



PRO AV AND THE INTERNET OF THINGS

AN INFOCOMM INTERNATIONAL® WHITE PAPER

Copyright 2016 InfoComm International®
All rights reserved.
Printed in the United States of America

Published by InfoComm International, 11242 Waples Mill Road, Suite 200, Fairfax, VA 22030-6079

No part of this work may be used, reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without prior agreement and written permission from InfoComm International®.

The contents of this work are subject to revision without notice due to continued progress in methodology, design, installation and manufacturing in the audiovisual industry. This material is provided as is, without warranty of any kind, respecting the contents of this work, including but not limited to implied warranties for this work's quality, performance, merchantability or fitness for any particular purpose. InfoComm International shall not be liable to the purchaser, user or any other entity with respect to any liability, loss or damage caused directly or indirectly by this work.

Table of Contents

Acknowledgments	iv
Executive Summary	5
What is the IoT?	6
Technologies Behind the IoT	10
New IP Standard	10
Wireless	10
Supporting Network Essentials	10
Big Data	11
Mandatory Security	11
What Does the IoT Mean for Pro AV?	13
Smart Buildings	13
Smart Buildings in Action	14
Digital Signage	14
Managed Services	15
Smart Conference Rooms	15
Mobile AV	16
On the Horizon: AV Drones and Robots	17
Challenges Incorporating the IoT in Pro AV.....	18
Privacy	18
Distributed Control	18
Security	19
Strategy and Planning.....	19
Power	19
Conclusion.....	21

Acknowledgments

InfoComm International would like to thank the following industry experts for their generous contribution of time and knowledge:

Richard Blackwell, President, Linked2

Michael Colburn, CTS-D, Associate, CallisonRTKL

Gary Hall, CTS-D, CTS-I, Chief Technology Officer, Federal Defense, Cisco Systems

Daniel Jackson, Manager, Research and Development, Crestron Electronics

Shane Long, CTS-D, PMP, Principal, Waveguide Consulting

Executive Summary

The Internet of Things (IoT) has become ubiquitous. You hear about it on television commercials, on elevators, in Ted Talks. Industries across the spectrum are taking notice — from retail and manufacturing to IT and education. But the audiovisual industry has a special relationship with the IoT.

For one thing, the technology behind the IoT — a networked connection of sensors and devices that allow for monitoring, control automation and analysis — has been in use by AV professionals for roughly two decades. In that time, each of the various technologies that provide these capabilities has improved immensely. Sensors and processors have gotten smaller, delivering richer services with a minimal footprint. Networking and communication have become vastly more efficient and powerful, allowing machine-to-machine communication that reduces the need for human involvement in routine operations. And technologies for transmitting, storing and analyzing data have allowed organizations to derive insights from the myriad bits of information flowing around the IoT.

The capabilities provided by the IoT are essentially limited only by the imagination of those applying them. But in order for AV professionals to take advantage of these capabilities, they must understand several networking and data concepts, including IPv6, wireless networking, Power over Ethernet (PoE) and industry standards for capabilities such as video transport, data compression and connectivity, which are key to the flow of information that fuels the IoT. Mastery of these supporting technologies isn't essential, but AV pros need a basic knowledge of them.

Further, attention to security is imperative. As the number of networked devices increases, so do the security threats that AV deployments face. The encryption of all traffic on an AV network is essential, and AV systems also must be capable of authenticating the identity of authorized users. Many experts see security as the biggest impediment to widespread adoption of IoT technologies. For the AV industry, unlocking the value of the IoT depends on mitigating the risks that it presents.

With security and the underlying technologies taken care of, AV professionals can begin to find ways to deploy IoT-enabled systems. The monitoring and command-and-control capabilities that the IoT offers make it a good fit for managed AV service providers, who can use them to keep tabs on the state of equipment they provide to clients to maximize the efficiency of their maintenance and support efforts. IoT systems can take advantage of information shared by numerous networked devices, allowing AV to enable the smart scheduling of conference rooms, control equipment within those rooms, and even oversee power, cooling and lighting to create smart buildings. Smart digital signage is another promising IoT offering, and even more advanced capabilities are just over the horizon.

As they look to implement IoT systems, AV pros must take care to address several challenges that face many deployments, such as preserving the privacy of users on networked systems and properly handling all the data that is created and compiled by these systems. AV professionals who overcome these challenges are likely to find that the near-limitless possibilities of the IoT deliver a valuable reward for their efforts.

What is the IoT?

While the networked connection of devices is nothing new, numerous advances in technology have enabled the capabilities that are essential to what has become known as the Internet of Things, or the IoT.

For devices to be capable of the machine-to-machine (M2M) communication that characterizes the IoT, they must be equipped with sensors, processors and network connectivity, as well as software that controls these elements.

Advances in technology have led manufacturers to produce sensors and processors that are smaller and less expensive than earlier components while offering more features and greater power. This trend has fueled the proliferation of a wide variety of smart devices, such as automobiles, refrigerators, buildings' thermostats and surveillance cameras. Cisco Systems estimates that 50 billion objects will be connected via the IoT by 2020, and the IoT will generate \$19 trillion over the next decade. As more and more of these devices connect to each other on the Internet, they can deliver more sophisticated capabilities. Further adding value is the data that can be produced and compiled by smart devices. When analyzed effectively, this data can yield insights that otherwise would have gone unnoticed and unutilized.



Figure courtesy of Cisco Systems

These characteristics offer a number of benefits for the AV industry. The monitoring capabilities of the IoT allow AV professionals to oversee far more devices than they could otherwise. For example, a

video display that lets an AV pro know when it needs maintenance or that it may be configured improperly is one that doesn't need to be checked on manually. Further, a centralized management console can allow one AV professional to manage an entire fleet of equipment without ever leaving a room.

M2M capabilities and smart software can allow devices themselves to take on more simple management responsibilities. A smart conference room can sense when it is empty and dim the lights to save energy. Or it can sense when sunlight may cause glare and require window shades to be engaged. Taking human interaction out of these equations makes audiovisual operation easier for both end users and AV pros.

The collection of data from smart devices presents further opportunity for organizations that use it strategically. Applying analytics to this data can transform it into actionable insight. These insights can include predictive maintenance, letting administrators know when equipment is likely to break down so they can address the situation before an outage, or they can forecast demand to figure out how best to meet users' needs before a crisis hits. The next step applies these insights to transform business processes so AV professionals can maximize efficiency and optimize performance.

While the Internet of Things involves sophisticated devices, widespread network connectivity, robust software and piles of data, it's important for AV professionals to remember that people are an even more important element. Ultimately, the AV industry's mission is to connect end users and foster an engaging exchange of information and ideas. Even as IoT technologies reduce the need for human input in management and control of AV systems, organizations should maintain a keen focus on optimizing the experience for end users.

Evolution of the IoT in Pro AV

The AV industry was one of the first to dabble in the early incarnations of the Internet of Things. AV professionals, stuck in fixed workspaces, tried to bridge the geographic divides between end users by enabling technologies such as telepresence, videoconferencing and streaming media. In 1997, Crestron Electronics carried out one of the first deployments of Ethernet-connected control systems. The company tied projectors into control systems, enabling AV engineers to gather information from the projectors, such as data about power and the status of the equipment. This information was reported back to a centralized management software system so AV professionals could monitor the equipment from a single location.

A perfect storm of technologies came together to enable IoT capabilities. The miniaturization of sensors made them cheaper and easier to build into devices such as projectors, displays and speakers. As these devices got smarter, AV professionals saw more opportunities to connect them. In the early days of the Internet, most of the data traffic was either communication between users, such as email, or communication initiated by users, such as website requests. But now, billions of devices are connected to the Internet — many initiating their own communication — creating a new paradigm of data transmission and messaging capability.

In some ways, the automation functions of the IoT represent a necessary response to this proliferation of devices and connections. It's one thing to connect multiple devices in a handful of rooms, but when AV pros started scaling up networked device deployments to much larger systems, automation became an essential part of the implementation. When a single AV engineer is called on to manage as many as 50 or 100 rooms, AV equipment must be connected to the network, so that it can be remotely monitored and managed. Many organizations simply no longer have the manpower these days to send engineers around to so many rooms to physically inspect and manage equipment.

In addition, when more (if not all) rooms are connected, the data they generate becomes exponentially more valuable. When only a fraction of available spaces in an organization are connected, it offers a limited view of operations. Today, with more rooms and spaces connected via the IoT, AV professionals, technology managers, facility managers and others have a comprehensive view of how people, processes, data and technology interact.

IoT technology further evolved with the emergence of mobile platforms that took computing out of the office. Smartphones have greatly expanded the scope of connectivity beyond traditional fixed workspace environments. This, in turn, has expanded the scope of capabilities that AV professionals can deliver.

The emergence of cloud computing has driven even more advancements in AV technology for the IoT. When networked equipment first arrived in the AV industry, an entire system was required to be based on premise. In many cases, monitoring applications didn't run on a server, but on an engineer's computer, limiting the system's capabilities and scalability while placing management burdens on AV pros. Later generations of connected AV systems moved to sophisticated infrastructure with dedicated servers and databases. Modern IoT deployments have further advanced to include redundant failover capabilities and support for thousands of rooms. The infrastructure supporting these systems can be virtualized hosted on-premise or in cloud environments.

The cloud also allows AV professionals to take the data produced or collected by networked equipment and store it securely. It allows for detailed analysis of the data and provides engineers with the ability to custom design an application ecosystem that allows AV devices to be controlled remotely. This allows organizations to offload AV support to cloud providers, giving them all the benefits of sophisticated technologies without the hassles of managing them. Many costs are moved from capital expenditures to operating expenses, allowing accounting departments to pay for the technology in manageable monthly payments while future proofing their consumption of new capabilities. Migrating AV support and management to the cloud also provides greater scalability and flexibility. In the event that services need to be easily increased or decreased, this can be done simply, often through an automated system.

Software has been another key piece in the evolution of the IoT for audiovisual equipment. The industry has long connected devices to monitor and control them, but advances in software have allowed AV professionals to move these capabilities far beyond where they were in years past. Where once an AV professional might have been able to control a single conference room remotely, now he or she can set up a management system to automate control over thousands of rooms.

These advances in software and automation have allowed AV professionals to deliver a better experience for end users. This is why many observers consider the IoT the “Holy Grail” of the AV industry. Ultimately, AV professionals strive to deliver the best user experience possible. Users want to be able to walk into meeting rooms, classrooms or workspaces and get their work done with minimal effort. They also want to leverage technology in live events venues to entertain, motivate, and elevate their experiences. The AV industry smoothes the touch points between technology and people, transforming machine signals into usable information and digitizing business processes and communication. The IoT allows AV professionals to create the experience users demand and automate it so that it is delivered consistently, efficiently and seamlessly.

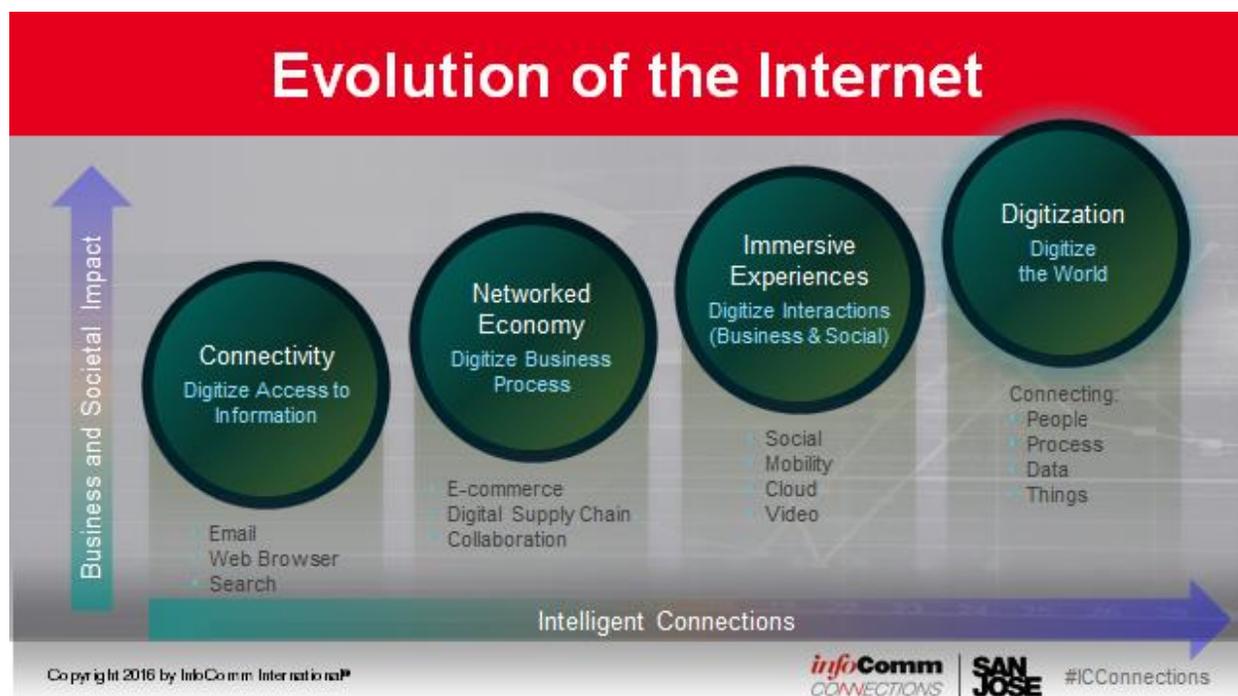


Figure courtesy of Cisco Systems

Technologies Behind the IoT

AV professionals who intend to take advantage of the capabilities offered by the Internet of Things must understand several foundational elements. Mastery of supporting technologies isn't essential, but AV pros need a basic knowledge of several important networking, communication, data and security concepts.

New IP Standard

Among those basics is IPv6, the most recent version of the Internet Protocol. IPv6 was developed to replace IPv4, the standard on which most of today's Internet-enabled equipment operates. IPv4 was established to route traffic on the Internet and provide information such as identification and location for networked computers. However, the standard uses 32-bit addresses, meaning that only 4.3 billion can be created using IPv4, a number that is being exhausted by the massive number of devices on the Internet. IPv6, which uses 128-bit addresses, offers an essentially unlimited number, which will allow for the deployment of the huge numbers of IoT devices in coming years.

Many organizations are only starting to implement IPv6-enabled equipment, but the standard is becoming more important to IoT deployments. Some government agencies require AV implementations to be IPv6-enabled, making it critical for AV firms looking to do business with the public sector. As more Internet traffic begins to flow across IPv6 equipment, familiarity with the standard will be more important for AV professionals in all sectors.

Wireless

Wireless networking is another foundational element that AV professionals must get up to speed on to make use of the IoT. The AV industry values wireless deployments because they eliminate the hazard of tripping as well as the desire to minimize the mess of unsightly cables. With the huge number of devices being added to networks for IoT applications, the benefits of wireless networking become even more valuable, starting with the advantage of being able to connect devices to the Internet without having to run copper or fiber cables.

However, the ease of connecting these devices leads to more of them being placed on a network, which increases the demands on bandwidth. Fortunately, the latest Wi-Fi standard, 802.11ac, greatly increases the throughput of a wireless network and offers several other features that further accommodate additional traffic. AV professionals can also take advantage of other wireless alternatives, such as WiDi, WiGig, WHDI and WirelessHD.

Supporting Network Essentials

For devices that are connected via copper cabling, the Power over Ethernet standard delivers another important capability. As devices and sensors proliferate, the ability to power them via the same cables that connect them becomes vital. POE allows AV professionals to maintain power to their IoT nodes without having to run electrical cables or rely on batteries.

PoE is a critical enabler of the IoT, and as such, it is ripe for continued development. For example, while standard PoE, as defined by IEEE 802.3af, can deliver up to 15.4 W of power to a device over Category cable, PoE+ (IEEE 802.3at) promises up to 25.5 W. Cisco Systems developed a proprietary PoE called Universal PoE (UPoE) capable of delivering more than double the power of PoE+.

AV professionals also need to understand industry standards for capabilities such as video transport, data compression and connectivity, including 3G, 4G and LTE, which are key to the flow of information that fuels the IoT.

Big Data

By some estimates, the amount of data generated by *things* on the Internet is 277 times greater than the amount of data generated by *people* on the Internet. To realize fully the potential of the IoT, AV professionals must handle data strategically and efficiently. Data must be transmitted across the network to make use of automation and monitoring. The vast amounts of data the Internet of Things produces make cloud computing an attractive option for computation, analytics and storage. AV professionals should have at least some familiarity with databases and how they work, because many of the capabilities the IoT offers are database-driven. The vast amounts of unstructured data produced by IoT systems must be analyzed with structured data from databases to provide additional context and deliver greater insights.

AV pros also should learn the basics of fog computing, an architecture that uses end-user clients or other devices to enable data analytics at the edge of a network, taking advantage of the IoT's machine-to-machine communications. When data is analyzed automatically at the edge, it can deliver real-time value without sending unwanted data to take up space in the cloud or in an organization's storage systems.

Mandatory Security

As the number of networked devices increases, so do the security threats that AV deployments face. AV professionals must understand the security challenges they face in fielding IoT deployments and have a working knowledge of the defenses they plan to use against these threats. Any new AV deployment that takes advantage of IoT capabilities such as monitoring or automation creates new threat vectors on the network that can be exploited. These threats grow in scope as IoT deployments add hundreds or even thousands of devices and sensors beyond the edge of the network.

In years past, security may not have been a top-of-mind concern for the AV industry, but that attitude has evolved with a changing AV landscape. When AV systems were "air-gapped," meaning they were not connected to the public Internet, engineers could focus on other issues ahead of security, but that's not the case with the vast majority of IoT deployments, which could be vulnerable to hackers if not protected properly. Security has become an imperative. AV systems need to be protected from security threats, because a network is only as good as its weakest link. No AV professional wants his or her systems to be that weakest link.

As IoT projects increase the number of connected devices, AV professionals must employ encryption on all network traffic. AV systems also must be capable of authenticating the identity of authorized users. Passwords for individual systems are insufficient to meet this need. More effective authentication can be achieved by integrating AV systems with an organization's Active Directory or Lightweight Directory Access Protocol service. AV professionals should also consider how using network segmentation can improve the security of connected devices and systems. This segmentation can be



achieved physically, through the use of different wireless frequencies, and digitally, via network routing techniques.

The importance of meeting the security challenge is difficult to overstate. AV professionals won't be able to realize the full value of the Internet of Things unless they can mitigate its security risks. Effective cybersecurity strategies are comprehensive and architectural. AV and the IoT are important aspects of end-to-end security, but integrated threat defense relies on protection and cooperation across all aspects of information and communication technologies.

While they have a lot to learn as they dive into IoT deployments, one thing that AV professionals don't have to do is become an expert in all these technologies. Simply understanding these concepts, knowing which questions to ask and where to find true experts who can answer them, should be enough to get their IoT projects off and running.

What Does the IoT Mean for Pro AV?

For AV professionals who understand the essential disciplines of the IoT, the opportunities it offers are limited only by the imagination. Monitoring capabilities allow AV pros to keep an eye on an entire fleet of far-flung audiovisual equipment, assessing maintenance needs and operational issues. The same connections that provide this monitoring information can also enable remote command and control, allowing an engineer to start meetings or manage equipment from a remote location. The IoT's machine-to-machine communication and automation capabilities can deliver an even more robust level of management, solving AV problems and managing systems such as digital signage without even requiring human intervention. The collection and analysis of the data created by these operations allows AV teams to gain deeper insights into their systems, such as predicting when a telepresence system may need maintenance or seeing a spike in demand for a conference room before it occurs.

Smart Buildings

AV professionals are integrating building systems such as HVAC and lighting to make them smarter. The various capabilities of the IoT allow a building to respond to residents' actions as well as changes in the surrounding environment, such as temperature and sunlight. For example, these smart systems can automatically turn the lights off and the heat down in an empty room. Buildings tend to consume tremendous amounts of energy, so providing these capabilities can deliver significant improvements in efficiency, saving energy and money while reducing greenhouse gas emissions. A study by the American Council for an Energy Efficient Economy determined that commercial buildings could save up to \$60 billion if investments in energy efficiency were ramped up by just 1 to 4 percent.

Installing high-efficiency systems for lighting, heat and air conditioning can yield significant improvements in energy consumption, and integrating these systems via the IoT can greatly enhance these improvements. But integrating these systems and running them more efficiently requires some expertise. Smart building operators must understand both the electronics and mechanics of a building. Integrated sensors are required to collect data from specific areas of the building. Numerous sensors are necessary for this effort, and they must be placed strategically throughout a building to collect data that can be mined and analyzed for insights to drive efficiencies.

The real value in these systems isn't in informing AV professionals of a problem that is happening currently, such as a burned-out bulb in a projector or a heating malfunction. Rather, the analysis of this data delivers true value by helping building engineers spot potential problems before something goes wrong, so they can be corrected without ever inconveniencing end users. For example, a smart building can inform an engineer that a damper is stuck or a valve is leaking, which can lead them to address the problem before the air conditioning system breaks down, leaving a building full of uncomfortable residents. Or smart buildings can let AV professionals know where systems are operating inefficiently, so that smart solutions can improve operations.

AV professionals who operate smart buildings must be able to integrate systems and components at a variety of levels. The most basic level, physical integration, connects systems throughout a building via structured cabling. The consolidation of cables and equipment yields efficiencies such as using only a

single cable contractor for an entire building. This simplifies maintenance, ensures standardization and reduces the cost of installation.

The integration of network components requires AV professionals to work with IT staff. Many solutions that allow for the intelligent automation and management of building systems use open protocols such as BACnet, Modbus and LonWorks.

Smart buildings can deliver even greater functionality by application integration. Connecting systems such as security and access control with heating/air conditioning, AV and lighting allows building systems to provide specific conditions for an individual employee who is identified by an access card. This level of integration also allows building managers to consolidate information from a variety of systems onto a single dashboard, simplifying management and improving performance.

Ultimately, smart buildings should help AV professionals deliver greater uptime at a reduced cost, which leads to greater satisfaction among tenants.

Smart Buildings in Action

The federal General Services Administration (GSA), which handles acquisition, travel, real estate and management responsibilities for many other federal agencies, expects to save as much as \$15 million per year through its Smart Buildings initiative.

The initiative integrates systems at federal buildings operated by GSA, allowing tenants to view the performance of these systems on dashboards that show energy savings and other metrics, as well as recommendations to further increase efficiency. For example, by connecting the agency's hoteling reservation system for user workstations with a building's energy systems, the initiative allows employees to check automatically into their reserved workstations. Once a user arrives at his or her workstation, the lighting and HVAC systems are engaged into active mode.

The management systems at each smart building feed to a central cloud-based platform that provides the agency with even more insights into operations, helping it to find even greater efficiencies.

Digital Signage

Networked digital signage is another product type that takes advantage of IoT capabilities. With network bandwidth increasing, the arrival of new infrastructure technologies and digital display prices dropping significantly in recent years, many organizations have greatly expanded their deployments of digital signage. AV professionals can network digital signage with other devices such as computers, sensors, cameras and databases to change displays dynamically.

Digital signage can benefit greatly from the flexibility offered by wireless networking, allowing easier deployment in hard-to-reach areas that might be infeasible by wired connections. Once deployed, these digital signs can take advantage of management, automation and data analysis capabilities to make use of data from numerous sources to adjust the content they show for specific audiences.

For example, digital signage can be deployed throughout a factory to give employees real-time updates on workflow and other conditions. The technology also can be used for retail deployments to interact with individual shoppers, offering them special deals or providing information on products in which they have expressed interest.

Managed Services

The monitoring, automation and command-and-control capabilities that the IoT offers make it a good fit for managed AV service providers. Service providers must keep close tabs on the state of solutions they provide to clients to maximize the efficiency of their maintenance and support efforts.

Industry research shows that managed services make up 41 percent of the North American pro-AV market, a portion that has grown over the past few decades. This growth reflects an evolution in the industry, with AV professionals focusing not only on products, but also design and integration services.

Competition in the AV industry has led companies to expand their offerings. Innovative AV firms recognize the needs of their clients and tailor services to meet these needs efficiently and precisely. These services include specific functions such as cloud-based video collaboration or remote monitoring of AV systems. AV companies can deliver these services in a variety of ways. The capabilities of the IoT provide numerous advantages for firms that offer AV services.

In a remote monitoring scenario, an AV company can deliver its staff expertise via connected devices. For example, AV professionals can monitor the status of a customer's networked audiovisual components to make sure they are operating properly. A staff member can diagnose problems remotely or even initiate corrective action online. The status of AV systems deployed at multiple locations and among numerous clients can be collected on a single dashboard, greatly improving the efficiency of the operation.

AV companies are also able to use IoT-enabled hardware and software to offer AV as a service. For example, if a client needs to deploy videoconferencing capabilities but doesn't want to pay for an entire system, the client can purchase this capability as a service. An AV company can either deliver these services on its own infrastructure or on hardware owned by another company, which it resells. Purchasing AV as a service allows clients to avoid hefty investments in hardware as well as expert staff, and instead they pay a monthly subscription fee for the services they need.

Smart Conference Rooms

AV hardware manufacturers have developed products that can power smart conference rooms aimed at elevating the whole room experience. In an ordinary conference room, users may find a cable that can be plugged into a computing device for presentations and perhaps a sign that offers instructions on how to get started. It's up to the meeting organizer to handle the AV equipment or to find help from a professional. Smart conference rooms deliver the services and user-friendliness that an AV professional provides without making demands on one.

Smart conference rooms may come equipped with a touch-screen outside the door that shows whether the room is booked or available. These rooms can let meeting organizers know when a room is available later in the day or whether other nearby rooms may be available. They allow users to book rooms easily and can determine if users who book a room actually show up for the scheduled meeting. If users don't show up by a particular time, the system can automatically change the booking status of

the room so others can use it. Sensors in the room can turn lights on and off depending on whether the room is occupied and even raise or lower shades depending on the position of the sun.

Smart conference rooms can be integrated with standard office systems such as email, web clients, IP phones and even users' smartphones, making it easier and more efficient to book, plan and conduct meetings. They can improve the collaboration and productivity of meetings, enhancing the experience of attendees, and boost the efficiency of systems such as power, heating and air conditioning. Some smart rooms also have reporting and business intelligence capabilities that provide insight into room utilization and help meeting organizers plan better.

Mobile AV

One IoT application that some AV manufacturers are working on is technology to enable mobile collaboration equipment that brings advanced video and communication hardware to users, instead of requiring them to visit a conference room with a lot of expensive AV technology. A user may summon a mobile setup that provides a high-definition videoconferencing camera and screen, increasing the availability and usability of the technology. AV professionals could utilize the monitoring capabilities of the IoT to keep tabs on the status of the equipment and remotely troubleshoot any problems that may arise.

By mobilizing audiovisual equipment itself, AV professionals would not have to install dedicated hardware in as many rooms. Instead, a room could be equipped with a dock for mobile AV equipment that can go where it's needed. This would reduce costs and allow AV to offer a richer experience with higher-end equipment that can be shared among a greater number of users. It also would enhance the convenience of meetings and save users' time.

Several manufacturers have demonstrated hardware products with mobile AV capabilities, but this technology is largely still in development. That said, there are several software collaboration solutions that run on mainstream mobile devices, such as Jabber, Skype, WebEx, and Spark. Moreover, so-called AV robots that mobilize collaboration systems are also now on the market (see "On the Horizon: AV Drones and Robots," page 17).

On the Horizon: AV Drones and Robots

When they hear the word “drone,” many end users may think of quadcopters taking in-flight video or unmanned military aircraft carrying out attacks. But the term can be applied to any mobile computing platform that can move under its own power. This concept presents some interesting possibilities for the AV industry.

In one promising application, connected mobile devices with wheels could carry teleconferencing technology, such as tablets or videoconferencing displays, to users. These telepresence robots, some available today (see below), could make communication simpler for users in far-flung offices. Instead of checking on a colleague’s status via a presence application or webcam, a remote user could log in and pilot a robot over to the colleague’s cubicle or office for a quick meeting. Such devices could facilitate collaboration when users are unable to visit conference rooms.

In another AV-oriented application, drones may be fitted with directional microphones for audio capture to improve communication in large conference rooms. However, the use of microphone-equipped drones may raise privacy concerns with some audiences. It remains to be seen how the industry may adopt AV drones.



Suitable Technologies' BeamPro is available today.

Photo courtesy of Suitable Technologies

Challenges Incorporating the IoT in Pro AV

While the IoT presents numerous opportunities for improving efficiency, productivity and collaboration, AV pros need to be aware of several hurdles they may face. Failing to address the issues that arise could hamstring IoT efforts and limit the return that organizations see on their investments in the technology, infrastructure and expertise that support these efforts.

At a basic level, it will be important for the industry to develop and adopt devices that are, for lack of a better term, “IoT-ready.” In a future dominated by the IoT, it will do little good for an organization if they install an HDMI switcher, for example, that can’t communicate whether it is connected or there is an HDCP problem. For AV solutions to take true advantage of IoT technology, the underlying AV equipment must be able to generate and communicate usable information in a format that is understandable by other systems. In other words, selecting the right equipment will be as important as it ever was, but for evolving different reasons. On top of that, AV professionals will have to pay attention to other issues that arise in light of IoT-enabled deployments.

Privacy

Privacy is an important consideration for AV professionals as they plan IoT deployments, and one that raises concerns for many parties. Connected systems, such as in smart buildings and conference rooms, use the data they collect to improve efficiency while delivering a valuable user experience. But some users may be worried about what a building knows, such as what they’re doing and where they’re going. These concerns are heightened by the collection and analysis of this data. Users may not have any particular concern about data transmitted by a single endpoint, but when data from multiple endpoints is compiled and analyzed, it may provide IoT operators with sensitive information.

Part of the privacy problem with IoT deployments is that end users may not understand they’re being monitored, how this monitoring takes place or what the information it yields is used for. Some organizations may want to offer end users some control over how they are tracked or even the choice to opt out of monitoring.

Distributed Control

Many of the benefits of the IoT are based on the distribution of monitoring and control, but achieving this distribution can present a challenge for AV professionals. Collecting data from and establishing control of widely disparate devices and sensors demands effective integration, and this challenge only grows as the number of connected devices increases.

Several vendors offer middleware products to connect complex systems that were not designed to be connected. Middleware essentially serves as the software glue that holds an IoT deployment together, linking sensors and applications to ensure effective communications among these disparate pieces.

Security

Many of the products that are now being connected to networks as part of the Internet of Things historically have not been manufactured with security in mind. Indeed, the security of refrigerators or projectors hasn't been a critical issue, but the connectivity of the IoT makes it one. Not only can unsecured AV hardware be vulnerable to compromise by hackers, but it potentially can serve as an entry point for a broader cyberattack. And the wider an IoT deployment extends, the wider an attack could spread.

Every party involved in an IoT project should take responsibility for security. The manufacturers of AV products must bake security into their products from initial design, rather than adding it as an afterthought. Hackers should not be able to consider devices in an IoT system as an easy target for attacks.

AV professionals who install devices and systems should recognize the special considerations of the IoT in their security policies. They also should stay up-to-date on security issues and best practices. Security threats are constantly evolving, and AV professionals should keep pace with cyberattackers. In deploying IoT systems, AV pros should utilize devices with built-in security features and make sure to enable these features. Any default passwords should be changed immediately to strong passwords, and functions such as encryption should be applied to traffic on any networked systems.

Finally, users should be aware of the role they play in maintaining an effective security posture. They should receive regular training so they understand an organization's security policies as well as the kinds of threats they face.

Strategy and Planning

One of the biggest challenges that AV integrators, consultants and technology managers face is planning an IoT project. An important first step is to talk to all relevant parties, including organizational decision makers, who can spell out their goals and objectives for any deployment, and IT managers, who can provide information about infrastructure and support technologies. AV planners should also talk to users to get a sense of their pain points and needs, as well as vendors who can explain product features and specifications.

These discussions should lead all parties to a solid understanding of the expectations for a given project. During planning, AV professionals and users must learn what is possible with an IoT project and establish realistic goals for what it will accomplish.

This planning should also include objectives for how data will be used. The command-and-control capabilities of the IoT are attractive to many organizations, but if a project doesn't also make use of the data it collects, it isn't delivering its full value.

Power

As the number of devices involved in an IoT deployment grows, so does the challenge of getting power to all of them and maintaining the reliability of that power. Electrical cabling offers a ready source of power for devices and network connections, but when electrical outlets aren't available, AV



professionals need a plan for getting power to their endpoints. Power over Ethernet offers a useful option for networks with copper cable infrastructure, but for wireless deployments and other remote equipment, batteries are an alternative.

Manufacturers of IoT-enabled AV products are taking power considerations into their design, in many cases focusing on improving efficiency to reduce the need for power. As IoT capabilities evolve, vendors are looking at incorporating power-generating elements such as solar cells or technologies to convert heat or vibration energy into electricity.

Conclusion

For many professionals, the Internet of Things delivers the “Holy Grail” of the audiovisual industry, but before they can take advantage of its benefits, they must engage in some serious thinking.

The IoT moves data about users and their activities across a variety of systems. AV professionals should be transparent about how this data will be used. They also need to address the hurdles of the IoT. Security should be a top concern for every AV professional who works on an IoT project. Organizations that don't address these security needs are likely to regret this oversight. The news is full of reports of catastrophic breaches that cost millions of dollars and cause irreparable damage to companies. AV professionals must ensure that they're not responsible for a breach.

But other hurdles also require AV's attention. To integrate systems effectively into an IT deployment, AV professionals need to understand how these systems operate and work with stakeholders to consolidate operations.

Once the hurdles have been overcome, AV pros have an opportunity for true innovation. One smart strategy to get innovative projects off the ground is to start small. Keep things simple at first, and expand operations as experience and expertise grow.

As the AV industry takes on a growing number of IoT projects, all parties have some important considerations to keep in mind. Product vendors should tailor their solutions for the IoT, taking into consideration factors such as connectivity, power and security. The challenges that AV pros face in their deployments will be minimized if vendors optimize their products for the IoT.

AV professionals who engage in IoT deployments need to map out carefully their objectives. The IoT can be a scary place, but proper planning can help organizations overcome problems and meet their goals. The possibilities are endless — AV pros just need to draw a roadmap to where they want to go. As they make their way, it's important to keep the primary objective in mind: an exceptional user experience. The Internet of Things can deliver numerous benefits — greater efficiency, cost savings, improved management and streamlined operations — but the ultimate measure of success is user satisfaction.