White Paper

Embracing the Internet of Things

Darryl Daniel, PMP, and Jim Davis, PE, RCDD
Burns Engineering

Virtual Ramp Control System at Ft. Lauderdale-Hollywood International Airport

Photo courtesy of Broward County Aviation Department

Smart Restroom at Los Angeles International Airport

Photo courtesy of Infax

Smart thermostats, camera-equipped doorbells, and talking virtual assistants have become commonplace in homes today. The goal of these technologies is to automate common tasks and make our lives easier.

Similarly, airports are in an advent of technology, and are seeing exciting innovation with the Internet of Things (IoT). Air travel can often be filled with anxiety. The uncertainty of large crowds, long lines, confusion and delays when traversing the airport is not something most passengers look forward to. Imagine a smart, information-rich airport experience beginning at arrival and check-in, continuing through security, finding your gate, the lounge and retail experience, boarding your plane, inflight entertainment and connectivity, all the way through the hunt for your bag when you arrive at your destination.

The IoT improves and interconnects technology, shifting the focus from people-to-people to thing-to-thing communication. In the end, though, the goal is to revolutionize the ways in which people access and consume useful information – and airports are at the forefront of this technology revolution.

Major airports are quickly adopting technology to deliver safety and operational efficiency benefits, while also enhancing the passenger experience. As Los Angeles World Airports CEO Deborah Flint said, “The future of airports is advancing at a rapid pace. It’s about 21st-century connected infrastructure—modern infrastructure that, through technology and excellent building, is providing quicker, more expedient, more certain, and more informed ways of transporting our passengers and doing business in and around the airport.”

IoT initiatives at airports have increased significantly in the last few years. While many initiatives focus on improving passenger experience, others target ease of building system monitoring and maintenance, improving security, or identifying additional sources of revenue for the airport operator and even its tenants.

With these benefits, however, come challenges in the form of increased burden on network infrastructure and heightened cybersecurity risk. A recent report by *The Economist* indicated that we have moved past the early hurdles of understanding and perception of IoT to more practical obstacles having to do with infrastructure cost (29% of those surveyed); and security and privacy concerns (26% of those surveyed).

The Infrastructure Challenge

This seemingly-utopian world where everyone receives an endless stream of actionable data is not without challenges. The deployment of ubiquitous connected devices requires ubiquitous connectivity, and many airport networks are not up to the challenge – yet. While large-scale new construction and major renovation projects at airports are happening with increasing frequency, many other airports are making the best of what they have as they rush to keep pace with technology innovations. Network infrastructure weaves its way through buildings behind finished walls, ceilings and floors, and is frequently difficult to upgrade without major disruptions to daily operations, and without impact to the passenger experience.

Infrastructure is frequently the costliest component when implementing or upgrading a network – IoT or otherwise. Take, for example, a $2.1B airport terminal project that is currently under construction in the U.S. The technology budget for the project is $112M, which includes $40M earmarked for advanced multimedia features. The remaining $72M includes funds for common use passenger processing and self-service, visual docking guidance systems, telephone, public safety and operational radio distributed antenna systems (DAS), life safety (including fire alarm and emergency paging), physical security systems (video surveillance and access control), active network components (switches, routers, wireless access points) and structured cabling (including cabling itself as well as conduits, raceway and patching). Of this $72M budget - structured cabling alone, not including active network equipment – accounts for more than one-fifth (22%).

Despite the necessary cost, network infrastructure is arguably the least visible component of any technology ecosystem. End users don't realize infrastructure is failing until the services, apps, and conveniences they rely on slow down or stop working entirely. Even with the initial expense, provisioning the proper infrastructure on day one is orders of magnitude cheaper than trying to retrofit later. Whether facing a greenfield installation or major retrofit, the key to keeping pace with IoT's proliferation is to observe technology trends and make informed, forward-thinking decisions regarding infrastructure. This lays a solid foundation for building successful technology initiatives.

One consideration regarding the cost of supporting infrastructure is the concept of shared networks. As shared networks are already common with distributed antenna systems (DAS) and public safety radio, Bluetooth Low Energy (BLE) beacon technology makes for an obvious choice where the cost of the network can be shared. It makes much more sense to deploy a single beacon network airport-wide, rather than to have each tenant, airport operator, or agency deploy their own. The beacon registry can be shared with all authorized partners, which reduces the RF clutter associated with multiple beacon networks in the same space. Due to the broadcast-only nature of beacons, the security risks with a shared network are low. Are there opportunities for cost savings with other

shared supporting network examples? The answer is yes, but at what cost to security and privacy concerns?

There is some good news on the way. It's called a transformational cellular network advancement - 5G. Improvements over now-traditional 3G and 4G cellular networks include increased speed and capacity, as well as decreased latency. With speeds approaching, or even exceeding, those of traditional wired networks, 5G looks to be ideal for many IoT scenarios. While it is important to understand the future promise of 5G, it is also critical to realize the limitations, namely the time of deployment by the major domestic cellular carriers and limited coverage areas, at least in the near term. The latest estimates indicate limited rollouts to select cities later this year, but do not expect to see any major deployments until 2019 – and certainly nothing approaching nationwide networks until at least 2020.

The Benefits of Being Connected

Indoor wayfinding is an example of passenger experience-boosting technology that has already gained a foothold internationally. Just like Google Maps guides you as you travel outdoors, these systems provide turn-by-turn directions inside an airport terminal to guide passengers to their desired destination, whether it be a specific restaurant, retail store, or gate. These applications employ BLE beacons or Wi-Fi based devices which interact with an app installed on the user's smartphone to ascertain their location and provide airport map data.

Airport tenants like restaurants or retail stores also stand to benefit - they can leverage the airport's wayfinding app to push promotional notifications to passengers when their mobile device is near their storefront. With proper data integration among airlines, airport operators and retailers, notifications can even be customized based on the user's airline, gate and departure time.

Conversely, airport operators are taking advantage of passengers' mobile devices to gain insight into how their airport is operating. Airport operators detect and track Wi-Fi and Bluetooth signals to map passenger flow throughout a terminal, track and display wait-times through TSA screening checkpoints, monitor restroom usage to inform maintenance frequency, and develop more informative key performance indicators (KPI) based on this data. Examples of KPIs include customer satisfaction with restroom cleanliness, or reduction of wait times at checkpoints or check-in counters.

Airports are also adding network-connected sensors and processors to traditionally standalone systems such as HVAC, facility lighting, energy metering, and more. HVAC and lighting setpoints can be automatically adjusted based on scheduled gate usage through integration with the Airport Operations Database (AODB). The resulting energy usage savings due to decreased HVAC load and reduction in lighting usage can be monitored thanks to smart, network-connected sub metering and energy monitoring.

Securing the Internet of Things

Almost any network-connected device can serve as a target for cybersecurity threats. The ever-decreasing barrier to entry in the purchase and deployment of IoT devices, combined with the sensitive types of systems and data they access, is a one-two punch for cybersecurity.

Ease-of-use is one of the hallmarks of the Internet of Things. Network-connected data storage has been around for decades, but it wasn't until the term "cloud" was coined and user-friendly services were marketed in the late 2000s and early 2010s, that the concept gained mainstream attention. Similarly, the first IP video surveillance camera was released by Axis Communications in 1996, but it wasn't until companies like Nest and Ring began producing user-friendly versions that home video surveillance gained a mainstream consumer foothold. These user-friendly devices allow those with very little IT expertise to connect to and operate them. Unfortunately, the associated security risks are seldom understood. For example, the average layperson installing a video-enabled doorbell likely doesn't understand what measures should be taken to segregate their cloud-connected device from their home PC which stores sensitive personal and financial data. In a commercial environment, these risks increase exponentially. It is important for airports to carefully examine their IT policies regarding connection of new devices to the network, implement appropriate security measures to prevent connection of unauthorized devices, and educate employees and tenants regarding the associated risks.

In addition to the connection of "rogue" devices, proper network architecture is key in secure IoT implementation. Take, for example, the 2013 breach of Target's payment systems, which allowed intruders to steal 40 million credit card numbers. Attackers gained access by obtaining a maintenance contractor's login credentials and exploiting an HVAC system's remote connection via the public internet. Although access to heating and cooling energy usage data is relatively benign, the system resided on the same network as the retailer's point of sale (POS) systems, which provided access to credit card records. Despite the external breakdown in security that occurred and gave the attacker access to login credentials, Target likely could have prevented this breach through proper network architecture. It would have been more secure for the HVAC and POS systems to reside on separate network segments, with robust security measures in place to prevent the exchange of data between them. In an airport environment, a similar example could apply to critical airport systems and public Wi-Fi access. Additionally, a passenger's public Wi-Fi connection should be securely segregated from the network that connects the terminal's building management system, airport operational database, and other sensitive systems.

A Recipe for Success

IoT continues to transform the way smart devices and humans communicate with one another. At airports, this technology enables passengers to experience an information-rich environment, tenants to increase revenue, and operators to gain in-depth insight into their airport's operational status. Airports can benefit from an investment in robust, well-thought out infrastructure that will support this proliferation of technology. Increased connectivity creates operational efficiencies and improves the passenger experience. Is your airport ready?

Darryl Daniel, PMP, is a Project Manager with Burns. Jim Davis, PE, RCDD, is a Special Systems Engineer with Burns. Burns is one of the nation's most respected providers of specialized engineering services, delivering highly technical, sought-after engineering expertise on complex transportation and critical infrastructure projects. For more than 50 years, aviation clients have turned to Burns for state-of-the-art innovation, rigorous engineering expertise, and outstanding client service. The company is ranked a Top Workplace and ENR Top 500 Design Firm.

burns-group.com