algorithms to search for anomalies that represent malfunctioning electrical or mechanical equipment, or inconsistent application of processes and policies (e.g. weekend shutdowns).

It can also detect equipment that is working at cross-purposes. For example, it is not uncommon for building operators to concurrently heat and cool a room, to reduce humidity to a comfortable level for occupants. However, it is also not uncommon for these systems to run simultaneously and go unnoticed for weeks or months, representing a significant waste of energy.

IBM and partner ESI are contributing a library of algorithms to the BuildingLink, many of which have been deployed in thousands of commercial buildings across the United States and have demonstrated significant savings.

IBM and GSA intend to use GSA's 10,000 buildings as a laboratory to develop even more advanced algorithms. IBM will establish a Sustainability Support Center for the GSA where IBM specialists and PBS subject matter experts will collaborate on the next generation of analytics.

Taxonomic Bias

The BuildingLink program will also help the GSA address a problem that organizations battle every day — taxonomic bias. Taxonomic bias is the tendency each of us has to specialize in areas that are relevant to us, and then to continue to build on that specialization.

You may have a building engineer in upstate New York that is an expert in heating systems, and a manager in Texas that runs his cooling system infrastructure better than anyone else. Or you may have a young woman in California who knows York equipment intimately because she worked at Johnson Controls after college. Each of these people has developed an expertise, and will continue to refine it because that's where their interests lie, or because they live in those environments.

The net result is that every organization, the GSA included, has deep but uneven pockets of specialization. The challenge for organizations is: how do you help people follow their interests and refine their specialization? And how do you take these individual silos of expertise and apply them across the enterprise so the organization can benefit?

The BuildingLink program provides an excellent platform to do both. The billions of data points captured every year, along with the analytic tool set included in BuildingLink, provide a workbench for these specialists to follow their interests, perform deeper analysis, test hypotheses, and codify validated observations into repeatable algorithms.

These algorithms can then be applied across the larger enterprise as a nationwide standard, or tailored to the appropriate subset of buildings (heating system algorithms for the northern regions, cooling system analytics across the south, and humidity control algorithms in Florida and Puerto Rico). The net result is that the GSA can use BuildingLink to encourage increased specialization by subject matter experts, and 'package' that knowledge into algorithms so that all eleven GSA regions can benefit.

Smart Buildings 3.0?

Smart Buildings 2.0 technologies (IP-addressable meters, sensors in buildings, digital data, streaming data, real-time analytics, etc.) are helping us take the first significant step in decades to address excessive energy consumption in buildings. However, the reality is that improving the performance of building systems can only drive costs down so far. A perfectly tuned building that is 50 percent occupied still represents an economic 'drag' on the organization.

The next opportunity on the horizon is to enable direct interactions between occupants and buildings, resulting in improved tenant productivity and satisfaction, as well as lower operating costs. Over the next few years, we will see buildings become socially aware as they connect to our social network and use that information to provide personalized service to each of us.

Buildings Will 'Friend' You

Consider a smartphone app issued by your employer that would allow buildings to have access to information, such as GPS location, daily work calendar, and employee profile (e.g. home address). The building could now monitor your professional social graph, and deduce who you are likely to interact with at work. The building could infer this from information already on file electronically at work, such as organization charts, project collaboration suites, email and instant messaging, and conference room reservation systems. For example, a building can differentiate between a local or virtual project team you are working with by comparing your IM buddy lists, email cc's, and home and office addresses for each person you interact with.

Buildings could also have access to relevant external data, such as inclement weather data, traffic patterns, or your GPS location (and that of your colleagues). By taking all of this data in aggregate, buildings will be able analyze your planned daily activities and recommend small changes that can have a dramatic impact on how buildings are utilized.

Buildings Will Tell You to Work from Home

Buildings will be able to make intelligent recommendations based on the internal and external information they aggregate. Imagine the building checking your calendar while you sleep, checking attendee lists for all of your scheduled meetings, and predicting the probability of meeting attendance. For example, the building may find that the majority of your colleagues are traveling in outside the office based on their smartphone GPS signals. Or perhaps, inclement weather is keeping people from driving in to the office.

Upon waking up, you could have an alert from the building recommending that you work from home. You could accept the recommendation, and the building

The next opportunity on the horizon is to enable direct interactions between occupants and buildings, resulting in improved tenant productivity and satisfaction, as well as lower operating costs.

will alert the remaining attendees that you will attend virtually. This simple recommendation, spread across hundreds or thousands of employees, would impact building usage and lower energy consumption, and cities would see less traffic along commuter channels.

Buildings Will 'Check You In' and Tell You Where to Sit
In an internal study, IBM found that utilization of a building in New York City fluctuated during the week. The building was utilized 25 percent less on Mondays and Fridays, because that was when staff traveled in to or out of the city for client visits. Buildings of the future could have the capability to assign desks and offices to optimize usage.

A socially aware building could assign desks by floor or section, filling up a wing before it opens up another. This would ensure that areas of the building are not partially used and yet fully supported (i.e., with heating and lighting turned on). If a team has reserved a large conference room, but attendance is low, the building can reassign them to a smaller team room.

Buildings Will Have an Opinion about You
Today's social media allows us to have an opinion, and to tell the world about it. Yelp and Trip Advisor allow us to comment publicly, Digg and Facebook allow us to 'like' someone or something. Soon, buildings may be able to similarly assess you. Do you reserve large conference rooms for small meetings? Do you drive to the office instead of using mass transit? Do you continuously print in today's paperless world? Buildings can apply metrics against each of these activities and 'rank' your performance.

Buildings Will Play Games with You
Given that buildings could aggregate information about behavior, the logical progression is creating an incentive structure to drive behavioral changes. Adding gamification provides a powerful opportunity to incentivize behavioral change. Buildings will sponsor competitions, for example by recognizing the most frequent user of mass transit each month (resulting in tons of CO_2 saved), or measuring energy consumption of competing departments in the same building.

Conclusion

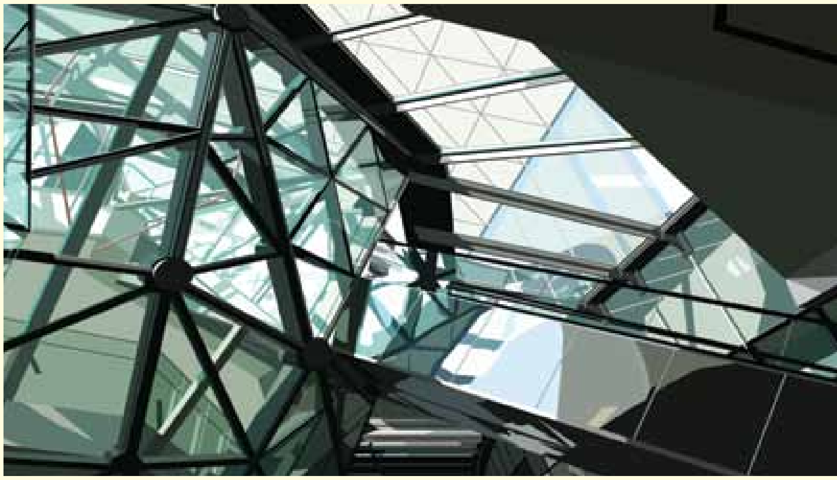
Over the last ten years we have seen commercial technologies migrate to the industrial space. Building systems are maturing from analog to digital. Analytic methods that have been used in the banking and financial sectors are now being applied in the building and industrial sectors.

Similarly, we will see today's social platform expand to include physical infrastructure. We will be able to react and interact with building systems in a manner that will improve the quality of our daily lives, increase productivity, and decrease operating costs across the board for large enterprises.

James Caton *is a Client Solutions Executive at IBM, responsible for architecting Smarter Planet solutions for Federal Civilian Agencies. He previously led IBM's Smarter Buildings consulting practice, coordinating staff from IBM Research, Software Group, and Global Business Services. He was also integral to IBM's acquisition of TRIRIGA, which now forms the backbone of IBM's Smarter Buildings capabilities. You can follow Caton on twitter at @jmcaton or email him directly at james.caton@us.ibm.com.*

CONNECTED AND SMART BUILDINGS: READY FOR PRIME TIME?

By Gordon Feller



Automation systems are becoming ubiquitous in new and remodeled structures, from individual residences to commercial buildings and campuses, and network technologies are driving the transformation of the control systems for these building automation environments. Solutions are now available that allow building owners, managers, and tenants to leverage IP-enabled networks in ways that provide for the convergence of the vast array of building control systems. These solutions have the potential to truly transform real estate as we know it — a massive industry where simple decisions can have huge repercussions both for building owners and tenants, as well as other industries (e.g., energy, construction, etc.).

The recent emergence of converged building systems has both immediate and long-term effects. These benefits are being realized through reduced capital expense during the early stages of design and construction, operational expense savings, and through facility management, building operations, and energy management in later stages.

The broad "Internet of Things" is exploding in size and impact because of the proliferation of sensors in industrial and consumer applications. It is taking rapid hold in the building automation environment and will enable owners to extract vital information from their real estate assets, thereby allowing them to aggregate data, monitor performance, and make much better business decisions based on the "big data" explosion that results from this proliferation of sensors.

This technology increases property value by lowering operations and maintenance (O&M) costs, creating energy savings, and increasing property lease renewal rates. The key to lowering these costs without increasing other costs (such as the O&M costs of the automation systems themselves) is the use of a converged IP network (which is typically cloud-hosted) to manage these systems. The network creates significant value by decreasing building costs by roughly 5 to 15 percent, decreasing the cost to operate facilities by around 20 to 40 percent, creating opportunities for new revenue streams via new tenant amenities and services, improving tenant attraction and retention, and increasing occupant safety.

The cost to implement these changes will vary based on whether a building is new or is being retrofitted. However, our recent studies suggest that the inclusion of the network for the purposes of convergence of building systems controls is cost comparable or slightly less than the traditional building approach.

Optimally, all building systems would require a network and would be based on three principles:

1. *Open:* Non-proprietary building controls that give owners greater flexibility to manage systems and reduce service costs;

2. *Converged:* Common sense elimination of overlapping controls infrastructure such as conduit and cabling;

3. *Normalized:* Various systems have the ability to "talk" to each other, allowing for more flexibility, management control, and resident services.

There are numerous case studies which demonstrate industry innovation and best practice. Tridel Corporation, Duke Energy Center, and Envision Charlotte have all completed analyses of energy savings methods for high-density residential and commercial buildings.

- **Tridel Corporation** conducted an in-depth study of one high-density residential building which focused on savings derived from one common infrastructure for all systems.
- **Duke Energy Center** performed an analysis of one commercial office tower with 17 building system controls sets converged on one IP network.
- **Envision Charlotte** conducted a study of a model for energy visualization based on 70 commercial office buildings in an urban core.

Smart building technologies are a stepping stone to smart communities and smart cities. No single company or city is truly equipped today to provide a comprehensive smart city solution. But just as the integration of individual building control systems into a comprehensive building management system improves the costs and efficiencies of smart buildings, the integration of individual buildings into smart communities and cities will become the next ideal for designing, planning, executing, and managing the city of the future. The converged networks of today's smart buildings will form the integration platform for the smart community. Just as the large enterprises of today are turning to converged networks and cloud-managed IT infrastructures to support their operations over multiple locations, smart communities and cities are likely to adopt cloud-based management of building infrastructures for manageability, redundancy, and efficiency.

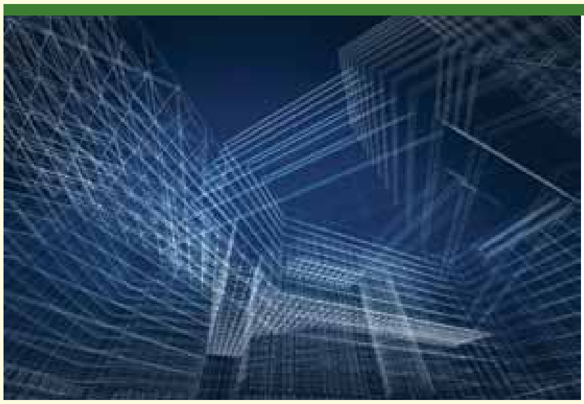
Winning strategies will be the ones that enable citizens, business leaders, and policy makers to drive job growth, increase economic opportunity, and provide improved citizen services. The goal is simple: enabling more effective partnerships by linking governments with private enterprises and citizen organizations and focusing on creating communities that are economically competitive, socially cohesive, and environmentally clean. With respect to building automation, converged networks and cloud-based services will be key to enabling these partnerships.

Savvy government leaders are recognizing the untapped power of the network and incorporating its potential into the early stages of planning and development. But how can these solutions be incorporated in a consistent, scalable, and replicable manner? Experimentation through small-scale "proof of concept" projects. Since budgets are so limited, city leaders know that it's impossible to adopt a purely centralized approach, which means trying new approaches and letting non-government organizations take the lead, wherever and whenever possible.

City leaders are also discovering that the broadband network has become the fourth utility. Governments regulate the three traditional utilities — water, gas, and electricity — with a clear and consistent framework. Regulations are clearly needed to standardize the uses of information and communication technologies in the development of new urban communities and in the provision of services to the public. Since governments cannot do it alone, a framework is needed for public-private partnerships. These can provide the successful conditions for new business models, which incentivizes the private sector to take a more active role in upgrading city services and infrastructure.

The possibility of government regulations on utilities and the potential for "smart regulations" prompt some questions:

- What are the design principles for smart regulations that can accelerate the development of smarter and better connected communities?
- What are the desired outcomes of smart regulations?
- What is the government's role in creating smart regulations, especially where there's an alternative to command-and-control?
- What is the role of industry in defining and shaping smart regulations, including the voluntary self-regulations?
- Which city development activities could best be guided and governed by smart regulations?



Just as the operating costs for conventional computing tasks take advantage of the economies of scale and management for services hosted in the Cloud, smart buildings and communities will see those same advantages.

- What are the emerging standards for the information and communication technologies integrated into smart city development?

Although the management of an individual building can be accomplished locally or hosted in the Cloud, as smart buildings merge into smart communities, cloud-based management becomes essential. Most importantly, it helps organizations address the unpredictable application demand on the data center.

But for many executives in government and enterprise, it's equally significant to say that cloud fuels top-line growth. Cloud-based management helps achieve top-line growth because it improves business agility, reach, and scalability; enables new services innovation; differentiates with new technologies; and enhances business resiliency by improving data center and application uptime.

These results apply to the management of smart building infrastructure as well. Moving operations and systems into the Cloud also has the effect of improving bottom-line economics for those buildings and communities. Just as the operating costs for conventional computing tasks take advantage of the economies of scale and management for services hosted in the Cloud, smart buildings and communities will see those same advantages.

There are several reasons why operating in the Cloud improves costs, the key one being that you pay only for what you consume when you need it. Improving employee productivity is another benefit, since it provides a consistent experience and access to state-of the-art cloud applications. The single factor which seems to outweigh many others is that today, the Cloud is delivering key benefits to classic IT applications: reducing total cost of ownership (TCO) by 50 percent, utilizing resources more efficiently, and reducing TCO of collaboration applications by 15 to 23 percent.[1] Similar benefits would be expected with respect to smart building management.

Cloud computing has many benefits, but the key advantage may be its ability to address unpredictable application demand on the data center. Cloud technology is especially well-suited to the following four scenarios:

- Managing applications with sharp, unpredictable usage spikes;
- Handling frequent, repeatable IT interactions;
- Controlling IT assets centrally rather than by department or application; and
- Increasing business agility to address new products, customers, and selling situations.

Top-line growth generated by utilizing cloud computing comes from a host of enhancements. First, it improves business agility, reach, and scalability, including faster provisioning (from 90 days to minutes).[2] Secondly, we're seeing new services innovation, which helps transform IT from a cost center to a business enabler, and allows many organizations to level the competitive playing field (e.g., Amazon, Netflix, Intuit, Apple). Thirdly, there's the competitive differentiation, which is made possible through the adoption of new technologies: mobility, video, sensors, business intelligence, and social computing. Finally, cloud computing provides improved business resiliency through better data center and application uptime.

The bottom-line impact is driven by at least three factors:

- The ability to pay only for what you consume, when you need it, which increases transparency and supports more direct revenue-to-cost operating models.
- Improved employee productivity that results from a consistent user experience and access to state-of-the-art applications (e.g., knowledge workers save up to four hours per week through use of SaaS collaboration applications).[3]
- IT-specific benefits, including TCO reductions of greater than 50 percent; more efficient resource utilization; and a reduction in IT TCO for collaboration applications.

There are several reasons for cloud computing's burgeoning adoption across both enterprises and small and medium-sized businesses (SMBs). By fostering business agility and delivering compelling economics, "the world of many clouds" provides certainty in uncertain times. Cloud computing enables enterprises to conserve cash by encouraging a transition from capital expenditure to operating expenditure (CapEx to OpEx). In addition, because a volatile economy places a premium on agility, the demand is growing for new IT consumption models such as cloud computing.

The Cloud enables new business and technology capabilities that are attractive to the emerging digital workforce and fit today's changing workplace. This new workforce requires a consistent experience across multiple environments: mobile, social, visual, and virtual. According to Cisco IBSG's published research, 70 percent of mobile users expect to consume cloud-delivered services in the next one to two years.[4]

Unhindered by legacy infrastructure, SMBs are using the public cloud to level the playing field against larger competitors. According to a recent Cisco IBSG survey, half of SMBs will spend more than one-third of their IT budgets on cloud services by 2013.[5]

Aiding cloud's adoption is the understanding that it's a proven model with multiple options (public, private, hybrid, community) and a choice of providers.

Just as today's enterprise applications residing in the Cloud have to deal with the security implications of the modern Internet, building management solutions have to consider these same implications, including data safety, data confidentiality, XML signature, browser security, and regulatory compliance. However, as policy makers and leaders recognize converged IP networks and cloud-managed IT infrastructures as the foundation for smart cities, we will begin to see the growth of smart buildings and smart communities. Q

Gordon Feller *is the Director of Urban Innovation at Cisco's Internet Business Solutions Group. Prior to Cisco, he was CEO of Urban Age Institute, an international research organization which began as a multilingual World Bank magazine. For nearly 30 years, Feller has advised on urban development issues with leaders of multinational companies, cities, NGOs/foundations, and national governments. Feller is the Convenor of "Meeting of the Minds," an annual leadership summit. He received his Bachelor's in political science, cum laude, and a Master's in international affairs, both from Columbia University, where he served as a Lehman Fellow, a Wallach Fellow, and a Dean's Fellow.*

REFERENCES

[1] Cisco Systems, Inc. "Cisco Cloud Computing - Data Center Strategy, Architecture, and Solutions: Point of View White Paper for U.S. Public Sector." San Jose, CA: 2009. http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf.

[2] Barbier, Joel, Joseph Bradley, et al. "Riding the Cloud to Improve Your Top- and Bottom-Line Economics." San Jose, CA: 2012. http://www.cisco.com/web/about/ac79/docs/Cloud-Computing-Economics_IBSG.pdf.

[3] Williams, Bill. *The Economics of Cloud Computing: An Overview for Decision Makers.* 1st ed. Cisco Press, 2012. Print.

[4] Taylor, Stuart, Andy Young, et al. "What Do Consumers Want from Wi-Fi?: Insights from Cisco IBSG Consumer Research." San Jose, CA: 2012. http://www.cisco.com/web/about/ac79/docs/sp/SP_Wi-Fi_Consumers.pdf.

[5] Taylor, Stuart, Tine Christensen, et al. "New Cisco IBSG Research Reveals Dramatic Growth in Cloud Interest Among SMBs." San Jose, CA: 2011. http://www.cisco.com/web/about/ac79/docs/sp/SMB-Cloud-Watch-POV_IBSG.pdf.

WHAT'S COMING IN SMART BUILDINGS: RESIDENTIAL AND LIGHT COMMERCIAL

By Jeremy Warren

To watch the market in residential home automation solutions over the past few years is to see a case study in Clayton Christensen's theory of disruptive innovation unfolding before one's eyes. Existing providers have focused almost exclusively on high-performance, high-cost custom solutions targeting the most profitable customers, and all but ignoring the majority of households.

New products and services, however, have enabled a new set of players to bring simpler, standardized, cost-effective solutions to the mass market by emphasizing core value propositions rather than exotic feature lists, and they are seeing spectacular business growth with penetration orders of magnitude greater than before. The new wave will continue to grow and move upmarket to offer more feature-rich solutions to residential and light commercial customers at a fraction of the cost of the legacy providers. This will ultimately disrupt their market and allow homes, small businesses, sandwich shops, dry cleaners, and doctors' offices to become smart buildings.

From Home Security to Home Automation

Companies such as AMX, Crestron, and Control4 have been offering custom home automation solutions for years. These can be used to intricately control almost every device in your home with an RS-232 serial port or Ethernet interface. At the touch of a single button, for example, you can select a movie to play and have the TV and DVD adjust settings in harmony, dim your lights, and knock the thermostat up a cozy couple of degrees. Average installs, however, can cost up to hundreds of thousands of dollars up front for custom design, installation, and low-volume equipment. Not surprisingly, these systems are only found in a small fraction of homes across the country. Lighting and HVAC control solutions from companies like Lutron are slightly more common in the commercial arena because of the relative price insensitivity and potential savings, but still far from ubiquitous.

Change has come initially from a seemingly unlikely source — the home security industry. But with their established business model of subsidizing up-front costs and amortizing them over the life of a three to five year contract, companies such as ADT and Vivint (formerly APX Alarm) were actually in prime position to bring simple home automation solutions to the mass market affordably. A security system that also provides the ability to control a few lights, thermostats, and door locks from a smartphone app may cost as little as a few hundred dollars up front and $50-75 per month, putting it within reach of most households. In addition, the combination of television advertising, door-to-door sales, and a turnkey full-service approach made it easier to sell an otherwise complicated and difficult-to-explain solution to the non-technical public. As a result, the security industry now dwarfs the traditional players with hundreds of thousands of home automation installs per year, attracting the attention of major players in the telecom space with tens of millions of existing customers among them. Comcast, Time Warner, AT&T, and Verizon are all now offering or market-testing security and home automation offerings. Expect ubiquity, and soon.

Innovative Technology

The technology behind these new market entrants is nothing revolutionary — like most disruptive innovation, it's largely a matter of combining existing technologies in interesting and attractive new forms. For this new wave of home automation the theme is wireless: wireless sensors, wireless devices, wireless uplinks, and wireless phones. While until recently only hard-wired security sensors (e.g., door and window sensors, passive infrared motion detectors, glass-break sensors, smoke and carbon monoxide detectors) were used, today wireless sensors enable systems to be installed in hours rather than days. Low-power wireless mesh network technologies such as Z-Wave and ZigBee and their associated home automation protocol standards have been around for years, but relatively few people were willing to assemble, program, and maintain their own systems from individual retail products. Including the same dimmers, switches, thermostats, door locks, and other devices in a turnkey solution opened up much larger opportunities. Traditionally, security systems used "POTS" (plain old telephone system) lines to signal security events to monitoring stations, allowing for limited information flow and almost no interactivity. But using cellular radios with low machine-to-machine (M2M) rate plans and IP communication enabled cloud-based services such as Alarm.com to broker alarm signaling and, more significantly, offer interactive services, web-based rule configuration, and more to anyone, anywhere. Finally, the explosion of smartphones and the app model put all of this information and control at the consumer's fingertips.

2GIG Technologies was the first company to offer an integrated security and home automation solution with a wireless receiver for security sensors, a Z-Wave radio for home automation, and a cellular radio for Internet connectivity in a color LCD touchscreen wall-mounted panel (contrasted with the then-industry-standard 12-button keypad). 2GIG's Go!Control product first came to market in 2010, and along with partner Alarm.com the company has provided its home automation solution to hundreds of thousands of homes and small businesses through security dealers across North America. Other companies have since followed suit with roughly comparable products, and this feature set is now the new standard in a market segment that continues to grow.

What Comes Next?

As with most disruptive innovations, after establishing a foothold with the simpler use cases, the progression is outward and upward — wider penetration, greater performance, and upmarket opportunities. So for these new home automation solutions, expect broader functionality to appeal to even more homeowners and to make similar mass progress in the light commercial space with small offices, retail stores, and restaurants. Simple home automation evolves into smart homes and buildings.

One of the key areas of innovation will be video. There are already solutions on the market that provide video surveillance, motion detection, remote viewing, video recording and playback, infrared lighting for night vision, and more. But these solutions are generally standalone, expensive, and dumb. As high-performance video equipment gets smaller and cheaper, it is now within reach to create a standardized, mass-market solution that incorporates all of the above features and integrates smartly and seamlessly with other devices in the home and capabilities outside the home. Simple, well-designed DVR functionality — at cash registers, in restricted areas, and outdoors — will provide use cases for mass success in light commercial installations.

Other devices in the home and office will join the smart system as well. Controllable refrigerators, dishwashers, laundry machines, and dryers are already available on the market. For home appliances in particular, the driver of "smart" adoption will be energy management, and today's home automation players are well-positioned to make it happen. Each year utilities are under more financial and regulatory

The technology behind these new market entrants is nothing revolutionary — like most disruptive innovation, it's largely a matter of combining existing technologies in interesting and attractive new forms.

pressure to keep peak power usage under production capacity, as increasing capacity is both capital-intensive and highly regulated. Moreover, while rolling blackouts may be better for the bottom line than purchasing astronomically expensive excess power on the open market, people tend to frown upon that strategy. As a result, time-of-day pricing plans and "peak demand response" programs, whereby consumers are paid a stipend for allowing the utility to temporarily shut off their HVAC system during extremely hot summer days, are quickly becoming the norm. Perhaps the single most power-hungry device in your home isn't your hot water heater or your air conditioner, but your refrigerator in its defrost cycle. In this new world, scheduling your large appliances to perform particularly intensive operations outside peak times can provide significant financial benefit. Moreover, companies that can offer to the utilities a pool of hundreds of thousands of consumers willing to raise their thermostat set point by 3 degrees every once in a while in exchange for a little cash will have a lucrative business model on their hands.

Beyond major appliances, energy management and cost savings will also drive greater integration of lighting controls into smart buildings. As noted earlier, lighting control is already somewhat common in the light commercial space, largely because lighting is generally the largest source of energy usage in commercial buildings (as opposed to HVAC systems in the residential space). But the relative high cost and inconvenience of standalone systems limits their penetration. Once again, integration and standardization will drive adoption. A system that automatically shuts off lights, changes thermostat settings, and locks doors when an alarm system is armed or notifies the manager when it isn't armed by 11 p.m. will impact the bottom line of most businesses. For residences, the target technology is LED bulbs with integrated wireless control interfaces — as it turns out, attaching a Z-Wave, ZigBee, or other mesh network radio to an LED ballast only adds a few dollars to a $40 device. As LED lighting becomes widely cost-effective, ubiquitous residential lighting control will follow.

Other innovations will play important roles in the spread and maturation of smart homes and businesses as well. Home healthcare and wellness are often mentioned as large and promising, albeit difficult, domains to conquer. Applications such as remote monitoring of elderly family members are available and affordable today with standard home control and video solutions, and by utilizing security sensors to notify loved ones of inactivity. But whether it's healthcare or entertainment or access control or energy management or some other frontier that powers the continued and accelerated adoption of smart building technologies, a few things are certain: the solutions will be simple and standardized rather than complex and custom; they will be mass-market and turnkey rather than niche and do-it-yourself; and most importantly, they will be integrated, coordinated, and smart rather than independent, standalone, and dumb.

What Do These Developments Mean for the Intelligence Community?

From a defensive perspective, these developments may provide some particular benefit to the Intelligence Community. While new smart home or smart building capabilities would probably be of little or no value (for example, energy savings are always nice, but government institutions would overwhelmingly need large enterprise solutions), the advances in residential and light commercial security systems offer new potential. Where there is a need for a basic security solution for a relatively small physical footprint, today's systems offer a solution that's less expensive and much faster to install. Allowing one person without any special skills to install a system quietly in two hours is certainly less conspicuous than requiring multiple people to pull wires through walls over multiple days. Moreover, as these systems become increasingly common around the world, a security system with day/night cameras and motion sensors will be less unusual.

But by far the most interesting ramifications of the coming ubiquity of smart buildings relate to the offensive potential. These systems offer information in tantalizing abundance — 2GIG and our partners are already using sensor activity to infer patterns of presence and absence to automatically set energy-saving thermostat schedules. Data from doors, motion sensors, lights, and other devices can create a general awareness of patterns of life. Moreover, the ease-of-use of today's systems means that sensors are labeled with useful names ("back door" rather than "zone 8"), and we find it significantly more common for users to create separate codes for individual residents, neighbors, employees, contractors, and other trusted visitors than with traditional systems. Regardless of whether this is done in order to enable more useful notifications ("Jennifer unlocked the front door") or for fine-grained access control (e.g., only allowing the delivery man to unlock the back door between 10 a.m. and noon), the greater detail in information captured enables more specific insight into activity.

Now note how today and tomorrow's smart building solutions are almost universally available remotely from smartphones. As convenience is such an important driving factor in the spread of these technologies, users are willing to let their fundamental security and privacy be tied to that of their mobile devices. Thus, in the hands of a determined and capable adversary, the smart building smart app can become a powerful tool of surveillance, control, and disruption. Q

Jeremy Warren *is the Chief Technology Officer of 2GIG Technologies, a manufacturer of innovative residential security and home management systems, whose Go!Control™ product is used in hundreds of thousands of homes across North America. Warren is responsible for overseeing the design, development, and manufacturing of 2GIG's products, as well as for providing technology vision and strategy. He was the Chief Technology Officer of the U.S. Department of Justice from 2007-2011, and studied Computer Science Engineering at the Massachusetts Institute of Technology.*

POPULATION AGING AND THE EVOLUTION OF HIGH-PERFORMANCE ENVIRONMENTS: IMPLICATIONS FOR A NEW SOCIAL INTELLIGENCE

By Joseph F. Coughlin, Bruce Mehler, and Bryan Reimer

Global aging presents new opportunities for technology to enable people to live longer, better lives. Public and personal demands for innovative ways to cost-effectively manage health and optimize well-being are now a focus for many technology developers, businesses, and governments. Based on the developments of the MIT AgeLab AwareCar, we present the concept of 'high-performance environments' that use ambient intelligent systems and biometrics to detect individual states of well-being and improve operator performance.

We suggest that the concept of high-performance environments will evolve to include settings far beyond the vehicle, offering the potential to collect data that could provide a new social intelligence to assess patterns of population stress and well-being in the home, workplace, public areas, communities, and geographic regions.

The single most defining demographic factor shaping the future of all developed economies and many emerging nations is demographic transition — the shift from societies that are comprised of primarily young populations to those in which the fastest growing proportion of the population is 60 years old and older. A combination of great strides in longevity and reduced fertility rates are transforming nearly all industrialized economies into graying nations with too few younger people to comfortably provide the economic resources necessary to meet the demands of social welfare policies, to ensure a robust and productive workforce, or to provide care.

Today, Europe's 65+ demographic is approximately 18 percent of the population, but by midcentury older adults will make up nearly 30 percent of the population. Approximately 40 percent of Japan's population will be over 65 years old by 2050. Even China's over-65 population will number more than 400 million — nearly the entire projected population of the United States in 2050.

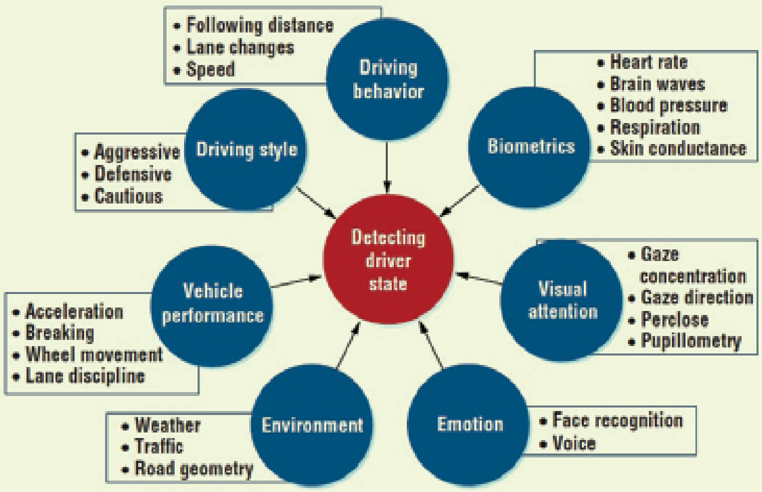


Figure 1 | MIT AgeLab's AwareCar

An aging society will obviously place new demands on national economies. However, given the growth of the oldest demographic (those 85+), there will also be significant costs associated with providing care for health conditions and supporting well-being. Among the challenges, chronic disease management will be crucial to control healthcare costs. In the United States alone more than 110 million Americans have at least one chronic condition, such as diabetes, that will drive costs and reduce quality of life in old age. A renewed focus on personal safety will also be needed. In short, there is an urgent and unprecedented need for creative strategies to support an aging society.

'Smart' Aging and Ambient Intelligence

Information communications technologies leveraging automated decision support offer a wide number of applications to monitor safety, manage conditions, and motivate healthy behaviors. Advances in ubiquitous computing research in ambient intelligent systems are providing new ways to support healthy aging. Ambient intelligent systems are human-centered technologies that can detect the context of behavior, personalize a response based on previous behaviors, and in some cases anticipate need. Perhaps most important to an older user, ambient systems are often invisible or embedded into everyday things and environments.

Technology to support the elderly is developing rapidly. Many people are familiar with the "Help, I've fallen and I can't get up" systems. Often referred to as personal emergency response systems or social alarms, these devices and next-gen services detect and respond to an accident. Intel, General Electric, Philips, and other consumer electronics leaders are vastly improving and expanding on the basic functions of these systems to provide comprehensive monitoring services and answer questions from "Did Mom take her medications?" to "Who is knocking on her door?" Related safety systems are also combining home monitoring with location-based services to detect an Alzheimer's patient who may have wandered.

New systems are taking a prognostic engineering approach to care and aging independently. The homes of older adults will become sensor-rich environments that will detect adverse events as well as changes in behavior that may predict future problems. Sensors under a rug, for example, may detect a change in gait that might foreshadow a fall. Everyday appliances from a stove to an electric toothbrush will indicate changes in sleep patterns, eating habits, and self-care behaviors that are illustrative of behavioral trends.

Development of the MIT AwareCar and the Evolution of High-Performance Environments

Aging well requires the capacity to motivate a wide range of regular healthy behaviors and deliver targeted interventions that will result in optimal performance. Optimal performance can be defined as the highest regular performance an individual can produce given their physical, mental, and associated capacities within the changing demands of their environment. This might include routine movement and daily exercise, food preparation and eating, house cleaning and maintenance, and regular communications. Emerging intelligent applications will not only detect events or selected behaviors but will facilitate personalized interventions to support optimal performance within the environment. High-performance environments, therefore, are settings that can detect individual behaviors, identify "normal" performance, sense changes in the environment or individual state, and apply embedded intelligence to deliver personalized services and interventions to support well-being.

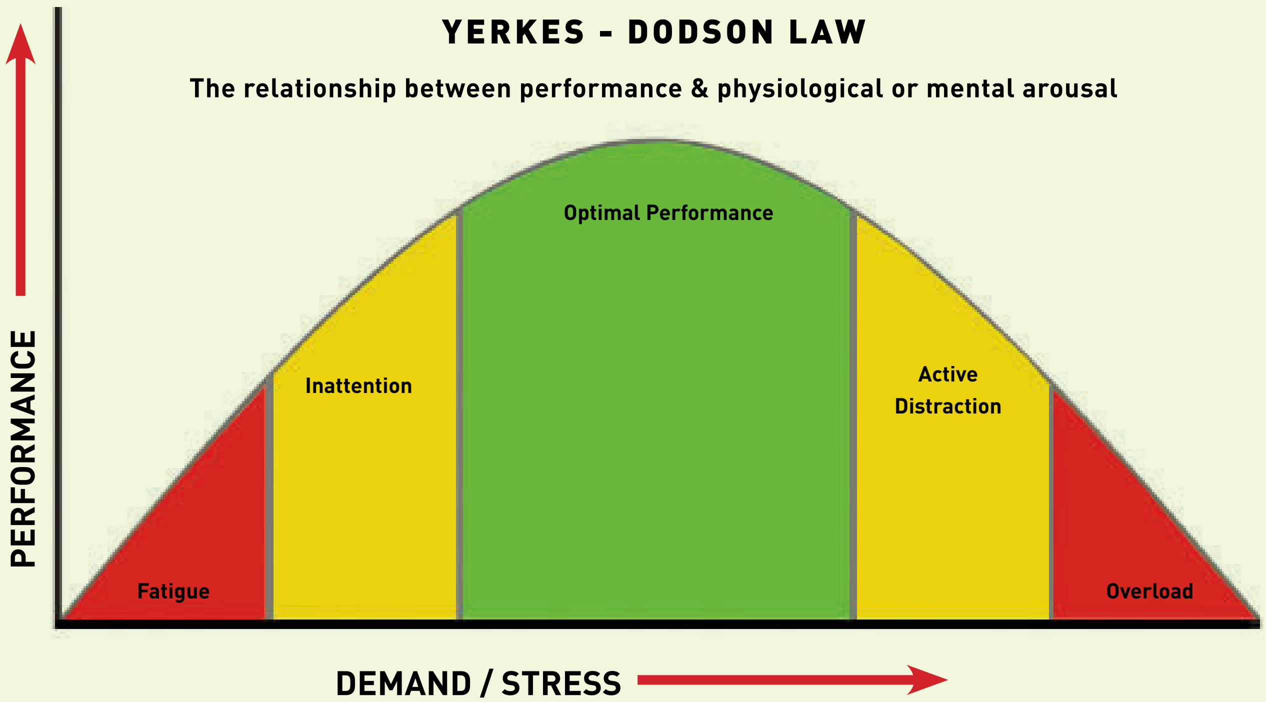


Figure 2 | Yerkes–Dodson Law

Driving is synonymous with freedom and independence in the United States. While many continue to debate how old is too old to drive, the more appropriate question may be what role driver health plays in safe driving. Given the importance of automobility, the MIT AgeLab sought to develop an in-vehicle system that would transform the car into a high-performance environment. The MIT AgeLab's AwareCar (see Figure 1) detects driver state and performance to indicate driver stress behind the wheel and serves as a platform for possible real-time interventions to achieve optimal driver performance. Driver stress can be caused by distraction, such as cell phone use, traffic congestion, behavior of other drivers, or events and thoughts outside the driving context. The Yerkes-Dodson Law (see Figure 2) suggests that while a certain amount of demand or stress is necessary for optimal performance, too much can erode performance. Consequently, optimal driving safety is most likely when the driver is stimulated just enough to be aware but not so overloaded that his or her performance declines. The AwareCar (see Figure 3) integrates ambient intelligence and biometrics, including heart rate, eye movement, and skin conductance to detect driver stress or arousal behind the wheel. An array of cameras and sensors detects changes in road conditions. These biometric, video, and vehicle data provide a more holistic view of the operating context to reveal driver state or performance in a given condition. Finally, the AwareCar provides a platform for targeted interventions to refresh the driver. For example, if the driver is stressed, certain aromas (e.g., lavender), lighting, or seat massage might relax the driver just enough to perform in his or her optimal zone. If the driver is fatigued, ambient lighting, sound, or temperature might be adjusted to enhance the driver's arousal to achieve optimal performance.

Application of High-Performance Environments

The AwareCar is indicative of a technology trend touching nearly all aspects of the built environment, including homes, cars, workplaces, and retail settings. In the near-term, the health needs and the associated costs of an aging population will be the primary driver for moving many of these systems from the laboratory to the living room.

Figure 3 | Driving subject in the MIT AwareCar

Aging is not about care and health alone. Global aging will introduce a profound transition from a predominantly young workforce to a multigenerational workforce in nearly all industrialized countries. Employers will seek systems that support well-being and high performance under a variety of conditions at any age in every type of workplace.

New Source of Collective Social Intelligence

Recent developments in technology and related public behaviors have contributed to an explosive growth in data that is the basis of a collective social intelligence. Clicks, tweets, and texts reveal the shape and contours of human behaviors at local and national levels. The social media Twitterverse is useful to share information but can also serve as an indicator of public sentiment faster and with greater accuracy than traditional surveys or newspaper content analyses. Mobile phone use and GPS provide high-resolution data that can indicate trends such as travel patterns and social interactions.

The growth of high-performance environments to support an aging society will add to this collective social intelligence. Data collected at the individual level will be aggregated and stored in the Cloud but is likely to be managed by telecommunications providers, utilities, health and disease management companies, insurance and financial services firms, transportation departments, and large retailers. Since the technology and related services will be ubiquitous, they will provide unique, comprehensive, and real-time "big data" on nearly every dimension of living. Imagine every environment as a data source transforming how we visualize everyday activities:

- Traffic reports predicting rather than just reporting congestion or even the likelihood of an accident based on data from millions of mobile sensors showing real-time driver stress;
- Public health intervention effectiveness revealed by actual behaviors reported by ambient systems rather than by surveys or physician reports; or,
- Public well-being indicated by real-time changes in population sleep patterns, eating habits, social interactions, etc.

Opportunities and Challenges

While the benefits of high-performance environments are many for an aging population and the possible conveniences they could provide for everyone are many, they present several technical and policy challenges.

Algorithm development. Ambient systems are rapidly developing; however, the type and volume of data is nearly limitless. Realizing the capacity to detect and deliver personalized interventions will require dramatic advances in learning algorithms.

Meaning. Many behaviors can be detected (e.g., watching TV), but which of these behaviors are accurate predictors of healthy outcomes? What does change in one behavior mean for that individual and what might it mean when aggregated across an entire region?

Secure storage and access. Data storage and seamless access will be vital. If high-performance environments become critical to individual and group well-being, redundancy, security, and resilience are crucial.

The associated policy and social issues are expansive and could present significant barriers to advances in the adoption of high-performance environments.

Privacy. Public concern for how much of their personal life is in the Cloud and accessible by whom is a major barrier to user acceptance. However, other services that potentially contain personal information (e.g., credit cards) have overcome privacy fears by instituting extraordinary security and by offering benefits so compelling that privacy becomes a secondary consumer value. For example, an older adult may decide that the threat to privacy from a high-performance environment is greatly outweighed by the capacity to live independently in his or her own home.

Affordability. "New" almost always translates to "more" — new technology costs more. While the technology will become more available over time, it will be important to ensure that the systems and services are available to lower income elderly to ensure the equitable distribution of technology innovation.

Access. How will data be stored and shared between various providers? For example, telecommunications firms or utilities may be the conduit of data from home to service provider but how will those relationships be governed and data managed and controlled by the consumer?

The creative application of technology presents new opportunities for an aging society to live longer, better lives. The integration of technology into everyday environments provides a platform for more than better care; it offers the potential to support optimal performance in daily living, work, and social interaction. While significant technical and social challenges remain, the data produced by evolving high-performance environments will contribute to a growing collective social intelligence that will provide high-resolution insight into the health and well-being of populations.

Joseph F. Coughlin *is Director of the Massachusetts Institute of Technology AgeLab. He teaches in MIT's Engineering Systems Division. Prior to joining MIT he was with EG&G, where he led a technical and analytical services group supporting several federal agencies and the White House Office of Science & Technology Policy. Coughlin writes for* Huffington Post Science *and produces the publication* Disruptive Demographics *on BigThink.com.*

Bruce Mehler *is a Research Scientist in the Massachusetts Institute of Technology AgeLab. He has an extensive background in the development and application of non-invasive physiological monitoring technologies and research interests in workload assessment, individual differences in response to cognitive demand and stress, and in how individuals adapt to new technologies.*

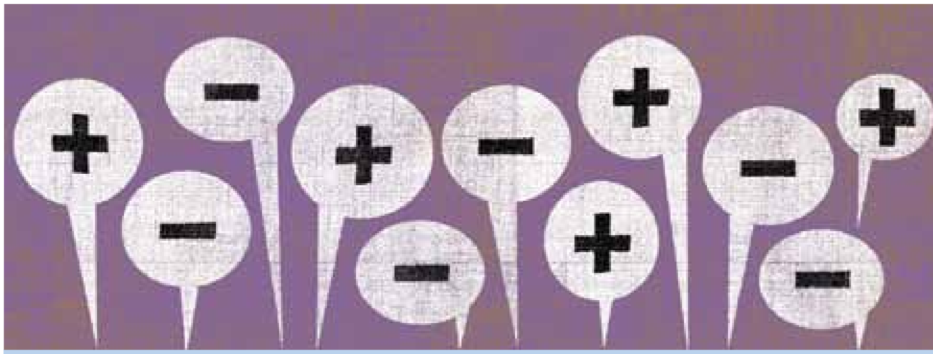
Bryan Reimer *is a Research Engineer in the Massachusetts Institute of Technology AgeLab. His research seeks to develop new models and methodologies to measure and understand human behavior in dynamic environments utilizing physiological signals, visual behavior monitoring, and overall performance measures.*

REFERENCES

Coughlin, J.F., Reimer, B. & Mehler, B. (2011). Monitoring, Managing and Motivating Driver Safety and Well-Being IEEE Pervasive Computing, 10(3), pp. 14-21.

Lee, C., Orszulak, J., Asai, D., Myrick, R., Coughlin, J. F. & de Weck, O. L. (2011). Integration of medication monitoring and communication technologies in designing a usability-enhanced home solution for older adults, IEEE International Conference on ICT Convergence.

Elements of the research presented in this article were funded by grants from the U.S. Department of Transportation, Healthways, and the Santos Foundation.



TECH CORNER

To supplement the ***IQT Quarterly***'s focus on technology trends, *Tech Corner* provides a practitioner's point of view of a current challenge in the field and insight into an effective response.

Securing the Mobile Workforce

Ensuring Secure and Reliable Access to Mission Critical Information in the Field

A technology overview from IQT portfolio company Connectify

Today, government and military teams encounter a variety of networks in the field, from slow satellite phone data connections to "smart buildings" that offer high-speed network access instantly. The smart, wired buildings of today and the future are raising the bar on what workers expect from their Internet connections. Workers expect high bandwidth connections that always work, and they need their traffic secured.

But workers aren't spending all of their time in these smart buildings. They're spending more and more time on the road with multiple devices and multiple network connections: corporate Wi-Fi, insecure hotel Wi-Fi networks, and 3G and 4G networks, just to name a few. While more network connections can mean increased vulnerability of information systems, next-generation Virtual Private Network (VPN) technology gives mobile workforces the ability to leverage multiple Internet connections for more secure and persistent access to mission-critical information than ever before.

Challenges Faced by Teams Requiring Mobile Access to Sensitive Data

Not only does wireless accessibility offer tremendous value to mobile workforces, helping to streamline processes and improve productivity, but today's government and military teams have come to rely on wireless technology to access mission-critical information in times of peril. Prompt and secure access to confidential information is more vital than ever before, and can be a lifeline during high-threat situations.

To be successful, the mobile workforce expects three factors from their network connections: speed, reliability, and security.

VPNs have long been the preferred solution for government agencies that must extend their private network resources across public networks like the Internet. However, an increasing number of hurdles mire the effective use of today's VPN technology by workforces in the field.

There are two major families of VPN software today.

Internet Protocol Security, or IPSec, was the first generation VPN security protocol approved for government and military sectors from the early-1990s onwards. IPSec operates on the network layer, with security mechanisms intertwined with the IP address of the connecting host. An unfortunate byproduct of this IP-reliant architecture is a disrupted user experience anytime the VPN is run across a fragmented network environment with different networks hosted by disparate providers.

Due partially to these various shortcomings, a second generation of VPN security protocol using SSL (Secure

Sockets Layer) was introduced in the late-'90s, and which has since been replaced by **TLS (Transport Layer Security)**. The TLS protocol has been designed, at the highest level, to be usable across a broad array of network technologies, and the advantages of utilizing TLS as the underlying security protocol for the next-generation military-grade VPN are numerous.

Still, all of today's VPNs work by creating a single encrypted connection back to the VPN server, and then forcing other applications to run over this socket, creating the illusion that the user is back in the office, while making sure that all the traffic is secure from prying eyes.

VPNs are a critical tool for allowing the workforce to get work done in a secure manner while outside of the office. Unfortunately, these traditional VPN solutions, while excellent for security, actually exacerbate the other two problems of reliability and speed.

Reliability is hurt because any time the user switches from one network to another, the VPN socket is broken. For mobile workers this happens multiple times per day as they move from one hotspot to another, or leave a hotspot and switch to 4G, until they arrive at their destination, and switch back to Wi-Fi automatically. Each time, the user is disconnected from the VPN, and must "redial" the VPN connection to reconnect on the new network. This is more than just inconvenient; applications are disrupted, downloads must start over. Ironically, more and more often, network firewall settings are blocking VPN connections, leading to conflicts between the service provider's security software (which wants to watch everything on the network), and the employer's security software (which wants to hide everything the worker is doing from the service provider).

Speed is hurt because the user's traffic is pushed through a single socket, over a single Internet connection; there is no ability to do anything in parallel. For example, a remote worker who has two cell phones that he or she can tether is out of luck: the VPN will pick one of the two, and put all the traffic over it.

Although security breaches can generate cataclysmic aftershocks in public safety, being "stranded" without access to sensitive data can mean the difference between life and death to teams in the field. Today's VPN technology is only as reliable as the single network used to access it. When mobile workforces are faced with a low-bandwidth connection, their lifeline to critical data can be slowed to a crawl at a time when each second counts, or worse, completely severed, rendering the mission doomed.

While operations in urban areas may benefit from a high density of available Internet connections, including but not limited to instant high-speed access in "smart buildings," many of today's military-grade VPN solutions offer no support for network roaming, resulting in terminated sessions each time the computer moves from one network to the next.

Between issues of security and reliability with today's VPN technology, government and military teams are faced with an excessive level of uncertainty in the field, while the architecture of military-grade VPNs have historically been slow to account for the constant seismic shifts in wireless technology.

Secure and Reliable Access with Next-Generation VPNs

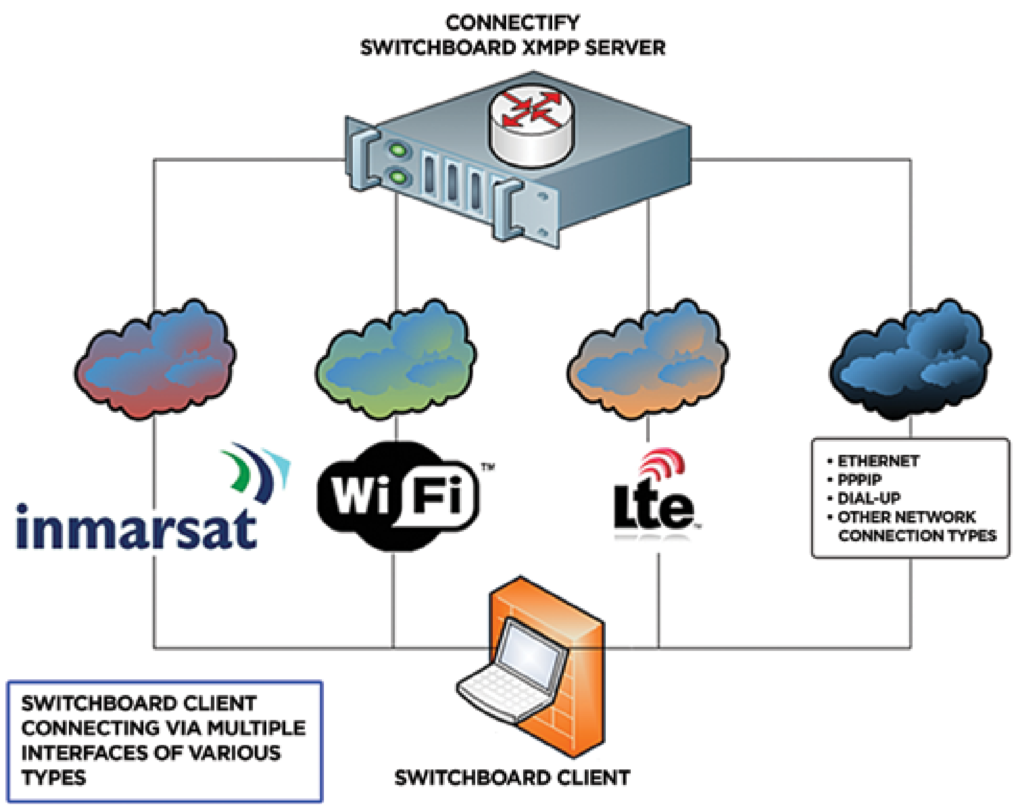
Responsive to the ever-increasing requirements of government and military teams in the field, and utilizing cutting-edge security protocol and software technology, Connectify turned the concept of VPN on its head, creating a secured virtual network. Instead of reducing mobility and throughput, the Connectify secured virtual network enhances both.

Connectify Switchboard is a software-based VPN that establishes an authenticated, encrypted tunnel, while utilizing innovative connection aggregation technology to offer simultaneous use of every available Internet connection for combined bandwidth.

In Connectify Switchboard, user authentication is separated from the individual socket that is used to move packets. Once a user is authenticated, Switchboard will create multiple sockets back to the VPN server, potentially using more than one Internet connection, and even different protocols to get through different firewalls at the same time. Switchboard decides which connection to use, on a packet-by-packet basis. This means that any application can benefit from this acceleration, without any changes.

These multiple connections make Switchboard fast: a user can plug in a 4G card, use a satellite phone, and join a Wi-Fi network, and get very close to the speed of all of them combined.

While Switchboard's connection aggregation technology is able to vastly increase speed, it also enhances reliability. Connectify Switchboard measures the connectivity and performance of each Internet



link in real-time. If any single connection fails, Switchboard will immediately re-route the traffic over other available Internet links. The software that is running over Switchboard will stay connected, seamlessly optimizing as Internet connections become available again. Switchboard gives users control over how the VPN behaves, allowing them to prioritize available Internet links, so that the expensive backup connections are not used unnecessarily. With Connectify Switchboard, teams in the field enjoy a seamless, persistent VPN session even as various low-bandwidth network connections come and go.

Unlike traditional VPNs, Connectify Switchboard uses advanced standards to navigate its way through firewalls and routers, including TURN (Traversal Using Relay NAT) and STUN (Session Transversal Utilities for NAT). This means that it can work on almost any network, discovering ways to connect even in restrictive network environments.

In fact, these speed and reliability features work so well that a user can, after connecting to a Switchboard VPN, connect to another IPSec- or TLS-based VPN (perhaps because the other VPN is certified for a particular application). Switchboard can take the encrypted traffic from the second VPN and spread it across multiple Internet connections to improve its speed and reliability, and then reassemble the packets and deliver them to the other VPN server. The employer gets the benefit of continuing to use the certified, proven security of their existing VPN service, and users get the extra speed and reliability that they have been hoping for.

The mobile workforce needs to be secured on the road, but they expect to get security without sacrificing their mobility or bandwidth. A new generation of VPN technologies will be needed to make this possible. Q

***Connectify**, an IQT portfolio company, creates easy-to-use software that improves bandwidth and reliability of mobile connectivity. To learn more, visit www.connectify.me.*

IN THE NEWS

The *IQT Quarterly* examines trends and advances in technology. IQT has made a number of investments in technologies that enable building automation, and several companies in the IQT portfolio are garnering attention for their unique solutions.

GainSpan

IQT portfolio company GainSpan makes Wi-Fi chip sets that enable Internet connectivity for a variety of everyday devices. As *Mobility Techzone* reported in July, GainSpan technology can support energy conservation through improved monitoring capabilities of essential services like water and electricity. Wi-Fi enabled chips can also be used to support a variety of healthcare and consumer applications, such as home alarm systems. GainSpan has been part of the IQT portfolio since March 2009. The company is headquartered in Sunnyvale, CA. **www.gainspan.com**

ikeGPS

ikeGPS, a product of New Zealand-based company Surveylab, makes a variety of portable systems for remote measuring and 3D modeling applications. The ikeGPS handheld device makes it possible for users to capture a variety of measurements and information about a building or object from a distance, while in the field. IQT initially invested in ikeGPS in December 2011. The company is headquartered in Wellington, New Zealand. **www.ikegps.com**

Lime Microsystems

Lime Microsystems recently announced that it has signed an agreement with Azio Electronics to distribute Lime's multi-band transceiver chips throughout China. These fully integrated RF chips enable connectivity to mobile devices that is tunable across 16 bandwidths. The company has also developed a Universal Wireless Communications Toolkit, which allows users to create highly configurable wireless systems of their own. Lime Microsystems has been a part of the IQT portfolio since March 2012. The company is headquartered in Guildford, UK. **www.limemicro.com**

Ember Corporation

Ember Corporation develops ZigBee wireless networking solutions that make buildings and homes smarter, allowing them to consume less energy and operate more efficiently. Ember's low-cost, low-power networking applications allow any business or industry to incorporate a variety of devices into a self-organizing network. The company ships more than 10 million chips per year for smart building devices. Ember was acquired by Silicon Labs in 2012 and is located in Boston, MA. In-Q-Tel first invested in Ember in September 2005. **www.ember.com**

IQT®

IN-Q-TEL