RETA The Real Estate Technology Alliance

INTERNET OF THINGS FOR REAL ESTATE

Version 1.00

21 May 2020

About RETA

Real Estate Technology Alliance (RETA) is an association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable real estate companies and their technology vendors to do business globally in the 21st century. RETA is recognized as the leading voice of the global real estate community, articulating the technology requirements of companies of all sizes to the vendor community. RETA facilitate the development of technology models that will foster innovation, improve the customer experience, increase the effectiveness and efficiency of real estate companies, and create a healthy ecosystem of technology suppliers.

TABLE OF CONTENTS

Introduction

Real estate, multifamily and other property types have been inundated with a marketing barrage detailing explosion of the “internet of things” (IoT) for the better part of a decade. While IoT solutions represent significant potential value and savings for real estate companies, every solution buyer needs to educate themselves prior to generating a thoughtful IoT strategy.

A viable IoT strategy evaluates:

- People – customers, renters, staff, maintenance, third party, corporate roles
- Process & business outcomes – access control, package management, building management, asset protection, risk mitigation, increased revenue
- Technology – devices, infrastructure, communications, interoperability

The first step in establishing this strategy is to define the goals implementation will achieve. The self-assessment checklist and vendor questionnaires in this document will help the reader build and socialize those goals within a company. After significant completion of those checklists, the reader will be able to go to the market and identify best of breed solutions based on the infrastructure, device management, security, and other best practices identified in this document. Ultimately, this will yield a decreased time to procurement and buy-in from your stakeholders at all property types.

While this document and companion material will educate the industry, it is not exhaustive and should be adapted to a companies’ specific needs. This document does not offer legal advice or contractual specifics but does demonstrate the right questions to ask potential partners.

Authors

While over thirty companies contributed to the writing of this document, the following individuals contributed the majority of the content. The Real Estate Technology Alliance thanks these individuals & companies for their work.

Author Name	Company
Tom Spahn, co-Chair	Camber Creek
Sean Miller, co-Chair	PointCentral
Felicite Moorman, co-Chair	STRATISIOT
Marshall Friday	ADT
Brian Bullock	Alliance Residential
Michael Hejtmanek	BuildingLink
Aaron Gray	Eleven
Robert Cooper	Embue
Elaine DeLude	LIVEbe Communities
Alec Page	RET Ventures
Patrick Dunphy	RETA
Josh Erosky	Secure Multi-Family
David Schrader	SightPlan
Demetrios Barnes	Smart Rent
Ryan Buchert	STRATISIOT
Joe Shiraz	Valet Living
Tim Koruna	White Oak Partners

IoT Solution Definitions

Some solutions or use cases may cross multiple categories of IoT systems.

- Resident Amenities - Products and/or services that drive residents to choose one property over another and/or pay more in rent or fees to access an amenity.
- Operational Efficiencies - Products and/or services that help property managers be more efficient in marketing, leasing and maintaining a property.
- Asset Protection - Products and/or services that help detect problems earlier, respond to issues quicker, and/or prevent misuse of assets in the first place.

Smart Access Control

A smart access control (SAC) system allows a user to control access to a physical space. Smart, in this context, means a computerized, interconnected system that enables a user to control access to any part of the property that is in scope of the SAC system. This is accomplished through the use of devices to secure the access points of a space, a method for collecting credentials of individuals attempting to access the space, and a back-end system that allows an asset manager to set the parameters that allow access. A SAC system should have a process for granting conditional access and a secure method for logging access, and attempted access, to a space. A SAC system will typically have multiple access layers, for example common areas and private spaces. SAC systems need to be able to effectively control access of tenants, prospective tenants, staff, visitors, customers, vendors, and other potential property users. Ideal SAC systems control access in the least obtrusive manner while prioritizing building safety and security. **Value created may include a return on investment, access for third parties, improved safety for staff and customers, operational efficiency, convenience, and other items.**

Facilities Condition & Event Monitoring

Facilities condition and event monitoring (FCEM) solutions are methods to measure, track **and notify on** key items of interest relating to a physical asset. The parameters monitored can be tailored to a specific asset's requirements but can include temperature, humidity, smoke, fire, CO levels, energy use, water usage, leak detection, presence/occupancy and potentially other components. On the back end, FCM solutions should have a method for timely notification of key stakeholders when time-sensitive conditions that require attention arise, as well as the ability to track trends to identify longer-term concerns. **FCEM is valuable for three main reasons: 1) occupant safety/comfort/convenience 2) asset loss prevention, and 3) operational expenditure (OPEX) savings.**

Building Control Systems

Building control systems (BCMs) allow a user to change the condition of an asset's physical components including lighting, HVAC, blinds, locks and more. BCMs can process command inputs directly from a user or

they can be linked to an FCM solution to automate changes based on user-defined parameters. **The advantages of BCMs can include utility operation cost savings (for both the owner and the customer), customer and staff convenience, and customer and staff safety.**

Checklists for The Real Estate Technology Ecosystem

Questions for Potential Vendor Partners

Operators, developers, and managers (ODMs) of real estate companies and properties should thoroughly review potential Internet of Things (IoT) solutions and platforms. The following questions are the minimum that buyers should consider before the procurement process.

Does the proposed product/service integrate with our current property management software?

Choosing a product/service that integrates with an ODM current property management software can lead to operational efficiency. Having an integration where data is automatically loaded from property management software into a product/service system reduces human error with data entry and makes for a more efficient process.

What are the requirements from our property management software for integration?

Although a product/service has an integration to the ODM's current property management software, there are technical requirements for the integration to be successful. The product/service may need access to a custom data set which could require communication between the vendor of the proposed product/service and the vendor of the property management software for a successful integration.

What technical type of integration is required?

Application Programming Interface (API) integrations, are integrations in which ODM's software connects to the vendor's back-end service to perform actions (over the Internet). API integrations are technically easy to accomplish and will enable the most flexibility in terms of future modifications, switching services or termination of service. API integrations can be with PMS systems, work order systems, resident apps, and most modern software applications. These integrations, in most cases, require the IoT devices to be connected to the Internet.

Software Development Kit (SDK) is an integration that requires a deeper level of technical expertise to implement, these are relevant especially when you want to control IoT devices directly and not over the Internet (e.g. Bluetooth).

Proprietary integrations are integrations that require ODM-specific software development to integrate. If a service is very sensitive to the software environment of the ODM, it may require special development efforts, causing much less flexibility moving forward in terms of modification, switching services or termination of service.

What technical requirements are needed?

It is vital for ODMs to have a clear understanding of their current infrastructure. This understanding combined with the technical requirements will help determine whether an Internet of things (IoT) solution can be implemented without any direct impact to the current infrastructure. Failure to review and understand the technical requirements could lead to unexpected costs or poor performance with the IoT solution.

What infrastructure is necessary to make this solution work?

It is important to consider how an IoT initiative will interact and intersect with existing or planned networking initiatives at the properties where IoT is being considered. How will the devices that are part of the solution under consideration connect to the Internet? Will this solution require new networking infrastructure to be installed, or can they leverage existing infrastructure?

How will house-owned devices interact with resident owned devices? Are they required to be on the same Wi-Fi network? If so, how is this handled? If there is a bulk/managed Wi-Fi solution in place, is the solution compatible?

How is the transition from resident to resident handled to ensure past residents no longer have access to, for example, smart locks? How easily can new residents connect with house-owned devices?

How many years has the service provider and/or hardware manufacturer been in business? Are they a profitable enterprise?

IoT devices have been around since the early 2000's. Up until several years ago, they were generally considered niche. Within a relatively short amount of time, there has been an explosion in value that these connected devices bring to all constituents. This exponential increase in interest has recently led to the property technology (PropTech) industry booming with startups. Approximately 10% of startups fail within the first year and about 90% of total startups fail. If an IoT vendor has been in business less than three years, research whether the vendor is working with other reputable ODMs before agreeing to any implementation. Factor in if the company funds its day to day operations from profits or from fundraising, as you might consider this an integral part of risk assessment in your decision-making.

What references does the manufacturer have?

References can be used as a factor in an ODMs comprehensive vetting process. The vendor may have a solution that meets your company's needs while promoting an exceptional ROI. However, if they have done business with other ODMs it would be ideal to verify how the solution is working within the industry. An ODM can gather information regarding the vendor's implementation, operations, customer service and support through other industry references.

What is the amount of capital supporting product/service research, development and marketing?

It is important to know if a startup company/service has sufficient capital to support the company's research, development, sales and marketing efforts.

Examine the level of venture capital interest and funding for a startup as a rough proxy for the vendor's potential "staying power". As a starting point, gather information through websites such as Crunchbase and LinkedIn for VC interest, leadership bios and technical staff backgrounds.

How many vendors provide this solution or a variant of the solution?

There is some risk associated with an IoT vendor who is the only provider offering a product/service. A product/service that has many providers in the field will provide less risk since there are multiple sources available to vet the product/service and the providers. Understanding the full spectrum of vendors and product offerings is essential to making a well-informed decision.

Does the manufacturer have any products/services that have duplicate products/services/pieces?

If products/services duplicate new product/services, determine if there is an opportunity to eliminate additional expenses for duplicate items.

Checklists for the Buyer

Does our current PM software integrate with the product/service?

If you use a specific PM software, you would want an IoT solution that has an integration into that PM software. If the IoT solution does not integrate with your specific PM software, and has no immediate plans for additional integrations, it may not be a suitable solution. Without the specific PM software integration, more resources could be required because processes and workflows may be manual.

What are you trying to solve for by implementing this product/service?

Understanding the full scope of the challenge(s) being faced helps not only in conversations with potential vendors, but also in the establishment of success criteria for the project.

How does this service/product support your goals/objectives?

Understanding how an IoT initiative fits within the broader set of corporate objectives helps determine the appropriate size of time and resource investments.

How does this service/product align with your company's core values?

It's good practice to verify any corporate initiative is in alignment with the core values of the organization.

How will you measure success?

Establishing success metrics and a plan for measurement is key to determine what expectations are being met, and where areas of adjustment may be necessary. Customer feedback is vital to the success of an IoT implementation. Customer feedback should be one of the metrics used to determine the success of a product/service.

What is the implementation speed?

The speed of an implementation is important to the overall success of the partnership. Slow implementation can result in lost ROI, poor customer experience and a reduction in operational efficiency. It would be ideal to have an agreed upon implementation schedule to keep all stakeholders on the same page.

What is the Return on Investment (ROI)?

Hard ROI refers to measurements which tend to be easy to quantify and can contribute to your organization's success. Quantifiable metrics such as hours saved and the end user/customer satisfaction rating can be used to determine the value of a product/service once implemented.

What customers and staff will be affected?

Customer experience should be considered when looking to implement a new product/service. A product/service that may appear to only affect back-end systems or office staff could also affect customer experience.

What resources (internal and external) will you need to launch the product?

It is important to understand the overall cost of a product/service which means understanding all soft costs and any additional resources that will be needed to launch/support the product/service.

What is the scope of onboarding?

To understand the resources needed, a comprehensive scope of onboarding is needed. Having the complete scope will help reduce disruptions.

Will you need any additional training for users?

Implementing a new product/service may require substantial training for office staff, residents/customers, or corporate employees. Identify if training is required for the product/service. If required, determine the proper audience, training schedule and length of the training. Also confirm if the training is included or an additional cost.

Will you need any additional hardware?

Hardware and software requirements should be identified during the vetting process. Adding hardware will have an impact on the capital costs for implementing an IoT system.

What potential disruptions may occur for users?

If an IoT system implementation will disrupt the normal activities of users/end users/customers, effective communication is a must. The type of disruption, who is affected and the duration of the disruption should be understood and communicated.

What on-going resources are needed to support the product/services?

After a successful implementation, the product/service may require resources for management and support. It should be determined which party will be responsible for operational management and support. If you will be responsible, it is important that appropriate training is given

Who oversees quality control within your organization?

It is a good idea to have a resource or group who oversees quality control in order to hold vendors and the company accountable.

Who owns the data that will be generated or inputted into this system?

The owner of customer data has a big responsibility to manage the data and have systems in place to prevent cyber security attacks. It is vital that the ODM understands if it will own the data or if the IoT provider/vendor will own the data. The owner of the data is accountable for the data, and it should be clearly defined in any contracts.

Who has license to use the data?

There are multiple stakeholders that may have an interest in the data including property owners, property developers, third-party managers, IoT platform providers and SaaS analytics providers. Those interests can be formalized by providing stakeholders with licenses to the data. The ODM must understand what rights it has to the raw data, and to the derived data created by the analytics provider. The ODM may wish to receive a perpetual worldwide license to use the data for any internal use within their organization, however, a company may wish to constrain the ability of the ODM to provide derived analytics data to a competitor.

If the IoT vendor owns the data, they may have a policy that allows for selling and/or sharing data to third-party vendors. An ODM would need to understand how the IoT vendor manages the data and what specific data will be collected and/or shared prior to signing an agreement.

If corporate owns the data, they will want to ensure that there is a policy in place on how the data is managed and clearly list what specific data is collected and shared to the IoT vendor.

If individual properties owns the data, they will want to ensure that there is a policy in place on how the data is managed and clearly list what specific data is collected and shared to the IoT vendor.

If there are others who owns the data, you will want to understand their data collection process and what specific data is collected.

Does this solution need to store customer data?

There are state regulations that dictate how customer data should be handled. If the solution needs to store data, you will need to understand what specific data is stored along with the policy regarding the data storage.

What data will this solution collect?

There are state regulations that dictate how customer data should be handled. If the solution needs to collect data, you will need to understand what specific data is collected along with the policy regarding the data collection.

Which stakeholders are responsible for compliance issues?

This could be corporate, vendors, individual properties, a service provider or anyone in between. It is extremely important to understand this nuance and have contractual language to support this.

Are both parties familiar with applicable consumer privacy protection laws?

The California Consumer Privacy Act (CCPA) has set specific requirements for companies that both collect and disseminate information about consumers with other organizations. It is important to understand how these requirements may affect you and to establish a plan for addressing them. More information about the CCPA law can be found at https://oag.ca.gov/privacy/ccpa.

The Nevada Privacy of Information Collected on the Internet from Consumers Act (NPICICA) has set specific requirements for companies that collect and monetize information about consumers by selling data to third parties. It is important to understand how these requirements may affect you and to establish a plan for addressing them.

New York is currently evaluating a new consumer privacy law (Senate Bill S5642), which has yet to be passed into law (as of Nov. 2019). It is important to monitor the progress of this bill (and be prepared should its ultimate contents affect your organization. Information about the law can be found at https://www.nysenate.gov/legislation/bills/2019/s5642.

Illinois and Washington both attempted to enact their own versions of consumer privacy protection with each ultimately not passing into law. It is uncertain yet whether amended versions may ultimately pass.

GDPR, or the General Data Protection Regulation is a set of privacy oriented laws that apply in the European Economic Area (EEA). If you conduct business or target customers in the EEA, you may be subject to GDPR.

How do I address device and software obsolescence?

Identify or ask for contractual language that handles hardware obsolescence and software upgrades.

What problem(s) are solved by this IoT installation?

Access: Holistic (building-wide) electronic access solves a plethora of problems in today's commercial real estate world. Package management, amenity access, enabling or disabling subletting and short-term rentals, multiple credentials per user, agentless leasing and self-tours, building security, instantaneous and remote credentialing and de-credentialing, and more.

Energy and Water: As urbanization increases, so will the scarcity and restriction of resources. Some states are already requiring the adoption of monitoring, metering and control mechanisms around energy and water usage and leak sensing.

Other: With today's labor shortage there is no efficiency in maintenance management that should be overlooked. Additionally, with the increased construction activity in the last decade, differentiation of products are increasingly challenging.

What value does the product or service create for the owners/community?

Access: The value created by electronic access is usually one of labor efficiencies, cost-savings, increased security and decreased liabilities. The value of single credentials for the entirety of a site is dependent on the site's size and demographic, as well as systems replaced. This may also reduce insurable risk.

Energy & Water: Connected wireless (IoT) devices enable reduced general spend, resource waste, improved reporting and maintenance, reduction of damages in the event of an incident, and cost of implementation.

Research also widely supports that both boomers and millennials will choose and often pay more for a green-focused building. This may also reduce insurable risk.

Other: Maintenance streamlining and enablement and preventative analytics and diagnostics can save as much as 40% in labor costs, in addition to inconvenience costs and possible loss of goodwill.

Additionally, many owners/communities are achieving rent lift in the short term by differentiating their properties with the above conveniences and enablement.

What value does the product or service create for the residents?

Access: Ease and convenience, as well as increased security, are front of mind as value propositions for today's savvy residents, guests and tenants, and enabled by holistic electronic access.

Energy & Water: Reduced spend (as much as 15%) and inconvenience in the event of an incident.

Life Safety: resident unit security, aging in place, environmental protection.

Does this product/service give your company a competitive advantage?

Every industry standard was first adopted as a competitive advantage. You may not need all that the IoT can provide today to get a competitive edge, but there's something for everyone. Whether you differentiate your property with smart apartments, create flex housing opportunities with an electronic access system, or manage energy spend better and market your carbon footprint reduction to eco-oriented investors, there's an edge for you.

Device Capabilities & Protocols

There is no one right answer on infrastructure needed for an IoT platform to function.

When considering the IoT technology for your implementation there are many factors to consider such as the power requirements for the devices, the distance the data will travel from the device to the network, how much data can be transferred at a time, whether communication will be wired or wireless, security and reliability of communication, the availability of hardware and its expected lifetime with software updates, and other considerations driven by the specific use case being addressed. The goal of this section is to define and lay out differences between options so operators and owners can choose the overall solution that matches the cost, risk and performance their firm is seeking.

Before diving into individual sections, below is a quick summary of some of the most common IoT communication protocols:

RFID/near field communication (NFC): RFID/NFC is primarily used to identify a person or thing in proximity; the best example for this application are access control systems. The data amount in identifying something is small and the range and power needed are so small the devices do not need to be powered. The implementations of these vary greatly and because it involves access control security in duplicating these identification devices, is important to understand.

Bluetooth/BLE, ZigBee, and Z-Wave: These are common standards for home automation devices such as light switches and thermostats. They are designed for devices in a building to communicate with property owners, renters, and automation systems. The uses of these standards vary, but most IoT device implementations use 'mesh networks' which is where every device acts as a repeater enabling connections across thousands of square feet of devices to connect to the Internet through a hub. How these hubs are connected to the Internet should be taken into account for reliability and data privacy. The notable differences currently between these standards are the number and types of devices using them, along with the interoperability of those devices. In commercial IoT, BLE has primarily been used for access control with tens of manufacturers using them with interoperability at a minimum. ZigBee has been implemented in hundreds of products with interoperability not as a requirement. Z-Wave has thousands of devices that are all required to be interoperable in order to be certified. Devices using these standards may be powered or battery powered, but battery powered life can vary greatly on application and a property that uses them should have a plan for when they are replacing the batteries based on the needs of the devices.

Wi-Fi: Wi-Fi is used for transmitting large amount data. Interoperability between Wi-Fi devices is generally good, but because of the higher data rate, these devices are rarely battery powered. Wi-Fi also is generally easy to attack, so extra caution needs to be taken to secure the communication from devices to hubs/routers.

It is also useful to note that the focus of this paper is on IoT communication protocols, which tend be local communication within a building or community. Below is a quick reference for how to think through the total connectivity picture from the residence, to the building, through the community and finally up to the Internet/cloud:

- Local communication (i.e. within a housing unit, building or community):
  - Wired: Ethernet, X10, UPB
  - Wireless: Wi-Fi, Bluetooth, Z-Wave, Zigbee/Thread, LoRaWAN
- External communication (i.e. from a building or community to the cloud):
  - Wired: Broadband (fiber, DSL, copper lines)
  - Wireless: Wi-Fi, Cellular (4G, 5G, satellite, Low-power wide-area networks (LPWAN) such as SigFox, LORA or NB-IOT

Range and Bandwidth

For any one method or standard chosen for connectivity of devices, there are two primary traits: bandwidth (the speed in which data can move) and range (the distance that data can move across). Generally speaking, the more data you want to move and/or the farther away the device is, the more power it will require. The primary connectivity standards can be found in the following illustration:

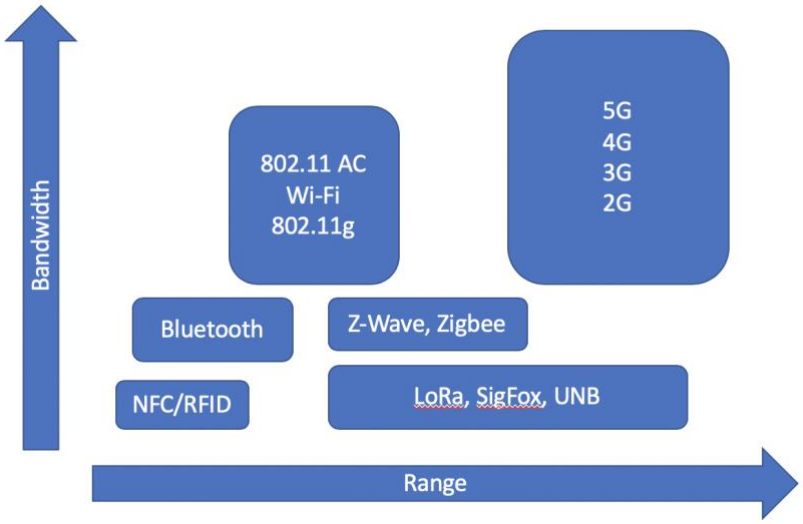

FIGURE 1 BANDWIDTH AND RANGE

In this graph it is possible to see the extreme differences of standards from RFID which is meant to move a couple of ID numbers a couple of inches with no battery and purchased for dollars a pieces, to cellular moving high speed data over miles with a battery that has to be charged every night and monthly subscriptions to attach to cell towers.

Connectivity is also affected by whether devices repeat signals or not. Point to point (P-P) or point to multi-point (P-MP) protocols are only effective over the distance they can transmit, such as how far your mobile phone is from a tower or a Wi-Fi device from a router. Mesh-based protocols such as Z-Wave or Zigbee use each other to relay signals so the messages are relayed by other devices, enabling devices to be further from each other and ensuring more connectivity options as more devices are present.

There are other factors that can affect cost outside of these technological definitions primarily affected by how adopted or mature a technology is which can primarily be judged by the number of devices designed for a set standard. There are also other factors that affect connectivity speed and distance based on topology and if the wireless spectrum is licensed (i.e. only approved traffic can use that bandwidth, which can help improve range since there is less interference) or unlicensed.

If you are considering wired protocols, such as Ethernet, as your IoT connectivity solution, remember that you will still likely need to connect to part of a wireless protocol to speak to all of the devices. Wired solutions are inherently more secure than wireless (you have to physically connect versus sniff a signal), though some wireless protocols use encryption to overcome this. Wired solutions also have a literal cost per inch.

For most protocols, outside of cellular, you will need to use a wired protocol, such as fiber, to haul data to the cloud at some point in the communication path. Also, for simplification of terminology, all wireless networks require some type of hub/gateway to transmit and receive wireless signals.

FIGURE 2 INFRASTRUCTURE COMMUNICATIONS

Please see the appendix for a chart that lists specifications for all known protocols.

Power Requirements

The choice of the wireless standard will affect your power infrastructure because faster data rates require more power. Power infrastructure comes in two general forms: hardwired or battery. Each form comes with pros and cons depending on the use case and existing power options.

Hardwired power options can come in multiple forms including wall power, Power over Ethernet (PoE), or power from what is being controlled such as a thermostat being powered off of the HVAC system. These systems do not require battery changes, but you must run cable throughout the building to convenient, logical places where the devices will be placed. Most IoT devices will be DC powered, so a transformer will be required to step the AC voltage down to DC. Depending on design, these transformers might make it difficult for the device's plug or power supply to use both outlets. Newer receptacles that also have one or two USB outlets are viable DC power options for IoT devices that residents bring or interact with (e.g. voice assistants) but are not ideal for devices you want to conceal (e.g. hubs).

Another hardwired power option, PoE, describes any several standards or systems, which pass electric power along with data on twisted pair Ethernet cabling, to allow a single cable to provide both data connection and electric power to devices. A powered device (PD) is any device powered by PoE, thus consuming energy. A few examples include wireless access points, VoIP phones and IP cameras. PoE can provide a reliable network signal but it requires newer network cables and equipment. Retrofitting existing Ethernet equipment to be PoE compatible may not be cost advantageous over simply using an AC or battery-powered device with a wireless protocol.

The pros of hardwired power include it being the most cost-effective source of power (watts per dollar spent) and it is best for high power devices, such as cameras and network infrastructure, mechanical controllers (such as value shut off), and critical infrastructure including access control systems. The cons of hardwired power include the fact that it can have a high CapEx cost when you have to run new wire, it doesn't allow for a lot of flexibility in device placement (a power source needs to be close by), and critical devices need to have power backup options, such as batteries or backup standby generators, or an offline contingency plan.

Battery power options focus on DC batteries of various sizes, voltages and amperage rating. Battery life will vary based on use, so battery powered devices should have indicators, preferably on the device and in any related app, when their battery is running low (ideally, the device indicates at several points as the battery life degrades). It is important to make sure batteries that will be needed to support deployed devices are readily available for purchase and/or in-stock with on-site staff.

One pro of batteries allows devices to be placed in areas where it is not as easy, desirable and/or cost-effective to get hardwired power. Batteries also allow for simpler device portability (i.e. a battery powered light switch can easily be moved to the most useful location for a resident). Cons of battery powered devices are that the batteries require a regular replacement cycle, and the cycle can vary based on device usage (i.e. a sensor which reports its data to the network every five minutes will consume much more power than a sensor that is configured to report its data once every 12 hours).

Batteries performance can also be somewhat finicky, being affected by environmental conditions (i.e. cold environments), brand and types (i.e. NiMH vs LiON).

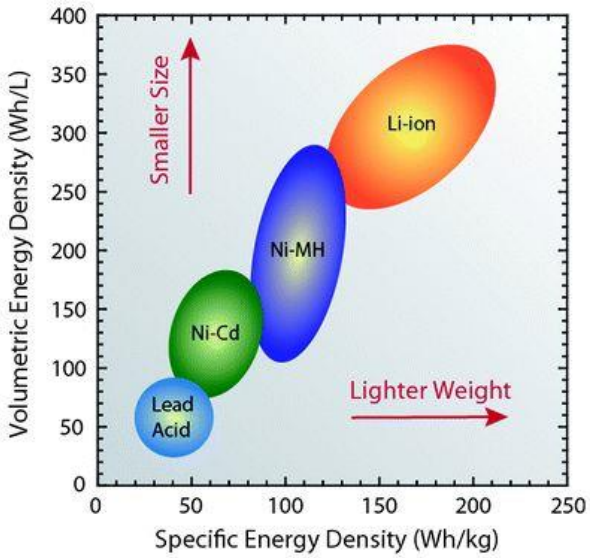

FIGURE 3 BATTERY TECHNOLOGY & ENERGY[i]

Interoperability

Interoperability between devices can happen at the local level if all the devices use the same communication protocol and/or speak to a hub/gateway that can speak multiple protocols. They can also happen at the cloud level by integrating cloud services between groups of devices. Generally speaking, the closer the integration is to the local level, the faster it potentially can be, but you also might need more robust hardware at more points to analyze the data, so the right answer depends on how sensitive you are to making decisions in milliseconds or seconds in a use case.

Integrations at the cloud level also allow for different software systems to integrate, such as a connection between an IoT platform and a property management system (PMS) or leasing CRM.

Integrations between multiple systems can extend the flexibility of any hardware deployed by allowing for more use cases to be supported (i.e. an IoT platform that not only helps staff and residents in long-term rentals, but also when units are rented out for short-term rentals, or a platform that integrates in external security cameras so residents feel more safe about their community). Cloud integrations can range from simple to complex, but all of them require regular updates to make sure they remain secure and reliable.

Key Learnings

When comparing infrastructure and device communication capabilities, here are the top questions buyers need to ask:

- What is the range of this communication protocol? Is it measured in centimeters, meters or kilometers?
- What is the inherent security of this communication protocol?
- Who provides firmware updates? How long are they available for?
- Do the devices have built in security or does this need to be administered by your IT team?
- What devices support this communication protocol? Is this protocol something your IT team needs to manage?
- What is the commercial availability of this product?
- Is this protocol closed or open-based? How is the technology licensed?
- What are the differences between proprietary versus standards-based communication protocols?
- What are the business implications of choosing a proprietary solution over a standards-based solution?
- How does this communication protocol scale? Can it handle 10 devices, 10000 devices?
- Do you care if resident data is sold?

New Builds & Retrofit Installations

Commercial Real Estate is already feeling the impact of IoT applications. From access, energy and water management in small to mid-size commercial and retail, to complex connected control and building management systems in multifamily and student housing, the opportunities to positively impact net operating income are innumerable.

Here are some considerations dependent upon when you engage.

Infrastructure

Construction Type	Considerations
New Construction (Greenfield)	• Building/campus type • Focus on optimizing network • Power requirements • Focus on GC schedule • Communications/ICT requirements • Focus on coordination with on-site telecom systems. • Wired/wireless considerations • Focus on materials and installation of wired networks while walls are open • Evaluation matrix for different technologies - what is effective vs. ineffective? • In-unit hub vs. enterprise network (ISP connectivity provided by property, i.e. open port on modem) • Focus on long(er)-term ownership goals
Retrofit (Brownfield)	• Building/campus type • Focus on advanced network technologies • Power requirements • Focus on available sources • Communications/ICT requirements • Focus on where infrastructure can be placed and adapting to existing networks • Wired/wireless considerations

	• Focus on cost optimization in connecting older or isolated buildings with wireless methods often less costly than running wires • Evaluation matrix for different technologies - what is effective vs. ineffective? • In-unit hub vs. enterprise network (ISP connectivity provided by property, i.e. open port on modem) • Focus on solving property specific pain points

Installation

Construction Type	Considerations
New Construction (Greenfield)	• Usually GC-dependent but still requires active PM • Often, but not always, consistent oversight
Retrofit (Brownfield)	• Inconsistent building materials and standards (after years of repairs and upgrades on turns, different units and parts of the property will be different) • Common area/access system coordination - new access system must be fully functional and accessible for all residents/tenants on day one • Current systems and installations below current code - neutral wires, aluminum wiring, fire codes, c-wires, etc.

Regulatory Considerations

Construction Type	Considerations
New Construction (Greenfield)	• Usually GC-managed but still requires active PM and general knowledge for compliance • Timing dependent, replacement of devices or network could trigger retrofit considerations for licensing and compliance • Occupancy permits will be granted only if all federal, state and municipal codes are followed properly, including fire codes and ADA requirements
Retrofit (Brownfield)	• Installs often beyond maintenance scope of skills (especially with current labor shortage) • Consider solutions that engage certified installers and for consultancies consider • Building Performance Institute (BPI) multifamily analyst • Certified Energy Manager (CEM) • Licensed mechanical engineer • Licensed electrical engineer • Low voltage license • Line voltage license • HVAC license • Locks license • Plumbing/gas license • Bicsi certification • Energy modeler • General contractor requirements • Certified Green Building Professional • Home Energy Rating System (HERS) rater • Retro-commissioning agent • Renewable energy expert • Licensed architect • Financial analyst

Project Management

Construction Type	Considerations
New Construction (Greenfield)	• Often (not always) GC • Extended construction schedule • Trades protection of scope • Deviation from plans • Power and network not necessarily available or available as scheduled • Hardware and site security/loss prevention • Installation by trade schedules - not unit completion/geography • Inspections/COI compliance
Retrofit (Brownfield)	• Identify onsite point of contact/decision maker • Coordinate w/PoC product delivery schedule • Coordinate w/PoC installation schedule • Minimize resident disruption • Maximize return on investment

Systems

Construction Type	Considerations
New Construction (Greenfield)	• PMS • Focus on choosing integrated products at outset. If merchant builder, coordinate with buyer as available • BMS • Focus on optimizing systems with integrated IoT where possible • Network • Focus on maximizing network offering for future capabilities • HVAC • Focus on integrating IoT for whole building systems • Access • Focus on optimizing efficiencies with building-wide integrated electronic access systems • Energy • Focus on innovative and advanced energy offerings including solar, advanced demand response, and whole building intelligence systems • Water • Focus on water management and control during construction, integration into deep infrastructure and advanced sensing and control capabilities • Other: well building
Retrofit (Brownfield)	• PMS • Focus on choosing a product(s) integrated with current system • BMS • Focus on whether legacy systems have integration capabilities or IoT expansions • Network

	• Focus on maximizing network offering for future capabilities • Innovative install • HVAC • Focus on whether legacy systems have integration capabilities or IoT expansions • Access • Focus on whether legacy systems have integration capabilities or IoT expansions • Energy • Focus on innovative and advanced energy offerings including solar, advanced demand response and whole building intelligence systems. • Water • Focus on cost-effective integrations into deep infrastructure, advanced sensing, alerts and control capabilities. • Other: Aesthetics challenges

Resident / Tenant Impact

Construction Type	Considerations
New Construction (Greenfield)	• Resident/tenant legal requirements • Credential strategy/policy • Resident/tenant training/engagement strategy • Opt-in/opt-out strategy/policy • Lease up/marketing plan
Retrofit (Brownfield)	• Resident/tenant notice requirements • Resident/tenant legal requirements • Credential replacement strategy • Access system impacts • Resident/tenant training/engagement strategy • Opt-in/opt-out Strategy/policy

	• Marketing plan

Costs & Financing

Construction Type	Considerations
New Construction (Greenfield)	• Averaging 1-1.5% of new development budget for fully networked intelligent building • If late specification of intelligent or smart system (change order), practically converts to retrofit • Are there local, state, and federal incentives or subsidies available for smart new development (focus on energy)? • Are there insurance subsidies or requirements for smart new development?
Retrofit (Brownfield)	• Averaging 10-15% more spend (primarily labor) for fully networked intelligent building than new development • What are the local, state and federal incentives or subsidies available for retrofits? • Are there insurance subsidies or requirements available for retrofits? • What are the trends and higher-than-average utility expenses for the portfolio? • What are the properties' partnership agreements, loan agreements and audited financials for refinancing or recapitalization potential? • What are the properties' regulatory agreements or requirements? • Who are the point staff to present financial analyses for approvals? • Are there complete capital needs assessments to estimate retrofit costs for financial analysis?

Solution Optimization

Construction Type	Considerations
New Construction (Greenfield)	• 75% of building costs are operational • GC incentivized to minimize installation costs, limiting utility and effectiveness of system • Early scope definition and requirements are critical
Retrofit (Brownfield)	• Consider curb appeal when choosing components • Consider submetering options so owner does not cover all bills • Reduce utility costs to reduce building costs or decrease renting speed. • Take into account cost and efficiency of all maintenance • Review upcoming equipment replacement timelines and potential earlier paybacks • See if recapitalization is an option

Security Considerations

Security of IoT devices has many layers. A system can be vulnerable at the device level, the wireless transmission, the hub/access point, in cloud storing and processing the data or the mobile app. Every level can have different standards such as S2 for Z-Wave communications, AES128 for cloud communications, or NIST for cloud servers. Security is difficult for a property to determine without an expert that can perform tests or certifications such as penetration testing or SOC-2 compliance. Data privacy, which is how data is analyzed and/or sold to third parties, should be considered as part of overall communication security.

FIGURE 4 COMMUNICATIONS PROCESS[ii]

Device and hub/gateway security starts at the physical level. If the hub is inside the resident unit, the hub can potentially be compromised by the resident simply by plugging in a device that could hack the hub. The next level is the software layer, specifically the firmware level. No system is completely impenetrable or up to date, and thus firmware updates provide the first line of defense in making sure that a device's known flaws are regularly fixed. After firmware, a device's vulnerability is a strong result of its communication protocol. Communication protocols can have built in security (i.e. Z-Wave and Zigbee use AES-128 symmetric encryption, the same encryption used by banks and government), which is generally effective and does not require any elaborate setup, or be open and allow for security (such as Wi-Fi using WEP or WPA), which requires someone to administer the security protocol amongst all devices on a regular basis. Wired connection devices inherently have a more secure connection than an open wireless connection because a device must physically connect to that network, but they are still vulnerable to attacks from outside the network (such as DDoS attacks).

When connecting local devices and hubs to the internet, the general way to protect this information is to encrypt it. Cellular networks encrypt their communication back to radio towers and then typically use encryption between the tower and the Internet. Broadband options can encrypt the data between the two points using a Virtual Private Network (VPN).

Once in the cloud, it is important to make sure that your data remains secure and is used properly (data privacy). An easy way to understand how a company makes sure its data remains secure is to understand its process and tools to access that data. SOC-II Type 2 certification is an accepted standard designed to help measure how well a given service organization conducts and regulates its information, specifically in regards to storing customer data in the cloud as it requires companies to establish and follow strict information security policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of customer data. As with any certification, SOC II compliance is an independent CPA certification that helps provide peace of mind for organizations when they engage third-party vendors, but certifications are only one step. Specifically related to SOC-II, make sure that the cloud provider not only has the certification, but that the processes your vendor and staff use upholds the goal of that certification.

Data privacy can have many forms, from who can see what data about a user of a property when they are there, to how securely the information is stored, to if and how data is anonymized or privatized when the user of a property is no longer there. There are many emerging standards around data privacy such as GDPR in Europe to CCPA in California. At a minimum, a property should understand who has access to what data when, how it is used and if the company storing the data is in compliance or working on compliance with these emerging standards.

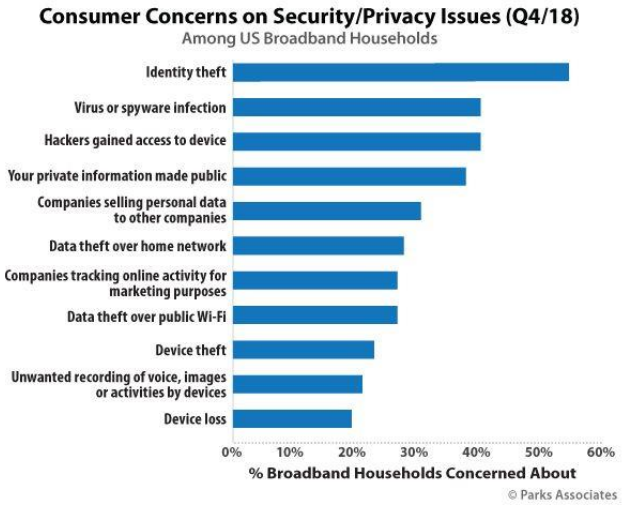

FIGURE 5 CONSUMER PRIVACY CONSIDERATIONS[iii]

Appendix

Z-Wave vs Zigbee/Thread

Key Component	Considerations
Security	Antennas for radio waves are not commonly found in consumer electronics, and thus not as easy to detect. Both protocols use AES-128 symmetric encryption, the same encryption used by banks and government. This sort of encryption is simple and effective and does not require any elaborate setup. Z-Waves new S2 framework, available in 500 series and above chipsets, further reduces security risks and power consumption.
Interference and Reliability	Z-Wave operates in the 908 MHz frequency band. It does not have to deal with the often crowded 2.4 GHz band that ZigBee uses. Crowded frequencies can cause interference which will result in lost or unreliable signals. Z-Wave (100ft) devices have more range than ZigBee (40ft), so you can expect fewer reliability problems stemming from range issues.
Interoperability	Since ZigBee is an open source protocol, any manufacturer can use ZigBee for free and when they do so, they often use software that is incompatible with another brand. Z-Wave, since it is proprietary and only made by, or under license to, Sigma Designs, is made so that it can “talk” to any other Z-Wave component.

Bluetooth/BLE

Key Component	Considerations
Security	As a common wireless technology, it is relatively easy to discover Bluetooth networks. There are some security measures available, but these can vary between devices/brands. This is dependent on residents keeping their controllers (phones) and Bluetooth devices up to date.
Interference and Reliability	30ft range Bluetooth/BLE operates within the 2.4Ghz band that can be congested with traffic from Wi-Fi and other devices.
Interoperability	There is decent interoperability between relatively newer versions, though this can also vary between devices/brands.

Wi-Fi

Key Component	Considerations
Security	It is relatively easy to discover Wi-Fi networks. Encryption protocols, such as WPA2, and VPN are available, but must be properly setup and maintained. High level of risk in keeping different modem/router/ISP combinations with up to date software/firmware. Difficulty grows exponentially when you rely on a resident versus a dedicated IT staff.

Interference and Reliability	Up to 150ft range indoors. Wi-Fi works on legacy 2.4Ghz (crowded) and 5Ghz frequencies. All Wi-Fi devices in one area are communicating with one router, if the number of users is too large, or the users are transmitting and receiving too much data, the router gets overwhelmed and cannot transmit data fast enough.
Interoperability	There is good interoperability between devices and hubs that run different versions.

Cellular

Key Component	Considerations
Security	Cellular is generally secure as you need a carrier license from a government authority to purchase equipment in order to access cellular networks. Private lines and VPN are available
Interference and Reliability	Generally two to 80 miles from a tower depending on usage and network generation
Interoperability	Devices are generally compatible on only one cellular network (i.e. AT&T or Verizon) in the US.

LPWAN/LoRaWAN/SIGFOX

Key Component	Considerations
Security	128-bit separate application and transport layer security keys for all devices
Interference and Reliability	Depends on implementation. One gateway may be sufficient for a 10-story residential building or a 10-acre community, but numerous factors interfere
Interoperability	For security purposes, LPWAN devices are generally pre-configured to operate on a specific network

The chart on the following pages lists all the above protocols with more details on these attributes. The listed wired standards are all point-to-point and require switching gear to connect multiple devices to a network.

Protocol	Speed kbps / range ft	Power	Maturity/ Devices	Frequency, Examples and Other Information
RFID LF	9.6kpbs / 0.1ft - 0.3ft P-P	No battery or 10 year lithium	Very Mature / Thousands of Devices	0.125MHz protocol primarily used for one-way access control protocols like Prox Cards
RFID HF / NFC	424kpbs/ 0.1ft to 4ft P-P	No battery or 10 year lithium	Very Mature / Thousands of Devices	13.56MHz protocol primarily used for more secure two-way access control protocols like MIFARE Classic and MIFARE, DES FIRE
BLE 4.X	1,000 kpbs / 30ft indoor P-P	Battery can give months to years	Very Mature / Thousands of Devices	2,400MHz protocol primarily point to point used for applications like unlocking doors
BLE 5.X	2,000 kbps / 120ft indoor P-P or Mesh	Battery can give months to years	Early Maturity / Few Devices	2,400MHz protocol with BLE 4.X abilities plus ability to mesh devices together for building communication
Z-Wave V4 300 Series	40kbps / 75ft indoor Mesh	Battery can give months to years	Late Maturity / Hundreds of Devices	915MHz protocol connecting thermostats, light switches, motion sensors, door locks, etc., requiring full interoperability of all devices
Z-Wave V6 500 Series	100kbps / 10 ft indoor Mesh	Battery can give months to years	Very Mature / Thousands of Devices	915MHz protocol connecting thermostats, light switches, motion sensors, door locks, etc., requiring full interoperability of all devices
Z-Wave V7 700 Series	100kbps / 150ft indoor Mesh	Battery gives months to 10 years	Early Maturity / Few Devices	915MHz protocol connecting thermostats, light switches, motion sensors, door locks, etc., requiring full interoperability of all devices

ZigBee HA 1.2	250kbps / 75ft indoor Mesh	Battery can give months to years	Very Mature / Hundreds of Devices	2,400MHz protocol connecting thermostats, light switches, motion sensors, door locks, etc., requiring compliance with the standard but with select features interoperable
ZigBee 3.0	250kbps / 150ft indoor Mesh	Battery can give months to years	Early Maturity / Few Devices	2,400MHz protocol connecting thermostats, light switches, motion sensors, door locks, etc., focused on interoperability of devices
ZigBee Light Link	250kbps / 75ft indoor Mesh	Primarily Line Powered	Very Mature / Few Devices	2,400MHz protocol for lighting devices including Phillips Hue
ZigBee Smart Energy	250kbps / 75ft indoor Mesh	Primarily Line Powered	Very Mature / Few Devices	2,400MHz protocol focused on smart meters and demand response applications for energy companies
BlueTooth V4.X	1,000kpbs / 30ft indoor P-P	Battery can give days	Very Mature / Thousands of Devices	2,400MHz protocol used for applications like wireless headsets
BlueTooth V5.X	2,000kpbs / 120ft indoor P-P or mesh	Battery can give days	Early Maturity / Few Devices	2,400MHz protocol used for applications like wireless headsets
WiFi 3 802.11g	54,000kpbs / 150ft	Battery can give hours to weeks	Late Maturity / Thousands of Devices	2,400MHz protocol used for connecting thermostats, door locks, etc., along with providing internet access.
WiFi 4 802.11n	600,000kbps/ 150ft, 50ft at 5,000MHz	Battery can give hours to weeks	Late Maturity / Thousands of Devices	2,400MHz / 5,000MHz protocol used for connecting thermostats, door locks, etc., along with providing internet access.
WiFi 5 802.11ac	1,300,000 kpbs 150ft, 50ft at 5,000MHz	Battery can give hours to weeks	Very Mature / Thousands of Devices	2,400MHz / 5,000MHz protocol used for connecting thermostats, door locks, etc., along with providing Internet access

WiFi 6 802.11ax	10,000,000 kpbs /150ft, 50ft at 5,000MHz	Battery can give hours to weeks	Early Maturity / Few Devices	2,400MHz / 5,000MHz protocol used for connecting thermostats, door locks, etc., along with providing Internet access
6LoWPAN Thread	250kbps / 75ft indoor Mesh	Battery can give months to years	Early Maturity / Few Devices	2,400MHz protocol connecting thermostats, light switches, motion sensors, door locks, etc., focused on interoperability of devices
LoRa	27kbps / 50,000ft	Battery can give months to years	Early Maturity / Few Devices	433MHz protocol connecting thermostats, light switches, motion sensors, door locks, etc.
SigFox	0.1kbps / 150,000ft	Battery can give months to years	Early Maturity / Few Devices	915MHz protocol connecting wireless sensors over larger areas
Cellular 3G W-CDMA / UMTS	8,000,000 kbps / 5,000ft to 50,000ft	Battery can give hours to days	Late Maturity / Thousands of Devices	600MHz to 6,000MHz primarily connecting mobile phones
Cellular 4G LTE FDD / LTE TDD	15,000,000 kbps / 1,000ft to 5,000 ft	Battery can give hours to days	Very Mature / Thousands of Devices	600MHz to 6,000MHz connecting mobile phone and some wired IoT devices
Cellular 5G NR	150,000,000 kbps / 50ft to 50,000 ft	Battery can give hours to days	Early Maturity / Few Devices	600MHz to 100,000MHz connecting mobile phones, IoT devices, cars, drones, etc.
1000Base-T 802.3ab CAT5	1,000,000 kbps / 328ft P-P	Primarily line powered	Late Maturity / Thousands of Devices	Commonly known as ethernet running at 100MHz

10GBase-T 802.3.an CAT5e	1,000,000 kbps / 328ft P-P	Primarily line powered	Very Mature / Thousands of Devices	Commonly known as ethernet CAT5, runs at 100MHz
10GBase-T 802.3.an CAT6	10,000,000 kbps / 328ft P-P	Primarily line powered	Very Mature / Thousands of Devices	Commonly known as ethernet CAT6, runs at 250MHz. 10Gbps runs are limited to 150ft
10GBase-T 802.3.an CAT6a	10,000,000 kbps / 328ft P-P	Primarily line powered	Very Mature / Thousands of Devices	Commonly known as ethernet CAT6, runs at 500MHz
1000Base-SX Fiber 802.3z	1,000,000 kbps / 1.500ft P-P	Primarily line powered	Very Mature / Thousands of Devices	Commonly known as single-mode fiber and runs at 850nm wavelength used for moving large amounts of data large distances
1000Base-LX Fiber 802.3z	1,000,000 kbps / 20,000ft P-P	Primarily line powered	Very Mature / Thousands of Devices	Commonly known as multi-mode fiber and runs at 1,310nm wavelength used for moving large amounts of data large distances

[i] Epectec.com https://www.epectec.com/batteries/cell-comparison.html
[ii] IOT-analytics.com https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/
[iii] Parks Associates https://www.parksassociates.com/blog/article/nest--confronts-smart-home-security--